TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 375, Number 7, July 2022, Pages 4619–4640
https://doi.org/10.1090/tran/8670
Article electronically published on April 21, 2022

ON REALIZATION OF ISOMETRIES FOR HIGHER RANK QUADRATIC LATTICES OVER NUMBER FIELDS

WAI KIU CHAN AND HAN LI

Abstract. Let F be a number field, and $n \geq 3$ be an integer. In this paper we give an effective procedure which (1) determines whether two given quadratic lattices on F^n are isometric or not, and (2) produces an invertible linear transformation realizing the isometry provided the two given lattices are isometric. A key ingredient in our approach is a search bound for the equivalence of two given quadratic forms over number fields which we prove using methods from algebraic groups, homogeneous dynamics and spectral theory of automorphic forms.

1. Introduction

Let F be a number field (finite extension of $\mathbb{Q}$), $\mathcal{O}$ the ring of integers of F, and V a finite dimensional vector space over F endowed with a non-degenerate quadratic form Q. We call the pair (V, Q), or simply V when the context is clear, a quadratic space over F. An isometry f from (V, Q) to another quadratic space (V', Q') is a vector space isomorphism from V to V' such that $Q'(f(x)) = Q(x)$ for all $x \in V$.

By a *lattice* on V we mean an ordered pair (M, Q) where M is a finitely generated $\mathcal{O}$-submodule of V which contains a basis of V. Again, we will usually just speak of M as a lattice on V when no confusion arises. Let M and N be lattices on the quadratic spaces (V, Q) and (V', Q'), respectively. By definition the lattices M and N are isometric if there is an isometry $f\colon V \to V'$ such that $f(M) = N$. Our work is driven by the following two problems:

- (Decision Problem): decide effectively whether two given M and N are isometric;
- (Realization Problem): produce effectively an isometry f, when M and N are isometric.

If one considers the Decision Problem for isometries of quadratic spaces instead of lattices, then the Hasse-Minkowski theorem provides a complete resolution: two quadratic spaces over F are isometric if and only if they are isometric over the completion F_v for each place v of F. This is also known as the local-global principle. However, for lattices the local-global principle no longer holds, that is, there are non-isometric quadratic lattices which are isometric over the completion $\mathcal{O}_v$ for each place v. Investigating the failure of the local-global principle led to the concepts of *genus* and *spinor genus* (see [20] for their precise definitions). Since then there has

Received by the editors September 6, 2021.

2020 *Mathematics Subject Classification.* Primary 11E12, 37A44; Secondary 11E20, 37A25.

Key words and phrases. Quadratic lattice, effective search bound, homogeneous dynamics.

The second author acknowledges support by the NSF grant DMS #1700109, and the Simons Foundation grant #853671.

been dramatic progress made for the Decision Problem by studying the genera and spinor genera of quadratic lattices. For the sake of convenience let us assume that $(V, Q) = (V', Q')$, or that M and N are lattices on the same quadratic space (V, Q). There is no harm for making this assumption because our problem is meaningful only when the quadratic spaces (V, Q) and (V', Q') are isometric. For our discussion let us accept and keep in mind that genera, spinor genera, and isometry classes are different measures of classification of quadratic lattices, with later ones finer than earlier ones. By the strong approximation theorem, when $\dim V \geq 3$ and when Q is isotropic over at least one archimedean completion of F, two quadratic lattices are isometric if and only if they are in the same spinor genus. In this case, the Decision Problem may be resolved in two steps: (1) decide whether two given lattices M and N are in the same genus; (2) decide whether M and N are in the same spinor genus provided the result of the first step is positive. As of this writing, algorithms related to genera and spinor genera of definite quadratic lattices may be found at `https://magma.maths.usyd.edu.au/magma/handbook/text/336#3251` from MAGMA. In view of the current development of the arithmetic theory of quadratic forms, one may reasonably expect the corresponding algorithms for indefinite quadratic lattices to be made available in the future. On the other hand, the method we discussed above says nothing but the existence of the isometry f in the Realization Problem.

Progress on the Realization Problem has been achieved mainly for equivalence of integral quadratic forms, which is a special case of isometries of quadratic lattices. For any $n \times n$ symmetric matrix A over $\mathbb{Z}$, let Q_A be the quadratic form in n variables with Gram matrix A. By definition two integral quadratic forms in n variables Q_A and Q_B are equivalent if the quadratic lattices $(\mathbb{Z}^n, Q_A)$ and $(\mathbb{Z}^n, Q_B)$ are isometric. It is easy to see that this is equivalent to the classical definition for there to exist a matrix $\gamma \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$A = \gamma^t B \gamma. \tag{1.1}$$

When A and B are given, the above is a system of quadratic Diophantine equations whose unknowns are the entries of γ. As frequently used in the study of Diophantine problems, if one can show that a given system of Diophantine equations has a solution of explicitly bounded height, then in principle determining solvability and finding a solution are both reduced to a finite search, and thus addressing both of the Decision and Realization Problems in one stroke. For this reason, results of this type are called *search bounds*. For equivalence of quadratic forms a search bound was essentially established in Siegel's work [19]. As later worked out by Straumann [21], Siegel's method produces the following *exponential* search bound: if Q_A and Q_B are equivalent, then there exists a $\gamma \in \mathrm{GL}_n(\mathbb{Z})$ satisfying (1.1) such that

$$\|\gamma\| < \exp(C_n |\det A|^{\frac{n^3+n^2}{2}}) \max(\|A\|, \|B\|)^{\frac{n^3-n^2}{2}}. \tag{1.2}$$

The exponential search bound is optimal for $n = 2$ due to Pell's equations. For $n \geq 3$ Masser conjectured in [17] the existence of a *polynomial* search bound for the equivalence of quadratic forms. For ternary quadratic forms the conjecture was solved in [8] by Dietmann, who also confirmed Masser's conjecture in [9] for a large class of quadratic forms in four or more variables. A complete resolution of Masser's conjecture was recently given in [15] by G. A. Margulis and the second author of the present paper, using an approach based on homogeneous dynamics. A consequence of the main result in [15] is that for $n \geq 3$ the estimate (1.2) may be improved as

$$\|\gamma\| < D_n(\|A\| + \|B\|)^{n^3}.$$

The goal of this paper is to further push the method developed in [15] to address the Realization Problem for quadratic lattices over number fields with rank $n \geq 3$ by giving (to our knowledge) a first search procedure. Note that when $\mathcal{O}$ is not a principal ideal domain, a finitely generated $\mathcal{O}$-module may not be free. Hence, over a number field, the equivalence of quadratic lattices may not set up directly using Gram matrices. Nevertheless, our procedure utilizes a polynomial search bound for the equivalence of quadratic forms over number fields *with congruence conditions*, which we prove using methods from algebraic groups, homogeneous dynamics and spectral theory of automorphic forms.

The paper is organized as follows. In Section 2 we state our effective search bound for the equivalence of quadratic forms over number fields (Theorem 2.1), and then use it to present and justify our search procedure for the Realization Problem of quadratic lattices over number fields with rank $n \geq 3$. The rest of the paper is devoted to the proof of Theorem 2.1, which is given in Section 7 after our technical preparation from Section 3 through Section 6.

Throughout the paper the notation $X \ll Y$ stands for that the quantities X and Y satisfy the inequality $X < CY$ where C is a positive constant depending only on the rank $n \geq 3$ and the number field F; and the notation $X \asymp Y$ means that $X \ll Y$ and $Y \ll X$ both hold true.

2. Search procedure for the realization problem

2.1. **Effective search bounds with congruence conditions.** We begin by introducing some notation for the sets of matrices which will be used extensively in the subsequent discussion. For a commutative ring R (with identity) and an integer $n > 0$, we denote by $\mathrm{M}_n(R)$ the ring of $n \times n$ matrices with entries in R, $\mathrm{GL}_n(R) = \{A \in \mathrm{M}_n(R) : A \text{ is invertible and } A^{-1} \in \mathrm{M}_n(R)\}$ the group of invertible matrices in $\mathrm{M}_n(R)$, $\mathrm{SL}_n(R)$ the subgroup of unimodular matrices in $\mathrm{GL}_n(R)$, and $\mathrm{Sym}_n(R)$ the set of symmetric matrices with entries in R. Throughout the paper, F is a number field having exactly ℓ archimedean places, and $\mathcal{O}$ is the ring of integers of F. The archimedean places of F is identified with a fixed family of inequivalent embeddings

$$\{\sigma_1 = \mathrm{id}, \sigma_2, \dots, \sigma_\ell\} \tag{2.1}$$

of F into $\mathbb{C}$. For any $1 \leq i \leq \ell$, we set $F_{\sigma_i} = \mathbb{R}$ if $\sigma_i(F) \subseteq \mathbb{R}$, and $F_{\sigma_i} = \mathbb{C}$ otherwise. Denote by

$$F_\infty = \{(y_1, y_2, \dots, y_\ell) \colon\ y_i \in F_{\sigma_i} \text{ for each } 1 \leq i \leq \ell\}.$$

The notation $\| \ \|_\infty$ stands for the sup-norm on $\mathrm{M}_n(\mathbb{R})$ or $\mathrm{M}_n(\mathbb{C})$. Identifying $\mathrm{M}_n(F_\infty)$ with the product space $\prod_{i=1}^{\ell} M_n(F_{\sigma_i})$, we define for each $y = (y_1, y_2, \cdots, y_\ell) \in \mathrm{M}_n(F_\infty)$

$$\|y\| = \max\{\|y_i\|_\infty \colon 1 \leq i \leq \ell\}. \tag{2.2}$$

The space $\mathrm{M}_n(F)$ is naturally embedded into $\mathrm{M}_n(F_\infty)$ via the map

$$\alpha \mapsto \widetilde{\alpha} = (\alpha, \sigma_2(\alpha), \dots, \sigma_\ell(\alpha)). \tag{2.3}$$

This allows us to measure the size of each *nonzero* element $\alpha \in \mathrm{M}_n(F)$ using the height function

$$\mathsf{H}(\alpha) := \max(\|\widetilde{\alpha}\|, 1). \tag{2.4}$$

Since $\|\widetilde{\alpha}\| \geq 1$ for each nonzero $\alpha \in \mathrm{M}_n(\mathcal{O})$, taking the maximum in (2.4) essentially guarantees $\mathsf{H}(\alpha) \geq 1$ for any $\alpha \in \mathrm{M}_n(F) \setminus \mathrm{M}_n(\mathcal{O})$. When $\alpha \in F \setminus \{0\}$, we will naturally use $\mathsf{H}(\alpha)$ to denote the height of the matrix $(\alpha) \in \mathrm{M}_1(F)$.

