

# Automorphs of indefinite binary quadratic forms and K3-surfaces with Picard number 2

Federica GALLUZZI, Giuseppe LOMBARDO and Chris PETERS

April 5, 2008

## Abstract

Every indefinite binary form occurs as the Picard lattice of some K3-surface. The group of its isometries, or automorphs, coincides with the automorphism group of the K3-surface, but only up to finite groups. The classical theory of automorphs for binary forms can then be applied to study these automorphism groups. Some extensions of the classical theory are needed to single out the orthochronous automorphs, i.e. those that conserve the “light cone”. Secondly, one needs to study in detail the effect of the automorphs on the discriminant group. The result is a precise description of all possible automorphism groups of “general” K3’s with Picard number two.

## Introduction

A K3-surface is a simply connected projective surface with trivial canonical bundle. Despite this abstract definition, K3’s have been classified in detail. See for instance [BHPV, Chap. 8] and the literature cited there. In § 3 we collect the necessary material.

The general theory of automorphisms of K3-surfaces is largely due to Nikulin, cf. [Nik1, Nik2, Nik3]. The case of Picard number 1 turns out to be quite easy to deal with. The automorphism group is finite and almost always the identity [Nik3]. The question of which finite groups are possible has been answered in detail by Nikulin and this question has been further investigated by Mukai [Muk] and Kondō [Kon1, Kon2]. Further attention has also been given to those groups that act trivially on the transcendental lattice, the *symplectic* automorphisms, [G-S1, G-S2].

The case of Picard number 2 has been briefly touched upon in [P-SS] where Severi’s example [Sev] of a K3 with the infinite dihedral group as automorphism group is put into perspective by tying it in with the classical theory of binary quadratic forms. Furthermore, some special cases of K3’s with Picard group of rank 2 appear in the literature [W, Bi, Ge, G-L].

This note can be viewed as a systematic study of possible automorphism groups of K3’s with Picard number 2. The above examples will be placed within this general context.

As one can surmise, number theory of integral bilinear forms plays a central role through the solutions for the classical Pell equations. Since many algebraic geometers are not very familiar with this classical theory we have collected some of these results in § 2. They are complemented with new results, e.g in § 2.3–2.6. In § 3 these are applied to automorphism groups of K3-surfaces. It turns out that for “most” K3-surfaces with Picard number 2 the automorphism group can be determined in terms of explicit number theoretic properties of the intersection form on the Picard group. In § 4 we give some examples for which the number theoretic data can be made explicit and we explain where the examples previously treated in the literature fit in.

The first two authors would like to thank Bert van Geemen for several fruitful discussions.

**Notation and terminology.** A quadratic form

$$q(x_1, \dots, x_n) = \sum_{i \leq j} q_{ij} x_i x_j$$

in  $n$  variables with coefficients in a field  $k$  of characteristic  $\neq 2$  determines and is determined by the bilinear form  $Q$  obtained from it by polarization. By convention  $Q$  is obtained from  $q$  by placing  $q_{ii}$  on the  $i$ -th diagonal entry and  $\frac{1}{2}q_{ij}$  on the  $(i, j)$ -th and  $(j, i)$ -th entry. Its determinant  $d(q)$  is called the *discriminant* of  $q$ . It is well defined up to squares in  $k$ . If  $d(q) = \pm 1$  the form is called *unimodular*. A word of warning: conventionally, for a quadratic form  $ax^2 + bxy + cy^2$  in two variables, its discriminant  $b^2 - 4ac$  is the negative of the discriminant of the associated bilinear form!

Note that if a quadratic form has integral coefficients, its associated bilinear form has half-integral off-diagonal elements. Nevertheless such quadratic forms are called *integral*.

If  $X$  is any complex projective variety we let  $\text{Aut}(X)$  be its group of biholomorphic automorphisms. A group  $G$  generated by  $a, b, c, \dots$  is denoted  $\langle a, b, c, \dots \rangle$ . The infinite dihedral group  $\mathbb{D}_\infty = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} = \langle s, t \rangle$  is the group generated by two non-commuting involutions  $s$  and  $t$ .

## 1 Automorphism groups of lattices

A *lattice* is a pair  $(S, Q)$  of a free finite rank  $\mathbb{Z}$ -module  $S$  together with a bilinear form  $Q : S \times S \rightarrow \mathbb{Z}$ . So  $S = \mathbb{Z}^r$  with the standard basis yields a bilinear form with integral coefficients. A lattice is *even* if  $Q(\mathbf{v}, \mathbf{v}) \in 2\mathbb{Z}$  for all  $\mathbf{v} \in S$ . If  $S = \mathbb{Z}^r$  this means that the diagonal entries of  $Q$  with respect to the standard basis are even. A lattice which is not even is called *odd*. For a bilinear form  $Q$  and  $m \in \mathbb{Z}$ , the form  $mQ$  denotes  $(\mathbf{v}, \mathbf{w}) \mapsto mQ(\mathbf{v}, \mathbf{w})$ . For instance, if  $q$  is integral, the form  $2Q$  determines an even lattice and conversely.

An even indefinite unimodular form is uniquely determined by its parity (i.e. if it is even or not) and its signature. See e.g. [Se]. For

instance, the hyperbolic plane  $H$  given by

$$(\mathbf{u}, \mathbf{v}) \mapsto {}^t \mathbf{u} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mathbf{v}.$$

is the unique unimodular even lattice of signature  $(1, 1)$  which is denoted by the same symbol. The group of isometries of a lattice  $(S, Q)$  is denoted either as  $O(S)$  or as  $O(Q)$ . Those of determinant 1 are denoted  $SO(S)$  or  $SO(Q)$ .

For any lattice  $(S, Q)$  the dual lattice  $S^*$  is defined by

$$S^* = \{x \in S \otimes \mathbb{Q} \mid Q(x, y) \in \mathbb{Z} \text{ for all } y \in S\}.$$

We have  $S \subset S^*$  and the quotient

$$\text{discr}(S) = S^*/S \quad \text{the } \textit{discriminant group} \text{ of } S$$

is a finite abelian group of order equal to the absolute value of the discriminant  $|d(Q)|$ . An isometry  $g$  of  $S$  induces a group automorphism on  $S^*/S$  which will be noted  $\bar{g}$ .

Now we assume that  $(S, Q)$  is a lattice of signature  $(1, k)$  with  $k \geq 1$ . In this situation the *light cone*

$$\{x \in S \otimes_{\mathbb{Z}} \mathbb{R} \mid Q(x, x) > 0\} = C \amalg -C \quad (1)$$

decomposes in two connected components  $C$  and  $-C$ . We introduce the *orthochronous Lorentz group* and the *special orthochronous Lorentz group*

$$O^+(S) = \{g \in O(S) \mid g(C) = C\}, \quad SO^+(S) = O^+(S) \cap SO(S).$$

A *root* of  $S$  is a vector  $\mathbf{d}$  with  $Q(\mathbf{d}, \mathbf{d}) = -2$ . It defines a reflection  $x \mapsto x + Q(x, \mathbf{d})\mathbf{d}$  which is an isometry of  $S$  with fixed hyperplane  $H_{\mathbf{d}}$ . All these reflections generate the *Weyl group*  $W_S$ .

The complement inside  $C$  of all hyperplanes  $H_{\mathbf{d}}$  forms a disjoint union of fundamental domains  $D$  for the action of the reflection group  $W(S)$  generated by these hyperplanes. For some subset  $R_D$  of roots the fundamental domain  $D$  can be written as

$$D = \{x \in C \mid Q(x, \mathbf{d}) > 0 \text{ for all } \mathbf{d} \in R_D.\} \quad (2)$$

The subset  $R_D$  turns out to be a set of *positive roots*: all roots are either positive or negative integral linear combinations of roots from  $R_D$ . Conversely any set  $R$  of positive roots determines a unique chamber  $D$  for which  $R_D = R$ . Choosing a different cone gives a different system of positive roots and the isometries preserving this one leads to a conjugate group. Indeed, introducing the *reduced orthochronous Lorentz group*

$$O^\dagger(S) = \{g \in O(S) \mid g(D) = D\}$$

we have

$$O^+(S) = O^\dagger(S) \ltimes W(S). \quad (3)$$

We also introduce the following group

$$\tilde{O}^\dagger(S) := \{(\epsilon, \mathbf{g}) \in \mu_2 \times O^\dagger(S) \mid \bar{\mathbf{g}} = \epsilon \in \text{discr}(S)\}. \quad (4)$$

*Remark 1.1.* The natural homomorphism  $\tilde{O}^\dagger(S) \rightarrow O^\dagger(S)$  is injective unless  $\text{discr}(S)$  is trivial or a 2-group.

