Non-congruence of homology Veech groups in genus two

Christian Weiß*

February 3, 2013

Abstract

We study the action of the Veech group of square-tiled surfaces of genus two on homology. This action defines the homology Veech group which is a subgroup of $\mathrm{SL}_2(\mathcal{O}_D)$ where $\mathcal{O}_D$ is a quadratic order of square discriminant. Extending a result of Weitze-Schmithüsen we show that also the homology Veech group is a totally non-congruence subgroup with exceptions stemming only from the prime ideals lying above 2. While Weitze-Schmithüsen's result for Veech groups is asymmetric with respect to the spin structure our use of the homology Veech group yields a completely symmetric picture.

Contents

1 Introduction **1**

2 The Special Linear Group over square quadratic orders **5**

3 Teichmüller curves **12**

4 Proof of the main result **18**

A Appendix **26**

1 Introduction

Veech groups of square-tiled surfaces are an interesting class of subgroups of $\mathrm{SL}_2(\mathbb{Z})$. Ellenberg and McReynolds showed in [ER12] that with some minor restrictions all subgroups of $\mathrm{SL}_2(\mathbb{Z})$ appear as a Veech group if the genus of the square-tiled surface is allowed to be large. However, for genus two square-tiled surfaces Weitze-Schmithüsen proved in [WS12] that these Veech groups

*The author is partially supported by the ERC-StG 257137.

are very far away from being congruence subgroups. In fact, the Veech group of a genus two square-tiled surface has two representations in $\mathrm{SL}_2(\mathbb{Z})$ given by its action on homology. These two representations yield a pair of matrices $(A_1, A_2) \in \mathrm{SL}_2(\mathcal{O}_D)$ where $\mathcal{O}_D$ is a quadratic order of square discriminant (see Section 2). The image of this representation is called homology Veech group. In this paper we generalize Weitze-Schmithüsen's result by showing that also the homology Veech group is very far away from being a congruence subgroup.

For our result Weitze-Schmithüsen's approach of using different prototypes in the sense of [Bai07] or [McM05] at the same time seems to be of limited use since the conjugation on the complementary part of homology (see Section 3) is unknown. Moreover her idea of using the Wohlfahrt level may not be easily carried over to subgroups of $\mathrm{SL}_2(\mathcal{O}_D)$ since it is not evident how to generalize the Wohlfahrt level to this case. Indeed our additional ingredients are therefore that we explicitly find coset representatives like in [Wei12] and use Nori's Theorem, which states that the number of elements of a subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ generated by parabolic elements is limited to only three possibilities (Corollary 2.12). Our arguments work step by step as we do consider congruence subgroups of decreasing level.

While Weitze-Schmithüsen takes into account principal congruence subgroups we look at Hecke congruence subgroups instead. Nori's Theorem [Nor87, Theorem 5.1] implies that the assertion for principal congruence subgroups follows from the case of Hecke congruence subgroups at least for all prime ideals. So on the level of Veech groups the two statements are almost equivalent and considering Hecke congruence subgroups is not a great restriction. Furthermore Weitze-Schmithüsen's theorem is asymmetric with respect to the spin structure of the square-tiled surfaces but our approach of using the homology Veech group symmetrizes the result.

Let us now make more precise what we mean by "being very far away from being a congruence subgroup": let $\mathcal{O}$ be either $\mathbb{Z}$ or more generally a quadratic order $\mathcal{O}_D$. Then a finite index subgroup of $\mathrm{SL}_2(\mathcal{O})$ is called a **congruence subgroup** if it contains a principal congruence subgroup $\Gamma(\mathfrak{a})$ (see Section 2). A finite index subgroup Γ of $\mathrm{SL}_2(\mathcal{O})$ is a congruence subgroup if and only if there exists an ideal $\mathfrak{a} \subset \mathcal{O}$ such that the **level index** $[\mathrm{SL}_2(\mathcal{O}/\mathfrak{a}) : \rho_\mathfrak{a}(\Gamma)]$ equals the index $[\mathrm{SL}_2(\mathcal{O}) : \Gamma]$ where $\rho_\mathfrak{a} : \mathrm{SL}_2(\mathcal{O}) \to \mathrm{SL}_2(\mathcal{O}/\mathfrak{a})$ is the natural projection. The group Γ is thus called a **non-congruence subgroup of level** $\mathfrak{a}$ if the two indices differ and Γ is called a **totally non-congruence subgroup of level** $\mathfrak{a}$ if $[\mathrm{SL}_2(\mathcal{O}/\mathfrak{a}) : \rho_\mathfrak{a}(\Gamma)] = 1$. Being a totally non-congruence subgroup of level $\mathfrak{a}$ is equivalent to the index $[\Gamma : \Gamma \cap \Gamma(\mathfrak{a})]$ being equal to the index $[\mathrm{SL}_2(\mathcal{O}) : \Gamma(\mathfrak{a})]$.

Weitze-Schmithüsen proved in [WS12] the following theorem on Veech groups of square-tiled surfaces in $\Omega\mathcal{M}_2(2)$:

Theorem 1.1. ***(Weitze-Schmithüsen, [WS12, Theorem 3])*** *Let L_d be a square-tiled surface in $\Omega\mathcal{M}_2(2)$ with d squares and let $\mathrm{SL}(L_d)$ be its Veech group. We distinguish the two different cases that L_d is in the orbit $\mathcal{A}_d$ and $\mathcal{B}_d$ in the classification of square-tiled surfaces in $\Omega\mathcal{M}_2(2)$ (Theorem 3.6).*

(1A) If d is even or d is odd and L_d is in $\mathcal{A}_d$, or $d = 3$, then we have $[\mathrm{SL}(L_d) : \mathrm{SL}(L_d) \cap \Gamma(n)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(n)]$ for all odd $n \in \mathbb{N}$.

(1B) If d is even or d is odd and L_d is in $\mathcal{A}_d$, or $d = 3$, then we have $[\mathrm{SL}(L_d) : \mathrm{SL}(L_d) \cap \Gamma(n)] = \frac{1}{3}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(n)]$ for all even $n \in \mathbb{N}$.

(2) If d is odd, $d \geq 5$ and L_d is in $\mathcal{B}_d$ then $\mathrm{SL}(L_d)$ is a totally non-congruence subgroup, i.e. $[\mathrm{SL}(L_d) : \mathrm{SL}(L_d) \cap \Gamma(n)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(n)]$ for all $n \in \mathbb{N}$.

Note that the theorem is asymmetric with respect to the spin structure. If one introduces the Hecke congruence subgroups $\Gamma_0(n)$ where only the lower left entry of the matrices has to be equal to $0 \mod n$, then the theorem implies:

Corollary 1.2. *Let L_d be a square-tiled surface in $\Omega\mathcal{M}_2(2)$ with d squares and let $\mathrm{SL}(L_d)$ be its Veech group.*

(1A) If d is even, or d is odd and L_d is in $\mathcal{A}_d$, or $d = 3$, then we have $[\mathrm{SL}(L_d) : \mathrm{SL}(L_d) \cap \Gamma_0(n)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n)]$ for all odd $n \in \mathbb{N}$.

(1B) If d is even, or d is odd and L_d is in $\mathcal{A}_d$, or $d = 3$, then we have $[\mathrm{SL}(L_d) : \mathrm{SL}(L_d) \cap \Gamma_0(n)] = \frac{2}{3}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n)]$ for all even $n \in \mathbb{N}$.

(2) If d is odd, $d \geq 5$ and L_d is in $\mathcal{B}_d$ then $[\mathrm{SL}(L_d) : \mathrm{SL}(L_d) \cap \Gamma_0(n)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(n)]$ for all $n \in \mathbb{N}$.

Conversely, Nori's Theorem [Nor87, Theorem 5.1] yields that the assertion of the theorem also follows from the corollary for all prime numbers $p \in \mathbb{N}$.

In this paper, we generalize Weitze-Schmithüsen's Theorem in the following setting: a square-tiled surface $\pi_1 : X \to E_1$ with $g(X) = 2$ and consisting of d unit squares is called **minimal** if it does not factor via an isogeny. For a minimal square-tiled surface there exists a covering $\pi_2 : X \to E_2$ of the same degree such that the induced morphism $\mathrm{Jac}(X) \to E_1 \times E_2$ is an isogeny (of degree d^2). We call E_2 the **complementary elliptic curve** (see Section 3, [BL04] or [Kan03] for details). This means that $H_1(X, \mathbb{Z})$ contains $\Lambda := H_1(E_1, \mathbb{Z}) \oplus H_1(E_2, \mathbb{Z})$ as a sublattice of index d^2 and that the symplectic pairing on $H_1(X, \mathbb{Z})$ respects this decomposition. The action of the

Veech group on X induces an action on homology and thus an action on Λ. For a given matrix A in the Veech group the induced action on Λ is given by a pair of matrices $\widetilde{A} := (A_1 = A, RA_2R^{-1})$ where A_i acts on $H_1(E_i, \mathbb{Z})$ and $R = \mathrm{diag}(-1, 1)$ (for details see Section 3). More precisely, $\widetilde{A}$ is a matrix in $\mathrm{SL}_2(\mathcal{O}_{d^2})$ where $\mathcal{O}_{d^2}$ is the quadratic order of discriminant d^2. We call the corresponding subgroup of $\mathrm{SL}_2(\mathcal{O}_{d^2})$ the **homology Veech group**.

In particular, the homology Veech group is a subgroup of a Lie group of rank 2 while the Veech group is only a subgroup of a Lie group of rank 1. However, the homology Veech group is a subgroup of $\mathrm{SL}_2(\mathcal{O}_{d^2})$ of infinite index. Note that the notion of being a totally non-congruence subgroup of level $\mathfrak{a}$ still makes sense in this situation if one defines this property via $[\Gamma : \Gamma \cap \Gamma(\mathfrak{a})] = [\mathrm{SL}_2(\mathcal{O}) : \Gamma(\mathfrak{a})]$.

Given those cases where Weitze-Schmithüsen's result implies total non-congruence it is the most interesting case to analyze primes where this fails for the homology Veech group. The asymmetry with respect to the spin structure which appeared in the theorem of Weitze-Schmithüsen then vanishes. The topological reason for this is that the number of integral Weierstraß points is well-defined not only for the square-tiled covering map but also for the complementary covering as we will prove:

Theorem 3.9. *Let $\pi_1 : L_d \to E_1$ be a square-tiled surface in $\Omega\mathcal{M}_2(2)$ and let E_2 denote the complementary elliptic curve. If $\pi_1 : L_d \to E_1$ has even spin, then $\pi_2 : L_d \to E_2$ has odd spin. If $\pi_1 : L_d \to E_1$ has odd spin, then $\pi_2 : L_d \to E_2$ has even spin.*

This result allows us to preserve the main properties of Weitze-Schmithüsen's theorem but to solve its strange asymmetry with respect to the spin structure.

Theorem 4.1. *Let L_d be a square-tiled surface in $\Omega\mathcal{M}_2(2)$ with d squares and let $\mathrm{SL}^1(L_d)$ be its homology Veech group. We distinguish the two different cases that L_d is in the orbit $\mathcal{A}_d$ and $\mathcal{B}_d$ in the classification of square-tiled surfaces in $\Omega\mathcal{M}_2(2)$. Moreover if d is odd let $2 = \mathfrak{p}_2\mathfrak{p}_2^\sigma$ be the decomposition of 2 into prime ideals, where $\mathfrak{p}_2$ is the distinguished common prime ideal divisor of 2 and $(2, 2-d)$ in $\mathcal{O}_D$.*

(1A) If d is odd and L_d is in $\mathcal{A}_d$, or $d = 3$, then $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = [\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ for all ideals $\mathfrak{a} \subset \mathcal{O}_{d^2}$ with $(\mathfrak{p}_2, \mathfrak{a}) = 1$.

(1B) If d is odd and L_d is in $\mathcal{A}_d$, or $d = 3$, then $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = \frac{2}{3}[\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ for all ideals with $\mathfrak{p}_2 | \mathfrak{a}$.

(2A) If d is odd and L_d is in $\mathcal{B}_d$, then we have $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = [\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ for all ideals $\mathfrak{a} \subset \mathcal{O}_{d^2}$ with $(\mathfrak{p}_2^\sigma, \mathfrak{a}) = 1$.

(2B) If d is odd and L_d is in $\mathcal{B}_d$, then we have $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = \frac{2}{3}[\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ *for all ideals with* $\mathfrak{p}_2^{\sigma}|\mathfrak{a}$.

(3A) If d is even, then $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = [\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ *for all ideals* $\mathfrak{a} \subset \mathcal{O}_{d^2}$ *with* $2 \nmid \mathcal{N}(\mathfrak{a})$ *(the norm of* $\mathfrak{a}$*).*

(3B) If d is even, then $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = \frac{2}{3}[\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ *for all ideals with* $2|\mathcal{N}(\mathfrak{a})$,

For primitive Teichmüller curves in $\Omega\mathcal{M}_2(2)$, i.e. those not stemming from square-tiled surfaces, and fundamental discriminants, a theorem which exactly corresponds to Theorem 4.1 was proven in [Wei12, Theorem 5.1]. Therefore this paper almost completes the picture for $\Omega\mathcal{M}_2(2)$ and Γ_0. Then Nori's theorem also almost closes the gap to principal congruence subgroups. To get a complete picture one only has to perform a similar analysis for those Teichmüller curves whose discriminants are neither square nor fundamental.

Acknowledgement. I am very grateful to Martin Möller for his constant support of my work on this paper and for many very fruitful discussions. Moreover I would like to thank André Kappes for showing me how to practically calculate elements of the homology Veech group and my office mate Quentin Gendron for always being willing to discuss my mathematical problems.

2 The Special Linear Group over square quadratic orders

In this section we introduce quadratic orders $\mathcal{O}_D$. We will almost exclusively deal here with the case of square discriminants. In particular, we will calculate Spec $\mathcal{O}_D$ (Proposition A.12) and discuss the ramification of prime numbers $p \in \mathbb{N}$ over $\mathcal{O}_D$. As most things here work exactly like in the case of fundamental discriminants we postpone most of the proofs to the appendix. Afterwards we will focus on the special linear group, define congruence subgroups and calculate some important indexes.

