PLANES IN FOUR SPACE AND FOUR ASSOCIATED CM POINTS

MENNY AKA, MANFRED EINSIEDLER, AND ANDREAS WIESER

ABSTRACT. To any two-dimensional rational plane in four-dimensional space one can naturally attach a point in the Grassmannian $\mathrm{Gr}(2,4)$ and four lattices of rank two. Here, the first two lattices originate from the plane and its orthogonal complement and the second two essentially arise from the accidental local isomorphism between $\mathrm{SO}(4)$ and $\mathrm{SO}(3)\times\mathrm{SO}(3)$. As an application of a recent result of Einsiedler and Lindenstrauss on algebraicity of joinings we prove simultaneous equidistribution of all of these objects under two splitting conditions.

1. Introduction

For a rational two-dimensional subspace L of $\mathbb{R}^4$ we define the discriminant of L as the square of the covolume of $L\cap\mathbb{Z}^4$ in L, i.e.

$$\mathrm{disc}(L)=\mathrm{vol}(L/L\cap\mathbb{Z}^4)^2\in\mathbb{N}.$$

For any $D\in\mathbb{N}$ we let $\mathcal{R}_D$ be the finite set of rational planes of discriminant D, which is a subset of the real Grassmannian $\mathrm{Gr}_{2,4}(\mathbb{R})$. The set $\mathcal{R}_D$ is non-empty if and only if

$$D\in\mathbb{D}:=\{D\in\mathbb{N}\mid D\not\equiv 0,7,12,15 \bmod 16\}.$$

This statement should be seen as an analogue of Legendre's theorem for sums of three squares and relates to works of Mordell [Mor32, Mor37] and Ko [Ko37] on representations of binary forms as sums of four squares.

We let $\mathbb{H}^2$ denote the hyperbolic plane and call the quotient $\mathrm{SL}_2(\mathbb{Z})\setminus\mathbb{H}^2$ the modular surface. Note that

$$\mathcal{X}_2:=\mathrm{PGL}_2(\mathbb{Z})\backslash\mathbb{H}^2=\mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R})/\mathrm{PO}(2)$$

is a two-to-one quotient of the modular surface obtained by using the orientation reversing reflection $z\in\mathbb{H}^2\mapsto-\overline{z}$ through the imaginary axis.

To each $L\in\mathcal{R}_D$ we will naturally attach a four-tuple $(z_1^L,z_2^L,z_3^L,z_4^L)$ of CM-points on $\mathcal{X}_2$. We conjecture that the set

$$\mathcal{J}_D=\left\{(L,z_1^L,z_2^L,z_3^L,z_4^L)\mid L\in\mathcal{R}_D\right\}$$

is equidistributing to the natural uniform measure on the product space

$$\mathrm{Gr}_{2,4}(\mathbb{R})\times\mathcal{X}_2^4$$

when $D\to\infty$ with $D\in\mathbb{D}$. In this paper we prove this conjecture under additional congruence conditions. In particular, our result implies the conjecture on average.

Date: July 10, 2019.
The authors were supported by the SNF (grants 152819 and 178958).

Let us now describe the points z_i^L for $i=1,2,3,4$ in more details. First, consider for any rational plane L the two-dimensional lattices

$$L(\mathbb{Z}) := L \cap \mathbb{Z}^4, \quad L^\perp(\mathbb{Z}) := L^\perp \cap \mathbb{Z}^4.$$

In order to compare these lattices for different planes, we now choose a rotation $k_L \in \mathrm{SO}_4(\mathbb{R})$ moving L to $\mathbb{R}^2 \times \{(0,0)\} \subseteq \mathbb{R}^4$ and $L^\perp$ to $\{(0,0)\} \times \mathbb{R}^2$. The shape $[L(\mathbb{Z})]$ (resp. $[L^\perp(\mathbb{Z})]$) is then defined to be the homothety class of the lattice $k_L.L(\mathbb{Z}) \subseteq \mathbb{R}^2 \times \{(0,0)\}$ (resp. $k_L.L^\perp(\mathbb{Z}) \subseteq \{(0,0)\} \times \mathbb{R}^2$) and is as such a well-defined element of $\mathcal{X}_2$. These are the points z_1^L, z_2^L from above. Indeed, $[L(\mathbb{Z})]$ (resp. $[L^\perp(\mathbb{Z})]$) may be thought of as the equivalence class of the integral positive definite binary quadratic form which is the restriction of the form $x_0^2+x_1^2+x_2^2+x_3^2$ to $L(\mathbb{Z})$ (resp. $L^\perp(\mathbb{Z})$). As such they correspond to CM-points. Due to the geometric construction we will refer to them as the **geometric CM points** attached to L.

The points z_3^L and z_4^L come from a natural identification of the Grassmannian $\mathrm{Gr}_{2,4}(\mathbb{R})$ with the space

$$\mathbf{K}(\mathbb{R}) = \big\{(a_1,a_2) \mid a_1,a_2 \in \mathbb{R}^3 \setminus \{0\},\ \|a_1\|_2 = \|a_2\|_2\big\} / \sim$$

where $(a_1,a_2) \sim (a_1',a_2')$ if there is $\lambda \in \mathbb{R}^\times$ with $(a_1,a_2) = (\lambda a_1', \lambda a_2')$. Note that $\mathbf{K}(\mathbb{R})$ is a two-to-one quotient of a product of two spheres.

To describe the above identification, it is useful to view $\mathbb{R}^4$ as the algebra of real Hamiltonian quaternions

$$\mathbf{B}(\mathbb{R}) = \{x_0 + x_1\mathrm{i} + x_2\mathrm{j} + x_3\mathrm{k} \mid x_0,x_1,x_2,x_3 \in \mathbb{R}\},$$

which is equipped with a conjugation given by $\overline{x} = x_0 - x_1\mathrm{i} - x_2\mathrm{j} - x_3\mathrm{k}$ and a trace given by $\mathrm{Tr}(x) = x + \overline{x} = 2x_0$ for $x = x_0 + x_1\mathrm{i} + x_2\mathrm{j} + x_3\mathrm{k} \in \mathbf{B}(\mathbb{R})$. Furthermore, we identify $\mathbb{R}^3$ with the traceless quaternions, i.e. quaternions of the form $x_1\mathrm{i}+x_2\mathrm{j}+x_3\mathrm{k}$ for $x_1,x_2,x_3 \in \mathbb{R}$. Then, the **Klein map**

$$L \in \mathrm{Gr}_{2,4}(\mathbb{R}) \mapsto [(a_1(L), a_2(L))] \in \mathbf{K}(\mathbb{R}) \tag{1.1}$$

is a diffeomorphism where $a_1(L), a_2(L) \in \mathbb{R}^3$ for $L = \mathbb{R}v_1 \oplus \mathbb{R}v_2$ are given by

$$\begin{aligned} a_1(L) &:= v_1\overline{v_2} - \tfrac{1}{2}\,\mathrm{Tr}(v_1\overline{v_2}),\\ a_2(L) &:= \overline{v_2}v_1 - \tfrac{1}{2}\,\mathrm{Tr}(\overline{v_2}v_1). \end{aligned} \tag{1.2}$$

The points $a_1(L), a_2(L)$ as defined here depend on the choice of basis but the equivalence class $[(a_1(L), a_2(L))]$ does not. Furthermore, if L is rational and v_1, v_2 are a $\mathbb{Z}$-basis of $L(\mathbb{Z})$ the resulting vectors $a_1(L), a_2(L)$ are integer vectors. As we will explain later, this yields that the subset $\mathcal{R}_D$ is (almost) in bijection with a set of points $[(a_1,a_2)]$ where $a_1,a_2 \in \mathbb{Z}^3$ are vectors of length $\|a_1\|_2 = \|a_2\|_2 = \sqrt{D}$.

The identification between $\mathrm{Gr}_{2,4}(\mathbb{R})$ and $\mathbf{K}(\mathbb{R})$ in (1.1) corresponds to the accidental local isomorphism between $\mathrm{SO}(4)$ and $\mathrm{SU}(2) \times \mathrm{SU}(2)$ (and hence also $\mathrm{SO}(3) \times \mathrm{SO}(3)$) and leads to the construction of the following two lattices.

For $i=1,2$ we define $\Lambda_{a_i(L)} = a_i(L)^\perp \cap \mathbb{Z}^3$. Fixing a copy of $\mathbb{R}^2$ in $\mathbb{R}^3$ we can rotate these two-dimensional lattices to it to obtain the shapes $z_3^L := [\Lambda_{a_1(L)}]$ and $z_4^L := [\Lambda_{a_2(L)}]$, two well-defined points on $\mathcal{X}_2$. Again, these also correspond to CM-points when viewed as the class of the binary form obtained by restriction of the ambient form $x_1^2+x_2^2+x_3^2$. We will refer to $[\Lambda_{a_1(L)}]$ and $[\Lambda_{a_2(L)}]$ as the **accidental CM points** attached to L.

Conjecture 1.1. *The normalized counting measure on the finite set*

$$\mathcal{J}_D = \left\{ \left(L, [L(\mathbb{Z})], [L^\perp(\mathbb{Z})], [\Lambda_{a_1(L)}], [\Lambda_{a_2(L)}]\right) : L \in \mathcal{R}_D \right\} \subseteq \mathrm{Gr}(\mathbb{R}) \times \mathcal{X}_2^4$$

equidistributes to the uniform probability measure on $\mathrm{Gr}_{2,4}(\mathbb{R}) \times \mathcal{X}_2^4$ *as* $D \to \infty$ *with* $D \in \mathbb{D}$. *That is,*

$$\tfrac{1}{|\mathcal{J}_D|} \sum_{x \in \mathcal{J}_D} \delta_x \to m_{\mathrm{Gr}_{2,4}(\mathbb{R}) \times \mathcal{X}_2^4}$$

in the weak**-topology where* $m_{\mathrm{Gr}_{2,4}(\mathbb{R}) \times \mathcal{X}_2^4}$ *is the probability measure obtained from an* $\mathrm{SO}(4)$*-invariant measure on* $\mathrm{Gr}_{2,4}(\mathbb{R})$ *and an* $\mathrm{SL}_2(\mathbb{R})$*-invariant measure on* $\mathbb{H}^2$.

Our main theorem verifies this conjecture under extra congruence conditions:

Theorem 1.2 (Equidistribution for a given discriminant)**.** *Let* p, q *be any two distinct odd primes. The normalized counting measure on the finite set* $\mathcal{J}_D$ *equidistributes to the uniform probability measure on* $\mathrm{Gr}_{2,4}(\mathbb{R}) \times \mathcal{X}_2^4$ *as* $D \in \mathbb{D}$ *goes to infinity while* D *satisfies the additional conditions* $-D \in (\mathbb{F}_p^\times)^2$ *and* $-D \in (\mathbb{F}_q^\times)^2$.

First results in the spirit of this theorem have previously been obtained by Maass [Maa56], [Maa59] and Schmidt [Sch98], who establish the averaged equidistribution of the pairs $(L, [L(\mathbb{Z})])$, where L varies over the rational planes of discriminant up to D. We obtain as a corollary of the above theorem the following strengthening of these results:

Corollary 1.3 (Averaged equidistribution)**.** *The normalized counting measure on the finite set*

$$\left\{ \left(L, [L(\mathbb{Z})], [L^\perp(\mathbb{Z})], [\Lambda_{a_1(L)}], [\Lambda_{a_2(L)}]\right) : L \in \mathcal{R}_d \text{ for some } d \leq D \right\}$$

equidistributes to the uniform probability measure on $\mathrm{Gr}_{2,4}(\mathbb{R}) \times \mathcal{X}_2^4$ *as* $D \to \infty$.

First non-averaged results as in Theorem 1.2 have been established by Linnik [Lin68] and Skubenko [Sku62] (with a congruence condition at one prime) and Duke [Duk88] (building on work of Iwaniec [Iwa87] and without any congruence condition). Duke's theorem shows equidistribution of integer points on two-dimensional spheres and of CM-points on $\mathcal{X}_2$.

We use these results to obtain the equidistribution on the individual factors of our space. Using a theorem [EL17, Thm. 1.4] of the second named author with Lindenstrauss we then upgrade this information to joint equidistribution. This method of proof has already been used in the work [AES16b] of the first and the second named author with Shapira.

Our main motivation for the study of the sets $\mathcal{J}_D$ has been geometric. As it turned out, the construction of the CM-points $z_1^L, z_2^L, z_3^L, z_4^L$ is in fact strongly related to the group law of the Picard group of an order in $\mathbb{Q}(\sqrt{-D})$. In this way our equidistribution result also has an arithmetic counterpart, see Theorem 7.1.

We would also like to remark that the proof of our theorem can be used to strengthen our result. In fact, Theorem 1.2 can be formulated to consider only planes $L \in \mathcal{R}_D$, whose glue group is of a fixed isomorphism type (see Theorem 8.1). Here, the glue group of a lattice L is an invariant which captures additional information on the lattice including the discriminant (see e.g. McMullen [McM11] or Section 8 for definitions).

1.1. **Outline of the paper.** This paper is organized as follows:

- In Section 2 we study properties of the Klein map (including the statements made above). This yields important information about the related stabilizer groups which play a crucial role in our dynamical argument.
- In Section 3 we discuss in more detail the four CM points attachted to each plane.
- In Section 4 we define the joint acting group for the dynamical setup and formulate a dynamical version (Theorem 4.2) of Theorem 1.2.
- In Section 5 we use the orbit of the stabilizer in order to generate additional points starting from one point (Propositions 5.1 and 5.2) and apply this to prove Theorem 1.2 assuming Theorem 4.2.
- In Section 6 we use the fact that any limit measure coming from Theorem 4.2 is a joining for a higher rank torus action and the algebraicity of such joinings [EL17] to deduce the theorem.
- In Sections 7 and 8 we explain further connections to existing work and in particular the above mentioned connection to the Picard group and to glue groups.
- In Appendix A we prove the averaged version (Corollary 1.3) of the main theorem. In Appendix B we study the Klein map in the case of the split quaternion algebra Mat_2.

Acknowledgements: We would like to thank Elon Lindenstrauss, Ilya Khayutin and Philippe Michel for discussions on this paper. We are also very grateful to Curtis McMullen for suggesting a refinement of our theorem with respect to glue groups.

2. The Klein map

In the following discussions we let $\mathbb{K}$ denote a field of characteristic zero.

2.1. **Hamiltonian quaternions.** As in the introduction, we denote by $\mathbf{B}$ the $\mathbb{Q}$-algebra of Hamiltonian quaternions, $\overline{x}$ the conjugate of any element $x \in \mathbf{B}$ and by $\mathrm{Tr}(x) = x + \overline{x}$ the (reduced) trace. Furthermore, the (reduced) norm on $\mathbf{B}$ is given by

$$\mathrm{Nr}(x) = x\overline{x} = \overline{x}x = x_0^2 + x_1^2 + x_2^2 + x_3^2 =: Q(x_0, x_1, x_2, x_3)$$

for any $x = x_0 + x_1\mathrm{i} + x_2\mathrm{j} + x_3\mathrm{k} \in \mathbf{B}$. As already mentioned we will identify $\mathbf{B}$ with the four-dimensional affine space and in particular write $\mathrm{Nr} = Q$. A quaternion with zero trace is said to be pure and will often be viewed as a point in three-dimensional space. The set of pure quaternions will be denoted by $\mathbf{B}_0$.

Denote by

$$\mathrm{SU}_2 = \{\alpha \in \mathbf{B} \mid \mathrm{Nr}(\alpha) = 1\}$$

the algebraic $\mathbb{Q}$-group of norm one elements of $\mathbf{B}$ and observe that the action of SU_2^2 on $\mathbf{B}$ given by $(\alpha, \beta).x = \alpha x \beta^{-1}$ preserves the norm. This yields a $\mathbb{Q}$-isogeny $P : \mathrm{SU}_2^2 \to \mathrm{SO}_4$ (and in particular a local isomorphism of the groups $\mathrm{SO}_4(\mathbb{R})$ and $\mathrm{SU}_2^2(\mathbb{R})$), where the kernel is given by $\{(1,1), (-1,-1)\}$.

Similarly, the action of SU_2 on pure quaternions by conjugation (i.e. by $\alpha.x = \alpha x \alpha^{-1}$ for $x \in \mathbf{B}_0$ and $\alpha \in \mathrm{SU}_2$) gives an isogeny $\mathrm{SU}_2 \to \mathrm{SO}_3$ with kernel $\{1, -1\}$. We define $P_1, P_2 : \mathrm{SU}_2^2 \to \mathrm{SO}_3$ to be the composition of this isogeny with the respective coordinate projections $\mathrm{SU}_2^2 \to \mathrm{SU}_2$.

We write $\mathrm{Gr}_{2,4}$ for the projective Grassmannian variety of two-dimensional subspaces in four-space. In particular, the set $\mathrm{Gr}_{2,4}(\mathbb{K})$ can be identified with the set of two-dimensional $\mathbb{K}$-subspaces in $\mathbb{K}^4$ (i.e. planes containing zero). The action of $\mathrm{SU}_2^2(\mathbb{K})$ on $\mathbb{K}^4$ induces naturally an action on $\mathrm{Gr}_{2,4}(\mathbb{K})$.

We denote the Zariski-connected component of the stabilizer subgroup of a plane $L \in \mathrm{Gr}_{2,4}(\mathbb{K})$ under SU_2^2 by

$$\mathbb{H}_L = \left\{ g \in \mathrm{SU}_2^2 \mid g.L \subseteq L \right\}^\circ$$

which is an algebraic group defined over $\mathbb{K}$. Furthermore, for any $v \in \mathbb{K}^3$ we define the connected $\mathbb{K}$-group

$$\mathbb{H}_v = \{ g \in \mathrm{SU}_2 \mid g.v = v \}.$$

2.2. **Definition of the Klein map.** We define

$$\mathbf{K}(\mathbb{K}) = \left\{ (a_1, a_2) \mid a_1, a_2 \in \mathbb{K}^3 \setminus \{0\},\ Q(a_1) = Q(a_2) \right\} / \sim$$

where $(a_1, a_2) \sim (a_1', a_2')$ if there exists $\lambda \in \mathbb{K}^\times$ with $(a_1, a_2) = (\lambda a_1', \lambda a_2')$. Also, observe that $\mathrm{SU}_2^2(\mathbb{K})$ acts on $\mathbf{K}(\mathbb{K})$ via $(g_1, g_2).[a_1, a_2] = [g_1.a_1, g_2.a_2]$ where $[a_1, a_2]$ denotes the equivalence class of (a_1, a_2) in $\mathbf{K}(\mathbb{K})$. In the following we will use the definition of $a_1(\cdot)$ and $a_2(\cdot)$ from Equation (1.2).

Proposition 2.1 (Klein map)**.** *The map*

$$\Phi : L \in \mathrm{Gr}_{2,4}(\mathbb{K}) \mapsto [a_1(L), a_2(L)] \in \mathbf{K}(\mathbb{K})$$

is a well-defined bijection and is equivariant for the actions of $\mathrm{SU}_2^2(\mathbb{K})$*. The inverse of* Φ *is given by*

$$\Phi^{-1}([a_1, a_2]) = \{ x \in \mathbf{B}(\mathbb{K}) \mid a_1 x = x a_2 \} \tag{2.1}$$

for all $[a_1, a_2] \in \mathbf{K}(\mathbb{K})$*. Furthermore, we have the following properties:*

- $\mathbb{H}_L = \mathbb{H}_{a_1(L)} \times \mathbb{H}_{a_2(L)}$ *for any* $L \in \mathrm{Gr}_{2,4}(\mathbb{K})$*.*
- $\Phi(L^\perp) = [a_1(L), -a_2(L)]$ *for any* $L \in \mathrm{Gr}_{2,4}(\mathbb{K})$ *where* $L^\perp$ *denotes the orthogonal complement with respect to* Q*.*

Proof. To see that Φ is well-defined, observe first that for any $L = \mathbb{K}v_1 \oplus \mathbb{K}v_2$ and $a_1(L), a_2(L)$ defined as in (1.2) using v_1, v_2, we have

$$\begin{aligned} Q(a_1(L)) = a_1(L)\overline{a_1(L)} &= (v_1\overline{v_2} - \tfrac{1}{2}\operatorname{Tr}(v_1\overline{v_2}))(v_2\overline{v_1} - \tfrac{1}{2}\operatorname{Tr}(v_1\overline{v_2})) \\ &= Q(v_1)Q(v_2) + \tfrac{1}{4}\operatorname{Tr}(v_1\overline{v_2})^2 - \tfrac{1}{2}\operatorname{Tr}(v_1\overline{v_2})(v_2\overline{v_1} + v_1\overline{v_2}) \\ &= Q(v_1)Q(v_2) - \tfrac{1}{4}\operatorname{Tr}(v_1\overline{v_2})^2 \end{aligned}$$

and analogously

$$Q(a_2(L)) = Q(v_1)Q(v_2) - \tfrac{1}{4}\operatorname{Tr}(\overline{v_1}v_2)^2 = Q(a_1(L)). \tag{2.2}$$

Furthermore, as the maps

$$\begin{aligned} &(u, v) \mapsto u\overline{v} - \tfrac{1}{2}\operatorname{Tr}(u\overline{v}), \\ &(u, v) \mapsto \overline{v}u - \tfrac{1}{2}\operatorname{Tr}(\overline{v}u) \end{aligned} \tag{2.3}$$

(that are used to define $a_1(L), a_2(L)$ in (1.2)) are bilinear and antisymmetric, it follows that $[a_1(L), a_2(L)]$ does not depend on the choice of the basis v_1, v_2 of L.

To verify the equivariance property, let $(\alpha,\beta) \in \mathrm{SU}_2^2(\mathbb{K})$ and $L = \mathbb{K}v_1 \oplus \mathbb{K}v_2$. Then $(\alpha,\beta).L = \mathbb{K}\alpha v_1\beta^{-1} \oplus \mathbb{K}\alpha v_2\beta^{-1}$ and applying (1.2) for this basis yields

$$\begin{aligned} a_1((\alpha,\beta).L) &= (\alpha v_1\beta^{-1})\overline{\alpha v_2\beta^{-1}} - \tfrac{1}{2}\operatorname{Tr}((\alpha v_1\beta^{-1})\overline{\alpha v_2\beta^{-1}}) \\ &= \alpha v_1\overline{v_2}\alpha^{-1} - \tfrac{1}{2}\operatorname{Tr}(v_1\overline{v_2}) = \alpha a_1(L)\alpha^{-1}. \end{aligned}$$

Similarly, $a_2((\alpha,\beta).L) = \beta a_2(L)\beta^{-1}$ and therefore Φ is equivariant.

