Invent. math. 105, 347–373 (1991)

Inventiones mathematicae

Rational points on K3 surfaces: A new canonical height

Joseph H. Silverman *

Brown University, Box 1917, Providence, RI 02912, USA

Oblatum 3-IX-1990 & 26-XI-1990

Introduction

A fundamental tenet of Diophantine Geometry is that the geometric properties of an algebraic variety should determine its basic arithmetic properties. This is certainly true for curves, where the sign of the Euler characteristic of C determines whether the set of rational points on C is finite ($\chi(C)<0$), a finitely generated group ($\chi(C)=0$), or parametrizable ($\chi(C)>0$). For higher dimensional varieties there are some precise conjectures due to Bombieri, Lang, and Vojta [15] which predict when the rational points on a variety should be finite or degenerate (i.e. not Zariski dense), and some conjectures of Manin et al. [2, 5] on the distribution of rational points in those cases when they are Zariski dense. But except for abelian varieties, their subvarieties, and some Fano varieties (varieties for which the anticanonical bundle is ample), there are very few general theorems.

In this paper we will study the rational points on a certain class of K3 surfaces defined over a number field K. The moduli space of marked algebraic K3 surfaces is a countable union of 19 dimensional quasi-projective varieties. We are going to look at the 18 dimensional family studied by Wehler [17]. Wehler's family consists of K3 surfaces S whose automorphism group $\mathrm{Aut}(S)$ contains a subgroup $\mathscr{A}$ isomorphic to the free product $\mathbb{Z}_2 * \mathbb{Z}_2$ of two cyclic groups of order 2. We will use the geometric information provided by this infinite automorphism group to study the K-rational points on S.

For any point $P \in S$, we can look at the orbit of P under the action of $\mathscr{A}$,

$$\mathscr{C}=\mathscr{C}(P)=\{\phi P : \phi \in \mathscr{A}\}.$$

We call such an orbit a *chain*. Then the study of the K-rational points on S is divided into two parts: (i) Describe the points in a given chain $\mathscr{C} \subset S(K)$. (ii) Describe the collection of chains in $S(K)$.

The chains themselves naturally separate into two sorts, those with finitely many elements and those with infinitely many elements. This is analogous to the points on an abelian variety, which generate either finite or infinite sub-

* Research partially supported by NSF DMS-8842154 and a Sloan Foundation Fellowship

groups. Our first main result says that $S(K)$ contains only finitely many finite chains. (Just as an abelian variety contains only finitely many points of finite order defined over any given number field.) Our second main result, which we describe more precisely below, gives the counting function for the number of points in a chain with height less than a given bound.

A basic tool in the study of Diophantine equations is the theory of height functions. On abelian varieties Néron and Tate developed a theory of canonical heights which have especially nice transformation properties. If A is an abelian variety and if $D \in \mathrm{Pic}(A)$ is a symmetric divisor class, then the canonical height $\hat{h}_D$ interacts with the group law on A via the formula $\hat{h}_D(nP) = n^2 \hat{h}_D(P)$. (See, e.g. [9].) In a similar way we will develop a theory of canonical heights on our K3 surface S which transforms canonically relative to the automorphism group $\mathscr{A}$. More precisely, we will prove the existence of two canonical heights $\hat{h}^+$ and $\hat{h}^-$ on S which satisfy the transformation formulas

$$\hat{h}^+(\phi P) = (2+\sqrt{3})^{\ell(\phi)} \hat{h}^{\chi(\phi)}(P)$$

and

$$\hat{h}^-(\phi P) = (2+\sqrt{3})^{-\ell(\phi)} \hat{h}^{-\chi(\phi)}(P)$$

for every $\phi \in \mathscr{A}$. Here $\ell(\phi) \in \mathbb{Z}$ and $\chi(\phi) \in \{\pm 1\}$ are functions that we will precisely describe in Sect. 2. The functions $\hat{h}^\pm$ have many properties similar to those enjoyed by canonical heights on abelian varieties. For example, $\hat{h}^\pm(P) \geqq 0$ for all points $P \in S(\bar{K})$, and

$$\hat{h}^+(P) = 0 \Leftrightarrow \hat{h}^-(P) = 0 \Leftrightarrow \mathscr{C}(P) \text{ is finite.}$$

In order to draw arithmetic conclusions, one ultimately must relate everything to heights relative to a projective embedding. So we also show that the function

$$\hat{h} = \tfrac{1}{2}(\sqrt{3}-1)(\hat{h}^+ + \hat{h}^-)$$

is a Weil height corresponding to a very ample divisor. These and other properties of the canonical heights $\hat{h}^+$ and $\hat{h}^-$ are described in Theorem 1.1 in Sect. 1.

From the transformation formulas it is clear that the product $\hat{h}^+ \hat{h}^-$ takes the same value at P and at ϕP for any automorphism $\phi \in \mathscr{A}$. This allows us to define a canonical height of a chain $\hat{H}(\mathscr{C}) = \hat{h}^+(P)\hat{h}^-(P)$ which can be calculated by choosing any point P in the chain. Notice that $\hat{H}(\mathscr{C}) = 0$ if and only if the chain $\mathscr{C}$ is finite; it is this observation which ultimately enables us to prove that $S(K)$ contains only finitely many finite chains. In the case that $\hat{H}(\mathscr{C}) > 0$, its value determines the arithmetic complexity of the chain. For example, $\hat{H}(\mathscr{C})$ appears in the following counting formula which we will prove in Sect. 4:

$$\#\{P \in \mathscr{C} : \hat{h}(P) \leqq B\} = \kappa \log(B^2/\hat{H}(\mathscr{C})) + O(1) \qquad \text{as } B \to \infty.$$

Here $\kappa = \kappa(\mathscr{C}) = 0.3796\ldots$ or $0.7593\ldots$ depending on whether the chain $\mathscr{C}$ is one or two sided, and the big-O constant is absolute (it is even independent of the surface S.)

The organization of this paper is as follows. We begin in Sect. 1 by setting notation and stating our main results. We also raise several questions for our K3 surfaces which are analogous to theorems and conjectures on abelian varieties. Section 2 is devoted to geometry. We determine how the automorphisms in $\mathscr{A}$ act on Pic(S), and use this information to draw various conclusions about chains, ample and effective divisors, and curves of low genus. In Sect. 3 we prove the existence and basic properties of the canonical height, and in Sect. 4 we apply our results to bound the number of finite chains and count the number of points in infinite chains. To illustrate our general theory, we present a numerical example in Sect. 5, including a list of the first few points in a particular infinite chain. This list has an unexpected arithmetic property. In the final section we show how a strong form of Vojta's conjecture [15] can be used to explain this property.

1 Notation and the main theorems

In this section we will state our main results and raise a number of interesting questions meriting further study. We begin by setting some notation which will remain fixed throughout this paper.

K a number field.

S/K a smooth surface contained in $\mathbb{P}^2 \times \mathbb{P}^2$ given by the intersection of two effective divisors, one of type (1, 1) and one of type (2, 2). In other words, S is the locus described by two equations of the form

$$\sum_{i,j=1}^{3} a_{ij} x_i y_j = \sum_{i,j,k,l=1}^{3} b_{ijkl} x_i x_j y_k y_l = 0$$

p_1, p_2 the projections $p_j\colon S \to \mathbb{P}^2$ induced by the natural projections

$$p_j\colon \mathbb{P}^2 \times \mathbb{P}^2 \to \mathbb{P}^2.$$

D_1, D_2 $\in \operatorname{Pic}(S)$, where D_j is the divisor class of $p_j^* H$, where $H \in \operatorname{Pic}(\mathbb{P}^2)$ is a hyperplane section.

σ_1, σ_2 $\in \operatorname{Aut}(S)$, where σ_j is the involution of S induced by the double cover $p_j\colon S \to \mathbb{P}^2$.

$\mathscr{A}$ $\subset \operatorname{Aut}(S)$. The subgroup of $\operatorname{Aut}(S)$ generated by σ_1 and σ_2.

α $= 2 + \sqrt{3}$.

E^+, E^- $\in \operatorname{Pic}(S) \otimes \mathbb{R}$, given by the formulas

$$E^+ = \alpha D_1 - D_2, \qquad E^- = -D_1 + \alpha D_2.$$

The surface S is a K3 surface. By varying the coefficients of the polynomials defining S, one can produce an 18 dimensional family of such surfaces (up to isomorphism over $\mathbb{C}$). For basic facts about K3 surfaces, see [3, 6]. This particular family of surfaces is studied by Wehler in [17]; he shows that the general member of this family has automorphism group exactly equal to $\mathscr{A}$. For our purposes it is enough to have $\mathscr{A}$ as a subgroup of $\operatorname{Aut}(S)$, so we will not need to worry about the fact that Wehler's proof does not guarantee the existence of even a single $S/\bar{\mathbb{Q}}$ with $\operatorname{Aut}(S) = \mathscr{A}$. (This is a failing common to all theorems in algebraic geometry which assert that the general member of a family has a certain property. For example, the Noether-Lefschetz theorem [7, 10] and the Dimension and Smoothness theorems in Brill-Noether theory [1, p. 214] have this form. Note that the term "general" means except for countably many proper Zariski closed subsets of the relevant moduli space. Since

$\mathbb{Q}$ itself is countable, there is nothing to prevent every $\mathbb{Q}$ point in the moduli space from being deleted!).

Our first result says that there are height functions $\hat{h}^+$ and $\hat{h}^-$ on $S(\bar{K})$ which transform "canonically" relative to the group of automorphisms $\mathscr{A}$.

Theorem 1.1 *There is a unique pair of functions*

$$\hat{h}^+, \hat{h}^- : S(\bar{K}) \to \mathbb{R}$$

satisfying the following two properties:

(i) $$\hat{h}^\pm = h_{E^\pm} + O(1).$$

(ii) $$\hat{h}^\pm \circ \sigma_1 = \alpha^{\mp 1} \hat{h}^\mp. \qquad \hat{h}^\pm \circ \sigma_2 = \alpha^{\pm 1} \hat{h}^\mp.$$

The functions $\hat{h}^+$ and $\hat{h}^-$ have the following additional properties:

(iii) $$\hat{h}^\pm \circ \phi = \alpha^{\pm \ell(\phi)} \hat{h}^{\pm \chi(\phi)} \qquad \text{for all } \phi \in \mathscr{A}.$$

[Here χ: $\mathscr{A} \to \{\pm 1\}$ and ℓ: $\mathscr{A} \to \mathbb{Z}$ are functions we will describe in Sect. 2; and $\hat{h}^{\pm 1}$ is an alternative notation for $\hat{h}^\pm$.]

(iv) *Define* $$\hat{h} = \hat{h}^+ + \hat{h}^-.$$

Then $\hat{h}$ is a Weil height function for the ample divisor class $(\alpha - 1)(D_1 + D_2)$.

(v) *The function $\hat{h}^+ \hat{h}^-$ is $\mathscr{A}$-invariant. That is,*

$$\hat{h}^+(\phi P) \hat{h}^-(\phi P) = \hat{h}^+(P) \hat{h}^-(P) \qquad \text{for all } \phi \in \mathscr{A} \quad \text{and all} \quad P \in S(\bar{K}).$$

(vi) $$\hat{h}^\pm(P) \geqq 0 \qquad \text{for all } P \in S(\bar{K}).$$

(vii) *Let $P \in S(\bar{K})$. Then*

$$\hat{h}^+(P) = 0 \Leftrightarrow \hat{h}^-(P) = 0 \Leftrightarrow \{\phi P : \phi \in \mathscr{A}\} \text{ is finite.}$$

The automorphisms in $\mathscr{A}$ act on the points of S. We will call the orbit of a point P a chain, since it can be pictured as

$$\ldots \overset{\sigma_2}{\leftrightarrow} \sigma_1 \sigma_2 P \overset{\sigma_1}{\leftrightarrow} \sigma_2 P \overset{\sigma_2}{\leftrightarrow} P \overset{\sigma_1}{\leftrightarrow} \sigma_1 P \overset{\sigma_2}{\leftrightarrow} \sigma_2 \sigma_1 P \overset{\sigma_1}{\leftrightarrow} \sigma_1 \sigma_2 \sigma_1 P \overset{\sigma_2}{\leftrightarrow} \ldots$$

Of course, such a chain may loop back on itself.