Theorem 2.1. *For any integer $n \geq 3$ and number field F, there exists a constant $C > 0$ satisfying the following property. Let $\mathcal{O}$ be the ring of integers of F, let A, $B \in \mathrm{Sym}_n(\mathcal{O})$ be non-singular, and let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. Denote by ℓ the number of archimedean places of F. Suppose that $A = \tau_0^t B \tau_0$ for some $\tau_0 \in \mathrm{GL}_n(\mathcal{O})$. Then there exists $\tau \in \mathrm{GL}_n(\mathcal{O})$ such that*

$$\begin{aligned} \det \tau &= \det \tau_0, \\ A &= \tau^t B \tau, \\ \tau &\equiv \tau_0 \pmod{\mathfrak{a}}, \end{aligned}$$

$$\begin{aligned} \mathsf{H}(\tau) < C \cdot |\mathcal{O}/\mathfrak{a}|^{3\ell n^2} \cdot \mathsf{H}(\det A)^{9\ell n} \\ \cdot \mathsf{H}(\det A^{-1})^{6\ell n^2} \cdot \mathsf{H}(A)^{\ell n^2} \cdot \mathsf{H}(B)^{5\ell n^3} \cdot \mathsf{H}(\det A/\det B)^{5\ell n^3+1/2}. \end{aligned}$$

Note that since for each $T > 0$ the set $\{x \in \mathrm{M}_n(\mathcal{O}) \colon \mathsf{H}(x) \leq T\}$ is finite, Theorem 2.1 provides an effective search bound for determining the equivalence of two given non-degenerate quadratic forms Q_A and Q_B with coefficients in $\mathcal{O}$, and for finding an invertible linear transformation $\tau \in \mathrm{GL}_n(\mathcal{O})$ to realize the equivalence when Q_A and Q_B are equivalent.

2.2. Search procedure and its justification.

Let Q be a non-degenerate quadratic form over F in $n \geq 3$ variables. The vector space F^n becomes a quadratic space over F by viewing Q as the underlying quadratic map from F^n to F. We also use Q to denote the Gram matrix with respect to the standard basis of F^n. An isomorphism $\sigma : F^n \to F^n$ is a isometry of (F^n, Q) if $Q(\sigma(x)) = Q(x)$ for all $x \in F^n$. This is tantamount to saying that $\sigma^t Q \sigma = Q$, after we identify every linear operator on F^n with its matrix representation with respect to the standard basis of F^n.

Recall that a finitely generated $\mathcal{O}$-submodule of F^n may not be free. So, in general, to specify a lattice on F^n we need a pseudo-basis of the lattice. Let $\mathcal{J}$ be a complete set of ideal class representatives of the ideal class group of F. For the purpose of later discussion, we choose the ideals in $\mathcal{J}$ to be fractional ideals containing $\mathcal{O}$. A lattice M on F^n can be written as

$$M = \mathfrak{a}_1 v_1 + \cdots + \mathfrak{a}_n v_n,$$

where the column vectors $v_1, \ldots, v_n$ form a basis of F^n and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are fractional ideals in $\mathcal{J}$. Let Λ be the matrix $[v_1 \cdots v_n]$ and I be the list $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ of fractional ideals. The pair (Λ, I) is called a pseudo-basis of M; see [6].

Let h be the smallest positive rational integer such that $h\mathfrak{a} \subseteq \mathcal{O}$ for all $\mathfrak{a} \in \mathcal{J}$. This h depends only on F. Let $\mathcal{F}(M)$ be the set of free sublattices of M containing hM. For example, the free lattice $\mathcal{O}v_1 + \cdots + \mathcal{O}v_n$ is in $\mathcal{F}(M)$. There are only finitely many sublattices in the family $\mathcal{F}(M)$, and there are effective algorithms which generate all of them. One of them is based on [6, Theorem 2.5] which we describe as follows. First, we note that the quotient $\mathcal{O}$-module M/hM is finite. For each of its submodule $\mathcal{W}$, we fix a finite set of vectors $U(\mathcal{W})$ in M whose images in M/hM generate $\mathcal{W}$. If $\overline{M}$ is the preimage of $\mathcal{W}$ under the natural quotient map $M \to M/hM$, then

$$\overline{M} = \sum_{w \in U(\mathcal{W})} \mathcal{O}w + \sum_{i=1}^{n} \mathfrak{a}_i h v_i.$$

The algorithm [6, Theorem 2.5] then returns a pesudo-basis of $\overline{M}$ such that

$$\overline{M} = \mathfrak{c}_1 z_1 + \cdots + \mathfrak{c}_n z_n.$$

We could further make use of the results in [6] to change $\mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1}$ to $\mathcal{O}$ (see the remark in [6, Page 1063]). So, we may very well assume that

$$\overline{M} = \mathcal{O}z_1 + \cdots + \mathcal{O}z_{n-1} + \mathfrak{c}_n z_n.$$

If $\mathfrak{c}_n$ is principal, then $\overline{M}$ is free; otherwise it is not. If $\mathfrak{c}_n = c\mathcal{O}$, then replacing z_n by cz_n we obtain a basis of $\overline{M}$. Testing if a fractional ideal is principal can be done effectively using the results developed in [5].

So, the lattices in $\mathcal{F}(M)$ can be determined effectively. We fix a basis for each free lattice $\overline{M}$ in the family $\mathcal{F}(M)$. Such a choice of basis gives rise to a Gram matrix $B_{\overline{M}}$. The maximum of the heights of these Gram matrices depends only on M.

Recall that two lattices on F^n are said to be isometric if there is an isometry of F^n which sends one to the other. It is clear that any lattice which is isometric to a free lattice must also be free. Let N be another lattice on F^n, given as

$$N = \mathfrak{f}_1 w_1 + \cdots + \mathfrak{f}_n w_n,$$

where $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ are fractional ideals in $\mathcal{J}$. We assume as we may that (1) M and N are isometric; and (2) the arithmetic volumes (see [20, 82:9]) of M and N are the same. There is no harm for making assumption (2) because isometric lattices have the same arithmetic volume, and arithmetic volume of a given lattice may be effectively computed from a specified pseudo-basis. As an application of Theorem 2.1 we will show that an explicit isometry σ from N to M can be found after a finite search.

Since M and N are assumed to be isometric, theoretically there exists an isometry σ_0 sending N to M. Let A be the Gram matrix of (F^n, Q) with respect to $\{w_1, \ldots, w_n\}$. The isometry σ_0 maps the free lattice $\overline{N} := \mathcal{O}w_1 + \cdots + \mathcal{O}w_n$ into a free sublattice $\overline{M}$ of M. Since $\overline{N}$ is in $\mathcal{F}(N)$, $\overline{M}$ must be in $\mathcal{F}(M)$. Let $\{z_1, \ldots z_n\}$ be the basis of $\overline{M}$ chosen at the outset as described earlier, and denote by $B_{\overline{M}}$ the Gram matrix of (F^n, Q) with respect to $\{z_1, \ldots z_n\}$. Let γ_0 be the matrix $Z^{-1}\sigma_0 W$, where

$$W = [w_1 \ \cdots \ w_n] \quad \text{and} \quad Z = [z_1 \ \cdots \ z_n].$$

Then, since $\gamma_0(\mathcal{O}^n) = \mathcal{O}^n$, γ_0 is an element of $\mathrm{GL}_n(\mathcal{O})$. Furthermore, we have

$$\gamma_0^t B_{\overline{M}} \gamma_0 = A.$$

By Theorem 2.1, there exists $\gamma \in \mathrm{GL}_n(\mathcal{O})$ satisfying $A = \gamma^t B_{\overline{M}} \gamma$ and $\gamma \equiv \gamma_0 \pmod{h\mathcal{O}}$, such that $\mathsf{H}(\gamma)$ is bounded above by a constant depending only on n,

F, M, and N. Let $\sigma = Z\gamma W^{-1}$. Then

$$\begin{aligned}\sigma^t Q \sigma &= W^{-t}\gamma^t Z^t Q Z \gamma W^{-1}\\ &= W^{-t}\gamma^t B_{\overline{M}}\gamma W^{-1}\\ &= W^{-t} A W^{-1}\\ &= W^{-t} W^t Q W W^{-1}\\ &= Q.\end{aligned}$$

Therefore, σ is an isometry from $\overline{N}$ to $\overline{M}$. The congruence condition of γ implies that $(\gamma - \gamma_0)x \in h\mathcal{O}^n$ for all $x \in \mathcal{O}^n$. Since $\overline{N} = W\mathcal{O}^n$ and $\overline{M} = Z\mathcal{O}^n$, we have

$$(\sigma - \sigma_0)(\overline{N}) = Z(\gamma - \gamma_0)W^{-1}(\overline{N}) \subseteq h\overline{M} \subseteq hM.$$

On the other hand, since $hx \in \overline{N}$ for any $x \in N$, we have $\sigma(hx) - \sigma_0(hx) \in hM$. This shows that $\sigma(x) - \sigma_0(x) \in M$, which implies that $\sigma(x) \in M$. Consequently, σ is an embedding of N into M. Recall that M and N are assumed to have the same arithmetic volume. Therefore, σ is actually an isometry of the lattices N and M!

Finally, since $\gamma \in \mathrm{M}_n(\mathcal{O})$ and $\mathsf{H}(\gamma)$ is bounded above by an effective constant depending only on n, F, M, N, γ can be found by a (theoretically) finite search and hence $\sigma = Z\gamma W^{-1}$ can also be found after a finite search.

3. Notation and preliminary results

3.1. **A standing assumption.** Recall from (2.1) that the archimedean places of F are identified with the embeddings $\{\sigma_1 = \mathrm{id}, \sigma_2, \dots, \sigma_\ell\}$ of F into $\mathbb{C}$. Suppose first that the quadratic form Q_A is totally definite, that is, when F is totally real and $Q_{\sigma_i(A)}$ is a definite real quadratic form for each $1 \le i \le \ell$. In this case, Theorem 2.1 has an easy solution using linear algebra which we leave to the readers as an exercise. From now on we shall consider only the case when $Q_{\sigma_i(A)}$ is isotropic for at least one archimedean completion σ_i of F, and document our assumption as follows.

Standing Assumption 3.1. The non-singular matrices A, $B \in \mathrm{Sym}_n(\mathcal{O})$ are given such that Q_A is isotropic over F_{σ_1}, and that the quadratic forms Q_A and Q_B are equivalent over $\mathcal{O}$.

Our assumption implies either that $F_{\sigma_1} = \mathbb{C}$, or that $F_{\sigma_1} = \mathbb{R}$ and Q_A is an indefinite quadratic form over F_{σ_1}.

3.2. **Group theoretic setups.** Following the notation from Section 2, we define

$$G = \mathrm{SL}_n(F_\infty) = \prod_{i=1}^{\ell} \mathrm{SL}_n(F_{\sigma_i}).$$

The identity matrix of order n will be denoted by I_n; and the identity element of G will be denoted by 1_G. Let L be a closed subgroup of G, and let $\delta > 0$ be a real number. We will denote by

$$B_L(\delta) = \{x \in L \colon \|x - 1_G\| < \delta\} \tag{3.1}$$

the ball of radius δ in L centered at 1_G, where the norm of each element of G was defined in (2.2).

Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. We set

$$\Gamma_{\mathfrak{a}} = \left\{\widetilde{\gamma} = (\gamma, \sigma_2(\gamma), \dots, \sigma_\ell(\gamma)) \colon \gamma \in \mathrm{SL}_n(\mathcal{O}) \text{ and } \gamma \equiv I_n \pmod{\mathfrak{a}}\right\}.$$

Since $\mathfrak{a}$ is nonzero, the quotient $\mathcal{O}/\mathfrak{a}$ is finite. It follows that $\Gamma_{\mathfrak{a}}$ is a lattice in G, that is, a discrete subgroup of finite covolume. We denote by $[g]_{\mathfrak{a}}$ the element in $G/\Gamma_{\mathfrak{a}}$ corresponding to the left coset $g\Gamma_{\mathfrak{a}}$. When $\mathfrak{a} = \mathcal{O}$, we will drop the subscript $\mathfrak{a}$. Hence, the notations Γ and $[g]$ will stand for, respectively, $\Gamma_{\mathcal{O}}$ and $[g]_{\mathcal{O}}$.