## 2 Indefinite integral binary quadratic forms

### 2.1 Pell's equation

Let  $d$  be any positive integer. The two Pell equations associated to  $d$  are:

$$x^2 - dy^2 = 4 : \quad \text{the positive Pell equation;} \quad (5)$$

$$x^2 - dy^2 = -4 : \quad \text{the negative Pell equation.} \quad (6)$$

Solutions of (5) always exist, but this is not true for (6).

There are also the *reduced* Pell equations where the right hand side has been replaced by  $\pm 1$ . Two cases are important for us:

1.  $d \equiv 0 \pmod{4}$ . In this case  $x$  is even, say  $x = 2\bar{x}$  and  $(\bar{x}, y)$  is a solution of the reduced equation for  $\frac{1}{4}d$  if and only if  $(x, y)$  is a solution of the (full) Pell equation for  $d$ ;
2.  $d \equiv 1 \pmod{4}$ . In this case  $x$  and  $y$  have the same parity and if they are both even, say  $x = 2\bar{x}$ ,  $y = 2\bar{y}$ , then  $(\bar{x}, \bar{y})$  is a solution of the reduced Pell equation for  $d$  if and only if  $(x, y)$  is a solution of the full Pell equation for  $d$ .

Note that if  $u^2 - dv^2 = 1$  gives a minimal positive solution, to any prime divisor  $p$  of  $d$  we can associate the unique number  $\epsilon(p) = \pm 1$  such that  $u \equiv \epsilon(p) \pmod{p}$ . In Table 1) we have collected the smallest positive solutions  $(x, y)$  of the two positive Pell equations for some values of  $d$ . In the first column we put  $d$  factored into primes, in the second column the minimal positive solution  $(u, v)$  is exhibited for  $x^2 - dy^2 = 1$ , while in the third column the minimal solution for  $x^2 - dy^2 = 4$  can be found. In the last column the numbers  $\epsilon(p)$  are gathered in a vector with entries according to the prime decomposition of  $d$ . The table has been composed using [Pell].

The solutions of the positive Pell equation behave fundamentally differently according to when  $d$  is a square or not:

**Lemma 2.1.** *If  $d$  is a square, the only solutions of (5) are  $u = \pm 2$  and  $v = 0$ .*

*If  $d$  is not a square, let  $(U, V)$  be the smallest positive solution of (5), i.e.  $U, V > 0$  are as small as possible and write  $\epsilon = \frac{1}{2}(U + V\sqrt{d})$ . Then all solutions are generated by powers of  $\epsilon$  in the sense that writing  $\epsilon^n = \frac{1}{2}(u + v\sqrt{d})$ ,  $(u, v)$  is a new solution and all solutions can be obtained that way.*

*If  $(U', V')$  is a minimal positive solution for (6) and  $\eta = \frac{1}{2}(U' + V'\sqrt{d})$ , then  $\eta^2 = \epsilon$  gives the minimal solution for (5), the even powers of  $\eta$  thus provide all solutions of the positive Pell equation, while the odd powers yield all solutions to the negative Pell equation.*

Note that  $\mathbb{Q}(\sqrt{d})$  is a quadratic extension of  $\mathbb{Q}$  and the units of norm 1 in the ring of integers  $\mathcal{O}(\sqrt{d})$  in this field are the elements

$d$	$N = 1$	$N = 4$	$\epsilon(p)$
3	(2, 1)	(4, 2)	-1
5	(9, 4)	(3, 1)	-1
$6 = 2 \cdot 3$	(5, 2)	(10, 4)	(1, -1)
7	(8, 3)	(16, 6)	1
$8 = 2 \cdot 2 \cdot 2$	(3, 1)	(6, 2)	1
11	(10, 3)	(20, 6)	-1
13	(649, 180)	(11, 3)	-1
17	(33, 8)	(66, 33)	-1
$15 = 3 \cdot 5$	(4, 1)	(8, 2)	(1, -1)
$20 = 5 \cdot 2 \cdot 2$	(9, 2)	(18, 3)	(1, -1)
$21 = 3 \cdot 7$	(55, 21)	(5, 1)	(1, -1)
$33 = 3 \cdot 11$	(23, 4)	(46, 8)	(-1, 1)
$35 = 5 \cdot 7$	(6, 1)	(12, 2)	(1, -1)
$39 = 3 \cdot 13$	(25, 4)	(50, 8)	(1, -1)
$44 = 11 \cdot 2 \cdot 2$	(199, 30)	(398, 60)	(1, 1)
$51 = 3 \cdot 17$	(50, 7)	(100, 14)	(-1, -1)
$55 = 5 \cdot 11$	(89, 12)	(178, 24)	(-1, 1)
$104 = 2 \cdot 2 \cdot 2 \cdot 13$	(51, 5)	(102, 10)	(1, -1)
$105 = 3 \cdot 5 \cdot 7$	(41, 4)	(82, 8)	(-1, 1, -1)
$165 = 3 \cdot 5 \cdot 11$	(1079, 84)	(13, 1)	(-1, -1, 1)

Table 1: Minimal positive solutions of  $x^2 - dy^2 = N$ .

$\alpha = \frac{1}{2}(u + v\sqrt{d})$  where  $(u, v)$  is an integer solution of (5). The trivial solution  $(2, 0)$  corresponds to 1 in this ring. The elements of norm -1 correspond to the solutions of (6). We shall need the following auxiliary result:

**Lemma 2.2.** *Let  $\eta = \frac{1}{2}(U + V\sqrt{d})$  be the unit corresponding to the minimal positive solution of (5). Then  $\eta^k = a_k\eta - b_k$ ,  $-\eta^{-k} = c_k\eta - d_k$  with  $a_k, b_k, c_k, d_k > 0$  for  $k > 0$ . In other words any solution of (5) is expressible as an integral linear combination of the two solutions  $\eta$  and  $-1$  with either negative or positive coefficients.*

*Proof:* Note that  $U \geq 2$  and that  $\eta^2 = U\eta - 1$  and hence  $a_2 = U$ ,  $b_2 = 1$ . Then we have the recursive formulas  $a_{k+1} = a_kU - b_k$ ,  $b_{k+1} = a_k$ . These inductively imply that for  $k > 0$  one has  $a_k/b_k \geq 1$ . One needs to show that  $a_k > 0$  and  $b_k > 0$ . The recursive formulas show that by induction we have  $a_{k+1} = \left(\frac{a_k}{b_k}U - 1\right)b_k \geq (U - 1)b_k > 0$  and  $b_{k+1} = a_k > 0$ . A similar argument applies to  $c_k$  and  $d_k$ .  $\square$

## 2.2 Isometries

In this section we summarize the classical theory of binary quadratic forms (over a field  $k$  of characteristic 0) in a way adapted to our needs. We are in particular interested in the associated orthogonal groups.

Recalling our convention, a quadratic form  $q(x, y) = ax^2 + bxy + cy^2$  is associated to the bilinear form  $Q$  given by

$$Q(\mathbf{v}, \mathbf{w}) = {}^t\mathbf{v} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \mathbf{w}.$$

**Definition 2.3.** We say that  $Q$  is *equivalent* to  $Q'$ , written  $Q' \sim Q$ , if for some invertible 2 by 2 matrix  $P$  one has  $Q' = {}^tPQP$ . The associated quadratic forms are also said to be equivalent:  $q' \sim q$ . The special case  $Q = Q'$  gives the *automorphs*  $T$  of  $q$ . If  $\det P > 0$  we speak of *proper equivalence*.

The quantity  $b^2 - 4ac$  is the *discriminant*  $d(Q)$  of  $Q$  (or of  $q$ ) and remains invariant under equivalence.

Recall that  $q$  is called *integral* if  $a, b, c \in \mathbb{Z}$ ; such a form is *primitive* if  $(a, b, c)$  have no common divisors. If  $q$  admits automorphs  $P$  with  $\det P = -1$  we say that  $q$  is *ambiguous*.