Quadratic orders. Recall that any quadratic order is isomorphic to one of the form

$$\mathcal{O}_D = \mathbb{Z}[T]/(T^2 + bT + c),$$

where $b, c \in \mathbb{Z}$ and $b^2 - 4c = D$ and the isomorphism class does only depend on the **discriminant** D (see e.g. [Bai07, Chapter 2.2]). For every $D \equiv 0, 1 \mod 4$ there hence exists a unique quadratic order. In this paper we will only be concerned about the case where $D = d^2$ is a square. To the best of our knowledge, there does not seem to be any good reference, where these special quadratic orders are treated in detail. Therefore we want to collect some elementary facts and to explain similarities and differences to the non-square case.

Square discriminants. Let us describe the structure of the quadratic order. As $D = d^2$ is a square we have that

$$\mathcal{O}_D = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \mod d\}.$$

The quadratic order is hence a subring of $K = \mathbb{Q} \oplus \mathbb{Q}$, where addition and multiplication are defined componentwise. The algebra K may be interpreted as a substitute for the quadratic number field $\mathbb{Q}(\sqrt{D})$ where $\mathcal{O}_D$ is contained in for non-square D (this is also the reason for our notation). Furthermore we can regard $\mathbb{Q}\oplus\mathbb{Q}$ as an extension of $\mathbb{Q}$ by the diagonal map $\mathbb{Q} \to \mathbb{Q}\oplus\mathbb{Q}$. This makes perfectly sense since $\mathbb{Z}$ is then embedded into $\mathcal{O}_D$ by this construction. The Galois automorphism of $\mathbb{Q} \oplus \mathbb{Q}$ is given by

$$(x,y) \mapsto (x,y)^\sigma := (y,x).$$

Norm and trace. We can use this to define norm and trace on $\mathcal{O}_D$ and $\mathbb{Q} \oplus \mathbb{Q}$ respectively in the following way:

$$\mathcal{N}((x,y)) := (x,y)(x,y)^\sigma,$$

$$\mathrm{tr}((x,y)) := (x,y) + (x,y)^\sigma.$$

We call $\mathbb{1} := (1,1)$ and $w := (0,d)$ the *standard basis* of $\mathcal{O}_D$ as they indeed generate $\mathcal{O}_D$ as a $\mathbb{Z}-$module (see Appendix A for a proof). We hence have:

Proposition 2.1. *The quadratic order $\mathcal{O}_D$ is Noetherian.*

Ideals. Of course, one may define ideals in $\mathcal{O}_D$, prime ideals, maximal ideals and so on in the usual way. It follows from Proposition 2.1 and Krull's Hauptidealsatz that every prime ideal in $\mathcal{O}_D$ is also maximal (see e.g. [Har77, Theorem 1.11A]). For an element $z \in \mathcal{O}_D$ we define the **principal ideal** generated by z by:

$$(z) := z\mathcal{O}_D := \{za | a \in \mathcal{O}_D\}.$$

Now let $(0) \neq \mathfrak{a} \subset \mathcal{O}_D$ be an arbitrary ideal in $\mathcal{O}_D$. Then its norm $\mathcal{N}(\mathfrak{a})$ is defined as the number of the elements in $\mathcal{O}_D/\mathfrak{a}$ if this quotient is finite. If the quotient is infinite we set $\mathcal{N}(\mathfrak{a}) := 0$. In particular, if $z \in \mathcal{O}_D$ is a zero divisor, then we have $\mathcal{N}((z)) = 0$. The definition perfectly generalizes the norm of an element as $\mathcal{N}((z)) = \mathcal{N}(z)$ holds for all $z \in \mathcal{O}_D$ (see Lemma A.5).

Ideals as modules. When we want to calculate Spec $\mathcal{O}_D$ it turns out to be very useful to consider ideals as $\mathbb{Z}-$modules. As in the case of non-square discriminants, it is essential to see that every $\mathbb{Z}-$module in $\mathcal{O}_D$ is generated by at most two elements.

Proposition 2.2. *Let $M \subset \mathcal{O}_D$ be a $\mathbb{Z}$-module in $\mathcal{O}_D$. Then there exist integers $m, n \in \mathbb{Z}_{\geq 0}$ and $a \in \mathbb{Z}$ such that*

$$M = [n\mathbb{1}; a\mathbb{1} + mw] := n\mathbb{1}\mathbb{Z} \oplus (a\mathbb{1} + mw)\mathbb{Z}.$$

Proof. See Proposition A.9 □

As it does simplify the notation and cannot cause any confusion we will from now on leave away the symbol $\mathbb{1}$ when we want to embed $\mathbb{Z}$ into $\mathcal{O}_D$. In other words, we write every $\mathbb{Z}$-module in $\mathcal{O}_D$ as $[n; a + mw]$ for some $a, n, m \in \mathbb{Z}$.

Since every ideal of $\mathcal{O}_D$ is also $\mathbb{Z}$-module, it is generated by at most two elements. The converse is not true since e.g. $M = [1; 0] = \mathbb{Z}$ is a $\mathbb{Z}$-submodule of $\mathcal{O}_D$, but not an ideal.

Proposition 2.3. *A nonzero $\mathbb{Z}$-module $M = [n; a + mw]$ is an ideal if and only if $m|n$, $m|a$, i.e. $a = mb$ for some $b \in \mathbb{Z}$, and $n|m\mathcal{N}(b + w)$.*

These conditions are just the same as in the case of non-square discriminants. From these one immediately gets (both facts are proven in the appendix).

Corollary 2.4. *Every ideal of prime norm p is of the form $[p; a + w]$ for some $a \in \mathbb{Z}$ with $p|\mathcal{N}(a + w)$. These ideals are indeed prime ideals.*

This corollary implies that there does not exist any inert prime number if D is a square because it is always possible to find an $a \in \mathbb{Z}$ such that $p|\mathcal{N}(a + w)$, i.e. $a = p$.

Proposition 2.5. *Let $\mathcal{O}_D$ be a quadratic order of square discriminant. Then*

$$\begin{aligned} \textit{Spec } \mathcal{O}_D &= \{[p; p + w],\ [p; p - d + w] \mid p \in \mathbb{Z} \textit{ prime with } p \nmid D\} \\ &\cup \{[p; p + w] \mid p \in \mathbb{Z} \textit{ prime with } p|D\}. \end{aligned}$$

Proof. See Proposition A.12. □

We are thus able to count the number of different prime ideals of a given norm p if p is a prime number. This is also an important step towards the ramification theory of prime numbers $p \in \mathbb{Z}$ over $\mathcal{O}_D$. Note, that for $p|D$ we have $(p) \neq [p; w]^2$ since p itself is not contained in the right-hand side.

Ramification. We may now deduce the ramification theory for prime numbers over $\mathcal{O}_D$ (a detailed proof is given in the appendix).

Theorem 2.6. *Let $p \in \mathbb{Z}$ be a prime number.*

(i) If $p \nmid d$ then $(p) = \mathfrak{a}\mathfrak{a}^\sigma$ for a prime ideal $\mathfrak{a}$ of norm p, i.e. p splits.

(ii) If $p|d$ then (p) is an irreducible ideal which is not prime.

Corollary 2.7. *Let $z \in \mathcal{O}_D$ be an arbitrary element with $(d, \mathcal{N}(z)) = 1$. Then the principal ideal (z) can be uniquely written as a product of prime ideals.*

Let us say a few words about ideals generated by elements $z \in \mathcal{O}_D$ with $(d, \mathcal{N}(z)) \neq 1$. One might have $z \in \mathbb{Z}$ with $z|d$. Then one can uniquely write z as a product of prime numbers $p_i \in \mathbb{Z}$ and each of these p_i defines an irreducible ideal by Theorem 2.6. However, there also exist irreducible ideals generated by $z \in \mathcal{O}_D$ with $z \nmid d$. An example for this to happen is $d = 2$ and $z = (4, 6)$. Then $2 \nmid z$ since $(2, 3) \notin \mathcal{O}_4$ and (z) is an irreducible ideal.

The special linear group. We define $\mathrm{SL}_2(\mathcal{O}_D)$ to be the group of all 2 by 2 matrices with entries in $\mathcal{O}_D$ and determinant 1. Let us describe the elements in $\mathrm{SL}_2(\mathcal{O}_D)$ differently. An element

$$A = \begin{pmatrix} (a_1, a_2) & (b_1, b_2) \\ (c_1, c_2) & (d_1, d_2) \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_D)$$

has determinant $(a_1 d_1 - b_1 c_1, a_2 d_2 - b_2 c_2) = (1, 1)$.

Congruence subgroups. Now we want to define some of the main objects of this paper, namely congruence subgroups. For an ideal $\mathfrak{a} \subset \mathcal{O}_D$ the **principal congruence subgroup of level** $\mathfrak{a}$ is defined by

$$\Gamma^D(\mathfrak{a}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_D) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod \mathfrak{a} \right\}.$$

As usual, a subgroup $\Gamma \subset \mathrm{SL}_2(\mathcal{O}_D)$ is called a **congruence subgroup**, if it contains a principal congruence subgroup. The two most examples of congruence subgroups which we will be interested in are

$$\Gamma_0^D(\mathfrak{a}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod \mathfrak{a} \right\}$$

and

$$\Gamma_1^D(\mathfrak{a}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod \mathfrak{a} \right\}.$$

One might also define $\Gamma^D(\mathfrak{a})$ as the kernel of the projection $\mathrm{SL}_2(\mathcal{O}_D) \to \mathrm{SL}_2(\mathcal{O}_D/\mathfrak{a})$. Indeed, we even get the following proposition.

Proposition 2.8. *The sequence*

$$0 \to \Gamma^D(\mathfrak{a}) \to \mathrm{SL}_2(\mathcal{O}_D) \to \mathrm{SL}_2(\mathcal{O}_D/\mathfrak{a}) \to 0$$

is exact.

The index of some congruence subgroups. We now want to calculate the indexes of $\Gamma^D(\mathfrak{a})$ and $\Gamma_0^D(\mathfrak{a})$ in $\mathrm{SL}_2(\mathcal{O}_D)$ for an arbitrary ideal $\mathfrak{a} \subset \mathcal{O}_D$. The formulas which we will deduce are reminiscent of the formulas for non-square discriminants. The reason is that one can imitate the standard proof, which is given e.g. in [Kil08, Chapter 2.4] although one has to keep in mind that there are irreducible elements which are not prime. Obviously, the following inclusions hold for any ideal $\mathfrak{a} \subset \mathcal{O}_D$:

$$\Gamma^D(\mathfrak{a}) \subset \Gamma_1^D(\mathfrak{a}) \subset \Gamma_0^D(\mathfrak{a}) \subset \mathrm{SL}_2(\mathcal{O}_D).$$

We now state a lemma about the indexes of these inclusions. For the proofs we refer the reader to [Kil08] or [Wei08].

Lemma 2.9. *Let $\mathfrak{a} \subset \mathcal{O}_D$ be an ideal of finite norm.*

(i) Then

$$[\mathrm{SL}_2(\mathcal{O}_D) : \Gamma_0^D(\mathfrak{a})] = \#P^1(\mathcal{O}_D/\mathfrak{a})$$

holds, where $P^1(\cdot)$ denotes the projective space of dimension one.

(ii) We have

$$[\Gamma_0^D(\mathfrak{a}) : \Gamma_1^D(\mathfrak{a})] = \mathcal{N}(\mathfrak{a}).$$

(iii) We have

$$[\Gamma_1^D(\mathfrak{a}) : \Gamma^D(\mathfrak{a})] = \phi^D(\mathfrak{a})$$

where $\phi^D(\cdot)$ is the generalized Euler totient function, i.e. it counts the number of units in $\mathcal{O}_D/\mathfrak{a}$.

What is left to do is to calculate the number of elements of the projective space and the number of units. We start with two special cases and then deduce from them the general formula. First let $N \in \mathcal{O}_D$ be an arbitrary element with $(\mathcal{N}(N), d) = 1$. Then Theorem 2.6 implies that the quotient $\mathcal{O}_D/N\mathcal{O}_D$ completely splits into groups of prime order. Therefore we get (compare [Wei12, Chapter 1.3])

$$\#P^1(\mathcal{O}_D/N\mathcal{O}_D) = \mathcal{N}(N) \prod_{\mathfrak{p}|N} (1 + 1/\mathcal{N}(\mathfrak{p}))$$

and

$$\phi^D(N) = \mathcal{N}(N) \prod_{\mathfrak{p}|N} (1 - 1/\mathcal{N}(\mathfrak{p}))$$

where both products are taken over all prime ideals $\mathfrak{p}$ dividing N. On the other hand, if $N \in \mathbb{Z}$ is an arbitrary element with $N|d$ then let $p_1, ..., p_n$ be all the prime numbers in $\mathbb{Z}$ that divide N. Then $\mathcal{O}_D/N\mathcal{O}_D$ splits into the product of the $\mathcal{O}_D/p_i\mathcal{O}_D$ but not any further by Theorem 2.6. Hence

$$\#P^1(\mathcal{O}_D/N\mathcal{O}_D) = \mathcal{N}(N) \prod_{p|N}(1 + 1/p))$$

and

$$\phi^D(N) = \mathcal{N}(N) \prod_{p|N}(1 - 1/p))$$

where both products are taken over all prime numbers $p \in \mathbb{Z}$ dividing N.

Now we come to the general case. So let $\mathfrak{a} \subset \mathcal{O}_D$ be an arbitrary ideal. By the symmetry of $\mathcal{O}_D$ it is clear that $\mathfrak{a}$ and $\mathfrak{a}^\sigma$ define congruence subgroups of the same index. On the other hand the product of $\mathfrak{a}$ and $\mathfrak{a}^\sigma$ is the ideal generated by the integer $\mathcal{N}(\mathfrak{a})$. We may write $\mathcal{N}(\mathfrak{a})$ uniquely as $f \cdot M$ with $(M, d) = 1$ and f sharing all of its prime divisors in $\mathbb{Z}$ with d. So we can apply the two special cases which we just discussed to get:

Theorem 2.10. *Let $\mathfrak{a} \subset \mathcal{O}_D$ be an arbitrary ideal.*

(i) Then the index of $\Gamma_0^D(\mathfrak{a})$ in $\mathrm{SL}_2(\mathcal{O}_D)$ is given as

$$\mathcal{N}(N) \prod_{\substack{(\mathfrak{p},\mathfrak{p}^\sigma)\\ \mathfrak{p}|\mathcal{N}(\mathfrak{a})\\ \mathfrak{p}\mathfrak{p}^\sigma \nmid \mathfrak{a}}} (1 + 1/\mathcal{N}(\mathfrak{p})) \prod_{\substack{(\mathfrak{p},\mathfrak{p}^\sigma)\\ \mathfrak{p}|\mathcal{N}(\mathfrak{a})\\ \mathfrak{p}\mathfrak{p}^\sigma | \mathfrak{a}}} (1 + 1/\mathcal{N}(\mathfrak{p}))^2 \prod_{\substack{p|\mathcal{N}(\mathfrak{a})\\ p|d}} (1 + 1/p)$$

where the first and the second product are taken over all pairs of conjugated prime ideals and the third is taken over all prime numbers dividing d.