The special orthogonal group of the quadratic form Q_A is

$$\mathrm{SO}_A = \left\{g \in \mathrm{SL}_n : g^t A g = A\right\}.$$

It is an algebraic group defined over the field F because the entries of A are in $\mathcal{O}$. Since $n \geq 3$, the group SO_A is semisimple. Let p and q be nonnegative integers such that $n = p + q$. We define

$$X_{p,q} = \begin{cases} \mathrm{diag}(1, -1, I_{p-1}, -I_{q-1}) & \text{if } 0 < p, q < n, \\ I_n & \text{if } p = n \text{ and } q = 0, \\ -I_n & \text{if } p = 0 \text{ and } q = n. \end{cases}$$

As we will see in (4.1), this choice of $X_{p,q}$ will allow us to make use of certain element b_y from the orthogonal group $\mathrm{SO}_{X_{p,q}}$.

Definition 3.2. *Let $A \in \mathrm{Sym}_n(\mathcal{O})$ be non-singular. For any $1 \leq i \leq \ell$ we set*

$$(3.2) \qquad X_i = \begin{cases} I_n, & F_{\sigma_i} = \mathbb{C}; \\ X_{p,q}, & F_{\sigma_i} = \mathbb{R} \textit{ and the signature of } Q_A \textit{ is } (p,q). \end{cases}$$

Such $(X_1, \ldots, X_n)$ will be called the associated standard forms of A or that of Q_A.

Since there are only finitely many possible associated standard forms for each dimension n, any constant depending on such data may be regarded as dependent only on n. Let $\mathrm{SO}^0_{X_i}(F_{\sigma_i})$ denote the identity component of $\mathrm{SO}_{X_i}(F_{\sigma_i})$. We define

$$(3.3) \qquad \widetilde{H} = \prod_{i=1}^{\ell} \mathrm{SO}_{X_i}(F_{\sigma_i}), \qquad H = \prod_{i=1}^{\ell} \mathrm{SO}^0_{X_i}(F_{\sigma_i}).$$

Then $\widetilde{H}$ is a closed, semisimple subgroup of G, whose identity component is H. The group H is noncompact, since Q_A is isotropic over F_{σ_1} by our Standing Assumption 3.1.

3.3. **Some results from linear algebra.**

Let us state and prove a linear algebra lemma which will be used extensively in the sequel.

Lemma 3.3. *The following statements hold.*

(1) *For each non-singular matrix $M \in \mathrm{Sym}_n(\mathbb{R})$ of signature (p,q), there exists a matrix $g \in \mathrm{SL}_n(\mathbb{R})$ such that*

$$M = |\det M|^{1/n} g^t X_{p,q} g,$$

and that

$$\|g\|_\infty \ll |\det M|^{-1/(2n)} \|M\|_\infty^{1/2}.$$

(2) *Let $M \in \mathrm{Sym}_n(\mathbb{C})$ be non-singular, and let $\lambda \in \mathbb{C}$ be such that $\lambda^n = \det M$. Then there exists a matrix $g \in \mathrm{SL}_n(\mathbb{C})$ such that*

$$M = \lambda g^t g,$$

and that

$$\|g\|_\infty \ll |\det M|^{-1/(2n)} \|M\|_\infty^{1/2}.$$

Proof.

(1) The signature of the non-singular real symmetric matrix $|\det M|^{-1/n}M$ is also equal to (p,q). Suppose that $|\det M|^{-1/n}M$ is diagonal, say $|\det M|^{-1/n}M = \mathrm{diag}(a_1,\dots a_n)$. Let $\mathrm{sgn}(\cdot)$ be the sign function of the real numbers. Then

$$|\det M|^{-1/n}M = \begin{pmatrix}\sqrt{|a_1|} & & \\ & \ddots & \\ & & \sqrt{|a_n|}\end{pmatrix}\begin{pmatrix}\mathrm{sgn}(a_1) & & \\ & \ddots & \\ & & \mathrm{sgn}(a_n)\end{pmatrix}\begin{pmatrix}\sqrt{|a_1|} & & \\ & \ddots & \\ & & \sqrt{|a_n|}\end{pmatrix}.$$

Since $\sqrt{|a_i|} \le |\det M|^{-1/(2n)}\|M\|_\infty^{1/2}$ for each $1 \le i \le n$, our claim follows. When $|\det M|^{-1/n}M$ is not diagonal, a standard result from linear algebra tells us that there exists an orthogonal real matrix $K \in \mathrm{O}(n)$ such that $|\det M|^{-1/n}K^tMK$ is diagonal. Since $\|K\|_\infty \le 1$, our result can thus be deduced from the previous diagonal case.

(2) Applying the Takagi Factorization to $\lambda^{-1}M$, we see that there exist a positive diagonal matrix $D = \mathrm{diag}(d_1,\dots,d_n)$ and a unitary complex matrix V such that

$$\lambda^{-1}M = V^tDDV,$$

and that d_1^4, d_2^4, $\dots$, d_n^4 are the eigenvalues of the self-adjoint matrix $(\lambda^{-1}M)(\lambda^{-1}M)^*$. Clearly,

$$\|(\lambda^{-1}M)(\lambda^{-1}M)^*\|_\infty = |\lambda|^{-2}\|MM^*\|_\infty \ll |\lambda|^{-2}\|M\|_\infty^2.$$

As $(\lambda^{-1}M)(\lambda^{-1}M)^*$ is self-adjoint, all its eigenvalues are bounded above by $\|(\lambda^{-1}M)(\lambda^{-1}M)^*\|_\infty$ and hence by $|\lambda|^{-2}\|M\|_\infty^2$, up to an absolute multiplicative constant. This implies that

$$\|D\|_\infty \ll (|\lambda|^{-2}\|M\|_\infty^2)^{1/4} = |\det M|^{-1/(2n)}\|M\|_\infty^{1/2}.$$

Since V is unitary, its norm $\|V\|_\infty \le 1$. From $\det(\lambda^{-1}M) = 1$ we get that $\det D = 1$, and $\det V \in \{-1,1\}$. If $\det V = 1$, then $g = DV$ satisfies our lemma. If $\det V = -1$, then we can take $g = \tau DV$, where τ is a fixed element in $\mathrm{O}(n,\mathbb{C})$ with $\det(\tau) = -1$. □

Lemma 3.3 allows us to introduce Definition 3.4.

Definition 3.4. *Let $(X_1,\dots,X_n)$ be the associated standard forms (Definition 3.2) of a non-singular $A \in \mathrm{Sym}_n(\mathcal{O})$. We call $g = (g_1,\dots,g_\ell) \in G$ a representative of A or say that $g \in G$ represents A, if for each $1 \le i \le \ell$ the matrices $\sigma_i(A)$ and $g_i^tX_ig_i$ are proportional. That is, for each $1 \le i \le \ell$ there exists a $\lambda_i \in F_{\sigma_i}$ such that*

$$\sigma_i(A) = \lambda_i g_i^tX_ig_i.$$

Since A is non-singular, by Lemma 3.3, a representative of A in G always exists. Lemma 3.5 shows that equivalent quadratic forms have representatives whose projections in G/Γ lie on the same orbit of the subgroup H.

Lemma 3.5. *Let A, $B \in \mathrm{Sym}_n(\mathcal{O})$ be non-singular, and denote by*

$$\widetilde{A} = (A, \sigma_2(A),\dots,\sigma_\ell(A)), \qquad \widetilde{B} = (B, \sigma_2(B),\dots,\sigma_\ell(B)).$$

Suppose that $A = \gamma_0^t B \gamma_0$ for some $\gamma_0 \in \mathrm{SL}_n(\mathcal{O})$. Then there exist a $g_A \in G$ representing A and a $g_B \in G$ representing B such that $H.[g_A] = H.[g_B]$, that

$$\|g_A\| \ll \mathsf{H}(\det A^{-1})^{1/(2n)} \mathsf{H}(A)^{1/2}, \qquad \|g_B\| \ll \mathsf{H}(\det B^{-1})^{1/(2n)} \mathsf{H}(B)^{1/2}, \tag{3.4}$$

and that for any $h \in H$ we have

$$\widetilde{A} = (g_B^{-1} h g_A)^t \widetilde{B} (g_B^{-1} h g_A). \tag{3.5}$$

Proof. Let the group $\widetilde{H}$ be as defined in (3.3), and let Σ be a fixed, finite set which contains exactly one element from each connected component of $\widetilde{H}$. Let $1 \le i \le \ell$ be given. Since $A = \gamma_0^t B \gamma_0$ and $\gamma_0 \in \mathrm{SL}_n(\mathcal{O})$, we have $\det A = \det B$ and the quadratic forms $\sigma_i(A)$ and $\sigma_i(B)$ are equivalent over F_{σ_i}. By Lemma 3.3, there exist $\lambda_i \in F_{\sigma_i}$ and $S_i, T_i \in \mathrm{SL}_n(F_{\sigma_i})$ such that

$$|\lambda_i|^n = |\det(\sigma_i(A))|, \qquad \sigma_i(A) = \lambda_i S_i^t X_i S_i, \qquad \sigma_i(B) = \lambda_i T_i^t X_i T_i,$$

and that the following estimates hold:

$$\|S_i\|_\infty \ll \mathsf{H}(\det A^{-1})^{1/(2n)} \mathsf{H}(A)^{1/2}, \qquad \|T_i\|_\infty \ll \mathsf{H}(\det B^{-1})^{1/(2n)} \mathsf{H}(B)^{1/2}.$$

Let $g_A = (S_1, \ldots, S_\ell)$ and $g_B = (T_1, \ldots, T_\ell)$. Then g_A, $g_B \in G$, and they satisfy (3.4). Write

$$\widetilde{\gamma_0} = (\gamma_0, \sigma_2(\gamma_0), \ldots, \sigma_\ell(\gamma_0)).$$

From $A = \gamma_0^t B \gamma_0$ we get that

$$\widetilde{A} = \widetilde{\gamma_0}^t \widetilde{B} \widetilde{\gamma_0}.$$

So for each $1 \le i \le \ell$, we have

$$S_i^t X_i S_i = \sigma_i(\gamma_0)^t T_i^t X_i T_i \sigma_i(\gamma_0).$$

Since $T_i \sigma_i(\gamma_0) S_i^{-1}$ preserves X_i for each $1 \le i \le \ell$, we get that

$$g_B \widetilde{\gamma_0} g_A^{-1} \in \widetilde{H}.$$

Replacing g_B by $k g_B$ for some k in Σ (fixed at the beginning of the proof), if necessary, we can assume that $g_B \gamma_0 g_A^{-1} \in H$. This implies that $H.[g_A] = H.[g_B]$. Finally, (3.5) follows from straightforward matrix computation, which we leave to the readers as an exercise. □

3.4. Measure theoretic setups.

Recall that an inner product on the Lie algebra $\mathrm{Lie}(G)$ gives rise to a left invariant Riemannian metric on G, which induces a Haar measure m_G on G. We shall fix an inner product on $\mathrm{Lie}(G)$ such that the covolume of Γ in G is equal to 1 with respect to m_G. The restriction of this inner product on $\mathrm{Lie}(H)$ induces a Haar measure m_H on H.