To see that the map Ψ defined in (2.1) is equal to the inverse of Φ we first show that Ψ is equivariant too. Indeed, using the substitution $\hat{x} = \alpha x\beta^{-1}$ we get

$$\begin{aligned} (\alpha,\beta).\Psi([a_1,a_2]) &= (\alpha,\beta).\{x \in \mathbf{B}(\mathbb{K}) \mid a_1x = xa_2\} = \left\{\alpha x\beta^{-1} \in \mathbf{B}(\mathbb{K}) \mid a_1x = xa_2\right\} \\ &= \left\{\hat{x} \in \mathbf{B}(\mathbb{K}) \mid \alpha a_1\alpha^{-1}\hat{x} = \hat{x}\beta a_2\beta^{-1}\right\} = \Psi([\alpha a_1\alpha^{-1}, \beta a_2\beta^{-1}]). \end{aligned}$$

Let $\overline{\mathbb{K}}$ denote an algebraic closure. As $\mathrm{SU}_2^2(\overline{\mathbb{K}})$ acts transitively on $\mathrm{Gr}_{2,4}(\overline{\mathbb{K}})$ and $\mathbf{K}(\overline{\mathbb{K}})$ and both Φ and Ψ are equivariant, it suffices to verify $\Psi\circ\Phi = \mathrm{id}$ and $\Phi\circ\Psi = \mathrm{id}$ at one point. Direct computations show that $\left\{\lambda \in \mathbf{B}(\overline{\mathbb{K}}) \mid \mathrm{i}\lambda = \lambda\mathrm{i}\right\} = \langle 1, \mathrm{i}\rangle_{\overline{\mathbb{K}}}$ as well as $[a_1(L), a_2(L)] = [\mathrm{i}, \mathrm{i}]$ for $L = \langle 1, \mathrm{i}\rangle_{\overline{\mathbb{K}}}$ and we obtain that Φ is a bijection with inverse Ψ for $\overline{\mathbb{K}}$ and also for $\mathbb{K}$.

The formula for the stabilizers follows from equivariance as for any $(\alpha,\beta) \in \mathrm{SU}_2^2$

$$\begin{aligned} (\alpha,\beta).L = L &\iff (\alpha,\beta).[a_1(L), a_2(L)] = [a_1(L), a_2(L)] \\ &\iff [\alpha a_1(L)\alpha^{-1}, \beta a_2(L)\beta^{-1}] = [a_1(L), a_2(L)]. \end{aligned}$$

By orthogonality this shows that $(\alpha,\beta).L = L$ if and only if there is $\lambda \in \{\pm 1\}$ with $\alpha a_1(L)\alpha^{-1} = \lambda a_1(L)$ and $\beta a_2(L)\beta^{-1} = \lambda a_2(L)$. As $\mathbb{H}_L$ is defined to be the connected component of the stabilizer, this shows the desired equality.

For the second property (which could also be verified using equivariance one more time) observe that $\mathbb{H}_L = \mathbb{H}_{L^\perp}$ and thus $\mathbb{H}_{a_i(L)} = \mathbb{H}_{a_i(L^\perp)}$ for $i = 1, 2$. Since the stabilizer of a line within $\mathrm{SO}(3)$ determines the line, we must therefore have $a_1(L^\perp) = \lambda a_1(L)$ and $a_2(L^\perp) = \mu a_2(L)$ for some $\lambda, \mu \in \mathbb{K}$. Since $a_1(L^\perp)$ and $a_2(L^\perp)$ have the same value for Q, we have $\mu = \pm\lambda$. This shows

$$\Phi(L^\perp) = [a_1(L^\perp), a_2(L^\perp)] = [\lambda a_1(L), \pm\lambda a_2(L)] = [a_1(L), \pm a_2(L)]$$

so that $\Phi(L^\perp) = [a_1(L), -a_2(L)]$ as $\Phi(L) \neq \Phi(L^\perp)$. □

2.3. **Associated integer points.** Given any rational plane $L \subseteq \mathbb{R}^4$ the points $a_1(L), a_2(L)$ defined using a $\mathbb{Z}$-basis v_1, v_2 of the lattice $L(\mathbb{Z})$ are in fact also integral by (1.2). Furthermore, the bilinearity and antisymmetry in (2.3) show that they are well-defined up to changing signs simultaneously. If not stated otherwise, we will construct $a_1(L), a_2(L)$ for rational planes L in this fashion and will refer to these points as the **integer points associated** to L.

Recall that the discriminant $\mathrm{disc}(L)$ of $L(\mathbb{Z})$ for a rational plane L was defined as the square of the covolume of $L(\mathbb{Z}) \subseteq L$. Alternatively, the discriminant of L may be defined as the discriminant of the restriction of the quadratic form Q to $L(\mathbb{Z})$. Recall that the discriminant of a quadratic form with $\mathbb{Z}$-coefficients is given by the determinant of any matrix representation of the form.

Lemma 2.2 (Equality of discriminants)**.** *For any $L \in \mathrm{Gr}_{2,4}(\mathbb{Q})$ we have*

$$Q(a_1(L)) = Q(a_2(L)) = \mathrm{disc}(L).$$

Proof. Representing $Q|_{L(\mathbb{Z})}$ in a basis v_1, v_2 of $L(\mathbb{Z})$ as

$$q(x,y) = Q(xv_1 + yv_2) = Q(v_1)x^2 + \operatorname{Tr}(v_1\overline{v_2})xy + Q(v_2)y^2$$

we obtain $\operatorname{disc}(L) = \operatorname{disc}(q) = Q(v_1)Q(v_2) - \frac{1}{4}\operatorname{Tr}(v_1\overline{v_2})^2$. The lemma thus follows from Equation (2.2). □

Notice that if $D \in \mathbb{N}$ is square-free and $L \in \mathcal{R}_D$, the associated integer points are in fact both primitive, since by Lemma 2.2 any integer m with $\frac{1}{m}a_1(L) \in \mathbb{Z}^3$ would satisfy $m^2 \mid D$ and similarly for $a_2(L)$.

For non-square-free D we have the following notion, which serves as a replacement of this observation. We say that a pair of vectors $(w_1, w_2) \in \mathbb{Z}^3 \times \mathbb{Z}^3$ is *pair-primitive* if $\frac{1}{p}w_1 \notin \mathbb{Z}^3$ or $\frac{1}{p}w_2 \notin \mathbb{Z}^3$ for all odd primes p and if $\frac{1}{4}(w_1 + w_2) \notin \mathbb{Z}^3$ or $\frac{1}{4}(w_1 - w_2) \notin \mathbb{Z}^3$.

In fact we will see examples below where the integer points associated to a plane behave differently with respect to the prime 2, but not too differently as pair-primitivity implies that one of the vector $\frac{1}{4}w_1$ and $\frac{1}{4}w_2$ is not integral.

Lemma 2.3 (Pair primitivity)**.** *The integer points $(a_1(L), a_2(L))$ associated to a rational plane $L \in \operatorname{Gr}_{2,4}(\mathbb{Q})$ are pair-primitive. Furthermore, they satisfy $a_1(L) \equiv a_2(L) \bmod 2$.*

Proof. The antisymmetry of the bilinear maps in (2.3) shows that Φ factors through the Plücker embedding

$$L = \mathbb{K}v_1 \oplus \mathbb{K}v_2 \in \operatorname{Gr}_{2,4}(\mathbb{K}) \mapsto [v_1 \wedge v_2] \in \mathbb{P}\big(\textstyle\bigwedge^2 \mathbb{K}^4\big).$$

Moreover, $\bigwedge^2 \mathbb{R}^4$ has an integral structure given by $\bigwedge^2 \mathbb{Z}^4$. Furthermore, for any $v_1, v_2 \in \mathbb{Z}^4$ the wedge $v_1 \wedge v_2$ is primitive if and only if[1] v_1, v_2 is a basis for $L(\mathbb{Z})$ where $L = \mathbb{R}v_1 \oplus \mathbb{R}v_2$. If this is the case, we may retrieve the wedge $v_1 \wedge v_2$ from $a_1(L)$, $a_2(L)$. In fact, identifying $\bigwedge^2 \mathbb{R}^4 \cong \mathbb{R}^6$ via the standard (integral) basis $1\wedge \mathrm{i},\ 1\wedge \mathrm{j},\ 1\wedge \mathrm{k},\ \mathrm{i}\wedge \mathrm{j},\ \mathrm{i}\wedge \mathrm{k},\ \mathrm{j}\wedge \mathrm{k}$ a direct calculation using bilinearity of $\wedge$ and the maps in (2.3) shows that

$$v_1 \wedge v_2 = \tfrac{1}{2}\big(-(a_1+a_2)_1, -(a_1+a_2)_2, -(a_1+a_2)_3, (a_2-a_1)_3, (a_1-a_2)_2, (a_2-a_1)_1\big)$$

where $a_i = a_i(L)$ for $i = 1, 2$.

We will now use this to prove the lemma. For the claims concerning the prime 2 notice that $\frac{1}{2}(a_1 + a_2) \in \mathbb{Z}^3$ as $v_1 \wedge v_2$ is integral and therefore $a_1 \equiv -a_2 \equiv a_2 \bmod 2$. (This can also be seen directly from the definition in (1.2).) Furthermore, if $\frac{1}{4}(a_1+a_2), \frac{1}{4}(a_1-a_2) \in \mathbb{Z}^3$ then $\frac{1}{2}(v_1\wedge v_2) \in \mathbb{Z}^6$ contradicting primitivity of $v_1\wedge v_2$.

If p is an odd prime with $\frac{1}{p}a_1, \frac{1}{p}a_2 \in \mathbb{Z}^3$ then $\frac{1}{p}(a_1 + a_2), \frac{1}{p}(a_1 - a_2) \in \mathbb{Z}^3$ and therefore $\frac{1}{p}(v_1 \wedge v_2) \in \mathbb{Z}^6$. This contradicts again primitivity of $v_1 \wedge v_2$ and shows that (a_1, a_2) are pair-primitive. □

Before discussing the appropriate converse to Lemma 2.3 (see Proposition 2.5 below), we would like to point out that the integer points associated to a plane $L \in \operatorname{Gr}_{2,4}(\mathbb{Q})$ need not be primitive in general. The same is true for the restriction of the ambient quadratic form Q to $L(\mathbb{Z})$, which can in fact be non-primitive even for square-free discriminants.

[1] This can be seen for instance using the Smith normal form.

Example 2.4. (a) The plane $L = \mathbb{R}(1+\mathrm{i}) \oplus \mathbb{R}(\mathrm{i}+\mathrm{j})$ has square-free discriminant $D = 3$ and primitive associated integer points $a_1(L) = -\mathrm{i}-\mathrm{j}-\mathrm{k}$ and $a_2(L) = -\mathrm{i}-\mathrm{j}+\mathrm{k}$. However, the form $Q|_{L(\mathbb{Z})}$ is represented by $2x^2 + 2xy + 2y^2$ (in the given basis) and thus non-primitive.

(b) The plane $L = \mathbb{R}(1+\mathrm{i}) \oplus \mathbb{R}(\mathrm{j}+\mathrm{k})$ of discriminant $D = 4$ has associated integer points $a_1(L) = -2\mathrm{k}$ and $a_2(L) = -2\mathrm{j}$, both of which are non-primitive. Furthermore, the quadratic form $Q|_{L(\mathbb{Z})}$ is represented by the non-primitive form $\mathrm{Nr}(1+\mathrm{i})x^2 + \mathrm{Nr}(\mathrm{j}+\mathrm{k})y^2 = 2x^2 + 2y^2$.

(c) The associated integer points of the plane $L = \mathbb{R}(1+2\mathrm{i}) \oplus \mathbb{R}(\mathrm{j}+3\mathrm{k})$ of discriminant $D = 50$ are the non-primitive vector $a_1(L) = 5(\mathrm{j}-\mathrm{k})$ and the vector $a_2(L) = -7\mathrm{j}-\mathrm{k}$. This shows that Lemma 2.3(a) cannot be improved to include indivisibility of each vector by odd primes. In the given integral basis of L the form $Q|_{L(\mathbb{Z})}$ is represented as $5x^2 + 10y^2$.

We will return to these primitivity questions in Section 8.2 where we will reformulate them in terms of glue groups. Such a reformulation is however not necessary for the proof of Theorem 1.2.

To help the reader we will usually point out the stronger statements for square-free discriminants. In this case, the associated integer points are primitive (and not only pair-primitive) and the quadratic forms on the lattices in question are primitive except possibly for the common divisor 2 (cf. Proposition 3.1, Lemma 3.4 and Example 2.4(a) above).

2.4. **Integrality properties of the Klein map.**

Proposition 2.5 (Pair primitivity, converse claim)**.** *Given* $(w_1, w_2) \in \mathbb{Z}^3 \times \mathbb{Z}^3$ *pair-primitive with* $Q(w_1) = Q(w_2)$ *the rational plane* $\Phi^{-1}([w_1, w_2])$ *has associated integer points* w_1, w_2 *if* $w_1 \equiv w_2 \bmod 2$ *and* $2w_1, 2w_2$ *otherwise.*

Moreover, for any $L \in \mathcal{R}_D$ *the orthogonal complement* $L^\perp$ *has associated integer points* $a_1(L), -a_2(L)$ *and discriminant* D*.*

Proof. Write $L = \Phi^{-1}([w_1, w_2])$ and choose by Proposition 2.1 coprime integers $m, n \in \mathbb{Z}$ with $ma_1(L) = nw_1$ and $ma_2(L) = nw_2$. Since (w_1, w_2) is pair-primitive, we must have that m is not divisible by any odd prime. Furthermore, m is also not divisible by 2. Otherwise, the equality

$$m(a_1(L) \pm a_2(L)) = n(w_1 \pm w_2)$$

combined with $a_1(L) \equiv a_2(L) \bmod 2$ (see Lemma 2.3) shows that $\frac{1}{4}(w_1 \pm w_2) \in \mathbb{Z}^3$ contradicting again the pair-primitivity of (w_1, w_2). Thus, $m = \pm 1$.

Repeating the same argument for the integer n (without any congruence condition on (w_1, w_2) modulo 2), we see that n is not divisible by any odd prime and not divisible by 4. If $w_1 \equiv w_2 \bmod 2$ then the above argument shows that $n = \pm 1$. If $w_1 \not\equiv w_2 \bmod 2$ then $2 \mid n$ as $a_1(L) \equiv a_2(L) \bmod 2$.

Now let $L \in \mathcal{R}_D$. Then one applies the first part to the pair $a_1(L), -a_2(L)$ to deduce that $L^\perp$ (which is equal to $\Phi^{-1}([a_1(L), -a_2(L)])$ by Proposition 2.1) indeed has associated integer points $a_1(L), -a_2(L)$. In fact, we have $a_1(L) \equiv a_2(L) \equiv -a_2(L) \bmod 2$ and pair-primitivity by Lemma 2.3. □

The complete correspondence (established by Lemma 2.3 and Proposition 2.5) between

- pairs of integer points up to common sign, which have the same length and are pair-primitive and congruent modulo 2 and
- rational planes

allows us to prove a claim from the beginning of the introduction.

Corollary 2.6. *For any $D \in \mathbb{N}$ the set $\mathcal{R}_D$ is non-empty if and only if D is not congruent to* 0, 7, 12 *or* $15 \bmod 16$ *(i.e. $D \in \mathbb{D}$).*

In particular, if D is not divisible by 4 (e.g. if D is square-free) and $D \not\equiv 7 \bmod 8$, then the corollary says that $\mathcal{R}_D$ is non-empty. The proof will essentially consist in applying the above correspondence (i.e. Lemma 2.3 and Proposition 2.5) and Legendre's theorem, which states that a number $D \in \mathbb{N}$ can be written as $D = x^2 + y^2 + z^2$ for $(x, y, z) \in \mathbb{Z}^3$ primitive if and only if $D \not\equiv 0, 4, 7 \bmod 8$.

Proof. Lemma 2.3 and Proposition 2.5 together imply that $\mathcal{R}_D$ is non-empty if and only if there exists a tuple $(v, v') \in \mathbb{Z}^3 \times \mathbb{Z}^3$ that is pair-primitive with $Q(v) = Q(v') = D$ and $v \equiv v' \bmod 2$.

Assume first that $4 \nmid D$. We claim that in this case the pair-primitive tuple (v, v') exists if and only if $D \not\equiv 7, 15 \bmod 16$. In fact, if the pair-primitive tuple exists, the vectors represent D as a sum of three squares which implies $D \not\equiv 7, 15 \bmod 16$. Conversely, we apply Legendre's theorem to find a primitive vector v and set the second integer v' equal to v.

So suppose now that $4 \mid D$. Then the set $\mathcal{R}_D$ is non-empty if and only if there exists $(w, w') \in \mathbb{Z}^3 \times \mathbb{Z}^3$ pair-primitive with $Q(w) = Q(w') = \frac{D}{4}$ and $w \not\equiv w' \bmod 2$. In fact, if $L \in \mathcal{R}_D$ then $w = \frac{1}{2} a_1(L)$ and $w' = \frac{1}{2} a_2(L)$ are integer vectors as $4 \mid D$ and are not congruent mod 2 by pair-primitivity of $(a_1(L), a_2(L))$, see Lemma 2.3. For the converse one can apply Proposition 2.5 to (w, w').

We claim that there is such a pair (w, w') if and only if $\frac{D}{4} \not\equiv 0, 3 \bmod 4$ i.e. $D \not\equiv 0, 12 \bmod 16$. Indeed, if (w, w') satisfies $Q(w) = Q(w') = \frac{D}{4}$ and $\frac{D}{4} \equiv 0 \bmod 4$ then w and w' have only even entries. Similarly, if $\frac{D}{4} \equiv 3 \bmod 4$ the vectors w, w' have only odd entries. In either case, w and w' are congruent mod 2. Conversely, if $\frac{D}{4} \not\equiv 0, 3 \bmod 4$ there is a primitive vector w with $Q(w) = \frac{D}{4}$ by Legendre's theorem. By assumption on D, w must have an even and an odd entry so that switching two coordinates yields a vector w' with $Q(w') = \frac{D}{4}$, $w \not\equiv w' \bmod 2$ and (w, w') pair-primitive.

This proves the corollary in both cases $4 \mid D$ and $4 \nmid D$. □

The above can also be used to obtain a count on the number of points in $\mathcal{R}_D$.

Corollary 2.7. *For any $D \in \mathbb{D}$ we have $|\mathcal{R}_D| = D^{1+o(1)}$.*

Proof. We denote by $r_3(D)$ the number of integer vectors on the sphere of radius $\sqrt{D}$ and by $r_{3,\mathrm{prim}}(D)$ the number of primitive integer vectors. Our first goal is to recall that

$$D^{\frac{1}{2}+o(1)} = r_{3,\mathrm{prim}}(D) \leq r_3(D) = D^{\frac{1}{2}+o(1)}. \tag{2.4}$$

It is a consequence of Siegel's lower bound [Sie36] that $r_3(D) = r_{3,\mathrm{prim}}(D)$ is of the size $D^{\frac{1}{2}+o(1)}$ when D is square-free. In this case, the class group $\mathrm{Cl}(\mathcal{O}_D)$ of the ring of integers $\mathcal{O}_D$ in $\mathbb{Q}(\sqrt{-D})$ acts freely and transitively on a quotient of $\{v \in \mathbb{Z}^3 \mid Q(v) = D\}$ by a subgroup of $\mathrm{SO}_3(\mathbb{Z})$ (see [EMV13, Prop. 3.5]).

Assume now that D is not necessarily square-free and write $D = D' f^2$ where D' is the largest square-free divisor of D. Then one can express (see e.g. [CH07]) the number $r_{3,\mathrm{prim}}(D)$ as

$$r_{3,\mathrm{prim}}(D) = r_3(D') f \prod_p \left(1 - p^{-1}\left(\tfrac{D'}{p}\right)\right)$$

where p runs over the odd prime divisors of f and $(\frac{\cdot}{p})$ denotes the Legendre symbol. From this, one deduces that $r_{3,\mathrm{prim}}(D) = D^{\frac{1}{2}+o(1)}$.

Finally we recall that the number of divisions of D is $D^{o(1)}$. Summing over $r_{3,\mathrm{prim}}(D' q^2)$ for all square divisors q^2 of D we obtain the upper bound in (2.4).

In particular, (2.4) implies that $|\mathcal{R}_D| \leq D^{1+o(1)}$ as the integer points associated to a plane are uniquely determined up to a simultaneous sign and are of norm $\sqrt{D}$.

If $4 \nmid D$ and (v, v') is any pair of primitive integer points of norm $\sqrt{D}$, there exists $g \in \mathrm{SO}_3(\mathbb{Z})$ such that $g.v' \equiv v \bmod 2$. Thus, $|\mathcal{R}_D| \gg r_{3,\mathrm{prim}}(D)^2$ concluding the proof in this case.

If $4 \mid D$ and (w, w') is any pair of primitive integer points of norm $\sqrt{D}/2$ there exists $g \in \mathrm{SO}_3(\mathbb{Z})$ such that $g.w' \not\equiv w \bmod 2$ (since $\frac{D}{4} \not\equiv 0, 3 \bmod 4$). Therefore, we have $|\mathcal{R}_D| \gg r_{3,\mathrm{prim}}(D/4)^2 = D^{1+o(1)}$ also in this case. □

2.5. **Pointwise stabilizers.** For any plane $L \in \mathrm{Gr}_{2,4}(\mathbb{K})$ define the pointwise stabilizer subgroup of L as the connected $\mathbb{K}$-group

$$\mathbb{H}_L^{\mathrm{pt}} = \left\{ g \in \mathrm{SU}_2^2 \mid g.x = x \text{ for all } x \in L \right\}.$$

The proof of the dynamical version of Theorem 1.2 will use the fact that the subgroup $\mathbb{H}_L^{\mathrm{pt}}$ exhibits a "45°-degree" twist with respect to the subgroups $\mathbb{H}_{a_1(L)}$, $\mathbb{H}_{a_2(L)}$. Let us illustrate this in an example first (see also Section B).

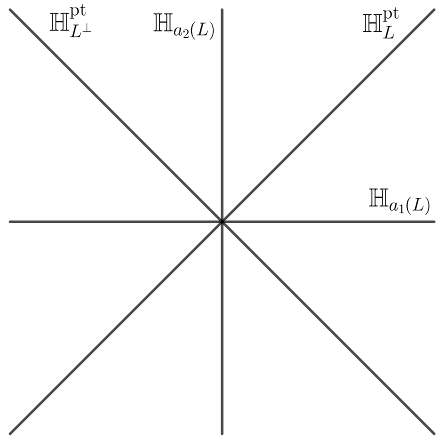
Example 2.8. Consider the plane $\langle 1, \mathrm{i} \rangle$ and let $h = (h_1, h_2)$ be an element of $\mathbb{H}_{\langle 1,\mathrm{i}\rangle}^{\mathrm{pt}}$. In particular, h fixes 1 or in other words $h_1 = h_2$. Furthermore, we have $h.\mathrm{i} = h_1 \mathrm{i} h_1^{-1} = \mathrm{i}$. This shows that

$$\mathbb{H}_{\langle 1,\mathrm{i}\rangle}^{\mathrm{pt}} = \{(h_1, h_1) \mid h_1 \in \mathbb{H}_{\mathrm{i}} = \mathrm{Stab}_{\mathrm{SU}_2}(\mathrm{i})\}.$$

Similarly, we claim that

$$\mathbb{H}_{\langle \mathrm{j},\mathrm{k}\rangle}^{\mathrm{pt}} = \left\{(h_1, h_1^{-1}) \mid h_1 \in \mathbb{H}_{\mathrm{i}}\right\}.$$

For this, let $h = (h_1, h_2) \in \mathbb{H}_{\langle \mathrm{j},\mathrm{k}\rangle}^{\mathrm{pt}}$. Since $\mathbb{H}_{\langle \mathrm{j},\mathrm{k}\rangle}^{\mathrm{pt}}$ is contained in $\mathbb{H}_{\langle \mathrm{j},\mathrm{k}\rangle} = \mathbb{H}_{\mathrm{i}} \times \mathbb{H}_{\mathrm{i}}$ (see Proposition 2.1), we have $h_1, h_2 \in \mathbb{H}_{\mathrm{i}}$. Furthermore, by assumption $h_1 \mathrm{j} = \mathrm{j} h_2$ or equivalently $h_1 = \mathrm{j} h_2 \mathrm{j}^{-1}$. However, notice that $h_1, h_2 \in \langle 1, \mathrm{i} \rangle$ and therefore $h_1 = \mathrm{j} h_2 \mathrm{j}^{-1} = h_2^{-1}$ as (j, j) acts by conjugation $x \mapsto \overline{x}$ on the plane $\langle 1, \mathrm{i} \rangle$.