(ii) The index of $\Gamma^D(N)$ in $\mathrm{SL}_2(\mathcal{O}_D)$ is given as

$$\mathcal{N}(N)^3 \prod_{\substack{(\mathfrak{p},\mathfrak{p}^\sigma)\\ \mathfrak{p}|\mathcal{N}(\mathfrak{a})\\ \mathfrak{p}\mathfrak{p}^\sigma \nmid \mathfrak{a}}} (1 - 1/\mathcal{N}(\mathfrak{p})^2) \prod_{\substack{(\mathfrak{p},\mathfrak{p}^\sigma)\\ \mathfrak{p}|\mathcal{N}(\mathfrak{a})\\ \mathfrak{p}\mathfrak{p}^\sigma | \mathfrak{a}}} (1 - 1/\mathcal{N}(\mathfrak{p})^2)^2 \prod_{\substack{p|\mathcal{N}(\mathfrak{a})\\ p|d}} (1 - 1/p^2)$$

where the products are taken over the same objects as in (i).

In other words, the indexes of $\Gamma_0^D(\mathfrak{a})$ and of $\Gamma^D(\mathfrak{a})$ are as big as one would expect if one regarded prime divisors of the discriminant as ramified prime numbers (which they are not by Theorem 2.6).

Non-congruence subgroups. Recall that a finite index subgroup Γ of $\mathrm{SL}_2(\mathcal{O}_D)$ is a congruence subgroup if and only if there exists an ideal $\mathfrak{a} \subset \mathcal{O}_D$ such that the **level index** $[\mathrm{SL}_2(\mathcal{O}_D/\mathfrak{a}) : \rho_\mathfrak{a}(\Gamma)]$ is equal to the index $[\mathrm{SL}_2(\mathcal{O}_D) : \Gamma]$ where $\rho_\mathfrak{a} : \mathrm{SL}_2(\mathcal{O}_D) \to \mathrm{SL}_2(\mathcal{O}_D/\mathfrak{a})$ is the natural projection. The group Γ is called a **non-congruence subgroup of level** $\mathfrak{a}$ if the two indices differ and Γ is called a **totally non-congruence subgroup of level** $\mathfrak{a}$ if $[\mathrm{SL}_2(\mathcal{O}_D/\mathfrak{a}) : \rho_\mathfrak{a}(\Gamma)] = 1$. Being a totally non-congruence subgroup of level $\mathfrak{a}$ is yet equivalent to the index $[\Gamma : \Gamma \cap \Gamma(\mathfrak{a})]$ being equal to the index $[\mathrm{SL}_2(\mathcal{O}_D) : \Gamma(\mathfrak{a})]$. Note that the notion of being a totally non-congruence subgroup of level $\mathfrak{a}$ still makes sense in the situation that Γ is of infinite index if one defines this property via $[\Gamma : \Gamma \cap \Gamma(\mathfrak{a})] = [\mathrm{SL}_2(\mathcal{O}_D) : \Gamma(\mathfrak{a})]$. More details on non-congruence subgroups can be found in [WS12, Chapter 3].

Nori's Theorem. We have just seen that congruence subgroups are closely related to subgroups of $\mathrm{GL}_n(\mathbb{F}_m)$ where $\mathbb{F}_m$ denotes the finite field with m elements. In this situation one of the most powerful tools is Nori's theorem. It describes the subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$ for $n \in \mathbb{N}$ arbitrary and $p \in \mathbb{N}$ a prime number with $p > n$. We closely follow the exposition in [Rap12, Chapter 3.2] here: Let H be an arbitrary subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ and let $X := \{x \in H \mid x^p = 1\}$ and let $H^+ = \langle X \rangle \subset H$. An element $x \in H$ lies in X if and only if $(x-1)^n = 1$. We may thus for fixed $x \in X$ define

$$\log x := -\sum_{i=1}^{p-1} \frac{(1-x)^i}{i}.$$

Observing that $\log(x)^n = 0$, we see that for any $t \in \overline{\mathbb{F}_p}$, the algebraic closure of $\mathbb{F}_p$, we can define

$$x(t) := \exp(t \cdot \log x) \quad \text{where} \quad \exp z = \sum_{i=0}^{p-1} \frac{z^i}{i!}.$$

We regard $x(t)$ as a 1-parameter subgroup of GL_n and let $\widetilde{H}$ be the $\mathbb{F}_p$-subgroup of GL_n generated by the $x(t)$.

Theorem 2.11. ***(Nori, [Nor87])*** *If p is large enough (for a given n), then H^+ coincides with $\widetilde{H}(\mathbb{F}_p)$, the subgroup of $\widetilde{H}(\mathbb{F}_p)^+$ generated by all unipotents contained in it.*

If we specify to the case of GL_2, which is the only case we will make use of, we get (compare [Rap12, Chapter 3.2]):

Corollary 2.12. *For any subgroup of $H \subset \mathrm{GL}_2(\mathbb{F}_p)$, the subgroup H^+ has either 1 or p or $p^3 - p$ elements.*

Theta functions and theta characteristic. The 2-torsion points on an elliptic curve are in a natural correspondence with theta characteristics [FK92, Corollary VI.1.5]. Moreover the Weiterstraß points on a curve of genus 2 correspond to the odd theta characteristics (see e.g. [FK92, Chapter VII.1]). We will therefore quickly introduce this concept, but restrict here to dimension 2: Let $\mathbb{H}_2$ denote the Siegel upper half space of genus 2. Then we define for $\epsilon, \epsilon' \in \{0,1\}^{2x1}$ the **theta function with theta characteristic** (ϵ, ϵ') on $\mathbb{C}^2 \times \mathbb{H}_2$ by

$$\theta \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix} (u, Z) := \sum_{x \in \mathbb{Z}^2 + \epsilon/2} \exp\left(2\pi i \left(\frac{1}{2} x Z x^T + x \left(u + \frac{\epsilon'}{2}\right)\right)\right).$$

The theta characteristic is called **odd** if $\epsilon(\epsilon')^T$ is odd and **even** otherwise. Accordingly we denote the zero-locus of the theta function by

$$\Theta := \left\{ z \in \mathbb{C}^g \mid \theta \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix} (z, \Pi) = 0 \right\}$$

where Π is a fixed element in $\mathbb{H}_2$. We leave away Π in the definition of Θ as it will be clear from the context which matrix is meant.

3 Teichmüller curves

A **Teichmüller curve** $C \to \mathcal{M}_g$ is an algebraic curve in $\mathcal{M}_g$ that is totally geodesic with respect to the Teichmüller metric. Every Teichmüller curve stems from the projection of a $\mathrm{SL}_2(\mathbb{R})$-orbit of a translation surface $(X, \omega) \in \Omega\mathcal{M}_g$ to $\mathcal{M}_g$ (see e.g. [Möl11]). The stabilizer of (X, ω) under the $\mathrm{SL}_2(\mathbb{R})$-action is called its **Veech group**. On the contrary, the projection of the $\mathrm{SL}_2(\mathbb{R})$-orbit of a flat surface (X, ω) to $\mathcal{M}_g$ yields a Teichmüller curve if and only if its **Veech group** is a lattice. Moreover the Veech group is never cocompact. Although Teichmüller curves in higher genera $\mathcal{M}_g$ are not satisfactorily well understood yet, there has been great progress on Teichmüller curves in $\mathcal{M}_2$ in the last ten years (see e.g. [Bai07], [McM03], [Muk11]).

The simplest examples of Teichmüller curves are generated by **square-tiled surfaces** (or **Origamis**), i.e. flat surfaces (X, ω), where X is obtained as a covering of a torus ramified over at most one point and ω is the pullback of the holomorphic one-form on the torus. A square-tiled surface is called **primitive** if the developing vectors of the saddle connections span $\mathbb{Z}^2$. The square-tiled surfaces which we will treat here exclusively are the L-shaped polygons $L(m, n)$ (compare Figure 1) that all lie $\Omega\mathcal{M}_2(2)$.

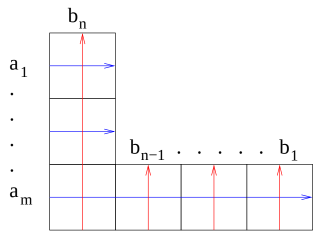

Figure 1. A $L(m, n)$ square-tiled surface with indicated pullback of the symplectic basis of $H_1(E_1, \mathbb{Z})$.

The decomposition of homology. A square-tiled surface $\pi_1 : X \to E_1$ with $g(X) = 2$ and consisting of d unit squares is called **minimal** if it does not factor via an isogeny. In this case, it is known that X is **split Jacobian**, i.e. for a minimal square-tiled surface there exists a torus E_2 and a covering $\pi_2 : X \to E_2$ of the same degree such that the induced morphism $\mathrm{Jac}(X) \to E_1 \times E_2$ is an isogeny of degree d^2 (compare [Kuh88]). We call E_2 the **complementary elliptic curve**. Note that we may identify the 2-torsion points of $\mathrm{Jac}(X)$ and the 2-torsion points of $E_1 \times E_2$ if d is odd. In our case, E_2 can be chosen in a canonical way. Roughly speaking, it is just the complementary variety of $E_1 \subset \mathrm{Jac}(X)$. An explicit construction of E_2 is given e.g. in [Kan03, Proposition 2.7] (see also [BL04, Chapters 5 and 12]). Then $H_1(E_2, \mathbb{Z})$ is the symplectic orthogonal complement of $H_1(E_1, \mathbb{Z})$ inside $H_1(X, \mathbb{Z})$.

Remark 3.1. *A square-tiled surface is minimal if and only if it is primitive (see [Kap11]).*

This implies that $H_1(X, \mathbb{Z})$ contains $\Lambda := H_1(E_1, \mathbb{Z}) \oplus H_1(E_2, \mathbb{Z})$ as a sublattice of index d^2 and that the symplectic pairing on $H_1(X, \mathbb{Z})$ respects this decomposition and is of type (d) on each direct summand. The action of the affine group $\mathrm{Aff}^+(\pi_1)$ induces an action on homology and thus induces an action on $H_1(E_i, \mathbb{Z})$. We denote these automorphism groups by Γ_i and let $\Gamma_i(\phi)$ be the image of $\phi \in \mathrm{Aff}^+(\pi_1)$.

Lemma 3.2. *If we regard the affine group* $\mathrm{Aff}^+(\pi_1)$ *as a subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ *(and not of* $\mathrm{PSL}_2(\mathbb{Z})$*) then the differential map* $D : \mathrm{Aff}^+ \to \Gamma(\pi_1)$ *is an isomorphism. More precisely,* $\Gamma_1(\phi) = D(\phi)$*. Hence there is a natural homomorphism* $f : \Gamma(\pi_1) \to \Gamma_2$*.*

Proof. The first statement follows from the fact that minimal genus 2 covers have no internal automorphisms if $d > 2$ [Kan03, Proposition 2.1]. Hence $D : \mathrm{Aff}^+(\pi_1) \to \Gamma(\pi_1)$ is an isomorphism. The second statement is just the definition of the action of the affine group. $\square$

From now on and until the end of this paper we fix the bases of both of the homology groups $H_1(E_i, \mathbb{Z})$. The explicit choice of the basis on $H_1(E_1, \mathbb{Z})$

is indicated in Figure 1. Kani's result in [Kan03, Chapter 4 and 5] imply that for this choice of bases the reduction of $f \mod d$ is conjugation by the diagonal matrix $R := \mathrm{diag}(-1, 1)$. Thus for a given matrix A in the Veech group the induced action on Λ is given by a pair of matrices $\widetilde{A} := (A_1 = A, RA_2R^{-1})$ where A_i acts on $H_1(E_i, \mathbb{Z})$ and $\widetilde{A} \in \mathrm{SL}_2(\mathcal{O}_D)$. We call the corresponding group the **homology Veech group**.

Example 3.3. *The homology Veech group of $L(2,2)$ is generated by the matrices*

$$\begin{pmatrix} 1 & 2-w \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 2-w & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Spin structure. Due to a result of Kani in [Kan03] the spin structure of a square-tiled surface in $\Omega\mathcal{M}_2(2)$ may be defined via the number of integral Weierstraß points: recall that in genus 2 the **Weierstraß points** of a square-tiled surface are the six fixed points of the hyperelliptic involution. A Weierstraß point is called **integral** if it is a vertex of one of the squares.

Proposition 3.4. ***(Kani, [Kan03, Proposition 2.4])*** *A primitive square-tiled surface in $\Omega\mathcal{M}_2(2)$ consisting of d squares has*

- *for $d = 3$, exactly 1 integral Weierstraß point*
- *for even d, exactly* 2 *integral Weierstaß points*
- *for odd d, either* 1 *or* 3 *integral Weierstraß points and both values occur.*

If d is odd then the **spin structure** of the square-tiled surface is called even if the number of Weierstraß point is 1 and otherwise it is called odd.

