Binary forms with the same value set II. The case of D4

Binary forms with the same value set II. The case of D_4

Étienne Fouvry[*1] and Peter Koymans[†2]

[1]Université Paris–Saclay
[2]ETH Zurich

April 23, 2024

Abstract

Let $F, G \in \mathbb{Z}[X, Y]$ be binary forms of degree ≥ 3, non-zero discriminant and with automorphism group isomorphic to D_4. If $F(\mathbb{Z}^2) = G(\mathbb{Z}^2)$, we show that F and G are $\mathrm{GL}(2, \mathbb{Z})$–equivalent.

1 Introduction

This paper is the continuation of [1] and deals with the following question:

Question 1.1. *Let $d \geq 3$ and let $F(X, Y)$ and $G(X, Y)$ two binary forms of $\mathrm{Bin}(d, \mathbb{Q})$ (the set of binary forms with degree d, with rational coefficients and with discriminant different from zero) such that $F(\mathbb{Z}^2) = G(\mathbb{Z}^2)$. Does there exist $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z})$ such that*

$$F(aX + bY, cX + dY) = G(X, Y)? \tag{1.1}$$

If there exists no such matrix γ, the pair (F, G) is called an extraordinary pair and the form F is called extraordinary.

In order to answer this question, the article [1] shows the crucial importance of the group of automorphisms of F defined as

$$\mathrm{Aut}(F, \mathbb{Q}) := \{\gamma \in \mathrm{GL}(2, \mathbb{Q}) : F \circ \gamma = F\},$$

where $F \circ \gamma$ denotes the action of γ by linear change of variables (see (1.1)). It is known that, for any $F \in \mathrm{Bin}(d, \mathbb{Q})$, the group $\mathrm{Aut}(F, \mathbb{Q})$ is $\mathrm{GL}(2, \mathbb{Q})$–conjugate to one element among the set $\mathfrak{K}$ of ten subgroups of $\mathrm{GL}(2, \mathbb{Z})$ defined by

$$\mathfrak{K} = \{\mathbf{C}_1, \mathbf{C}_2, \mathbf{C}_3, \mathbf{C}_4, \mathbf{C}_6, \mathbf{D}_1, \mathbf{D}_2, \mathbf{D}_3, \mathbf{D}_4, \mathbf{D}_6\}, \tag{1.2}$$

where the letters $\mathbf{C}_k$ and $\mathbf{D}_\ell$ respectively correspond to cyclic and dihedral subgroups with cardinality k and 2ℓ. For the definition of these subgroups, we refer the reader to [1, Lemma

[*]CNRS, Laboratoire de mathématiques d'Orsay, Université Paris–Saclay, 91405 Orsay, France, etienne.fouvry@universite-paris-saclay.fr

[†]Institute for Theoretical Studies, ETH Zurich, 8092 Zurich, Switzerland, peter.koymans@eth-its.ethz.ch

5.1]. In [1], we treated the cases of $\mathbf{C}_1, \mathbf{C}_2, \mathbf{C}_3, \mathbf{C}_4, \mathbf{C}_6, \mathbf{D}_1, \mathbf{D}_2$, where we prove that an affirmative answer to Question 1.1 depends on the existence, in the group of automorphisms, of elements of order 3 with special type. The cases of $\mathbf{D}_3$ and $\mathbf{D}_6$ will be treated in [2], bringing to light a similar characterization but in a more intricate context.

In the present paper, we are concerned with the case of $\mathbf{D}_4$, which is the dihedral subgroup of $\mathrm{GL}(2, \mathbb{Z})$ generated by the two matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

This subgroup has order 8 and every element has order 1, 2 or 4. Write

$$G(X, Y) = a_d X^d + a_{d-1} X^{d-1} Y + \cdots + a_1 X Y^{d-1} + a_0 Y^d.$$

Let $G \in \mathrm{Bin}(d, \mathbb{Q})$. It is not difficult to show that $\mathbf{D}_4 \subseteq \mathrm{Aut}(G, \mathbb{Q})$ if and only if one has the equalities

$$a_k = 0 \text{ if } k \equiv 1 \bmod 2 \text{ and } a_k = a_{d-k} \text{ for } 0 \leq k \leq d. \tag{1.3}$$

In particular, d is even so $d \geq 4$. Furthermore, we have $\mathrm{Aut}(G, \mathbb{Q}) = \mathbf{D}_4$, since, in the list $\mathfrak{K}$ (see (1.2)) there is no group with cardinality strictly divisible by 8. Finally, every form F satisfying $\mathrm{Aut}(F, \mathbb{Q}) = \lambda^{-1} \mathbf{D}_4 \lambda$, with $\lambda \in \mathrm{GL}(2, \mathbb{Q})$, has the shape

$$F = G \circ \lambda,$$

where G satisfies (1.3). This follows from the general conjugation formula $\mathrm{Aut}(F \circ \lambda, \mathbb{Q}) = \lambda^{-1} \mathrm{Aut}(F, \mathbb{Q}) \lambda$.

Our central result is

Theorem 1.2. *Let $d \geq 4$. Then there is no extraordinary form F such that*

$$\mathrm{Aut}(F, \mathbb{Q}) \simeq_{\mathrm{GL}(2, \mathbb{Q})} \mathbf{D}_4.$$

This theorem was already announced in [1, Theorem A]. One simple consequence is

Corollary 1.3. *Let $F \in \mathrm{Bin}(4, \mathbb{Q})$ such that*

$$F(\mathbb{Z}^2) = \{m : m = t^4 + u^4 \text{ for some } (t, u) \in \mathbb{Z}^2\}.$$

Then there exists $(a, b, c, d) \in \mathbb{Z}^4$, with $ad - bc = \pm 1$, such that

$$F(X, Y) = (aX + cY)^4 + (bX + dY)^4.$$

The corollary follows upon combing Theorem 1.2 with [3, Lemma 3.3], which asserts that $\mathrm{Aut}(X^4 + Y^4, \mathbb{Q}) = \mathbf{D}_4$.

Acknowledgements

2 From extraordinary forms to coverings

2.1 Some definitions

By a *lattice*, we mean an additive subgroup of $\mathbb{Z}^2$ with rank 2. This lattice is *proper* when it is different from $\mathbb{Z}^2$. If Λ is a lattice generated by $\vec{u}, \vec{v} \in \mathbb{Z}^2$, the *index* of Λ is the positive integer

$$[\mathbb{Z}^2 : \Lambda] = |\mathbb{Z}^2 / \Lambda| = |\det(\vec{u}, \vec{v})|. \tag{2.1}$$

Definition 2.1. *Let* $\gamma \in \mathrm{GL}(2, \mathbb{Q})$. *By definition the lattice associated to* γ *is the subset* $L(\gamma)$ *of* $\mathbb{Z}^2$ *defined by*

$$L(\gamma) := \left\{ (x, y) \in \mathbb{Z}^2 : \gamma \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \right\}.$$

We will use the obvious remarks

$$L(\gamma) = L(-\gamma) \tag{2.2}$$

and

$$L(\gamma) = \mathbb{Z}^2 \iff \gamma \text{ has integer coefficients.} \tag{2.3}$$

We recall the following property, which is proved by a direct calculation (see [1, Lemma 6.9]).

Lemma 2.2. *Let* $\gamma \in \mathrm{GL}(2, \mathbb{Q})$. *Then* $[\mathbb{Z}^2 : L(\gamma)]$ *is an integer multiple of* $|\det \gamma|^{-1}$.

Several times we will use the next easy lemma, where $v_2(n)$ is the 2–adic valuation of the integer n with the convention $v_2(0) = +\infty$.

Lemma 2.3. *Let* $\alpha, \beta, \gamma \in \mathbb{Z}$ *with* $\gamma \neq 0$. *Suppose that* $v_2(\alpha) < v_2(\beta)$ *and* $v_2(\alpha) < v_2(\gamma)$. *Then the lattice defined by the equation*

$$\alpha x_1 + \beta x_2 \equiv 0 \bmod \gamma$$

is included in the lattice

$$\{(x_1, x_2) : x_1 \equiv 0 \bmod 2\}.$$

Definition 2.4. *Let* F_1 *and* F_2 *be two forms in* $\mathrm{Bin}(d, \mathbb{Q})$. *By definition, an isomorphism from* F_1 *to* F_2 *is an element* $\phi \in \mathrm{GL}(2, \mathbb{Q})$ *such that* $F_1 \circ \phi = F_2$. *The set of all such isomorphisms is denoted by* $\mathrm{Isom}(F_1 \to F_2, \mathbb{Q})$. *Suppose* $\mathrm{Isom}(F_1 \to F_2, \mathbb{Q})$ *is not empty and let* ρ *be one of its elements. Then we have the equalities*

$$\mathrm{Isom}(F_1 \to F_2, \mathbb{Q}) = \rho \cdot \mathrm{Aut}(F_2, \mathbb{Q}) = \mathrm{Aut}(F_1, \mathbb{Q}) \cdot \rho$$
$$\mathrm{Isom}(F_2 \to F_1, \mathbb{Q}) = \rho^{-1} \cdot \mathrm{Aut}(F_1, \mathbb{Q}) = \mathrm{Aut}(F_2, \mathbb{Q}) \cdot \rho^{-1}.$$

We extract from [1] the following key proposition

Proposition 2.5. *Let* $d \geq 3$ *and let* (F_1, F_2) *be a pair of extraordinary forms. Then there exists* $\rho \in \mathrm{GL}(2, \mathbb{Q})$, *a pair of extraordinary forms* (G_1, G_2) *and a pair* (D, ν) *of positive integers such that*

1. we have $F_1 = F_2 \circ \rho$,

2. we have

$$\left(G_1 \sim_{\mathrm{GL}(2,\mathbb{Z})} F_1 \text{ and } G_2 \sim_{\mathrm{GL}(2,\mathbb{Z})} F_2\right) \text{ or } \left(G_1 \sim_{\mathrm{GL}(2,\mathbb{Z})} F_2 \text{ and } G_2 \sim_{\mathrm{GL}(2,\mathbb{Z})} F_1\right),$$

3. we have

$$D, \nu \geq 1, D\nu > 1, D \mid \nu \text{ and } 1 \leq \nu \leq D^2. \tag{2.4}$$

The matrix

$$\gamma := \begin{pmatrix} D & 0 \\ 0 & D/\nu \end{pmatrix} \tag{2.5}$$

satisfies $G_1 = G_2 \circ \gamma$,

4. we have

$$[\mathbb{Z}^2 : L(\gamma)] = \min\left\{[\mathbb{Z}^2 : L(\tau)] : \tau \in \mathrm{Isom}(G_1 \to G_2, \mathbb{Q}) \cup \mathrm{Isom}(G_2 \to G_1, \mathbb{Q})\right\}, \tag{2.6}$$

5. and finally, we have the two coverings

$$\mathbb{Z}^2 = \bigcup_{\tau \in \mathrm{Isom}(G_1 \to G_2, \mathbb{Q})} L(\tau) = \bigcup_{\tau \in \mathrm{Isom}(G_2 \to G_1, \mathbb{Q})} L(\tau).$$

This proposition essentially gathers the following contents of [1]: Lemma 2.4, §7.1, §7.2 (particularly the relations (7.7), (7.8), (7.9)) and Proposition 9.1.