Positive discriminant means that  $Q$  is indefinite. Indeed, one has:

**Lemma 2.4.** *In the field  $k$  the quadratic form  $q$  is equivalent to the diagonal form  $d_{4,-d} := 4x^2 - dy^2$ :*

$$16aQ = {}^tP \begin{pmatrix} 4 & 0 \\ 0 & -d \end{pmatrix} P, \quad P = \begin{pmatrix} 2a & b \\ 0 & 2 \end{pmatrix} \quad (7)$$

Assume that  $q$  is integral. By (7) one can find  $O(Q)$  by comparing  $d_{4,-d}$  and  $16aQ$ . We may furthermore assume that  $q$  is *primitive*. Automorphs of the diagonal form  $d_{4,-d}$  immediately lead to solutions of the first of the two Pell equations which are associated to  $d$ ; indeed, using (7) and Lemma 2.1 one finds:

**Proposition 2.5** ([Jones, Th. 50, Th. 51c], [Dickson, Theorem 87]). *Suppose that the quadratic form  $q$  is primitive and that  $a \neq 0$ . The group of special isometries  $SO(Q)$  of  $Q$  is isomorphic to the direct product of the cyclic group  $\mathbb{Z}/2\mathbb{Z}$  generated by  $-\text{id}$  and the infinite cyclic group generated by*

$$\mathbf{u} := \begin{pmatrix} \frac{1}{2}[U - bV] & -cV \\ aV & \frac{1}{2}[U + bV] \end{pmatrix}. \quad (8)$$

where as before,  $(U, V)$  is a minimal positive solution of the Pell equation (5). A general proper automorph  $\pm \mathbf{u}^k$  of  $Q$  is (up to sign) of the form (8) with  $(U, V)$  replaced with a suitable solution  $(u, v)$  of the Pell equation (5) (see Lemma 2.1).

If  $d$  is a square,  $SO(Q) = \pm \text{id}$ .

*Remark 2.6.* To see the connection with the units in the quadratic field  $K = \mathbb{Q}(\sqrt{d})$  we proceed as follows. Let  $\{\omega_+, \omega_-\}$  be the two roots of

$$a\omega^2 + b\omega + c = 0, \quad \omega_{\pm} = \frac{-b \pm \sqrt{d}}{2a}. \quad (9)$$

Then in  $K$  the form  $q$  is equivalent to the standard hyperbolic form  $h(x, y) = 2xy$ :

$$8aQ = {}^t P \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} P, \quad P = 2a \begin{pmatrix} 1 & -\omega_- \\ 1 & -\omega_+ \end{pmatrix}.$$

Moreover, we have

$$\mathbf{u} = P^{-1} \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} P.$$

This representation shows that  $\mathrm{SO}^+(Q)$  is generated by  $\mathbf{u}$ : the first quadrant can be taken to represent the cone  $C$  (see (1)) and  $\mathbf{u}$  preserves  $C$  while  $-\mathrm{id}$  does not.

To find all isometries, one needs to add at most one involution:

**Proposition 2.7** ([Jones, Th. 52]). *If  $q$  is ambiguous, i.e.  $Q$  admits an isometry of determinant  $-1$ , then the form is properly equivalent to either one of the following two classes of special forms*

$$d_{[a,c]} = ax^2 + cy^2 \tag{10}$$

$$\tilde{d}_{[a,c]} = ax^2 + axy + cy^2. \tag{11}$$

*Such forms are indeed ambiguous: in the diagonal case put  $w = 0$  and in the non-diagonal case put  $w = 1$ , then the involution  $\mathbf{a}' = \begin{pmatrix} 1 & w \\ 0 & -1 \end{pmatrix}$  is an isometry of the corresponding bilinear form. If  $\mathbf{a}$  is the corresponding involution for  $q$ , we have  $\mathrm{O}^+(Q) = \langle \mathbf{a}, \mathbf{u} \rangle$ .*

*Remark 2.8.* In fact, Jones does not prove that  $\mathbf{a}$  preserves the components of the light cone. In the diagonal case this can be seen as follows. One can take  $C$  to be (smallest) sector of the plane bounded by the two lines  $x = \pm\sqrt{-c/ay}$  and  $\mathbf{a}'$  preserves this sector. The non-diagonal case is similar.

Proper equivalence makes use of *adjacency*: we say  $q'$  is right adjacent to  $q$  (or  $q$  left adjacent to  $q'$ ) if  $q' = {}^t P q P$  with  $P = P_e := \begin{pmatrix} 0 & -1 \\ 1 & e \end{pmatrix}$ ,  $e \in \mathbb{Z}$ . It replaces the coefficients  $(a, b, c)$  of  $q$  by  $(c, -b + 2ec, a - eb + ce^2)$ .

**Example 2.9.** Using  $P_0$  the form  $x^2 + bxy + cy^2$  is adjacent to  $cx^2 - bxy + y^2$  which in turn, using  $P_{-e}$  is adjacent to  $x^2 + (b - 2e)xy + (c - be + e^2)y^2$ . So, if  $b = 2e$  is even, our form is equivalent to the diagonal form  $x^2 + (c - e^2)y^2$ . On the other hand, if  $b = 2e + 1$  is odd, the discriminant  $d$  is equivalent to 1 modulo 4 and the form is equivalent to  $x^2 + xy + (c - e - e^2)y^2$ . In both cases, according to Prop. 2.7 there is an involution of determinant  $-1$ . Explicitly,

$$\mathbf{a} = \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}$$

### 2.3 Discriminant groups of ambiguous forms

Up to now we assumed that  $q = ax^2 + bxy + cy^2$  is primitive. For the computation of the groups  $\tilde{O}^\dagger(Q)$  we can no longer assume this. Since  $Q$  is even, we can always write  $Q = 2nq$  with  $n \in \mathbb{Z}$  and  $q$  primitive. The discriminant form  $\text{discr}(Q)$  then is generated by the columns of the matrix

$$\frac{1}{nd} \begin{pmatrix} 2c & -b \\ -b & 2a \end{pmatrix}, \quad d = d(q) = b^2 - 4ac.$$

This enables us to find explicit sufficient conditions for  $\bar{\mathbf{u}}^k = \pm 1$  to hold. Indeed, let  $(U, V)$  be the minimal positive solution of the Pell equation (5) and let  $(u_k, v_k)$  be the solution obtained by writing  $\frac{1}{2}(u_k + \sqrt{d}v_k) = \left[ \frac{1}{2}(U + \sqrt{d}V) \right]^k$ . Then we have:

**Lemma 2.10.** *Suppose that the following conditions hold*

$$(u_k - 2)c \equiv 0 \pmod{nd} \quad (12)$$

$$\frac{1}{2}dv_k + \left(-\frac{1}{2}u_k + 1\right)b \equiv 0 \pmod{nd}, \quad (13)$$

$$-\frac{1}{2}dv_k + \left(-\frac{1}{2}u_k + 1\right)b \equiv 0 \pmod{nd} \quad (14)$$

$$(u_k - 2)a \equiv 0 \pmod{nd} \quad (15)$$

then  $\bar{\mathbf{u}}^k = 1$ . For  $n = \pm 1$  these conditions are always verified with  $k = 2$ .

*Proof:* That (12)–(15) imply  $\bar{\mathbf{u}}^k = 1$  is a direct calculation using Prop. 2.5. That these condition are satisfied for  $n = \pm 1$  uses that  $u_2 = 2 + dV^2$  and  $v_2 = UV$ . Indeed (12) and (14) then are immediate. For (13), note that the left hand side equals  $\frac{1}{2}(U - bV)dV$  and hence is divisible by  $d$ . Equation (15) can be replaced by  $dv_2 \equiv 0 \pmod{d}$  in this case which is trivially true.  $\square$

Let us now pass to ambiguous forms. We first consider the diagonal case  $q = ax^2 + cy^2$  with  $a$  and  $c$  coprime. Then  $d(q) = -4ac$ . The associated forms are  $Q = n \begin{pmatrix} 2a & 0 \\ 0 & 2c \end{pmatrix}$  with

$$\text{discr}(Q) = \left\langle \begin{pmatrix} \frac{1}{2na} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{1}{2nc} \end{pmatrix} \right\rangle.$$

Let  $(S, V)$  be the minimal positive solution of  $x^2 + acy^2 = 1$ , that is  $(2S, V)$  is the minimal positive solution of  $x^2 - dy^2 = 4$  as in Prop.2.5. In this case  $ac < 0$  and we may assume that  $a > 0, c < 0$  and  $a < |c|$ . We allow  $n$  to be negative.