In general the following holds:

Lemma 2.9 (Pointwise stabilizers)**.** *Let $L \in \mathrm{Gr}_{2,4}(\mathbb{K})$ be a plane and let $g \in \mathbf{B}(\mathbb{K})^\times$ be any element with $a_2(L) = g a_1(L) g^{-1}$. Then*

$$\mathbb{H}^{\mathrm{pt}}_L = \left\{ (h_1, g h_1 g^{-1}) \mid h_1 \in \mathbb{H}_{a_1(L)} \right\},$$
$$\mathbb{H}^{\mathrm{pt}}_{L^\perp} = \left\{ (h_1, g h_1^{-1} g^{-1}) \mid h_1 \in \mathbb{H}_{a_1(L)} \right\}.$$

We remark that for any invertible $x \in L(\mathbb{K})$ the element $g = x^{-1}$ has the property[2] required in the lemma (see Proposition 2.1).

Proof. Let $(\alpha, \beta) \in \mathrm{SU}_2^2$ be such that $(\alpha,\beta).\langle 1, \mathrm{i}\rangle = L$. Applying Proposition 2.1 we have

$$\mathbb{H}_{a_1(L)} \times \mathbb{H}_{a_2(L)} = \mathbb{H}_L = (\alpha,\beta)\mathbb{H}_{\langle 1,\mathrm{i}\rangle}(\alpha,\beta)^{-1} = \alpha \mathbb{H}_{\mathrm{i}} \alpha^{-1} \times \beta \mathbb{H}_{\mathrm{i}} \beta^{-1}$$

and in particular $\alpha \mathbb{H}_{\mathrm{i}} \alpha^{-1} = \mathbb{H}_{a_1(L)}$. By Example 2.8

$$\begin{aligned} \mathbb{H}^{\mathrm{pt}}_L &= (\alpha,\beta)\mathbb{H}^{\mathrm{pt}}_{\langle 1,\mathrm{i}\rangle}(\alpha,\beta)^{-1} = \left\{ (\alpha h_1 \alpha^{-1}, \beta h_1 \beta^{-1}) \mid h_1 \in \mathbb{H}_{\mathrm{i}} \right\} \\ &= \left\{ (h_1, \beta\alpha^{-1} h_1 \alpha \beta^{-1} \mid h_1 \in \mathbb{H}_{a_1(L)} \right\}. \end{aligned}$$

Furthermore, notice that

$$\beta\alpha^{-1} a_1(L) \alpha \beta^{-1} = \beta \mathrm{i} \beta^{-1} = a_2(L) = g a_1(L) g^{-1}.$$

Hence, $\beta\alpha^{-1}\mathbb{H}_{a_1(L)} = g\mathbb{H}_{a_1(L)}$ and one may replace $\beta\alpha^{-1}$ by g in the above equality to obtain the first part of the lemma.

The second part follows analogously by noting that $(\alpha,\beta).\langle \mathrm{j}, \mathrm{k}\rangle = L^\perp$ and applying Example 2.8 again. □

We finish this section by clarifying the meaning of the assumed congruence conditions in Theorem 1.2.

Lemma 2.10. *Let $L \in \mathcal{R}_D$ be a rational plane. If p is an odd prime so that $-D \in (\mathbb{F}_p^\times)^2$, then $\mathbb{H}_L(\mathbb{Q}_p)$ is a split torus of rank two.*

[2]Alternatively, recall that the projective group of invertible quaternions is isomorphic over $\mathbb{Q}$ to SO_3 via the action by conjugation on $\mathbf{B}_0$ (see [Vig80, Thm. 3.3]). Thus there exists $g \in \mathbf{B}(\mathbb{K})^\times$ with $g a_1 g^{-1} = a_2$ by Witt's theorem, see e.g. [Cas78, p. 21].

Proof. Let $v \in \mathbf{B}_0(\mathbb{Z})$ be any vector with $Q(v) = D$ and note that there is an isomorphism $\mathbf{B}(\mathbb{Q}_p) \cong \mathrm{Mat}_2(\mathbb{Q}_p)$ of $\mathbb{Q}_p$-algebras mapping v to some traceless $X \in \mathrm{Mat}_2(\mathbb{Q}_p)$ of determinant D. The stabilizer subgroup $\mathbb{H}_v(\mathbb{Q}_p)$ is thus isomorphic to

$$\{g \in \mathrm{SL}_2(\mathbb{Q}_p) \mid gX = Xg\}.$$

By assumption and by Hensel's lemma the characteristic polynomial $x^2 + D$ of X has two distinct, non-zero roots in $\mathbb{Q}_p$ so X is diagonalizable over $\mathbb{Q}_p$. Thus, $\mathbb{H}_v(\mathbb{Q}_p)$ is a one-dimensional split torus.

By Lemma 2.2 one can apply the above to $v = a_1(L)$ and $v = a_2(L)$. The claim then follows as $\mathbb{H}_L(\mathbb{Q}_p) = \mathbb{H}_{a_1(L)}(\mathbb{Q}_p) \times \mathbb{H}_{a_2(L)}(\mathbb{Q}_p)$ by Proposition 2.1. ☐

3. CM-points

3.1. **Defining the shapes.** We recall that P, P_1, P_2 denote the factor maps from $\mathrm{SU}_2 \times \mathrm{SU}_2$ to SO_4 respectively SO_3 using the first or second factor, see Section 2.1. In the following we identify $\mathbf{B}(\mathbb{R})$ with row vectors in $\mathbb{R}^4$ using the basis $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$ and $\mathbf{B}_0(\mathbb{R})$ with row vectors in $\mathbb{R}^3$ using the basis $\mathrm{i}, \mathrm{j}, \mathrm{k}$. In particular, we choose to let $g \in \mathrm{SO}_4(\mathbb{R})$ act on row vectors $v \in \mathbb{R}^4$ via $g.v = vg^t$. Observe that this action simply corresponds to the usual action on column vectors.

Let us now fix a plane $L \in \mathcal{R}_D$ for some $D \in \mathbb{D}$. We choose an integer matrix $A_{1,L} \in \mathrm{SL}_4(\mathbb{Z})$ whose first two rows form a basis of $L(\mathbb{Z})$ and fix an isometry $k_L = (\alpha_L, \beta_L) \in \mathrm{SU}_2^2(\mathbb{R})$ with $k_L.\langle 1, \mathrm{i}\rangle_{\mathbb{R}} = L(\mathbb{R})$. In particular, this also implies $k_L.\langle \mathrm{j}, \mathrm{k}\rangle_{\mathbb{R}} = L^\perp(\mathbb{R})$ by orthogonality, respectively

$$\alpha_L^{-1}.a_1(L) = \beta_L^{-1}.a_2(L) = \pm\sqrt{D} \cdot \mathrm{i}. \tag{3.1}$$

by the equivariance of the isomorphism in Proposition 2.1. Then we have

$$A_{1,L}P(k_L) \in \left\{ \left(\begin{array}{cc|cc} * & * & 0 & 0 \\ * & * & 0 & 0 \\ \hline * & * & * & * \\ * & * & * & * \end{array} \right) \right\}.$$

Here, we used that for any $v \in L$ viewed as a row vector the vector $vP(k_L)$ corresponds to $k_L^{-1}.v$ when viewed as an element of $\mathbf{B}(\mathbb{R})$ and that $k_L^{-1}.v \in \langle 1, \mathrm{i}\rangle$ where $\langle 1, \mathrm{i}\rangle$ is identified with $\mathbb{R}^2 \times \{(0,0)\}$. The **shape** of $L(\mathbb{Z})$ is defined as

$$[L(\mathbb{Z})] := \mathrm{PGL}_2(\mathbb{Z})\pi_1(A_{1,L}P(k_L))\,\mathrm{PO}(2) \in \mathcal{X}_2$$

where π_1 is the projection onto the upper left block and where as in the introduction

$$\mathcal{X}_2 = \mathrm{PGL}_2(\mathbb{Z})\backslash\mathbb{H}^2 = \mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R})/\mathrm{PO}(2)$$

Note that the definition of the shape is independent of the choices of $A_{1,L}$ and k_L.

Similarly, one can choose a matrix $A_{2,L} \in \mathrm{SL}_4(\mathbb{Z})$ whose last two rows form a basis of $L^\perp(\mathbb{Z})$ so that

$$A_{2,L}P(k_L) \in \left\{ \left(\begin{array}{cc|cc} * & * & * & * \\ * & * & * & * \\ \hline 0 & 0 & * & * \\ 0 & 0 & * & * \end{array} \right) \right\}.$$

Denoting by π_2 the projection onto the lower right block the shape of $L^\perp(\mathbb{Z})$ is

$$[L^\perp(\mathbb{Z})] := \mathrm{PGL}_2(\mathbb{Z})\pi_2(A_{2,L}P(k_L))\,\mathrm{PO}(2) \in \mathcal{X}_2,$$

which is again independent of the choice of $A_{2,L}$ and k_L.

As in the introduction, the shapes $[L(\mathbb{Z})]$ and $[L^\perp(\mathbb{Z})]$ will be called the geometric CM points attached to L. By Proposition 2.5 the plane $L^\perp$ also has discriminant D and so

$$\det(\pi_1(A_{1,L}P(k_L))) = \det(\pi_2(A_{2,L}P(k_L))) = \pm\sqrt{D}. \tag{3.2}$$

By adapting $A_{1,L}$ and $A_{2,L}$ we may assume that these determinants are positive. We note that in case D is not square-free the discriminant of the geometric CM points may be a divisor of D instead of D itself, we will explain this in detail in Proposition 3.1 below.

Define as in the introduction the orthogonal lattices $\Lambda_{a_1(L)}$ and $\Lambda_{a_2(L)}$. If D is square-free, $a_1(L)$ and $a_2(L)$ are primitive and the orthogonal lattices have discriminant D (c.f. [AES16b, p. 379]). Otherwise, the discriminant of these lattices are the squared lengths of primitive vectors in $\mathbb{Q}\,a_1(L)$ resp. $\mathbb{Q}\,a_2(L)$. Let $A_{3,L} \in \mathrm{SL}_3(\mathbb{Z})$ be a matrix whose last two rows are a basis of $\Lambda_{a_1(L)}$ and define $A_{4,L}$ analogously for $a_2(L)$. The above choices together with (3.1) yield

$$A_{3,L}P_1(k_L),\ A_{4,L}P_2(k_L) \in \left\{ \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix} \right\}.$$

Denoting by π the projection onto the lower right block we obtain the shapes

$$[\Lambda_{a_1(L)}] = \mathrm{PGL}_2(\mathbb{Z})\,\pi(A_{3,L}P_1(k_L))\ \mathrm{PO}(2) \in \mathcal{X}_2,$$
$$[\Lambda_{a_2(L)}] = \mathrm{PGL}_2(\mathbb{Z})\,\pi(A_{4,L}P_2(k_L))\ \mathrm{PO}(2) \in \mathcal{X}_2,$$

which are indepedent of the choices made. These are the accidental CM points attached to L. Note that an analogous construction defines the shape $[\Lambda_v]$ of an orthogonal lattice $\Lambda_v = v^\perp \cap \mathbb{Z}^3$ for any primitive integer point $v \in \mathbb{Z}^3$.

3.2. **CM points and relationship to shapes.** The notions *shapes of two-dimensional lattices*, *binary quadratic forms* and *CM-points* are related as we now explain. Recall that GL_2 acts on binary forms via

$$q(x,y) \mapsto g.q(x,y) = \tfrac{1}{\det(g)}q((x,y)g)$$

preserving the discriminant and that this action factors through PGL_2. In particular, $\mathrm{PGL}_2(\mathbb{Z})$ acts on integral binary forms; we will denote by $[\cdot]$ the orbit equivalence classes for the latter action. For any equivalence class $[q]$ associated to a positive definite integral form $q(x,y) = ax^2 + bxy + cy^2$ we obtain a well-defined point

$$\mathbf{z}_{[q]} = \mathrm{PGL}_2(\mathbb{Z}).\frac{-b + \sqrt{|b^2 - 4ac|}\mathrm{i}}{2a} \in \mathrm{PGL}_2(\mathbb{Z})\backslash\mathbb{H}^2 = \mathcal{X}_2,$$

which doesn't depend on the choice of representative and which satifies $\mathbf{z}_{[q]} = \mathbf{z}_{[\alpha q]}$ for any $\alpha \in \mathbb{N}$.

Given a rational plane L one obtains a well-defined point $\mathbf{z}_{[Q|_{L(\mathbb{Z})}]}$. Using the basis of $L(\mathbb{Z})$ contained in $A_{1,L}$ one can represent the quadratic form $Q|_{L(\mathbb{Z})}$ by

$$q_L(x,y) = Q((x,y,0,0)A_{1,L}).$$

Similarly, we represent the form $Q|_{L^\perp(\mathbb{Z})}$ by

$$q_{L^\perp}(x,y) = Q((0,0,x,y)A_{2,L}).$$

Both binary forms q_L and $q_{L^\perp}$ have discriminant D as $L^\perp \in \mathcal{R}_D$ by Proposition 2.5.

Proposition 3.1 (Geometric CM points). *Let $L \in \mathcal{R}_D$ for $D \in \mathbb{D}$. Then*

$$\mathbf{z}_{[Q|_{L(\mathbb{Z})}]} = \mathbf{z}_{[q_L]} = [L(\mathbb{Z})]$$

and analogously $\mathbf{z}_{[Q|_{L^\perp(\mathbb{Z})}]} = \mathbf{z}_{[q_{L^\perp}]} = [L^\perp(\mathbb{Z})]$.

If D is square-free, either $Q|_{L(\mathbb{Z})}$ is a primitive integral form or $\frac{1}{2}Q|_{L(\mathbb{Z})}$ is a primitive integral form.

The situation for non-square-free discriminants will be analyzed later (see Proposition 3.2) using local considerations.

Proof. Let us first prove the statement in the proposition concerning the CM points $\mathbf{z}_{[Q|_{L(\mathbb{Z})}]}, \mathbf{z}_{[Q|_{L^\perp(\mathbb{Z})}]}$. For this we apply a similar argument as in [AES16b, p. 391-392]. Write v_1, v_2 for the first two rows of $A_{1,L}$ and note that

$$q_L(x,y) = ax^2 + bxy + cy^2$$

for $a = Q(v_1)$, $b = 2(v_1, v_2)$ and $c = Q(v_2)$ where $(\cdot,\cdot)$ denotes the (standard) bilinear form induced by Q. Furthermore, set $\pi_1(A_{1,L}P(k_L)) = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$. By definition, we have $a_{11}^2 + a_{12}^2 = Q(v_1) = a$, $a_{21}^2 + a_{22}^2 = Q(v_2) = c$ and $a_{11}a_{21} + a_{12}a_{22} = (v_1, v_2) = \frac{b}{2}$. As $\sqrt{D}$ is the covolume of $L(\mathbb{Z})$ (see (3.2)), we further note that

$$a_{11}a_{22} - a_{12}a_{21} = \det(\pi_1(A_{1,L}P(k_L))) = \sqrt{D} = \sqrt{ac - \tfrac{1}{4}b^2}.$$

To compute a representative of $\pi_1(A_{1,L}P(k_L)).\mathrm{i}$ in $\mathcal{X}_2$ we may also conjugate $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$ with $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{SO}_2(\mathbb{Z})$ to obtain

$$\begin{aligned}\begin{pmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{pmatrix}.\mathrm{i} &= \frac{a_{22}\mathrm{i} - a_{21}}{-a_{12}\mathrm{i} + a_{11}} = \frac{(-a_{12}a_{22} - a_{11}a_{21}) + \mathrm{i}(-a_{12}a_{21} + a_{11}a_{22})}{a} \\ &= \frac{-\frac{b}{2} + \mathrm{i}\sqrt{D}}{a} = \frac{-b + \mathrm{i}\sqrt{4D}}{2a}\end{aligned}$$

For the equality $\mathbf{z}_{[Q|_{L^\perp(\mathbb{Z})}]} = [L^\perp(\mathbb{Z})]$ we note that the discriminant of $L^\perp(\mathbb{Z})$ is also D by Proposition 2.5 so that the above proof applies.

For the second part of the proposition assume that D is square-free. We recall that by definition $ac - \frac{b^2}{4} = D$. This implies that $p \nmid \gcd(a,b,c)$ for any odd prime p (as otherwise $p^2 \mid D$) and $4 \nmid \gcd(a,b,c)$ as claimed. □

3.3. **Local analysis at odd primes.** Here, we generalize the second part of Proposition 3.1 that addresses primitivity issues of $Q|_{L(\mathbb{Z})}$ for $L \in \mathcal{R}_D$ to non-square-free discriminants D. The reader only interested in the square-free case may thus skip this section.

If D is not square-free, the form $Q|_{L(\mathbb{Z})}$ might be non-primitive and the discriminant[3] of the primitive forms $\widetilde{q}_L$ might be much smaller than D. In the proposition to follow we will compute the discriminant of the form $\widetilde{q}_L$.

Given a binary integral form q and a prime p we denote by $\mathrm{ord}_p(q)$ the largest integer k for which $p^{-k}q$ is integral. Similarly, given a vector $v \in \mathbb{Z}^3$ we let $\mathrm{ord}_p(v)$ for a prime p be the largest integer k with $p^{-k}v \in \mathbb{Z}^3$. We also set $\widetilde{v}$ to be the primitive integer vector in the half-line $\mathbb{Q}_+ v$.

[3]By definition of the discriminant in Section 2.3, the discriminant of a binary quadratic form $ax^2 + bxy + cy^2$ is given by $ac - \frac{b^2}{4}$.

Proposition 3.2 (Geometric CM points and non-square-free discriminants)**.** *Let* $L \in \mathcal{R}_D$ *for* $D \in \mathbb{D}$*. Then*

$$\operatorname{ord}_p(Q|_{L(\mathbb{Z})}) = \operatorname{ord}_p(q_L) = \max\left\{ \operatorname{ord}_p(a_1(L)), \operatorname{ord}_p(a_2(L))\right\}$$

for any odd prime p *and* $\operatorname{ord}_2(Q|_{L(\mathbb{Z})}) \leq 4$*. Furthermore, the discriminant of the primitive form* $\widetilde{q}_L$ *(or* $\widetilde{q}_{L^\perp}$*) satisfies*

$$\operatorname{disc}(\widetilde{q}_L) \asymp \frac{Q(\widetilde{a}_1(L))Q(\widetilde{a}_2(L))}{D}. \tag{3.3}$$

The proposition essentially says that the quadratic form $Q|_{L(\mathbb{Z})}$ inherits the "arithmetic complexity" from the integer points of the plane L. More precisely, if one of the vectors $a_1(L)$ and $a_2(L)$ is "very non-primitive" then the same will hold for the form. This fact is also reflected in Lemma 2.9. We also note that the statement at the prime 2 could be sharpened. This however is not needed for the proof of (3.3).

Let p be a fixed odd prime (the statement for the prime 2 will be a simple consequence of the congruence condition $D \in \mathbb{D}$). Then the quaternion algebra $\mathbf{B}$ is split over $\mathbb{Q}_p$ i.e. $\mathbf{B}(\mathbb{Q}_p) \cong \operatorname{Mat}_2(\mathbb{Q}_p)$ (and in fact $\mathbf{B}(\mathbb{Z}_p) \cong \operatorname{Mat}_2(\mathbb{Z}_p)$). Under this fixed isomorphism, conjugation on $\mathbf{B}(\mathbb{Q}_p)$ corresponds to the adjunct on $\operatorname{Mat}_2(\mathbb{Q}_p)$, the (reduced) trace to the usual trace on matrices and the (reduced) norm to the determinant. Now note that the Klein map (see Proposition 2.1) was defined using only these operations and can thus be defined for two-dimensional subspaces of Mat_2 as well[4]. We will therefore freely identify the resulting Klein map for $\operatorname{Mat}_2(\mathbb{Q}_p)$ with the Klein map for $\mathbf{B}(\mathbb{Q}_p)$.

Let $\mathcal{R}_{D,p}$ be the set of two-dimensional subspaces L in $\mathbb{Q}_p^4$ with $\operatorname{disc}(L) = D(\mathbb{Z}_p^\times)^2$ and note that $\mathrm{SU}_2^2(\mathbb{Z}_p)$ acts on $\mathcal{R}_{D,p}$ (preserving in fact also $\mathbb{Z}_p$-equivalence class of the form $Q|_{L(\mathbb{Z}_p)}$ for any $L \in \mathcal{R}_{D,p}$). Observe also that the Klein map using an integral basis associates to any $L \in \mathcal{R}_{D,p}$ a pair of vectors $(a_1(L), a_2(L)) \in \mathbb{Z}_p^3 \times \mathbb{Z}_p^3$ with $Q(a_1(L)) = Q(a_2(L)) \in D(\mathbb{Z}_p^\times)^2$, which is well-defined up to simultaneous multiples in $\mathbb{Z}_p^\times$.

Lemma 3.3. *Let* $L \in \mathcal{R}_{D,p}$*. Then there is some* $g \in \mathrm{SU}_2^2(\mathbb{Z}_p)$ *such that*

$$g.L(\mathbb{Z}_p) = \mathbb{Z}_p \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \oplus \mathbb{Z}_p \begin{pmatrix} 0 & 1 \\ -\frac{D}{\alpha_1\alpha_2} & 0 \end{pmatrix} \tag{3.4}$$

for some $\alpha_1, \alpha_2 \in \mathbb{Z}_p \backslash \{0\}$ *with* $\operatorname{ord}_p(\alpha_1) = \operatorname{ord}_p(a_1(L))$ *and* $\operatorname{ord}_p(\alpha_2) = \operatorname{ord}_p(a_2(L))$.

Proof. Choose a basis of L for which $Q(a_1(L)) = Q(a_2(L)) = D$. We may assume without loss of generality that $\operatorname{ord}_p(a_1(L)) = k = \max\{\operatorname{ord}_p(a_1(L)), \operatorname{ord}_p(a_2(L))\}$ which implies $\operatorname{ord}_p(a_2(L)) = 0$ by pair-primitivity. (Otherwise, one can replace L by $\overline{L}$ which interchanges $a_1(L)$ and $a_2(L)$.)

In order to obtain a plane of the desired form we use equivariance of the Klein map. Note that the action of $\mathrm{SU}_2(\mathbb{Z}_p)$ on the set of primitive vectors $v \in \mathbf{B}_0(\mathbb{Z}_p)$ with $N(v) = d$ for some fixed non-zero $d \in \mathbb{Z}_p$ has at most two orbits which can be

[4] In fact, the Klein map makes sense for two-dimensional subspaces of any quaternion algebra. In principle, the arguments of this paper carry over to yield a more general statement about such planes and the induced shapes (for the norm form).

represented by

$$b_\lambda(d,p) = \begin{pmatrix} 0 & \lambda \\ -d\lambda^{-1} & 0 \end{pmatrix} \tag{3.5}$$

Here, $\lambda \in \{1, \varepsilon_p\}$ where ε_p a non-square in $\mathbb{Z}_p^\times$. In fact, one shows that $\mathrm{GL}_2(\mathbb{Z}_p)$ acts transitively on the above set of vectors, and the matrices $b_1(d,p)$ and $b_{\varepsilon_p}(d,p)$ are not conjugate by a matrix in $\mathrm{SL}_2(\mathbb{Z}_p)$ if and only if p divides d (see also the proof of [EMV13, Prop. 3.7]).