Comments 2.6. *1. This proposition is quite general, since it requires no assumption concerning the automorphism groups of F_1 or F_2.*

2. Item 1. will not be used in the sequel of the proof of Theorem 1.2. It recalls the starting point of the construction of γ and it implies that both $\mathrm{Aut}(F_1, \mathbb{Q})$ and $\mathrm{Aut}(F_2, \mathbb{Q})$ are $\mathrm{GL}(2, \mathbb{Q})$–conjugate by the formula (4.1).

3. The pair (G_1, G_2) is extraordinary with automorphism groups $\mathrm{GL}(2, \mathbb{Z})$–conjugate with the automorphism groups of F_1 and F_2.

4. The initial problem is symmetrical in (F_1, F_2). We eventually break this symmetry in item 4. to ensure the minimality of the index in (2.6). Note that $[\mathbb{Z}^2 : L(\gamma)] = \nu D^{-1}$.

5. Since γ belongs to $\mathrm{Isom}(G_2 \to G_1, \mathbb{Q})$, we can explicitly write the isomorphisms appearing in item 5. in terms of γ and $\mathrm{Aut}(G_1, \mathbb{Q})$ or $\mathrm{Aut}(G_2, \mathbb{Q})$ (see Definition 2.4).

6. In fact, we will only use the first equality written in item 5. The second one will be used in [2].

3 About coverings

3.1 General notions

Let a, b, c and d be four integers. To shorten notations, we write

$$\mathbb{Z} \begin{pmatrix} a \\ b \end{pmatrix} + \mathbb{Z} \begin{pmatrix} c \\ d \end{pmatrix} =: \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

for the subgroup of $\mathbb{Z}^2$ generated by $(a, b)^T$ and $(c, d)^T$. Recall that if $ad - bc \neq 0$, this subgroup is a lattice. Furthermore, if $|ad - bc| \geq 2$, this is a proper lattice.

Definition 3.1. *Let $k \geq 1$ be an integer and let $(\Lambda_i)_{1 \leq i \leq k}$ be k lattices. We say that*

$$\mathcal{C} = \{\Lambda_1, \ldots, \Lambda_k\}$$

is a covering of $\mathbb{Z}^2$ (or a covering) if and only if

$$\bigcup_{1 \leq i \leq k} \Lambda_i = \mathbb{Z}^2.$$

Definition 3.2 (Minimal covering). *Let $k \geq 1$, let Λ_i be lattices and let $\mathcal{C} = \{\Lambda_1, \ldots, \Lambda_k\}$ be a covering. We say that $\mathcal{C}$ is a minimal covering of length k if and only if replacing any Λ_i by some proper sublattice $\Lambda_i' \subsetneq \Lambda_i$, the set*

$$\{\Lambda_1, \ldots, \Lambda_{i-1}, \Lambda_i', \Lambda_{i+1}, \ldots, \Lambda_k\}$$

is not a covering.

If $\mathcal{C}$ is a minimal covering and if $1 \leq i \neq j \leq k$, we never have $\Lambda_i \subseteq \Lambda_j$. In particular, for $k \geq 2$, every Λ_i is a proper lattice. The following lemma asserts that from any covering one can extract a minimal covering

Lemma 3.3. *Let $k \geq 1$ and let*
$$\mathcal{C} := \{\Lambda_1, \ldots, \Lambda_k\}$$

be a covering. Then there exists an integer $1 \leq k' \leq k$, an injection $\phi : \{1, \ldots, k'\} \to \{1, \ldots, k\}$, and lattices Λ_j' $(1 \leq j \leq k')$, such that

$$\mathcal{C}' := \{\Lambda_1', \ldots, \Lambda_{k'}'\}$$

is a minimal covering, and for all $1 \leq j \leq k'$ one has $\Lambda_j' \subseteq \Lambda_{\phi(j)}$.

Proof. By reordering and suppressing some Λ_i if necessary, we suppose that

$$\bigcup_{1 \leq i \leq s} \Lambda_i = \mathbb{Z}^2 \quad \text{and} \quad \bigcup_{\substack{1 \leq i \leq s \\ i \neq j}} \Lambda_i \neq \mathbb{Z}^2 \quad \text{for all } 1 \leq j \leq s \tag{3.1}$$

for some $1 \leq s \leq k$. The case where $s = 1$ is trivial, so we suppose $s \geq 2$. Let

$$\mathcal{L}_s := \{M_s \text{ lattice} : M_s \subseteq \Lambda_s, \ \Lambda_1 \cup \Lambda_2 \cup \cdots \cup \Lambda_{s-1} \cup M_s = \mathbb{Z}^2\}.$$

We then have the equality

$$\mathbb{Z}^2 = \Lambda_1 \cup \cdots \cup \Lambda_{s-1} \cup \Lambda_s', \tag{3.2}$$

with $\Lambda_s' := \bigcap_{M_s \in \mathcal{L}_s} M_s$. The set Λ_s' is a subgroup of $\mathbb{Z}^2$. Its rank can not be 0 or 1, because we would have the equality $\cup_{1 \leq i \leq s-1} \Lambda_i = \mathbb{Z}^2$, which contradicts (3.1). So Λ_s' is a lattice and, by construction, it is the smallest lattice included in Λ_s and satisfying (3.2). We continue the same process for the covering

$$\{\Lambda_1, \Lambda_2, \ldots, \Lambda_{s-1}, \Lambda_s'\}$$

to replace Λ_{s-1} by a smaller lattice Λ_{s-1}'. By iterating this process, we prove the existence of lattices $(\Lambda_1', \ldots, \Lambda_s')$ with the following three properties

1. (inclusion) $\Lambda_i' \subseteq \Lambda_i$ for $1 \leq i \leq s$,

2. (covering) $\bigcup_{1 \le i \le s} \Lambda'_i = \mathbb{Z}^2$,

3. (partial minimality) let $1 \le k \le s$ and let M_k be a lattice such that $M_k \subseteq \Lambda'_k$ and such that
$$\Lambda_1 \cup \cdots \cup \Lambda_{k-1} \cup M_k \cup \Lambda'_{k+1} \cup \cdots \cup \Lambda'_s = \mathbb{Z}^2, \tag{3.3}$$
then $M_k = \Lambda'_k$.

We now prove that $(\Lambda'_1, \ldots, \Lambda'_s)$ is a minimal covering associated with $\{\Lambda_1, \ldots, \Lambda_s\}$. So we consider lattices M_i such that $M_i \subseteq \Lambda'_i$ and such that
$$\mathbb{Z}^2 = M_1 \cup \cdots \cup M_s. \tag{3.4}$$

Our aim is to show that $M_i = \Lambda'_i$. The equality (3.4) implies
$$\mathbb{Z}^2 = \Lambda_1 \cup \cdots \cup \Lambda_{s-1} \cup M_s.$$

Therefore we deduce from the partial minimality property (see (3.3)) that $M_s = \Lambda'_s$. We now have the equality
$$\mathbb{Z}^2 = M_1 \cup M_2 \cup \cdots \cup M_{s-1} \cup \Lambda'_s,$$

which implies
$$\mathbb{Z}^2 = \Lambda_1 \cup \Lambda_2 \cup \cdots \cup \Lambda_{s-2} \cup M_{s-1} \cup \Lambda'_s.$$

From the partial minimality property (see (3.3)) we obtain the equality $M_{s-1} = \Lambda'_{s-1}$. The end of the proof is by induction. $\square$

3.2 Minimal coverings with length at most 4

We now list all the minimal coverings with length bounded by 4.

Theorem 3.4. *The following is a complete list (up to permutation) of the minimal coverings of $\mathbb{Z}^2$ of length at most four*

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \tag{3.5}$$

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} \right\} \tag{3.6}$$

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix} \right\} \tag{3.7}$$

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 4 \end{bmatrix} \right\} \tag{3.8}$$

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 3 & 4 \end{bmatrix} \right\} \tag{3.9}$$

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix} \right\}. \tag{3.10}$$

Proof. By [1, Lemma 6.6 & 6.7], there is no minimal covering with length two and only one with length three. So we are left with finding all the minimal coverings with length four.

● *Checking that the sets of lattices (3.7), (3.8), (3.9) and (3.10) are coverings.* One way to prove this is to give explicit equations of these lattices. Let us focus on (3.9) since the other cases are similar. The equations of the four corresponding lattices are respectively

$$y \equiv 0 \bmod 2, \; x \equiv 0 \bmod 2, \; 3x + y \equiv 0 \bmod 4, \; x + y \equiv 0 \bmod 4.$$

It remains to check that any pair (a, b) of congruence classes modulo 4 satisfies at least one of the four equations above.

● *Construction of the minimal coverings.* Let $L_1, \ldots, L_4$ be such that

$$L_1 \cup L_2 \cup L_3 \cup L_4 = \mathbb{Z}^2.$$

Ruling out the trivial covering (3.5), we may assume that L_1, L_2, L_3 and L_4 are all proper subgroups of $\mathbb{Z}^2$. The argument will proceed by repeatedly looking at points outside of $L_1 \cup L_2 \cup L_3 \cup L_4$ and then analyzing in which possible L_i such a point can be. For convenience, these points will be chosen with small coordinates.

By permuting the L_i if necessary, we may assume without loss of generality that

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1.$$

Since $L_1 \neq \mathbb{Z}^2$, we see that $\begin{pmatrix} 0 \\ 1 \end{pmatrix} \notin L_1$. By permuting the L_i again if necessary, we may assume without loss of generality that

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \in L_2.$$

Finally, a similar argument shows that we may assume without loss of generality that

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in L_3.$$

Summarizing, we have so far

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in L_2, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in L_3.$$

We will now consider the vector $(1, -1)^T$, and the proof naturally splits into two cases (case 1 and case 2). Note that we must have $(1, -1)^T \in L_3$ (case 1) or $(1, -1)^T \in L_4$ (case 2).