**Lemma 2.11.** *If  $|n| \geq 2$  no isometry of determinant  $-1$  induces  $\pm \text{id}$  on  $\text{discr}(Q)$ .*

*For  $n = \pm 1$  and  $a \neq 1$  the necessary and sufficient condition for such an involution to exist is that  $V$  be even,  $S \equiv \pm 1 \pmod{2a}$  and  $S \equiv \mp 1 \pmod{2c}$  and then always  $\bar{\mathbf{a}}' \bar{\mathbf{u}} = \pm \text{id}$ .*

*For  $n = \pm 1$  and  $a = 1$  one has  $\bar{\mathbf{a}}' = -\text{id}$ .*

*Proof:* We let  $(s_k, v_k)$  be the solution of  $x^2 + acy^2 = 1$ , obtained from  $(S + \sqrt{-ac}V)^k$  (cf. Lemma 2.1). For simplicity we write  $(s, v)$  instead of  $(s_k, v_k)$ . We calculate

$$\mathbf{b} := \mathbf{a}' \mathbf{u}^k = \begin{pmatrix} s & -cv \\ -av & -s \end{pmatrix},$$

$$\mathbf{b} \begin{pmatrix} \frac{1}{2na} \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{s}{2na} \\ \frac{-v}{2n} \end{pmatrix}, \quad \mathbf{b} \begin{pmatrix} 0 \\ \frac{1}{2nc} \end{pmatrix} = \begin{pmatrix} \frac{-v}{2n} \\ \frac{-s}{2nc} \end{pmatrix}.$$

Secondly,  $\bar{\mathbf{b}} = \pm \text{id}$  only if  $n = \pm 1$  and then  $v$  has to be even while  $s \equiv \pm 1 \pmod{2a}$ ,  $s \equiv \mp 1 \pmod{2c}$  is a necessary and sufficient condition. Since in this case by Lemma 2.10  $\bar{\mathbf{u}}^2 = 1$ , we can reduce to the case  $k = 0$  or  $k = 1$ . If  $k = 0$  we see that  $a = 1$  and if  $a \neq 1$  the necessary and sufficient conditions are as stated.  $\square$

*Remark.* If  $n = \pm 1$  and  $S \equiv \pm 1 \pmod{2a}$  and  $S \equiv \mp 1 \pmod{2c}$  hold simultaneously, two cases occur: if  $V$  is even, then  $\bar{\mathbf{a}}' \bar{\mathbf{u}} = \pm \text{id}$  but if  $V$  is odd  $\bar{\mathbf{a}}' \bar{\mathbf{u}}^\ell$  can never be equal  $\pm 1$ .

For  $a = 1$  and  $n = \pm 1$  the situation is different: if  $V$  is even and  $S \equiv \mp 1 \pmod{2c}$  we have  $\bar{\mathbf{u}} = \pm \text{id}$ , and if  $V$  is odd then  $\bar{\mathbf{u}}^2 = \text{id}$ .

**Examples 2.12.** Using Table 1 it is easy to find examples where the conditions hold and where these fail: they hold for  $(a, c) = (1, -5)$ ,  $(1, -13)$ ,  $(1, -17)$ ,  $(1, -3)$ ,  $(1, -7)$ ,  $(1, -11)$ ,  $(3, -11)$ ,  $(3, -13)$ ,  $(4, -5)$  but fail for  $(a, c) = (3, -5)$ ,  $(3, -7)$ ,  $(3, -17)$ ,  $(2, -4)$ . See table 2 for more complete information.

$(a, c)$	smallest $k$ with $\bar{\mathbf{u}}^k = \pm \text{id}$	ditto for $\bar{\mathbf{a}}' \bar{\mathbf{u}}^k = \pm \text{id}$
$(1, -5)$	$\bar{\mathbf{u}} = \text{id}$	$\bar{\mathbf{a}}' = -\text{id}$
$(1, -13)$	$\bar{\mathbf{u}} = \text{id}$	$\bar{\mathbf{a}}' = -\text{id}$
$(1, -17)$	$\bar{\mathbf{u}} = \text{id}$	$\bar{\mathbf{a}}' = -\text{id}$
$(1, -3)$	$\bar{\mathbf{u}}^2 = \text{id}$	$\bar{\mathbf{a}}' = -\text{id}$
$(1, -7)$	$\bar{\mathbf{u}}^2 = \text{id}$	$\bar{\mathbf{a}}' = -\text{id}$
$(1, -11)$	$\bar{\mathbf{u}}^2 = \text{id}$	$\bar{\mathbf{a}}' = -\text{id}$
$(3, -11)$	$\bar{\mathbf{u}} = \text{id}$	$\bar{\mathbf{a}}' \bar{\mathbf{u}} = -\text{id}$
$(3, -13)$	$\bar{\mathbf{u}} = \text{id}$	$\bar{\mathbf{a}}' \bar{\mathbf{u}} = -\text{id}$
$(3, -5)$	$\bar{\mathbf{u}}^2 = \text{id}$	none
$(3, -7)$	$\bar{\mathbf{u}}^2 = \text{id}$	none
$(3, -17)$	$\bar{\mathbf{u}}^2 = \text{id}$	none

Table 2: Minimal numbers  $k$  with  $\bar{\mathbf{u}}^k = \text{id}$  and  $\bar{\mathbf{a}}' \bar{\mathbf{u}}^k = -\text{id}$ .

We now pass to the non-diagonal case  $q = ax^2 + axy + cy^2$ ,  $(a, c) = 1$ . Here  $Q = n \begin{pmatrix} 2a & a \\ a & 2c \end{pmatrix}$ ,  $d(q) = a(a - 4c)$ . Since  $d(q) > 0$  we may suppose  $a > 0$  and  $a > 4c$ . Again, we allow  $n$  to be negative. We have

$$\text{discr}(Q) = \left\langle \begin{pmatrix} \frac{1}{na} \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{n(a-4c)} \\ \frac{-2}{n(a-4c)} \end{pmatrix} \right\rangle$$

and in this case:

**Lemma 2.13.** *If  $|n| \geq 2$  and  $(n, a) \neq (\pm 2, 1)$  no isometry of determinant  $-1$  induces  $\pm \text{id}$  on  $\text{discr}(Q)$ .*

*For  $n = \pm 1, a \neq 1, 2$  the necessary and sufficient condition for such an involution to exist is that  $U \equiv \pm 2 \pmod{a}$  and  $U \equiv \mp 2 \pmod{a-4c}$ . If this is the case  $\bar{\mathbf{a}}'\bar{\mathbf{u}} = \pm \text{id}$ .*

*For  $(n, a) = (\pm 1, 1), (\pm 1, 2)$  or  $(\pm 2, 1)$  we always have  $\bar{\mathbf{a}}' = -\text{id}$ .*

*Proof:* For simplicity we write  $(u, v)$  instead of  $(u_k, v_k)$ . We find

$$\mathbf{b} := \mathbf{a}'\mathbf{u}^k = \begin{pmatrix} \frac{1}{2}(u+av) & \frac{1}{2}(u+av) - cv \\ -av & -\frac{1}{2}(u+av) \end{pmatrix}$$

so that

$$\mathbf{b} \begin{pmatrix} \frac{1}{na} \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{\frac{1}{2}(u+av)}{\frac{na}{n}} \\ \frac{-\frac{1}{2}(u+av) - cv}{n} \end{pmatrix} = \pm \begin{pmatrix} \frac{1}{na} \\ 0 \end{pmatrix},$$

$$\mathbf{b} \begin{pmatrix} \frac{1}{n(a-4c)} \\ \frac{-2}{n(a-4c)} \end{pmatrix} = \begin{pmatrix} \frac{-\frac{1}{2}(u+av) + 2cv}{\frac{n(a-4c)}{n}} \\ \frac{u}{n(a-4c)} \end{pmatrix} = \pm \begin{pmatrix} \frac{1}{n(a-4c)} \\ \frac{-2}{n(a-4c)} \end{pmatrix}.$$

Now the proof proceeds as in the diagonal case.  $\square$

**Examples 2.14.** Using Table 1 one finds the examples gathered in Table 3.

$(a, c)$	smallest $k$ with $\bar{\mathbf{u}}^k = \pm \text{id}$	ditto for $\bar{\mathbf{a}}'\bar{\mathbf{u}}^k = \pm \text{id}$
$(1, -1)$	$\bar{\mathbf{u}}^2 = \text{id}$	$\bar{\mathbf{a}}' = -\text{id}$
$(1, -3)$	$\bar{\mathbf{u}}^2 = \text{id}$	$\bar{\mathbf{a}}' = -\text{id}$
$(1, -4)$	$\bar{\mathbf{u}}^2 = \text{id}$	$\bar{\mathbf{a}}' = -\text{id}$
$(3, -1)$	$\bar{\mathbf{u}} = \text{id}$	none
$(3, -2)$	$\bar{\mathbf{u}}^2 = \text{id}$	none
$(7, 1)$	$\bar{\mathbf{u}}^2 = \text{id}$	none
$(21, 4)$	$\bar{\mathbf{u}}^2 = \text{id}$	$\bar{\mathbf{a}}'\bar{\mathbf{u}} = -\text{id}$
$(15, 1)$	$\bar{\mathbf{u}}^2 = \text{id}$	none
$(35, 8)$	$\bar{\mathbf{u}}^2 = \text{id}$	$\bar{\mathbf{a}}'\bar{\mathbf{u}} = -\text{id}$

Table 3: Minimal numbers  $k$  with  $\bar{\mathbf{u}}^k = \text{id}$  and  $\bar{\mathbf{a}}'\bar{\mathbf{u}}^k = -\text{id}$ .