Applying this to $p^{-k}a_1(L)$ and $a_2(L)$ to find $g \in \mathrm{SU}_2^2(\mathbb{Z}_p)$ such that

$$g_1.a_1(L) = p^k b_{\lambda_1}(D/p^k, p) \text{ and } g_2.a_2(L) = b_{\lambda_2}(D,p) \tag{3.6}$$

for some $\lambda_1, \lambda_2 \in \{1, \varepsilon_p\}$. A direct computation using either the Klein map on (3.4) or its inverse on (3.6) shows that $g.L$ is of the form desired in the lemma where we set $\alpha_1 = \lambda_1 p^k$ and $\alpha_2 = \lambda_2$. □

Proof of Proposition 3.2. Let p be an odd prime and let $L \in \mathcal{R}_D \subseteq \mathcal{R}_{D,p}$. Furthermore, let g, α_1, α_2 be chosen as in Lemma 3.3 for L and set

$$k = \max\{\mathrm{ord}_p(a_1(L)), \mathrm{ord}_p(a_2(L))\} = \mathrm{ord}_p(\alpha_1\alpha_2).$$

Clearly, $Q|_{L(\mathbb{Z}_p)}$ is $\mathbb{Z}_p$-equivalent to $Q|_{g.L(\mathbb{Z}_p)}$. In the orthogonal basis for $g.L(\mathbb{Z}_p)$ of Lemma 3.3 the form $Q|_{g.L(\mathbb{Z}_p)}$ is represented by $q(x,y) = \alpha_1\alpha_2 x^2 + \frac{D}{\alpha_1\alpha_2}y^2$. Since $p^{2k} \mid D$, we obtain $k = \mathrm{ord}_p(q) = \mathrm{ord}_p(Q|_{L(\mathbb{Z}_p)})$ as claimed.

For the statement at the prime 2 note that for any $L \in \mathcal{R}_D$ we have

$$\mathrm{ord}_2(Q|_{L(\mathbb{Z})}) \leq \mathrm{ord}_2(D) + 1 \leq 4$$

as $D \in \mathbb{D}$.

To prove Equation (3.3) note that by pair-primitivity

$$\begin{aligned}\mathrm{disc}(\widetilde{q}_L) &\asymp \frac{D}{\prod_{p \text{ odd}} p^{2\,\mathrm{ord}_p(a_1(L)) + 2\,\mathrm{ord}_p(a_2(L))}} \\ &= \frac{1}{D}\frac{Q(a_1(L))}{\prod_{p \text{ odd}} p^{2\,\mathrm{ord}_p(a_1(L))}}\frac{Q(a_2(L))}{\prod_{p \text{ odd}} p^{2\,\mathrm{ord}_p(a_2(L))}} \asymp \frac{Q(\widetilde{a}_1(L))Q(\widetilde{a}_2(L))}{D}\end{aligned}$$

as claimed (where $\asymp$ is used in order to ignore the prime 2). □

3.4. **Accidental CM points.** As for the geometric CM points, we use the basis of $\Lambda_{a_1(L)}$ contained in $A_{3,L}$ to represent $Q|_{\Lambda_{a_1(L)}}$ via the binary form $q_{a_1(L)}(x,y) = Q|_{\mathbf{B}_0}((0,x,y)A_{3,L})$. The form $q_{a_2(L)}$ is defined analogously. As mentioned, in [AES16b, p. 391-392] and [AES16a, Lemma 3.3] (in the non-square-free case) a discussion similar to Proposition 3.1 was carried out for the shapes $[\Lambda_{a_1(\cdot)}]$ and $[\Lambda_{a_2(\cdot)}]$, which we summarize in the following lemma.

Lemma 3.4 (Accidental CM points). *Let $v \in \mathbb{Z}^3$ and set $d = Q(\widetilde{v})$. Then we have $\mathbf{z}_{[Q|_{\Lambda_v}]} = [\Lambda_v] = [\Lambda_{\widetilde{v}}]$.*

If $d \equiv 1,2 \bmod 4$, the quadratic form $Q|_{\Lambda_v}$ is primitive. If $d \equiv 3 \bmod 4$, the quadratic form $\frac{1}{2}Q|_{\Lambda_v}$ is integral and primitive. Furthermore, $\mathrm{disc}(\widetilde{q}_v) \asymp Q(\widetilde{v})$.

4. The dynamical formulation of the theorem

4.1. **The joint acting group.** In this section we first determine the stabilizer subgroups for the CM points associated to a given rational plane and use these to define the acting group appearing in the dynamical version of Theorem 1.2.

Let $D \in \mathbb{D}$ and let $L \in \mathcal{R}_D$. For any $h \in \mathrm{SU}_2^2$ we (trivially) have

$$q_L(x,y) = Q((x,y,0,0)A_{1,L}P(h)) = Q((x,y,0,0)A_{1,L}P(h)A_{1,L}^{-1}A_{1,L}).$$

Moreover, for any $h \in \mathbb{H}_L$ the matrix $P(h)$ preserves L by definition and therefore $A_{1,L}P(h)A_{1,L}^{-1}$ is of the block-form $\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)$. Projecting this to the upper left block we obtain a homomorphism

$$\Psi_{1,L} : h \in \mathbb{H}_L \mapsto \pi_1(A_{1,L}P(h)A_{1,L}^{-1}) \in \mathrm{Stab}_{\mathrm{SL}_2}(q_L) =: \mathbb{H}_{q_L}$$

defined over $\mathbb{Q}$. Notice that the image lies indeed in SL_2 as $\mathbb{H}_L$ is (by definition) connected. The map $\Psi_{1,L}(h)$ for $h \in \mathbb{H}_L$ should be thought of as the restriction of the action of h to the plane L represented in our basis of $L(\mathbb{Z})$. Analogously, we have

$$\Psi_{2,L} : h \in \mathbb{H}_L \mapsto \pi_2(A_{2,L}P(h)A_{2,L}^{-1}) \in \mathrm{Stab}_{\mathrm{SL}_2}(q_{L^\perp}) =: \mathbb{H}_{q_{L^\perp}}.$$

when projecting to the lower right block. Observe furthermore that $\Psi_{1,L}(h)$ is trivial if and only if $h \in \mathbb{H}_L^{\mathrm{pt}}$ and that $\Psi_{2,L}(h)$ is trivial if and only if $h \in \mathbb{H}_{L^\perp}^{\mathrm{pt}}$. In Appendix B the above isogenies (and also the isogenies for the accidental CM points defined below) are computed explicitly in a special case.

Lemma 4.1 (About the image)**.** *Let $\mathbb{K}$ be a field with $\mathrm{char}(\mathbb{K}) = 0$ and let $L \in \mathcal{R}_D$. The maps $\Psi_{1,L} : \mathbb{H}_L(\mathbb{K}) \to \mathbb{H}_{q_L}(\mathbb{K})$ and $\Psi_{2,L} : \mathbb{H}_L(\mathbb{K}) \to \mathbb{H}_{q_{L^\perp}}(\mathbb{K})$ are surjective. In particular, the natural map induced by $\Psi_{1,L}$*

$$\mathbb{H}_L(\mathbb{Q})\backslash \mathbb{H}_L(\mathbb{A}) / \mathbb{H}_L(\mathbb{R}\times\widehat{\mathbb{Z}}) \to \mathbb{H}_{q_L}(\mathbb{Q})\backslash \mathbb{H}_{q_L}(\mathbb{A}) / \mathbb{H}_{q_L}(\mathbb{R}\times\widehat{\mathbb{Z}})$$

is surjective (and similarly for $\Psi_{2,L}$).

Proof. It suffices to show that the restriction ψ of $\Psi_{1,L}$ to $\mathbb{H}_{a_1(L)}$ is a $\mathbb{Q}$-isomorphism. Now note that the kernel of ψ is $\mathbb{H}_{a_1(L)} \cap \mathbb{H}_L^{\mathrm{pt}}$ and thus trivial by Lemma 2.9. As an injective $\mathbb{Q}$-homomorphism between $\mathbb{Q}$-tori of rank 1 is a $\mathbb{Q}$-isomorphism. (We remark that the inverse can be explicitly constructed in the case at hand.) □

For the accidental CM points the analogous maps are given by

$$\Psi_{3,L} : h \in \mathbb{H}_L \mapsto \pi(A_{3,L}P_1(h)A_{3,L}^{-1}) \in \mathrm{Stab}_{\mathrm{SL}_2}(q_{a_1(L)}) =: \mathbb{H}_{q_{a_1(L)}},$$
$$\Psi_{4,L} : h \in \mathbb{H}_L \mapsto \pi(A_{4,L}P_2(h)A_{4,L}^{-1}) \in \mathrm{Stab}_{\mathrm{SL}_2}(q_{a_2(L)}) =: \mathbb{H}_{q_{a_2(L)}}$$

and are also defined over $\mathbb{Q}$. The analogue of Lemma 4.1 in this case states that the image of the $\mathbb{K}$-points under these isogenies is the set of squares and similarly for the class groups. We refer to [Wie18, Sec. 7.1.1] for a thorough discussion of this, see also [EMV13, Sec. 4.2].

Overall, we define the $\mathbb{Q}$-group $\mathbb{T}_L < \mathrm{SU}_2^2 \times \mathrm{SL}_2^4$ to be the group consisting of points of the form

$$t_L(h) := \big(h, \Psi_{1,L}(h), \Psi_{2,L}(h), \Psi_{3,L}(h), \Psi_{4,L}(h)\big) \tag{4.1}$$

for $h \in \mathbb{H}_L$.

4.2. **S-arithmetic setup.** For any locally compact group G we denote by m_G a Haar measure on G. Furthermore, for a quotient $\Gamma \setminus G$ by a lattice Γ we write $m_{\Gamma \setminus G}$ for the unique G-invariant probability measure where G acts via $g.(\Gamma g') = \Gamma g' g^{-1}$.

Given a set of places $S \subseteq V_{\mathbb{Q}} = \{\infty, 2, 3, 5, \ldots,\}$ of $\mathbb{Q}$ we set $\mathbb{Q}_S$ to be the restricted product of the $\mathbb{Q}_p$ for $p \in S \setminus \{\infty\}$ and $\mathbb{Q}_\infty = \mathbb{R}$ if $\infty \in S$. Furthermore, we set $\mathbb{Z}^S = \mathbb{Z}[\frac{1}{p} : p \in S \setminus \{\infty\}]$ and $\widehat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p$. If $\mathbb{G}$ is a semisimple algebraic group defined over $\mathbb{Q}$, the subgroup $\mathbb{G}(\mathbb{Z}^S) < \mathbb{G}(\mathbb{Q}_S)$ is a lattice by a Theorem of Borel and Harish-Chandra if $\infty \in S$. Here and in the following, we identify $\mathbb{G}(\mathbb{Z}^S)$ with its image under the diagonal embedding into $\mathbb{G}(\mathbb{Q}_S)$. The group $\mathbb{G}$ is said to have class number one if for all S containing the archimedean place

$$\mathbb{G}(\mathbb{Q}_S) = \mathbb{G}(\mathbb{Z}^S)\, \mathbb{G}\Big(\mathbb{R} \times \prod_{p \in S \text{ prime}} \mathbb{Z}_p\Big).$$

The class number one property in particular implies that there are well-defined projections $\mathbb{G}(\mathbb{Z}^S) \setminus \mathbb{G}(\mathbb{Q}_S) \to \mathbb{G}(\mathbb{Z}^{S'}) \setminus \mathbb{G}(\mathbb{Q}_{S'})$ when $\infty \in S' \subseteq S$ by taking the quotient with $\mathbb{G}\Big(\prod_{p \in S \setminus S'} \mathbb{Z}_p\Big)$ from the right.

In this paper we will consider the groups SU_2, SL_2 and products of these, all of which have class number one (see [EMV13, p. 29] for SU_2). Furthermore, we will use the S-arithmetic extensions

$$X_{1,S} = X_{2,S} = {\mathrm{SU}_2(\mathbb{Z}^S)}\backslash{\mathrm{SU}_2(\mathbb{Q}_S)},$$
$$X_{3,S} = X_{4,S} = X_{5,S} = X_{6,S} = {\mathrm{SL}_2(\mathbb{Z}^S)}\backslash{\mathrm{SL}_2(\mathbb{Q}_S)}.$$

of the real quotients $\mathrm{SU}_2(\mathbb{Z}) \setminus \mathrm{SU}_2(\mathbb{R})$ and $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathrm{SL}_2(\mathbb{R})$. For simplicity we write $X_{n,\infty} = X_{n,\{\infty\}},\ X_{n,\mathbb{A}} = X_{n,V_{\mathbb{Q}}}$ for $n = 1, \ldots, 6$. Also, let

$$\mathbb{G} = \mathrm{SU}_2 \times \mathrm{SU}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2$$

and

$$X_S = {\mathbb{G}(\mathbb{Z}^S)}\backslash{\mathbb{G}(\mathbb{Q}_S)} = \prod_{n=1}^{6} X_{n,S}$$

for any set of places S as above.

4.3. **Toral packets and the dynamical result.** Let $L \in \mathrm{Gr}_{2,4}(\mathbb{Q})$ be a rational plane. Following the discussion in Section 4.1 we will study orbits in X_S under the $\mathbb{Q}_S$-points of the $\mathbb{Q}$-group $\mathbb{T}_L$. First, let us consider the compact adelic orbit $\mathbb{G}(\mathbb{Q})\mathbb{T}_L(\mathbb{A}) \subseteq X_{\mathbb{A}}$. The projection $\mathcal{O}_L$ of this orbit to X_S, where $S = \{\infty, p, q\}$ and p, q are two distinct odd primes is an example of a *homogeneous toral packet*, see [ELMV11, Sec. 4,5] for this terminology.

In order to normalize the behavior on the real quotient X_∞ we choose for every plane $L \in \mathrm{Gr}_{2,4}(\mathbb{Q})$ an element $\ell_L \in \mathbb{G}(\mathbb{R})$ such that

$$\ell_L^{-1}\mathbb{T}_L(\mathbb{R})\ell_L < K := \mathrm{Stab}_{\mathrm{SU}_2^2(\mathbb{R})}(\langle 1, \mathrm{i}\rangle) \times \mathrm{SO}(2)^4$$

and also consider the pushed packet $\ell_L^{-1}.\mathcal{O}_L$. Furthermore, let μ_L be the pushforward of the normalized Haar measure on the shifted orbit $\mathbb{G}(\mathbb{Q})\mathbb{T}_L(\mathbb{A})\ell_L$ to $\ell_L^{-1}.\mathcal{O}_L$ (under the natural projection to X_S).

In the following we shall call a sequence $(L_n)_n$ of rational planes in $\mathbb{R}^4$ *admissible* (with respect to p, q) if the following conditions are satisfied:

- For every n the discriminant $\mathrm{disc}(L_n) = D_n$ satisfies the assumptions in Theorem 1.2 for the fixed primes p, q.
- As n goes to infinity
$$Q(\widetilde{a}_1(L_n)),\ Q(\widetilde{a}_2(L_n)),\ \frac{Q(\widetilde{a}_1(L_n))Q(\widetilde{a}_2(L_n))}{\mathrm{disc}(L_n)}$$
go to infinity. Here, $\widetilde{a}_1(L_n)$, $\widetilde{a}_2(L_n)$ denote the primitive vectors in the half-lines $\mathbb{Q}_+a_1(L_n)$, $\mathbb{Q}_+a_2(L_n)$ as in Proposition 3.2.

We remark that the second condition is automatically satisfied if the discriminants D_n are square-free or more generally if the square-free part of D_n goes to infinity.

The following implies our main theorem (Theorem 1.2).

Theorem 4.2 (Equidistribution of packets)**.** *Let $(L_n)_n$ be an admissible sequence of rational planes. Then $\mu_{L_n} \to m_{X_S}$ as $n \to \infty$.*

5. Proof of the main theorem from the dynamical version

In this section we show that Theorem 4.2 does indeed imply Theorem 1.2. For this we will use adelic orbits of the form $\mathbb{G}(\mathbb{Q})\mathbb{T}_L(\mathbb{A}) \subseteq X_{\mathbb{A}}$ for some $L \in \mathcal{R}_D$ in order to generate additional points in $\mathcal{J}_D$ as in Theorem 1.2 from one such point (see for instance [PR94, Thm. 8.2]).

Let $L \in \mathrm{Gr}_{2,4}(\mathbb{Q})$ be a rational plane. Recall that the class number

$$\left| \mathbb{T}_L(\mathbb{Q}) \backslash \mathbb{T}_L(\mathbb{A}) / \mathbb{T}_L(\mathbb{R} \times \widehat{\mathbb{Z}}) \right| \tag{5.1}$$

of the group $\mathbb{T}_L$ is finite (c.f. [PR94, Thm. 5.1]) and that $\mathbb{G} = \mathrm{SU}_2^2 \times \mathrm{SL}_2^4$ has class number one (i.e. $\mathbb{G}(\mathbb{Q})\mathbb{G}(\mathbb{R} \times \widehat{\mathbb{Z}}) = \mathbb{G}(\mathbb{A})$). We may thus write

$$\mathbb{G}(\mathbb{Q})\mathbb{T}_L(\mathbb{A}) = \bigsqcup_{\rho \in \mathcal{M}_L} \mathbb{G}(\mathbb{Q})\rho\mathbb{T}_L(\mathbb{R} \times \widehat{\mathbb{Z}}) \tag{5.2}$$

for a finite set $\mathcal{M}_L \subseteq \mathbb{G}(\mathbb{R} \times \widehat{\mathbb{Z}})$ of representatives. Note that by construction the cardinality of $\mathcal{M}_L$ is the class number of $\mathbb{T}_L$ in (5.1).

We now construct points in $\mathrm{SU}_2^2(\mathbb{Z}) \backslash \mathcal{J}_D$ using the above stabilizer orbit, where $\mathrm{SU}_2^2(\mathbb{Z})$ acts naturally on $\mathcal{R}_D$ not affecting the other components. We will implicitly identify $\mathrm{Gr}_{2,4}(\mathbb{Q})$ with the image in $\mathrm{Gr}_{2,4}(\mathbb{A})$ under the injective map

$$L \in \mathrm{Gr}_{2,4}(\mathbb{Q}) \mapsto L \otimes_{\mathbb{Q}} \mathbb{A} \in \mathrm{Gr}_{2,4}(\mathbb{A})$$

and analogously for binary quadratic forms with rational coefficients. In the following, points $g \in \mathbb{G}(\mathbb{A})$ will sometimes be written as $g = (g_1, \ldots, g_6)$ for the corresponding elements $g_1, g_2 \in \mathrm{SU}_2(\mathbb{A})$ and $g_3, g_4, g_5, g_6 \in \mathrm{SL}_2(\mathbb{A})$.

Proposition 5.1 (Generating integer points)**.** *Let $L \in \mathcal{R}_D$ be a rational plane and let $g \in \mathbb{G}(\mathbb{R} \times \widehat{\mathbb{Z}})$ with $\mathbb{G}(\mathbb{Q})g \in \mathbb{G}(\mathbb{Q})\mathbb{T}_L(\mathbb{A})$.*

(i) The plane $L_g = (g_1, g_2).L$ is rational and has the same discriminant as L. Furthermore,
$$Q(\widetilde{a}_1(L_g)) = Q(\widetilde{a}_1(L)), \quad Q(\widetilde{a}_2(L_g)) = Q(\widetilde{a}_2(L)).$$

(ii) The quadratic form $g_3.q_L$ is an integral binary form and is equivalent to q_{L_g}. The analogous statement also holds for $q_{L^\perp}$, $q_{a_1(L)}$ and $q_{a_2(L)}$.

It follows that for any $\rho \in \mathcal{M}_L$ we obtain a corresponding point in the set $\mathcal{J}_D$ and in particular a rational plane L_ρ.

Proof. Choose $t \in \mathbb{T}_L(\mathbb{A})$ and $\gamma \in \mathbb{G}(\mathbb{Q})$ such that $\gamma t = g$ and write $t = t_L(h)$ as in (4.1) for some $h \in \mathbb{H}_L(\mathbb{A})$.

To see (i) notice first that L_g is rational as

$$L_g = (g_1, g_2).L = (\gamma_1, \gamma_2)h.L = (\gamma_1, \gamma_2).L. \tag{5.3}$$

To compute the discriminant let v_1, v_2 be a $\mathbb{Z}$-basis of $L(\mathbb{Z})$. Recall that for any group G acting on a module V there is a natural corresponding action of G on $\bigwedge^2 V$ given by $g.(w_1 \wedge w_2) = (g.w_1) \wedge (g.w_2)$ for $w_1, w_2 \in V$. We observe

$$\begin{aligned}\textstyle\bigwedge^2(\mathbb{R} \times \widehat{\mathbb{Z}})^4 \ni (g_1, g_2).(v_1 \wedge v_2) &= (\gamma_1 h_1, \gamma_2 h_2).(v_1 \wedge v_2) \\ &= (\gamma_1, \gamma_2).(v_1 \wedge v_2) \in \textstyle\bigwedge^2 \mathbb{Q}^4\end{aligned}$$

since $h = (h_1, h_2)$ preserves L. As $\mathbb{Q} \cap (\mathbb{R} \times \widehat{\mathbb{Z}}) = \mathbb{Z}$ it follows that $(g_1, g_2).(v_1 \wedge v_2)$ is integral.

To show primitivity we write $g_{1,p}, g_{2,p} \in \mathrm{SU}_2(\mathbb{Z}_p)$ for the p-adic coordinate of g_1, g_2. Then

$$\|(g_1, g_2).(v_1 \wedge v_2)\|_p = \|(g_{1,p}, g_{2,p}).(v_1 \wedge v_2)\|_p = \|v_1 \wedge v_2\|_p = 1$$

for all p (for the maximum norm[5] $\|\cdot\|_p$ on the wedge product). Therefore, $(g_1, g_2).(v_1 \wedge v_2)$ is primitive. Hence, the Euclidean norm of $(g_1, g_2).(v_1 \wedge v_2)$ is exactly the discriminant of L_g. As $g_1, g_2 \in \mathrm{SU}_2$ the former is the Euclidean norm of $v_1 \wedge v_2$ which in turn is the discriminant of L.

It remains to show the equality for the lengths of the primitive vectors. By the equivariance in Proposition 2.1, we have $a_1(L_g) = g_1.a_1(L)$. As above, it follows from considering every prime that $g_1.\widetilde{a}_1(L)$ as a multiple of $a_1(L_g) = g_1.a(L)$ is primitive. Thus, $Q(\widetilde{a}_1(L_g)) = Q(g_1.\widetilde{a}_1(L)) = Q(\widetilde{a}_1(L))$ as desired. The argument for $\widetilde{a}_2(L_g)$ is analogous.

For (ii) we begin by showing that $g_3.q_L$ is an integral form. To this end, we just note that

$$g_3.q_L = \gamma_3 t_3.q_L = \gamma_3.q_L$$

where the form on the left has coefficients in $\mathbb{R} \times \widehat{\mathbb{Z}}$ and the form on the right has coefficients in $\mathbb{Q}$. The analogous argument shows that $g_4.q_{L^\perp}$ is integral.

We now wish to show that $\gamma_3.q_L$ and q_{L_g} are equivalent. Recall that (as is implicit in the definition of q_L resp. q_{L_g}) we have chosen a matrix $A_{1,L} \in \mathrm{SL}_4(\mathbb{Z})$ (resp. $A_{1,L_g} \in \mathrm{SL}_4(\mathbb{Z})$) so that the first two rows form a basis of $L(\mathbb{Z})$ (resp. $L_g(\mathbb{Z})$).