Case 1

Let us assume that $(1, -1)^T \in L_3$. Then we have

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in L_2, \quad L_3 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Note that equality must indeed hold for L_3, since the subgroup

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

has prime index in $\mathbb{Z}^2$ and $L_3 \neq \mathbb{Z}^2$ by assumption. For the rest of the proof, we will often use the above observation implicitly. Looking at the vector $(2,1)^T$, we get two further cases, namely $(2,1)^T \in L_2$ (case 1.1) or $(2,1)^T \in L_4$ (case 1.2), since the cases $(2,1)^T \in L_1$ or $(2,1)^T \in L_3$ are impossible (because this forces $L_1 = \mathbb{Z}^2$ respectively $L_3 = \mathbb{Z}^2$).

Case 1.1

In this case we have $(2,1)^T \in L_2$ and therefore

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad L_2 = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Considering the vector $(1,2)^T$ yields two subcases: $(1,2)^T \in L_1$ (case 1.1.1) or $(1,2)^T \in L_4$ (case 1.1.2).

Case 1.1.1

We have

$$L_1 = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

which corresponds to the covering (3.6).

Case 1.1.2

Currently, we know that

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad L_2 = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{pmatrix} 1 \\ 2 \end{pmatrix} \in L_4.$$

We analyze the possibilities for the vector $(1,-2)^T$. If we add this vector to L_1, then the resulting covering is not minimal, as L_4 may be removed to obtain the covering (3.6). Therefore we arrive at the covering

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad L_2 = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 2 & -2 \end{bmatrix} \subseteq L_4.$$

To finish the argument for this case, we consider the vector $(1,4)^T$. If we add it to L_4, then the corresponding covering is not minimal, as L_1 may be removed to get the covering (3.6). Thus we obtain

$$L_1 = \begin{bmatrix} 1 & 1 \\ 0 & 4 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad L_4 = \begin{bmatrix} 1 & 1 \\ 2 & -2 \end{bmatrix},$$

which is the covering (3.8).

Case 1.2

At this point we have

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in L_2, \quad L_3 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{pmatrix} 2 \\ 1 \end{pmatrix} \in L_4.$$

We have that $(-2, 1)^T \in L_2$ (case 1.2.1) or $(-2, 1)^T \in L_4$ (case 1.2.2).

Case 1.2.1

The following information is available to us

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad L_2 = \begin{bmatrix} 0 & -2 \\ 1 & 1 \end{bmatrix} \quad L_3 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{pmatrix} 2 \\ 1 \end{pmatrix} \in L_4.$$

Since the vectors $(2, 1)^T, (1, -2)^T, (1, 2)^T$ together generate $\mathbb{Z}^2$, at least one of $(1, -2)^T$ or $(1, 2)^T$ must be in L_1. Thus we get the covering (3.6) after removing L_4.

Case 1.2.2

We obtain that

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in L_2, \quad L_3 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 2 & -2 \\ 1 & 1 \end{bmatrix} \subseteq L_4.$$

We must have that $(1, -2)^T \in L_1$. We will now consider the vector $(4, 1)^T$. We either have $(4, 1)^T \in L_2$, in which case we have the covering (3.7), or $(4, 1) \in L_4$, in which case we get the covering (3.6) after removing L_2.

Case 2

We will now assume that $(1, -1)^T \in L_4$. Then we are in the situation

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in L_2, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in L_3, \quad \begin{pmatrix} 1 \\ -1 \end{pmatrix} \in L_4.$$

Inspecting the possibilities for the point $(2, 1)^T$, we come to the conclusion that $(2, 1)^T \in L_2$ (case 2.1) or $(2, 1)^T \in L_4$ (case 2.2).

Case 2.1

We have arrived at the following configuration

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad L_2 = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in L_3, \quad \begin{pmatrix} 1 \\ -1 \end{pmatrix} \in L_4.$$

Considering the vector $(1, 2)^T$, we will split into the cases $(1, 2)^T \in L_1$ (case 2.1.1) or $(1, 2)^T \in L_4$ (case 2.1.2).

9

Case 2.1.1

Gathering the information so far, we have

$$L_1 = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in L_3, \quad \begin{pmatrix} 1 \\ -1 \end{pmatrix} \in L_4.$$

We inspect the different locations for the vector $(3,1)^T$. If $(3,1)^T \in L_3$, we obtain the cover (3.6) after dropping the lattice L_4. Suppose instead that $(3,1)^T \in L_4$. Then we have

$$L_1 = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in L_3, \quad \begin{bmatrix} 1 & 3 \\ -1 & 1 \end{bmatrix} \subseteq L_4.$$

At last we consider the vector $(3,-1)^T$. If $(3,-1)^T \in L_3$, we get

$$L_1 = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 3 \\ 1 & -1 \end{bmatrix}, \quad L_4 = \begin{bmatrix} 1 & 3 \\ -1 & 1 \end{bmatrix},$$

which corresponds to the covering (3.9). If instead $(3,-1)^T \in L_4$, we get the covering (3.6) upon removing L_3.

Case 2.1.2

At this stage we may write

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad L_2 = \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in L_3, \quad \begin{bmatrix} 1 & 1 \\ -1 & 2 \end{bmatrix} \in L_4.$$

Looking at $(3,1)^T$, we obtain $(3,1)^T \in L_3$. Then looking at $(3,2)^T$, we conclude that $(3,2)^T \in L_1$. Once we discard L_4, we get the covering (3.6).

Case 2.2

We know that

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in L_2, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in L_3, \quad L_4 = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}.$$

Considering the vector $(3,1)^T$, the argument splits in two cases, namely $(3,1)^T \in L_2$ (case 2.2.1) and $(3,1)^T \in L_3$ (case 2.2.2).

Case 2.2.1

We have arrived at

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad L_2 = \begin{bmatrix} 0 & 3 \\ 1 & 1 \end{bmatrix}, \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in L_3, \quad L_4 = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}.$$

This forces $(4,1)^T \in L_3$ and then $(1,3)^T \in L_1$, thus giving

$$L_1 = \begin{bmatrix} 1 & 1 \\ 0 & 3 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & 3 \\ 1 & 1 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 4 \\ 1 & 1 \end{bmatrix}, \quad L_4 = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}.$$

This is precisely the covering (3.10).

Case 2.2.2

Finally, we have to consider the configuration

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in L_1, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in L_2, \quad L_3 = \begin{bmatrix} 1 & 3 \\ 1 & 1 \end{bmatrix}, \quad L_4 = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}.$$

Considering the vectors $(2,3)^T$ and $(3,2)^T$ simultaneously, this gives two cases

$$L_1 = \begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & 2 \\ 1 & 3 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 3 \\ 1 & 1 \end{bmatrix}, \quad L_4 = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}$$

and

$$L_1 = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & 3 \\ 1 & 2 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 3 \\ 1 & 1 \end{bmatrix}, \quad L_4 = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}.$$

In the first case, the lattice L_4 is redundant, and we get the covering (3.6) upon discarding L_4. The last case does not correspond to any non-trivial minimal covering. Indeed, all the L_i have prime index, but their union does not contain the point $(1,4)^T$. $\quad\square$

Theoretically speaking, the method employed above leads to the complete list of minimal coverings with length $\leq k$, where k is a given integer. The case $k \leq 6$ is vital for our work [2], which handles the case where the automorphism group is conjugate to $\mathbf{D}_3$ or $\mathbf{D}_6$. However, when $k = 5$ and $k = 6$, the number of cases is huge and the method is no longer feasible to execute by hand. This is the reason why we have written algorithms to produce the list of 9 minimal coverings with length equal to 5, and the list of 49 minimal coverings with length equal to 6. To make this paper independent of computer calculations, we have decided to prove Theorem 3.4 by hand, but the results of Theorem 3.4 are rapidly reproduced by our algorithms that will be published in [2].

4 Proof of Theorem 1.2

4.1 Preparation of the covering

The proof of this theorem is accomplished by contradiction by exploiting Proposition 2.5. We start from a pair of extraordinary forms (F_1, F_2) such that $\mathrm{Aut}(F_1, \mathbb{Q}) \simeq_{\mathrm{GL}(2,\mathbb{Q})} \mathbf{D}_4$. By Comment 2 of 2.6 we also have $\mathrm{Aut}(F_2, \mathbb{Q}) \simeq_{\mathrm{GL}(2,\mathbb{Q})} \mathbf{D}_4$. By item *2.* of Proposition 2.5, we also have

$$\mathrm{Aut}(G_1, \mathbb{Q}), \, \mathrm{Aut}(G_2, \mathbb{Q}) \simeq_{\mathrm{GL}(2,\mathbb{Q})} \mathbf{D}_4$$

thanks to the conjugation formula

$$\mathrm{Aut}(F \circ \lambda, \mathbb{Q}) = \lambda^{-1} \mathrm{Aut}(F, \mathbb{Q}) \lambda, \text{ for all } \lambda \in \mathrm{GL}(2, \mathbb{Q}) \text{ and for all } F \in \mathrm{Bin}(d, \mathbb{Q}). \quad (4.1)$$

Recall that

$$G_1 \circ \gamma^{-1} = G_2,$$

where γ is defined in (2.5). We write $\mathbf{D}_4$ explicitly as

$$\mathbf{D}_4 = \{\mathrm{id}, A_1, A_2, A_3, -\mathrm{id}, -A_1, -A_2, -A_3\},$$

11

with

$$A_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ and } A_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

So we have the equality

$$\text{Aut}(G_2, \mathbb{Q}) = T_2^{-1} \mathbf{D}_4 T_2,$$

where T_2 is some matrix of $\text{GL}(2, \mathbb{Q})$ that we write as

$$T_2 = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix},$$

where the t_i are coprime integers. An important integer is

$$d_2 := |\det T_2| = |t_1 t_4 - t_2 t_3|. \tag{4.2}$$

Thus we split $\text{Aut}(G_2, \mathbb{Q})$ into two disjoint sets

$$\text{Aut}(G_2, \mathbb{Q}) = \mathfrak{S} \cup (-\mathfrak{S}),$$

with

$$\mathfrak{S} := \{\text{id}, T_2^{-1} A_1 T_2, T_2^{-1} A_2 T_2, T_2^{-1} A_3 T_2\}.$$