Definition. A *chain* $\mathscr{C} \subset S(\bar{K})$ is a set of points of the form

$$\mathscr{C}(P) = \{\phi P : \phi \in \mathscr{A}\}$$

for some $P \in S(\bar{K})$. We will say that a chain $\mathscr{C}$ is *K-rational* if $\mathscr{C} \subset S(K)$. We define the (*canonical*) *height of a chain* $\mathscr{C}$ to be

$$\hat{H}(\mathscr{C}) = \hat{h}^+(P) \hat{h}^-(P) \qquad \text{for any } P \in \mathscr{C}.$$

(Note that Theorem 1.1(v) says that $\hat{H}(\mathscr{C})$ is independent of the choice of $P \in \mathscr{C}$.)

Since $S(K)$ is a disjoint union of chains, we can break up the study of $S(K)$ into two questions:

What do the points in a K-rational chain look like?

What does the set of K-rational chains look like?

We will be able to answer the first question quite well. For the second, we will be able to limit the number of finite K-rational chains; but at present we do not have any good description of the infinite K-rational chains. We begin with our description of the finite chains.

Theorem 1.2 (a) *$\mathscr{C}$ is finite $\Leftrightarrow \hat{H}(\mathscr{C})=0 \Leftrightarrow \hat{h}(P)=0$ for all $P\in\mathscr{C}$.*

(b) *For any constant B, the set*

$$\{\text{chains } \mathscr{C}\subset S(K)\colon \hat{H}(\mathscr{C})\leqq B\}$$

is finite. In particular, there are only finitely many chains $\mathscr{C}\subset S(K)$ with $\#\mathscr{C}<\infty$.

Remark. We can actually prove something a little bit stronger concerning the set of finite chains. For any $P\in S(\bar{K})$, let $\mathscr{C}(P)$ denote the chain containing P. Then we can prove that

$$\{P\in S(\bar{K})\colon \#\mathscr{C}(P)<\infty\}$$

is a set of bounded height. Thus this set contains only finitely many points defined over fields of bounded degree.

Next we investigate the heights of the points in a given infinite chain. We give an estimate for the point of smallest height and count the number of points with height less than a given bound.

Theorem 1.3 *Let $\mathscr{C}\subset S(K)$ be a chain with $\#\mathscr{C}=\infty$.*

(a)

$$2\sqrt{\hat{H}(\mathscr{C})}\leqq \min_{P\in\mathscr{C}} \hat{h}(P)\leqq 2\alpha\sqrt{\hat{H}(\mathscr{C})}.$$

(b) *Let*

$$\mu(\mathscr{C})=\#\{\sigma\in\mathscr{A}\colon \sigma Q=Q\}$$

be the order of the stabilizer of Q for any point $Q\in\mathscr{C}$, so $\mu(\mathscr{C})$ equals 1 or 2. If $B^2\geqq 4\hat{H}(\mathscr{C})$, then

$$\left|\#\{P\in\mathscr{C}\colon \hat{h}(P)\leqq B\}-\frac{1}{\mu(\mathscr{C})}\log_\alpha\frac{B^2}{4\hat{H}(\mathscr{C})}\right|\leqq 4.$$

(Note that from (a), *if $B^2<4\hat{H}(\mathscr{C})$, then no point $P\in\mathscr{C}$ satisfies $\hat{h}(P)\leqq B$.*)

(c) *For any ample divisor $D\in\operatorname{Pic}(S)$,*

$$\#\{P\in\mathscr{C}\colon h_D(P)\leqq B\}=\frac{1}{\mu(\mathscr{C})}\log_\alpha\frac{B^2}{\hat{H}(\mathscr{C})}+O(1)\qquad \text{as } B\to\infty.$$

The $O(1)$ constant depends only on D and the choice of Weil height function h_D.

Using Theorem 1.3, we can reduce the question of counting points in $S(K)$ to the question of counting rational chains.

Theorem 1.4 *Let*

$$S(K)_{\mathrm{fin}}=\{P\in S(K)\colon \hat{h}(P)=0\}=\{P\in S(K)\colon \mathscr{C}(P)\text{ is finite}\},$$

and let $\mu(\mathscr{C})$ *be as in Theorem 3. Then*

$$\#\{P\in S(K)\colon \hat{h}(P)\leqq B\}=\#S(K)_{\mathrm{fin}}+\sum_{\substack{\mathscr{C}\subset S(K)\\ 0<4\hat{H}(\mathscr{C})\leqq B^2}}\left\{\frac{1}{\mu(\mathscr{C})}\log_\alpha\frac{B^2}{4\hat{H}(\mathscr{C})}+\varepsilon(\mathscr{C})\right\},$$

where $\#S(K)_{\mathrm{fin}}$ *is finite, and* $|\varepsilon(\mathscr{C})|\leqq 4$ *for all chains* $\mathscr{C}$.

We have defined a K-rational chain to be a chain whose points are all defined over K. As the referee has pointed out, it is also natural to look at those chains $\mathscr{C}$ which are Galois invariant. We can use the canonical height to quickly give a very explicit description of all such chains.

Corollary 1.5 *Let* $P\in S(\bar{K})$ *be a point whose chain* $\mathscr{C}(P)$ *is stable under the action of* $\mathrm{Gal}(\bar{K}/K)$. *Then* P *satisfies one of the following three conditions.*

(i) $P\in S(K)$. *(I.e.* $\mathscr{C}(P)$ *is* K*-rational.)*

(ii) $P\in S_{\mathrm{fin}}$. *(I.e.* $\mathscr{C}(P)$ *is finite.)*

(iii) $[K(P)\colon K]=2$. *More precisely, there is a* $\tau\in\mathscr{A}$ *and a* $j\in\{1,2\}$ *so that* $p_j(\tau P)\in\mathbb{P}^2(K)$. *Further, in this case there are no non-trivial elements of* $\mathscr{A}$ *that fix* P.

The results stated above raise a number of interesting questions which are very much analogous to problems which have been extensively studied on abelian varieties.

Question 1 (K3 Analogue of Néron's Theorem) Describe the counting function for rational chains,

$$\#\{\mathscr{C}\subset S(K)\colon \hat{H}(\mathscr{C})\leqq B\},$$

as $B\to\infty$. Bogomolov and Mumford (cf. the appendix to [11]) have shown that a K3 surface always contains (singular) curves of genus 0 and 1, so this number will grow rapidly, at least if K is large enough. Batyrev and Manin [2] have a precise conjecture which predicts that "most" of the rational points on S will lie on curves of genus 0. However, it is an easy consequence of a result of Wehler [18] that a general surface of this type contains no smooth curves of genus less than 2. (See Corollary 2.6.) It seems to be a difficult question to determine all of the singular curves of genus 0 and 1. We define

$$S(K)^*=\{P\in S(K)\colon P\text{ lies on no curve of genus 0 or 1 in }S\},$$

and ask for the order of growth of

$$\#\{\mathscr{C}\subset S(K)^*\colon \hat{H}(\mathscr{C})\leqq B\}.$$

(A bold conjecture of Bogomolov (cf. [2, p. 35]) asserts that $S(\bar{K})^*=\emptyset$, which would make the answer to our last question very easy!)

Question 2 (K3 Analogue of Torsion Conjecture) Is there a bound for $S(K)_{\mathrm{fin}}$ that depends only on K, independent of the choice of K3 surface $S/K\subset\mathbb{P}^2\times\mathbb{P}^2$?

Question 3 (K3 Analogue of Raynaud's Theorem) Let $C \subset S$ be an irreducible curve which is not fixed by any non-trivial element of $\mathscr{A}$. Is it true that $C \cap S_{\mathrm{fin}}$ is finite? (Here S_{fin} is an abreviation for $S(\bar{K})_{\mathrm{fin}}$, the set of all points of S having finite chains.)

We observe that if C_1 and C_2 denote the branch loci of the projections p_1 and p_2 respectively, then for any $\phi \in \mathscr{A}$, every point in $C_1 \cap \phi C_2$ will be in S_{fin}. Now varying ϕ will undoubtedly yield infinitely many points in $C_1 \cap S_{\mathrm{fin}}$. This is why we must restrict ourselves to curves not fixed by elements of $\mathscr{A}$.

Question 4 (K3 Analogue of Lang Conjecture) Is there a positive lower bound for $\hat{h}(P)$, independent of S, valid for points $P \in S(K) \setminus S(K)_{\mathrm{fin}}$? More generally, let $h(S)$ be the height of the point in moduli space corresponding to S, where we fix a projective embedding of the moduli space. Is there a constant $c>0$, depending only on K, so that for all S/K,

$$\hat{h}(P) \geqq c h(S) \qquad \text{for all } P \in S(K),\ P \notin S(K)_{\mathrm{fin}}?$$

Question 5 (K3 Analogue of Lehmer Conjecture) Are there constants $c=c(S)>0$ and $d=d(S)$ so that for all extension fields L/K,

$$\hat{h}(P) \geqq \frac{c}{[L:K]^d} \qquad \text{for all } P \in S(L),\ P \notin S(L)_{\mathrm{fin}}?$$

More precisely, can one take $d=\frac{1}{2}$, as is expected to be true for abelian surfaces?

Question 6 (K3 Analogue of Serre's "Image of Galois" Theorem) Let

$$\mathscr{A}_P = \{\phi \in \mathscr{A} : \phi P = P\}$$

denote the stabilizer of a point $P \in S$; and for any subgroup $\mathscr{B} \subset \mathscr{A}$, let

$$S[\mathscr{B}] = \{P \in S(\bar{K}) : \mathscr{A}_P = \mathscr{B}\}.$$

Thus if $P \in S[\mathscr{B}]$, then there is a bijection $\mathscr{A}/\mathscr{B} \leftrightarrow \mathscr{C}(P)$.

Assume now that $[\mathscr{A}:\mathscr{B}] < \infty$. Then every element in $S[\mathscr{B}] \cap S(K)$ generates a finite K-rational chain, so Theorem 1.2(b) implies that $S[\mathscr{B}] \cap S(K)$ is a finite set. The question we pose is to describe the Galois group $\mathrm{Gal}(K(S[\mathscr{B}])/K)$ as a subgroup of the symmetric group of $S[\mathscr{B}]$. In particular, is the index of $\mathrm{Gal}(K(S[\mathscr{B}])/K)$ in the symmetric group of $S[\mathscr{B}]$ bounded independently of $\mathscr{B}$, subject always to the assumption that $[\mathscr{A}:\mathscr{B}] < \infty$?

2 The geometry of the K3 surface S

Let $S \subset \mathbb{P}^2 \times \mathbb{P}^2$ be a smooth surface as described in Sect. 1. Then the projections $p_j\colon S \to \mathbb{P}^2$ each exhibit S as a double cover of $\mathbb{P}^2$ branched along a smooth sextic curve. The subgroup $\mathscr{A}$ of $\mathrm{Aut}(S)$ generated by σ_1 and σ_2 is isomorphic to the free product $\mathbb{Z}_2 * \mathbb{Z}_2$ of two groups of order 2. (See [17].) In this section we are going to study the geometry of S. We begin with a simple geometric calculation

Lemma 2.1 (a)

$$\sigma_1^* D_1 = D_1, \qquad \sigma_1^* D_2 = 4D_1 - D_2,$$

$$\sigma_2^* D_1 = -D_1 + 4D_2, \qquad \sigma_2^* D_2 = D_2,$$

(b)

$$\sigma_1^* E^+ = \alpha^{-1} E^-, \qquad \sigma_1^* E^- = \alpha E^+,$$

$$\sigma_2^* E^+ = \alpha E^-, \qquad \sigma_2^* E^- = \alpha^{-1} E^+.$$

Proof. (a) First, letting H be a generator of $\mathrm{Pic}(\mathbb{P}^2)$, we find that

$$\sigma_j^* D_j = \sigma_j^* p_j^* H = (p_j \sigma_j)^* H = p_j^* H = D_j.$$

This proves two of the desired equalities.