Suppose that $g \in G$ represents A. Then

$$g^{-1} H g = \prod_{i=1}^{\ell} \mathrm{SO}^0_{\sigma_i(A)}(F_{\sigma_i}) = \mathrm{SO}^0_A(F_\infty).$$

Since the coefficients of A are in $\mathcal{O}$, the subgroup $g^{-1} H g \cap \Gamma_{\mathfrak{a}}$ is a lattice in $g^{-1} H g$, and thus $H \cap g \Gamma_{\mathfrak{a}} g^{-1}$ is a lattice in H. So, if Ω is a Borel fundamental domain of the right action of $H \cap g\Gamma_{\mathfrak{a}} g^{-1}$ on H, then $m_H(\Omega)$ is finite. The value of $m_H(\Omega)$, or equivalently the covolume of $H \cap g\Gamma_{\mathfrak{a}} g^{-1}$ in H, will be referred to as the volume of the orbit $H.[g]_{\mathfrak{a}}$ and denoted by $\mathrm{vol}_H(H.[g]_{\mathfrak{a}})$. Note that this volume is independent of the choice of the representative g of A. In this case, the orbit $H.[g]_{\mathfrak{a}}$ is *periodic* in the sense that there is a unique H-invariant probability measure $\mu_{H.[g_A]}$ supported on $H.[g]_{\mathfrak{a}}$. This measure may be explicitly realized as the push-forward measure of the probability measure $\frac{1}{m_H(\Omega)} m_\Omega$, where m_Ω is the restriction of m_H on Ω, under the natural projection $H \to H.[g]_{\mathfrak{a}}$ defined by $h \mapsto h[g]_{\mathfrak{a}}$. Let $\{Z_1, \dots, Z_m\}$ be an orthonormal basis of $\mathrm{Lie}(H)$ with respect to the fixed inner product. For $f \in C_c^\infty(H.[g]_{\mathfrak{a}})$, we consider the second order Sobolev norm $\mathcal{S}_2(f)$:

$$\mathcal{S}_2(f) = \max\left\{\|Z_i Z_j(f)\|_2 \colon 1 \le i, j \le m\right\}.$$

This Sobolev norm will be used in Section 4 to analyze the quantitative behavior of the action of H on $H.[g]_{\mathfrak{a}}$.

4. Ergodic theory and spectral gaps

Let $A \in \mathrm{Sym}_n(\mathcal{O})$ be non-singular, and let $(X_1, \dots, X_\ell)$ be the associated standard forms of A (see Definition 3.2). Denote by $e_1, \dots, e_n$ the standard basis of $F_{\sigma_1}^n$. We define

$$S_0 = \{h \in \mathrm{SO}^0_{X_1}(F_{\sigma_1}) \colon h(e_i) = e_i \text{ for any } i \neq 1, 2, 3\}.$$

Since A is isotropic over F_{σ_1} by our Standing Assumption 3.1, we have

$$S_0 \cong \begin{cases} \mathrm{SO}_3(\mathbb{C}) & \text{if } F_{\sigma_1} = \mathbb{C}; \\ \mathrm{SO}^0(2,1) & \text{if } F_{\sigma_1} = \mathbb{R} \text{ and } p \ge 2; \\ \mathrm{SO}^0(1,2) & \text{if } F_{\sigma_1} = \mathbb{R} \text{ and } p = 1. \end{cases}$$

Letting

$$\alpha = \begin{cases} -1 & \text{if } F_{\sigma_1} = \mathbb{R} \\ \sqrt{-1} & \text{if } F_{\sigma_1} = \mathbb{C}, \end{cases}$$

we have for each $y > 0$

$$b_y = \begin{pmatrix} \frac{1}{2}(y + \frac{1}{y}) & \frac{\alpha}{2}(y - \frac{1}{y}) & \\ \frac{\alpha^3}{2}(y - \frac{1}{y}) & \frac{1}{2}(y + \frac{1}{y}) & \\ & & I_{n-2} \end{pmatrix} \in S_0. \tag{4.1}$$

Finally, we let S be the closed subgroup of H defined by

$$S = \{(s_1, I_n, \dots, I_n) \in H \colon s_1 \in S_0\} = S_0 \times \{I_n\} \times \cdots \times \{I_n\}; \tag{4.2}$$

and for each $y > 0$, we specify the element

$$a_y = (b_y, I_n, \dots, I_n) \in S.$$

Then, clearly, for each $0 < y < 1$

$$\|a_y\| \asymp y^{-1}. \tag{4.3}$$

Lemma 4.1. *Let $A \in \mathrm{Sym}_n(\mathcal{O})$ be non-singular, let $g \in G$ be a representative of A, and let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. Then, in the notation of the preceding paragraph,*

(1) *the group S acts ergodically on $(H.[g]_{\mathfrak{a}}, \mu_{H.[g]_{\mathfrak{a}}})$;*
(2) *for any functions φ, $\psi \in C_c^\infty(H.[g]_{\mathfrak{a}})$ and any $0 < y < 1$,*

$$\left|\langle a_y \varphi, \psi\rangle - \mu_{H.[g]_{\mathfrak{a}}}(\varphi)\mu_{H.[g]_{\mathfrak{a}}}(\psi)\right| \ll y^{1/3}\mathcal{S}_2(\varphi)\mathcal{S}_2(\psi). \tag{4.4}$$

Proof.

(1) Since the stabilizer of $[g]_{\mathfrak{a}}$ in H is $H \cap g\Gamma_{\mathfrak{a}}g^{-1}$, the H action on $H.[g]_{\mathfrak{a}}$ is equivalent to its action on $H/(H \cap g\Gamma_{\mathfrak{a}}g^{-1})$. Letting $H_A = g^{-1}Hg$, it suffices to show the ergodicity of the action of $g^{-1}Sg$ on $H_A/(H_A \cap \Gamma_{\mathfrak{a}})$. Consider the subgroup $H_1 = \mathrm{SO}^0_{X_1}(F_{\sigma_1}) \times \{I_n\} \times \cdots \times \{I_n\}$ of H. Clearly, $S \subseteq H_1$ and

$$g^{-1}H_1g = \mathrm{SO}^0_A(F_{\sigma_1}) \times \{I_n\} \times \cdots \times \{I_n\} \subseteq H_A.$$

By the strong approximation theorem (see [16, Chapter 2 - Theorem 6.8] and the Remark thereafter), $g^{-1}H_1g\Gamma_{\mathfrak{a}}$ is dense in H_A.

Suppose that the Lie group $g^{-1}H_1g$ is simple. This happens when H is not isomorphic to $\mathrm{SO}_4(\mathbb{C})$ or $\mathrm{SO}(2,2)^0$. Since $g^{-1}H_1g\Gamma_{\mathfrak{a}}$ is dense in H_A, by [16, Chapter 2 - Theorem 7.2], the $g^{-1}H_1g$ action on $H_A/(H_A \cap \Gamma_{\mathfrak{a}})$ is ergodic. By Howe-Moore's Theorem, the action of the noncompact subgroup $g^{-1}Sg$ on the quotient $H_A/(H_A \cap \Gamma_{\mathfrak{a}})$ is mixing, and hence is ergodic.

Suppose now that $g^{-1}H_1g$ is semisimple but not simple. In this case, H_1 is isomorphic to $\mathrm{SO}(4,\mathbb{C})$ or $\mathrm{SO}(2,2)^0$. In either case, the projection of S to each simple factor of H_1 is surjective. This implies, again by [16, Chapter 2 - Theorem 7.2], that the action of $g^{-1}Sg$ on the quotient $H_A/(H_A \cap \Gamma_{\mathfrak{a}})$ is ergodic.

(2) The estimate is determined by the set of irreducible unitary representations S which appears in the representation of S on $L^2_0(H.[g]_{\mathfrak{a}}, \mu_{H.[g]_{\mathfrak{a}}})$, the space of square integrable functions with vanishing integration. We begin by specifying a parametrization for the unitary dual of S.

When $F_{\sigma_1} = \mathbb{R}$, we have $S \cong \mathrm{SO}^0(2,1)$ or $S \cong \mathrm{SO}^0(1,2)$. Following [14, Section 3] we parametrize the unitary dual of S using the set

$$\{1/2 + i\mathbb{R}\} \cup [1/2, 1] \subseteq \mathbb{C},$$

where the vertical line $\{1/2+i\mathbb{R}\}$ corresponds to principal series and $(1/2, 1]$ to complementary series, with the endpoint $\{1\}$ standing for the one dimensional trivial representation.

When $F_{\sigma_1} = \mathbb{C}$, we have $S \cong \mathrm{SO}(3,\mathbb{C})$. (Note that the Lie groups $\mathrm{SO}(3,\mathbb{C})$ and $\mathrm{SO}^0(1,3)$ are isomorphic.) Following [13, Section 5] we parametrize the unitary dual of S using the set

$$\{1 + i\mathbb{R}\} \cup [1, 2] \subseteq \mathbb{C},$$

so that the vertical line $\{1+i\mathbb{R}\}$ corresponds to principal series and the interval $(1, 2]$ to complementary series, with the endpoint $\{2\}$ standing for the one dimensional trivial representation. The proof of the lemma relies crucially on the following spectral gap estimate, which is uniform in the sense that it is independent of the quadratic form A and the representative g.

Claim. The parameter of any irreducible unitary representation of S which is weakly contained in the representation of S on $L^2_0(H.[g]_{\mathfrak{a}}, \mu_{H.[g]_{\mathfrak{a}}})$ belongs to $\{1/2 + i\mathbb{R}\} \cup [1/2, 39/64]$ if $F_{\sigma_1} = \mathbb{R}$; and to $\{1 + i\mathbb{R}\} \cup [1, 71/64]$ if $F_{\sigma_1} = \mathbb{C}$.

Assuming this Claim, the proof of (4.4) involves a standard and well-known procedure of analyzing the decay of matrix coefficients which can be found in [13, Proposition 5.3]. Here we have chosen to use the exponent 1/3 in (4.4) for the convenience of computation in later sections of the paper, instead of the best possible one resulted from this method.