## 2.4 Roots

There is a general theory of representations of integers by  $q$ . See [Dickson, § 46]. We only need the theory of representations of  $-1$ . These correspond to representations of  $-2$  by  $2Q$ , i.e. to the roots of the corresponding even lattice. This general prescription yields:

**Lemma 2.15.** *Suppose that  $(x, y)$  is a solution for  $q(x, y) = -1$  with relative prime integers  $x$  and  $y$ . Then either*

(\*)  $d \equiv 0 \pmod{4}$  and  $q \sim d_{[-1, \frac{1}{4}d]}$  hence, if  $(u, v)$  is a positive solution for (5), then  $(\frac{1}{2}u, v)$  gives a positive representation of  $-1$  for  $d_{[-1, \frac{1}{4}d]}$  and conversely.

or

(\*\*)  $d \equiv 1 \pmod{4}$  and  $q \sim \tilde{d}_{[-1, \frac{1}{4}(d-1)]}$  and  $(\frac{1}{2}(u-v), v)$  gives a positive representation for  $-1$  for  $\tilde{d}_{[-1, \frac{1}{4}(d-1)]}$  and conversely.

*Remark 2.16.* By Prop. 2.7 this Lemma implies that the quadratic forms  $q$  for which  $2Q$  has roots are automatically ambiguous.

We study these two forms in more detail.

**Lemma 2.17.** *Let  $(U, V)$  the minimal positive solution for (5). The solutions of the equation  $d_{[-1, \frac{1}{4}d]}(x, y) = -1$  are either positive or negative linear combinations of the two basic solutions  $\mathbf{e} = (-1, 0)$  and  $\mathbf{f} = (\frac{1}{2}U, V)$ . The solutions of the equation  $\tilde{d}_{[-1, \frac{1}{4}(d-1)]} = -1$  are either positive or negative linear combinations of the two basic solutions  $\mathbf{e} = (-1, 0)$  and  $\mathbf{f} = (\frac{1}{2}(U - V), V)$ . In both cases the involution  $-\mathbf{a}'\mathbf{u}$  generates the group  $O^\dagger(2Q)$*

*The group  $\tilde{O}^\dagger(2Q)$  is trivial unless (6) is solvable and then the involution  $(-\text{id}, -\mathbf{a}'\mathbf{u})$  generates  $\tilde{O}^\dagger(2Q)$ .*

*Proof:* The first assertion follows from Lemma 2.2 since in both cases  $1 \in \mathcal{O}(\sqrt{d})$  corresponds to  $(1, 0)$ , while  $\eta \in \mathcal{O}(\sqrt{d})$  corresponds to  $(\frac{1}{2}U, V)$  in the first case and to  $(\frac{1}{2}(U - V), V)$  in the second case.

We only treat the diagonal case  $q = d_{[-1, \frac{1}{4}d]}$ ; in the non-diagonal case the computations are similar. Recall the notion of positive root from § 1. Here we can take the two basic roots as positive roots with respect to  $2Q$ . Since  $O(2Q)$  consists of elements of the form  $\pm \mathbf{u}^k$  or  $\pm \mathbf{a}'\mathbf{u}^k$  it suffices to determine which of these elements preserve the set of basic roots. By direct computation one finds that  $\mathbf{a}'\mathbf{u}(\mathbf{e}) = -\mathbf{f}$  and  $\mathbf{a}'\mathbf{u}(\mathbf{f}) = -\mathbf{e}$  and hence  $-\mathbf{a}'\mathbf{u}$  preserves the cone  $D$  defined in (2). By a similar computation one sees that all the other elements of  $O(2Q)$  do not preserve the set of basic roots. The first statement follows. The second assertion follows from Lemma 2.1. Indeed, since the negative Pell equation has a minimal solution of the form  $(2s, t)$ , the minimal solution for the positive Pell equation is of the form  $(U, V) = (4s^2 + 2, 2st)$  and since  $V$  is even and  $U \equiv -2 \pmod{d}$  one calculates directly, as in the proof of Lemma 2.11 that  $\mathbf{a}'\mathbf{u} = \text{id}$ . Conversely, suppose that  $\mathbf{a}'\mathbf{u}$  induces  $\pm \text{id}$ . Again, as in the proof of Lemma 2.11, we must have that  $V$  is even and  $U \equiv \mp 2 \pmod{d}$ . In this case write  $\frac{1}{2}U = \mp 1 + \frac{1}{2}kd, V = 2m$ . Then  $m^2 = k(\frac{1}{4}dk \mp 1)$  shows that  $k = t^2$  and  $\frac{1}{4}dk \mp 1 = s^2$  are squares of integers  $(s, t)$  for which then  $s^2 - \frac{1}{4}dt^2 = \mp 1$  (remember that  $d$  is divisible by 4 in this situation so that  $k$  and  $\frac{1}{4}dk \mp 1$  are coprime). Note that the plus sign is excluded since  $(U, V)$  was supposed to be a minimal solution. So  $\mathbf{a}'\mathbf{u}$  induces  $\text{id}$  and  $(s, t)$  solves the negative Pell equation.  $\square$

The drawback of Lemma 2.15 is that it is hard to apply in general. But Lemma 2.17 suggest a further link with the solvability of (6). Indeed, if  $q$  has leading coefficient 1 one verifies immediately:

**Lemma 2.18.** *Let  $q = x^2 + bxy + cy^2$  with discriminant  $d = b^2 - 4c$ . Then (6) is solvable if and only if  $q$  represents  $-1$ . Indeed, a solution  $(u, v)$  of (6) yields a solution*

$$\mathbf{v} = \begin{pmatrix} \frac{1}{2}[u - bv] \\ v \end{pmatrix}$$

of  $q(\mathbf{v}) = -1$  and conversely.

As in the proof of Lemma 2.17 to test solvability of (6) it can be useful to investigate the minimal solution of the positive Pell equation. This is illustrated by the following example.

**Example 2.19.** Consider the form  $q_\delta := x^2 + \delta xy + y^2$  with discriminant  $d = (\delta^2 - 4)$ . Then  $(U, V) = (\delta, 1)$  gives the smallest positive solution of (5) and if a solution for the negative Pell equation would exist we would have  $U'^2 + (\delta^2 - 4)V'^2 = 2\delta$  and  $U' \cdot V' = 1$  which forces  $\delta = 3$ . Hence, unless  $\delta = 3$ , the form  $q_\delta$  does not represent  $-1$ . We conclude that the associated even form with matrix

$$Q'_\delta := \begin{pmatrix} 2 & \delta \\ \delta & 2 \end{pmatrix}$$

does not represent  $-2$  unless  $\delta = 3$ . So  $O^+(Q) = O^\dagger(Q)$  in this case and the group is generated by  $\mathbf{u}$  and  $\mathbf{a}'$ .

## 2.5 The discriminant $d$ is a square

An integral form  $q = ax^2 + bxy + cy^2$  represents 0 if and only if  $d(q)$  is a square:  $d(q) = \delta^2$  with  $\delta \in \mathbb{Z}$ . Indeed, this follows immediately from Lemma 2.4. We suppose that  $q$  is primitive. We have to consider all even multiples of  $q$ . We prove here:

**Proposition 2.20.** 1) *If  $d$  is a square and  $q$  is not ambiguous, then  $O^\dagger(2nq) = \tilde{O}^\dagger(2nq) = \text{id}$ .*

2) *If  $q$  is ambiguous and equivalent to the diagonal form there are three cases: 2a)  $q = (x^2 - y^2)$ , 2b)  $q = (x^2 - a^2y^2)$   $a \geq 2$ , 2c)  $q = (a^2x^2 - y^2)$ ,  $a \geq 2$ . In all cases  $O^\dagger(2nq)$  is cyclic of order 2 while  $\tilde{O}^\dagger(2nq) = \text{id}$  except in the case when  $n = 1$  and  $a = 1$ . Then  $O^\dagger(2q) = \text{id}$ , but  $\tilde{O}^\dagger(q) = \mu_2$ .*

3) *In the non-diagonal case we must have  $q(x, y) = \pm(ux + vy)(ux + (u - v)y)$  with  $u \geq 1$  and  $u$  and  $v$  coprime. So  $q = \tilde{a}_{u^2, v(u-v)}$ . We have the following cases: 3a)  $2q$  is unimodular:  $u = 1, v = 0$  or  $u = v = 1$  and then  $2q$  is equivalent to the hyperbolic plane, 3b)  $u = 1$  but  $v \neq 0, 1$ , 3c)  $u \neq 1$ . In case 3a)  $O^\dagger(2nq)$  is cyclic of order two generated by the involution  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ , but only for  $n = 1$  or  $n = 2$  this involution induces*

*id on  $\text{discr}(nq)$ . In case 3b) the group  $O^\dagger(2nq) = \tilde{O}^\dagger(2nq)$  is cyclic of order 2 for  $n = 1$  or  $n = 2$ . In the remaining cases  $O^\dagger(2nq)$  is cyclic of order 2 but  $\tilde{O}^\dagger(2nq) = \text{id}$ .*

*Proof:* Prop. 2.5 implies the results in case  $q$  is not ambiguous, since then  $O(q) = SO(q) = \pm \text{id}$ . Next consider the case of an ambiguous form  $q$ . By Prop. 2.7  $q$  must be equivalent to  $d_{[a,c]}$  or to  $\tilde{d}_{[a,c]}$ .