Next, from the definition of σ_j, we see that

$$p_j^*(p_j P) = (P) + (\sigma_j P).$$

(This is an equality of zero-cycles.) Hence for any $D \in \mathrm{Pic}(S)$,

$$p_j^* p_{j*} D = D + \sigma_{j*} D = D + \sigma_j^* D.$$

(Since σ_j is an involution, we have $\sigma_{j*} = \sigma_j^*$.) Now we let $H_1 = H \times \mathbb{P}^2$ and $H_2 = \mathbb{P}^2 \times H$ be a basis for $\mathrm{Pic}(\mathbb{P}^2 \times \mathbb{P}^2)$ and compute an intersection number:

$$\begin{aligned}(p_{2*} D_1) \cdot H &= (p_{2*} p_1^* H) \cdot H \\ &= (p_1^* H) \cdot (p_2^* H), \quad \text{by "push-pull" formula,} \\ &= S \cdot H_1 \cdot H_2, \quad \text{intersection in } \mathbb{P}^2 \times \mathbb{P}^2, \\ &= (H_1 + H_2) \cdot (2H_1 + 2H_2) \cdot H_1 \cdot H_2, \quad \text{since } S \text{ is the intersection of a (1, 1) form and a (2, 2) form,} \\ &= 4.\end{aligned}$$

Since $\mathrm{Pic}(\mathbb{P}^2) = \mathbb{Z} H$ and $H^2 = 1$, we see that $p_{2*} D_1 = 4H$. Substituting above gives

$$\sigma_2^* D_1 = p_2^* p_{2*} D_1 - D_1 = p_2^*(4H) - D_1 = 4D_2 - D_1.$$

This is the third equality, and the fourth is proven similarly.

(b) These all follow from (a), the definition of $E^{\pm}$, and the fact that $4 - \alpha = \alpha^{-1}$. For example,

$$\sigma_1^* E^+ = \sigma_1^*(\alpha D_1 - D_2) = \alpha D_1 - (4D_1 - D_2) = -\alpha^{-1} D_1 + D_2 = \alpha^{-1} E^-.$$

The others are similar. □

It will actually be useful to have a complete description of how the automorphisms in $\mathscr{A}$ act on E^+ and E^-. To do this we need to describe two maps. The first is the unique character

$$\chi: \mathscr{A} \to \{\pm 1\}$$

of order 2 on $\mathscr{A}$. This is most simply defined by

$$\chi(\sigma_{i_1}\sigma_{i_2}\sigma_{i_3}\ldots\sigma_{i_n})=(-1)^n.$$

The kernel of χ is the cyclic subgroup of $\mathscr{A}$ generated by $\sigma_1\sigma_2$.

The other function

$$\ell: \mathscr{A}\to\mathbb{Z}$$

is defined inductively by the rules:

$$\ell(e)=0, \quad \ell(\sigma_1\phi)=-1-\ell(\phi), \quad \ell(\sigma_2\phi)=1-\ell(\phi).$$

The following brief table should make the definition clear, while the subsequent lemma explains why it is natural to look at function ℓ.

ϕ	...	$\sigma_1\sigma_2\sigma_1$	$\sigma_1\sigma_2$	σ_1	e	σ_2	$\sigma_2\sigma_1$	$\sigma_2\sigma_1\sigma_2$	...
$\ell(\phi)$	...	-3	-2	-1	0	1	2	3	...
$\chi(\phi)$	...	-1	1	-1	1	-1	1	-1	...

Proposition 2.2 (a) *The map $\ell: \mathscr{A}\to\mathbb{Z}$ is a bijection of sets.*

(b)

$$\ell(\phi\psi)=\ell(\phi)+\chi(\phi)\,\ell(\psi) \quad \textit{for all } \phi,\psi\in\mathscr{A}.$$

Thus ℓ represents a (non-trivial) element of the cohomology group $H^1(\mathscr{A},\mathbb{Z})$, where we make $\mathbb{Z}$ into an $\mathscr{A}$-module via the action $\chi: \mathscr{A}\to\{\pm 1\}=\mathrm{Aut}(\mathbb{Z})$.

(c)

$$\phi^* E^{\pm}=\alpha^{\pm\ell(\phi)}E^{\pm\chi(\phi)}.$$

(Here $E^{\pm 1}$ means the same thing as $E^{\pm}$.)

Proof. (a) This is clear from the table; or more rigorously, one can easily check by induction that if $i_1, i_2, \ldots, i_n$ is an alternating sequence of 1's and 2's, then

$$\ell(\sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_n})=\begin{cases} n, & \text{if } i_1=2;\\ -n, & \text{if } i_1=1.\end{cases}$$

(b) This, too, is easily checked by induction. It is clearly true if $\phi=e$. Assume now it is true for ϕ; we need to check it for $\sigma_1\phi$ and $\sigma_2\phi$. We will do the former; the latter is done similarly.

$$\begin{aligned}\ell(\sigma_1\phi\psi)&=-1-\ell(\phi\psi), \quad \text{definition of } \ell,\\ &=-1-\{\ell(\phi)+\chi(\phi)\,\ell(\psi)\}, \quad \text{induction hypothesis},\\ &=\ell(\sigma_1\phi)-\chi(\phi)\,\ell(\psi), \quad \text{definition of } \ell,\\ &=\ell(\sigma_1\phi)+\chi(\sigma_1\phi)\,\ell(\psi), \quad \text{since } \chi(\sigma_1)=-1.\end{aligned}$$

We have just verified the cocycle relation, so ℓ represents an element of the cohomology group $H^1(\mathscr{A},\mathbb{Z})$. To see it is non-trivial, we note that $\ker(\chi)\cong\mathbb{Z}$

via the identification $\sigma_2\sigma_1 \leftrightarrow 1$, and that $\ker(\chi)$ acts trivially on $\mathbb{Z}$. Hence under the restriction map

$$H^1(\mathscr{A}, \mathbb{Z}) \xrightarrow{\text{res}} H^1(\ker(\chi), \mathbb{Z}) \cong \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z},$$

the image of ℓ is $\ell(\sigma_2\sigma_1)=2$; so ℓ represents a non-trivial cohomology class.
(c) Again the proof is by induction. The desired result is clearly true for $\phi=e$. Assuming it is true for ϕ, we must check it for $\sigma_1\phi$ and $\sigma_2\phi$. Thus

$$\begin{aligned}(\sigma_1\phi)^* E^{\pm} &= \phi^*(\sigma_1^* E^{\pm})\\ &= \phi^*(\alpha^{\mp 1} E^{\mp}), \quad \text{from Lemma 5.1(b)},\\ &= \alpha^{\mp 1}(\alpha^{\mp \ell(\phi)} E^{\mp \chi(\phi)}), \quad \text{induction hypothesis},\\ &= \alpha^{\mp(1+\ell(\phi))} E^{\mp \chi(\phi)}\\ &= \alpha^{\pm \ell(\sigma_1\phi)} E^{\pm \chi(\sigma_1\phi)}, \quad \text{definition of } \ell \text{ and } \chi.\end{aligned}$$

The verification for $\sigma_2\phi$ is done similarly. □

We are now going to describe several geometric properties of our surface S. These results are relevant to our discussion in Sect. 1, and should prove useful in further studying the arithmetic of S. However, they are not actually needed for the construction and applications of the canonical height, so the reader who is mainly interested in arithmetic results can skip directly to Sect. 3.

As a first geometric application of Prop. 2.2, we show that an infinite chain is always Zariski dense in S.

Corollary 2.3 *Let $\mathscr{C} \subset S$ be a chain with $\#\mathscr{C}=\infty$. Then $\mathscr{C}$ is Zariski dense in S.*

Proof. Suppose that $\mathscr{C}$ is not Zariski dense, and let Γ be the one-dimensional part of the Zariski closure of $\mathscr{C}$. Since $\#\mathscr{C}=\infty$, we know that $\Gamma \neq \emptyset$. Write

$$\Gamma = \bigcup_{i=1}^{n} C_i$$

as a union of irreducible curves $C_i \subset S$. By construction, $\#(\mathscr{C} \cap C_i)=\infty$ for each $1 \leqq i \leqq n$; and the C_i's are the only irreducible curves on S with this property.

For any $\phi \in \mathscr{A}$, we have $\phi\mathscr{C}=\mathscr{C}$. Since ϕ is one-to-one, it follows that

$$\infty = \#(\mathscr{C} \cap C_i) = \#(\phi\mathscr{C} \cap C_i) = \#(\mathscr{C} \cap \phi^{-1} C_i).$$

Hence $\phi^{-1} C_i$ is one of the C_j's. In other words, we get a map (clearly a homomorphism) from $\mathscr{A}$ to the symmetric group $\mathscr{S}_n$,

$$\pi: \mathscr{A} \to \mathscr{S}_n, \qquad \text{determined by } \phi(C_i) = C_{\pi_\phi(i)}$$

The kernel of π has finite index in $\mathscr{A}$, so we can find an integer $k \geqq 1$ such that $\pi((\sigma_2\sigma_1)^k)=e$.

In particular, we see that $(\sigma_2\sigma_1)^k C_1 = C_1$. On the other hand, when we compute intersection indices using Prop. 2.2, we find

$$\begin{aligned} E^{\pm}\cdot C_1 &= E^{\pm}\cdot(\sigma_2\sigma_1)^k C_1 \\ &= ((\sigma_2\sigma_1)^k)^* E^{\pm}\cdot C_1 \\ &= \alpha^{\pm 2k} E^{\pm}\cdot C_1. \end{aligned}$$

Since $k \neq 0$ and $\alpha = 2+\sqrt{3}$, we conclude that $E^+\cdot C_1 = E^-\cdot C_1 = 0$. Hence

$$0 = C_1\cdot(E^+ + E^-) = (\alpha-1)(C_1\cdot(D_1+D_2)).$$

But D_1+D_2 is ample and C_1 is a curve, so this is a contradiction. Therefore $\mathscr{C}$ is Zariski dense in S. $\square$

Remark. We just proved that an infinite chain $\mathscr{C}\subset S$ is Zariski dense in S. If $\mathscr{C}\subset S(\mathbb{Q})$, it is natural to ask how $\mathscr{C}$ is distributed in $S(\mathbb{R})$. The map that takes a point $P\in S(\mathbb{R})$ to its chain $\mathscr{C}(P)\subset S(\mathbb{R})$ is a (non-linear) dynamical system which certainly merits further study. Preliminary computer calculations reveal some interesting patterns, but at present we have nothing definitive to say.

It is an easy exercise to classify the subgroups of $\mathscr{A}$; in particular, the subgroups of finite index are precisely the subgroups which contain $(\sigma_2\sigma_1)^k$ for some non-zero integer k. So a point $P\in S$ will generate a finite chain (i.e. in our earlier notation, $P\in S_{\text{fin}}$) if an only if it is fixed by some $(\sigma_2\sigma_1)^k$. We can use Prop. 2.2 to show that each $(\sigma_2\sigma_1)^k$ has only a finite number of fixed points. More generally, we prove the following.

Corollary 2.4 *For any $\phi\in\mathscr{A}$, let*

$$\mathscr{F}_\phi = \{P\in S\colon \phi P = P\}$$

be the set of fixed points of ϕ. Also let $C_i\subset S$ be the ramification locus of p_i: $S\to\mathbb{P}^2$ for $i=1,2$.