Furthermore, we have $\text{Isom}(G_1 \to G_2, \mathbb{Q}) = \gamma^{-1} \text{Aut}(G_2, \mathbb{Q})$, by Definition 2.4 and we put

$$\Lambda(\sigma) := \{\mathbf{x} \in \mathbb{Z}^2 : \gamma^{-1} \sigma(\mathbf{x}) \in \mathbb{Z}^2\} = L(\gamma^{-1}\sigma), \tag{4.3}$$

see Definition 2.1. The equality $\Lambda(-\sigma) = \Lambda(\sigma)$ follows from (2.2). Combining these remarks with the first equality of item 5. of Proposition 2.5, we have the covering of $\mathbb{Z}^2$

$$\mathbb{Z}^2 = \bigcup_{\sigma \in \mathfrak{S}} \Lambda(\sigma) \tag{4.4}$$

by at most four lattices. We will require the explicit equations defining the $\Lambda(\sigma)$. By a direct computation we have

Lemma 4.1. For $\sigma \in \mathfrak{S}$, the lattice $\Lambda(\sigma)$ is the set of $(x_1, x_2) \in \mathbb{Z}^2$ such that

$$\Lambda(\text{id}) : \begin{cases} x_1 & \equiv 0 \mod D \\ \nu x_2 & \equiv 0 \mod D \end{cases} \tag{4.5}$$

$$\Lambda(T_2^{-1} A_1 T_2) : \begin{cases} (t_1 t_2 + t_3 t_4)x_1 + (t_2^2 + t_4^2)x_2 & \equiv 0 \mod d_2 D \\ \nu((t_1^2 + t_3^2)x_1 + (t_1 t_2 + t_3 t_4)x_2) & \equiv 0 \mod d_2 D \end{cases} \tag{4.6}$$

$$\Lambda(T_2^{-1} A_2 T_2) : \begin{cases} (t_3 t_4 - t_1 t_2)x_1 + (t_4^2 - t_2^2)x_2 & \equiv 0 \mod d_2 D \\ \nu((t_1^2 - t_3^2)x_1 + (t_1 t_2 - t_3 t_4)x_2) & \equiv 0 \mod d_2 D \end{cases} \tag{4.7}$$

$$\Lambda(T_2^{-1} A_3 T_2) : \begin{cases} (t_2 t_3 + t_1 t_4)x_1 + (2t_2 t_4)x_2 & \equiv 0 \mod d_2 D \\ \nu((2t_1 t_3)x_1 + (t_2 t_3 + t_1 t_4)x_2) & \equiv 0 \mod d_2 D. \end{cases} \tag{4.8}$$

12

By (2.4), the second equation of (4.5) is redundant and thus we have the equality

$$[\mathbb{Z}^2 : \Lambda(\mathrm{id})] = D. \tag{4.9}$$

Several times we will use the following important lemma.

Lemma 4.2. *We adopt the hypotheses of Proposition 2.5 and the notations above. Then the covering* (4.4) *satisfies*

$$\Lambda(\sigma) \neq \mathbb{Z}^2 \text{ for all } \sigma \in \mathfrak{S}. \tag{4.10}$$

Proof. For the sake of contradiction, suppose that $\Lambda(\sigma) = \mathbb{Z}^2$ for some $\sigma \in \mathfrak{S}$. By the definition (4.3) and the remark (2.3), the matrix associated with $\gamma^{-1}\sigma$ (with $\sigma \in \mathrm{Aut}(G_2, \mathbb{Q})$) has integer coefficients. This means that there exists a matrix M_1 with integer coefficients such that

$$G_1 \circ M_1 = G_2. \tag{4.11}$$

We use the minimality of the index of $L(\gamma)$ (see item *4.* of Proposition 2.5) to write

$$1 = [\mathbb{Z}^2 : \Lambda(\sigma)] = [\mathbb{Z}^2 : L(\gamma^{-1}\sigma)] \geq [\mathbb{Z}^2 : L(\gamma)] \geq 1.$$

Again by the remark (2.3) we deduce that the matrix M_2 associated with γ (see (2.5)), has integer coefficients. So we have the equality

$$G_2 \circ M_2 = G_1.$$

Combining with (4.11), we obtain

$$G_1 \circ (M_1 \cdot M_2) = G_2 \circ M_2 = G_1,$$

which implies that $|\det(M_1 \cdot M_2)| = 1$, hence $|\det M_1| = |\det M_2| = 1$. So the matrices M_1 and M_2 belong to $\mathrm{GL}(2, \mathbb{Z})$. Therefore the equality (4.11) shows that G_1 and G_2 are $\mathrm{GL}(2, \mathbb{Z})$–equivalent, which is contrary to the hypothesis that (G_1, G_2) is an extraordinary pair (see Comment 3 of 2.6). $\square$

We now initiate the proof of Theorem 1.2 by successively restricting the values of D.

4.2 The integer D satisfies $2 \leq D \leq 4$

We want to prove the inequality

$$2 \leq D \leq 4. \tag{4.12}$$

We separate our discussion into two subcases based on the value of the union of the lattices $\Lambda(\sigma)$ with $\sigma \neq \mathrm{id}$.

4.2.1 If the last three lattices do not cover $\mathbb{Z}^2$

We suppose that

$$\mathbb{Z}^2 \neq \bigcup_{\sigma \in \mathfrak{S} - \{\mathrm{id}\}} \Lambda(\sigma). \tag{4.13}$$

This condition means that $\Lambda(\mathrm{id})$ is essential to obtain the covering (4.4). By Lemma 4.2 we know that none of the lattices appearing in this covering are trivial. By the existence of a minimal covering (see Lemma 3.3), there exist four subgroups Λ_i' ($0 \le i \le 3$) such that

$$
\begin{cases}
\Lambda_i' \text{ is either } \{0\} \text{ or a proper lattice,} \\
\Lambda_0' \subseteq \Lambda(\mathrm{id}) \text{ and } \Lambda_i' \subseteq \Lambda(T_2^{-1} A_i T_2) \ (1 \le i \le 3), \\
\cup_{0 \le i \le 3} \Lambda_i' = \mathbb{Z}^2, \\
\mathcal{C} := \{\Lambda_i' : \Lambda_i' \ne \{0\}\} \text{ is a minimal covering of } \mathbb{Z}^2.
\end{cases}
$$

In particular, by (4.4) and by (4.13), we deduce that $\Lambda_0' \ne \{0\}$. Thus the covering $\mathcal{C}$ contains three or four lattices and $\mathcal{C}$ appears as one of the minimal coverings $(3.6), \ldots, (3.10)$ of Theorem 3.4. Thus the lattice Λ_0' is necessarily one of the lattices of these five minimal coverings. By (2.1), all these lattices have an index equal to 2, 3 or 4. In particular, we have $[\mathbb{Z}^2 : \Lambda_0'] \in \{2, 3, 4\}$. Finally, $[\mathbb{Z}^2 : \Lambda(\mathrm{id})]$ is a divisor (different from 1) of $[\mathbb{Z}^2 : \Lambda_0']$. By (4.9), we deduce the inequality $2 \le D \le 4$, and (4.12) is proved.

4.2.2 If the last three lattices cover $\mathbb{Z}^2$

We now suppose that

$$
\mathbb{Z}^2 = \bigcup_{\sigma \in \mathfrak{S} - \{\mathrm{id}\}} \Lambda(\sigma). \tag{4.14}
$$

By (4.10), the equality (4.14) exhibits a non-trivial covering of $\mathbb{Z}^2$ by three lattices. By Theorem 3.4 and by Lemma 3.3 we have the equality

$$
\{\Lambda(T_2^{-1} A_1 T_2), \Lambda(T_2^{-1} A_2 T_2), \Lambda(T_2^{-1} A_3 T_2)\} = \{\Lambda_0, \Lambda_1, \Lambda_2\}, \tag{4.15}
$$

where the covering (3.6) is written as $\{\Lambda_0, \Lambda_1, \Lambda_2\}$ respectively.

4.2.2.1 If (4.14) holds, then the integer D is not divisible by an odd prime p

For the sake of contradiction, suppose that D is divisible by some $p \ge 3$. We will show that there exists at least one $\sigma \in \mathfrak{S} - \{\mathrm{id}\}$ such that

$$
p \mid [\mathbb{Z}^2 : \Lambda(\sigma)]. \tag{4.16}
$$

Such a divisibility is impossible since, on the right–hand side of (4.15), all the lattices have an index equal to 2. To prove (4.16), we will argue by contradiction. So we suppose that

$$
p \nmid [\mathbb{Z}^2 : \Lambda(\sigma)] \text{ for all } \sigma \ne \mathrm{id}. \tag{4.17}
$$

By keeping only the first equation of the systems defining the lattices modulo p, we see that the lattices $\Lambda(T_2^{-1} A_1 T_2)$, $\Lambda(T_2^{-1} A_2 T_2)$ and $\Lambda(T_2^{-1} A_3 T_2)$ (see (4.6), (4.7) and (4.8)) are respectively included in the following lattices $\mathcal{L}_p$

$$
\mathcal{L}_p(T_2^{-1} A_1 T_2) : (t_1 t_2 + t_3 t_4) x_1 + (t_2^2 + t_4^2) x_2 \equiv 0 \bmod p, \tag{4.18}
$$

$$
\mathcal{L}_p(T_2^{-1} A_2 T_2) : (t_3 t_4 - t_1 t_2) x_1 + (t_4^2 - t_2^2) x_2 \equiv 0 \bmod p, \tag{4.19}
$$

$$
\mathcal{L}_p(T_2^{-1} A_3 T_2) : (t_2 t_3 + t_1 t_4) x_1 + (2 t_2 t_4) x_2 \equiv 0 \bmod p. \tag{4.20}
$$

The index of these three lattices is 1 or p. It can not be equal to p, otherwise we would have (4.16) for some σ. So the index is always equal to 1, which means that p divides all the coefficients

$$(t_1 t_2 + t_3 t_4), \ (t_2^2 + t_4^2), \ (t_3 t_4 - t_1 t_2), \ (t_4^2 - t_2^2), \ (t_2 t_3 + t_1 t_4) \text{ and } (2 t_2 t_4). \tag{4.21}$$

This implies that p divides t_2 and t_4. Let $g := \gcd(t_2, t_4, p^\infty) \geq p, \tilde{t}_2 = t_2/g, \tilde{t}_4 = t_4/g$. We observe that g divides d_2, by its definition (4.2). We return to the original system of equations (4.6), (4.7) and (4.8), where we keep the first equation of each system. After division by g, we observe that the lattices $\Lambda(T_2^{-1} A_1 T_2)$, $\Lambda(T_2^{-1} A_2 T_2)$ and $\Lambda(T_2^{-1} A_3 T_2)$ are respectively included in the following lattices

$$\tilde{\mathcal{L}}_p(T_2^{-1} A_1 T_2) : (t_1 \tilde{t}_2 + t_3 \tilde{t}_4) x_1 \equiv 0 \bmod p, \tag{4.22}$$

$$\tilde{\mathcal{L}}_p(T_2^{-1} A_2 T_2) : (t_3 \tilde{t}_4 - t_1 \tilde{t}_2) x_1 \equiv 0 \bmod p, \tag{4.23}$$

$$\tilde{\mathcal{L}}_p(T_2^{-1} A_3 T_2) : (\tilde{t}_2 t_3 + t_1 \tilde{t}_4) x_1 \equiv 0 \bmod p. \tag{4.24}$$

We observe that $\gcd(t_1, t_3, p) = 1$ (otherwise the integers t_i would not be coprime altogether), and that $\gcd(\tilde{t}_2, \tilde{t}_4, p) = 1$.