The rest of the proof is devoted to justifying the Claim. It involves a number of deep results in the spectral theory of automorphic forms which we shall collect from various literatures. As in the proof of part (1), the S action on $H.[g]_{\mathfrak{a}}$ is equivalent to its action on $H/(H \cap g\Gamma_{\mathfrak{a}} g^{-1})$; and this action is equivalent to the action of $g^{-1}Sg$ on $H_A/(H_A \cap \Gamma_{\mathfrak{a}})$. In what follows, when k is a field containing F and Σ a subspace of k^n, the notation $\Sigma^{\perp}$ shall stand for the orthogonal complement of Σ with respect to the non-degenerate symmetric bilinear form induced by A. That is, with vectors in k^n considered as columns,

$$\Sigma^{\perp} = \left\{x \in k^n \colon y^t A x = 0 \text{ for any } y \in \Sigma\right\}.$$

Write $g = (g_1, \dots, g_\ell)$. Then $g^{-1}Sg = (g_1^{-1}S_0 g_1) \times \{I_n\} \times \cdots \times \{I_n\}$. From the definition of S_0, we see that there is a 3-dimensional subspace $W \subseteq F_{\sigma_1}^n$ such that the signature of the restriction of the quadratic form A on W is the same as that of in the definition of S_0, and that

$$g_1^{-1} S_0 g_1|_{W^{\perp}} = \mathrm{id}.$$

On the other hand, by diagonalizing A over F we conclude that there is a 3-dimensional subspace $V \subseteq F^n$ such that the restriction of the quadratic form A on $V \otimes_F F_{\sigma_1}$ has the same signature with the restriction of A on W. Let

$$\mathbf{L} = \{l \in \mathrm{SO}_A \colon l|_{V^{\perp}} = \mathrm{id}\}.$$

Then $\mathbf{L}$ is an algebraic group defined over F with $\mathbf{L}^0(F_{\sigma_1})$ isomorphic to S_0. By Witt's extension theorem (see [4]), there exists a $t \in \mathrm{SO}_A^0(F_{\sigma_1})$ such that $t.W = V \otimes_F F_{\sigma_1}$. This implies

$$t^{-1} g_1^{-1} S_0 g_1 t = \mathbf{L}^0(F_{\sigma_1}).$$

Therefore, it suffices to analyze the action of $L = \mathbf{L}^0(F_{\sigma_1}) \times \{I_n\} \times \cdots \times \{I_n\}$ on $L^2(H_A/(H_A \cap \Gamma_{\mathfrak{a}}))$.

Let π be an irreducible unitary representations of L which is weakly contained in the representation of L on $L^2(H_A/(H_A \cap \Gamma_{\mathfrak{a}}))$. By the Burger-Sarnak restriction principle [3], such π must lie in the automorphic spectrum of $\mathbf{L}^0(F_{\sigma_1})$. But since $\dim V = 3$, the group $\mathbf{L}$ is an F-form of PGL_2. By the Jacquet-Langlands correspondence [10], the parameter of π belongs to the automorphic spectrum of the split form $\mathrm{PGL}_2(F_{\sigma_1})$ which has been extensively studied as the Generalized Ramanujan Conjecture. As of this writing, the automorphic spectrum of the split form $\mathrm{PGL}_2(F_{\sigma_1})$ is known to be contained in $\{1/2 + i\mathbb{R}\} \cup [1/2, 39/64]$ if $F_{\sigma_1} = \mathbb{R}$ by the work of Kim-Sarnak [11]; and in $\{1 + i\mathbb{R}\} \cup [1, 71/64]$ if $F_{\sigma_1} = \mathbb{C}$ thanks to the work of Blomer-Brumley [2]. (Notice that both [11] and [2] produced a parameter $7/64$ which translates, respectively, to the parameters $39/64 = 1/2 + 7/64$ and $71/64 = 1 + 7/64$ used in this proof.) This finishes the proof of the Claim and consequently the lemma. □

Proposition 4.2 establishes a quantitative result on the "distance" of two given points on the same periodic H-orbit.

Proposition 4.2. *Let $A \in \mathrm{Sym}_n(\mathcal{O})$ be non-singular, let $g \in G$ be a representative of A, and let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. Let x_1, $x_2 \in G$ and assume that $[x_1]_{\mathfrak{a}}$, $[x_2]_{\mathfrak{a}} \in H.[g]_{\mathfrak{a}}$. Let $0 < \delta_1, \delta_2 < 1$ be such that for any $i = 1, 2$ the map*

$$B_H(\delta_i) \to H.[g]_{\mathfrak{a}}, \qquad h \mapsto h.[x_i]_{\mathfrak{a}}$$

is injective. (See (3.1) *for the definition of $B_H(\delta)$.) Then there exists an $h \in H$ such that $h.[x_1]_{\mathfrak{a}} = [x_2]_{\mathfrak{a}}$, and that*

$$\|h\| \ll \mathrm{vol}_H(H.[g]_{\mathfrak{a}})^3 \cdot (\delta_1\delta_2)^{-4\dim H}. \tag{4.5}$$

Proof. Let $V = \mathrm{vol}_H(H.[g]_{\mathfrak{a}})$. For each $i = 1, 2$ we can choose (see for instance [12, Lemma 2.4.7]) a smooth function ψ_i which is supported in $B_H(\delta_i).[x_i]_{\mathfrak{a}}$ and satisfies

$$\mu_{H.[g]_{\mathfrak{a}}}(\psi_i) = \frac{1}{V}, \qquad \mathcal{S}_2(\psi_i) \ll \frac{\delta_i^{-(2+\frac{\dim H}{2})}}{\sqrt{V}} \leq \frac{\delta_i^{-\frac{4\dim H}{3}}}{\sqrt{V}}.$$

Therefore, in view of (4.4), when

$$\mu_{H.[g]_{\mathfrak{a}}}(\psi_1)\mu_{H.[g]_{\mathfrak{a}}}(\psi_2) \gg y^{1/3}\mathcal{S}_2(\psi_1)\mathcal{S}_2(\psi_2),$$

and in particular for some

$$y^{-1} \asymp V^3(\delta_1\delta_2)^{-4\dim H},$$

we have $\langle a_y\psi_1, \psi_2\rangle \neq 0$. But this implies $\mathrm{supp}(a_y\psi_1) \cap \mathrm{supp}(\psi_2) \neq \emptyset$. Hence, we get

$$(a_yB_H(\delta_1).[x_1]_{\mathfrak{a}}) \cap B_H(\delta_2).[x_2]_{\mathfrak{a}} \neq \emptyset.$$

Recall from (4.3) that $\|a_y\| \asymp y^{-1}$. So there exists some $h \in H$ such that $h.[x_1]_{\mathfrak{a}} = [x_2]_{\mathfrak{a}}$, and that

$$\|h\| \asymp \|a_y\| \ll V^3(\delta_1\delta_2)^{-4\dim H}.$$

This proves our proposition. □

5. Injectivity radius and volumes of periodic orbits

The key estimate (4.5) for the H-translates on periodic orbits involves the injectivity radius for the points and the volume of the orbit. The goal of this section is to build more explicit connections between these quantities and the data of the given quadratic forms. Our first result explores the injectivity radius for points in quotients of the group G.

Lemma 5.1. *For each $n \geq 3$ and number field F, there exists a constant $c > 0$ satisfying the following property. For any $g \in G$, any $\gamma \in \Gamma$, and any nonzero ideal $\mathfrak{a}$ of $\mathcal{O}$, the map $B_G(c|g|^{-n}) \to G/\Gamma_{\mathfrak{a}}$ defined by $k \mapsto k[g\gamma]_{\mathfrak{a}}$ is injective. (See* (3.1) *for the definition of $B_G(\delta)$.)*

Proof. Let 1_G be the identity element of G. We first show that for some $\delta_1 \asymp \|g\|^{-n}$, we have $B_G(\delta_1) \cap g\Gamma g^{-1} = \{1_G\}$. Let $\tau \in \Gamma\backslash\{1_G\}$. Since $\tau - 1_G = g^{-1}(g\tau g^{-1} - 1_G)g$, we have

$$\|g\tau g^{-1} - 1_G\| \gg \|\tau - 1_G\| \cdot \|g\|^{-1} \cdot \|g^{-1}\|^{-1}.$$

As $\tau \in \Gamma \setminus \{1_G\}$, there exists a nonzero matrix $M \in M_n(\mathcal{O})$, such that

$$\tau - 1_G = (\sigma_1(M), \sigma_2(M), \dots, \sigma_\ell(M)).$$

Since M is integral and nonzero, there is an $1 \leq i \leq \ell$ such that $\|\sigma_i(M)\|_\infty \geq 1$. Hence, we get

$$\|\tau - 1_G\| \geq 1.$$

As the determinant of each component of g is equal to one, the inverse matrix formula gives us $\|g^{-1}\| \ll \|g\|^{n-1}$. So

$$\|g\tau g^{-1} - 1_G\| \gg \|g\|^{-n}.$$

This implies that for some $\delta_1 \asymp \|g\|^{-n}$, we have $B_G(\delta_1) \cap g\Gamma g^{-1} = \{1_G\}$.

Let $\delta \asymp \|g\|^{-n}$ be such that for any k_1, $k_2 \in B_G(\delta)$ the product

$$k_2^{-1}k_1 \in B_G(\delta_1).$$

Let $g \in G$, let $\gamma \in \Gamma$, and let k_1, $k_2 \in B_G(\delta)$ be such that

$$k_1[g\gamma]_{\mathfrak{a}} = k_2[g\gamma]_{\mathfrak{a}}.$$

Then $k_2^{-1}k_1 \in g\Gamma_{\mathfrak{a}}g^{-1} \subseteq g\Gamma g^{-1}$. But our choice of δ forces $k_2^{-1}k_1 \in B_G(\delta_1)$. From $k_2^{-1}k_1 \in B_G(\delta_1) \cap g\Gamma g^{-1} = \{1_G\}$ we get that $k_1 = k_2$. This finishes the proof of our lemma. □

Our next result is concerned with the uniform recurrence of periodic H-orbits in G/Γ. It states that for each periodic orbit most points lie in a fixed compact subset of G/Γ. The argument is close to that of [1, Section 4].

Lemma 5.2. *For any $\varepsilon > 0$, there exists a compact subset $\Omega \subseteq G/\Gamma$ such that for any non-singular $A \in \mathrm{Sym}_n(\mathcal{O})$ and any $g \in G$ representing A, we have*

$$\mu_{H.[g]}(\Omega) > 1 - \varepsilon.$$

Proof. Let $\varepsilon > 0$ be given. Note that with respect to the standard $\mathbb{Q}$-structure, we have $G = (\mathrm{Res}_{F/\mathbb{Q}}\,\mathrm{SL})(\mathbb{R})$ and $\Gamma = (\mathrm{Res}_{F/\mathbb{Q}}\,\mathrm{SL})(\mathbb{Z})$. By a theorem of Dani-Margulis (see [7, Theorem 2]), there exists a compact subset $\Omega \subseteq G/\Gamma$ such that for any unipotent one-parameter subgroup $\{u_t\}$ of G and for any $y \in G$, one of the followings must hold:

(DM1) There exists a $T_y > 0$ such that $|\{0 < t < T\colon u(t).[y] \in \Omega\}| > (1-\varepsilon)T$ for all $T > T_y$.

(DM2) There exists a parabolic subgroup $P \subseteq G$, a closed subgroup $P_1 \subseteq P$, and a $\lambda \in (\mathrm{Res}_{F/\mathbb{Q}}\,\mathrm{SL})(\mathbb{Q})$ such that $y^{-1}Uy \subseteq \lambda P_1 \lambda^{-1}$ and that $\lambda P_1 \lambda^{-1}.[1_G]$ is closed in G/Γ.