(a) *If $\phi = \tau\sigma_i\tau^{-1}$ for some $\tau\in\mathscr{A}$, then $\mathscr{F}_\phi = \tau C_i$.*
(b) *If $\phi = (\sigma_1\sigma_2)^k$ for some $k\in\mathbb{Z}$, $k\neq 0$, then $\mathscr{F}_\phi$ is finite.*

Proof. (a) The definition of the σ_i's shows immediately that $\mathscr{F}_{\sigma_i} = C_i$. Hence

$$\begin{aligned} P\in\mathscr{F}_\phi &\Leftrightarrow \tau\sigma_i\tau^{-1}P = P \Leftrightarrow \sigma_i(\tau^{-1}P) = \tau^{-1}P \\ &\Leftrightarrow \tau^{-1}P\in\mathscr{F}_{\sigma_i} = C_i \Leftrightarrow P\in\tau C_i. \end{aligned}$$

(b) Suppose $\#\mathscr{F}_\phi = \infty$. Since $\mathscr{F}_\phi$ is a Zariski closed subset of S, it follows that there is an irreducible curve $C\subset\mathscr{F}_\phi$. Then $\phi|_C$ is the identity map on C, so $\phi^* C = C$. Since ϕ has degree 1, it follows that for any divisor $D\in\operatorname{Div}(S)$,

$$C\cdot D = \phi^* C\cdot\phi^* D = C\cdot\phi^* D.$$

Taking $D = E^{\pm}$ and $\phi = (\sigma_1\sigma_2)^k$, we observe that $\chi(\phi) = 1$, so

$$C\cdot E^{\pm} = C\cdot\phi^* E^{\pm} = C\cdot(\alpha^{\pm\ell(\phi)} E^{\pm\chi(\phi)}) = C\cdot(\alpha^{\pm\ell(\phi)} E^{\pm}).$$

Hence

$$(1-\alpha^{\pm\ell(\phi)})(C\cdot E^{\pm}) = 0.$$

Now $\phi=(\sigma_1\sigma_2)^k\neq e$, so $\ell(\phi)\neq 0$, which means that $\alpha^{\pm\ell(\phi)}\neq 1$. Therefore $C\cdot E^+=C\cdot E^-=0$. Now we obtain a contradiction by observing that C is effective and that $E^++E^-=(\alpha-1)(D_1+D_2)$ is in the ample cone of Pic$(S)\otimes\mathbb{R}$. Therefore $\mathscr{F}_\phi$ contains no curves, so it is a finite set of points. □

Remark. For any subgroup $\mathscr{B}\subset\mathscr{A}$, let $S[\mathscr{B}]$ be as in Question 6 of Sect. 1. It follows immediately from Corollary 2.4 and the remarks preceding it that if $[\mathscr{A}:\mathscr{B}]<\infty$, then $S[\mathscr{B}]$ is finite, since $S[\mathscr{B}]$ will be contained in $\mathscr{F}_{(\sigma_1\sigma_2)^k}$ for some non-zero integer k. It is an interesting problem to try to determine the order of $S[\mathscr{B}]$ for particular subgroups.

For example, let $\mathscr{B}_\tau$ be the subgroup generated by σ_1 and $\tau\sigma_2\tau^{-1}$ for some $\tau\in\mathscr{A}$. Then one easily sees that $S[\mathscr{B}_\tau]$ is contained in $C_1\cap\tau C_2$. We can compute the intersection index $C_1\cdot\tau C_2$ as follows: Each p_i is ramified over a smooth curve of degree 6, so $C_2=6D_i$ in Pic(S). Hence

$$C_1\cdot\tau C_2=\tau^*(6D_1)\cdot(6D_2)=\frac{432\alpha^2}{(\alpha^2-1)^2}(\alpha^{\ell(\tau)+(\chi(\tau)+1)/2}+\alpha^{-\ell(\tau)-(\chi(\tau)+1)/2}).$$

This certainly suggests that $\#S[\mathscr{B}_\tau]\to\infty$ as $|\ell(\tau)|\to\infty$, but a rigorous proof would need to take multiplicities into account, as well as the possibility that some points in $C_1\cap\tau C_2$ might have stabilizer strictly larger than $\mathscr{B}_\tau$.

Next let $\mathscr{B}_\tau$ be the (cyclic) subgroup of $\mathscr{A}$ generated by $(\sigma_1\sigma_2)^k$ for some integer $k\neq 0$. Alan Landman has sketched for me a proof that the Lefschetz number of $(\sigma_1\sigma_2)^k$ is

$$\alpha^{2k}+\alpha^{-2k}+22,$$

which again suggests that $\#S[\mathscr{B}_k]\to\infty$ as $k\to\infty$. We briefly indicate Landman's proof.

Consider the action of σ_1 on the Hodge diamond $H^*=H^{i,j}(S,\mathbb{C})$ of S. Since σ_1 is an involution, very eigenvalue of σ_1 on H^* is ±1, say n^+ plus ones and n^- minus ones. By the generalized Lefschetz fixed point formula,

$$n^+-n^-=L(\sigma_1)=(\text{Euler characteristic of fixed point set of }\sigma_1)=-18,$$

since σ_1 fixes the branch locus of p_1, which is a smooth sextic curve in $\mathbb{P}^2$. On the other hand, $n^++n^-=\dim H^*=24$. Hence $n^+=3$ and $n^-=21$. Now σ_1 acts as $+1$ on H^0 and H^4, and it also acts as $+1$ on the subspace of $H^{1,1}$ spanned by the image of D_1, since $\sigma_1^*D_1=D_1$. Hence it acts as -1 on the rest of H^*. In particular, if we let V be the image of Pic$(S)\otimes\mathbb{C}$ in $H^{1,1}$ and $V^\perp$ its orthogonal complement, then σ_1 acts as -1 on $V^\perp$, since it is diagonalizable and all of it's eigenvalues are -1. Further, σ_1 acts as -1 on $H^{0,2}\cong\mathbb{C}$ and $H^{2,0}\cong\mathbb{C}$. By a similar argument, the same holds for σ_2. Hence $(\sigma_1\sigma_2)^k$ acts as $+1$ on all of H^* except for V; in other words, $H^*\cong V\oplus\mathbb{C}^{22}$ as a representation space for $(\sigma_1\sigma_2)^k$. Using the basis $V=\mathbb{C}E^+\oplus\mathbb{C}E^-$, we find that

$$L((\sigma_1\sigma_2)^k)=\text{Trace}(\sigma_1\sigma_2)^k|_V+\text{Trace}(\sigma_1\sigma_2)^k|_{\mathbb{C}^{22}}=\alpha^{2k}+\alpha^{-2k}+22,$$

which is Landman's formula for the Lefschetz number of $(\sigma_1\sigma_2)^k$.

We can also describe the effective and ample divisors in Pic(S), or at least in that part of Pic(S) spanned by D_1 and D_2.

Proposition 2.5 *Let $D \in \mathrm{Pic}(S)$ be a divisor which can be written in the form*

$$D = n_1 D_1 + n_2 D_2.$$

Then the following are equivalent:

(i) *D is effective.*

(ii) *D is ample.*

(iii) *$D \cdot E^+ > 0$ and $D \cdot E^- > 0$.*

(iv) *$n_1 > -\alpha n_2$ and $n_2 > -\alpha n_1$.*

In its entirety, this proposition only holds for divisors in $\mathrm{Span}\{D_1, D_2\}$; *it may not be true for all divisors in* $\mathrm{Pic}(S)$. *However, the following implications are true for every $D \in \mathrm{Pic}(S)$:*

$$\text{(ii)} \Rightarrow \text{(i)} \Rightarrow \text{(iii)}$$

Proof. Before starting the proof, we note that $D_1^2 = D_2^2 = 2$ and $D_1 \cdot D_2 = 4$. So using the definition of $E^\pm$ and $\alpha^2 = 4\alpha - 1$, one easily computes

$$E^+ \cdot E^+ = E^- \cdot E^- = 0 \quad \text{and} \quad E^+ \cdot E^- = 12\alpha.$$

We begin by showing that (i) implies (iii) for every divisor $D \in \mathrm{Pic}(S)$. So let D be any effective divisor on S. We write

$$D = t_1 E^+ + t_2 E^- + \Gamma \in \mathrm{Pic}(S) \otimes \mathbb{R}$$

with

$$t_1 = \frac{D \cdot E^-}{12\alpha}, \quad t_2 = \frac{D \cdot E^+}{12\alpha}, \quad \text{and} \quad \Gamma \cdot E^+ = \Gamma \cdot E^- = 0.$$

Since E^+ and E^- span the same subspace of $\mathrm{Pic}(S) \otimes \mathbb{R}$ as D_1 and D_2, we note that $\Gamma \cdot D_1 = \Gamma \cdot D_2 = 0$.

For any integer k, let $\phi_k = (\sigma_2 \sigma_1)^k \in \mathrm{Aut}(S)$. Since $D_1 + D_2$ is very ample and ϕ_k is an automorphism, the divisor $\phi_k^*(D_1 + D_2)$ is very ample. Hence its intersection with the effective divisor D is a positive integer. Thus

$$\begin{aligned}
1 &\leqq D \cdot \phi_k^*(D_1 + D_2), && \text{intersection of effective and very ample,} \\
&= (\alpha - 1)(D \cdot \phi_k^*(E^+ + E^-)), && \text{definition of } E^\pm, \\
&= (\alpha - 1)(t_1 E^+ + t_2 E^-) \cdot (\alpha^{2k} E^+ + \alpha^{-2k} E^-), && \text{from Prop. 2.2(c),} \\
&= (\alpha - 1)\, 12\alpha(\alpha^{-2k} t_1 + \alpha^{2k} t_2).
\end{aligned}$$

This inequality holds for all $k \in \mathbb{Z}$, which implies that $t_1 > 0$ and $t_2 > 0$. We conclude that $D \cdot E^+ > 0$ and $D \cdot E^- > 0$.

Next we show that (ii) implies (i), again for arbitrary divisors on S. We will use the following general facts that hold on all K3 surfaces. (See, e.g., [3] or [6].)

$$h^2(\mathcal{O}_S) = h^0(\Omega_S) = p_g(S) = 1,$$

$$h^1(\mathcal{O}_S) = q = b_1(S) = 0,$$

$$p_a(S) = h^2(\mathcal{O}_S) - h^1(\mathcal{O}_S) = 1,$$

$$\mathcal{K}_S = 0, \quad (\mathcal{K}_S \text{ the canonical class on } S.)$$

Let $D \in \mathrm{Pic}(S)$ be any divisor. The Riemann-Roch theorem [6, p. 472], [8, V.1.6] for surfaces says that

$$h^0(D) - h^1(D) + h^0(\mathscr{K}_S - D) = \tfrac{1}{2}(D^2 - D \cdot \mathscr{K}_S) + p_a(S) + 1.$$

So for a K3 surface we find that

$$h^0(D) + h^0(-D) = h^1(D) + \tfrac{1}{2} D^2 + p_a(S) + 1 \geqq \tfrac{1}{2} D^2 + 2.$$

By assumption, D is ample, so $h^0(-D) = 0$ and $D^2 > 0$. Hence $h^0(D) > 2$, so D is effective.

The proof that (iii) and (iv) are equivalent is immediate once one calculates

$$D \cdot E^+ = 2\sqrt{3}(n_1 + \alpha n_2) \quad \text{and} \quad D \cdot E^- = 2\sqrt{3}(\alpha n_1 + n_2).$$

We have now proven (ii)$\Rightarrow$(i)$\Rightarrow$(iii)$\Leftrightarrow$(iv), so it remains to show that (iii) implies (ii). We will use the Nakai-Moishezon criterion [8, V.1.10]. Write $D = t_1 E^+ + t_2 E^-$ with $t_1, t_2 \in \mathbb{R}$ as above. Note this is where we use the assumption that D is a linear combination of D_1 and D_2. Our assumption (iii) implies that $t_1 > 0$ and $t_2 > 0$. Hence

$$D^2 = 24 \alpha t_1 t_2 > 0.$$

Next let $C \subset S$ be any irreducible curve. Then C gives an effective divisor, so from (i) implies (iii) we deduce that $C \cdot E^+ > 0$ and $C \cdot E^- > 0$. (Remember that we proved (i)$\Rightarrow$(iii) for every divisor in $\mathrm{Pic}(S)$.) Hence

$$C \cdot D = t_1 (C \cdot E^+) + t_2 (C \cdot E^-) > 0.$$

By the Nakai-Moishezon criterion, D is ample. □

If $\mathrm{Pic}(S)$ has rank 2, we can also pick out the curves on S of small arithmetic genus. Wehler's generalization of the Noether-Lefschetz theorem [18, Theorem 5.6] says that a general surface like S satisfies this rank 2 condition, although it does not appear to be known how to find such surfaces defined over $\mathbb{Q}$ or over a number field. And even if one had such a surface, in order to describe the rational points on S, one really needs to find the curves of *geometric* genus 0 and 1; this seems in general to be a difficult problem. (See also [14, § 5] for a computation of all curves of arithmetic genus 0 on a particular K3 surface having a very large Picard group, and a discussion of the problem of singular curves of geometric genus 0.)