– Suppose that p does not divide $(t_1 \tilde{t}_2 + t_3 \tilde{t}_4)$, then the lattice $\tilde{\mathcal{L}}_p(T_2^{-1} A_1 T_2)$ has its index equal to p, and since this lattice contains $\Lambda(T_2^{-1} A_1 T_2)$, we obtain a contradiction with (4.17).

– Same type of reasoning when p does not divide $(t_3 \tilde{t}_4 - t_1 \tilde{t}_2)$.

– Now suppose that p divides $(t_1 \tilde{t}_2 + t_3 \tilde{t}_4)$ and $(t_3 \tilde{t}_4 - t_1 \tilde{t}_2)$, then p divides $t_1 \tilde{t}_2$ and $t_3 \tilde{t}_4$. The above coprimality conditions imply that p does not divide the coefficient of x_1 in (4.24), contradicting (4.17).

So D has no odd prime divisor when (4.14) holds.

4.2.2.2   If (4.14) holds, then the integer D is not divisible by 8

The strategy is the same as in §4.2.2.1. We suppose that D is divisible by 8. We will prove that there is a $\sigma \in \mathfrak{S} - \{\mathrm{id}\}$ such that

$$4 \mid [\mathbb{Z}^2 : \Lambda(\sigma)]. \tag{4.25}$$

Such a divisibility contradicts the equality (4.15), since all the lattices Λ_i ($1 \leq i \leq 3$) have index equal to 2. To prove (4.25), we will argue by contradiction. So we suppose that

$$4 \nmid [\mathbb{Z}^2 : \Lambda(\sigma)] \text{ for all } \sigma \neq \mathrm{id}. \tag{4.26}$$

The lattices $\Lambda(T_2^{-1} A_1 T_2)$, $\Lambda(T_2^{-1} A_2 T_2)$ and $\Lambda(T_2^{-1} A_3 T_2)$ are respectively included in the following lattices

$$\mathcal{L}_8(T_2^{-1} A_1 T_2) : (t_1 t_2 + t_3 t_4) x_1 + (t_2^2 + t_4^2) x_2 \equiv 0 \bmod 8,$$

$$\mathcal{L}_8(T_2^{-1} A_2 T_2) : (t_3 t_4 - t_1 t_2) x_1 + (t_4^2 - t_2^2) x_2 \equiv 0 \bmod 8,$$

$$\mathcal{L}_8(T_2^{-1} A_3 T_2) : (t_2 t_3 + t_1 t_4) x_1 + (2 t_2 t_4) x_2 \equiv 0 \bmod 8.$$

These lattices have an index equal to 1, 2, 4 or 8. It can not be divisible by 4 (otherwise, we would contradict (4.26)). So these indexes are equal to 1 or 2, which means that 4 divides all the coefficients listed in (4.21). This implies that 2 divides t_2 and t_4. Let $g = (t_2, t_4, 2^\infty) \geq 2$,

15

$\tilde{t}_2 = t_2/g$, $\tilde{t}_4 = t_4/g$. We return to the initial definitions of the lattices (4.6), (4.7) and (4.8), where we only keep the first equation. Since g divides d_2, we observe that the lattices $\Lambda(T_2^{-1}A_1T_2)$, $\Lambda(T_2^{-1}A_2T_2)$ and $\Lambda(T_2^{-1}A_3T_2)$ are respectively included in the following lattices

$$\tilde{\mathcal{L}}_8(T_2^{-1}A_1T_2) : (t_1\tilde{t}_2 + t_3\tilde{t}_4)x_1 + g(\tilde{t}_2^2 + \tilde{t}_4^2)x_2 \equiv 0 \bmod 8, \tag{4.27}$$

$$\tilde{\mathcal{L}}_8(T_2^{-1}A_2T_2) : (t_3\tilde{t}_4 - t_1\tilde{t}_2)x_1 + g(\tilde{t}_4^2 - \tilde{t}_2^2)x_2 \equiv 0 \bmod 8, \tag{4.28}$$

$$\tilde{\mathcal{L}}_8(T_2^{-1}A_3T_2) : (\tilde{t}_2 t_3 + t_1\tilde{t}_4)x_1 + g(2\tilde{t}_2\tilde{t}_4)x_2 \equiv 0 \bmod 8. \tag{4.29}$$

We exploit the coprimality $\gcd(t_1, t_3, 2) = 1$ (otherwise, the integers t_i would not be coprime altogether) and the coprimality $\gcd(\tilde{t}_2, \tilde{t}_4, 2) = 1$ to deduce that at least one of the three coefficients attached to x_1 in (4.27), (4.28) and (4.29) is not divisible by 4. This implies that the corresponding lattice $\tilde{\mathcal{L}}_8(\sigma)$ has index equal to 4 or 8. Hence the associated lattice $\Lambda(\sigma)$ (contained in $\tilde{\mathcal{L}}_8(\sigma)$) has index divisible by 4. This contradicts our assumption (4.26).

We have considered all the possible cases. The proof of (4.12) is complete.

4.3 The integer D is different from 3

Our task is to prove that

$$D \neq 3. \tag{4.30}$$

We will now assume that $D = 3$ to derive a contradiction. We already know that $[\mathbb{Z}^2 : \Lambda(\mathrm{id})] = D = 3$ by (4.9) and $\Lambda(\sigma) \neq \mathbb{Z}^2$ for all $\sigma \in \mathfrak{S}$ by Lemma 4.2. Reasoning as before, when we obtained (4.16), there exists $\sigma \in \mathfrak{S} - \{\mathrm{id}\}$ such that

$$3 \mid [\mathbb{Z}^2 : \Lambda(\sigma)].$$

Then the minimal covering contained in the covering $\{\Lambda(\sigma) : \sigma \in \mathfrak{S}\}$ (see (4.4)), which exists by Lemma 3.3, can only be the covering (3.10) by Theorem 3.4. Then the covering $\{\Lambda(\sigma) : \sigma \in \mathfrak{S}\}$ from (4.4) must coincide with (3.10).

Write $g = \gcd(t_2, t_4, 3^\infty)$, $\tilde{t}_2 = t_2/g$ and $\tilde{t}_4 = t_4/g$. We now split our discussion according to the classes modulo 3 of the numbers g, t_2 and t_4.

4.3.1 If $3 \mid g$

We follow the arguments that led to equation (4.16). In particular, consider the three lattices $\tilde{\mathcal{L}}_p$ defined by (4.22), (4.23) and (4.24) with $p = 3$. At least, one of the coefficients of x_1 is non-zero modulo 3. Thus we get the existence of some $\sigma \in \mathfrak{S} - \{\mathrm{id}\}$, such that

$$\Lambda(\sigma) \subseteq \{(x_1, x_2) : x_1 \equiv 0 \bmod 3\}.$$

But $\Lambda(\mathrm{id}) = \{(x_1, x_2) : x_1 \equiv 0 \bmod 3\}$ (see (4.5) and (2.4)). So the covering (4.4) can never be equal to (3.10), which is the desired contradiction.

4.3.2 If $3 \nmid g$, $3 \nmid t_2$, $3 \nmid t_4$ and $t_2 \equiv t_4 \bmod 3$

Under these assumptions, we have the congruences

$$t_2^2 + t_4^2 \equiv 2 \bmod 3, \ 2t_2 t_4 \equiv 2 \bmod 3$$

and

$$t_1t_2 + t_3t_4 \equiv t_2t_3 + t_1t_4 \bmod 3.$$

By (4.18) and (4.20), we see that the lattices $\mathcal{L}_3(T_2^{-1}A_1T_2)$ and $\mathcal{L}_3(T_2^{-1}A_3T_2)$ coincide. Both have index 3. This implies that the two lattices $\Lambda(T_2^{-1}A_1T_2)$ and $\Lambda(T_2^{-1}A_3T_2)$ sit inside the same lattice with index 3. We obtain the same contradiction as in §4.3.1.

4.3.3   If $3 \nmid g$, $3 \nmid t_2$, $3 \nmid t_4$ and $t_2 \not\equiv t_4 \bmod 3$

In this situation, we obtain

$$t_2^2 + t_4^2 \equiv 2 \bmod 3, 2t_2t_4 \equiv 1 \bmod 3$$

and

$$t_1t_2 + t_3t_4 \equiv (2t_2t_4)(t_1t_2 + t_3t_4) \equiv 2(t_1t_4 + t_2t_3) \bmod 3.$$

Up to a factor 2 the equations (4.18) and (4.20) coincide. Once again, this implies that two of the lattices appearing in the covering (4.4) are sublattices of the same lattice with index 3. We obtain the same contradiction as above.

4.3.4   If $3 \nmid g$ and if either $3 \mid t_2$ or $3 \mid t_4$

Consider the lattices $\mathcal{L}_3(T_2^{-1}A_1T_2)$ and $\mathcal{L}_3(T_2^{-1}A_2T_2)$ defined by (4.18) and (4.19). Their equations reduce to $\pm(ax_1 + x_2) \equiv 0 \bmod 3$ (for some integer a). So these two lattices coincide, and $\Lambda(T_2^{-1}A_1T_2)$ and $\Lambda(T_2^{-1}A_2T_2)$ are both included in the same lattice with index 3. Therefore we obtain a contradiction with the covering (4.4) in this case as well.

The proof of (4.30) is complete. Combining (4.12) and (4.30), we have reduced our theorem to the following situation.