Now notice that

$$\begin{aligned}\gamma_3.q_L(u) &= Q((u\gamma_3, 0)A_{1,L}) = Q((u\gamma_3, 0)A_{1,L}P(\gamma_1, \gamma_2)^{-1}) \\ &= Q\big((u\gamma_3, 0)A_{1,L}P(\gamma_1, \gamma_2)^{-1}A_{1,L_g}^{-1}A_{1,L_g}\big) = Q((u, 0)CA_{1,L_g})\end{aligned}$$

where

$$C = \begin{pmatrix}\gamma_3 & 0 \\ 0 & \mathrm{id}\end{pmatrix} A_{1,L}P(\gamma_1, \gamma_2)^{-1}A_{1,L_g}^{-1} \in \mathrm{Mat}_4(\mathbb{Q}).$$

Observe that C (acting on row vectors) maps $\mathbb{R}^2 \times \{(0,0)\}$ to itself. Indeed, $A_{1,L}$ maps $\mathbb{R}^2 \times \{(0,0)\}$ to L, by (5.3) $P(\gamma_1, \gamma_2)^{-1}$ maps L to L_g, and finally A_{1,L_g}^{-1} maps L_g back to $\mathbb{R}^2 \times \{(0,0)\}$. In other words, C is of the block form $\left(\begin{array}{c|c} * & 0 \\ \hline * & * \end{array}\right)$. Denoting

[5] To define the norm $\|\cdot\|_p$ one chooses a $\mathbb{Z}_p$-basis of $\bigwedge^2 \mathbb{Z}_p^4$ and takes the maximum of p-adic absolute values of the coordinates in this basis.

by $\pi_1(C)$ the projection onto the upper left block (as in Section 3.1) the above calculation can be summarized as $\gamma_3.q_L(u) = \pi_1(C).q_{L_g}(u)$.

We want to show that $\pi_1(C) \in \mathrm{GL}_2(\mathbb{Z})$. To see that $\pi_1(C)$ is integral, we use the third component of $\gamma t = g$ together with (4.1) to obtain

$$\begin{aligned}\pi_1(C) &= \gamma_3\pi_1\left(A_{1,L}P(\gamma_1,\gamma_2)^{-1}A_{1,L_g}^{-1}\right)\\ &= g_3\underbrace{\pi_1\left(A_{1,L}P(h^{-1})A_{1,L}^{-1}\right)}_{=t_3^{-1}=\Psi_{1,L}(h^{-1})}\pi_1\left(A_{1,L}P(\gamma_1,\gamma_2)^{-1}A_{1,L_g}^{-1}\right)\\ &= g_3\pi_1\left(A_{1,L}P(h^{-1})P(\gamma_1,\gamma_2)^{-1}A_{1,L_g}^{-1}\right) = g_3\pi_1\left(A_{1,L}P(g_1,g_2)^{-1}A_{1,L_g}^{-1}\right)\\ &\in \mathrm{Mat}_2(\mathbb{Q})\cap\mathrm{Mat}_2(\mathbb{R}\times\widehat{\mathbb{Z}}) = \mathrm{Mat}_2(\mathbb{Z}).\end{aligned}$$

We note that $A_{1,L}P(g_1,g_2)^{-1}A_{1,L_g}^{-1} \in \mathrm{GL}_4(\mathbb{R}\times\widehat{\mathbb{Z}})$ is a block matrix with 0 in the right top 2-by-2 block, which implies that the upper left block

$$\pi_1\left(A_{1,L}P(g_1,g_2)^{-1}A_{1,L_g}^{-1}\right)$$

and hence also $\pi_1(C) = g_3\pi_1\left(A_{1,L}P(g_1,g_2)^{-1}A_{1,L_g}^{-1}\right) \in \mathrm{GL}_2(\mathbb{R}\times\widehat{\mathbb{Z}})$ are invertible. This implies that $\pi_1(C) \in \mathrm{GL}_2(\mathbb{Z})$ as claimed.

This concludes (ii) for q_L. The argument to verify that $g_4.q_{L^\perp}$ is equivalent to $q_{L_g^\perp}$ is completely analogous.

For the remaining copies one can use the equivariance property in Proposition 2.1 to reduce the statement to [AES16b, Prop. 3.2]. □

For $L \in \mathcal{R}_D$ we have by definition of the generated planes in Proposition 5.1 that $L_{\gamma\rho t} = \gamma.L_\rho$ for $\rho \in \mathcal{M}_L$, $t \in \mathbb{T}_L(\mathbb{R}\times\widehat{\mathbb{Z}})$ and $\gamma \in \mathrm{SU}_2^2(\mathbb{Z})$ and the analogous statement holds for the binary forms. The function

$$\mathbb{G}(\mathbb{Q})\mathbb{T}_L(\mathbb{A}) \to \mathrm{SU}_2^2(\mathbb{Z})\backslash\mathcal{J}_D \tag{5.4}$$

which maps $\mathbb{G}(\mathbb{Q})\rho t$ for $\rho \in \mathcal{M}_L$ and $t \in \mathbb{T}_L(\mathbb{R}\times\widehat{\mathbb{Z}})$ to $\mathrm{SU}_2^2(\mathbb{Z}).L_\rho$ and the attached CM points is thus well-defined (i.e. independent of the choice of $\mathcal{M}_L$).

Call a plane $L \in \mathcal{R}_D$ *exceptional* if the finite group $\mathbb{H}'_L(\mathbb{Z})$ strictly contains $\{(\pm1,\pm1)\}$ where $\mathbb{H}'_L = \{g \in \mathrm{SU}_2^2 : g.L \subseteq L\}$ denotes the full stabilizer subgroup.

Proposition 5.2 (On the collection of generated points)**.** *Let $L \in \mathcal{R}_D$ for $D \in \mathbb{D}$.*

(a) Every fiber of the map in (5.4) *is a union of at most two $\mathbb{T}_L(\mathbb{R}\times\widehat{\mathbb{Z}})$-orbits.*
(b) Amongst the fibers in (5.4) *of non-exceptional planes the number of $\mathbb{T}_L(\mathbb{R}\times\widehat{\mathbb{Z}})$-orbits is equal.*
(c) The set of exceptional planes in $\mathcal{R}_D$ is of size $D^{o(1)}$.
(d) The volume of the $\mathbb{T}_L(\mathbb{R}\times\widehat{\mathbb{Z}})$-orbit through $\mathbb{G}(\mathbb{Q})\rho$ is independent of $\rho \in \mathcal{M}_L$.

We will call the image of (5.4) the *packet* attached to L and denote it by $\mathcal{P}(L)$.

Proof. We begin by proving parts (a) and (b). Clearly, if two points lie on the same $\mathbb{T}_L(\mathbb{R}\times\widehat{\mathbb{Z}})$-orbit, they give rise to the same point in $\mathrm{SU}_2^2(\mathbb{Z})\setminus\mathcal{J}_D$. By Proposition 5.1(ii) it suffices to prove the analogous statement to (a) and (b) for the fibers of the map

$$\mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_L(\mathbb{A}) \to \mathrm{SU}_2^2(\mathbb{Z})\backslash\mathcal{R}_D. \tag{5.5}$$

To prove this, we first claim that we can view the fibers as orbits under the group

$$F_L = \left\{ h' \in \mathbb{H}'_L(\mathbb{R} \times \widehat{\mathbb{Z}}) \mid \mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_L(\mathbb{A})h' = \mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_L(\mathbb{A}) \right\}.$$

By definition of F_L and the generated planes in Proposition 5.1, the fiber through a point $x \in \mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_L(\mathbb{A})$ contains xF_L. Conversely, if $y \in \mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_L(\mathbb{A})$ is another point in the fiber through x, we write $x = \mathrm{SU}_2^2(\mathbb{Q})g_x$ and $y = \mathrm{SU}_2^2(\mathbb{Q})g_y$ for elements $g_x, g_y \in \mathrm{SU}_2^2(\mathbb{R} \times \widehat{\mathbb{Z}})$ and replace g_y if necessary so that $g_x.L = g_y.L$. Then $h' = g_x^{-1}g_y$ is an element of $\mathbb{H}'_L(\mathbb{A}) \cap \mathrm{SU}_2^2(\mathbb{R} \times \widehat{\mathbb{Z}}) = \mathbb{H}'_L(\mathbb{R} \times \widehat{\mathbb{Z}})$ and satisfies $xh' = y$. Moreover, since $\mathbb{H}_L < \mathbb{H}'_L$ is normal

$$\mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_L(\mathbb{A})h' = x\mathbb{H}_L(\mathbb{A})h' = xh'\mathbb{H}_L(\mathbb{A}) = y\mathbb{H}_L(\mathbb{A}) = \mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_L(\mathbb{A})$$

and so $h' \in F_L$ as claimed.

To compute the number $n(x)$ of $\mathbb{H}_L(\mathbb{R} \times \widehat{\mathbb{Z}})$-orbits in the fiber xF_L through a point $x \in \mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_L(\mathbb{A})$ write $x = \mathrm{SU}_2^2(\mathbb{Q})g$ for $g \in \mathrm{SU}_2^2(\mathbb{R} \times \widehat{\mathbb{Z}})$. Then

$$\begin{aligned} n(x) &= \left| g^{-1}\,\mathrm{SU}_2^2(\mathbb{Q})g \cap F_L \backslash F_L /\ \mathbb{H}_L(\mathbb{R} \times \widehat{\mathbb{Z}}) \right| \\ &= \left| \mathrm{SU}_2^2(\mathbb{Q}) \cap gF_Lg^{-1} \backslash gF_Lg^{-1} /\ g\mathbb{H}_L(\mathbb{R} \times \widehat{\mathbb{Z}})g^{-1} \right|. \end{aligned}$$

Now note that $g\mathbb{H}_L(\mathbb{R} \times \widehat{\mathbb{Z}})g^{-1} = \mathbb{H}_{g.L}(\mathbb{R} \times \widehat{\mathbb{Z}})$ by definition of $\mathbb{H}_L$ and integrality of g. Also, we have that $gF_Lg^{-1} = F_{g.L}$. Indeed, as for any $h' \in F_L$ the element $gh'g^{-1}$ is in $g\mathbb{H}'_L(\mathbb{R} \times \widehat{\mathbb{Z}})g^{-1} = \mathbb{H}'_{g.L}(\mathbb{R} \times \widehat{\mathbb{Z}})$ and as

$$\begin{aligned} \mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_{g.L}(\mathbb{A})gh'g^{-1} &= \mathrm{SU}_2^2(\mathbb{Q})g\mathbb{H}_L(\mathbb{A})g^{-1}gh'g^{-1} = x\mathbb{H}_L(\mathbb{A})h'g^{-1} \\ &= \mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_L(\mathbb{A})h'g^{-1} = \mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_L(\mathbb{A})g^{-1} \\ &= \mathrm{SU}_2^2(\mathbb{Q})g\mathbb{H}_L(\mathbb{A})g^{-1} = \mathrm{SU}_2^2(\mathbb{Q})\mathbb{H}_{g.L}(\mathbb{A}). \end{aligned}$$

In particular, $gF_Lg^{-1} \cap \mathrm{SU}_2^2(\mathbb{Q}) \subseteq \mathbb{H}'_{g.L}(\mathbb{Z})$ and using normality of $\mathbb{H}_L$ in $\mathbb{H}'_L$ equality holds. We conclude that

$$\begin{aligned} n(x) &= \left| \mathbb{H}'_{g.L}(\mathbb{Z}) \setminus F_{g.L} \,/\, \mathbb{H}_{g.L}(\mathbb{R} \times \widehat{\mathbb{Z}}) \right| \\ &\leq [F_{g.L} : \mathbb{H}_{g.L}(\mathbb{R} \times \widehat{\mathbb{Z}})] = [F_L : \mathbb{H}_L(\mathbb{R} \times \widehat{\mathbb{Z}})]. \end{aligned} \tag{5.6}$$

To prove the claim in (a) notice first that by (5.6) it suffices to estimate the index $[F_L : \mathbb{H}_L(\mathbb{R} \times \widehat{\mathbb{Z}})]$. For this, observe that if $h' \in F_L$ satisfies $h'_\infty \in \mathbb{H}_L(\mathbb{R})$ then $h' \in \mathbb{H}_L(\mathbb{R} \times \widehat{\mathbb{Z}})$. Indeed, we can write the point $\mathrm{SU}_2^2(\mathbb{Q})h'$ as $\mathrm{SU}_2^2(\mathbb{Q})h$ for $h \in \mathbb{H}_L(\mathbb{A})$ and so there is $\gamma \in \mathrm{SU}_2^2(\mathbb{Q})$ with $\gamma h = h'$. Thus, $\gamma = h'h^{-1} \in \mathbb{H}'_L(\mathbb{Q})$ and since $h'_\infty \in \mathbb{H}_L(\mathbb{R})$ we further have $\gamma = h'_\infty h_\infty^{-1} \in \mathbb{H}_L(\mathbb{R})$ so that $\gamma \in \mathbb{H}_L(\mathbb{Q})$. This proves that $h' = \gamma h \in \mathbb{H}_L(\mathbb{A}) \cap \mathbb{H}'_L(\mathbb{R} \times \widehat{\mathbb{Z}}) = \mathbb{H}_L(\mathbb{R} \times \widehat{\mathbb{Z}})$. As the index of $\mathbb{H}_L(\mathbb{R})$ in $\mathbb{H}'_L(\mathbb{R})$ is 2, $[F_L : \mathbb{H}_L(\mathbb{R} \times \widehat{\mathbb{Z}})] \leq 2$ and (5.6) implies the claim in (a).

To see (b), note that if the plane $g.L$ generated by x is non-exceptional, we have $\mathbb{H}'_{g.L}(\mathbb{Z}) = \{(\pm 1, \pm 1)\} = \mathbb{H}_{g.L}(\mathbb{Z})$ which is contained in the center. In this case, equality holds in equation (5.6). Since the right hand side in (5.6) is independent of the point $x = \mathrm{SU}_2^2(\mathbb{Q})g$, this proves (b).

For (c) it suffices to show that for any $g \in \mathrm{SU}_2^2(\mathbb{Z}) \setminus \{(\pm 1, \pm 1)\}$ the number of planes $L' \in \mathcal{R}_D$ with $g.L' = L'$ is of size $D^{o(1)}$. We decompose $\mathbb{R}^4$ into irreducible invariant subspaces V_n for g. First, observe that if one of the V_n is 2-dimensional, g can only stabilize one plane L' (and its orthogonal complement) and thus the claim follows in this case. So suppose that $\dim(V_n) = 1$ for every n. Since the action of

g has determinant one and $g \neq (\pm 1, \pm 1)$, there must be exactly two 1-dimensional subspaces, say V_1, V_2, such that $g|_{V_1} = 1$ and $g|_{V_2} = 1$. Let $L_0 = V_1 \oplus V_2$. If L' is a plane with $g.L' \subseteq L'$ then either $L' \in \{L_0, L_0^\perp\}$ or $\dim(L_0 \cap L') = \dim(L_0^\perp \cap L') = 1$. In the latter case, g is a reflection when restricted to L' and therefore $g_1.a_1(L') = -a_1(L')$ and $g_2.a_2(L') = -a_2(L')$. This shows that $a_1(L') \perp a_1(L_0)$ and $a_2(L') \perp a_2(L_0)$ as g_1, g_2 act by orthogonal transformations and preserve $a_1(L_0)$ resp. $a_2(L_0)$. So the latter case corresponds to counting the number of representations of D by an integral binary form, which is of order $D^{o(1)}$ (cf. [Cas78, p. 372]). Thus, the number of such pairs $(a_1(L'), a_2(L'))$ is $D^{o(1)}$. This proves (c).

For (d) observe that for any $\rho \in \mathcal{M}_L$

$$\begin{aligned}\mathrm{Stab}_{\mathbb{T}_L(\mathbb{R}\times\widehat{\mathbb{Z}})}(\mathbb{G}(\mathbb{Q})\rho) &= \mathrm{Stab}_{\mathbb{T}_L(\mathbb{R}\times\widehat{\mathbb{Z}})}(\mathbb{G}(\mathbb{Q})t) = \mathrm{Stab}_{\mathbb{T}_L(\mathbb{R}\times\widehat{\mathbb{Z}})}(\mathbb{G}(\mathbb{Q})) \\ &= \mathbb{T}_L(\mathbb{R}\times\widehat{\mathbb{Z}}) \cap \mathbb{G}(\mathbb{Q}) = \mathbb{T}_L(\mathbb{Z})\end{aligned}$$

where $t \in \mathbb{T}_L(\mathbb{A})$ was chosen with $\mathbb{G}(\mathbb{Q})\rho = \mathbb{G}(\mathbb{Q})t$ and where we used that $\mathbb{T}_L$ is abelian in the second equality. □

Remark 5.3 (Decomposing into packets). Note that given two planes $L, L' \in \mathcal{R}_D$ the question whether or not L' can be generated from L as in Proposition 5.1 is equivalent to asking whether or not $\gamma \in \mathrm{SU}_2^2(\mathbb{Q})$ and $g \in \mathrm{SU}_2^2(\mathbb{R}\times\widehat{\mathbb{Z}})$ exist with $\gamma.L = g.L = L'$. This defines an equivalence relation and hence we can decompose the set $\mathrm{SU}_2^2(\mathbb{Z}) \setminus \mathcal{J}_D$ into disjoint packets.

Let $L \in \mathcal{R}_D$ for $D \in \mathbb{D}$. We now project the set in (5.2) onto the $S = \{\infty, p, q\}$-arithmetic quotient X_S to obtain the packet of orbits

$$\mathcal{O}_L = \bigsqcup_{\rho \in \mathcal{M}_L} \mathbb{G}(\mathbb{Z}^S)(\rho_\infty, \rho_p, \rho_q)\mathbb{T}_L(\mathbb{R}\times\mathbb{Z}_p\times\mathbb{Z}_q) \subseteq X_S$$

invariant under $\mathbb{T}_L(\mathbb{Q}_S)$. The union is still disjoint: If $x = \mathbb{G}(\mathbb{Q})t$, $x' = \mathbb{G}(\mathbb{Q})t'$ have the same image in $\mathcal{O}_L$ there exists $g \in \mathbb{G}(\prod_{\sigma\notin S}\mathbb{Z}_\sigma)$ and $\gamma \in \mathbb{G}(\mathbb{Q})$ with $\gamma t = t'g$. In particular, this equation at the infinite place yields $\gamma \in \mathbb{T}_L(\mathbb{Q})$ so that $g \in \mathbb{G}(\prod_{\sigma\notin S}\mathbb{Z}_\sigma) \cap \mathbb{T}(\mathbb{A}) = \mathbb{T}_L(\prod_{\sigma\notin S}\mathbb{Z}_\sigma)$ as desired. Note that the projection (5.4) factors through the projection to $\mathcal{O}_L$.

Proof of Theorem 1.2 assuming Theorem 4.2. For any plane $L \in \mathrm{Gr}_{2,4}(\mathbb{Q})$ choose an element $\ell_L \in \mathbb{G}(\mathbb{R})$ with $\ell_L^{-1}\mathbb{T}_L(\mathbb{R})\ell_L < K$. By Theorem 4.2 we know that $\mu_{L_n} \to m_{X_S}$ along any admissible sequence $(L_n)_n$. In particular, the convergence holds after pushforward to the real quotient X_∞ and to

$$X_\infty/K = \left(\mathrm{SU}_2^2(\mathbb{Z})\backslash \mathrm{Gr}_{2,4}(\mathbb{R})\right) \times \mathcal{X}_2^4 =: Y. \tag{5.7}$$

For any $D \in \mathbb{D}$ and $L \in \mathcal{R}_D$ we let ν_L be the normalized sum of Dirac measures over the packet $\mathcal{P}(L) \subseteq \mathcal{J}_D^Y = \mathrm{SU}_2^2(\mathbb{Z}) \setminus \mathcal{J}_D$ attached to L – see Proposition 5.2. By part (b)-(d) of that proposition, the pushforward measure on μ_L to Y and ν_L differ for $f \in C(Y)$ by at most $\|f\|_\infty D^{-1+o(1)}$ as the weights of these measures on $\mathcal{P}(L)$ need to be changed by at most 1 on exceptional planes only. So the measures ν_{L_n} are also equidistributing as $n \to \infty$.

By a similar argument, the sets $\mathcal{J}_D$ equidistribute in $\mathrm{Gr}_{2,4}(\mathbb{R}) \times \mathcal{X}_2^4$ if and only if the sets $\mathcal{J}_D^Y$ equidistribute in Y. We claim that the latter is true.

To see this, write the set $\mathcal{J}_D^Y$ for $D \in \mathbb{D}$ with $-D \in (\mathbb{F}_p^\times)^2$ and $-D \in (\mathbb{F}_q^\times)^2$ as a disjoint union of packets – see Proposition 5.1(i). Let $\mathscr{G}_D$ be the union of the packets attached to planes $L_D \in \mathcal{R}_D$ with $Q(\widetilde{a}_1(L_D)) \geq D^{\frac{2}{3}}$ and $Q(\widetilde{a}_2(L_D)) \geq D^{\frac{2}{3}}$.

Recall from Corollary 2.7 that $\mathcal{J}_D^Y$ is of size $D^{1+o(1)}$. Also, observe that the number of pairs of primitive integer points where one of the points has quadratic value at most $D^{\frac{2}{3}}$ is of size $D^{\frac{1}{2}+o(1)}D^{\frac{1}{3}+o(1)} = D^{\frac{5}{6}+o(1)}$ (see the proof of Corollary 2.7). Thus, the sets $\mathcal{J}_D^Y$ equidistribute if and only if the subsets $\mathscr{G}_D$ equidistribute.

However, by Theorem 4.2 and the above discussion any sequence of packets $\mathcal{P}(L_D) \subseteq \mathscr{G}_D$ equidistributes since

$$\frac{Q(\widetilde{a}_1(L_D))Q(\widetilde{a}_2(L_D))}{D} \geq D^{\frac{1}{3}}$$

(which implies admissibility of the underlying planes L_D). This implies that the sets $\mathscr{G}_D$ equidistribute (as finite unions of equidistributing subsets) and hence concludes the proof of Theorem 1.2. □

6. Proof of Theorem 4.2

Let $(L_j)_j$ be a sequence of admissible planes so that the sequence of measures $\mu_j = \mu_{L_j}$ converges to a measure μ. We want to show that μ is the normalized Haar measure m_{X_S} on $X_S = \mathbb{G}(\mathbb{Z}^S) \setminus \mathbb{G}(\mathbb{Q}_S)$. Since the limit μ is then independent of the arbitrarily chosen sequence $(L_j)_j$, this implies Theorem 4.2. To prove that $\mu = m_{X_S}$ we will use the fact that the pushforward of μ under all projections to the factors in X_S is the Haar measure on the respective factor and then apply a joinings classification of Lindenstrauss and the second named author [EL17].

Proposition 6.1 (Limit measures are joinings)**.** *The push-forward of μ under any projection $X_S \to X_{i,S}$ for $i = 1, \ldots, 6$ is the Haar measure on $X_{i,S}$. In particular, μ is a probability measure.*

This proposition should be seen as a version of Duke's Theorem [Duk88] or its strengthenings to subcollections (see specifically [HM06]). As we assume splitting conditions, it may be proven by means of Linnik's ergodic method [Lin68], since the total volume of the packets we consider is large enough in each factor.