Let S be as in (4.2), and let $U = \{u(t)\colon t \in \mathbb{R}\}$ be a one parameter unipotent subgroup of S. Recall from Lemma 4.1 that S acts ergodically on $H.[g]$. By the Howe-Moore theorem, the action of U on $H.[g]$ is mixing. Let $x \in G$ be such that $[x] \in H.[g]$ is U-generic in the sense of Birkhoff ergodic theorem. That is, for any continuous function f on $H.[g]$ with compact support

$$\lim_T \frac{1}{T}\int_0^T f(u(t).[x])\ \mathrm{d}t = \int_{H.[g]} f\ \mathrm{d}\mu_{H.[g]}. \tag{5.1}$$

We shall now eliminate the possibility of (DM2) for our choice of U and x. Suppose, for the sake of contradiction, that (DM2) holds true for U and x. Then, on one hand, we have

$$\overline{x^{-1}Ux.[1_G]} \subseteq \lambda P_1 \lambda^{-1}.[1_G].$$

By (5.1), $U.[x]$ is dense in $H.[x]$. This implies

$$\overline{x^{-1}Ux.[1_G]} = \overline{x^{-1}Ux\Gamma/\Gamma} = x^{-1}Hx\Gamma/\Gamma = x^{-1}Hx.[1_G].$$

The two relations above imply $x^{-1}Hx \subseteq \lambda P \lambda^{-1}$. On the other hand, since $G = (\mathrm{Res}_{F/\mathbb{Q}}\,\mathrm{SL})(\mathbb{R})$ and $P \subseteq G$ is parabolic, there exists a parabolic $\mathbb{Q}$-subgroup $\mathbb{P}$ of SL_n such that $P = (\mathrm{Res}_{F/\mathbb{Q}}\mathbb{P})(\mathbb{R})$ (see for instance [16, Chapter I - Section 1.7]). Hence $x^{-1}Hx \subseteq \lambda P \lambda^{-1}$ is impossible, because for each $1 \leq i \leq \ell$ there is no connected, closed subgroup of $\mathrm{SL}_n(F_{\sigma_i})$ which properly contains $\mathrm{SO}_{X_i}(F_{\sigma_i})$. In particular, $\mathrm{SO}_{X_i}(F_{\sigma_i})$ is not contained in any parabolic subgroup other than

$\mathrm{SL}_n(F_{\sigma_i})$. This leads to a contradiction. Therefore, (DM1) most hold for our choice of U and x.

Combining (DM1) and (5.1), we get that

$$\mu_{H.[g]}(\Omega) > 1 - \varepsilon.$$

This proves our lemma. □

Proposition 5.3 relates the height of the determinant of A and the volume of the periodic H-orbit in G/Γ passing through the projection of a representative of A. In establishing such result we will make crucial use of Lemma 5.2 on the uniform recurrence of periodic H-orbits.

Proposition 5.3. *For any non-singular $A \in \mathrm{Sym}_n(\mathcal{O})$ and any $g \in G$ which represents A, we have*

$$\mathrm{vol}_H(H.[g]) \ll \mathsf{H}(\det A)^{(\dim G - \dim H)/n}. \tag{5.2}$$

Proof. Let 1_G be the identity element of the group G. By Lemma 5.2, we may fix a compact subset $\Omega \subseteq G/\Gamma$ independent of A and g, and satisfying

$$\mu_{H.[g]}(\Omega) > 0.99.$$

We first show that Ω contains two points on the orbit $H.[g]$ which are "close" along a direction within G but transversal to H: there exist a $u \in G \setminus \widetilde{H}$, where the group $\widetilde{H}$ was defined in (3.3), and an $x \in G$ such that

$$[x] \in H.[g] \cap \Omega, \qquad u.[x] \in H.[g] \cap \Omega, \qquad \|u - 1_G\| \ll \mathrm{vol}_H(H.[g])^{-1/(\dim G - \dim H)}. \tag{5.3}$$

To this end, we consider the decomposition $\mathfrak{g} = \mathrm{Lie}(G)$ with respect to the adjoint action of H:

$$\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{h}_0.$$

We set for any subspace $\mathfrak{b} \subseteq \mathfrak{g}$ and any $r > 0$

$$B_{\mathfrak{b}}(r) = \{X \in \mathfrak{b} \colon \|X\|_\infty < r\}.$$

Let $0 < \varepsilon_0 < 1$ be such that the exponential map $\exp\colon B_{\mathfrak{g}}(\varepsilon_0) \to G$ is one-to-one. Suppose that $0 < r < \varepsilon_0$ and that the map

$$B_{\mathfrak{h}_0}(r) \times (H.[g] \cap \Omega) \to G/\Gamma, \qquad (U, [y]) \mapsto \exp(U).[y] \tag{5.4}$$

is injective. Computing the volume for these sets shows that such $r > 0$ has to be sufficiently small:

$$r^{\dim G - \dim H} \cdot 0.99 \cdot \mathrm{vol}_H(H.[g]) \ll \mathrm{vol}_G(B_{\mathfrak{h}_0}(r)(H.[g] \cap \Omega)) < \mathrm{vol}_G(G/\Gamma) = 1.$$

This implies that for some

$$r_1 \asymp \mathrm{vol}_H(H.[g])^{-1/(\dim G - \dim H)}$$

the map in (5.4) would fail to be one-to-one. So there exist $(U_1, [x]), (U_2, [y]) \in B_{\mathfrak{h}_0}(r_1) \times (H.[g] \cap \Omega)$ such that

$$(U_1, [x]) \neq (U_2, [y]), \qquad \exp(U_1).[x] = \exp(U_2).[y].$$

Note that $U_1 \neq U_2$ (for otherwise $[x] = [y]$). So $u = \exp(-U_2)\exp(U_1)$ and $[x]$ satisfy (5.3).

Next we show that

$$\|u - 1_G\| \gg \mathsf{H}(\det A)^{-1/n}. \tag{5.5}$$

Since $[x] \in \Omega$, we may assume that $x \in G$ and $\|x - 1_G\| < C_0$ for some $C_0 > 0$ depending on the compact set Ω. In the sequel, for any $Y \in \mathrm{M}_n(\mathcal{O})$ the notation $\widetilde{Y}$ shall stand for

$$\widetilde{Y} = (Y, \sigma_2(Y), \dots, \sigma_\ell(Y)).$$

Let $(X_1, \dots, X_\ell)$ be the associated standard forms (Definition 3.2) of A. As $g = (g_1, \dots, g_\ell) \in G$ represents A, there exists $(\lambda_1, \dots \lambda_\ell) \in F_{\sigma_1} \times \cdots \times F_{\sigma_\ell}$ such that

$$|\lambda_i|^n = |\det \sigma_i(A)|, \qquad \widetilde{A} = (\lambda_1 g_1^t X_1 g_1, \dots, \lambda_\ell g_\ell^t X_\ell g_\ell).$$

Write $x \in G$ as $x = (x_1, \dots, x_\ell)$. From $[x] \in H.[g]$ we get that $x \in Hg\Gamma$. So there exists a non-singular $B \in \mathrm{Sym}_n(\mathcal{O})$ equivalent to A, such that

$$\widetilde{B} = (\lambda_1 x_1^t X_1 x_1, \dots, \lambda_\ell x_\ell^t X_\ell x_\ell).$$

Likewise, since $ux \in Hg\Gamma = Hx\Gamma$, there exists a non-singular $D \in \mathrm{Sym}_n(\mathcal{O})$ such that

$$\widetilde{D} = (\lambda_1 x_1^t u_1^t X_1 u_1 x_1, \dots, \lambda_\ell x_\ell^t u_\ell^t X_\ell u_\ell x_\ell).$$

Write $ux = hx\gamma$ with $h \in H$ and $\gamma \in \Gamma$. Then $\widetilde{B} = \gamma^t \widetilde{D} \gamma$. We note that $\widetilde{B} \neq \widetilde{D}$, for otherwise, that γ preserves $\widetilde{D}$ would force u to preserve $(X_1, \dots, X_\ell)$, implying $u \in \widetilde{H}$ (a contradiction!). Because $B - D$ is integral and nonzero, there exists $1 \le i \le \ell$ such that

$$|\lambda_i| \cdot \|x_i^t X_i x_i - x_i^t u_i^t X_i u_i x_i\|_\infty \ge 1.$$

Since $\|x_i\|_\infty \le \|x\| < C_0 + 1$ and since matrix multiplication are polynomials, we have

$$\|x_i^t X_i x_i - x_i^t u_i^t X_i u_i x_i\|_\infty \ll \|u_i - I_n\|_\infty \le \|u - 1_G\|.$$

The previous two inequalities give us

$$\|u - 1_G\| \gg 1/|\lambda_i| \ge 1/\mathsf{H}(\det A)^{1/n},$$

thus proving (5.5).

Finally, combining the estimates of $\|u - 1_G\|$ from (5.3) and (5.5), we get

$$\mathsf{H}(\det A)^{-1/n} \ll \|u - 1_G\| \ll \mathrm{vol}_H(H.[g])^{-1/(\dim G - \dim H)}.$$

This implies (5.2), finishing the proof of our proposition. □

6. Small coset representatives for subgroups

In this section we shall complete the final preparation for the proof of Theorem 2.1. Let us begin by introducing some notation.

Notation 6.1. Let $B \in \mathrm{Sym}_n(\mathcal{O})$ be non-singular, and let $\widetilde{B} = (B, \sigma_2(B), \dots, \sigma_\ell(B))$. We will use the notation $\widetilde{H}_B$ to denote the group

$$\widetilde{H}_B = \mathrm{SO}_B(F_\infty) = \{x \in G \colon x^t \widetilde{B} x = \widetilde{B}\},$$

and the notation H_B to denote the identity component of $\widetilde{H}_B$.

This notation is chosen in analogy to that of $\widetilde{H}$ and H as defined in (3.3). Suppose that $g \in G$ represents B. Then it is easy to see that

$$\widetilde{H}_B = g^{-1} \widetilde{H} g, \qquad H_B = g^{-1} H g. \tag{6.1}$$

Proposition 6.2. *Let $B \in \mathrm{Sym}_n(\mathcal{O})$ be non-singular, and let $u \in \widetilde{H}_B$ be such that $uH_B \cap \Gamma$ is nonempty. Then there exists a $\theta \in \mathrm{SO}_B(\mathcal{O})$ such that*

$$\widetilde{\theta} = (\theta, \sigma_2(\theta), \ldots, \sigma_\ell(\theta)) \in uH_B \cap \Gamma,$$

and that

$$\mathsf{H}(\theta) \ll \mathsf{H}(\det B)^{3(\dim G - \dim H)/n} \cdot \mathsf{H}(\det B^{-1})^{(8\dim H+1)/2} \cdot \mathsf{H}(B)^{n(8\dim H+1)/2}.$$

In other words, each connected component of $\widetilde{H}_B$ having an integral point must contain an integral point of small height.