Diagonal case. Since  $d$  is a square we have the three cases as stated.

The group of isometries equals  $\{\pm \text{id}, \pm \mathbf{a} = \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\}$ . The isotropic vectors are the multiples of  $\mathbf{f}_\pm = (1, \pm 1)$  (in case a),  $\mathbf{f}_\pm = (a, \pm 1)$  (in case b),  $\mathbf{f}_\pm = (\pm 1, a)$  (in case c) and  $\mathbf{a}$  interchanges  $\mathbf{f}_+$  and  $\mathbf{f}_-$ . The cone  $C$  is bounded by the half lines  $\mathbb{R}_+ \cdot \mathbf{f}_+$  and  $\mathbb{R}_+ \cdot \mathbf{f}_-$  and  $\mathbf{a}$  preserves  $C$ . Hence  $O^+(q) = O^\dagger(q) = \{\text{id}, \mathbf{a}\}$  unless  $2q$  has roots. The latter is only the case if  $q = 2x^2 - 2y^2$ , and then the roots are  $\mathbf{d} = \pm(0, 1)$ . In this case the line  $H_{\mathbf{d}}$  orthogonal to  $\mathbf{d}$  divides  $C$  in two half cones  $C^\dagger$  and  $\mathbf{a}C^\dagger$  hence  $O^+(q) = O^\dagger(q) = \text{id}$ . In this case  $\text{discr}(2q) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  and hence  $\tilde{O}^\dagger(2q) = \mu_2$  in this case. If  $d \neq 4$  we have that  $\text{discr}(2nq) \neq 1$  is not a 2-group and hence  $\tilde{O}^\dagger(2nq) = \text{id}$  (compare with Remark 1.1).  
Non-diagonal case. In the second case there exists  $u, v \in \mathbb{Z}$  for which  $a = \pm u^2$ ,  $c = \pm v(u - v)$ . The form is equivalent to  $(ux + vy)(ux + (u - v)y)$ . The two independent isotropic vectors  $(v, -u)$  and  $(v - u, u)$  span  $C$  and are interchanged by  $\mathbf{a}$ . Hence  $O^+(q) = \{\text{id}, \mathbf{a}\}$ .

As before,  $2q$  only has roots if  $q \sim x^2 + xy$ , or, equivalently  $2q \sim H$ . This is case a). For the hyperbolic plane the roots are  $\pm \mathbf{d}$  with  $\mathbf{d} = (1, -1)$  and the line  $H_{\mathbf{d}}$  divides  $C$  in  $C^\dagger$  and  $\mathbf{a}C^\dagger$  so that  $O^+(Q) = \{\text{id}\}$  in this case. However  $\tilde{O}^\dagger(H) = \mu_2$  also  $\tilde{O}^\dagger(2H) = \mu_2$  while  $\tilde{O}^\dagger(nH) = \text{id}$  for  $n \geq 3$ .

In case b) we have  $2nq = \pm n \begin{pmatrix} 2 & 1 \\ 1 & -2v(v-1) \end{pmatrix}$  and  $\text{discr}(2nq)$  is generated by  $\frac{1}{n(2v-1)^2} \begin{pmatrix} -1 \\ 2 \end{pmatrix}$  and  $\frac{1}{n} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ . One sees that  $\bar{\mathbf{a}} = -\text{id}$  if  $n = 1$  or  $n = 2$  so that then  $\tilde{O}^\dagger(2nq)$  is generated by the involution  $(-\text{id}, \mathbf{a})$ . If  $n \geq 3$  we have  $\tilde{O}^\dagger(2nq) = \text{id}$ .

In case c) we easily find that  $\bar{\mathbf{a}} \neq \pm \text{id}$  so that  $\tilde{O}^\dagger(2nq) = \text{id}$ .  $\square$

## 2.6 The discriminant $d$ is not a square

**Proposition 2.21.** *If  $Q$  has no roots and  $q$  is not ambiguous  $\tilde{O}^\dagger(Q)$  is infinite cyclic. If  $Q$  has no roots and  $q$  is ambiguous  $\tilde{O}^\dagger(Q)$  is either infinite cyclic or the infinite dihedral group  $\mathbb{D}_\infty$ . If  $Q$  admits roots,  $\tilde{O}^\dagger(Q)$  is cyclic of order two if the negative Pell equation (6) for  $d = d(q)$  is solvable and trivial otherwise.*

*Proof:* Let us first consider the case when  $q$  is not ambiguous, i.e.  $SO(Q) = O(Q)$ . By Prop. 2.5 this group is a product of  $\pm \text{id}$  and the cyclic group generated by  $\mathbf{u}$ . In this case there are no roots, since roots are only possible for ambiguous forms (see Remark 2.16). Hence by Remark 2.6 we have that  $O^+(Q) = O^\dagger(Q)$  is the cyclic group with  $\mathbf{u}$  as generator. It follows that some power of  $\mathbf{u}$  acts as  $\pm \text{id}$  on the discriminant group and hence in this case  $\tilde{O}^\dagger(Q)$  is an infinite cyclic group with this generator.

Next, suppose that  $q$  is ambiguous. Then  $O(Q)$  is generated by  $-\text{id}$ ,  $\mathbf{u}$  and the involution  $\mathbf{a}$  corresponding to  $\mathbf{a}'$  (see Prop 2.7). One has  $\mathbf{a}\mathbf{u}\mathbf{a} = \mathbf{u}^{-1}$  as a generating relation. Hence the group  $O(Q)$  consists of the elements  $\pm\mathbf{u}^k$ , and  $\pm\mathbf{a}\mathbf{u}^\ell$ , where  $k, \ell \in \mathbb{Z}$ .

First assume that there are no roots. Then  $O^\dagger(Q) = O^+(Q)$  and using Remark 2.6 and 2.8 we see that  $O^+(Q)$  is generated by  $\mathbf{u}$  and  $\mathbf{a}$ . There is a second involution  $\mathbf{a}\mathbf{u}$  and the automorphism group  $O^+(Q) = O^\dagger(Q)$  is the group  $\mathbb{D}_\infty$  with generators  $\{\mathbf{a}, \mathbf{a}\mathbf{u}\}$ . One next has to study the effect of  $\mathbf{u}$  and  $\mathbf{a}$  on the group  $\text{discr}(Q)$ . Since this group is finite, there will be a smallest positive integer  $k$  for which  $\mathbf{u}^k$  induces  $\pm\text{id}$  on  $\text{discr}(Q)$ . Now either there is a smallest positive integer  $\ell$  for which  $\mathbf{a}\mathbf{u}^\ell$  induces  $\pm\text{id}$  or such an integer does not exist. In the former case  $\mathbf{a}\mathbf{u}^\ell$  and  $\mathbf{a}\mathbf{u}^{k+\ell}$  generate the subgroup of isometries inducing  $\pm\text{id}$  on  $\text{discr}(S)$ . So  $\tilde{O}^\dagger(Q)$  is the free product generated by two distinct non commuting involutions. In the latter case the group  $\tilde{O}^\dagger(Q)$  is cyclic generated by  $\mathbf{u}^k$ .

Finally the case that  $q$  has roots. Then Lemma 2.17 gives the answer.  $\square$

### 3 Automorphism groups of K3-surfaces

For the results in this section we refer to [BHPV] and [P-SS]. From now on the intersection product between two classes  $c, d$  in the lattice  $L$  will be written  $c \cdot d$  instead of  $Q(c, d)$  and we write  $c^2$  instead of  $c \cdot c$ .