Corollary 2.6 *Assume that* $\mathrm{Pic}(S)$ *has rank* 2. *Let* $C \subset S$ *be an irreducible curve on* S. *Then the arithmetic genus of* C *satisfies*

$$p_a(C) \geqq 2.$$

Further, if $p_a(C) = 2$, *then there is an automorphism* $\phi \in \mathscr{A}$ *such that*

$$\phi^* C = D_1 \ \text{or} \ D_2 \quad \text{in } \mathrm{Pic}(S).$$

Proof. Write $C=n_1 D_1+n_2 D_2$ in $\operatorname{Pic}(S)$, where $n_1, n_2 \in \mathbb{Z}$. Then the adjunction formula [8, V.1.5 and Ex. V.1.3] gives (note S has trivial canonical bundle)

$$\begin{aligned} p_a(C) &= \tfrac{1}{2}(C^2+C\cdot\mathscr{K}_S)+1 \\ &= n_1^2+4n_1n_2+n_2^2+1=\frac{(\alpha n_1+n_2)(n_1+\alpha n_2)}{\alpha}+1. \end{aligned}$$

Since C is effective, Prop. 2.5 implies that $\alpha n_1+n_2>0$ and $n_1+\alpha n_2>0$, so we see that $p_a(C)>1$ (strict inequality.) Further, $p_a(C)$ is an integer, from which it follows that $p_a(C)\geqq 2$. This proves the first assertion.

For the second assertion, we observe that

$$p_a(C)=2 \Leftrightarrow n_1^2+4n_2n_2+n_2^2=1.$$

As above, we factor the quadratic form as

$$1=n_1^2+4n_1n_2+n_2^2=(n_1+\alpha n_2)(n_1+\alpha^{-1}n_2)$$

in the ring $\mathbb{Z}[\alpha]=\mathbb{Z}[\sqrt{3}]$. Each factor is a unit, and the fundamental unit in $\mathbb{Z}[\alpha]$ is α, so there is an integer k such that

$$n_1+\alpha n_2=\alpha^k \quad\text{and}\quad n_1+\alpha^{-1}n_2=\alpha^{-k}.$$

Next we write C in terms of the basis $\{E^+, E^-\}$ for $\operatorname{Pic}(S)\otimes\mathbb{R}$.

$$\begin{aligned} C &= \left(\frac{1}{\alpha^2-1}\right)((\alpha n_1+n_2)E^+ +(n_1+\alpha n_2)E^-) \\ &= \left(\frac{1}{\alpha^2-1}\right)(\alpha^{1-k}E^+ +\alpha^k E^-). \end{aligned}$$

Using Prop. 2.2, we can find an automorphism $\phi\in\mathscr{A}$ such that $\ell(\phi)=k$. Note that $\phi^* E^{\pm}=\alpha^{\pm\ell(\phi)}E^{\pm\chi(\phi)}$. Hence

$$\begin{aligned} \phi^* C &= \left(\frac{1}{\alpha^2-1}\right)(\alpha\cdot\alpha^{-\ell(\phi)}\phi^* E^+ +\alpha^{\ell(\phi)}\phi^* E^-) \\ &= \left(\frac{1}{\alpha^2-1}\right)(\alpha E^{\chi(\phi)}+E^{-\chi(\phi)}) \\ &= \begin{cases} D_1 & \text{if } \chi(\phi)=1, \\ D_2 & \text{if } \chi(\phi)=-1. \end{cases} \quad\square \end{aligned}$$

3 Existence of the canonical height

In this section we are going to prove that the canonical heights $\hat{h}^+$ and $\hat{h}^-$ exist, are unique, and satisfy properties (i)–(vii) of Theorem 1.1. We start with uniqueness. Suppose that $\hat{h}^{\pm}$ and $\hat{g}^{\pm}$ satisfy (i) and (ii). Using (i) we see that $\hat{f}^{\pm}=\hat{h}^{\pm}-\hat{g}^{\pm}$ is bounded, and then using (ii) repeatedly gives

$$\hat{f}^{\pm}((\sigma_2\sigma_1)^{\pm n}P)=\alpha^{2n}\hat{f}^{\pm}(P).$$

The left-hand-side is bounded independently of n, so dividing by α^{2n} and letting $n\to\infty$ shows that $\hat{f}^{\pm}(P)=0$. Hence $\hat{h}^{\pm}=\hat{g}^{\pm}$.

To show the $\hat{h}^{\pm}$ exist, we use Tate's averaging method. From Prop. 2.1(b) we have the divisor class relations

$$(\sigma_2\sigma_1)^*E^+=\alpha^2E^+, \qquad (\sigma_1\sigma_2)^*E^-=\alpha^2E^-;$$

and these give the height relations

$$h_{E^+}(\sigma_2\sigma_1P)=\alpha^2h_{E^+}(P)+O(1), \qquad h_{E^-}(\sigma_1\sigma_2P)=\alpha^2h_{E^-}(P)+O(1).$$

Now Tate's method shows that the limits

$$\hat{h}^+(P)=\lim_{n\to\infty}\alpha^{-2n}h_{E^+}((\sigma_2\sigma_1)^nP)$$

and

$$\hat{h}^-(P)=\lim_{n\to\infty}\alpha^{-2n}h_{E^+}((\sigma_1\sigma_2)^nP)$$

exist and satisfy

(i) $\hat{h}^+=h_{E^+}+O(1), \quad \hat{h}^-=h_{E^-}+O(1)$.

(ii)′ $\hat{h}^+(\sigma_2\sigma_1P)=\alpha^2\hat{h}^+(P), \quad \hat{h}^-(\sigma_1\sigma_2P)=\alpha^2\hat{h}^-(P)$.

We briefly sketch the argument for $\hat{h}^+$. (See, e.g., [12, VIII.9.1] or [9, Chap. 5] for the analogous construction on abelian varieties.)

Thus let $P\in S(\bar{K})$. Then for any $n\geqq m$ we have

$$\begin{aligned}
&|\alpha^{-2n}h_{E^+}((\sigma_2\sigma_1)^nP)-\alpha^{-2m}h_{E^+}((\sigma_2\sigma_1)^mP)|\\
&=\left|\sum_{i=m+1}^{n}\alpha^{-2i}h_{E^+}((\sigma_2\sigma_1)^iP)-\alpha^{-2i+2}h_{E^+}((\sigma_2\sigma_1)^{i-1}P)\right|\\
&\leqq\sum_{i=m+1}^{n}\alpha^{-2i}|h_{E^+}(\sigma_2\sigma_1Q_i)-\alpha^2h_{E^+}(Q_i)|, \qquad \text{where } Q_i=(\sigma_2\sigma_1)^{i-1}P,\\
&\leqq\sum_{i=m+1}^{\infty}\alpha^{-2i}\kappa, \qquad \text{where } |h_{E^+}\circ(\sigma_2\sigma_1)-\alpha^2h_{E^+}|\leqq\kappa=\kappa(S),\\
&=\frac{\alpha^{-2m}\kappa}{\alpha^2-1}.
\end{aligned}$$

Hence the sequence $\alpha^{-2n}h_{E^+}((\sigma_2\sigma_1)^nP)$ is Cauchy, so the limit defining $\hat{h}^+$ exists. Further, taking $m=0$ and letting $n\to\infty$ in the above inequality shows that

$$|\hat{h}^+(P)-h_{E^+}(P)|\leqq\frac{\kappa}{\alpha^2-1}.$$

We now have functions $\hat{h}^{\pm}$ satisfying (i); and in place of (ii) we have the conditions we denoted above by (ii)$'$. Using (i) and Lemma 2.1(b) we have

$$\begin{aligned}\hat{h}^{+}(\sigma_2 P)&=h_{E^+}(\sigma_2 P)+O(1)=h_{\sigma_2^* E^+}(P)+O(1)\\&=\alpha h_{E^-}(P)+O(1)=\alpha\hat{h}^{-}(P)+O(1).\end{aligned}$$

Now replace P by $(\sigma_1\sigma_2)^n P$ and use (ii)$'$ to get

$$\begin{aligned}\alpha^{2n}\hat{h}^{+}(\sigma_2 P)&=\hat{h}^{+}((\sigma_2\sigma_1)^n\sigma_2 P)\\&=\hat{h}^{+}(\sigma_2(\sigma_1\sigma_2)^n P)\\&=\alpha\hat{h}^{-}((\sigma_1\sigma_2)^n P)+O(1)\\&=\alpha^{2n+1}\hat{h}^{-}(P)+O(1).\end{aligned}$$

Dividing by α^{2n} and letting $n\to\infty$ gives the equality $\hat{h}^{+}(\sigma_2 P)=\alpha\hat{h}^{-}(P)$. This is one of the equations in (ii); the other three are proven similarly.

Next we verify (iii) by induction on ϕ. It is clearly true for $\phi=e$, so we assume it is true for ϕ and verify it for $\sigma_1\phi$ and $\sigma_2\phi$. Thus

$$\begin{aligned}\hat{h}^{\pm}\circ(\sigma_1\phi)&=\alpha^{\mp 1}\hat{h}^{\mp}\circ\phi, &&\text{from (ii)},\\&=\alpha^{\mp 1\mp\ell(\phi)}\hat{h}^{\mp\chi(\phi)}, &&\text{induction hypothesis},\\&=\alpha^{\pm\ell(\sigma_1\phi)}\hat{h}^{\pm\chi(\sigma_1\phi)}, &&\text{definition of } \ell \text{ and } \chi.\end{aligned}$$

This proves (iii) for $\sigma_1\phi$, and $\sigma_2\phi$ is proven similarly.

Property (iv) follows immediately from (i) and the definition of $E^{\pm}$:

$$\begin{aligned}\hat{h}&=\hat{h}^{+}+\hat{h}^{-}=h_{E^+}+h_{E^-}+O(1)\\&=h_{\alpha D_1-D_2}+h_{-D_1+\alpha D_2}+O(1)=(\alpha-1)h_{D_1+D_2}+O(1).\end{aligned}$$

Similarly, property (v) is immediate from (iii):

$$\hat{h}^{+}(\phi P)\hat{h}^{-}(\phi P)=\{\alpha^{\ell(\phi)}\hat{h}^{\chi(\phi)}(P)\}\cdot\{\alpha^{-\ell(\phi)}\hat{h}^{-\chi(\phi)}(P)\}=\hat{h}^{+}(P)\hat{h}^{-}(P).$$

To prove property (vi), we use (iv), which implies that the function $\hat{h}=\hat{h}^{+}+\hat{h}^{-}$ is bounded below. (A Weil height corresponding to an ample divisor is always bounded below.) Hence

$$\hat{h}^{+}=\hat{h}-\hat{h}^{-}\geqq-\hat{h}^{-}-O(1);$$

so for any point $P\in S(\bar{K})$ and any $n\geqq 0$,

$$\begin{aligned}\hat{h}^{+}(P)&=\alpha^{-2n}\hat{h}^{+}((\sigma_2\sigma_1)^n P)\\&\geqq\alpha^{-2n}\{-\hat{h}^{-}((\sigma_2\sigma_1)^n P)-O(1)\}\\&=-\alpha^{-4n}\hat{h}^{-}(P)-O(\alpha^{-2n}).\end{aligned}$$

Letting $n\to\infty$ gives $\hat{h}^{+}(P)\geqq 0$. A similar argument gives $\hat{h}^{-}(P)\geqq 0$.