Proof. Fix a finite set $\Sigma \subseteq \widetilde{H}$ which contains exactly one element from each connected component of $\widetilde{H}$. Let $g \in G$ be a representative of B with $|g|$ satisfying the estimate in (3.4):

$$\|g\| \ll \mathsf{H}(\det B^{-1})^{1/(2n)} \mathsf{H}(B)^{1/2}.$$

Suppose that $s \in \widetilde{H}$ and $g^{-1}sg \in uH_B \cap \Gamma$. Let $k \in \Sigma$ be such that $kH = sH$. Then

$$g^{-1}kg \in uH_B. \tag{6.2}$$

Since $\mathrm{SO}(n, \mathbb{C})$ is connected and since $\mathrm{SO}(p,q)$ has exactly two connected component, each non-identity element in the quotient group $\widetilde{H}/H$ has order two. This implies $ks \in H$. So

$$Hkg\Gamma = Hkg(g^{-1}sg)\Gamma = Hg\Gamma,$$

where the first equality follows since $g^{-1}sg \in \Gamma$, and the second since $ks \in H$. In other words,

$$H.[g] = H.[kg].$$

By Proposition 4.2 and Lemma 5.1, there exists an $h \in H$ such that $h.[kg] = [g]$ and that

$$\|h\| \ll \mathrm{vol}_H(H.[g])^3 \cdot (\|g\|^{-n} \cdot \|kg\|^{-n})^{-4\dim H} \ll \mathrm{vol}_H(H.[g])^3 \cdot \|g\|^{8n\dim H}.$$

From $hkg\Gamma = g\Gamma$ we get that $g^{-1}hkg \in \Gamma$. So there exists $\theta \in \mathrm{SL}_n(\mathcal{O})$ such that

$$\widetilde{\theta} = (\theta, \sigma_2(\theta), \ldots, \sigma_\ell(\theta)) = g^{-1}hkg.$$

It remains to show that this θ satisfies our proposition. Since H_B is a normal subgroup of $\widetilde{H}_B$, we have $uH_B = H_Bu$. Combining this fact with (6.1) and (6.2) gives us

$$\widetilde{\theta} = g^{-1}hkg = (g^{-1}hg)(g^{-1}kg) \in H_BuH_B = uH_B.$$

Therefore, $\widetilde{\theta} \in uH_B \cap \Gamma$, and this implies $\theta \in \mathrm{SO}_B(\mathcal{O})$. Finally, combining (5.2) and our estimates on $\|g\|$ and $\|h\|$ gives us

$$\begin{aligned}\mathsf{H}(\theta) = \|\widetilde{\theta}\| &\ll \|g^{-1}\| \cdot \|h\| \cdot \|k\| \cdot \|g\| \\ &\ll \|g\|^n \cdot \|h\| \\ &\ll \mathsf{H}(\det B)^{3(\dim G - \dim H)/n} \cdot \mathsf{H}(\det B^{-1})^{(8\dim H+1)/2} \cdot \mathsf{H}(B)^{n(8\dim H+1)/2}.\end{aligned}$$

This proves our proposition. □

To deal with the congruence condition in Theorem 2.1, we need the next result which asserts that certain congruence subgroups admit a complete coset representatives consisting of elements of small height.

Proposition 6.3. *Let $B \in \mathrm{Sym}_n(\mathcal{O})$ be non-singular, and let*

$$\Lambda_B = \{\gamma \in \mathrm{SO}_B(\mathcal{O})\colon \widetilde{\gamma} = (\gamma, \sigma_2(\gamma), \ldots, \sigma_\ell(\gamma)) \in H_B\}.$$

Suppose that $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}$, and consider the congruence subgroup

$$\Lambda_B(\mathfrak{a}) = \{\gamma \in \Lambda_B : \gamma \equiv I_n \pmod{\mathfrak{a}}\}.$$

Then for any $\xi \in \Lambda_B$, there exists an $\eta \in \xi\Lambda_B(\mathfrak{a})$ such that

$$\mathsf{H}(\eta) \ll |\mathcal{O}/\mathfrak{a}|^{3\ell n^2} \cdot \mathsf{H}(\det B)^{3(\dim G - \dim H)/n} \cdot \mathsf{H}(\det B^{-1})^{(8\dim H+1)/2} \cdot \mathsf{H}(B)^{n(8\dim H+1)/2}. \tag{6.3}$$

In other words, each coset of $\Lambda_B(\mathfrak{a})$ in Λ_B contains a representative of small height.

Proof. Let $g \in G$ be a representative of B with $\|g\|$ satisfying the estimate in (3.4):

$$\|g\| \ll \mathsf{H}(\det B^{-1})^{1/(2n)} \mathsf{H}(B)^{1/2}.$$

Since $\xi \in \Lambda_B$, we have $\widetilde{\xi} = (\xi, \sigma_2(\xi), \ldots, \sigma_\ell(\xi)) \in H_B = g^{-1}Hg$. This implies $g\widetilde{\xi} \in Hg$. So

$$H.[g\widetilde{\xi}]_{\mathfrak{a}} = H.[g]_{\mathfrak{a}}.$$

By Lemma 5.1, the injectivity radius of both $[g\widetilde{\xi}]_{\mathfrak{a}}$ and $[g]_{\mathfrak{a}}$ are $\gg \|g\|^{-n}$. It follows from Proposition 4.2 that there exists an $h \in H$ such that $h.[g]_{\mathfrak{a}} = [g\widetilde{\xi}]_{\mathfrak{a}}$ and that

$$\|h\| \ll \mathrm{vol}_H(H.[g]_{\mathfrak{a}})^3 \cdot (\|g\|^{-n} \cdot \|g\|^{-n})^{-4\dim H} = \mathrm{vol}_H(H.[g])^3 \cdot \|g\|^{8n\dim H}.$$

Since $Hg\widetilde{\xi}\Gamma_{\mathfrak{a}} = Hg\Gamma_{\mathfrak{a}}$, we have $g^{-1}hg \in \widetilde{\xi}\Gamma_{\mathfrak{a}}$. Since $H_B = g^{-1}Hg$, there exists $\eta \in \Lambda_B$ such that $\widetilde{\eta} = (\eta, \sigma_2(\eta), \ldots, \sigma_\ell(\eta)) = g^{-1}hg \in \widetilde{\xi}\Gamma_{\mathfrak{a}}$. This implies that $\eta \in \xi\Lambda_B(\mathfrak{a})$.

Note also that

$$\mathrm{vol}_H(H.[g]_{\mathfrak{a}}) \leq [\Gamma : \Gamma_{\mathfrak{a}}] \cdot \mathrm{vol}_H(H.[g]) \leq |\mathcal{O}/\mathfrak{a}|^{\ell n^2}\, \mathrm{vol}_H(H.[g]).$$

Finally, combining

$$\mathsf{H}(\eta) = \|\widetilde{\eta}\| \ll \|g^{-1}\| \cdot \|h\| \cdot \|g\| \ll \|h\| \cdot \|g\|^n$$

and above estimates of $\|g\|$ and $\|h\|$ gives us the desired estimate. □

7. Proof of Theorem 2.1

We first prove a slightly weaker version of Theorem 2.1, in which we assume that the two given quadratic forms over $\mathcal{O}$ are strongly equivalent. That is, the equivalence can be realized by a matrix in $\mathrm{SL}_n(\mathcal{O})$. In general, strongly equivalent quadratic forms are equivalent, but not vice versa.

Theorem 7.1. *For any integer $n \geq 3$ and number field F, there exists a constant $C > 0$ satisfying the following property. Let $\mathcal{O}$ be the ring of integers of F, let A, $B \in \mathrm{Sym}_n(\mathcal{O})$ be non-singular, and let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}$. Denote by ℓ the number of Archimedean places of F. Suppose that $A = \gamma_0^t B\gamma_0$ for some $\gamma_0 \in \mathrm{SL}_n(\mathcal{O})$. Then there exists $\gamma \in \mathrm{SL}_n(\mathcal{O})$ such that*

$$A = \gamma^t B\gamma;$$

$$\gamma \equiv \gamma_0 \pmod{\mathfrak{a}};$$

$$\mathsf{H}(\gamma) < C \cdot |\mathcal{O}/\mathfrak{a}|^{3\ell n^2} \cdot \mathsf{H}(\det A)^{9\ell n} \cdot \mathsf{H}(\det A^{-1})^{6\ell n^2} \cdot \mathsf{H}(A)^{\ell n^3} \cdot \mathsf{H}(B)^{5\ell n^3}.$$

Remark 7.2. Since we will be well-served by "an estimate" of $\mathsf{H}(\gamma)$, the upper bound is left in a rather crude form, for the sake of neatness.

Proof. Our first step in this proof is to find a $\gamma_1 \in \mathrm{SL}_n(\mathcal{O})$ of small height such that

$$A = \gamma_1^t B \gamma_1.$$

Suppose that $g_A \in G$ represents A, $g_B \in G$ represents B, and they together satisfy Lemma 3.5:

$$H.[g_A] = H.[g_B], \quad \|g_A\| \ll \mathsf{H}(\det A^{-1})^{1/(2n)}\mathsf{H}(A)^{1/2},$$
$$\|g_B\| \ll \mathsf{H}(\det B^{-1})^{1/(2n)}\mathsf{H}(B)^{1/2}.$$

Since $A = \gamma_0^t B \gamma_0$ for some $\gamma_0 \in \mathrm{SL}_n(\mathcal{O})$, we have

$$\det A = \det B.$$

By Proposition 4.2 and Lemma 5.1, there exists an $h \in H$ such that $h.[g_A] = [g_B]$ and that

$$\begin{aligned}\|h\| &\ll \mathrm{vol}_H(H.[g])^3 \cdot (\|g_A\|^{-n} \cdot \|g_B\|^{-n})^{-4\dim H}\\ &= \mathrm{vol}_H(H.[g])^3 \cdot \|g_A\|^{4n\dim H} \cdot \|g_B\|^{4n\dim H}.\end{aligned}$$

Combining the estimate of $\mathrm{vol}_H(H.[g])$ from (5.2) and our estimates of $\|g_A\|$ and $\|g_B\|$, we get that

$$\begin{aligned}\|h\| &\ll \mathsf{H}(\det A)^{3(\dim G - \dim H)/n} \cdot (\mathsf{H}(\det A^{-1})\\ &\quad \cdot \mathsf{H}(\det B^{-1}))^{2\dim H} \cdot (\mathsf{H}(A)\cdot \mathsf{H}(B))^{2n\dim H}\\ &= \mathsf{H}(\det A)^{3(\dim G - \dim H)/n} \cdot \mathsf{H}(\det A^{-1})^{4\dim H} \cdot (\mathsf{H}(A)\cdot\mathsf{H}(B))^{2n\dim H}.\end{aligned}$$

From $h.[g_A] = [g_B]$ we get that $hg_A\Gamma = g_B\Gamma$ and that $g_B^{-1}hg_A \in \Gamma$. So there exists a $\gamma_1 \in \mathrm{SL}_n(\mathcal{O})$ satisfying

$$\widetilde{\gamma_1} = (\gamma_1, \sigma_2(\gamma_1), \ldots, \sigma_\ell(\gamma_1)) = g_B^{-1}hg_A \in \Gamma.$$

It follows from Lemma 3.5 that

$$A = \gamma_1^t B \gamma_1.$$

Finally, we have

$$\mathsf{H}(\gamma_1) = \|\widetilde{\gamma_1}\| \ll \|g_B^{-1}\| \cdot \|h\| \cdot \|g_A\| \ll \|g_B\|^{n-1} \cdot \|h\| \cdot \|g_A\|.$$

This finishes the first step proposed at the beginning of the proof.