Remark 3.5. *The result of Kani was originally formulated in the language of abstract algebraic geometry. Its relevance for square-tiled surfaces was first observed in [Möl05, Remark 3.4]. Our formulation of the result goes back to [HL06, Proposition 4.3].*

Hubert and Lelièvre proved in [HL06] that the $\mathrm{SL}_2(\mathbb{R})$-orbits of square-tiled surfaces in $\Omega\mathcal{M}_2(2)$ can be distinguished by their spin structure. We restate their result in a way which is more applicable for us (compare also [WS12]):

Theorem 3.6. ***(Hubert/Lelièvre)*** *The set of primitive square-tiled surfaces in $\Omega\mathcal{M}_2(2)$ with d squares forms one single $\mathrm{SL}_2(\mathbb{Z})$ orbit, if d is even or $d = 3$. They form two orbits called $\mathcal{A}_d$ and $\mathcal{B}_d$ distinguished by their number of integral Weierstraß points, if d is odd and greater than* 3*. A square-tiled surface $L(m,n)$ with $d = m + n - 1$ squares belongs to $\mathcal{A}_d$ if both m and n are even and belongs to $\mathcal{B}_d$ if both m and n are odd. Each such square-tiled surface-orbit is generated by some $L(m,n)$.*

Remark 3.7. *More generally, Teichmüller curves in $\Omega\mathcal{M}_2(2)$ have been completely classified by McMullen in [McM05] by their spin structure and their discriminant.*

We embed the Teichmüller curve $X \subset \mathcal{M}_2$ in its Jacobian in the following way: we choose an arbitrary Weierstraß point $z \in X$ and define

$$\varphi_z : X \to \mathrm{Jac}(X), \quad x \mapsto [x - z].$$

Then $\varphi_z(X) = \Theta$ if $[z] = \frac{1}{2}(\mathrm{Id}\epsilon' + \Pi\epsilon)$ (compare [FK92, Chapter VII.1.2]).

Spin structure of the complementary elliptic curve. By counting the number of integral Weierstraß points also the complementary elliptic curve may be given a spin structure in a canonical way if $d > 3$ is *odd*. We fix E_1 by choosing the marked point as $p =: (0,0)$. By construction also the complementary elliptic curve E_2 is then fixed (it is the symplectic orthogonal complement of E_1 inside the Jacobian). The Weierstraß points of the square-tiled surface $\pi : L_d \to E_1$ are preimages of the 2-torsion points on E_1 and 1 or 3 of them are integral, i.e. lie over p.

Since $\mathrm{Jac}(X) \to E_1 \times E_2$ is an isogeny of degree d where d is odd all Weierstraß points of X are 2-torsion points of $E_1 \times E_2$. There is a one-to-one correspondence between the Weierstraß points of X and odd theta characteristics. The latter are:

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

More precisely, if we use the fact that $\mathrm{Jac}(X)$ is isogenous to $E_1 \times E_2$ of odd degree d, then by renormalizing the odd theta characteristics by an odd translation the correspondence can be made as follows (compare [FK92, Chapter VI.3]): the first column of the theta characteristic divided by 2 corresponds to the coordinates of the projection of the Weierstraß points of L_d to E_1 and the second column of the theta characteristic divided by 2 corresponds to the coordinates of the projection of the Weierstraß points of L_d to E_2.

Lemma 3.8. *If the odd theta characteristics are translated by an odd theta characteristic*

- *with first column* $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ *then there is one translated characteristic with second column* $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$.
- *with first column* $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ *or* $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ *or* $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ *then there are three translated characteristics with second column* $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$.

Proof. This is an immediate calculation. □

Theorem 3.9. *Let $\pi_1 : L_d \to E_1$ be a square-tiled surface in $\Omega\mathcal{M}_2(2)$ and let E_2 denote the complementary elliptic curve. If $\pi_1 : L_d \to E_1$ has even spin, then $\pi_2 : L_d \to E_2$ has odd spin. If $\pi_1 : L_d \to E_1$ has odd spin, then $\pi_2 : L_d \to E_2$ has even spin.*

Proof. If $\pi_1 : L_d \to E_1$ has three 3 integral Weiterstraß points then we have to renormalize the odd theta characteristics by adding a odd theta characteristic with first column $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$. Thus $\pi_2 : L_d \to E_2$ has exactly 1 integral Weierstraß point by Lemma 3.8. If $\pi_1 : L_d \to E_1$ has one integral Weierstraß point then we have to renormalize the odd theta characteristics by adding an odd characteristic with first column $\neq \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ to each element of the list (although we do, of course, not know precisely which one). Then $\pi_2 : L_d \to E_2$ has three integral Weierstraß points again by Lemma 3.8. □

Calculating elements of the homology Veech group. Having described how the Veech group acts on homology and how this action yields matrices in $\mathrm{SL}_2(\mathcal{O}_D)$, we now calculate some elements of the homology Veech group of $L(m,n)$ with $m+n-1=d$. We denote its Veech group by $\mathrm{SL}(L_d)$ and accordingly its homology Veech group by $\mathrm{SL}^1(L_d)$. Let a, b be the symplectic basis of $H_1(E_1, \mathbb{Z})$ and consider its pullback to $H_1(L(m,n), \mathbb{Z})$ (compare Figure 1). Note that the classes $a_1, ..., a_{m-1}$ and the classes $b_1, ..., b_{n-1}$ respectively each define only a single classes in $H_1(L(m,n), \mathbb{Z})$. Therefore the pullback of the symplectic basis of $H_1(E_i, \mathbb{Z})$ yields the elements

$$c_1 = (m-1)a_1 + a_m \quad \text{and} \quad d_1 = (n-1)b_1 + b_n.$$

of $H_1(L(m,n), \mathbb{Z})$. For their symplectic pairing we have

$$(c_1, d_1) = (m-1)(n-1) \cdot 0 + (m-1) \cdot 1 + (n-1) \cdot 1 + 1 = d.$$

The set c_1, d_1 may be extended to a symplectic basis of Λ by choosing $c_2 := na_1 - a_m$ and $d_2 := -mb_1 + b_n$ as

$$(c_1, c_2) = (n-1) + (-n) + 1 = 0 \quad \text{and} \quad (d_1, d_2) = (m-1) + (-m) + 1 = 0$$

and

$$(c_2, d_2) = n + m - 1 = d.$$

Before we start with the calculation of some elements of the homology Veech group, let us first fix the notation for some special matrices in $\mathrm{SL}_2(\mathbb{Z})$ first, namely

$$T' := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \; Z' := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad S' = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Recall that the Veech group of $L(m,n)$ always contains the element T'^n. This matrix acts on the a_i and b_i by

$$a_i \mapsto a_i \quad i = 1, m$$

$$b_1 \mapsto b_1 + a_m$$

$$b_n \mapsto b_n + a_m + n(m-1)a_1$$

since the matrix T'^n yields a single Dehn-twist on the lower cylinder and a n-fold Dehn-twist on the upper cylinder and since the a_i are parallel to the twist direction. Therefore

$$c_2 \mapsto c_2 \;\text{ and }\; d_2 \mapsto c_2 + (m-1)d_2.$$

The action of the Veech group on the homology of $L(m,n)$ hence yields the element $T := (T'^n, T'^{n-d}) \in \mathrm{SL}_2(\mathcal{O}_D)$. Analogously, the homology Veech group always contains $Z := (Z'^m, Z'^{m-d}) \in \mathrm{SL}_2(\mathcal{O}_D)$.
Furthermore the Veech group of $L(m,n)$ always contains the element

$$E' := \begin{pmatrix} 1-d & d \\ -d & 1+d \end{pmatrix}.$$

Analyzing the action of this element on the homology basis a_i, b_i we get

$$a_1 \mapsto ma_1 + a_m + (n-1)b_1 + b_n$$

$$a_m \mapsto (m-1)na_1 + (n+1)a_m + (n-1)nb_1 + nb_n$$

$$b_1 \mapsto -((m-1)a_1 + a_m + (n-2)b_1 + b_n)$$

$$b_n \mapsto -((m-1)ma_1 + ma_m + (n-1)mb_1 + (m-1)b_m).$$

This yields that the homology Veech group contains the matrix

$$E := (E', \mathrm{Id}) = \begin{pmatrix} 1-(d-w) & d-w \\ -(d-w) & 1+(d-w) \end{pmatrix}.$$

If $n = 3$ and m is odd, then we can compute an element in the homology from the cylinder decomposition in direction $(2/m, 1)$, namely

$$\begin{aligned} F \; &:= \; \begin{pmatrix} (1-2(d-2), 1+(4-d)) & (4, 4-d) \\ (-(d-2)^2, -(4-d)) & (1+2(d-2), 1-(4-d)) \end{pmatrix} \\ &= \; \begin{pmatrix} 1-(2(d-2)+w) & 4-w \\ -(d-2)^2+(d-3)w & 1+(2(d-2)+w) \end{pmatrix} \end{aligned}$$

Finally, let us specify to the case $n = 2$. Then the cylinder decomposition in direction $(2/m, 1)$ yields the following elements in the homology Veech group:

- If $m \equiv 2 \mod 4$:

$$F := \begin{pmatrix} (1-3/2m, 2-m/2) & (3, -(m-2)) \\ (-3/4m^2, (m-2)/4) & (1+3/2m, m/2) \end{pmatrix} = \begin{pmatrix} * & 3-w \\ * & * \end{pmatrix}$$

- If $m \equiv 0 \mod 4$:

$$F := \begin{pmatrix} (1-3m, 3-m) & (6, -2(m-2)) \\ (-3/2m^2, (m-2)/2) & (1+3m, m-1) \end{pmatrix} = \begin{pmatrix} * & 2(3-w) \\ * & * \end{pmatrix}$$

- If $m \equiv 1 \mod 2$:

$$F := \begin{pmatrix} (1-6a, 5-2m) & (12, 4(m-2)) \\ (-3m^2, m-2) & (1+6m, 2m-3) \end{pmatrix} = \begin{pmatrix} * & 4(3-w) \\ * & * \end{pmatrix}$$

4 Proof of the main result

In this section, we calculate the index of $\Gamma_0^D(\mathfrak{a}) \cap \mathrm{SL}^1(L_d)$ in $\mathrm{SL}^1(L_d)$ for an arbitrary ideal $\mathfrak{a} \subset \mathcal{O}_D$ and thereby show our main theorem.

Theorem 4.1. *Let L_d be a square-tiled surface in $\Omega\mathcal{M}_2(2)$ with d squares and let $\mathrm{SL}^1(L_d)$ be its homology Veech group. We distinguish the two different cases that L_d is in the orbit $\mathcal{A}_d$ and $\mathcal{B}_d$ in the classification of square-tiled surfaces in $\Omega\mathcal{M}_2(2)$. Moreover if d is odd let $2 = \mathfrak{p}_2\mathfrak{p}_2^\sigma$ be the decomposition of 2 into prime ideals, where $\mathfrak{p}_2$ is the distinguished common prime ideal divisor of 2 and $2-w$ in $\mathcal{O}_D$.*

(1A) If d is odd and L_d is in $\mathcal{A}_d$, or $d = 3$, then $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = [\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ for all ideals $\mathfrak{a} \subset \mathcal{O}_{d^2}$ with $(\mathfrak{p}_2, \mathfrak{a}) = 1$.

(1B) If d is odd and L_d is in $\mathcal{A}_d$, or $d = 3$, then $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = \frac{2}{3}[\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ for all ideals with $\mathfrak{p}_2|\mathfrak{a}$.

(2A) If d is odd and L_d is in $\mathcal{B}_d$, then we have $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = [\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ for all ideals $\mathfrak{a} \subset \mathcal{O}_{d^2}$ with $(\mathfrak{p}_2^\sigma, \mathfrak{a}) = 1$.

(2B) If d is odd and L_d is in $\mathcal{B}_d$, then we have $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = \frac{2}{3}[\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ for all ideals with $\mathfrak{p}_2^\sigma|\mathfrak{a}$.

(3A) If d is even, then $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = [\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ for all ideals $\mathfrak{a} \subset \mathcal{O}_{d^2}$ with $2 \nmid \mathcal{N}(\mathfrak{a})$ (the norm of $\mathfrak{a}$).

(3B) If d is even, then $[\mathrm{SL}^1(L_d) : \mathrm{SL}^1(L_d) \cap \Gamma_0(\mathfrak{a})] = \frac{2}{3}[\mathrm{SL}_2(\mathcal{O}_{d^2}) : \Gamma_0(\mathfrak{a})]$ for all ideals with $2|\mathcal{N}(\mathfrak{a})$,

Remark 4.2. *The case $d = 3$ may be directly read off from example 3.3. We will therefore not treat this case in the following.*

Remark 4.3. *As every ideal $\mathfrak{a} \subset \mathcal{O}_D$ is contained in a principal ideal generated by an element $h \in \mathbb{Z}$, we may restrict to the case $\mathfrak{a} = (h)$ whenever necessary.*

Before we start with the proof let us fix some notation. We have seen that we may (h) decompose uniquely as

$$(h) = \prod_{\substack{p|d,\\ p|n}} p^{e_p} \prod_{\mathfrak{q}|n} \mathfrak{q}^{f_\mathfrak{q}} \mathfrak{q}^{\sigma f_\mathfrak{q}}$$

with $e_i, f_i \in \mathbb{N}$ where the first product is taken over all prime numbers and the second is taken over all prime ideals. Furthermore we set $H := \mathcal{N}(h)$.

We will prove Theorem 4.1 step by step: As the index of $\mathrm{SL}^1(L_d) \cap \Gamma^D(h)$ in $\mathrm{SL}^1(L_d)$ does not depend on the ordering of the divisors of (h) which we choose, we may first divide out the prime number divisors of the discriminant and then the prime divisors of split prime numbers. Moreover we may always assume that we consider the divisor $\mathfrak{p}$ of (h) which has the highest order in (h) of all divisors $\mathfrak{p}_i$ of the given type.

To prove the theorem we will proceed in the following way: We first calculate for an arbitrary prime ideal $\mathfrak{p} \subset \mathcal{O}_D$ and with $((h), \mathfrak{p}) = 1$ the index

$$[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D((h)\mathfrak{p}^k) : (\mathrm{SL}^1(L_d) \cap \Gamma^D((h)\mathfrak{p}^{k+1}))]$$

for all $k \in \mathbb{N}$ and then the index

$$[(\mathrm{SL}^1(L_d) \cap \Gamma^D((h))) : (\mathrm{SL}^1(L_d) \cap \Gamma^D((h)\mathfrak{p}))].$$

Of course, this suffices to prove the theorem. We will from now leave away brackets indicating ideals since this will facilitate notation. As a shortcut we write

$$T := \begin{pmatrix} 1 & \eta^+ \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad Z := \begin{pmatrix} 1 & 0 \\ \eta^- & 1 \end{pmatrix}.$$

Remark 4.4. *For all $L(m.n)$ we have*

$$\eta^* := \eta^+\eta^- = (n-w)(m-w) = mn - w.$$

Furthermore we will frequently make use of the following lemma:

Lemma 4.5. *(i) If $b \in \mathcal{O}_D$ is not a zero divisor and $a, c \in \mathcal{O}_D$ then $ab|cb$ if and only if $a|c$.*

(ii) If $p \in \mathbb{Z}$ is a prime number and $a, b \in \mathbb{Z}$ then $p|a + wb$ if and only if $p|a$ and $p|b$.