It remains to prove property (vii). Suppose first that $\hat{h}^+(P)=0$. Then using (iii) and (iv) we find that

$$\begin{aligned}\hat{h}((\sigma_2\sigma_1)^n P) &= \hat{h}^+((\sigma_2\sigma_1)^n P)+\hat{h}^-((\sigma_2\sigma_1)^n P)\\ &= \alpha^{2n}\hat{h}^+(P)+\alpha^{-2n}\hat{h}^-(P)\\ &= \alpha^{-2n}\hat{h}^-(P).\end{aligned}$$

Therefore $\{(\sigma_2\sigma_1)^n P\colon n=1, 2, \ldots\}$ is a set of bounded height for the height $\hat{h}$. Since $\hat{h}$ is a height relative to an ample divisor, it follows that this is a finite set. Hence there is an integer $n \geqq 1$ such that $(\sigma_2\sigma_1)^n P=P$, and so

$$\frac{\mathscr{A}}{(\sigma_2\sigma_1)^{n\mathbb{Z}}} \to \{\phi P\colon \phi\in\mathscr{A}\}, \qquad \phi\mapsto\phi P,$$

is a well-defined surjective map. Since the subgroup $(\sigma_2\sigma_1)^{n\mathbb{Z}}$ has finite index in $\mathscr{A}$, (precisely, it has index $2n$,) it follows that the set of ϕP's is finite.

Conversely, suppose that there are only finitely many ϕP's. Then $\hat{h}^+(\phi P)$ is bounded independently of ϕ, so

$$\hat{h}^+(P)=\alpha^{-2n}\hat{h}^+((\sigma_2\sigma_1)^n P)\xrightarrow[n\to\infty]{}0.$$

This completes the proof that

$$\hat{h}^+(P)=0 \Leftrightarrow \{\phi P\colon \phi\in\mathscr{A}\} \text{ is finite.}$$

The proof for $\hat{h}^-$ is done similarly. □

4 Applications of the canonical height

In this section we use canonical height functions to prove our main theorems describing the rational points of S.

Proof of Theorem 1.2. (a) Since $\hat{H}(\mathscr{C})=\hat{h}^+(P)\hat{h}^-(P)$ for any point $P\in\mathscr{C}$, this is just a restatement of Theorem 1.1(vii).

Proof of Theorem 1.3. (a) Fix any $Q\in\mathscr{C}$. Then

$$\begin{aligned}\min_{P\in\mathscr{C}} \hat{h}(P) &= \min_{\phi\in\mathscr{A}} \hat{h}(\phi Q)\\ &= \min_{\phi\in\mathscr{A}} \hat{h}^+(\phi Q)+\hat{h}^-(\phi Q)\\ &= \min_{\phi\in\mathscr{A}} \alpha^{\ell(\phi)}\hat{h}^{\chi(\phi)}(Q)+\alpha^{-\ell(\phi)}\hat{h}^{-\chi(\phi)}(Q), \quad \text{from Theorem 1.1(iii),}\\ &= \min_{n\in\mathbb{Z}} \alpha^n\hat{h}^{\chi(n)}(Q)+\alpha^{-n}\hat{h}^{-\chi(n)}(Q).\end{aligned}$$

Here we are writing $\chi\colon \mathbb{Z}\to\{\pm 1\}$ for $\chi(n)=(-1)^n$. We have also used the fact that $\ell\colon \mathscr{A}\to\mathbb{Z}$ is surjective (Prop. 2.2(a)).

If we let

$$f(n)=\alpha^n\hat{h}^{\chi(n)}(Q)+\alpha^{-n}\hat{h}^{-\chi(n)}(Q),$$

then we must find the minimum of $f(n)$ over all $n\in\mathbb{Z}$. The lower bound is immediate:

$$\min_{n\in\mathbb{Z}} f(n) \geqq \inf_{t\in\mathbb{R}}\{t\hat{h}^+(Q)+t^{-1}\hat{h}^-(Q)\} = 2\sqrt{\hat{h}^+(Q)\hat{h}^-(Q)} = 2\sqrt{\hat{H}(\mathscr{C})}.$$

For the upper bound, we let

$$m = 2\left[\frac{1}{2}\log_\alpha\sqrt{\frac{\hat{h}^-(Q)}{\hat{h}^+(Q)}}+\frac{1}{2}\right].$$

(Here $[\cdot]$ denotes greatest integer.) Then m is even and

$$\alpha^{-1}\sqrt{\frac{\hat{h}^-(Q)}{\hat{h}^+(Q)}} \leqq \alpha^m \leqq \alpha\sqrt{\frac{\hat{h}^-(Q)}{\hat{h}^+(Q)}},$$

so

$$\min_{n\in\mathbb{Z}} f(n) \leqq f(m) \leqq 2\alpha\sqrt{\hat{h}^+(Q)\hat{h}^-(Q)} = 2\alpha\sqrt{\hat{H}(\mathscr{C})}.$$

This completes the proof of Theorem 1.3(a). □

Proof of Theorem 1.2. (b) Let $\mathscr{C}\subset S(K)$ be a chain with $\hat{H}(\mathscr{C})\leqq B$. From Theorem 1.3(a), there is a point $P\in\mathscr{C}$ with $\hat{h}(P)\leqq 2\alpha\sqrt{B}$. Hence

$$\#\{\mathscr{C}\subset S(K)\colon \hat{H}(\mathscr{C})\leqq B\} \leqq \#\{P\in S(K)\colon \hat{h}(P)\leqq 2\alpha\sqrt{B}\}.$$

But $\hat{h}$ is a Weil height with respect to an ample divisor class (Theorem 1.1(iv)), so this last set is finite. This proves the first half of Theorem 1.2(b); and the second half follows from (a), which says that

$$\{\mathscr{C}\subset S(K)\colon \#\mathscr{C}<\infty\} = \{\mathscr{C}\subset S(K)\colon \hat{H}(\mathscr{C})=0\}. \quad \square$$

Proof of Theorem 1.3. (b) Let

$$\nu(\mathscr{C},\hat{h};B) = \#\{P\in\mathscr{C}\colon \hat{h}(P)\leqq B\}$$

be the counting function of $\mathscr{C}$ relative to the canonical height $\hat{h}$. Fix any point $Q\in\mathscr{C}$. Then the map

$$\mathscr{A}\to\mathscr{C}, \qquad \phi\mapsto\phi Q,$$

is surjective and $\mu(\mathscr{C})$-to-1, so

$$\begin{aligned}
\mu(\mathscr{C})\,\nu(\mathscr{C},\hat{h};B) &= \#\{\phi\in\mathscr{A}\colon \hat{h}(\phi Q)\leqq B\}\\
&= \#\{\phi\in\mathscr{A}\colon \alpha^{\ell(\phi)}\hat{h}^{\chi(\phi)}(Q)+\alpha^{-\ell(\phi)}\hat{h}^{-\chi(\phi)}(Q)\leqq B\}\\
&= \#\{n\in\mathbb{Z}\colon \alpha^n\hat{h}^{\chi(n)}(Q)+\alpha^{-n}\hat{h}^{-\chi(n)}(Q)\leqq B\}\\
&= \#\{m\in\mathbb{Z}\colon (\alpha^2)^m\hat{h}^+(Q)+(\alpha^2)^{-m}\hat{h}^-(Q)\leqq B\}\\
&\quad + \#\{m\in\mathbb{Z}\colon (\alpha^2)^m(\alpha\hat{h}^+(Q))+(\alpha^2)^{-m}(\alpha^{-1}\hat{h}^-(Q))\leqq B\}.
\end{aligned}$$

To conclude the proof of Theorem 1.3(b), we will apply the following elementary counting lemma to each of the last two terms.

Lemma. *Let a, b, $B>0$ and $\lambda>1$ be constants, and let*

$$\Sigma(B)=\{m\in\mathbb{Z}:\ \lambda^m a+\lambda^{-m} b\leqq B\}.$$

If $B^2<4ab$, then $\Sigma(B)=\emptyset$. If $B^2\geqq 4ab$, then

$$-1\leqq \#\Sigma(B)-\log_\lambda\frac{B^2}{4ab}\leqq 1+\log_\lambda(4).$$

Proof. Notice that

$$m\in\Sigma(B)\Leftrightarrow a\lambda^{2m}-B\lambda^m+b\leqq 0$$
$$\Leftrightarrow \frac{2b}{B+\sqrt{B^2-4ab}}\leqq\lambda^m\leqq\frac{B+\sqrt{B^2-4ab}}{2a}.$$

In particular, if $B^2<4ab$, then there are no values of m, so $\#\Sigma(B)=0$.

Now we assume that $B^2\geqq 4ab$. Then every $m\in\Sigma(B)$ satisfies the inequality $b/B\leqq\lambda^m\leqq B/a$, so

$$\#\Sigma(B)\leqq\#\left\{m\in\mathbb{Z}:\ \log_\lambda\frac{b}{B}\leqq m\leqq\log_\lambda\frac{B}{a}\right\}\leqq 1+\log_\lambda\frac{B^2}{ab}.$$

Similarly, if $2b/B\leqq\lambda^m\leqq B/2a$, then m will be in $\Sigma(B)$, so

$$\#\Sigma(B)\geqq\#\left\{m\in\mathbb{Z}:\ \log_\lambda\frac{2b}{B}\leqq m\leqq\log_\lambda\frac{B}{2a}\right\}\geqq -1+\log_\lambda\frac{B^2}{4ab}.$$

This concludes the proof of the Lemma.

Resuming the proof of Theorem 1.3(b), we use the Lemma twice (and the assumption that $B^2\geqq 4\hat{H}(\mathscr{C})$) to conclude that

$$-2\leqq\mu(\mathscr{C})\,\nu(\mathscr{C},\hat{h};B)-2\log_{\alpha^2}\frac{B^2}{4\hat{H}(\mathscr{C})}\leqq 2+2\log_{\alpha^2}(4).$$

(Note that $\hat{H}(\mathscr{C})=\hat{h}^+(Q)\,\hat{h}^-(Q)$ by definition.) Since $2\log_{\alpha^2}4=\log_\alpha 4\approx 1.05$, this is stronger than the desired result.

(c) Since $\hat{h}$ and h_D are both Weil height functions with respect to ample divisors, there is a constant $c>0$ such that

$$c^{-1}h_D(P)\leqq\hat{h}(P)\leqq c\,h_D(P)\qquad\text{for all }P\in S(\bar{K}).$$

Hence continuing with the notation from (b), we have

$$\nu(\mathscr{C},h_D;c^{-1}B)\leqq\nu(\mathscr{C},\hat{h};B)\leqq\nu(\mathscr{C},h_D;cB),$$

so (c) follows immediately from (b). □

Proof of Theorem 1.4. From Theorem 1.2(a), a point has canonical height 0 if and only if it is in $S(K)_{\text{fin}}$; and from Theorem 1.3(a), a chain $\mathscr{C}$ has no points with canonical height less than $2\sqrt{\hat{H}(\mathscr{C})}$. Hence using Theorem 1.3(b), we find

$$\#\{P\in S(K):\ \hat{h}(P)\leqq B\}=\#S(K)_{\text{fin}}+\sum_{\substack{\mathscr{C}\subset S(K)\\ 0<4\hat{H}(\mathscr{C})\leqq B^2}}\ \sum_{\substack{P\in\mathscr{C}\\ \hat{h}(P)\leqq B}}1$$
$$=\#S(K)_{\text{fin}}+\sum_{\substack{\mathscr{C}\subset S(K)\\ 0<4\hat{H}(\mathscr{C})\leqq B^2}}\left\{\frac{1}{\mu(\mathscr{C})}\log_\alpha\frac{B^2}{4\hat{H}(\mathscr{C})}+\varepsilon(\mathscr{C})\right\}.$$

From Theorem 1.2(b), the set $S(K)_{\text{fin}}$ is finite; and from Theorem 1.3(b), the error $\varepsilon(\mathscr{C})$ satisfies $|\varepsilon(\mathscr{C})|\leqq 4$. □

Proof of Corollary 1.5 Let $P \in S(\bar{K})$ be a point whose chain $\mathscr{C}(P)$ is stable under the action of $\mathrm{Gal}(\bar{K}/K)$, and let

$$\mathscr{A}_P = \{\phi \in \mathscr{A} : \phi P = P\}$$

be the stabilizer of P. We consider two cases, according to whether or not $\mathscr{A}_P$ is trivial.