4.4   Study when $D \in \{2, 4\}$

Our first task is to circumscribe the possible values of ν. Recall the conditions (2.4). They lead to the following possibilities for (D, ν): $(2, 2)$, $(2, 4)$, $(4, 4)$, $(4, 8)$, $(4, 12)$ and $(4, 16)$. We will restrict this list to

$$(D, \nu) \in \{(2, 2), (2, 4), (4, 4), (4, 8)\}. \tag{4.31}$$

To prove (4.31), we start from the covering (4.4) with the condition (4.10). Two possibilities occur

- If for some $\sigma^\dagger \in \mathfrak{S}$, one has $\cup_{\sigma \in \mathfrak{S} - \{\sigma^\dagger\}} \Lambda(\sigma) = \mathbb{Z}^2$. This is a covering by three lattices. By Theorem 3.4, these three lattices have index 2. So we have

$$[\mathbb{Z}^2 : \Lambda(\sigma_0)] = 2 \text{ for some } \sigma_0 \neq \text{id}. \tag{4.32}$$

- If such a $\sigma^\dagger$ does not exist. The covering (4.4) corresponds to one of the coverings (3.7), (3.8), (3.9) or (3.10) of Theorem 3.4. Since $\Lambda(\text{id})$ has index equal to 2 or 4, we can eliminate the covering (3.10) (because the lattices comprising this covering all have an index equal to 3). Now, in the coverings (3.7), (3.8) and (3.9), there are exactly two lattices with index 2. So (4.32) is also true in that case.

We now exploit the relation (2.6), with the choice $\tau = \sigma_0$, and the relation $[\mathbb{Z}^2 : L(\gamma)] = \nu/D$ by Comment 4 of 2.6 to obtain

$$\nu D^{-1} \leq 2,$$

which leads to the divisibility

$$\nu \mid 2D,$$

since νD^{-1} is an integer. This gives the condition (4.31).

We can further restrict the set of possible values for the pair (D, ν) as follows. By (4.3), we have $\Lambda(\sigma_0) = L(\gamma^{-1}\sigma_0)$, where σ_0 satisfies (4.32). But $|\det(\gamma^{-1}\sigma_0)| = \frac{\nu}{D^2}$. By Lemma 2.2, we deduce that 2 is a multiple of D^2/ν. This gives the inequality $D^2 \leq 2\nu$. So we know that the set defined in (4.31) is restricted to

$$(D, \nu) \in \{(2, 2), (2, 4), (4, 8)\}. \tag{4.33}$$

4.5 Possible values for d_2

We now investigate the possible values for d_2.

4.5.1 The integer d_2 has no odd prime divisor

We will prove that

$$d_2 \in \{1, 2, 4, 8, 16, \dots\}. \tag{4.34}$$

Suppose that d_2 is divisible by some odd prime p. We recall that $\nu \in \{2, 4, 8\}$ (see (4.33)) and we return to the definitions (4.6), (4.7) and (4.8) to deduce that the lattices $\Lambda(T_2^{-1}A_1T_2)$, $\Lambda(T_2^{-1}A_2T_2)$ and $\Lambda(T_2^{-1}A_3T_2)$ are respectively included in the following lattices

$$\mathcal{M}_{1,p} : \begin{cases} (t_1t_2 + t_3t_4)x_1 + (t_2^2 + t_4^2)x_2 \equiv 0 \bmod p, \\ (t_1^2 + t_3^2)x_1 + (t_1t_2 + t_3t_4)x_2 \equiv 0 \bmod p, \end{cases}$$

$$\mathcal{M}_{2,p} : \begin{cases} (t_3t_4 - t_1t_2)x_1 + (t_4^2 - t_2^2)x_2 \equiv 0 \bmod p, \\ (t_1^2 - t_3^2)x_1 + (t_1t_2 - t_3t_4)x_2 \equiv 0 \bmod p, \end{cases}$$

$$\mathcal{M}_{3,p} : \begin{cases} (t_2t_3 + t_1t_4)x_1 + (2t_2t_4)x_2 \equiv 0 \bmod p, \\ (2t_1t_3)x_1 + (t_2t_3 + t_1t_4)x_2 \equiv 0 \bmod p. \end{cases}$$

We use a combinatorial lemma dealing with the antidiagonal coefficients in the above system of equations.

Lemma 4.3. *Let p be an odd prime. Let $(t_1, t_2, t_3, t_4) \in \mathbb{Z}^4$ be such that $p \nmid \gcd(t_1, t_2, t_3, t_4)$. Consider the following three 2–sets of quadratic forms*

$$S_1 := \{t_2^2 + t_4^2, t_1^2 + t_3^2\}, \quad S_2 := \{t_4^2 - t_2^2, t_1^2 - t_3^2\}, \quad S_3 := \{2t_2t_4, 2t_1t_3\}.$$

Then for all pairs (i, j) with $1 \leq i < j \leq 3$, there exists $P \in S_i \cup S_j$ such that $p \nmid P$.

Proof. Omitted. $\qquad \square$

Lemma 4.3 implies that there exist i and j such that $\mathcal{M}_{i,p}$ and $\mathcal{M}_{j,p}$ have index divisible by p. Hence the indices of the corresponding lattices $\Lambda(T_2^{-1}A_iT_2) \subseteq \mathcal{M}_{i,p}$ and $\Lambda(T_2^{-1}A_jT_2) \subseteq \mathcal{M}_{j,p}$ are divisible by p. This is incompatible with the covering (4.4) and Theorem 3.4, since the index of $\Lambda(\mathrm{id})$ is 2 or 4. The proof of (4.34) is complete.

4.5.2 The case $d_2 = 1$ is impossible

Recall that $D \in \{2, 4\}$. By keeping only the first equation in the systems (4.5), (4.6), (4.7) and (4.8) and by replacing $d_2 D$ by 2, we deduce that the four lattices $\Lambda(\sigma)$ ($\sigma \in \mathfrak{S}$) are respectively included in the four lattices defined by the equations

$$\mathcal{L}_2(\mathrm{id}) : x_1 \equiv 0 \bmod 2,$$
$$\mathcal{L}_2(T_2^{-1} A_1 T_2) : (t_1 t_2 + t_3 t_4) x_1 + (t_2^2 + t_4^2) x_2 \equiv 0 \bmod 2,$$
$$\mathcal{L}_2(T_2^{-1} A_2 T_2) : (t_3 t_4 - t_1 t_2) x_1 + (t_4^2 - t_2^2) x_2 \equiv 0 \bmod 2,$$
$$\mathcal{L}_2(T_2^{-1} A_3 T_2) : (t_2 t_3 + t_1 t_4) x_1 \equiv 0 \bmod 2.$$

The assumption $d_2 = 1$ implies $t_1 t_4 + t_2 t_3 \equiv 1 \bmod 2$, from which we deduce the equality

$$\mathcal{L}_2(\mathrm{id}) = \mathcal{L}_2(T_2^{-1} A_3 T_2).$$

Considerations of parities also lead to the equality

$$\mathcal{L}_2(T_2^{-1} A_1 T_2) = \mathcal{L}_2(T_2^{-1} A_2 T_2).$$

Again playing with the parities of the t_i and using $1 = d_2 \equiv t_1 t_4 + t_2 t_3 \bmod 2$, we see that we never have $t_1 t_2 + t_3 t_4 \equiv t_2^2 + t_4^2 \equiv 0 \bmod 2$, which means that $\mathcal{L}_2(T_2^{-1} A_1 T_2) \neq \mathbb{Z}^2$. These considerations show that the covering (4.4) leads to the non-trivial covering

$$\mathbb{Z}^2 = \mathcal{L}_2(\mathrm{id}) \cup \mathcal{L}_2(T_2^{-1} A_1 T_2),$$

which is in contradiction with Theorem 3.4.

4.5.3 The case $d_2 = 2$ is impossible

The strategy is the same as in the section above, but more intricate since we will distinguish cases based on the parity of t_2 and t_4. We suppose that $d_2 = 2$ and we will arrive at a contradiction. Since $4 \mid d_2 D$, the four lattices $\Lambda(\sigma)$ ($\sigma \in \mathfrak{S}$) are respectively included in the four lattices defined by the equations

$$\mathcal{L}_2(\mathrm{id}) : x_1 \equiv 0 \bmod 2,$$
$$\mathcal{L}_4(T_2^{-1} A_1 T_2) : (t_1 t_2 + t_3 t_4) x_1 + (t_2^2 + t_4^2) x_2 \equiv 0 \bmod 4,$$
$$\mathcal{L}_4(T_2^{-1} A_2 T_2) : (t_3 t_4 - t_1 t_2) x_1 + (t_4^2 - t_2^2) x_2 \equiv 0 \bmod 4,$$
$$\mathcal{L}_4(T_2^{-1} A_3 T_2) : (t_2 t_3 + t_1 t_4) x_1 + (2 t_2 t_4) x_2 \equiv 0 \bmod 4.$$

Recall the equality $|t_1 t_4 - t_2 t_3| = d_2 = 2$.

4.5.3.1 If t_2 and t_4 have different parities

We then have the equalities

$$\gcd(t_2^2 + t_4^2, 4) = \gcd(t_4^2 - t_2^2, 4) = 1,$$

which implies

$$[\mathbb{Z}^2 : \mathcal{L}_4(T_2^{-1} A_1 T_2)] = [\mathbb{Z}^2 : \mathcal{L}_4(T_2^{-1} A_2 T_2)] = 4$$

by a direct study of the equations defining these lattices. Furthermore, the coefficient of x_1 in the equation defining $\mathcal{L}_4(T_2^{-1}A_3T_2)$ satisfies one of the following two relations

$$t_2t_3 + t_1t_4 = \begin{cases} d_2 + 2t_2t_3 \equiv 2 \bmod 4 \\ d_2 + 2t_1t_4 \equiv 2 \bmod 4. \end{cases} \tag{4.35}$$

This implies the equality between lattices

$$\mathcal{L}_2(\mathrm{id}) = \mathcal{L}_4(T_2^{-1}A_3T_2).$$

The covering (4.4) leads to the covering

$$\mathbb{Z}^2 = \mathcal{L}_2(\mathrm{id}) \cup \mathcal{L}_4(T_2^{-1}A_1T_2) \cup \mathcal{L}_4(T_2^{-1}A_2T_2),$$

which is nonsense, since the index of these three lattices are 2, 4 and 4 respectively. Therefore this covering does not correspond to a minimal covering in Theorem 3.4.

4.5.3.2   If t_2 and t_4 are both even

Under this assumption, we have the following similarities between the coefficients of the lattices $\mathcal{L}_4(T_2^{-1}A_1T_2)$ and $\mathcal{L}_4(T_2^{-1}A_2T_2)$ defined in §4.5.3:

$$t_2^2 + t_4^2 \equiv t_4^2 - t_2^2 \equiv 0 \bmod 4,$$

and

$$t_1t_2 + t_3t_4 \equiv t_3t_4 - t_1t_2 \equiv 0 \bmod 2.$$

We now discuss on the class $t_1t_2 + t_3t_4 \equiv t_3t_4 - t_1t_2 \bmod 4$.