(ii) *If $p, m, x \in \mathcal{O}_D$ and $p \in \mathbb{Z}$ is a prime number with $p|d$ and $p|mx$. Then $p \nmid \mathcal{N}(m)$ implies $p|x$.*

Proof. (i) and (ii) are immediately clear by definition.
(iii) Let $m = (m_1, m_2)$ and $x = (x_1, x_2)$. Then $p|mx$ implies $\mathcal{N}(p)|\mathcal{N}(mx)$ or in other words $p^2|m_1m_2x_1x_2$. Since $p \nmid \mathcal{N}(m)$ hence $p|x_1x_2$ and since $p|d$ we must have $p|x_1$ and $p|x_2$, i.e. $x_1 = pk_1$ and $x_2 = x_1 + jd = pk_1 + pk_2$ with $k_1, k_2 \in \mathbb{Z}$. Then $(p,p)|(pk_1m_1, (pk_1 + pk_2)(m_1 + ld))$ is equivalent to

$$(p,p)|(pm_1k_1, p(m_1k_1 + m_1k_2 + k_1ld + k_2ld)$$

which implies $d|m_2k_2+(k_1+k_2)ld$. From this it follows either that $p|m_1$ which contradicts the fact $p \nmid \mathcal{N}(m)$ or $p|k_2$. In the latter case $x_2 = p(k_1 + dk_2)$ and so $p|x$ as we claim. □

Divisors of the discriminant. We begin with the case which is the most special compared to [Wei12] since prime numbers $p \in \mathbb{Z}$ with $p|d$ are in our case irreducible but not prime. The main difference to the proof of [Wei12, Theorem 5.1] is that we need to use Weitze-Schmithüsen's result at some point (Proposition 4.8).

Proposition 4.6. *Let $p \in \mathbb{Z}$ be a prime number with $p|d$ and $(m,p) = 1$ and let $h \in \mathbb{Z}$ be an arbitrary element with $(h,p) = 1$. Then for all $k \in \mathbb{N}$*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(hp^k)) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(hp^{k+1}))\right] = \mathcal{N}(p) = p^2$$

holds.

Proof. We want to find matrix W which is a word in T and Z such that the matrices

$$W^l Z^{hp^k j}, \quad j = 1, ..., p, \quad l = 1, ..., p$$

lie $\Gamma_0^D(hp^k)$ but are all incongruent modulo $\Gamma_0^D(hp^{k+1})$. The matrix

$$W := ZT^{hp^k}Z^{-1}$$

is a good a choice for this. First, it is in $\Gamma_0^D(hp^k)$. Secondly

$$W^y Z^{hp^k j} \equiv W^l Z^{hp^k i}$$

is equivalent to $W^y Z^{hp^k(j-i)} W^{-l} \in \Gamma_0^D(hp^{k+1})$. Setting $x := j - i$ we thus need to check when

$$\begin{aligned} (W^y Z^{hp^k x} W^{-l})_{2,1} \quad &= \quad \underbrace{p^{3k}h^3\eta^{-3}\eta^{+2} \cdot ylx}_{v_1} \\ &+ \quad \underbrace{p^{2k}h^2\eta^{-2}\eta^{+} \cdot (y+l)x}_{v_2} \\ &+ \quad \underbrace{p^k h\eta^{-}(x + \eta^{-}\eta^{+} \cdot (l-y))}_{v_3} \end{aligned}$$

is divisible by hp^{k+1}. We already know that $hp^{k+1}|v_1 + v_2$. So we are interested in which cases we have $hp^{k+1}|hp^k\eta^-(x + \eta^-\eta^+ \cdot (l - y))$. By Lemma 4.5 we only have to check when $p|\eta^-(x + \eta^-\eta^+ \cdot (l - y))$ holds. We have $\eta^-\eta^+ = mn - w$, by Remark 4.4. Thus we ask when $p|(m - w)((mn - w) \cdot (l - y) + x)$. We now just look at the *real part* of the right hand side (i.e. the part which does lie in $\mathbb{Z}$). This gives us that $p|x + mn(l - y)$ since $p \nmid m$. Considering the *imaginary part* (i.e. the part which does lie in $\mathbb{Z}$) we then get $p|m(l - y)$. Thus $l = y$ and therefore $p|x$. This yields $x = 0$ or in other words $i = j$. $\square$

Since the proof did not depend on the condition $k > 0$ we get an immediate corollary:

Corollary 4.7. *Let $p \in \mathbb{Z}$ be an inert prime number with $p|d$ and $(m,p) = 1$. Moreover let $h \in \mathbb{Z}$ be an arbitrary elements with $(h,p) = 1$. Then*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h)) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(hp))\right] \geq p^2$$

holds.

Before we are able to prove that this index is indeed as big as possible, i.e. equal to $p(p+1)$, we have to do some abstract group theory. Recall our situation: the homology Veech group $\mathrm{SL}^1(L_d)$ is given by pairs (A_i, B_i) with A_i in the ordinary Veech group $\mathrm{SL}(L_d)$ and B_i is in the complementary Veech group $\mathrm{SL}^c(L_d)$. Two elements (A_1, B_1) and (A_2, B_2) in $\mathrm{SL}^1(L_d)$ yield the same representative in $\mathrm{SL}^1(L_d)/(\mathrm{SL}^1(L_d) \cap \Gamma_0((h_1, h_2)))$ if and only if A_1 and A_2 yield the same representative in $\mathrm{SL}(L_d)(\mathrm{SL}(L_d) \cap \Gamma_0(h_1))$ and B_1 and B_2 yield the same representative in $\mathrm{SL}^c(L_d)/(\mathrm{SL}^c(L_d) \cap \Gamma_0(h_2))$. Now we can easily prove:

Proposition 4.8. *Let $p \in \mathbb{Z}$ be an inert prime number with $p|d$ and $(m,p) = 1$. Moreover let $h \in \mathbb{Z}$ be an arbitrary element with $(h,p) = 1$. Then*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(m)) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(mp))\right] = p(p+1)$$

holds.

Proof. Let q be the index $\left[(\mathrm{SL}(L_D) \cap \Gamma_0^D(m)) : (\mathrm{SL}(L_D) \cap \Gamma_0^D(mp))\right]$. We know by Corollary 4.7 that $q \geq p^2$. Then we get by Corollary 1.2 that $p+1|q$ since the index $[\mathrm{SL}(L_d) : (\mathrm{SL}(L_d) \cap \Gamma_0(h_1))]$ divides the index $[\mathrm{SL}^1(L_d) : (\mathrm{SL}^1(L_d) \cap \Gamma_0((h_1, h_2)))]$. Finally, $(p+1)(p-1) = p^2 - 1$ yields the claim. $\square$

Divisors of split prime numbers. The second case which we treat concerns prime numbers $p \in \mathbb{Z}$ that split, i.e. $p \in \mathbb{Z}$ with $p \nmid d$.

Lemma 4.9. *Let $p \in \mathbb{Z}$ with $p = \mathfrak{p}\mathfrak{p}^\sigma$ and let $(\mathfrak{p}, \eta^-) = 1$. Moreover let $h \subset \mathcal{O}_D$ be an arbitrary ideal with $(h, \mathfrak{p}) = 1$. Then for all $k \in \mathbb{N}$*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p}^k) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p}^{k+1})\right] = p$$

holds.

Proof. The aim is to find p matrices in $\Gamma_0^D(h\mathfrak{p}^k)$ which are inequivalent modulo $\Gamma_0^D(h\mathfrak{p}^{k+1})$. We will now describe the simplest set of matrices which we found. We have to distinguish two cases.

1. Case: $\mathfrak{p}$ *is not conjugated to any of the* $\mathfrak{q}$ *dividing* h
Then $Z^{Hp^k i}$, $i = 1, ..., p$ are obviously in $\Gamma_0^D(h\mathfrak{p}^k)$ but inequivalent modulo $\Gamma_0^D(h\mathfrak{p}^{k+1})$.

2. Case: $\mathfrak{p}$ *is conjugated to a certain* $\mathfrak{q}$ *dividing* h *with order* $f_\mathfrak{q}$
We set $\mathfrak{h} := h\mathfrak{q}^{-f_\mathfrak{q}}$ and $H' := \mathcal{N}(\mathfrak{h})$. Let us assume that $\mathfrak{q}^l | \eta^-$ and $\mathfrak{q}^{l+1} \nmid \eta^-$ for some $l \in \mathbb{Z}_{\geq 0}$. We now have to distinguish two subcases.
Case (a) $f_\mathfrak{q} - l > k$
In particular, this implies that $\mathfrak{q}$ has a higher order in h than k. We therefore want to divide out powers of $\mathfrak{q}$ first. This means that we have to show

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(\mathfrak{h}\mathfrak{q}^{f_\mathfrak{q}-1}\mathfrak{p}^k)) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(\mathfrak{h}\mathfrak{q}^{f_\mathfrak{q}}\mathfrak{p}^k))\right] = p.$$

We set $u := f_\mathfrak{q} - l - 1$ and $v := p^u$. The matrices $Z^{H'vi}$, $1 \leq i \leq p$ lie in $\Gamma_0^D(\mathfrak{h}\mathfrak{q}_h^{f_\mathfrak{q}-1}\mathfrak{p}^k))$ since $\mathfrak{h}\mathfrak{q}^{f_\mathfrak{q}-1}\mathfrak{p}^k | H'v\eta^- \cdot i$ but the matrices are incongruent modulo $\Gamma_0^D(\mathfrak{h}\mathfrak{q}^{f_\mathfrak{q}}\mathfrak{p}^k)$ since $\mathfrak{h}\mathfrak{q}^{f_\mathfrak{q}}\mathfrak{p}^k | H'v\eta^- \cdot i$ implies $\mathfrak{q}|i$ by the definition of v. This means that we may restrict to case (b), namely:
Case (b) $k \geq f_\mathfrak{q} - l$.
We then set $v = p^k$ and look at the matrices $Z^{H'vi}$, $1 \leq i \leq p$. These matrices are all in $\Gamma_0^D(h\mathfrak{p}^k)$ but are not equivalent modulo $\Gamma_0^D(h\mathfrak{p}^{k+1})$ by definition of v. ☐

Lemma 4.10. *Let $p \in \mathbb{Z}$ with $p = \mathfrak{p}\mathfrak{p}^\sigma$ and $(\mathfrak{p}, \eta^*) = 1$. Moreover let $h \subset \mathcal{O}_D$ be an arbitrary ideal with $(\mathcal{N}(h), \mathfrak{p}) = 1$. Then*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h) : (\mathrm{SL}(L_D) \cap \Gamma_0^D(h\mathfrak{p})\right] = p + 1$$

holds.

Proof. We want to find a $k \in \mathbb{N}$ such that the matrices

$$\begin{array}{lll} (I) & Z^{Hi}, & i = 1, ..., p \\ (II) & Z^{Hk}T & \end{array}$$

lie in $\Gamma_0^D(h)$ and are pairwise incongruent modulo $\Gamma_0^D(h\mathfrak{p})$. Indeed, we choose k as follows: let $k \in \{1, ..., p\}$, such that $\mathfrak{p}|kH\eta^-\eta^+ + 1$. This is always possible since $\mathfrak{p} \nmid \eta^*$ and $\mathfrak{p} \nmid H$ and $1, .., p$ are incongruent modulo $\mathfrak{p}$. Furthermore we know that $k \neq p$ because otherwise it would follow that $\mathfrak{p}|1$. By definition, it is clear that all the matrices (I) and (II) lie in $\Gamma_0^D(h)$ and that the matrices in (I) are pairwise incongruent. Finally, we calculate

$$(Z^{Hk}TZ^{-Hi})_{2,1} = H\eta^-(-(kH\eta^-\eta^+ + 1)i + k).$$

Now suppose $\mathfrak{p}|H\eta^-(-(kH\eta^-\eta^+ + 1)i + k)$. In other words this means $\mathfrak{p}|(-i(kH\eta^-\eta^+ + 1) + k)$ which is yet equivalent to $\mathfrak{p}|k$ as $\mathfrak{p}|(kH\eta^-\eta^+ + 1)$. This is a contradiction.

$\square$

Lemma 4.11. *Let $p \in \mathbb{Z}$ with $p = \mathfrak{p}\mathfrak{p}^\sigma$ and $(p, \eta^*) = 1$. Moreover let $h \subset \mathcal{O}_D$ be an arbitrary ideal with $(\mathcal{N}(h), \mathfrak{p}) = 1$. Then*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p}^\sigma) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p}^\sigma\mathfrak{p})\right] = p + 1$$

holds.

Proof. We want to find a matrix W which is a word in T and Z such that the matrices

(I) WT^i, $i = 1, ..., p$

(II) Id

lie in $\Gamma_0^D(h\mathfrak{p}^\sigma)$ and are pairwise incongruent modulo $\Gamma_0^D(h\mathfrak{p}^\sigma\mathfrak{p})$. This time, we choose k as follows: let $k \in \{1, ..., p\}$, such that $\mathfrak{p}^\sigma|k\eta^-\eta^+ + 1$. This is possible since $\mathfrak{p}^\sigma \nmid \eta^*$. Now suppose that $\mathfrak{p}|k\eta^-\eta^+ + 1$. Since $(\mathfrak{p}, \mathfrak{p}^\sigma) = 1$ we would then have $\mathfrak{p}\mathfrak{p}^\sigma|k\eta^-\eta^+ + 1$ which would imply $p|k$ (by Remark 4.4 and Lemma 4.5). This is a contradiction. Hence $\mathfrak{p} \nmid k\eta^-\eta^+ + 1$.
We now choose $W := ZT^kZ^HT^{-k}Z^{-1}$. Then we have

$$(WT^i)_{2,1} = H\eta^-(k\eta^+\eta^- + 1)^2$$

and so all the matrices lie in $\Gamma_0^D(h\mathfrak{p}^\sigma)$ but none of them is equivalent to the identity. Finally, we calculate

$$(WT^xW^{-1})_{2,1} = -H\eta^{-2}\eta^+(k\eta^-\eta^+ + 1)^4 \cdot x.$$

As $\mathfrak{p} \nmid H$, $\mathfrak{p} \nmid \eta^*$ and $\mathfrak{p} \nmid (k\eta^-\eta^+ + 1)$ the matrices in (I) are pairwise incongruent modulo $\Gamma_0^D(h\mathfrak{p}^\sigma\mathfrak{p})$. $\square$

Summarizing we have proven:

Proposition 4.12. *Let $p \in \mathbb{Z}$ with $p = \mathfrak{p}\mathfrak{p}^\sigma$ and $(p, \eta^*) = 1$. Then for all ideals $h \subset \mathcal{O}_D$ with $(h, \mathfrak{p}) = 1$*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h)) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p})\right] = p + 1$$

holds.