Suppose first that $\# \mathscr{A}_P > 1$. If it contains an element of the form $(\sigma_1 \sigma_2)^k$, $k \neq 0$, then $\mathscr{A}_P$ has finite index inside $\mathscr{A}$. Since $\mathscr{A}/\mathscr{A}_P \xleftrightarrow{\text{one-to-one}} \mathscr{C}(P)$, this implies that $\mathscr{C}(P)$ is finite, so (ii) holds. Otherwise $\mathscr{A}_P$ must contain an element of the form $\tau \sigma_j \tau^{-1}$, since these are the only other elements in $\mathscr{A}$. Let $\psi \in \mathscr{A}_P$ be such an element of order 2, and notice that $\chi(\psi) = -1$.

Now if $P \in S(K)$, then P satisfies (i) and we're done with this case; so we may as well assume that there is some $\gamma \in \mathrm{Gal}(\bar{K}/K)$ with $\gamma P \neq P$. On the other hand, we know that $\gamma P \in \mathscr{C}(P)$, say $\gamma P = \phi P$ for some $\phi \in \mathscr{A}$. Since $\psi P = P$, we also have $\gamma P = \phi \psi P$. Using the fact that $\chi(\phi\psi) = \chi(\phi)\chi(\psi) = -\chi(\phi)$ and replacing ϕ by $\phi\psi$ if necessary, we may assume that

$$\gamma P = \phi P, \quad \chi(\phi) = 1, \quad \text{and} \quad \ell(\phi) \neq 0.$$

(Note $\ell(\phi) = 0 \Rightarrow \phi = e \Rightarrow \gamma P = \phi P = P$, contrary to our assumptions.)

We next observe that height functions are Galois invariant. (See, e.g., [12, VIII.5.10].) Hence

$$\hat{h}^+(P) = \hat{h}^+(\gamma P) = \hat{h}^+(\phi P) = \alpha^{l(\phi)} \hat{h}^+(P), \qquad \text{since } \chi(\phi) = 1.$$

But $\alpha^{\ell(\phi)} \neq 1$, so we conclude that $\hat{h}^+(P) = 0$, and from Theorem 1.1(vii) that $\mathscr{C}(P)$ is finite. Thus P again satisfies (ii).

It remains to consider the case that $\mathscr{A}_P$ is trivial. In this case, for every $\gamma \in \mathrm{Gal}(\bar{K}/K)$ there is a *unique* $\phi_\gamma \in \mathscr{A}$ such that $\gamma P = \phi_\gamma P$. We thus get a well-defined homomorphism

$$\mathrm{Gal}(\bar{K}/K) \to \mathscr{A}, \qquad \gamma \mapsto \phi_\gamma,$$

whose kernel is precisely $\mathrm{Gal}(\bar{K}/K(P))$. Hence $K(P)$ is a Galois extension of K, and its Galois group injects into $\mathscr{A}$. But the only finite subgroups of $\mathscr{A}$ are groups of order 1 or 2. Therefore either $K(P) = K$, which is condition (i); or else $[K(P):K] = 2$, which is the first part of condition (iii). It remains to show that in this last case, the other parts of condition (iii) are true.

If we write $\mathrm{Gal}(K(P)/K) = \{e, \gamma\}$, then we know that ϕ_γ has order 2, so $\phi_\gamma = \tau^{-1} \sigma_j \tau$ for some $\tau \in \mathscr{A}$, $j \in \{1, 2\}$. It follows that

$$\gamma(\tau P) = \tau(\gamma P) = \tau \phi_\gamma P = \sigma_j(\tau P), \text{ so}$$

$$\gamma(p_j(\tau P)) = p_j(\gamma(\tau P)) = p_j(\sigma_j(\tau P)) = p_j(\tau P).$$

Therefore $p_j(\tau P)$ is fixed by $\mathrm{Gal}(K(P)/K)$, hence $p_j(\tau P) \in \mathbb{P}^2(K)$. This proves the second part of condition (iii); and the third part is immediate, since we are considering the case where $\# \mathscr{A}_P = 1$. $\square$

5 A numerical example

In this section we will choose a particular K3 surface and calculate the heights of some of its rational points. By changing coordinates, we may as well asssume that our bilinear form gives the usual flag manifold in $\mathbb{P}^2 \times \mathbb{P}^2$,

$$L(\mathbf{x}, \mathbf{y}) = x_1 y_1 + x_2 y_2 + x_3 y_3.$$

We intersect the flag manifold with a "randomly chosen" surface of type (2, 2) given by the equation

$$\begin{aligned} Q(\mathbf{x}, \mathbf{y}) = {} & x_1^2 y_1^2 + 3x_1 x_2 y_1^2 + x_2^2 y_1^2 + 4x_1^2 y_1 y_2 + 3x_1 x_2 y_1 y_2 - 2x_3^2 y_1 y_2 \\ & - x_1^2 y_2^2 + 2x_2^2 y_2^2 - x_1 x_3 y_2^2 - 4x_2 x_3 y_2^2 + 5x_1 x_3 y_1 y_3 \\ & - 4x_2 x_3 y_1 y_3 + 7x_1^2 y_2 y_3 + 4x_2^2 y_2 y_3 + x_1 x_2 y_3^2 + 3x_3^2 y_3^2. \end{aligned}$$

Then our surface is the locus in $\mathbb{P}^2 \times \mathbb{P}^2$ given by the two equations

$$S\colon L(\mathbf{x}, \mathbf{y}) = Q(\mathbf{x}, \mathbf{y}) = 0.$$

A brief (5 hours on a Macintosh IIcx) search reveals that there are twelve rational points on S with multiplicative height less than or equal to 40.

$$\begin{aligned} \{ & ([0,1,1],[1,1,-1]), ([1,0,0],[0,0,1]), ([0,1,0],[0,0,1]), \\ & ([1,0,-1],[0,1,0]), ([0,0,1],[0,1,0]), ([0,0,1],[1,0,0]), \\ & ([3,1,3],[-3,3,2]), ([1,0,0],[0,7,1]), ([8,6,9],[-6,5,2]), \\ & ([1,0,-1],[9,1,9]), ([3,8,11],[1,1,-1]), ([12,1,-20],[2,-4,1]) \} \end{aligned}$$

These twelve points lie in six distinct chains, each of which is (undoubtedly) infinite, although two of them are one sided. More precisely, ([0, 1, 0], [0, 0, 1]) is on the ramification locus of π_1, so is fixed by σ_1; and ([0, 0, 1], [1, 0, 0]) is on the ramification locus of π_2, so is fixed by σ_2. To illustrate the rapid growth of points in a given chain, we will look at the chain generated by ([0, 1, 0], [0, 0, 1]), which begins

$$P_1 \xrightarrow{\sigma_2} ([1,0,0],[0,0,1]) \xrightarrow{\sigma_1} ([1,0,0],[0,7,1])$$

$$\xrightarrow{\sigma_2} ([1645, -344, 2408], [0,7,1]) \xrightarrow{\sigma_1}.$$

In Table 1 we have listed the first few points in the chain generated by P_1. As expected, the coordinates grow extremely rapidly.

Table 1

ϕ	ϕP_1
e	[(0, 1, 0], [0, 0, 1])
σ_2	([1, 0, 0], [0, 0, 1])
$\sigma_1 \sigma_2$	([1, 0, 0], [0, 7, 1])
$\sigma_2 \sigma_1 \sigma_2$	([1645, −344, 2408], [0, 7, 1])
$(\sigma_1 \sigma_2)^2$	([1645, −344, 2408], $[-1.3 \cdot 10^{13}, 5.6 \cdot 10^{12}, 9.7 \cdot 10^{12}]$)
$\sigma_2 (\sigma_1 \sigma_2)^2$	($[2.2 \cdot 10^{49}, -3.0 \cdot 10^{49}, 4.6 \cdot 10^{49}]$, $[-1.3 \cdot 10^{13}, 5.6 \cdot 10^{12}, 9.7 \cdot 10^{12}]$)
$(\sigma_1 \sigma_2)^3$	($[2.2 \cdot 10^{49}, -3.0 \cdot 10^{49}, 4.6 \cdot 10^{49}]$, $[2.2 \cdot 10^{186}, 1.6 \cdot 10^{186}, 6.4 \cdot 10^{184}]$)
$\sigma_2 (\sigma_1 \sigma_2)^3$	($[-7.9 \cdot 10^{695}, 1.0 \cdot 10^{696}, 1.5 \cdot 10^{695}]$, $[2.2 \cdot 10^{186}, 1.6 \cdot 10^{186}, 6.4 \cdot 10^{184}]$)

Table 2

ϕ	$\ell(\phi)$	$\chi(\phi)$	$h_{E^+}(\phi P_1)$	$h_{E^-}(\phi P_1)$	$\alpha^{-\ell} h_{E^\chi}$ $(\ell(\phi) \geqq 0)$	$\alpha^{\ell} h_{E^{-\chi}}$ $(\ell(\phi) \leqq 0)$
e	0	1	0	0	0	0
σ_2	1	-1	0	0	0	
$\sigma_1 \sigma_2$	-2	1	-1.94591	7.26224		0.5214
$\sigma_2 \sigma_1 \sigma_2$	3	-1	27.1139	-0.524316	0.5216	
$(\sigma_1 \sigma_2)^2$	-4	1	-1.13758	104.912		0.5408
$\sigma_2(\sigma_1 \sigma_2)^2$	5	-1	396.612	-1.66497	0.5478	
$(\sigma_1 \sigma_2)^3$	-6	1	-2.22648	1486.82		0.5503
$\sigma_2(\sigma_1 \sigma_2)^3$	7	-1	5552.05	-1.44477	0.5506	

For any point $P = (\mathbf{x}, \mathbf{y}) \in \mathbb{P}^2 \times \mathbb{P}^2$, we normalize our height functions by taking the usual Weil height on $\mathbb{P}^2$ and setting

$$h_{E^+}(P) = \alpha h(\mathbf{x}) - h(\mathbf{y}) \quad \text{and} \quad h_{E^-}(P) = -h(\mathbf{x}) + \alpha h(\mathbf{y}).$$

In Table 2 we have computed the heights of the first few elements in the chain generated by P_1.

From Table 2 we see that

$$\hat{h}^+(P_1) \approx 2.1 \quad \text{and} \quad \hat{h}^-(P_1) \approx 0.55.$$

We are computing these values by the formula

$$\hat{h}^\pm(P) = \alpha^{\mp \ell(\phi)} \hat{h}^{\pm \chi(\phi)}(\phi P) = \alpha^{\mp \ell(\phi)} h_{E^{\pm \chi(\phi)}}(\phi P) + O(\alpha^{\mp \ell(\phi)}).$$

In order to make the error term on the right-hand-side of this equation small, we need to choose the plus/minus sign so that $\mp \ell(\phi) < 0$. So for each ϕ, Table 2 provides an approximation only to $\hat{h}^-(P_1)$, not to $\hat{h}^+(P_1)$. However, since our point P_1 satisfies $\sigma_1(P_1) = P_1$, it follows from the general theory that

$$\hat{h}^+(P_1) = \hat{h}^+(\sigma_1 P_1) = \alpha \hat{h}^-(P_1).$$

This allows us to approximate both canonical heights from Table 2.

In order to compute $\hat{h}^-(P_1)$ to d decimal places, we would need to choose ϕ so that $\alpha^{-|\ell(\phi)|} \ll 10^{-d}$. Taking $\phi = (\sigma_1 \sigma_2)^n$, this means that we would need to compute $(\sigma_1 \sigma_2)^n P_1$ with $n \geqq 0.87 d + O(1)$ in order to get d decimal places of accuracy. This is completely infeasible for even moderate values of d, since (some of) the coordinates of $(\sigma_1 \sigma_2)^n P_1$ will have around $\alpha^{2n} \approx 10^{1.14 n}$ digits. It seems worthwhile to consider some other method of computing the canonical heights $\hat{h}^+$ and $\hat{h}^-$, possibly by decomposing them into canonical local height functions, as is done for abelian varieties. (See [9, Chap. 11] for the general theory on abelian varieties, and [13] for the Silverman-Tate algorithm which allows one to efficiently compute canonical heights on elliptic curves.) We will consider this question of local decomposition and a computational algorithm in a subsequent paper.