4.5.3.2.1   If t_2 and t_4 are both even and if $t_1t_2 + t_3t_4 \equiv t_3t_4 - t_1t_2 \equiv 2 \bmod 4$.   We return to the definitions of the lattices to deduce the equalities between lattices

$$\mathcal{L}_2(\mathrm{id}) = \mathcal{L}_4(T_2^{-1}A_1T_2) = \mathcal{L}_4(T_2^{-1}A_2T_2),$$

which certainly can not lead to a covering.

4.5.3.2.2   If t_2 and t_4 are both even and if $t_1t_2 + t_3t_4 \equiv t_3t_4 - t_1t_2 \equiv 0 \bmod 4$.   In (4.35), we have already seen that

$$t_2t_3 + t_1t_4 \equiv 2 \bmod 4. \tag{4.36}$$

We split our discussion according to the value of D (see (4.33)).

$\diamond$ **Case 1: $D = 4$.** In that case, we have $\nu = 8$ and $d_2D = 8$, so the second equations of (4.6), (4.7) and (4.8) are automatically satisfied. We observe that

$$\Lambda(\mathrm{id}) = \{(x_1, x_2) : x_1 \equiv 0 \bmod 4\}.$$

By (4.36), we have the inclusion

$$\Lambda(T_2^{-1}A_3T_2) \subseteq \Lambda(\mathrm{id}).$$

The covering (4.4) is simplified to the covering

$$\mathbb{Z}^2 = \Lambda(\mathrm{id}) \cup \Lambda(T_2^{-1} A_1 T_2) \cup \Lambda(T_2^{-1} A_2 T_2),$$

where the first lattice has index 4 and where the last two lattices have an index ≥ 2. This covering with three lattices does not resonate with Theorem 3.4.

$\diamond$ **Case 2:** $D = 2$. We then have

$$d_2 = D = 2, \quad \nu \in \{2, 4\}, \quad t_2 \equiv t_4 \equiv 0 \bmod 2 \quad \text{and} \quad t_1 t_2 + t_3 t_4 \equiv 0 \bmod 4.$$

Actually, the case $\nu = 4$ can never happen. Indeed, by the formula given in Lemma 4.1, with the values $d_2 = D = 2$, $\nu = 4$ and the constraints of the congruence modulo 4 of the t_i, we see that $\Lambda(T_2^{-1} A_1 T_2) = \mathbb{Z}^2$. This is forbidden by Lemma 4.2.

So we restrict to $\nu = 2$. The equations of the lattices $\Lambda(\sigma)$ ($\sigma \in \mathfrak{S}$) given in Lemma 4.1 are equivalent to a single equation

$$\begin{cases} \Lambda(\mathrm{id}) & : x_1 \equiv 0 \bmod 2, \\ \Lambda(T_2^{-1} A_1 T_2) & : (t_1^2 + t_3^2) x_1 \equiv 0 \bmod 2, \\ \Lambda(T_2^{-1} A_2 T_2) & : (t_1^2 - t_3^2) x_1 \equiv 0 \bmod 2, \\ \Lambda(T_2^{-1} A_3 T_2) & : x_1 \equiv 0 \bmod 2. \end{cases}$$

Since $\Lambda(\sigma) \neq \mathbb{Z}^2$ by Lemma 4.2, this implies that the coefficients of x_1 in the second and the third equations are odd. We deduce that these four equations show the equality

$$\Lambda(\sigma) = \{(x_1, x_2) : x_1 \equiv 0 \bmod 2\} \text{ for all } \sigma \in \mathfrak{S}.$$

This contradicts the covering (4.4).

4.5.3.3 If t_2 and t_4 are both odd

The equality $t_1 t_4 - t_2 t_3 = \pm 2$ implies that t_1 and t_3 have the same parity. We now split the argument according to this parity.

4.5.3.3.1 If t_2 and t_4 are both odd and if $t_1 \equiv t_3 \equiv 0 \bmod 2$. Since $d_2 = 2$, these conditions imply that $(t_1, t_3) \equiv (0, 2)$ or $(2, 0)$ modulo 4. Therefore we have

$$t_1 t_2 + t_3 t_4 \equiv t_3 t_4 - t_1 t_2 \equiv t_2 t_3 + t_1 t_4 \equiv 2 \bmod 4.$$

We implement these congruences into the first equations of (4.6), (4.7) and (4.8) to deduce the inclusions

$$\Lambda(T_2^{-1} A_1 T_2), \Lambda(T_2^{-1} A_3 T_2) \subseteq \{(x_1, x_2) : x_1 + x_2 \equiv 0 \bmod 2\},$$

and

$$\Lambda(T_2^{-1} A_2 T_2) \subseteq \{(x_1, x_2) : x_1 \equiv 0 \bmod 2\}.$$

Recalling the inclusion

$$\Lambda(\mathrm{id}) \subseteq \{(x_1, x_2) : x_1 \equiv 0 \bmod 2\}, \tag{4.37}$$

and returning to the covering (4.4), we obtain a covering of $\mathbb{Z}^2$ by two lattices with index 2. This contradicts Theorem 3.4.

4.5.3.3.2 If t_2 and t_4 are both odd and if $t_1 \equiv t_3 \equiv 1 \bmod 2$. Since $d_2 = 2$, the following congruences hold

$$t_1 t_2 + t_3 t_4 \equiv t_2 t_3 + t_1 t_4 \equiv 0 \bmod 4 \quad \text{and} \quad t_3 t_4 - t_1 t_2 \equiv 2 \bmod 4.$$

We insert these congruences and the condition $4 \mid d_2 D$ into the first equations of the systems (4.6), (4.7) and (4.8) to obtain the inclusions

$$\Lambda(T_2^{-1} A_1 T_2), \Lambda(T_2^{-1} A_3 T_2) \subseteq \{(x_1, x_2) : x_2 \equiv 0 \bmod 2\},$$

and

$$\Lambda(T_2^{-1} A_2 T_2) \subseteq \{(x_1, x_2) : x_1 \equiv 0 \bmod 2\}.$$

These inclusions and the inclusion (4.37) contradict (4.4), since we would once more obtain a covering of $\mathbb{Z}^2$ by two lattices with index 2.

Gathering all these cases, we proved that $d_2 \neq 2$.

4.5.4 The case $4 \mid d_2$ is impossible

We will suppose that $4 \mid d_2$ to arrive at a contradiction. This implies that $8 \mid d_2 D$ thanks to (4.33). We divide our proof according to the parity of t_2 and t_4.

4.5.4.1 If t_2 and t_4 have different parities

In that case, we have $\gcd(t_2^2 \pm t_4^2, 8) = 1$ and the first equations of (4.6) and (4.7) give the divisibility

$$8 \mid [\mathbb{Z}^2 : \Lambda(T_2^{-1} A_i T_2)] \quad \text{for } i \in \{1, 2\}.$$

The covering (4.4) can not hold: we would obtain a covering with four proper lattices, with at least two with index divisible by 8. This does not exist by Theorem 3.4.

4.5.4.2 If t_2 and t_4 have the same parity

Our first step is to show that we necessarily have

$$t_1 \equiv t_3 \bmod 2. \tag{4.38}$$

Suppose that this does not hold. We always have

$$t_1^2 + t_3^2 \equiv t_1^2 - t_3^2 \bmod 2.$$

We argue as follows:

• If $t_1 \not\equiv t_3 \bmod 2$ and $t_2 \equiv t_4 \equiv 0 \bmod 2$. By (4.33), we know that $2 \mid d_2 D / \nu$. By the first equation of (4.5) and the second equation of (4.6) and (4.7), we deduce the inclusions

$$\Lambda(\sigma) \subseteq \{(x_1, x_2) : x_1 \equiv 0 \bmod 2\} \text{ for } \sigma \in \mathfrak{S} - \{T_2^{-1} A_3 T_2\}.$$

By (4.4), we would obtain a covering by two proper lattices, and this contradicts Theorem 3.4.

• If $t_1 \not\equiv t_3 \bmod 2$ and $t_2 \equiv t_4 \equiv 1 \bmod 2$. We only study the first equations of (4.6), (4.7) and (4.8). We use the congruences

$$t_1 t_2 + t_3 t_4 \equiv t_3 t_4 - t_1 t_2 \equiv t_2 t_3 + t_1 t_4 \equiv 1 \bmod 2 \quad \text{and} \quad 8 \mid d_2 D$$

to deduce that
$$8 \mid [\mathbb{Z}^2 : \Lambda(T_2^{-1} A_i T_2)] \quad \text{for } 1 \leq i \leq 3.$$

The covering (4.4) then would be incompatible with Theorem 3.4. So (4.38) is proved.

To summarize, we necessarily have the congruence conditions

$$t_2 \equiv t_4 \bmod 2 \text{ and } t_1 \equiv t_3 \bmod 2.$$

Recall that the t_i are coprime altogether, so modulo 2, the quadruplet (t_1, t_2, t_3, t_4) belongs to the following set Ω with three elements

$$\Omega := \{(1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1)\}.$$

These possibilities will be the basis of our discussion below.

4.5.4.2.1   If $(t_1, t_2, t_3, t_4) \equiv (0, 1, 0, 1)$ or $(1, 1, 1, 1)$ mod 2.   We then have the congruences $t_2^2 + t_4^2 \equiv 2 \bmod 8$ and $2t_2 t_4 \equiv \pm 2 \bmod 8$. By considering the first equations in the systems (4.6) and (4.8), we obtain the inequality

$$v_2([\mathbb{Z}^2 : \Lambda(T_2^{-1} A_i T_2)]) \geq 2 \text{ for } i \in \{1, 3\}.$$

Furthermore, for this to be an equality, we must have $d_2 D = 8$, which means $d_2 = 4$ and $D = 2$.

When $(D, d_2) \neq (2, 4)$ (which is equivalent to $16 \mid d_2 D$), the lattices $\Lambda(T_2^{-1} A_i T_2)$ for $i \in \{1, 3\}$ have index divisible by 8. The covering (4.4) is therefore impossible thanks to Theorem 3.4.