- For the first four components this follows from the fact the packets correspond to the set of squares in the attached Picard group – see Lemma 4.1 (in the case of the factors $X_{3,S}$ and $X_{4,S}$) and [Wie18, Lemma 7.2]. Since the 2-torsion of the Picard group has size $D^{o(1)}$ (see e.g. [Cas78, p. 342]), the total volume of the packets is large enough in these components.
- In the fifth and the sixth component we then see the set of fourth powers (see for instance [EMV13, Sec. 4.2]) which is large as the 4-torsion can also be bounded by $D^{o(1)}$.

Thus, one can apply the ergodic method in this situation (see [Wie18]).

Essential to the characterization of the joining μ is the fact that μ exhibits invariance under a higher rank diagonalizable action. This is the reason why the additional congruence conditions in Theorem 1.2 are needed (see also Lemma 2.10).

Lemma 6.2. *There exist planes $\Lambda_p \subseteq \mathbb{Q}_p^4$ and $\Lambda_q \subseteq \mathbb{Q}_q^4$ so that μ is invariant under the two commuting, diagonalizable subgroups*

$$T_p := \big\{\big(h, \Psi_{1,\Lambda_p}(h), \Psi_{2,\Lambda_p}(h), \Psi_{3,\Lambda_p}(h), \Psi_{4,\Lambda_p}(h)\big) : h \in \mathbb{H}_{\Lambda_p}(\mathbb{Q}_p)\big\} \subseteq \mathbb{G}(\mathbb{Q}_p),$$
$$T_q := \big\{\big(h, \Psi_{1,\Lambda_q}(h), \Psi_{2,\Lambda_q}(h), \Psi_{3,\Lambda_q}(h), \Psi_{4,\Lambda_q}(h)\big)\big) : h \in \mathbb{H}_{\Lambda_q}(\mathbb{Q}_q)\big\} \subseteq \mathbb{G}(\mathbb{Q}_q).$$

In other words, μ is invariant under $\mathbf{T} = T_p \times T_q$. Furthermore, $\mathbf{T}$ contains a subgroup $\mathbf{A} \cong \mathbb{Z}^4$ of class-$\mathcal{A}'$, which acts ergodically with respect to the Haar measure on each factor $X_{i,S}$ where $i = 1, \ldots, 6$.

Here, the homomorphisms $\Psi_{1,\Lambda_p}, \Psi_{2,\Lambda_p}, \ldots$ can be defined as in Section 4.1.

For the general definition of the term *class-$\mathcal{A}'$* we refer to [EL17, Def.1.3]. In our case it suffices to show that the group $\mathbb{H}_{\Lambda_p}(\mathbb{Q}_p)$ contains a subgroup generated by some $h_1 \in \mathbb{H}_{a_1(\Lambda_p)}$ and $h_2 \in \mathbb{H}_{a_2(\Lambda_p)}$ each with eigenvalues $p^2, 1, p^{-2}$ and that the same holds for $\mathbb{H}_{\Lambda_q}(\mathbb{Q}_q)$. Notice that the so obtained subgroup (isomorphic to $\mathbb{Z}^2$) of $\mathbb{H}_{\Lambda_p}(\mathbb{Q}_p)$ is mapped under each of the maps $\Psi_{1,\Lambda_p}, \ldots, \Psi_{4,\Lambda_p}$ to a subgroup of rank one (and not two) by the discussion in Section 4.1.

Proof. By compactness we may assume that $A_{i,L_j} \to A_i \in \mathrm{SL}_4(\mathbb{Z}_p)$ as $j \to \infty$ for all $i \in \{1, 2, 3, 4\}$. Denote by Λ_p (resp. $\tilde{\Lambda}_p$) the $\mathbb{Q}_p$-plane spanned by the first two rows of A_1 (resp. the last two rows of A_2). By continuity $a_1(\Lambda_p) \in \mathbb{Z}_p^3$ (with respect to the basis in A_1) is the limit of the sequence $a_1(L_j)$ and the same is true for $a_2(\Lambda_p)$. By Proposition 2.1 and by continuity of the Klein map we also have $\Phi(\tilde{\Lambda}_p) = [a_1(\Lambda_p), -a_2(\Lambda_p)]$ and hence $\tilde{\Lambda}_p = \Lambda_p^{\perp}$.

The admissability assumption on the planes L_j yields that

$$Q(a_1(\Lambda_p)) = Q(a_2(\Lambda_p))$$

modulo p is in $-(\mathbb{F}_p^{\times})^2$. In particular, the proof of Lemma 2.10 shows that the stabilizer group $\mathbb{H}_{\Lambda_p}(\mathbb{Q}_p) < \mathrm{SU}_2^2(\mathbb{Q}_p) \cong \mathrm{SL}_2^2(\mathbb{Q}_p)$ is a maximal split torus.

Furthermore, as in Section 3.1 we obtain four binary forms (defined over $\mathbb{Z}_p$) using A_1, A_2, A_3, A_4 each of which represents a restriction of Q to a $\mathbb{Z}_p$-submodule of rank two (e.g. the restriction of Q to $\Lambda_p(\mathbb{Z}_p)$ uses the basis contained in A_1). By the above these forms have discriminant in $-(\mathbb{Z}_p^{\times})^2$ and are hence isotropic by Hensel's lemma. This shows that T_p is diagonalizable.

The same discussion applies to define Λ_q (along a further subsequence) and to see that the obtained group T_q is diagonalizable. Since the measure μ_j is $\mathbb{T}_{L_j}(\mathbb{Q}_p \times \mathbb{Q}_q)$-invariant, it follows directly that μ is $\mathbf{T}$-invariant. The existence of the subgroup $\mathbf{A}$ as in the lemma follows from the fact that any maximal torus in $\mathrm{SU}_2^2(\mathbb{Q}_p) \cong \mathrm{SL}_2^2(\mathbb{Q}_p)$ is conjugate to the diagonal one. □

Proof of Theorem 4.2. As mentioned, we now want to apply the joinings classification in [EL17, Thm.1.4]. To this end, recall that SL_2 and SU_2 are simply-connected ([PR94, p.64]) so that $\mathbb{G}$ is also simply-connected. In particular, it follows that X_S is saturated by unipotents in the sense of [EL17] i.e. the subgroup generated by the unipotent elements acts ergodically. Let $\mathbf{A}$ be a subgroup as in Lemma 6.2. Then almost every ergodic component of μ is again a joining for the $\mathbb{Z}^2$-action on X_S given by $\mathbf{A}$. Let ν be one such ergodic component. It is sufficient to show that $\nu = m_{X_S}$ to prove the theorem.

Moreover, by Corollary 1.5 in [EL17] we may as well show that the projection $\nu_{m,n}$ of ν to any product of two factors $X_{m,S} \times X_{n,S}$ for $m < n$ is the trivial joining. Let $\mathbb{G}_m, \mathbb{G}_n \in \{\mathrm{SL}_2, \mathrm{SU}_2\}$ be the corresponding $\mathbb{Q}$-groups. By Theorem 1.4 in [EL17] there exists a linear algebraic group $\mathbb{M} < \mathbb{G}_m \times \mathbb{G}_n$ defined over $\mathbb{Q}$, a finite-index subgroup $M' < \mathbb{M}(\mathbb{Q}_S)$ and some $h \in (\mathbb{G}_m \times \mathbb{G}_n)(\mathbb{Q}_S)$ so that $\nu_{m,n}$ is the Haar measure on $\Gamma M' h$ where $\Gamma = (\mathbb{G}_m \times \mathbb{G}_n)(\mathbb{Z}^S)$. The measure $\nu_{m,n}$ is exactly invariant under the subgroup $h^{-1}M'h$, which has finite index in $M = M_\infty \times M_p \times M_q := h^{-1}\mathbb{M}(\mathbb{Q}_S)h$. Since $h^{-1}M'h$ contains the projection of

$\mathbf{A}$ to the (m,n)-th coordinate pair, the subgroup M contains the projection of the Zariski-closure $\mathbf{T}$ of $\mathbf{A}$.

Assuming for a moment that $\mathbb{M} = \mathbb{G}_m \times \mathbb{G}_n$ then for instance [BT73, Cor. 6.7, p. 534] proceeds to show that $\mathbb{M}(\mathbb{Q}_S)$ does not have any proper, finite-index subgroup (as $\mathbb{M}$ is simply-connected). In particular, $h^{-1}M'h = \mathbb{G}_m(\mathbb{Q}_S) \times \mathbb{G}_n(\mathbb{Q}_S)$ and $\nu_{m,n}$ is the trivial joining.

So suppose that $\mathbb{M} \neq \mathbb{G}_m \times \mathbb{G}_n$. As $\nu_{m,n}$ is a joining and as $\mathbb{G}_m$ or $\mathbb{G}_n$ are both simply-connected groups, the projections of $\mathbb{M}$ to $\mathbb{G}_m$ and $\mathbb{G}_n$ are isomorphisms. In other words, $\mathbb{M}$ is the graph of some isomorphism between $\mathbb{G}_m$ and $\mathbb{G}_n$ defined over $\mathbb{Q}$ and in particular, M_p is the graph of an isomorphism between $\mathbb{G}_m(\mathbb{Q}_p)$ and $\mathbb{G}_n(\mathbb{Q}_p)$. To obtain a contradiction, we distinguish three cases.

Case 1: $m,n \leq 2$. By assumption the maximal torus in $M_p \cong \mathrm{SU}_2(\mathbb{Q}_p)$ is of rank 1. On the other hand, by Lemma 6.2 the subgroup $M_p < \mathrm{SU}_2^2(\mathbb{Q}_p)$ contains the torus $\mathbb{H}_{\Lambda_p}(\mathbb{Q}_p)$, which is of rank two (see Proposition 2.1 or Lemma 6.2).

Case 2: $m \leq 2, n \geq 3$. In this case there is no isomorphism between $\mathbb{G}_m = \mathrm{SU}_2$ and $\mathbb{G}_n = \mathrm{SL}_2$ as $\mathrm{SU}_2(\mathbb{R})$ is compact and $\mathrm{SL}_2(\mathbb{R})$ is not.

Case 3: $m,n \geq 3$. We exhibit elements of $M_p < \mathrm{SL}_2(\mathbb{Q}_p)^2$ of the form (Id, a) for some non-trivial $a \in \mathrm{SL}_2(\mathbb{Q}_p)$ contradicting the assumption.

- If $(m,n) = (3,4)$ we can consider $(\Psi_{1,\Lambda_p}(h), \Psi_{2,\Lambda_p}(h)) \in M_p$ for some non-trivial $h \in \mathbb{H}^{\mathrm{pt}}_{\Lambda_p}(\mathbb{Q}_p)$. This element is of the desired form (Id, a) as $\Psi_{1,\Lambda_p}(h) = \mathrm{Id}$ for any $h \in \mathbb{H}^{\mathrm{pt}}_{\Lambda_p}(\mathbb{Q}_p)$ and as $\Psi_{2,\Lambda_p}(h)$ is non-trivial.
- If $(m,n) = (3,5)$ we can consider $(\Psi_{1,\Lambda_p}(h), \Psi_{3,\Lambda_p}(h)) \in M_p$ for some non-trivial $h \in \mathbb{H}^{\mathrm{pt}}_{\Lambda_p}(\mathbb{Q}_p)$ so that again $\Psi_{1,\Lambda_p}(h) = \mathrm{id}$. Recall that by Lemma 2.9 (the "45°-degree" twist) the pointwise stabilizer of Λ_p acts non-trivially on the orthogonal complement of $a_1(\Lambda_p)$ so that $a = \Psi_{3,\Lambda_p}(h)$ is in fact non-trivial. The cases $(m,n) = (3,6), (4,5), (4,6)$ are analogous (in particular using Lemma 2.9 again).
- If $(m,n) = (5,6)$ we can consider $(\Psi_{3,\Lambda_p}(h), \Psi_{4,\Lambda_p}(h)) \in M_p$ for some non-trivial $h = (\mathrm{id}, h_2)$ where $h_2 \in \mathbb{H}_{a_2(\Lambda_p)}(\mathbb{Q}_p)$.

This concludes the proof. □

7. Further comments and relations to class groups

In this section we formulate an arithmetic interpretation of Theorem 1.2 which permits (possible) generalizations thereof. Let us first describe how the class group $\mathrm{Cl}(\mathcal{O}_D)$ acts on the projections of the collections appearing in Theorem 1.2 to each factor. Here, $D \in \mathbb{N}$ is square-free and $\mathcal{O}_D$ is the maximal order in $\mathbb{Q}(\sqrt{-D})$.

- First, recall that for $D \in \mathbb{D}$ square-free the class group $\mathrm{Cl}(\mathcal{O}_D)$ acts on the set of CM-points $\mathcal{CM}_D$ (as they are simply ideal classes in $\mathrm{Cl}(\mathcal{O}_D)$).
- Similarly, the quotient $\widetilde{\mathcal{R}_3}(D)$ of the set of integer points of norm $\sqrt{D}$ by $\mathrm{SO}_3(\mathbb{Z})$ carries a transitive action[6] of the class group (see [EMV13, Sec. 3]). We will identify the set $\widetilde{\mathcal{R}_3}(D)$ with the image in $\mathrm{SO}_3(\mathbb{Z})\backslash\mathbb{S}^2$

[6] To be more precise, denote by $\mathcal{O}_{\mathbf{B}}$ the (maximal) order of Hurwitz quaternions in $\mathbf{B}$. For any $x, y \in \mathbf{B}_0$ with $\mathrm{Nr}(x) = \mathrm{Nr}(y) = D$ consider

$$\Lambda_{x\to y} = \{\lambda \in \mathcal{O}_{\mathbf{B}} \mid x\lambda = \lambda y\} = \mathcal{O}_{\mathbf{B}} \cap \Phi^{-1}([x,y])$$

which is a left-$\mathcal{O}_x$-ideal where $\mathcal{O}_x = \mathbb{Q}[x] \cap \mathcal{O}_{\mathbf{B}} \widehat{=} \mathcal{O}_D$. The element of the class group mapping x to y is then given by the class of $\Lambda_{x\to y}$ (up to finite index issues) – see [EMV13, Prop. 3.5].

after projection. The Klein map then yields an action of $\mathrm{Cl}(\mathcal{O}_D)^2$ on the set $\mathcal{R}_D$ (or more precisely a finite-to-one quotient thereof).

All of the above actions of the class group $\mathrm{Cl}(\mathcal{O}_D)$ will be denoted by $[\mathfrak{a}].(\cdot)$ for any element $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_D)$.

7.1. **Monomials in ideals and simultaneous equidistribution.** Using these actions we may now give an analogous formulation of Theorem 1.2 which may be thought of as an arithmetic (rather than geometric) interpretation of it.

Theorem 7.1 (Arithmetic version). *Let p and q be two distinct odd primes. For any square-free $D \in \mathbb{N}$ which is not of the form[7] $4^a(8b+7)$ for integers a, b fix basepoints $v^{(D)}, w^{(D)} \in \widetilde{\mathcal{R}_3}(D)$ as well as $\mathbf{z}_1^{(D)}$, $\mathbf{z}_2^{(D)}$, $\mathbf{z}_3^{(D)}$, $\mathbf{z}_4^{(D)}$ in $\mathcal{CM}_D$. Then the subsets*

$$\Big\{\big([\mathfrak{a}].v^{(D)}, [\mathfrak{b}].w^{(D)}, [\mathfrak{a}][\mathfrak{b}].\mathbf{z}_1^{(D)}, [\mathfrak{a}][\mathfrak{b}]^{-1}.\mathbf{z}_2^{(D)}, [\mathfrak{a}]^2.\mathbf{z}_3^{(D)}, [\mathfrak{b}]^2.\mathbf{z}_4^{(D)}\big) : [\mathfrak{a}], [\mathfrak{b}] \in \mathrm{Cl}(\mathcal{O}_D)\Big\}$$

of $(\mathrm{SO}_3(\mathbb{Z}) \backslash \mathbb{S}^2)^2 \times \mathcal{X}_2^4$ equidistribute when D goes to infinity while D is square-free and satisfies $-D \in (\mathbb{F}_p^\times)^2$ and $-D \in (\mathbb{F}_q^\times)^2$.

Note the symmetry in the actions here. Clearly, the acting element in the first (resp. the second) coordinate in $\mathcal{X}_2$ is the quotient (resp. the product) of the two acting elements in the coordinates in $\widetilde{\mathcal{R}_3}(D)$. Also, the acting element $[\mathfrak{a}]^2$ in the third coordinate in $\mathcal{X}_2$ is given by the product of the acting elements $[\mathfrak{a}][\mathfrak{b}]^{-1}$ and $[\mathfrak{a}][\mathfrak{b}]$ in the first resp. second coordinate in $\mathcal{X}_2$. Similarly, the acting element $[\mathfrak{b}]^2$ in the fourth coordinate in $\mathcal{X}_2$ is the quotient of $[\mathfrak{a}][\mathfrak{b}]$ and $[\mathfrak{a}][\mathfrak{b}]^{-1}$.

The authors find it to be a pleasing coincidence that the objects in Theorem 1.2 obtained by geometric constructions (the Klein map and the orthogonal complement) admit a description as in Theorem 7.1. Observe that the relation between the basepoints is determined by these geometric constructions. We will hint at this relation in Appendix B.

7.2. **Extensions.** The above arithmetic game may be extended. For instance, one can change the 45°-degree picture (see Lemma 2.9) and show that the triples

$$\big([\mathfrak{a}].\mathbf{z}_1^{(D)}, [\mathfrak{b}].\mathbf{z}_2^{(D)}, [\mathfrak{a}][\mathfrak{b}]^3.\mathbf{z}_3^{(D)}\big)$$

for $[\mathfrak{a}], [\mathfrak{b}] \in \mathrm{Cl}(\mathcal{O}_D)$ equidistribute where $\mathbf{z}_1^{(D)}, \mathbf{z}_2^{(D)}, \mathbf{z}_3^{(D)}$ denotes any choice of basepoints. Another interesting case (as first studied by M. Bhargava) concerns the triples

$$\big([\mathfrak{a}].\mathbf{z}_1^{(D)}, [\mathfrak{b}].\mathbf{z}_2^{(D)}, ([\mathfrak{a}][\mathfrak{b}])^{-1}.\mathbf{z}_3^{(D)}\big).$$

Here one can prove equidistribution under weakened congruence conditions. This will appear in an upcoming preprint [ELM18] of the second-named author with E. Lindenstrauss and Ph. Michel.

Given $k \in \mathbb{N}$ one could also ask about the distribution of the set of tuples

$$\big([\mathfrak{a}].\mathbf{z}_1^{(D)}, [\mathfrak{a}]^2.\mathbf{z}_2^{(D)}, \ldots, [\mathfrak{a}]^k.\mathbf{z}_k^{(D)}\big) \in \mathcal{X}_2^k \tag{7.1}$$

for $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_D)$ and any fixed choice of basepoints $\mathbf{z}_1^{(D)}, \ldots, \mathbf{z}_k^{(D)} \in \mathcal{CM}_D$. The difficulty here lies in the individual equidistribution as there is no sufficient quantitative control on the k-torsion of the class group. Assuming individual equidistribution, the joinings classification in [EL17] can be used to show equidistribution of

[7] This guarantees that $\widetilde{\mathcal{R}_3}(D)$ is non-empty.

these tuples under sufficient congruence conditions. Such a theorem will appear in [ELM18] in the case of $k = 2$ (as there is control on the 2-torsion).

One may combine this theorem with the problems from the beginning of this subsection (and the like) to obtain an equidistribution statement of the following kind. If $n = (n_1, n_2) \in \mathbb{Z}^2$ is primitive with $n_1 \neq 0 \neq n_2$ then the tuples

$$\big([\mathfrak{a}].\mathbf{z}_1^{(D)}, [\mathfrak{b}].\mathbf{z}_2^{(D)}, [\mathfrak{a}]^{n_1}[\mathfrak{b}]^{n_2}.\mathbf{z}_3^{(D)}, [\mathfrak{a}]^{2n_1}[\mathfrak{b}]^{2n_2}.\mathbf{z}_4^{(D)}\big) \in \mathcal{X}_2^4$$

for $[\mathfrak{a}], [\mathfrak{b}] \in \mathrm{Cl}(\mathcal{O}_D)$ and any fixed choice of basepoints $\mathbf{z}_1^{(D)}, \mathbf{z}_2^{(D)}, \mathbf{z}_3^{(D)}, \mathbf{z}_4^{(D)} \in \mathcal{CM}_D$ equidistribute as $D \to \infty$ under sufficient congruence conditions. Note that one can apply [EL17, Cor. 1.4] in order to generalize this to any finite number of primitive vectors (weights) $n \in \mathbb{Z}^2$ as long as no two vectors are equal or opposite to each other[8].

7.3. **Subcollections.** Given any subset $\mathcal{S}_D \subseteq \mathrm{Cl}(\mathcal{O}_D)^2$ for every D one could enquire about equidistribution of the tuples considered in Theorem 1.2 or Section 7.2 when restricted to $\mathcal{S}_D$. Let us discuss this question only in the context of Theorem 7.1 and in a concrete example here.

Motivated by the mixing conjecture of Michel and Venkatesh fix an ideal class $[\mathfrak{b}] \in \mathrm{Cl}(\mathcal{O}_D)$ and consider the subset

$$\mathcal{S}_D = \{([\mathfrak{a}], [\mathfrak{a}][\mathfrak{b}]) : \mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_D)\} \subseteq \mathrm{Cl}(\mathcal{O}_D)^2.$$

Given the collections from Theorem 7.1 for equal basepoints $v^{(D)} = w^{(D)}$ and $\mathbf{z}_1^{(D)} = \ldots = \mathbf{z}_4^{(D)} = \mathbf{z}^{(D)}$ one obtains along the subset $\mathcal{S}_D$ the finite set of tuples of the form

$$\big([\mathfrak{a}].v^{(D)}, [\mathfrak{a}][\mathfrak{b}].v^{(D)}, [\mathfrak{a}]^2[\mathfrak{b}].\mathbf{z}^{(D)}, [\mathfrak{b}]^{-1}.\mathbf{z}^{(D)}, [\mathfrak{a}]^2.\mathbf{z}^{(D)}, [\mathfrak{a}]^2[\mathfrak{b}]^2.\mathbf{z}^{(D)}\big)$$

for $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_D)$. Clearly, equidistribution in the fourth component is impossible as only one point in $\mathcal{X}_2$ is considered. Recent work of Khayutin [Kha] yields equidistribution under sufficient assumptions on $[\mathfrak{b}]$ and on the quadratic field $\mathbb{Q}(\sqrt{-D})$.

8. Glue groups

In this section we formulate a further strengthening of Theorem 1.2 in terms of glue groups, whose definition we now recall.

The *dual lattice* of a lattice $\Lambda \subseteq \mathbb{Q}^n$ is defined as

$$\Lambda^\vee = \{v \in \Lambda \otimes \mathbb{Q} \mid (v, w) \in \mathbb{Z} \text{ for all } w \in \Lambda\} \cong \mathrm{Hom}(\Lambda, \mathbb{Z}).$$

When Λ is integral (i.e. $(\cdot,\cdot)$ restricted to Λ takes values in $\mathbb{Z}$), then $\Lambda^\vee$ contains Λ and the *glue group* (or *discriminant group*) of Λ

$$\mathcal{G}(\Lambda) = \Lambda^\vee/\Lambda$$

is a finite abelian group of order $\mathrm{disc}(\Lambda)$. A glue group comes with a naturally attached binary form

$$\langle\langle \cdot, \cdot \rangle\rangle : \mathcal{G}(\Lambda) \times \mathcal{G}(\Lambda) \to \mathbb{Q}/\mathbb{Z},$$
$$\langle\langle v + \Lambda, w + \Lambda \rangle\rangle = (v, w) + \mathbb{Z}$$

called the *fractional form* of the glue group.