6 Integral points and Vojta's conjecture

A brief look at Table 1 in the previous section reveals a somewhat surprising pattern. Suppose we agree to write points $P \in S(\mathbb{Q})$ in the normalized form

$$(*) \qquad P=([x_1, x_2, x_3], [y_1, y_2, y_3]) \quad \text{with } x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{Z}$$
$$\text{and} \quad \gcd(x_1, x_2, x_3)=\gcd(y_1, y_2, y_3)=1.$$

Then the larger points in Table 1 seem to satisfy

$$|x_1| \approx |x_2| \approx |x_3| \quad \text{and} \quad |y_1| \approx |y_2| \approx |y_3|.$$

This is similar to a phenomenon which occurs for elliptic curves. Thus suppose we take an elliptic curve

$$E: y^2 z = 4x^3 - g_2 x z^2 - g_3 z^3$$

defined over $\mathbb{Q}$ and a sequence of distinct points $P_n=[x_n, y_n, z_n] \in E(\mathbb{Q})$ written as above in normalized form. Such a point is integral if $|z_n|=1$. A famous theorem of Siegel says that there are only finitely many integral points. But Siegel actually proved the considerably stronger result that

$$\lim_{n\to\infty} \frac{\log \min\{|x_n|, |y_n|, |z_n|\}}{\log \max\{|x_n|, |y_n|, |z_n|\}} = 1.$$

(See [12, IX.3.3].)

The proof of Siegel's theorem uses the Thue-Siegel-Roth theorem. The following higher dimensional analogue of the Thue-Siegel-Roth theorem has been conjectured by Paul Vojta.

Conjecture (Vojta, [15]) *Let K be a number field, Σ a finite set of places of K, V/K a smooth projective variety, $A \in \mathrm{Div}(V)$ an ample divisor, $D \in \mathrm{Div}(V)$ an effective divisor with at worst normal crossings. There is a proper Zariski closed subset $Z=Z(V, D) \subset V$ so that for every $\varepsilon>0$,*

$$\sum_{v\in\Sigma} \lambda_D(P, v) + h_{\mathscr{K}_V}(P) \leqq \varepsilon h_A(P) + O(1) \qquad \textit{for all } P \in V(K),\ P \notin Z.$$

Here $\mathscr{K}_V$ is a canonical divisor on V, and $\lambda_D(\cdot, v)$ is a local height function on V for the divisor D and absolute value v. (Cf. [9, Chap. 10].) *The $O(1)$ constant depends on K, Σ, V, A, D, ε.*

Remark. Vojta states his conjecture with $Z=Z(K, \Sigma, V, A, D, \varepsilon)$, and says that the components of Z, other than individual points, can be chosen to depend only on V and D. We have merely adjusted the $O(1)$ to accomodate the finitely many isolated points in the original Z.

Taking the special case of Vojta's conjecture applied to K3 surfaces, we can prove the following result, which (conjecturally) explains the pattern in Table 1.

Proposition 6.1 *Let $S/\mathbb{Q}$ be a K3 surface as described in Sect. 1, and normalize the coordinates of $P \in S(\mathbb{Q})$ as described above in $(*)$. Let h be a height function* *on S corresponding to any ample divisor. Assume that Vojta's conjecture is true for S. Then there is a finite union of curves $Z \subset S$ so that*

$$\lim_{\substack{P \in S(\mathbb{Q}) \setminus Z \\ h(P) \to \infty}} \frac{\log \min\{|x_1(P)|, |x_2(P)|, |x_3(P)|\}}{\log \max\{|x_1(P)|, |x_2(P)|, |x_3(P)|\}} = 1.$$

A similar statement holds with x_1, x_2, x_3 replaced by y_1, y_2, y_3.

Proof. Let $f \in \mathbb{Q}[X_1, X_2, X_3]$ be a non-zero linear form, and let $H = \{f = 0\} \subset \mathbb{P}^2$ be the corresponding hyperplane section. We observe that the local height of a point $\mathbf{t} = [t_1, t_2, t_3] \in \mathbb{P}^2$ relative to the divisor H is given by the simple formula

$$\lambda_{\mathbb{P}^2, H}(\mathbf{t}, v) = \log \max\left\{\left|\frac{t_1}{f(\mathbf{t})}\right|_v, \left|\frac{t_2}{f(\mathbf{t})}\right|_v, \left|\frac{t_3}{f(\mathbf{t})}\right|_v\right\}.$$

(See [15, p. 8].) On the other hand, if $\mathbf{t} \in \mathbb{P}^2(\mathbb{Q})$ is normalized, then

$$h_{\mathbb{P}^2, H}(\mathbf{t}) = \log \max\{|t_1|, |t_2|, |t_3|\} + O(1),$$

where the $O(1)$ depends only on the linear form f defining H.

We are going to apply Vojta's conjecture with

$$V = S, \quad A = D_1 + D_2, \quad \text{and} \quad D = \pi_1^* H.$$

We observe first that

$$\alpha h_{D_1} = h_{D_2} + h_{E^+} + O(1) = h_{D_2} + \hat{h}^+ + O(1) \geqq h_{D_2} + O(1) \quad \text{since } \hat{h}^+ \geqq 0.$$

(Note we could not conclude directly from general principles that $h_{D_1} \gg h_{D_2}$, since D_1 is not ample.) Hence if we write $P = (\mathbf{x}, \mathbf{y})$ normalized as above, then

$$\begin{aligned} h_{S,A}(P) &= h_{S,D_1}(P) + h_{S,D_2}(P) + O(1) \\ &\leqq (\alpha + 1) h_{S,D_1}(P) + O(1) \\ &\leqq 4 h_{S,\pi_1^* H}(P) + O(1), \quad \text{since } D_1 \sim \pi_1^* H, \\ &= 4 h_{\mathbb{P}^2, H}(\mathbf{x}) + O(1) \\ &= 4 \log \max\{|x_1|, |x_2|, |x_3|\} + O(1). \end{aligned}$$

Now we apply Vojta's conjecture, using the field $\mathbb{Q}$ and the set consisting of the archimedean absolute value $\{\infty\}$. The canonical bundle on a K3 surface is trivial, so $\mathscr{K}_S = 0$. Hence there is a proper Zariski closed subset $Z \subset S$ so that

$$\lambda_{S, \pi_1^* H}(P, \infty) \leqq \varepsilon h_{S,A}(P) + O(1) \quad \text{for all } P \in S(\mathbb{Q}),\ P \notin Z.$$

Now $\lambda_{S, \pi_1^* H} = \lambda_{\mathbb{P}^2, H} \circ \pi_1 + O(1)$ by functoriality. So combining Vojta's inequality with the formula for $\lambda_{\mathbb{P}^2, H}$ and the estimate for $h_{S,A}(P)$ derived above, we find that

$$(1 - 4\varepsilon) \log \max\{|x_1|, |x_2|, |x_3|\} \leqq \log |f(\mathbf{x})| + O(1).$$

This holds for all $P=(\mathbf{x},\mathbf{y})\notin Z$, where $Z\subset S$ is fixed, and the $O(1)$ depends on S, f, and ε.

Applying this result three times, taking successively $f=X_1$, $f=X_2$, and $f=X_3$, we conclude that

$$\begin{aligned}&(1-4\varepsilon)\log\max\{|x_1|,|x_2|,|x_3|\}\\ &\qquad\leqq\log\min\{|x_1|,|x_2|,|x_3|\}+O_\varepsilon(1),\qquad \text{for all } P\in S(\mathbb{Q}),\ P\notin Z.\end{aligned}$$

Hence

$$1-4\varepsilon-O_\varepsilon\left(\frac{1}{h(P)}\right)\leqq\frac{\log\min\{|x_1|,|x_2|,|x_3|\}}{\log\max\{|x_1|,|x_2|,|x_3|\}}\leqq 1,\qquad \text{for all } P\in S(\mathbb{Q}),\ P\notin Z.$$

Now let $h(P)\to\infty$ with $P\in S(\mathbb{Q})$, $P\notin Z$. This gives

$$\begin{aligned}1-4\varepsilon&\leqq\liminf_{\substack{P\in S(\mathbb{Q})\setminus Z\\ h(P)\to\infty}}\frac{\log\min\{|x_1|,|x_2|,|x_3|\}}{\log\max\{|x_1|,|x_2|,|x_3|\}}\\ &\leqq\limsup_{\substack{P\in S(\mathbb{Q})\setminus Z\\ h(P)\to\infty}}\frac{\log\min\{|x_1|,|x_2|,|x_3|\}}{\log\max\{|x_1|,|x_2|,|x_3|\}}\leqq 1.\end{aligned}$$

Since this holds for every $\varepsilon>0$, the limit exists and equals 1. □

Remark. A proof of Vojta's conjecture, even for K3 surfaces, seems difficult, although possibly not hopeless in view of the recent advances made by Vojta [16] and Faltings [4]. A more tractable problem might be to show that on the K3 surfaces studied in this paper, if one fixes a chain $\mathscr{C}$ of rational points, then the conclusion of Proposition 6.1 holds if the limit is taken over points in $\mathscr{C}$. Note that this does not reduce to Siegel's theorem (i.e. integral points on a curve), since we have shown that $\mathscr{C}$ is Zariski dense in S. But one might hope to use the additional structure provided by the group of automorphisms $\mathscr{A}$ acting on $\mathscr{C}$ and $\mathrm{Pic}(S)$, just as the group structure on an abelian variety is exploited in the proofs of Faltings and Vojta.

Acknowledgements. I would like to thank Alan Landman, Yuri Manin, Gisbert Wüstholz, and the referee for their valuable assistance and suggestions.

References

1. Arbarello, E., Cornalba, M., Griffiths, P.A., Harris, J.: Geometry of algebraic curves, vol. 1. (Grund. math. Wiss., vol. 267.) Berlin Heidelberg New York: Springer 1985
2. Batyrev, V.V., Manin, Yu.: Sur le nombre des points rationnels de hauteur borné des variétés algébriques. Math. Ann. **286**, 27–44 (1990)
3. Beauville, A.: Complex Algebraic Surfaces. (Lond. Math. Soc. Lect. Note Ser., vol. 68.) Cambridge: Cambridge University Press 1983
4. Faltings, G.: Diophantine approximation on abelian varieties. Ann. Math. (to appear)
5. Franke, J., Manin, Yu., Tschinkel, Yu.: Rational points of bounded height on Fano varieties. Invent. Math. **95**, 421–435 (1989)
6. Griffiths, P., Harris, J.: Algebraic Geometry. New York: Wiley Interscience 1978

7. Griffiths, P., Harris, J.: On the Noether-Lefschetz theorem and some remarks on codimension-two cycles. Math. Ann. **271**, 31–51 (1985)
8. Hartshorne, R.: Algebraic Geometry. Berlin Heidelberg New York: Springer 1977
9. Lang, S.: Fundamentals of Diophantine Geometry. Berlin Heidelberg New York: Springer 1983
10. Lefschetz, S.: L'analysis situs et la géométrie algébrique. Paris: Gauthier-Villars 1924
11. Mori, S., Mukai, Sh.: The uniruledness of the moduli space of curves of genus 11 (Lect. Notes Math., vol. 1016, pp. 334–353). Berlin Heidelberg New York: Springer 1983
12. Silverman, J.H.: The Arithmetic of Elliptic Curves. Berlin Heidelberg New York: Springer 1986
13. Silverman, J.H.: Computing heights on elliptic curves. Math. Comput. **51**, 339–358 (1988)
14. Swinnerton-Dyer, H.P.F.: Applications of algebraic geometry to number theory. Proc. Symp. Pure Math., vol. 20) Providence: Am. Math. Soc. 1971
15. Vojta, P.: Diophantine approximations and value distribution theory (Lect. Notes Math., vol. 1239). Berlin Heidelberg New York: Springer 1987
16. Vojta, P.: Siegel's theorem in the compact case. Ann. Math. (to appear)
17. Wehler, J.: K3-surfaces with Picard number 2. Arch. Math. **50**, 73–82 (1988)
18. Wehler, J.: Hypersurfaces of the Flag Variety. Math. Z. **198**, 21–38 (1988)