Let  $X$  be an algebraic K3-surface, i.e. a simply connected projective surface with trivial canonical bundle. Up to multiplicative constants there is a unique holomorphic 2-form  $\omega_X$  on  $X$  and it is nowhere zero. The second cohomology integral group equipped with the unimodular intersection form is known to be isometric to the unique even unimodular lattice  $(L, Q)$  of signature  $(3, 19)$ . Any choice of such an isometry (a *marking*) identifies the line  $\mathbb{C} \cdot \omega_X \subset H^2(X; \mathbb{C})$  with a line  $\mathbb{C} \cdot \omega \subset L \otimes \mathbb{C}$ , the *period* of  $X$ . An automorphism  $g$  of  $X$  induces an automorphisms of  $L$  which preserve the complex line  $\mathbb{C}\omega$ . So  $g$  preserves the lattice  $S = \omega^\perp \cap L$  which corresponds to the Picard lattice  $S_X$  as well as its orthogonal complement  $T = S^\perp \subset L$ , which corresponds to the *transcendental lattice*.

First consider the action on  $S$ . It has signature  $(1, r)$ . Hence, the description of § 1 applies to  $O(S)$ . The canonical choice for the subcone  $C^\dagger$  is the ample cone which corresponds to the effective roots:

$$C^\dagger = \{x \in C^+ \mid x \cdot d > 0, \text{ for all effective roots } d\}.$$

The automorphisms of  $X$  preserve this subcone so that  $\text{Aut}(X)$  acts on  $S$  as a subgroup of  $O^\dagger(S)$ . From the Torelli theorem one can deduce the complete description of the automorphism group as follows.

**Theorem 3.1.** *Let  $X$  be a K3-surface. Choose an isometry  $H^2(X) \xrightarrow{\sim} L$ . The group  $\text{Aut}(X)$  corresponds to the subgroup  $G \subset O(L)$  consisting of those  $g \in O(L)$  which preserve the period of  $X$  and for which  $g|_S \in O^\dagger(S)$ .*

To determine the full group  $G$  it suffices to know its restriction to  $S$  and  $T$ . Since  $L$  is unimodular, the groups  $\text{discr}(S)$  and  $\text{discr}(T)$  are naturally isomorphic. An automorphism of  $L$  induces the same automorphism on both groups. Conversely, a pair  $(g_1, g_2) \in \text{O}(S) \times \text{O}(T)$  can be lifted to an automorphism of  $L$  if  $g_1$  and  $g_2$  induce the same automorphism on  $\text{discr}(S) \simeq \text{discr}(T)$ . In particular, if  $g_2 = \pm \text{id}$ , this states that any  $g_1 \in \text{O}(S)$  which induces  $\pm \text{id}$  on  $\text{discr}(S)$  lifts to a unique isometry of  $L$  restricting to  $\pm \text{id}$  on  $T$ .

The first condition for  $g \in \text{O}(L)$  to belong to  $G$  reads  $g(\omega) = \lambda\omega$  for some root of unity  $\lambda$ . In particular, the automorphisms of  $X$  acts as a finite group on  $T$ . If  $\lambda \neq \pm 1$  the period point  $\omega$  is an eigenvector of a non-trivial isometry of  $L$ . This imposes algebraic conditions on  $\omega$  and hence for very general  $\omega$  such automorphisms cannot exist. This leads to:

**Definition 3.2.** An algebraic K3-surface  $X$  is *general with respect to automorphisms*, or *Aut-general* if its automorphisms preserve its period up to sign.

It is equivalent to the statement that the automorphisms act as  $\pm \text{id}$  on the lattice  $T$ . Hence:

**Proposition 3.3.** *Let  $X$  be an Aut-general algebraic K3-surface. Choose a marking to identify  $H^2(X)$  with the lattice  $L$  and let  $S$  be the sublattice of  $L$  which corresponds to the Picard lattice of  $X$ . The automorphism group of  $X$  can be identified with the group  $\tilde{\text{O}}^\dagger(S)$  (see (4)).*

As a consequence of the previous discussion and the results in § 2 we have:

**Corollary 3.4.** *For  $X$  a K3-surface with Picard number 2 the group  $\text{Aut}(X)$  is finite precisely when the Picard lattice  $S_X$  contains divisors  $L$  with  $L^2 = 0$  or with  $L^2 = -2$ . If moreover,  $X$  is Aut-general we have in this situation that  $\text{Aut}(X) = \text{id}$  or  $\text{Aut}(X)$  is cyclic of order 2. See Prop. 2.5 and Lemma 2.17 for more details.*

*If  $S_X$  does not contain such divisors and if moreover  $S_X$  is not ambiguous, then  $\text{Aut}(X)$  is infinite cyclic, but if  $S_X$  is ambiguous, then  $\text{Aut}(X)$  is either infinite cyclic or the infinite dihedral group  $\mathbb{D}_\infty$ .*

*Remark.* This reproves the finiteness criterion from [P-SS, § 6].

To extend the result to K3-surfaces which are not Aut-general we consider the action of  $\text{Aut}(X)$  on  $T$ . The group  $G$  acts on  $\mathbb{C}\cdot\omega$  through a finite cyclic group  $G'$  of order say  $d$  as a character. On the other hand, the rational vector space  $T \otimes \mathbb{Q}$  is a  $G'$ -representation space which splits into a number of copies of the unique  $\varphi(d)$ -dimensional irreducible  $\mathbb{Q}$ -representation space. Here  $\varphi(d)$  is the Euler function. This imposes restrictions on  $G'$ .

**Example 3.5.** Let  $\text{rank}(S) = 2$ . Then  $\text{rank}(T) = 20$  and hence  $\varphi(d)$  divides 20 and as in [Nik3, Thm. 10.1.2] we find:

*If there is a non-trivial kernel  $\text{O}^\dagger(L) \rightarrow \text{O}^\dagger(S)$ , the discriminant group  $\text{discr}(S)$  belongs to the following list:  $\mathbb{Z}/2\mathbb{Z}$ ,  $(\mathbb{Z}/2\mathbb{Z})^2$ ,  $(\mathbb{Z}/2\mathbb{Z})^3$ ,  $\mathbb{Z}/3\mathbb{Z}$ ,  $\mathbb{Z}/5\mathbb{Z}$ ,  $(\mathbb{Z}/5\mathbb{Z})^2$  or  $\mathbb{Z}/11\mathbb{Z}$ .*

In particular, if the discriminant of  $S$  is different from 2, 4, 8, 3, 5, 25 or 11 the automorphism group of any K3-surface whose Picard lattice is  $S$  is the group  $\tilde{O}^\dagger(S)$  we just introduced and in these cases the K3-surface is automatically Aut-general.

## 4 Examples

By [Mor, Thm. 1.14.4] every even lattice of signature  $(1, r)$  with  $r \leq 9$  occurs as the Picard lattice  $S$  of some algebraic K3-surface and the primitive embedding  $S \hookrightarrow L$  is unique. In particular, all indefinite even lattices of rank 2 may occur. In general however it is not so easy to describe the surfaces geometrically.

We now give some examples illustrating the theory of § 2 some of which can be found in the existing literature.

1. Consider the hyperbolic lattice  $H$ . It represents 0 as well as  $-2$ . We have seen (Prop. 2.20) that  $O(H)$  is the identity and  $\tilde{O}^\dagger(H) = \mu_2$  which means that the automorphism group of a general K3-surface with  $H$  as Picard lattice is generated by an involution acting trivially on the Picard lattice but as  $-\text{id}$  on the transcendental lattice. The surface has a unique elliptic fibration over  $\mathbb{P}^1$  with a  $(-2)$ -section. See [Ge, § 5.4]
2. More generally, consider  $\Lambda_{b,c} = \begin{pmatrix} 0 & b \\ b & 2c \end{pmatrix}$ . This matrix represents zero and  $O^\dagger(\Lambda_{b,c})$  is either trivial or cyclic of order two. The group  $\tilde{O}^\dagger(\Lambda_{b,c})$  is trivial unless  $(b, c) = (1, 0), (2, 0)$  or  $(b, 1), b \geq 2$ . This follows immediately from Prop. 2.20. The corresponding K3-surfaces have been studied in [Ge] where interesting projective models are exhibited. For instance  $\Lambda_{2,0}$  is realized by a double cover of  $\mathbb{P}^1 \times \mathbb{P}^1$  branched in a curve of bidegree  $(4, 4)$ . The rulings give two elliptic pencils and the covering involution is the unique non-trivial automorphism.
3. Consider  $\begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix}$ . This matrix is equivalent to the diagonal form  $d_{2,-6} = \langle 2 \rangle \oplus \langle -6 \rangle$ . For this form  $\mathbf{u} = \begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix}$  and  $\mathbf{a} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ . These preserve  $C$ . The action on the discriminant group is as follows:  $\mathbf{u}^2$  acts as the identity while  $\mathbf{a}$  acts as  $-\text{id}$ . So  $\tilde{O}^\dagger(d_{2,-6})$  is generated by the two commuting involutions  $\mathbf{a}\mathbf{u}^2$  and  $\mathbf{a}$  which both act as  $-\text{id}$  on the transcendental lattice. In fact this example has been treated geometrically. See [W] where it is shown that the corresponding K3-surface  $X$  is a complete intersection inside  $\mathbb{P}^2 \times \mathbb{P}^2$  of bidegree  $(1, 1)$  and  $(2, 2)$ . The two projections onto the factors  $\mathbb{P}^2$  realize  $X$  as a double cover and the two involutions induce  $\mathbf{a}\mathbf{u}^2$  and  $\mathbf{a}$  on the Picard lattice.
4. More generally  $Q'_\delta := \begin{pmatrix} 2 & \delta \\ \delta & 2 \end{pmatrix}$ , an example from [G-L]. In Example 2.19 we have seen that unless  $\delta = 3$  this form represents

neither 0 nor  $-2$ . If  $\delta \neq 3$  one has

$$\mathbf{u} = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}, \quad \mathbf{a} = \begin{pmatrix} 1 & \delta \\ 0 & -1 \end{pmatrix}$$