Divisors of η^*. So far we have only treated ideals $\mathfrak{a}$ with $(\mathfrak{a}, \eta^*) = 1$. Before we come to the case $(\mathfrak{a}, \eta^*) \neq 1$ let us analyze the prime divisors of $m - w$ and $n - w$. By Corollary 2.4 there are essentially two different types of prime ideals of norm p, namely

$$\mathfrak{p}_1 = [p, p + w] \quad \text{and} \quad \mathfrak{p}_2 = [p, p - d + w].$$

If the prime ideal is of type 1 and divides $m - w$ then it follows that $p|m$ and that $\mathfrak{p}_1 \nmid d - w$ since $p \nmid d$. If the prime ideal is of type 2 and divides $m - w$ then it follows that $p|m + d$ and that $\mathfrak{p}_2|d - w$. Now we choose $m = d - 1$ and $n = 2$ whenever this is possible by Corollary 3.6 and $m = d - 2$ and $n = 3$ otherwise. Note that the only possible common divisor of $m - w$ and $n - w$ are then the prime ideal divisors of 2.

Remark 4.13. *By the choice of m there does not exist a $p \in \mathbb{Z}$ with $p|d$ and $p|m$. Thus the main theorem is proven for all divisors of the discriminant.*

Lemma 4.14. *Let $p \in \mathbb{Z}$ with $p = \mathfrak{p}\mathfrak{p}^\sigma$ with $\mathfrak{p}|\eta^-$. Moreover let $h \subset \mathcal{O}_D$ be an arbitrary element with $(h, \mathfrak{p}) = 1$. Then for all $k \in \mathbb{N}$*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p}^k) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p}^{k+1})\right] = p$$

holds.

Proof. Case $n = 2$: Note that $\mathfrak{p} \nmid d$ since p splits. Since $\mathfrak{p}$ is a prime ideal it is either of the form $[p, p + w]$ or $[p, p - d + w]$ (Corollary 2.4). As $\mathfrak{p}|\eta^-$ it must even be of the form $[p, p + w]$. Hence we have that $\mathfrak{p} \nmid (d - w)$ but $\mathfrak{p}^\sigma|(d - w)$. Then we set $H' = \mathcal{N}(h(h, \mathfrak{p}^\sigma)^{-1})$ and claim that the matrices $E^{H'p^k i}, 1 \leq i \leq p$ are a set of coset representatives. Now assume that $\mathfrak{p}^{k+1}|H'(d - w)p^k i$. This yields $\mathfrak{p}|(d - w)i$ (Lemma 4.5). Since $\mathfrak{p} \nmid d - w$ the claim follows.
Case $n = 3$: We have to treat the case $\mathfrak{p}|\eta^-$ and $\mathfrak{p}|2$ separately. If $\mathfrak{p} = [2, -d + w]$ divides $3 - w$ then $d - 3$ is odd and thus $\mathfrak{p}$ does not divide $F_{2,1}$. Hence the claim follows. □

Lemma 4.15. *Let $p \in \mathbb{Z}$ with $p = \mathfrak{p}\mathfrak{p}^\sigma$ and let $\mathfrak{p}|\eta^-$ with $\mathfrak{p} \nmid 2$. Moreover let $h \subset \mathcal{O}_D$ be an arbitrary ideal with $(h, \mathfrak{p}) = 1$. Then*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p})\right] = p + 1$$

holds.

Proof. Case (1) $\mathfrak{p} \nmid d - n$: Note that since $\mathfrak{p}|\eta^-$ and $\mathfrak{p} \nmid d - n$ we get that $\mathfrak{p} \nmid (d - w)$ but $\mathfrak{p}^\sigma|(d - w)$. Let $H' = \mathcal{N}(h(h, \mathfrak{p}^\sigma)^{-1})$. Then we claim that the matrices

(I) $\quad E^{H'}T^k \quad k = 1, ..., p$

(II) $\quad \mathrm{Id}$

lie in $\Gamma_0^D(h)$ and are pairwise incongruent modulo $\Gamma_0^D(h\mathfrak{p})$. Since

$$(E^{H'}T^k)_{2,1} = H'(d-w)$$

none of the matrices in (I) is congruent to the identity. On the other hand

$$(E^M T^k E^{-M})_{2,1} = -H'^2\eta^+(d-w)^2 \cdot k$$

and thus the matrices (I) are pairwise incongruent modulo $\Gamma_0^D(h\mathfrak{p})$.
Case (2) $\mathfrak{p}|d-n$: By case (1) we may assume that $\mathfrak{p} \nmid \mathcal{N}(h)$. Then the arguments work as above after replacing E by F. $\square$

For the divisors of η^+, Nori's theorem significantly facilitates the proof.

Lemma 4.16. *Let $p \in \mathbb{Z}$ with $p = \mathfrak{p}\mathfrak{p}^\sigma$ and let $\mathfrak{p}|\eta^+$. Moreover let $h \subset \mathcal{O}_D$ be an arbitrary ideal with $(h, \mathfrak{p}) = 1$. Then*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p})\right] = p+1$$

holds.

Proof. Case $n=2$: Note that since $\mathfrak{p}|\eta^+ = 2-w$ we have that $\mathfrak{p} \nmid 3-w$. By what we have proven so far, we may assume that $(\mathcal{N}(h), \mathfrak{p}) = 1$. Then the matrices F^{Mi} and T^{Mi} all lie in $\Gamma_0^D(h)$ and they all yield different elements when they are projected to $\mathrm{SL}_2(\mathcal{O}_D/\mathfrak{p}\mathcal{O}_D) \cong \mathrm{SL}_2(\mathbb{F}_p)$. By the corollary to Nori's theorem (Corollary 2.12), this map has to be surjective and therefore $\mathrm{SL}^1(L_d) \cap \Gamma_D^0(h\mathfrak{p})$ must have the maximal possible index in $\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h)$.
Case $n=3$: The same reasoning as above is possible since $\eta^+ = 3-w$ and $F_{1,2} = (4-w)$. $\square$

The divisors of 2. We finally come to the missing prime ideal divisors of 2.

Lemma 4.17. *If 2 splits, let $\mathfrak{p}_2 = (2, \eta^-)$ and let $h \subset \mathcal{O}_D$ be an arbitrary ideal with $(h, 2) = 1$. If $L_d \in \mathcal{A}_d$, then*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(2h)\right] = 6$$

and

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p}_2)\right] = 2.$$

Proof. It can easily be checked that the matrices $T^H, Z^H, Z^H T^H, E^H, E^H T^H$ are inequivalent modulo $\Gamma_0^D(2h)$. By Weitze-Schmithüsen's Theorem respectively Corollary 1.2, we have that the index is divisible 2 and that it is at most 6. Thus the claim follows. $\square$

Lemma 4.18. *If $2|d$ then*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(2h)\right] = 4.$$

Proof. The matrices $T^H, Z^H, Z^H T^H$ are inequivalent modulo $\Gamma_0^D(2h)$, the index is divisible by 2 and at most 4. $\square$

This finishes the proof of Theorem 4.1, (1) and (3).

The most special case is the case where d is odd and $L_d \in \mathcal{B}_d$. Then $m = 3$ and $\eta^- = 3 - w$. Since the norm of η^- is positive we have that $\mathfrak{p}_2^\sigma | 3 - w$ (but $\mathfrak{p}_2 \nmid 3 - w$). So we are now only interested in $\Gamma_0^D(\mathfrak{p}_2^\sigma)$.

Remark 4.19. *By considering the matrix F we immediately see that for all ideals $h \subset \mathcal{O}_D$ with $(h, \mathfrak{p}_2) = 1$*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p}_2^\sigma)\right] \geq 2$$

holds if $L_d \in \mathcal{B}_d$.

So it remains to show that the index is not greater than 2. To prove this, it is convenient to consider the subgroup $\mathrm{SL}^1(L_D) \cap \Gamma^D(2)$ instead and to show that this index is at most $\frac{1}{3}[\mathrm{SL}_2(\mathcal{O}_D) : \Gamma^D(2)]$. By projection on the second factor of the homology Veech group and by the arguments given in the proof of [WS12, Theorem 3 (ii)] it suffices to show that one of the non-integral Weierstraß points on E_2 can be distinguished from the others. This is clear by Theorem 3.9 since E_2 has only one integral Weierstraß point. Thus we have proven:

Proposition 4.20. *We have*

$$\left[(\mathrm{SL}^1(L_d) : (\mathrm{SL}^1(L_d) \cap \Gamma^D(2)\right] \leq \frac{1}{3}[\mathrm{SL}_2(\mathcal{O}_D) : \Gamma^D(2)]$$

if $L_d \in \mathcal{B}_d$.

Corollary 4.21. *For all ideals $h \subset \mathcal{O}_D$ with $(h, \mathfrak{p}_2^\sigma) = 1$*

$$\left[(\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h) : (\mathrm{SL}^1(L_d) \cap \Gamma_0^D(h\mathfrak{p}_2^\sigma)\right] = 2$$

holds if $L_d \in \mathcal{B}_d$.

This finishes the proof of Theorem 4.1, (2).

A Appendix

In the appendix we collect some results on quadratic orders $\mathcal{O}_D$ of square discriminant. In particular, we will give proofs of the results mentioned in the main part of the paper.

Norm and trace. Analogously as in the non-square case we have:

Remark A.1. *An element $z \in K$ is in $\mathbb{Q}$ if and only if $z = z^\sigma$, since $\mathcal{O}_D$ is diagonally embedded into K.*

Recall that if D is square-free, then the order $\mathcal{O}_D$ is the ring of integers of $K = \mathbb{Q}(\sqrt{D})$ and an element $z \in K$ is in $\mathcal{O}_D$ if and only both trace and norm of z lie in $\mathbb{Z}$.[1] In accordance with this property, a similar property does also hold if D is the square of a prime number. We can however not expect that $z \in \mathcal{O}_D$ if and only if $\mathrm{tr}(z)$ and $\mathcal{N}(z)$ are in $\mathbb{Z}$, as we can see by the example $d = 5$ and $z = (1, 2)$. Indeed, one has to additionally impose some congruence conditions on the trace and the norm.

Lemma A.2. *Let $z \in K$. If $D = d^2$ and d has no prime divisor of order greater than 1, then $z \in \mathcal{O}_D$ if and only if $\mathrm{tr}(z), \mathcal{N}(z) \in \mathbb{Z}$ and $\mathrm{tr}(z) \equiv 2v \mod d$ and $\mathcal{N}(z) \equiv v^2 \mod d$ for some $v \in \mathbb{Z}$.*

Proof. If $z \in \mathcal{O}_D$ then $z = (x, y)$ for some $x, y \in \mathbb{Z}$. Then $\mathrm{tr}(z) = (x+y, x+y)$ and $\mathcal{N}(z) = (xy, xy)$ and hence $\mathrm{tr}(z), \mathcal{N}(z) \in \mathbb{Z}$. Moreover $x \equiv y \mod d$ implies that $x + y \equiv 2x \mod d$ and $xy \equiv x^2 \mod d$.
On the other hand, let $z = (x, y)$ for some $x, y \in \mathbb{Q}$ and let $\mathrm{tr}(z)$ and $\mathcal{N}(z)$ be in $\mathbb{Z}$. Since $x + y$ and xy are both in $\mathbb{Z}$ and therefore both x and y are in $\mathbb{Z}$. Then $\mathrm{tr}(z) \equiv 2v \mod d$ implies that $y \equiv 2v - x \mod d$. Inserting this into $\mathcal{N}(z) \equiv v^2 \mod d$ gives $(x - v)^2 \equiv 0 \mod d$. Since d has no quadratic term we have $x \equiv v \mod d$ and thus $x \equiv y \mod d$. □

Noetherian rings. We now want to prove that $\mathcal{O}_D$ is a Noetherian ring as in the case of non-square-discriminants. For this it suffices to prove, that $\mathcal{O}_D$ is a finitely generated $\mathbb{Z}$-module.

Lemma A.3. *The ring $\mathcal{O}_D$ is finitely generated as $\mathbb{Z}$-module. We call $\mathbb{1} = (1, 1)$ and $w = (0, d)$ the **standard basis** of $\mathcal{O}_D$.*

Proof. One easily checks that $(\mathbb{1}, w)$ is indeed a basis of $\mathcal{O}_D$ as $\mathbb{Z}$-module. □

Proposition A.4. *The quadratic order $\mathcal{O}_D$ is Noetherian.*

Ideals. So far, the notion of the norm has only been defined for elements in K but not for ideals. Note that one may define ideals in $\mathcal{O}_D$, prime ideals, maximal ideals and so on in the usual way. It follows from Proposition A.4 and Krull's Hauptidealsatz that every prime ideal in $\mathcal{O}_D$ is also maximal (see e.g. [Har77, Theorem 1.11A]). For an element $z \in \mathcal{O}_D$ we define the **principal ideal** generated by z by:

$$(z) := z\mathcal{O}_D := \{za | a \in \mathcal{O}_D\}.$$

[1] This in not true any more if D is not square-free as the example $D = 45$ and $z = (2 + 5w)/3$ shows.