[8] An elementary argument shows that the sets $\{([\mathfrak{a}].\mathbf{z}^{(D)}, [\mathfrak{a}]^{-1}.\mathbf{z}^{(D)}) : [\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_D)\}$ for a basepoint $\mathbf{z}^{(D)} \in \mathcal{CM}_D$ are not equidistributed in $\mathcal{X}_2^2$ as $D \to \infty$.

We remark that the name "glue" originates from the question whether or not two lattices Λ_1, Λ_2 can be glued together in the sense that there is a unimodular lattice Λ and an embedding of the orthogonal sum $\Lambda_1 \oplus \Lambda_2 \hookrightarrow \Lambda$ such that $\Lambda \cap (\Lambda_1 \otimes \mathbb{R}) = \Lambda_1$ and $\Lambda \cap (\Lambda_2 \otimes \mathbb{R}) = \Lambda_2$. In fact, Λ_1, Λ_2 can be glued in this way if and only if there is an isomorphism $\phi : \mathcal{G}(\Lambda_1) \to \mathcal{G}(\Lambda_2)$ that maps the fractional form on $\mathcal{G}(\Lambda_1)$ to the negative of the fractional form on $\mathcal{G}(\Lambda_2)$. For this and for further background on glue groups we refer to [CS99] and [McM11].

Following a question raised by C. McMullen we consider the distribution of rational planes L in $\mathrm{Gr}_{2,4}(\mathbb{Q})$ whose glue group $\mathcal{G}(L(\mathbb{Z}))$ is of a given isomorphism type. Here, two glue groups $(\mathcal{G}(\Lambda_1), \langle\langle \cdot, \cdot \rangle\rangle_1)$ and $(\mathcal{G}(\Lambda_2), \langle\langle \cdot, \cdot \rangle\rangle_2)$ are called isomorphic if there is an isomorphism $\varphi : \mathcal{G}(\Lambda_1) \to \mathcal{G}(\Lambda_2)$ between the abstract groups with $\langle\langle \varphi(x), \varphi(y) \rangle\rangle_2 = \langle\langle x, y \rangle\rangle_1$ for all $x, y \in \mathcal{G}(\Lambda_1)$. For simplicity, we just write this as $\mathcal{G}(\Lambda_1) \cong \mathcal{G}(\Lambda_2)$.

Theorem 8.1 (Equidistribution along prescribed isomorphism types)**.** *Let p, q be any two distinct odd primes. For any $D \in \mathbb{D}$ fix a plane $L_D \in \mathcal{R}_D$ and set*

$$\mathcal{R}_D(L_D) = \{L \in \mathcal{R}_D \mid \mathcal{G}(L(\mathbb{Z})) \cong \mathcal{G}(L_D(\mathbb{Z}))\}.$$

Let $\mathcal{J}_D(L_D) \subseteq \mathcal{J}_D$ be the subset of points, whose underlying planes are in $\mathcal{R}_D(L_D)$. Then the normalized counting measure on the finite sets $\mathcal{J}_D(L_D)$ equidistributes to the uniform probability measure on $\mathrm{Gr}_{2,4}(\mathbb{R}) \times \mathcal{X}_2^4$ when D goes to infinity along any sequence for which the planes L_D are admissible with respect to p, q.

Here, admissible sequences of planes were defined in Section 4.3. Given the local interpretation of glue groups from the next subsection and Theorem 4.2 this result is quite directly deduced.

8.1. **Local glue groups.** The glue group of a lattice $\Lambda \subseteq \mathbb{Q}^n$ can be computed from local quantities. For any prime p denote by $\Lambda_p = \Lambda \otimes \mathbb{Z}_p$ the completion at p and define the *p-glue group* of Λ as the abelian p-group

$$\mathcal{G}(\Lambda)_p = \Lambda_p^\vee / \Lambda_p.$$

Notice that $\mathcal{G}(\Lambda)_p$ also comes equipped with a fractional form

$$\langle\langle \cdot, \cdot \rangle\rangle_p : \mathcal{G}(\Lambda)_p \times \mathcal{G}(\Lambda)_p \to \mathbb{Q}_p / \mathbb{Z}_p.$$

Then the glue group of Λ can be computed as

$$\mathcal{G}(\Lambda) \cong \prod_p \mathcal{G}(\Lambda)_p$$

and for any $v, w \in \Lambda^\vee$ the value $\langle\langle v + \Lambda, w + \Lambda \rangle\rangle$ is uniquely determined by the values $\langle\langle v + \Lambda_p, w + \Lambda_p \rangle\rangle_p$ for all primes p. We remark that the p-glue group is clearly also defined for general $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^n$.

Proof of Theorem 8.1. By Theorem 4.2 it suffices to show that for any $L \in \mathcal{R}_D$ the planes underlying the points generated from the adelic orbit $\mathbb{G}(\mathbb{Q})\mathbb{T}_L(\mathbb{A})$ all have the same isomorphism type as $\mathcal{G}(L(\mathbb{Z}))$. If $L' \in \mathcal{R}_D$ is any such plane and p is a prime, then the construction shows that there is $g \in \mathrm{SU}_2^2(\mathbb{Z}_p)$ such that $g.L(\mathbb{Z}_p) = L'(\mathbb{Z}_p)$. In particular, $\mathcal{G}(L(\mathbb{Z}))_p \cong \mathcal{G}(L'(\mathbb{Z}))_p$ for all primes p and thus $\mathcal{G}(L(\mathbb{Z})) \cong \mathcal{G}(L'(\mathbb{Z}))$. □

8.2. **Primitivity and glue.** In this section we compute the glue group for lattices of the form $L(\mathbb{Z})$ where $L \in \mathcal{R}_D$. Notice that this is not needed for the proof of Theorem 8.1, but relates our discussion of glue groups to questions from Section 2.3 and yields interpretations of Theorem 8.1. We refrain from discussing the fractional forms here and focus on the abstract groups.

Proposition 8.2 (Primitivity at odd primes)**.** *For an odd prime p let $L \in \mathcal{R}_{D,p}$ and define the numbers $k = \max\{\mathrm{ord}_p(a_1(L)), \mathrm{ord}_p(a_2(L))\}$ and $n = \mathrm{ord}_p(D)$. Then the p-glue group of $L(\mathbb{Z}_p)$ satisfies*

$$\mathcal{G}(L(\mathbb{Z})))_p \cong \mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}/p^{n-k}\mathbb{Z}.$$

Proof. Notice that the action of $\mathrm{SU}_2^2(\mathbb{Z}_p)$ on the set $\mathcal{R}_{D,p}$ preserves the isomorphism class of p-glue groups (that is, including the fractional form). Recall that by Lemma 3.3 and under the identification $\mathbf{B}(\mathbb{Q}_p) \cong \mathrm{Mat}_2(\mathbb{Q}_p)$ there exists some $g \in \mathrm{SU}_2^2(\mathbb{Z}_p)$ and non-zero $\alpha_1, \alpha_2 \in \mathbb{Z}_p$ such that

$$g.L(\mathbb{Z}_p) = \mathbb{Z}_p \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \oplus \mathbb{Z}_p \begin{pmatrix} 0 & 1 \\ -\frac{D}{\alpha_1\alpha_2} & 0 \end{pmatrix}$$

with $\mathrm{ord}_p(\alpha_1) = \mathrm{ord}_p(a_1(L))$ and $\mathrm{ord}_p(\alpha_2) = \mathrm{ord}_p(a_2(L))$. By pair-primitivity we have $k = \mathrm{ord}_p(\alpha_1) + \mathrm{ord}_p(\alpha_2) = \mathrm{ord}_p(\alpha_1\alpha_2)$.

Since this direct sum is orthogonal, the p-glue group of $g.L(\mathbb{Z}_p)$ is simply the product of the p-glue groups of the summands. Now for any primitive vector $v \in \mathbb{Z}_p^3$ the p-glue group of $\mathbb{Z}_p v$ is $\mathbb{Z}_p \,/\, Q(v)\mathbb{Z}_p \cong \mathbb{Z} \,/\, p^{\mathrm{ord}_p(Q(v))}\mathbb{Z}$. For $v = \left(\begin{smallmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{smallmatrix}\right)$ this gives

$$\mathcal{G}\left(\mathbb{Z}_p\left(\begin{smallmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{smallmatrix}\right)\right) \cong \mathbb{Z}_p/\alpha_1\alpha_2\mathbb{Z}_p \cong \mathbb{Z}/p^{\mathrm{ord}_p(\alpha_1\alpha_2)}\mathbb{Z} \cong \mathbb{Z}/p^k\mathbb{Z}.$$

Similarly, $\mathcal{G}\left(\mathbb{Z}_p\left(\begin{smallmatrix} 0 & 1 \\ -\frac{D}{\alpha_1\alpha_2} & 0 \end{smallmatrix}\right)\right) \cong \mathbb{Z} \,/\, p^{n-k}\mathbb{Z}$ and the proposition follows. □

Contrary to the behaviour at odd primes, the local glue groups at 2 are determined by the discriminant only.

Proposition 8.3 (Primitivity at 2)**.** *Let $L \in \mathcal{R}_{D,2}$ for $D \in \mathbb{D}$ and assume that $n = \mathrm{ord}_2(D)$ is positive. Then*

$$\mathcal{G}(L(\mathbb{Z}))_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z}.$$

Proof. By Corollary 2.6 (describing the assumption $D \in \mathbb{D}$) we only need to handle the cases $n = 1, 2, 3$. Note that for $n = 1$ the statement is clear, as $\mathcal{G}(L(\mathbb{Z}))_2$ is a finite group of order 2.

In the cases $n = 2$ or $n = 3$ we will heavily use the fact that $\mathbf{B}(\mathbb{Q}_2)$ is a division algebra (compare the discussion to follow with [EMV13, Prop. 3.7]). As D is divisible by 4, the vectors $w_1 = \frac{1}{2}a_1(L)$ and $w_2 = \frac{1}{2}a_2(L)$ are integral. Choose a non-zero element $g \in L(\mathbb{Z}_2)$ of maximal norm. Looking at the inverse Klein map (cf. Proposition 2.1), this element satisfies $w_1 g = g w_2$. Moreover,

$$\begin{aligned} L(\mathbb{Q}_2) &= \{x \in \mathbf{B}(\mathbb{Q}_2) \mid w_1 x = x w_2\} = \left\{x \in \mathbf{B}(\mathbb{Q}_2) \mid w_1 x = x g^{-1} w_1 g\right\} \\ &= \{y \in \mathbf{B}(\mathbb{Q}_2) \mid w_1 y = y w_1\}\, g = \mathbb{Q}_2 g \oplus \mathbb{Q}_2 w_1 g, \end{aligned}$$

which is in fact an orthogonal sum as $\mathrm{Tr}(w_1 g\overline{g}) = \mathrm{Tr}(w_1) g\overline{g} = 0$.

If $x \in L(\mathbb{Z}_2)$ is any non-zero vector and $x_1, x_2 \in \mathbb{Q}_2$ are such that $x = x_1 g + x_2 w_1 g$ then $\mathrm{Nr}(x) = \mathrm{Nr}(g)(x_1^2 + \mathrm{Nr}(w_1)x_2^2)$. We introduce the short-hand $d = \frac{D}{4} = \mathrm{Nr}(w_1)$ and note that by our choice of g we have $x_1^2 + dx_2^2 \in \mathbb{Z}_2$. Since $d \equiv 1, 2 \bmod 4$ (as

$D \in \mathbb{D}$), the congruence equation $z_1^2 + dz_2^2 \equiv 0 \bmod 4$ has no non-trivial solutions. This implies in particular for any $z_1, z_2 \in \mathbb{Q}_2$ with $z_1^2 + dz_2^2 \in \mathbb{Z}_2$ that $z_1, z_2 \in \mathbb{Z}_2$. Hence, we have $x_1, x_2 \in \mathbb{Z}_2$ and

$$L(\mathbb{Z}_2) = \mathbb{Z}_2 g \oplus \mathbb{Z}_2 w_1 g.$$

In particular, $\mathrm{disc}(L(\mathbb{Z}_2)) = D = 4\,\mathrm{Nr}(w_1)$ equals $\mathrm{Nr}(g)^2\,\mathrm{Nr}(w_1)$ up to a square in $\mathbb{Z}_2^\times$ which implies that $\mathrm{ord}_2(\mathrm{Nr}(g)) = 1$. As $\mathrm{ord}_2(\mathrm{Nr}(w_1)) = \mathrm{ord}(d) = n - 2$, the statement for the glue group can be obtained as in the conclusion of the proof of Proposition 8.2. □

As mentioned after Proposition 2.1, one can refine the statement at the prime 2 therein. For instance, one can show for $L \in \mathcal{R}_D$ that $\mathrm{ord}_2(Q|_{L(\mathbb{Z})}) = 0$ whenever $D \equiv 1, 2 \bmod 4$ and that $\mathrm{ord}_2(Q|_{L(\mathbb{Z})}) = 1$ whenever $D \equiv 0 \bmod 4$. For this, one can apply the technique in the proof of Proposition 8.3 above. We omit this here.

Appendix A. Proof of Corollary 1.3

In this section, we will prove the averaged version (Corollary 1.3) of our main theorem (Theorem 1.2) using the homogeneous counting results of Duke-Rudnick-Sarnak [DRS93] and Eskin-McMullen [EM93].

Consider first the following tentative argument. Let $\mathbb{P}_m$ be the set of the first m odd primes. The 'probability' that $-D \in \mathbb{Z}$ is zero or a non-square modulo p is bounded from above by $\frac{2}{3}$. Thus, the probability that there are no two distinct primes $p, q \in \mathbb{P}_m$ with $-D \bmod p \in (\mathbb{F}_p^\times)^2$ and with $-D \bmod q \in (\mathbb{F}_q^\times)^2$ is at most $(m+1)(\frac{2}{3})^m$ (essentially by the Chinese remainder theorem). Somewhat similarly, we would now like to know the proportion of the set of planes L in $\mathcal{R}_{<D} = \bigcup_{d<D} \mathcal{R}_d$ for which the discriminant $\mathrm{disc}(L)$ satisfies $-\mathrm{disc}(L) \bmod p \in (\mathbb{F}_p^\times)^2$ for at most one $p \in \mathbb{P}_m$. In fact, we claim that this proportion is also $\ll (m+1)(\frac{2}{3})^m$. To prove this, we will use the counting results mentioned above to estimate the number of points in $\mathcal{R}_{<D}$ that satisfy certain congruence conditions. Notice that from the claim Corollary 1.3 follows quite immediately from Theorem 1.2 (cf. the proof below).

A.1. **Definition of the homogeneous space.** Let W be the affine variety of pure wedges in $\bigwedge^2 \mathbb{R}^4 \simeq \mathbb{R}^6$ where we choose the standard basis e_{mn} with $m < n$ for the identification. Let us denote by x_{mn} the coordinates in this basis. Notice that W is the zero locus of the quadratic form $w \in \bigwedge^2 \mathbb{R}^4 \mapsto w \wedge w$ which is represented in the standard basis by the form $x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23}$.

A.1.1. *Integral structure.* As in the proof of Lemma 2.3 we impose on $\bigwedge^2 \mathbb{R}^4$ the integral structure given by $\bigwedge^2 \mathbb{Z}^4$ so that under the above choice of basis $\bigwedge^2 \mathbb{Z}^4 \simeq \mathbb{Z}^6$. Let $W(\mathbb{Z}) = W \cap \mathbb{Z}^6$ and $W_{\mathrm{prim}}(\mathbb{Z}) = W \cap \mathbb{Z}^6_{\mathrm{prim}}$ where $\mathbb{Z}^6_{\mathrm{prim}}$ is the set of primitive vectors. Recall that a wedge of the form $v_1 \wedge v_2$ for $v_1, v_2 \in \mathbb{Z}^4$ is primitive if and only if v_1, v_2 is a basis for $L(\mathbb{Z})$ where $L = \mathbb{R}v_1 \oplus \mathbb{R}v_2$. Thus, $W_{\mathrm{prim}}(\mathbb{Z}) / \{\pm 1\}$ can be identified with the set of rational planes.

Let $\|\cdot\|$ be the Euclidean norm on $\mathbb{R}^6$. We may retrieve the discriminant of a rational plane $L \in \mathrm{Gr}_{2,4}(\mathbb{Q})$ with integral basis $v_1, v_2 \in \mathbb{Z}^4$ by the formula

$$\|v_1 \wedge v_2\|^2 = \mathrm{disc}(L).$$

In particular,

$$2\big|\mathcal{R}_{<D}\big| = \big|W_{\mathrm{prim}}(\mathbb{Z}) \cap B_{\sqrt{D}}(0)\big|.$$

A.1.2. *W as a homogeneous variety.* Note that $\mathrm{SL}_4(\mathbb{R})$ acts transitively on the variety W via $g.(v_1 \wedge v_2) = (g.v_1) \wedge (g.v_2)$ (this is simply the natural action on planes). The induced action of $\mathrm{SL}_4(\mathbb{Z})$ on $W_{\mathrm{prim}}(\mathbb{Z})$ is transitive. Furthermore, the stabilizer of the wedge $e_1 \wedge e_2$ under the action of $\mathrm{SL}_4(\mathbb{R})$ is the group

$$H = \left\{ \begin{pmatrix} A & * \\ 0 & B \end{pmatrix} : A, B \in \mathrm{SL}_2(\mathbb{R}) \right\}.$$

We may thus identify W with the quotient G/H. More generally, we denote by H_w the stabilizer of $w \in W$.

A.1.3. *Reducing points on the variety.* Let $N \in \mathbb{N}$ be odd and square-free. We consider the finite set

$$W\left(\mathbb{Z}/N\mathbb{Z}\right) \subseteq \textstyle\bigwedge^2 \left(\mathbb{Z}/N\mathbb{Z}\right)^4 \simeq \left(\mathbb{Z}/N\mathbb{Z}\right)^6$$

and let $W_{\mathrm{prim}}(\mathbb{Z}/N\mathbb{Z})$ to be the set of primitive vectors $\mathbf{a} \in W\big(\mathbb{Z}/N\mathbb{Z}\big)$. Denote by $W_{\mathbf{a}}(\mathbb{Z}) \subseteq W_{\mathrm{prim}}(\mathbb{Z})$ the set of wedges w with $w \equiv \mathbf{a} \bmod N$. By the Chinese remainder theorem we have

$$W_{\mathrm{prim}}\left(\mathbb{Z}/N\mathbb{Z}\right) \simeq \prod_{p \mid N} W_{\mathrm{prim}}\left(\mathbb{F}_p\right) \tag{A.1}$$

where taking the discriminant on the left-hand side corresponds to taking the discriminant componentwise on the right-hand side. Clearly, $W_{\mathrm{prim}}(\mathbb{F}_p) = W(\mathbb{F}_p) \setminus \{0\}$.

A.2. **Proof of Corollary 1.3.** The proof of Corollary 1.3 uses (apart from Theorem 1.2) the following two ingredients.

Proposition A.1 (Counting under congruence conditions)**.** *Let $N \in \mathbb{N}$ be odd and square-free and let $\mathbf{a} \in W_{\mathrm{prim}}(\mathbb{Z}/N\mathbb{Z})$ so that $W_{\mathbf{a}}(\mathbb{Z}) \neq \emptyset$. Then we have*

$$|W_{\mathbf{a}}(\mathbb{Z}) \cap B_{\sqrt{D}}(0)| \asymp \tfrac{2}{|W_{\mathrm{prim}}(\mathbb{Z}/N\mathbb{Z})|} |\mathcal{R}_{<D}|.$$

Proposition A.2. *Let $N \in \mathbb{N}$ be odd and square-free. Then the relative number of vectors $\mathbf{a} \in W_{\mathrm{prim}}(\mathbb{Z}/N\mathbb{Z})$ with the property that $-\operatorname{disc}(\mathbf{a})$ is a non-zero square mod p for at most one prime $p|N$ is $\ll m(\frac{2}{3})^m$ where m is the number of prime divisors of N.*

We note that the homogeneous counting results [DRS93] and [EM93] are used to prove Proposition A.1. Also, we remark that explicit asymptotics for $|\mathcal{R}_{<D}|$ as $D \to \infty$ are known (see Schmidt [Sch68], [Sch98]), but will not be needed here. We will prove Propositions A.1 and A.2 below, but let us first explain how they can be combined to obtain the corollary of Theorem 1.2.

Proof of Corollary 1.3. Let $m \geq 1$ and let N be the product of the first m odd primes. Furthermore, we set $\mathcal{B}_m$ to be the subset of points $\mathbf{a}$ in $W_{\mathrm{prim}}(\mathbb{Z}/N\mathbb{Z})$ for which $-\operatorname{disc}(\mathbf{a})$ is a non-zero square modulo at most one prime $p \mid N$. Denote by $\mathcal{B}_m(D)$ the subset of points in the set $\mathcal{J}_{<D} = \bigcup_{d<D} \mathcal{J}_d$ whose underlying planes $L \in W_{\mathrm{prim}}(\mathbb{Z})$ satisfy $L \bmod N \in \mathcal{B}_m$. Then by Proposition A.1 and Proposition A.2

$$|\mathcal{B}_m(D)| \ll \sum_{\mathbf{a} \in \mathcal{B}_m} \tfrac{1}{|W_{\mathrm{prim}}(\mathbb{Z}/N\mathbb{Z}|)} |\mathcal{R}_{<D}| \ll m(\tfrac{2}{3})^m |\mathcal{R}_{<D}|$$

Therefore, the average of a continuous function $f : \mathrm{Gr}_{2,4}(\mathbb{R}) \times \mathcal{X}_2^4 \to \mathbb{C}$ over $\mathcal{J}_{<D}$ differs from the average over $\mathcal{J}_{<D} \setminus \mathcal{B}_m(D)$ by $\ll m(\frac{2}{3})^m \|f\|_\infty$. Notice that each discriminant appearing in $\mathcal{J}_{<D} \setminus \mathcal{B}_m(D)$ satisfies the splitting conditions of Theorem 1.2

at least at two prime divisiors of N. Thus, Theorem 1.2 implies equidistribution of these finite subsets and so

$$\limsup_{D\to\infty}\Big|\tfrac{1}{|\mathcal{J}_{<D}|}\sum_{x\in\mathcal{J}_{<D}} f(x)-\int f\Big| \ll m(\tfrac{2}{3})^m\|f\|.$$

Since m was arbitrary, Corollary 1.3 follows. □

A.3. **Counting under congruence conditions.** Let $\mathbf{a}\in W_{\mathrm{prim}}(\mathbb{Z}\,/\,N\mathbb{Z})$ be fixed. Furthermore, let $\Gamma_{\mathbf{a}}$ be the subgroup of $\mathrm{SL}_4(\mathbb{Z})$ consisting of the elements which preserve the subset $W_{\mathbf{a}}(\mathbb{Z})\subseteq W_{\mathrm{prim}}(\mathbb{Z})$.