The group  $\text{discr}(Q'_\delta)$  is generated by  $\mathbf{e} = \frac{1}{d} \begin{pmatrix} -2 \\ \delta \end{pmatrix} \in \mathbb{Z}/d\mathbb{Z}$ , or, equivalently, by  $\mathbf{f} = \frac{1}{d} \begin{pmatrix} -\delta \\ 2 \end{pmatrix} \bmod \mathbb{Z}/d\mathbb{Z}$ . One verifies that  $\mathbf{ue} = -\mathbf{f}$ , so that  $\mathbf{u} \neq \pm 1$ , but  $\mathbf{u}^2 = 1$ . On the other hand  $\mathbf{a}$  acts as  $-1 \in (\mathbb{Z}/d\mathbb{Z})^\times$ . It follows that the automorphism group of the K3-surface is isomorphic to the group generated by  $\mathbf{u}^2$  and  $\mathbf{a}$ . The first preserves the period while the second sends it to its opposite.

5. Consider  $Q_\delta := \begin{pmatrix} 2 & \delta \\ \delta & -2 \end{pmatrix}$ . In this case  $(\delta, 1)$  is the smallest positive solution for the negative Pell equation and corresponds to the matrix

$$\mathbf{u}_- = \begin{pmatrix} 0 & 1 \\ 1 & \delta \end{pmatrix}$$

and

$$\mathbf{u} = \mathbf{u}_-^2, \quad \mathbf{a} = \begin{pmatrix} 1 & \delta \\ 0 & -1 \end{pmatrix}$$

This matrix represents  $-2$ : take  $x = 0, y = 1$ . It follows that the automorphism group of the K3-surface is finite. In fact, by Lemma 2.17 it is generated by  $-\mathbf{au}$  and hence cyclic of order 2. This example has been treated in [G-L].

6. The **diagonal form**  $Q = 2nq$  with  $q = ax^2 + by^2$ ,  $(a, b) = 1$ . These represent all the **ambiguous forms with**  $d(q) \equiv 0 \pmod{4}$ . Bini considers the case  $(a, b) = (d, -1)$ . We find back his main result [Bi, Theorem 1]. Indeed the form represents zero if  $d$  is a square and then by Prop. 2.20  $\tilde{\mathcal{O}}^\dagger(Q)$  is trivial unless  $n = d = 1$  in which case it is cyclic of order two. If  $d$  is not a square and  $n = 1$  there are roots and the group  $\tilde{\mathcal{O}}^\dagger(Q)$  is cyclic of order two by Lemma 2.17. If however  $n \geq 2$  the group  $\tilde{\mathcal{O}}^\dagger(Q)$  is always infinite cyclic by Prop 2.21. There are several projective models described in loc. cit. For example the complete intersection of bidegree  $(2, 1)$  and  $(1, 2)$  in  $\mathbb{P}^1 \times \mathbb{P}^3$  has  $n = 2$  and  $a = 1$ . For other values of the numbers  $(a, b)$  the reader should look at Table 2.
7. The forms  $Q = 2nq$ , with  $q$  **ambiguous and**  $d(q) \equiv 1 \pmod{4}$ . Such a form is equivalent to  $\tilde{q}_{[a,c]} = ax^2 + axy + cy^2$ ,  $(a, c) = 1$ : for some values of  $(a, c)$  Table 3 give some results.
8. Forms  $Q = 2nq$  with  $q = x^2 + bxy + cy^2$  a **monic form**. By Example 2.9 such  $q$  is either equivalent to a diagonal form  $q_{[1,c']} = x^2 + c'y^2$ , and such forms are covered by Bini's results [Bi], or  $q$  is equivalent to  $\tilde{q}_{[1,c']} = x^2 + xy + c'y^2$ . By Lemma 2.18 the latter form represents  $-1$  if and only (6) has a solution. This

gives roots if and only if  $n = 2$  and by Lemma 2.17  $\tilde{O}^\dagger(Q)$  is then cyclic of order 2. If (6) has no solution Lemma 2.13 gives a recipe for determining  $\tilde{O}^\dagger(Q)$ .

## References

- [BHPV] Barth, W., Hulek, K., Peters. C. and A. Van de Ven: *Compact complex surfaces*, second enlarged edition, Springer Verlag 2004.
- [Bi] Bini, G.: On automorphisms of some K3 surfaces with Picard Number Two, *MCEFA Annals* (2005).
- [Dickson] Dickson, L. E.: *Introduction to the theory of numbers*, Dover Publ. Inc. New York 1954
- [G-L] Federica Galluzzi, F. and G. Lombardo: On automorphisms groups of some K3 surfaces, preprint [arXiv:mathAG0610972](https://arxiv.org/abs/math/0610972)
- [G-S1] Garbagnati, A. and A. Sarti: Symplectic automorphisms of prime order on K3 surfaces, *J. of Algebra* **318** (2007) 323–350
- [G-S2] Garbagnati, A. and A. Sarti: Elliptic fibrations and symplectic automorphisms on K3 surfaces, preprint [arXiv:matAG0801.3992](https://arxiv.org/abs/math/0801.3992)
- [Ge] Geemen, B. van: Some remarks on Brauer groups of K3 surfaces, *Adv. in Math.* **197** (2005) 222–247
- [Jones] Jones, B. W.: *The arithmetic of quadratic forms*, The Carus Mathematical Monographs **10**, MAA, John Wiley Sons, 1950.
- [Kon1] Kondō, S.: The maximum order of finite groups of automorphisms of K3 surfaces, *Am. Math. J.* **121** (1999), 1245–1252
- [Kon2] Kondō, S.: Niemeier lattices, Mathieu groups, and finite groups of symplectic automorphisms of K3 surfaces. With an appendix by Shigeru Mukai, *Duke Math. J.* **92** (1998) 593–603
- [Mor] Morrison, D. R.: On K 3 surfaces with large Picard number, *Invent. Math.* **75** (1984) 105–121
- [Muk] Mukai, S.: Finite groups of automorphism of K3 surfaces and the Mathieu group, *Inv. Math.* **94** (1988) 183–221
- [Nik1] Nikulin, V.: Integral symmetric bilinear forms and some of their applications, *Math. USSR Izv.* **14** (1980) 103–167
- [Nik2] Nikulin, V.: Finite groups of automorphisms of Kählerian K3 surfaces. (Russian) *Trudy Moskov. Mat. Obshch.* **38** (1979), 75–137
- [Nik3] Nikulin, V.: Factor groups of automorphisms of hyperbolic forms with respect to subgroups generated by 2-reflections. *Algebriogeometric applications*, *J. Soviet Math.* **22**, 1401–1476, (1981)

- [P-SS] Pjatečkii-Shapiro, I. and I. Shafarevič: A Torelli theorem for algebraic surfaces of type K-3, *Izv. Akad. Nauk. SSSR. Ser. Math.* **35** (1971) 503–572.
- [Sev] Severi, F. :Complementi alla teoria della base per la totalità delle curve di una superficie algebrica, *Rend. Circ. Mat. Palermo* **30** (1910), 265–288
- [W] Wehler, J.: *K3-surfaces with Picard number 2.* *Arch. Math.* **50** (1988), 73–82
- [Pell] Quadratic diophantine equations and fundamental unit BC-MATH programs,  
<http://www.numbertheory.org/php/PELL.html>
- [Se] Serre, J.-P.: *A course in arithmetic*, Springer Verlag, Berlin etc. (1973)