Now let $(0) \neq \mathfrak{a} \subset \mathcal{O}_D$ be an arbitrary ideal in $\mathcal{O}_D$. Then its norm $\mathcal{N}(\mathfrak{a})$ is defined as the number of the elements in $\mathcal{O}_D/\mathfrak{a}$ if this quotient is finite. If the quotient is infinite we set $\mathcal{N}(\mathfrak{a}) := 0$. In particular, if $z \in \mathcal{O}_D$ is 0 or a zero divisor we then have $\mathcal{N}((z)) = 0$. The definition perfectly generalizes the norm of an element:

Lemma A.5. *For $z \in \mathcal{O}_D$ we have $\mathcal{N}((z)) = \mathcal{N}(z)$. In particular, we have $\mathcal{N}((z)) = z^2$ for all $z \in \mathbb{Z}$.*

Proof. Let $z = (x, y)$, $u = (p, q)$, $v = (r, s)$ be three elements in $\mathcal{O}_D$. Then $(p, q) - (r, s) = (p - r, q - s) \in (z)$ if and only if $x|(p - r)$ and $y|(q - s)$. Hence there are $x \cdot y$ elements in $\mathcal{O}_D/(z)$ and thus the two a priori different definitions of the norm agree. $\square$

The Lasker-Noether theorem. Recall that a **Dedekind ring** is an one-dimensional, Noetherian, normal integral domain. In a Dedekind ring one always has unique prime factorization in the sense of ideals. Note however that $\mathcal{O}_D$ is never a Dedekind ring since it is not an integral domain. Nevertheless, there remains a very important tool, namely the Lasker-Noether factorization, because $\mathcal{O}_D$ is Noetherian. In order to understand its importance one has to introduce primary ideals first. A **primary ideal** is a proper ideal $\mathfrak{a}$ such that whenever $xy \in \mathfrak{a}$ with $x, y \in \mathcal{O}_D$ either x or y^n is in $\mathfrak{a}$ for some $n \in \mathbb{N}$. The most important class of examples of primary ideals are evidently prime ideals. A primary ideal $\mathfrak{a} \subset \mathcal{O}_D$ is a prime ideal if and only if it is **semiprime**, i.e. if $x^k \in \mathfrak{a}$ for $x \in \mathcal{O}_D$ and $k \in \mathbb{N}$ then $x \in \mathfrak{a}$. This implies that there might (and there actually do) exist primary ideals in $\mathcal{O}_D$ which are not prime. If $\mathfrak{a}$ is a primary ideal, then its radical $\sqrt{\mathfrak{a}}$ is a prime ideal and it is customary to say that $\sqrt{\mathfrak{a}}$ is the prime ideal **associated** to $\mathfrak{a}$.

Definition A.6. *Let $\mathfrak{a} \subset \mathcal{O}_D$ be an ideal. Then a tuple $(\mathfrak{a}_1, ..., \mathfrak{a}_k)$ is said to be a **primary decomposition** of $\mathfrak{a}$ if all the $\mathfrak{a}_i$ are primary ideals and $\mathfrak{a} = \mathfrak{a}_1 \cap ... \cap \mathfrak{a}_k$. The decomposition is called **minimal** (or **irredudant**) if we further get: For all $j = 1, ..., k$ we have $\mathfrak{a} \neq \cap_{i \neq j} \mathfrak{a}_i$ and for $i \neq j$ we have $\sqrt{\mathfrak{a}_i} \neq \sqrt{\mathfrak{a}_j}$.*

Primary ideals are so to say what one has to buy whenever a Noetherian ring is not Dedekind.

Theorem A.7. ***(Lasker, Noether)*** *Let $\mathfrak{a} \neq \mathcal{O}_D$ be an ideal in $\mathcal{O}_D$. Then it admits a minimal primary decomposition and in this decomposition the associated prime ideals are uniquely determined by $\mathfrak{a}$.*

Primary principal ideals. The Lasker-Noether theorem suggests that it is important to detect the primary ideals among the ideals of $\mathcal{O}_D$. This will be done now. Let us start with principal ideals.

Proposition A.8. *Let $(z) = ((x, y))$ be a principal ideal. Then (z) is a primary ideal if and only if $x = p^e$ and $y = p^f$ for a prime number $p \in \mathbb{Z}$ and $e, f \in \mathbb{N}$.*

Proof. Let $x = p_1^{e_1} \cdots p_n^{e_n}$ and $y = q_1^{f_1} \cdots q_m^{f_m}$ be the prime decompositions of x and y. If (z) is a primary ideal then $(a, b)(c, d) \in (z)$ implies that $(a, b) \in (z)$ or $(c, d)^n \in (z)$. In particular we must have that $x|ac$ yields $x|a$ or $x|c^n$. This implies that $x = p^e$ with p a prime number and $e \in \mathbb{N}$. The same reasoning shows that $y = q^f$ with q a prime number and $f \in \mathbb{N}$. Now assume that $p \neq q$. Then we choose $(a, b) = (p^e, p^e) \in \mathcal{O}_D$ and $(c, d) = (q^f, q^f) \in \mathcal{O}_D$. Then $(a, b)(c, d)$ lies in $((x, y))$ but neither $(a, b)^n$ nor $(c, d)^n$ does. This is a contradiction. On the other hand, it is clear that the tuple (p^e, p^f) with $d|p^e - p^f$ defines a primary ideal. $\square$

Ideals as modules. Let us now describe all ideals in $\mathcal{O}_D$. Recall that every ideal of $\mathcal{O}_D$ is also a $\mathbb{Z}$-module. The point of view that ideals are modules will be very useful for giving a list of primary ideals. Moreover it allows us to calculate the spectrum of $\mathcal{O}_D$. As in the case of non-square discriminants, it is essential to see that every $\mathbb{Z}$-module in $\mathcal{O}_D$ is generated by at most two elements.

Proposition A.9. *Let $M \subset \mathcal{O}_D$ be a $\mathbb{Z}$-module in $\mathcal{O}_D$. Then there exist integers $m, n \in \mathbb{Z}_{\geq 0}$ and $a \in \mathbb{Z}$ such that*

$$M = [n\mathbb{1}; a\mathbb{1} + mw] := n\mathbb{1}\mathbb{Z} \oplus (a\mathbb{1} + mw)\mathbb{Z}.$$

Proof. Consider the subgroup $H := \{s \in \mathbb{Z} : r\mathbb{1} + sw \in M\}$ of $\mathbb{Z}$. As H is a subgroup of $\mathbb{Z}$, it is of the form $m\mathbb{Z}$ for some $m \geq 0$. By construction, there exists an $a \in \mathbb{Z}$ with $a\mathbb{1} + mw \in M$. Furthermore we know that $M \cap \mathbb{Z}\mathbb{1}$ can be regarded a subgroup of $\mathbb{Z}$ and so $M \cap \mathbb{1}\mathbb{Z} = n\mathbb{1}\mathbb{Z}$ for some $n \geq 0$. We claim that $M = n\mathbb{1}\mathbb{Z} \oplus (a\mathbb{1} + mw)\mathbb{Z}$. The inclusion $\supseteq$ is evident. Hence let us assume that $r\mathbb{1} + sw \in M$. Since $s \in H$ we have $s = um$ for some $u \in \mathbb{Z}$, and thus

$$r\mathbb{1} - ua\mathbb{1} = r\mathbb{1} + sw - u(a\mathbb{1} + mw) \in M \cap \mathbb{1}\mathbb{Z}.$$

Hence $r - ua = nv$. But then

$$r\mathbb{1} + sw = (r - ua)\mathbb{1} + u(a\mathbb{1} + mw) = nv\mathbb{1} + u(a\mathbb{1} + mw) \in n\mathbb{1}\mathbb{Z} \oplus (a\mathbb{1} + mw)\mathbb{Z}.$$

$\square$

As it does simplify the notation and cannot cause any confusion we will from now on leave away the symbol $\mathbb{1}$ when we want to embed $\mathbb{Z}$ into $\mathcal{O}_D$. In other words, we write every $\mathbb{Z}$-module in $\mathcal{O}_D$ as $[n; a + mw]$ for some $a, n, m \in \mathbb{Z}$.

As every ideal of $\mathcal{O}_D$ is also $\mathbb{Z}$-module, it is generated by at most two elements. The converse is not true since e.g. $M = [1; 0] = \mathbb{Z}$ is a $\mathbb{Z}$-submodule of $\mathcal{O}_D$, but not an ideal. We therefore now describe under which conditions on a, m, n the $\mathbb{Z}$-module M is also an ideal. These conditions are just the same as in the case of non-square discriminants.

Proposition A.10. *A nonzero $\mathbb{Z}$-module $M = [n; a+mw]$ is an ideal if and only if $m|n$, $m|a$, i.e. $a = mb$ for some $b \in \mathbb{Z}$, and $n|m\mathcal{N}(b+w)$.*

Proof. Suppose that M is an ideal. We consider the group H from the proof of Proposition A.9. Then $c \in M \cap \mathbb{Z}$ implies $cw \in M$ and hence $c \in H$. This shows that $n\mathbb{Z} = M \cap \mathbb{Z} \subset H = m\mathbb{Z}$ or in other words that $m|n$. Observe that $w^2 = dw$. Since M is an ideal, $a + mw \in$ M implies that $(a + mw)w = (a + md)w \in M$. By the definition of H we therefore have that $a \in H$ and hence $m|a$. Finally we put $\beta := a + mw = m(b + w)$. Then $\beta \in M$ implies $\beta(b + w^\sigma) \in M$. Hence $n|m\mathcal{N}(b + w)$.
Now suppose that all the divisibility relations are fulfilled by M. We only have to show that nw and $(a + mw)w$ both lie in M. We have

$$nw = \frac{n}{m}mw = \frac{n}{m}(a + mw) - \frac{n}{m}a = \frac{n}{m}(a + mw) - bn$$

and so $nw \in M$ since $m|n$. And

$$(a + mw)w = aw + mw^2 = (a + md)w = (b + d)(a + mw) - ((b + d)bm) =$$
$$(b + d)(a + mw) - m\mathcal{N}(b + d)$$

implies that $(a + mw)w \in M$ since $n|m\mathcal{N}(b + w)$. □

This proposition gives a nice possibility to calculate the norm of an arbitrary ideal $\mathfrak{a} = [n; a + mw]$: it is straightforward to check (by giving an explicit list of representatives) that $\mathcal{N}(\mathfrak{a}) = mn$. Note that if $M = [n; a+mw]$ is an ideal then its conjugated module is given by $[n; a + mw]^\sigma = [n; a + md - mw]$ which does not need to be an ideal even if M was an ideal, i.e. ideals are not closed under conjugation although the conjugated module has the same norm as M.[2] On the other hand, if $\mathfrak{a} = ((x, y))$ is a principal ideal then also $\mathfrak{a}^\sigma = ((y, x))$ is a principal ideal. Furthermore one immediately sees:

Corollary A.11. *Every ideal of prime norm p is of the form $[p; a + w]$ for some $a \in \mathbb{Z}$ with $p|\mathcal{N}(a + w)$. These ideals are indeed prime ideals.*

Proof. The first assertion is clear from Proposition A.10. The second assertion follows since $[p; a + w]$ is contained in a prime ideal $\mathfrak{p}$ since all prime ideals are maximal. As p is a prime number, the quotient $\mathcal{O}_D/\mathfrak{p}$ must either have p or 1 elements. Therefore we must either have $[p; a+w] = \mathfrak{p}$ or $\mathfrak{p} = \mathcal{O}_D$. Hence $[p; a + w]$ is a prime ideal. □

[2] An example for this to happen is $\mathcal{O}_9$ and $M = [25, 25 + 5w]$.

This corollary shows that there does not exist any inert prime number if D is a square because it is always possible to find an $a \in \mathbb{Z}$ such that $p|\mathcal{N}(a+w)$, i.e. $a = p$. We are now even able to count the number of different prime ideals of norm p if p is a prime number. This is an important step towards a ramification theory of prime numbers over $\mathcal{O}_D$.

Proposition A.12. *Let $p \in \mathbb{Z}$ be a prime number. If $p|D$ then there exists exactly one prime ideal $\mathfrak{a}$ of norm p and $\mathfrak{a}^\sigma = \mathfrak{a}$. Otherwise there exist exactly two different prime ideals $\mathfrak{a}, \mathfrak{b}$ of norm p and $\mathfrak{a}^\sigma = \mathfrak{b}$.*

Proof. Let $p \in \mathbb{Z}$ be a prime number with $p|D$. Then every ideal of norm p is of the form $\mathfrak{a} = [p; a+w]$ with $p|a(a+d)$. As $p \in \mathfrak{a}$ we may without loss of generality assume that $1 \leq a \leq p$. Since $p|d$ we always have $p|a$ and therefore $a = p$. So there exists exactly one ideal of norm p if $p|d$. It is then clear that $\mathfrak{a}^\sigma = \mathfrak{a}$.
If $p \in \mathbb{Z}$ is a prime number with $p \nmid d$ then we may again assume that $1 \leq a \leq p$. So there remain the two possibilities $p|a$ and $p|(a+d)$. These ideals $\mathfrak{a}$ and $\mathfrak{b}$ are indeed different since $p \nmid d$ and one can immediately check that $\mathfrak{a}^\sigma = \mathfrak{b}$. □

We can also characterize primary ideals.

Proposition A.13. *If $\mathfrak{a} = [n; a+mw]$ is a primary ideal if and only if it is an ideal and $\mathcal{N}(\mathfrak{a}) = p^l$ for some prime number $p \in \mathbb{Z}$ and some $l \in \mathbb{N}$, i.e. $m = p^k$ and $n = p^{l-k}$ for a $k \in \mathbb{Z}$ with $0 \leq k \leq l/2$.*

Proof. Assume that $\mathfrak{a}$ is a primary ideal. Then $m \neq 0$. Since $m|n$ and $\mathcal{N}(\mathfrak{a}) = nm$, it suffices to show that n has a unique prime divisor. Assume that $n = p_1^{e_1} \cdots p_r^{e_r}$ with $r \geq 2$. Then $p_1^{e_1} \cdot (p_2^{e_2} \cdots p_r^{e_r}) \in \mathfrak{a}$ but neither the first factor nor any power of the second factor is in $\mathfrak{a}$ as one sees by regarding $\mathfrak{a}$ as $\mathbb{Z}$-module. This is a contradiction.