The rest of the proof is devoted to finding appropriate matrices in $\mathrm{SO}_B(\mathcal{O})$ to multiply γ_1 from the left, so as to produce a matrix γ to satisfy our theorem. We first note, since $A = \gamma_0^t B \gamma_0$, that

$$B = (\gamma_0^{-1})^t A \gamma_0^{-1} = (\gamma_1\gamma_0^{-1})^t B (\gamma_1 \gamma_0^{-1}).$$

There is no guarantee for $\gamma_1\gamma_0^{-1}$ to be in

$$\Lambda_B = \{\gamma \in \mathrm{SO}_B(\mathcal{O})\colon \widetilde{\gamma} = (\gamma, \sigma_2(\gamma), \ldots, \sigma_\ell(\gamma)) \in H_B\}.$$

Nevertheless, there exists $\theta \in \mathrm{SO}_B(\mathcal{O})$ satisfying Proposition 6.2 such that $\widetilde{\theta}\widetilde{\gamma_1}(\widetilde{\gamma_0}^{-1}) \in H_B \cap \Gamma$. This implies that

$$\theta\gamma_1\gamma_0^{-1} \in \Lambda_B.$$

So there exists an $\eta \in \mathrm{SO}_B(\mathcal{O})$ satisfying the estimate in Proposition 6.3 such that

$$\eta\theta\gamma_1\gamma_0^{-1} \in \Lambda_B(\mathfrak{a}) = \{\gamma \in \Lambda_B \colon \gamma \equiv I_n \pmod{\mathfrak{a}}\}.$$

Letting $\gamma = \eta\theta\gamma_1$, we see that

$$A = \gamma_0^t B \gamma_0 = \gamma_0^t [(\eta\theta\gamma_1\gamma_0^{-1})^t B (\eta\theta\gamma_1\gamma_0^{-1})]\gamma_0 = \gamma^t B \gamma.$$

Since $\gamma\gamma_0^{-1} \equiv I_n \pmod{\mathfrak{a}}$, we get that

$$\gamma \equiv \gamma_0 \pmod{\mathfrak{a}}.$$

Finally, combining the estimates for γ_1, θ and η gives us

$$\begin{aligned}\mathsf{H}(\gamma) = \|\widetilde{\gamma}\| &\ll \mathsf{H}(\eta)\cdot\mathsf{H}(\theta)\cdot\mathsf{H}(\gamma_1)\\ &\ll |\mathcal{O}/\mathfrak{a}|^{3\ell n^2}\cdot\mathsf{H}(\det A)^{9\ell n}\cdot\mathsf{H}(\det A^{-1})^{6\ell n^2}\cdot\mathsf{H}(A)^{\ell n^3}\cdot\mathsf{H}(B)^{5\ell n^3}.\end{aligned}$$

This proves our theorem. □

To conclude the present paper, we prove Theorem 2.1 using Theorem 7.1.

Proof of Theorem 2.1. By the assumption of the theorem, $A = \tau_0^t B \tau_0$ for some $\tau_0 \in \mathrm{GL}_n(\mathcal{O})$. Then $\det\tau_0$ is a unit in $\mathcal{O}$, and we denote by x its multiplicative inverse so that $x \in \mathcal{O}$, and $x\cdot\det\tau_0 = 1$. Consider the matrix

$$\Delta = \mathrm{diag}(x, 1, \dots, 1) \in \mathrm{GL}_n(\mathcal{O}).$$

We observe that $\Delta\tau_0 \in \mathrm{SL}_n(\mathcal{O})$, and that

$$A = \tau_0^t B \tau_0 = (\Delta\tau_0)^t \Delta^{-1} B \Delta^{-1} (\Delta\tau_0).$$

Applying Theorem 7.1 to the matrices A, $\Delta^{-1}B\Delta^{-1} \in \mathrm{Sym}_n(\mathcal{O})$, which is legitimate since $\Delta\tau_0 \in \mathrm{SL}_n(\mathcal{O})$, we conclude that there exists a $\gamma \in \mathrm{SL}_n(\mathcal{O})$ such that

$$A = \gamma^t \Delta^{-1} B \Delta^{-1} \gamma;$$
$$\gamma \equiv \Delta\tau_0 \pmod{\mathfrak{a}};$$
$$\mathsf{H}(\gamma) \ll |\mathcal{O}/\mathfrak{a}|^{3\ell n^2}\cdot\mathsf{H}(\det A)^{9\ell n}\cdot\mathsf{H}(\det A^{-1})^{6\ell n^2}\cdot\mathsf{H}(A)^{\ell n^3}\cdot\mathsf{H}(\Delta^{-1}B\Delta^{-1})^{5\ell n^3}.$$

Let $\tau = \Delta^{-1}\gamma \in \mathrm{GL}_n(\mathcal{O})$. Then we have

$$A = \tau^t B \tau;$$
$$\tau \equiv \tau_0 \pmod{\mathfrak{a}}.$$

Since $\det A = \det(\tau_0)^2 \det B$, we get that

$$\mathsf{H}(\Delta^{-1}) = \mathsf{H}(\det\tau_0) = \mathsf{H}(\det A/\det B)^{1/2}.$$

Putting things together gives us

$$\begin{aligned}\mathsf{H}(\tau) &\ll \mathsf{H}(\Delta^{-1})\cdot\mathsf{H}(\gamma)\\ &\ll |\mathcal{O}/\mathfrak{a}|^{3\ell n^2}\cdot\mathsf{H}(\det A)^{9\ell n}\cdot\mathsf{H}(\det A^{-1})^{6\ell n^2}\cdot\mathsf{H}(A)^{\ell n^2}\\ &\qquad\cdot\mathsf{H}(B)^{5\ell n^3}\cdot\mathsf{H}(\det A/\det B)^{5\ell n^3+1/2}.\end{aligned}$$

This proves Theorem 2.1. □

Acknowledgments

The second author would like to thank Gregory Margulis for introducing him to the subject of studying quadratic forms using homogeneous dynamics and for his collaboration in [15] which is tremendously influential to the current paper, and Alex Kontorovich for explaining to him spectral theory of automorphic forms.

References

[1] Menny Aka, Manfred Einsiedler, Han Li, and Amir Mohammadi, *On effective equidistribution for quotients of* $\mathrm{SL}(d, \mathbb{R})$, Israel J. Math. **236** (2020), no. 1, 365–391, DOI 10.1007/s11856-020-1978-z. MR4093891

[2] Valentin Blomer and Farrell Brumley, *On the Ramanujan conjecture over number fields*, Ann. of Math. (2) **174** (2011), no. 1, 581–605, DOI 10.4007/annals.2011.174.1.18. MR2811610

[3] M. Burger and P. Sarnak, *Ramanujan duals. II*, Invent. Math. **106** (1991), no. 1, 1–11, DOI 10.1007/BF01243900. MR1123369

[4] J. W. S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, vol. 13, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978. MR522835

[5] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993, DOI 10.1007/978-3-662-02945-9. MR1228206

[6] Henri Cohen, *Hermite and Smith normal form algorithms over Dedekind domains*, Math. Comp. **65** (1996), no. 216, 1681–1699, DOI 10.1090/S0025-5718-96-00766-1. MR1361805

[7] S. G. Dani and G. A. Margulis, *Asymptotic behaviour of trajectories of unipotent flows on homogeneous spaces*, Proc. Indian Acad. Sci. Math. Sci. **101** (1991), no. 1, 1–17, DOI 10.1007/BF02872005. MR1101994

[8] Rainer Dietmann, *Small solutions of quadratic Diophantine equations*, Proc. London Math. Soc. (3) **86** (2003), no. 3, 545–582, DOI 10.1112/S0024611502013898. MR1974390

[9] Rainer Dietmann, *Polynomial bounds for equivalence of quadratic forms with cube-free determinant*, Math. Proc. Cambridge Philos. Soc. **143** (2007), no. 3, 521–532, DOI 10.1017/S0305004107000710. MR2373956

[10] H. Jacquet and R. P. Langlands, *Automorphic forms on* $\mathrm{GL}(2)$, Lecture Notes in Mathematics, Vol. 114, Springer-Verlag, Berlin-New York, 1970. MR0401654

[11] H. H. Kim, P. Sarnak: *Refined estimates towards the Ramanujan and Selberg conjectures,* Appendix to *Functoriality for the exterior square of* GL_4 *and the symmetric fourth of* GL_2. J. Amer. Math. Soc. 16 (2003), no. 1, 139-183.

[12] D. Y. Kleinbock and G. A. Margulis, *Bounded orbits of nonquasiunipotent flows on homogeneous spaces*, Sinaĭ's Moscow Seminar on Dynamical Systems, Amer. Math. Soc. Transl. Ser. 2, vol. 171, Amer. Math. Soc., Providence, RI, 1996, pp. 141–172, DOI 10.1090/trans2/171/11. MR1359098

[13] Alex Kontorovich and Hee Oh, *Apollonian circle packings and closed horospheres on hyperbolic 3-manifolds*, J. Amer. Math. Soc. **24** (2011), no. 3, 603–648, DOI 10.1090/S0894-0347-2011-00691-7. With an appendix by Oh and Nimish Shah. MR2784325

[14] Alex Kontorovich and Hee Oh, *Almost prime Pythagorean triples in thin orbits*, J. Reine Angew. Math. **667** (2012), 89–131, DOI 10.1515/crelle.2011.128. MR2929673

[15] Han Li and Gregory A. Margulis, *Effective estimates on integral quadratic forms: Masser's conjecture, generators of orthogonal groups, and bounds in reduction theory*, Geom. Funct. Anal. **26** (2016), no. 3, 874–908, DOI 10.1007/s00039-016-0379-2. MR3540455

[16] G. A. Margulis, *Discrete subgroups of semisimple Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 17, Springer-Verlag, Berlin, 1991, DOI 10.1007/978-3-642-51445-6. MR1090825

[17] D. W. Masser, *Search bounds for Diophantine equations*, A panorama of number theory or the view from Baker's garden (Zürich, 1999), Cambridge Univ. Press, Cambridge, 2002, pp. 247–259, DOI 10.1017/CBO9780511542961.017. MR1975456

[18] Peter Sarnak, *Notes on the generalized Ramanujan conjectures*, Harmonic analysis, the trace formula, and Shimura varieties, Clay Math. Proc., vol. 4, Amer. Math. Soc., Providence, RI, 2005, pp. 659–685. MR2192019

[19] Carl Ludwig Siegel, *Zur Theorie der quadratischen Formen* (German), Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1972), 21–46. MR311578

[20] O. T. O'Meara, *The integral representations of quadratic forms over local fields*, Amer. J. Math. **80** (1958), 843–878, DOI 10.2307/2372837. MR98064

[21] S. Straumann, *Das Äquivalenzproblem ganzer quadratischer Formen: Einige explizite Resultate*, Diplomarbeit. Universität Basel, 1999.

Department of Mathematics and Computer Science, Wesleyan University, Middletown, Connecticut 06459
Email address: `wkchan@wesleyan.edu`

Department of Mathematics and Computer Science, Wesleyan University, Middletown, Connecticut 06459
Email address: `hli03@wesleyan.edu`