Lemma A.3 (Index of $\Gamma_{\mathbf{a}}$)**.** *Whenever $W_{\mathbf{a}}(\mathbb{Z})$ is non-empty, $\Gamma_{\mathbf{a}}$ acts transitively on $W_{\mathbf{a}}(\mathbb{Z})$ and the index of $\Gamma_{\mathbf{a}}$ in $\mathrm{SL}_4(\mathbb{Z})$ is equal to $|W_{prim}(\mathbb{Z}\,/\,N\mathbb{Z})|$. Furthermore, $\Gamma_{\mathbf{a}}$ is a congruence subgroup.*

Proof. Denote by $w\in\mathbb{Z}^6\mapsto\overline{w}$ the reduction mod N and let $w\in W_{\mathrm{prim}}(\mathbb{Z})$ with $\overline{w}=\mathbf{a}$. Then for any $\gamma\in\mathrm{SL}_4(\mathbb{Z})$ we have $\overline{\gamma.w}=\overline{\gamma}.\mathbf{a}$ where we used the analogous notation for the (surjective) reduction map $\mathrm{SL}_4(\mathbb{Z})\to\mathrm{SL}_4(\mathbb{Z}\,/\,N\mathbb{Z})$. In particular, if $H_{\mathbf{a}}<\mathrm{SL}_4(\mathbb{Z}\,/\,N\mathbb{Z})$ denotes the stabilizer of $\mathbf{a}$ then $\Gamma_{\mathbf{a}}$ is the preimage of $H_{\mathbf{a}}$ under the reduction map. Therefore, the index of $\Gamma_{\mathbf{a}}$ in $\mathrm{SL}_4(\mathbb{Z})$ is the index of $H_{\mathbf{a}}$ in $\mathrm{SL}_4(\mathbb{Z}\,/\,N\mathbb{Z})$. Notice that $\mathrm{SL}_4(\mathbb{Z}\,/\,N\mathbb{Z})$ acts transitively on $W_{\mathrm{prim}}(\mathbb{Z}\,/\,N\mathbb{Z})$. Indeed, this follows from the Chinese remainder theorem in (A.1) and its analogue for SL_4 as well as the fact that $\mathrm{SL}_4(\mathbb{F}_p)$ acts transitively on $W(\mathbb{F}_p)\setminus\{0\}$ for any odd prime p. Therefore, $W_{\mathrm{prim}}(\mathbb{Z}\,/\,N\mathbb{Z})=\mathrm{SL}_4(\mathbb{Z}\,/\,N\mathbb{Z})\,/\,H_{\mathbf{a}}$ which implies the latter claim in the lemma.

To prove transitivity of the action of $\Gamma_{\mathbf{a}}$, let $w_1,w_2\in W_{\mathbf{a}}(\mathbb{Z})$ and choose some $\gamma\in\mathrm{SL}_4(\mathbb{Z})$ with $\gamma.w_1=w_2$. But then $\overline{\gamma}.\mathbf{a}=\overline{\gamma.w_1}=\overline{w_2}=\mathbf{a}$ and so $\gamma\in\Gamma_{\mathbf{a}}$. □

Proof of Proposition A.1. As mentioned, we use the technique in [EM93] (see also [DRS93]). We begin by recalling the necessary dynamical statement. Fix some $w\in W_{\mathbf{a}}(\mathbb{Z})$. Note that $\Gamma_{\mathbf{a}}\cap H_w=H_w(\mathbb{Z})$ is a lattice in H_w (since H_w has no non-trivial $\mathbb{Q}$-characters). Let m_W be a non-trivial measure on W invariant under $G=\mathrm{SL}_4(\mathbb{R})$ and assume (after rescaling of the Haar measure m_{H_w} on H_w) that for any $f\in C_c(G)$ we have

$$\int_G f\,\mathrm{d}m_G=\int_W\int_{H_w} f(gh)\,\mathrm{d}m_{H_w}(h)\,\mathrm{d}m_W(gH_w).$$

Since $H_w(\mathbb{Z})=\Gamma_{\mathbf{a}}\cap H_w$ we may set

$$C:=\mathrm{vol}\left({H_w}/{H_w(\mathbb{Z})}\right)=\mathrm{vol}\left({H_w}/{\Gamma_{\mathbf{a}}\cap H_w}\right).$$

To simplify notation we substitute $r=\sqrt{D}$ and write $B_r=B_r(0)$. The balls B_r are well-rounded in the sense of [EM93]. We have the following mixing statement on average for $f\in C_c(G/\Gamma_{\mathbf{a}})$

$$\frac{1}{C}\frac{1}{m_W(B_r)}\int_{B_r}\int_{H_w\Gamma_{\mathbf{a}}} f(gh\Gamma_{\mathbf{a}})\,\mathrm{d}m_{H_w\,/\,\Gamma_{\mathbf{a}}\cap H_w}(h(\Gamma_{\mathbf{a}}\cap H_w))\,\mathrm{d}m_W(gH_w)$$
$$\to\frac{1}{\mathrm{vol}(G\,/\,\Gamma_{\mathbf{a}})}\int_{G/\Gamma_{\mathbf{a}}} f.$$

Then [EM93, Thm. 1.4] implies

$$\begin{aligned}|W_{\mathbf{a}}(\mathbb{Z}) \cap B_r| = |\Gamma_{\mathbf{a}}.w \cap B_r| &\asymp \frac{C}{\mathrm{vol}(G\,/\,\Gamma_{\mathbf{a}})} m_W(B_r)\\ &= \frac{C}{[\mathrm{SL}_4(\mathbb{Z}) : \Gamma_{\mathbf{a}}]\,\mathrm{vol}(G\,/\,G(\mathbb{Z}))} m_W(B_r).\end{aligned}$$

By the analogous argument using the whole lattice $\mathrm{SL}_4(\mathbb{Z})$ instead of the congruence subgroup $\Gamma_{\mathbf{a}}$ we have

$$|W_{\mathrm{prim}}(\mathbb{Z}) \cap B_r| = |\,\mathrm{SL}_4(\mathbb{Z}).w \cap B_r| \asymp \frac{C}{\mathrm{vol}(G\,/\,G(\mathbb{Z}))} m_W(B_r).$$

Since $|W_{\mathrm{prim}}(\mathbb{Z}) \cap B_r| = 2|\mathcal{R}_{<D}|$ and $[\mathrm{SL}_4(\mathbb{Z}) : \Gamma_{\mathbf{a}}] = |W_{\mathrm{prim}}(\mathbb{Z}\,/\,N\mathbb{Z})|$ this proves that

$$|W_{\mathbf{a}}(\mathbb{Z}) \cap B_r| \asymp \frac{1}{|W_{\mathrm{prim}}(\mathbb{Z}\,/\,N\mathbb{Z})|} \frac{C}{\mathrm{vol}(G\,/\,G(\mathbb{Z}))} m_W(B_r) \asymp \frac{2}{|W_{\mathrm{prim}}(\mathbb{Z}\,/\,N\mathbb{Z})|} |\mathcal{R}_{<D}|$$

as desired. □

A.4. **Counting representations by the discriminant.** To prove Proposition A.2 we will use the following auxiliary lemma which can be found in greater generality in [Kit93, Lemma 1.3.1 and Thm. 1.3.2].

Lemma A.4 (Counting solutions to quadratic equations)**.** *Let p be an odd prime and let $\alpha \in \mathbb{F}_p$. The number $r_p(\alpha)$ of solutions to $x_1^2 + x_2^2 + x_3^2 = \alpha$ over $\mathbb{F}_p$ satisfies $|r_p(\alpha) - p^2| \ll p$ where the implicit constant is independent of α and p. Also, $r_p(u^2\alpha) = r_p(\alpha)$ for all $u \in \mathbb{F}_p^\times$.*

Proof. Since $x_1^2 + x_2^2 + x_3^2$ is isotropic, it is equivalent to $x_1x_2 - x_3^2$ (by discriminant comparison) and so $r_p(\alpha)$ is equal to the number of solutions to $x_1x_2 = \alpha + x_3^2$. We let $S = \{\alpha + x_3^2 : x_3 \in \mathbb{F}_p\}$ and note that any $s \in S$ is represented by exactly two values x_3 except for α. Also, $|S| = \frac{p+1}{2}$. For any non-zero $s \in S$ the number of solutions to $x_1x_2 = s$ is equal to the number of solutions to $x_1x_2 = 1$ which is $|\mathbb{F}_p^\times| = p - 1$. Furthermore, the number of solutions to $x_1x_2 = 0$ is $2p - 1$. We now distinguish two cases.

Case 1: $0 \notin S$ (i.e. $-\alpha$ is not a square). Then $\alpha \neq 0$ and

$$r_p(\alpha) = (p-1)2(|S|-1) + (p-1) = p^2 - p.$$

Case 2: $0 \in S$. If $\alpha = 0$ then

$$r_p(0) = (p-1)2(|S|-1) + (2p-1) = p^2.$$

Otherwise,

$$r_p(\alpha) = (p-1)2(|S|-2) + (p-1) + (2p-1)2 = p^2 + p$$

which concludes the proof. □

Proof of Proposition A.2. Let us first assume that $N = p$ is an odd prime and let us begin by counting non-zero (i.e. primitive) points in $W(\mathbb{F}_p)$ of discriminant $\alpha \in \mathbb{F}_p$. Choosing the standard basis of $\bigwedge^2 \mathbb{F}_p^4$ the quadratic form disc is represented by

$x_{12}^2 + \ldots + x_{34}^2$. Furthermore, $W(\mathbb{F}_p)$ is the set of solutions to $x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23} = 0$. By adding and subtracting one sees that the system of equations

$$\begin{cases} x_{12}^2 + \ldots + x_{34}^2 = \alpha \\ x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23} = 0 \end{cases}$$

is equivalent to the decoupled system

$$\begin{cases} y_1^2 + y_2^2 + y_3^2 = \alpha \\ y_4^2 + y_5^2 + y_6^2 = \alpha \end{cases}$$

where $y_1 = x_{12} - x_{34}$, $y_2 = x_{13} + x_{24}$, $y_3 = x_{14} - x_{23}$, $y_4 = x_{12} + x_{34}$, $y_5 = x_{13} - x_{24}$ and $y_6 = x_{14} + x_{23}$. If $\alpha \neq 0$, the number of (non-zero) solutions to the latter system is equal to $r_p(\alpha)^2$ and so

$$|\{\mathbf{a} \in W_{\mathrm{prim}}(\mathbb{F}_p) : \mathrm{disc}(\mathbf{a}) = \alpha\}| = r_p(\alpha)^2. \tag{A.2}$$

If $\alpha = 0$, the number of non-zero solutions is $r_p(0)^2 - 1$.

Fix $\alpha_1, \alpha_2 \in \mathbb{F}_p^\times$ with $-\alpha_1 \in (\mathbb{F}_p^\times)^2$ and $-\alpha_2 \notin (\mathbb{F}_p^\times)^2$. We now apply (A.2) to estimate

$$\begin{aligned} &\frac{1}{|W_{\mathrm{prim}}(\mathbb{F}_p)|}\big|\{\mathbf{a} \in W_{\mathrm{prim}}(\mathbb{F}_p) : -\mathrm{disc}(\mathbf{a}) \notin (\mathbb{F}_p^\times)^2\}\big| \\ &\qquad = \frac{(r_p(0)^2 - 1) + |(\mathbb{F}_p^\times)^2| r_p(\alpha_2)^2}{(r_p(0)^2 - 1) + r_p(\alpha_1)^2|(\mathbb{F}_p^\times)^2| + r_p(\alpha_2)^2|(\mathbb{F}_p^\times)^2|} \\ &\qquad \leq \frac{r_p(0)^2}{r_p(\alpha_1)^2|(\mathbb{F}_p^\times)^2|} + \frac{r_p(\alpha_2)^2}{r_p(\alpha_1)^2 + r_p(\alpha_2)^2} = \frac{\left(\frac{r_p(0)}{r_p(\alpha_1)}\right)^2}{|(\mathbb{F}_p^\times)^2|} + \frac{1}{1 + \left(\frac{r_p(\alpha_1)}{r_p(\alpha_2)}\right)^2} \end{aligned}$$

By Lemma A.4, $\frac{r_p(x_1)}{r_p(x_2)}$ converges to 1 as p goes to infinity uniformly in $x_1, x_2 \in \mathbb{F}_p$ and so we have

$$\frac{|\{\mathbf{a} \in W_{\mathrm{prim}}(\mathbb{F}_p) : -\mathrm{disc}(\mathbf{a}) \in (\mathbb{F}_p^\times)^2\}|}{|W_{\mathrm{prim}}(\mathbb{F}_p)|} \leq \frac{1}{15} + \frac{1}{1 + \frac{2}{3}} = \frac{2}{3} \tag{A.3}$$

for all but finitely many odd primes p.

Now let N be an arbitrary odd and square-free number and let $N = p_1 \ldots p_m$ be its prime decomposition. Let M_k be the number of vectors $\mathbf{a} \in W_{\mathrm{prim}}(\mathbb{Z} / N\mathbb{Z})$ for which $-\mathrm{disc}(\mathbf{a})$ is a non-zero square only modulo p_k. Then by the application of the Chinese remainder theorem in (A.1) and the estimate (A.3)

$$\frac{M_k}{|W_{\mathrm{prim}}(\mathbb{Z} / N\mathbb{Z})|} \leq \Big(\frac{2}{3}\Big)^{m-1-m_0} \ll \Big(\frac{2}{3}\Big)^m$$

where m_0 is the number of exceptions to (A.3). Similarly, if M_0 is the number of vectors $\mathbf{a} \in W_{\mathrm{prim}}(\mathbb{Z} / N\mathbb{Z})$ for which $-\mathrm{disc}(\mathbf{a})$ is not a non-zero square modulo any p_k, we have $\frac{M_0}{|W_{\mathrm{prim}}(\mathbb{Z} / N\mathbb{Z})|} \ll (\frac{2}{3})^m$. This proves the proposition. □

Appendix B. Class groups and Theorem 7.1

In this section we would like to explain the relationship between Theorem 1.2 and Theorem 7.1 by illustrating it in a special case. This will also give more intuition on the 45°-twist discussed in Lemma 2.9.

B.1. **Planes in the split quaternion algebra.** We consider the quaternion algebra $\mathbf{B} = \mathrm{Mat}_2$ and the group SL_2 of norm one units (see also Section 3.3). Here, recall that the conjugation on Mat_2 is given by the adjunct

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\mathrm{ad}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

The norm is the determinant

$$Q(a,b,c,d) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\mathrm{ad}} = (ad - bc)\,\mathrm{id}$$

and the trace is the usual trace

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\mathrm{ad}} = \begin{pmatrix} a+d & 0 \\ 0 & d+a \end{pmatrix} = (a+d)\,\mathrm{id}\,.$$

As before, we let SL_2^2 act on $\mathrm{Mat}_{2,2}$ and SL_2 act on the traceless matrices $\mathbf{B}_0 = \mathfrak{sl}_2$. The formula (1.2) as well as Proposition 2.1 on the Klein map can directly be generalized to this setup and so one can identify two-dimensional subspaces $L \subseteq \mathrm{Mat}_2$ with equivalence class of pairs $[(a_1(L), a_2(L))]$ where $a_1(L), a_2(L) \in \mathbf{B}_0$ satisfy $\det(a_1(L)) = \det(a_2(L))$.

Note that $\mathrm{Mat}_{2,2}$ carries an integral structure given by $\mathrm{Mat}_{2,2}(\mathbb{Z})$. The analogue of formula (1.2) does not directly yield integral matrices (the trace is not automatically divisible by 2) which is why we multiply the defining expression by 2.

B.2. **The acting tori in a special case.** For the purposes of this subsection we would like to consider the plane

$$L = \langle E_{11}, E_{22} \rangle$$

where E_{ij} denotes the matrix which is one at the (i,j)-th entry and zero otherwise. An integral basis of $L(\mathbb{Z}) = L \cap \mathrm{Mat}_{2,2}(\mathbb{Z})$ is then given by E_{11}, E_{22}. So the integer points associated L (see also Section 2.3) are given by

$$\begin{aligned} a_1(L) &= 2E_{11}E_{22}^{\mathrm{ad}} - \mathrm{Tr}(E_{11}E_{22}^{\mathrm{ad}}) = 2E_{11} - \mathrm{Tr}(E_{11}) = 2E_{11} - \mathrm{id} \\ &= E_{11} - E_{22} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = a_2(L). \end{aligned}$$

The analogue of Proposition 2.1 thus yields

$$\mathrm{Stab}_{\mathrm{SL}_2^2}(L) = \mathrm{Stab}_{\mathrm{SL}_2}(a_1(L)) \times \mathrm{Stab}_{\mathrm{SL}_2}(a_2(L)) = A \times A$$

where $A = \left\{ a_s = \mathrm{diag}(s, s^{-1}) \right\}$ denotes the subgroup of diagonal matrices. A direct computation provides the pointwise stabilizers

$$\begin{aligned} \mathrm{Stab}^{\mathrm{pt}}_{\mathrm{SL}_2^2}(L) &= \{(a,a) \mid a \in A\} \\ \mathrm{Stab}^{\mathrm{pt}}_{\mathrm{SL}_2^2}(L^\perp) &= \left\{(a,a^{-1}) \mid a \in A\right\} \end{aligned}$$

in analogy to Lemma 2.9. We now fix ourselves an element $(a_s, a_t) \in A^2$ and examine the way it acts on all relevant subspaces (see Section 4.1).

- The action of (a_s, a_t) on the subspace L is represented by $a_{st^{-1}} \in A$ in the integral basis E_{11}, E_{22} as

$$a_s E_{11} a_t^{-1} = st^{-1} E_{11}, \quad a_s E_{22} a_t^{-1} = s^{-1} t E_{22}.$$

Note that the restriction of Q to L represented in the basis E_{11}, E_{22} is exactly the binary form $q_L(x,y) = xy$ so that $A = \mathrm{Stab}_{\mathrm{SL}_2}(q_L)$. In other words, the homomorphism $\Psi_{1,L}$ defined in analogy to Section 4.1 is given by

$$\Psi_{1,L} : (a_s, a_t) \in A \times A \mapsto a_{st^{-1}} \in A.$$

- We proceed similarly for $L^\perp$ for which we consider the integral basis given by E_{12}, E_{21}. Then
$$a_s E_{12} a_t^{-1} = s E_{12} a_t^{-1} = st E_{11}, \quad a_s E_{21} a_t^{-1} = (st)^{-1} E_{22}.$$
Therefore,
$$\Psi_{2,L} : (a_s, a_t) \in A \times A \mapsto a_{st} \in A.$$
- The orthogonal complement $a_1(L)$ inside $\mathbf{B}_0$ is given by $L^\perp$, for which we again choose the integral basis E_{12}, E_{21}. Then
$$\Psi_{3,L} : (a_s, a_t) \in A \times A \mapsto a_{s^2} \in A.$$
This is because the action of (a_s, a_t) on $a_1(L)^\perp \subseteq \mathbf{B}_0$ is the conjugation with a_s (by the analogon of Proposition 2.5) so that one can apply the previous calculation with $s = t$.
- Since $a_1(L) = a_2(L)$ one analogously obtains
$$\Psi_{4,L} : (a_s, a_t) \in A \times A \mapsto a_{t^2} \in A.$$

References

[AES16a] M. Aka, M. Einsiedler, and U. Shapira, *Integer points on spheres and their orthogonal grids*, J. London Math. Soc. **93** (2016), no. 1, 143–158.

[AES16b] ———, *Integer points on spheres and their orthogonal lattices*, Invent. Math. **206** (2016), no. 2, 379–396.

[BT73] A. Borel and J. Tits, *Homomorphismes 'abstraits' de groupes algebriques simples*, Ann. Math. **97** (1973), no. 3, 499–571.

[Cas78] J.W.S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, vol. 13, Academic Press Inc., 1978.

[CH07] S. Cooper and M. Hirschhorn, *On the number of primitive representations of integers as sums of squares*, Ramanujan J. **13** (2007), 7–25.

[CS99] J.H. Conway and N.J.A. Sloane, *Sphere packings, lattices and groups*, third ed., Grundlehren der mathematischen Wissenschaften, vol. 290, Springer-Verlag, 1999.

[DRS93] W. Duke, Z. Rudnick, and P. Sarnak, *Density of integer points on affine homogeneous varieties*, Duke Math. J. **71** (1993), no. 1, 143–179.

[Duk88] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Invent. Math. **92** (1988), no. 1, 73–90.

[EL17] M. Einsiedler and E. Lindenstrauss, *Joinings of higher rank torus actions on homogeneous spaces*, arXiv:1502.05133 (2017).

[ELM18] M. Einsiedler, E. Lindenstrauss, and Ph. Michel, *Arithmetic joint equidistribution*, In preparation.

[ELMV11] M. Einsiedler, E. Lindenstrauss, Ph. Michel, and A. Venkatesh, *Distribution of periodic torus orbits and Duke's theorem for cubic fields*, Ann. Math. **173** (2011), 815–885.

[EM93] A. Eskin and C. McMullen, *Mixing, counting and equidistribution in Lie groups*, Duke Math. J. **71** (1993), no. 1, 181–209.

[EMV13] J.S. Ellenberg, P. Michel, and A. Venkatesh, *Linnik's ergodic method and the distribution of integer points on spheres*, Tata Inst. Fundam. Res. Stud. **22** (2013), 119–185.

[HM06] G. Harcos and P. Michel, *The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points. II*, Invent. Math. **163** (2006), no. 3, 581–655.

[Iwa87] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Invent. Math. **87** (1987), no. 2, 385–401.

[Kha] I. Khayutin, *Joint equidistribution of CM points*, to appear in Ann. Math.

[Kit93] Y. Kitaoka, *Arithmetic of quadratic forms*, vol. 106, Cambridge University Press, 1993.

[Ko37] C. Ko, *On the representation of a quadratic form as a sum of squares of linear forms*, Q. J. Math. **1** (1937), 81–98.

[Lin68] Yu. V. Linnik, *Ergodic properties of algebraic fields*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 45, Springer-Verlag, New York, 1968, Translated from the Russian by M.S. Keane.

[Maa56] H. Maass, *Spherical functions and quadratic forms*, J. Indian Math. Soc. **20** (1956), 117–162.

[Maa59] ———, *Über die Verteilung der zweidimensionalen Untergitter in einem euklidschen Gitter*, Mathematische Annalen **137** (1959), 319–327.

[McM11] C. McMullen, *K3 surfaces, entropy and glue*, J. Reine Angew. Math **658** (2011), 1–25.

[Mor32] L.J. Mordell, *On the representations of a binary quadratic form as a sum of squares of linear forms*, Mathematische Zeitschrift **35** (1932), no. 1, 1–15.

[Mor37] ———, *An applications of quaternions to the representation of a binary quadratic form as a sum of four linear squares*, Q. J. Math. **1** (1937), 58–61.

[PR94] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., 1994, Translated from the 1991 Russian original by R. Rowen.

[Sch68] W. Schmidt, *Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height*, Duke Math. J. **35** (1968), no. 2, 327–339.

[Sch98] ———, *The distribution of sublattices of* $\mathbb{Z}^m$, Monatsh. Math. **125** (1998), no. 1, 37–81.

[Sie36] C. L. Siegel, *Über die Klassenzahl quadratischer Zahlenkörper*, Acta Arithmetica **1** (1936), 83–86.

[Sku62] B. F. Skubenko, *The asymptotic distribution of integers on a hyperboloid of one sheet and ergodic theorems*, Izv. Akad. Nauk SSSR Ser. Mat. **26** (1962), 721–752.

[Vig80] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, 1980, (French).

[Wie18] A. Wieser, *Linnik's problems and maximal entropy methods*, arXiv:1801.09012 (2018).

Departement Mathematik, ETH Zürich, Rämistrasse 101, 8092 Zürich, Switzerland