Now assume that $\mathfrak{a}$ is an ideal and fulfills the above relations. If $k \neq 0$ then $ef \in \mathfrak{a}$ if and only if either e or f is divisible by p (because $p^k|a$). Hence $\mathfrak{a}$ is primary. If $k = 0$ then $p^l|\mathcal{N}(a+w)$, i.e. p divides a or $a+d$. We now have to distinguish two cases, namely $p \nmid d$ and $p|d$.
Let us first assume that $p \nmid d$. Then p^l either divides a or $a+d$, i.e. not both of them at the same time. Let us assume that $p^l|(a+d)$ and let $e = (e_1, e_2), f = (f_1, f_2) \in \mathcal{O}_D$ with $ef \in \mathfrak{a}$. Since $\mathfrak{a} = [p^l; a+w]$ we hence have that $p|e_2$ or $p|f_2$. We may without loss of generality assume that $p|f_2$. By passing to powers of f if necessary, we may furthermore assume that $f_2 = p^l r$ with $r \in \mathbb{Z}$. Moreover we know that $a + d = p^l z$ for some $z \in \mathbb{Z}$ and that $f_1 = p^l r + sd$ for some $s \in \mathbb{Z}$. We now want to show that $f = (f_1, f_2)$ lies in $\mathfrak{a}$. To see this, we look at the equation (in the usual coordinates of $\mathcal{O}_D$)

$$x(p^l, p^l) + y(zp^l - d, zp^l) = (p^l r + sd, p^l r).$$

As we want to see that $(f_1, f_2) \in \mathfrak{a}$ we have to show that $x, y \in \mathbb{Z}$. The first coordinate yields $x = r - yz \in \mathbb{Z}$. Inserting this into the second coordinate we get that $y = -s \in \mathbb{Z}$ and hence the claim. If $p^l | a$ the proof works analogously.
Secondly assume that $p|d$. Then $p|a$ and $p|a+d$ since $p|\mathcal{N}(a+w) = a(a+d)$. Let $e = (e_1, e_2), f = (f_1, f_2) \in \mathcal{O}_D$ with $ef \in \mathfrak{a}$. Since $p|a$ we may then assume that $p|f_1$. But then also $p|f_2$ since $f_2 = f_1 + kd$. After passing to powers if necessary we hence have $p^l|f_1$ and $p^l|f_2$ and so $f \in \mathfrak{a}$. □

Ramification. We may now deduce the ramification theory for prime numbers over $\mathcal{O}_D$. In order to do this, we have to better understand how to multiply two prime ideals. Let us first assume that p is a prime number with $p|d$ and let $\mathfrak{a} = [p, p+w]$ be the unique prime ideal of norm p. Then $\mathfrak{a}^2 = [p, p+w][p, p+w] = [p^2, p^2 + pw]$. This implies that p with $p|d$ cannot be written as the product of two prime ideals and that $\mathcal{N}(\cdot)$ is in general not multiplicative. If $p \nmid d$ then let $\mathfrak{a} = [p, p+w]$ and $\mathfrak{b} = [p, p-d+w]$ be the two different ideals of norm p. Then $\mathfrak{a}\mathfrak{b} = [p, p+w][p, p-d+w] = [n, a+mw]$ and

$$(ep + f(p+w))(gp + h(p-d+w)) =$$
$$p\left((g+h)(e+f)p - h(e+f)d\right) + (eh + gf + 2fh)pw.$$

and therefore $m = p$. Since $(p, d) = 1$ we must evidently have that $\mathfrak{a}\mathfrak{b} \cap \mathbb{Z} = p\mathbb{Z}$ and hence $n = p$ and by Proposition 2.3 that $a = pc$ with $c \in \mathbb{Z}$. Since $p \in \mathfrak{a}\mathfrak{b}$ we may therefore choose $a = p$, i.e. $\mathfrak{a}\mathfrak{b} = [p, p(1+w)]$. On the other hand we have $[p, p(1+w)] = (p)$ and hence we have established:

Theorem A.14. *Let $p \in \mathbb{Z}$ be a prime number.*

(i) If $p \nmid d$ then $(p) = \mathfrak{a}\mathfrak{a}^\sigma$ for a prime ideal $\mathfrak{a}$ of norm p, i.e. p splits.

(ii) If $p|d$ then (p) is an irreducible ideal which is not prime.

Corollary A.15. *Let $n \in \mathbb{Z}$ be an arbitrary number with $(n, d) = 1$. Then the principal ideal (n) can be uniquely written as a product of prime ideals.*

Proof. We decompose $n = p_1^{e_i} \cdots p_l^{e_l}$ in $\mathbb{Z}$. Then each p_i can be written as the product of two prime ideals $(p) = \mathfrak{a}\mathfrak{a}^\sigma$ by Theorem 2.6. Hence the claim follows. □

If $\mathfrak{a} = ((x, y))$ is a principal ideal then also $\mathfrak{a}^\sigma = ((y, x))$ is a principal ideal and $\mathfrak{a}\mathfrak{a}^\sigma = \mathcal{N}((x, y))\mathcal{O}_D$. Thus for $(x, y) \in \mathcal{O}_D$ with $(d, \mathcal{N}((x, y)) = 1$ we may write

$$\mathfrak{a}\mathfrak{a}^\sigma = \prod_i \mathfrak{p}_i^{e_i} \mathfrak{p}_i^{e_i \sigma}$$

where all the $\mathfrak{p}_i$ are prime ideals as in Corollary A.15. Let us first assume that $(x, y) = 1$. Then either $\mathfrak{p}_i^{e_i}$ or $\mathfrak{p}_i^{e_i\sigma}$ divides $\mathfrak{a}$ but not both of them.

Therefore we can find a unique decomposition of $((x, y))$ into prime ideals. If $(x, y) = n$ then $((x, y)) = ((n, n))((x', y'))$ with $(x', y') = 1$. Hence we have established:

Corollary A.16. *Let $z \in \mathcal{O}_D$ be an arbitrary element with* $\gcd(d, \mathcal{N}(z)) = 1$. *Then the principal ideal (z) can be uniquely written as a product of prime ideals.*

Let us say a few words about ideals generated by elements $z \in \mathcal{O}_D$ with $\gcd(d, \mathcal{N}(z)) \neq 1$. On the one hand we might have $z \in \mathbb{Z}$ with $z|d$. Then one can uniquely write z as a product of prime numbers $p_i \in \mathbb{Z}$ and each of these p_i defines an irreducible ideal by Theorem 2.6. However, there also exist irreducible ideals generated by $z \in \mathcal{O}_D$ with $z \nmid d$. An example for this to happen is $d = 2$ and $z = (4, 6)$. Then $2 \nmid z$ since $(2, 3) \notin \mathcal{O}_4$ and so (z) is an irreducible ideal.

Finally, we compose all the results which we have achieved in a table which compares the case of square discriminants to non-square discriminants. Let f be a square-free positive integer and $d \in \mathbb{N}$ be arbitrary.

	$D = f$	$D = d^2 f$	$D = d^2$
Structure of $\mathcal{O}_D$	Dedekind	Noetherian Integral domain	Noetherian
Prime decomposition	All ideals	Ideals with $(\mathcal{N}(\mathfrak{a}), d) = 1$	Ideals with $(\mathcal{N}(\mathfrak{a}), d) = 1$
Ramification of primes with $(d, p) = 1$	Ramifation law	Ramification law	all primes splitting

Lasker-Noether factorization. We now come back to the factorization of an arbitrary (principal) ideal into primary ideals. Let us at first look at the two examples:

Example A.17. *(i) Consider $\mathcal{O}_{16}$ and the principal ideal $\mathfrak{a} = ((3, 7))$. Since $\mathfrak{a} \cap \mathbb{Z} = 21\mathbb{Z}$ and since the norm $\mathcal{N}(\mathfrak{a}) = 21$ we must have $n = 21, m = 1$ and since $3 + w \in \mathfrak{a}$ we get $a = 3$. Hence*

$$\mathfrak{a} = [21; 3 + w]$$

From this it is evident that the Lasker-Noether decomposition is

$$\mathfrak{a} = [7; 3 + w] \cap [3; 3 + w].$$

(ii) We now look at the principal ideal $\mathfrak{a} = ((2, 6)) = (2+w)$. There happens something quite different from the first example, namely $\mathfrak{a} \cap \mathbb{Z} = 12\mathbb{Z}$. Then we get $m = 2$ and $a = 2$. Thus

$$\mathfrak{a} = [12; 2 + w]$$

and the primary decomposition is

$$\mathfrak{a} = [4; 2 + w] \cap [3; 2 + w].$$

Let us deduce from this the general recipe how to find the Lasker-Noether decomposition of any principal ideal in $\mathcal{O}_D$: let $(e + fw) = ((e, e + fd))$ be an arbitrary principal ideal. The norm of $(e + fw)$ is $e(e + fd)$. Let us now calculate n. We have $(e, e + fd)(x, x + dy) = (ex, ex + fdx + fd^2y + edy)$. Since we want to calculate $M \cap \mathbb{Z}$ we set $fdx + fd^2y + edy = 0$ to get $x = -y\frac{e+fd}{f}$. Hence $n = \frac{e(e+fd)}{\gcd(e,f)}$ and $m = \gcd(e, f)$. From this data it is now possible to also calculate $a = \gcd(e, f)b$ (a more precise expression for a would be hardly of any use in the following). So we may assume that

$$\mathfrak{a} = \left[\frac{e(e + fd)}{\gcd(e, f)}; \gcd(e, f)(b + w)\right].$$

Let $m = \gcd(e, f) = p_1^{e_1} \cdots p_r^{e_r}$ and $n = p_1^{f_1} \cdots p_r^{f_r} \cdot q_1^{g_1} \cdots q_s^{g_s}$ be the prime decomposition of m and n. Then the Lasker-Noether decomposition of $\mathfrak{a}$ is

$$\mathfrak{a} = \bigcap_{i=1}^{r} \left[p_i^{f_i}; p_i^{e_i}(b + w)\right] \bigcap_{j=1}^{s} \left[q_j^{g_j}; (b + w)\right].$$

The special linear group. Here we just prove the claim of Proposition 2.8 with the help of the following two lemmas.

Lemma A.18. *Let R, S be two commutative rings such that there exists a surjective homomorphism of rings $f : S \to R$. If $\mathrm{SL}_2(R)$ is generated by elementary matrices then the induced map $\mathrm{SL}_2(S) \to \mathrm{SL}_2(S)$ is also surjective.*

Proof. Any elementary matrix over R lifts to an elementary matrix of S. □

Lemma A.19. *If R is a finite commutative ring, then $\mathrm{SL}_2(R)$ is generated by elementary matrices.*

Proof. Every finite commutative ring is a direct product of local rings. Since the claim is true for local rings (see e.g. [Ros94, Chapter 2.2]) this finishes the proof. □

Proof (of Proposition 2.8). By definition $\Gamma^D(\mathfrak{a})$ is the kernel of the projection $\mathrm{SL}_2(\mathcal{O}_D) \to \mathrm{SL}_2(\mathcal{O}_D/\mathfrak{a})$. The projection map is surjective by the preceding two lemmas. □

References

[Bai07] Bainbridge, M. “Euler Characteristics of Teichmüller Curves in genus two”, Geometry & Topology 11, 1887-2013 (2007).

[BL04] Birkenhake, C., Lange, H., "Complex Abelian Varieties", Springer, Berlin Heidelberg New York (2004).

[ER12] Ellenberg, J., McReynbolds D., “Arithmetic sublattices of $SL(2, \mathbb{Z})$, Duke Math. J., 161(3), 415-429 (2012).

[FK92] Farkas, H., Kra, I., "Riemann Surfaces", Springer, Berlin Heidelberg New York (1992).

[Har77] Hartshorne, D., “Algebraic Geometry”, Springer, Berlin Heidelberg New York (1977).

[HL06] Hubert, P. and Lelièvre, S., “Prime arithmetic Teichmüller discs in $\mathcal{H}(2)$”, Israel Journal of Mathematics 151, 501-526 (2006).

[Kan03] Kani, E., “Hurwitz spaces of genus 2 covers of an elliptic curve”, Collect. Math., 54(1), 1-51 (2003).

[Kap11] Kappes, A., "Monodromy Representations and Lyapunov Exponents of Origamis", *PhD-thesis*, Karlsruhe (2011).

[Kil08] Kilford, L.J.P., "Modular forms - A classical and computational introduction", Imperial College Press, London (2008).

[Kuh88] Kuhn, R., “Curves of genus 2 with split Jacobians”, Trans. of the AMS, 307(1), 41-49 (1988).

[McM03] McMullen, C., "Billiards and Hilbert modular surfaces", J. Amer. Math. Soc., 16 (4), 857-885 (2003).

[McM05] McMullen, C., "Teichmüller curves in Genus Two: Discriminant and Spin", Math Ann., 333, 87-130 (2005).

[Möl05] Möller, M., “Teichmüller curves, Galois actions and GT-relations”, Math. Nachrichten 278 No. 9 (2005).

[Möl11] Möller, M., "Teichmüller Curves from the Viewpoint of Algebraic Geometry", *preprint* (2011).

[MZ11] Möller, M., Zagier D.B., "Theta derivatives and Teichmüller curves", *preprint* (2011).

[Muk11] Mukamel, R., “Orbifold points on Teichmüller curves and Jacobians with complex multiplication”, *PhD-thesis*, Harvard (2011).

[Nor87] Nori, M., “On subgroups of $\mathrm{GL}_n(F_p)$”, Invent. math. 88, 257-275 (1987).

[Rap12] Rapinchuk, A, “On strong approximation for algebraic groups”, *preprint*, arXiv:1207.4425 (2012).

[Ros94] Rosenberg, J., “Algebraic K-Theory and its applications”, Springer, Berlin Heidelberg New York (1994).

[Vee89] Veech, W.A., "Teichmüller curves in moduli space, Eisenstein series and an application to triangular billiards", Invent. Math., 97 (3), 553-583 (1989).

[Wei08] Weiß, C., "Hecke Operators and Orthogonality on $\Gamma_1[N]$", *diploma thesis*, Heidelberg (2008).

[Wei12] Weiß, C., "Twisted Teichmüller curves", *PhD-thesis*, Frankfurt (2012).

[WS12] Weitze-Schmithüsen, G., "The deficiency of being a congruence group for Veech groups of Origamis", arXiv:1208.1936 (2012).

Goethe-Universtität Frankfurt, Institut für Mathematik, Robert-Mayer-Str. 6-8, D-60325 Frankfurt (Main)
E-mail address: weiss@math.uni-frankfurt.de