When $(D, d_2) = (2, 4)$, the congruences

$$\pm d_2 = t_1 t_4 - t_2 t_3 \equiv 4 \bmod 8,$$

and $t_2 \equiv t_4 \equiv 1 \bmod 2$ imply

$$4 \equiv t_1 t_4 - t_2 t_3 \equiv t_2 t_4 (t_1 t_4 - t_2 t_3) \equiv t_1 t_2 - t_3 t_4 \bmod 8.$$

Since we also have $t_4^2 - t_2^2 \equiv 0 \bmod 8$, we conclude that

$$\Lambda(T_2^{-1} A_2 T_2) \subseteq \{(x_1, x_2) : x_1 \equiv 0 \bmod 2\}$$

by (4.7) and by Lemma 2.3. Since $\Lambda(\mathrm{id})$ satisfies the same inclusion (see (4.37)) we obtain a contradiction with (4.4), since we would obtain a covering of $\mathbb{Z}^2$ by three lattices with index 2, 4 and 4.

4.5.4.2.2   If $(t_1, t_2, t_3, t_4) \equiv (1, 0, 1, 0)$ mod 2.   This case is more delicate. We handle this case by splitting the proof in three cases.

⋄ **Case 1: $v_2(t_2) \neq v_2(t_4)$ (≥ 1).** We have the sequence of relations

$$2 \leq v_2(d_2) = \min(v_2(t_2), v_2(t_4)) = v_2(t_1 t_2 + t_3 t_4) = v_2(t_3 t_4 - t_1 t_2) = v_2(t_2 t_3 + t_1 t_4),$$

and the inequalities (recall that $D \in \{2, 4\}$)

$$2 \min(v_2(t_2), v_2(t_4)) = v_2(t_2^2 + t_4^2) = v_2(t_4^2 - t_2^2) \geq v_2(d_2 D) \text{ and } v_2(2t_2 t_4) \geq v_2(d_2 D).$$

With these remarks, we consider the first equations of the systems (4.5), (4.6), (4.7) and (4.8) to deduce the inclusions

$$\Lambda(\sigma) \subseteq \{(x_1, x_2) : x_1 \equiv 0 \bmod 2\} \text{ for all } \sigma \in \mathfrak{S}.$$

These relations obviously contradict the covering (4.4).

Now we suppose that $v_2(t_2) = v_2(t_4) \ (\geq 1)$. Since, by hypothesis, the integers t_1 and t_3 are both odd, we have $v_2(d_2) > v_2(t_2) = v_2(t_4)$. So we split our forthcoming discussion according to the difference between $v_2(d_2)$ and $v_2(t_2) = v_2(t_4)$.

$\diamond$ **Case 2: $v_2(t_2) = v_2(t_4) \geq 1$ and $v_2(d_2) = v_2(t_2) + 1$.** Under these hypotheses, we have

$$v_2(t_1 t_2 + t_3 t_4) > v_2(d_2) \text{ and } v_2(t_2^2 + t_4^2) > v_2(d_2). \tag{4.39}$$

For the first equality of (4.39), we use that

$$t_1 t_2 + t_3 t_4 \equiv t_1 t_4 + t_2 t_3 \equiv \pm d_2 + 2 t_2 t_3 \equiv 0 \bmod 2 d_2.$$

For the second equation, we use the equality $v_2(t_2^2 + t_4^2) = 1 + 2 v_2(t_2)$. By (4.33), we have three possibilities

$$(d_2, D, \nu) = (4, 2, 4), \quad v_2(d_2 D/\nu) > 1 \quad \text{or} \quad D = 4. \tag{4.40}$$

$\bullet$ The first possibility is impossible because, with the above values of d_2, D and ν and with the conditions on the 2-adic valuations of the t_i, the two equations defining $\Lambda(T_2^{-1} A_1 T_2)$ (see (4.6)) are congruences modulo 8, and all the coefficients of x_1 and x_2 are $\equiv 0 \bmod 8$. So we would have $\Lambda(T_2^{-1} A_1 T_2) = \mathbb{Z}^2$, which is contrary to Lemma 4.2.

$\bullet$ The second possibility of (4.40) can not hold for the following reason: consider the second equations of the systems (4.6) and (4.8). We benefit from the congruences

$$t_1^2 + t_3^2 \equiv 2 t_1 t_3 \equiv 2 \bmod 4$$

to deduce the two inclusions

$$\Lambda(T_2^{-1} A_i T_2) \subseteq \{(x_1, x_2) : x_1 \equiv 0 \bmod 2\} \quad \text{for } i \in \{1, 3\}.$$

Since the same inclusion holds for $\Lambda(\mathrm{id})$ and since $\Lambda(T_2^{-1} A_2 T_2) \neq \mathbb{Z}^2$, the covering (4.4) is impossible by Theorem 3.4.

$\bullet$ We now prove that the third possibility of (4.40) can not hold. Indeed, suppose that $D = 4$ and, as usual, let $g := \gcd(t_2, t_4), \tilde{t}_2 := t_2/g$ and $\tilde{t}_4 := t_4/g$. Since $g \mid d_2$, g is necessarily a power of 2 and we have $v_2(g) = v_2(t_2) = v_2(t_4) = v_2(d_2) - 1 \ (\geq 1)$ and the integers $\tilde{t}_2$ and $\tilde{t}_4$ are odd. We then have

$$2 \equiv t_1 \tilde{t}_4 - \tilde{t}_2 t_3 \equiv (t_1 t_3)(t_1 \tilde{t}_4 - \tilde{t}_2 t_3) \equiv t_3 \tilde{t}_4 - t_1 \tilde{t}_2 \bmod 4,$$

and therefore

$$v_2(t_3 t_4 - t_1 t_2) = v_2(d_2). \tag{4.41}$$

Since $v_2(t_2) \geq 1$, it follows that

$$t_4^2 - t_2^2 \equiv 0 \bmod d_2 D. \tag{4.42}$$

To prove (4.42), write $t_2 = 2^t a_2$, $t_4 = 2^t a_4$ with odd a_2 and a_4 and $t \geq 1$. Then $t_4^2 - t_2^2 = 2^{2t}(a_4^2 - a_2^2) \equiv 0 \bmod 2^{2t+2}$. Furthermore, $d_2 D = 2^{t+1} \cdot 4 = 2^{t+3}$. We obtain the desired congruence (4.42), since $2t + 2 \geq t + 3$ for $t \geq 1$.

By the first equations of (4.5) and (4.7), by (4.41) and (4.42) and by the hypothesis $D = 4$, we obtain the inclusions

$$\Lambda(\mathrm{id}), \ \Lambda(T_2^{-1} A_2 T_2) \subseteq \{(x_1, x_2) : x_1 \equiv 0 \bmod 4\}.$$

These inclusions are not compatible with the covering (4.4), since we would obtain a covering of $\mathbb{Z}^2$ by three lattices containing one lattice with index 4 (see Theorem 3.4). Hence the case $D = 4$ does not happen.

◇ **Case 3:** $v_2(t_2) = v_2(t_4) \geq 1$ **and** $v_2(d_2) > v_2(t_2) + 1$. We will first prove the two equalities

$$v_2(t_1 t_2 + t_3 t_4) = v_2(t_2) + 1 \quad \text{and} \quad v_2(t_2 t_3 + t_1 t_4) = v_2(t_2) + 1. \tag{4.43}$$

• To prove the first equality, we write

$$v_2(t_1 t_2 + t_3 t_4) = v_2(t_1 t_2 t_3 + t_3^2 t_4) = v_2(t_1(t_1 t_4 \pm d_2) + t_3^2 t_4) = v_2((t_1^2 + t_3^2) t_4 \pm t_1 d_2).$$

We now observe that

$$v_2(\pm t_1 d_2) = v_2(d_2)$$

and

$$v_2((t_1^2 + t_3^2) t_4) = v_2(t_1^2 + t_3^2) + v_2(t_4) = v_2(t_2) + 1,$$

because t_1 and t_3 are both odd. Therefore we conclude that

$$v_2(t_1 t_2 + t_3 t_4) = v_2((t_1^2 + t_3^2) t_4 \pm t_1 d_2) = v_2(t_2) + 1,$$

since $v_2(t_2) + 1 < v_2(d_2)$ by assumption.
• To prove the second equality of (4.43), we write

$$v_2(t_2 t_3 + t_1 t_4) = v_2(2 t_2 t_3 + t_1 t_4 - t_2 t_3) = v_2(2 t_2 t_3 \pm d_2) = v_2(2 t_2 t_3) = v_2(2 t_2) = v_2(t_2) + 1.$$

The proof of (4.43) is complete.

We now use (4.43) to deduce from the first equations of (4.6) and (4.8) the two inclusions

$$\Lambda(T_2^{-1} A_i T_2) \subseteq \{(x_1, x_2) : x_1 \equiv 0 \bmod 2\} \quad \text{for } i \in \{1, 3\}. \tag{4.44}$$

• Proof of (4.44) for $i = 1$. The coefficient of x_1 in the first equation of (4.6) satisfies $v_2(t_1 t_2 + t_3 t_4) = v_2(t_2) + 1 < v_2(d_2) < v_2(d_2 D)$. Furthermore, the coefficient of x_2 satisfies $v_2(t_2^2 + t_4^2) = 1 + 2 v_2(t_2) > v_2(t_2) + 1 = v_2(t_1 t_2 + t_3 t_4)$. Lemma 2.3 gives the inclusion (4.44) when $i = 1$.

• Proof of (4.44) for $i = 3$. The coefficient of x_1 in the first equation of (4.8) satisfies $v_2(t_2 t_3 + t_1 t_4) = v_2(t_2) + 1 < v_2(d_2) < v_2(d_2 D)$. Furthermore, the coefficient of x_2 satisfies $v_2(2 t_2 t_4) = 2 v_2(t_2) + 1 > v_2(t_2) + 1 = v_2(t_2 t_3 + t_1 t_4)$. Lemma 2.3 gives the inclusion (4.44) when $i = 3$.

The proof of (4.44) is complete. Combining the inclusions (4.44) with the inclusion $\Lambda(\mathrm{id}) \subseteq \{(x_1, x_2) : x_1 \equiv 0 \bmod 2\}$ and with the covering (4.4), we arrive at a covering of $\mathbb{Z}^2$ by two proper lattices, which does not exist by Theorem 3.4.

We investigated all the cases to assert that $4 \nmid d_2$. Gathering the properties of d_2 proved in §4.5.1, §4.5.2, §4.5.3 and §4.5.4, we see that d_2 does not exist.

The proof of Theorem 1.2 is complete.

References

[1] É. Fouvry and P. Koymans, *Binary forms with the same value set I.* Preprint.

[2] É. Fouvry and P. Koymans, *Binary forms with the same value set III. The case of* $\mathbf{D}_3$ *and* $\mathbf{D}_6$. Preprint.

[3] C. L. Stewart and S. Y. Xiao, *On the representation of integers by binary forms.* Math. Ann. **375** (2019), no. 1–2, 133–163.