CONSTRUCTIVE AND STABLE CARTAN–DIEUDONNÉ AND APPLICATIONS TO BINARY QUADRATIC FORMS OVER NUMBER FIELDS

ZE FAN AND HAN LI

Abstract. We construct an explicit Cartan–Dieudonné decomposition for orthogonal group elements of binary quadratic forms over non-archimedean local fields of characteristic zero, expressing each group element as a product of reflections defined by vectors. A key feature of our construction is its stability: we establish quantitative control on how the reflection matrices vary under small perturbations of the underlying vectors. Using this decomposition, we establish an effective result for the equivalence of binary quadratic forms over number fields. Specifically, let K be a number field and S a finite set of non-archimedean places of K. Given two K-equivalent binary quadratic forms integrally equivalent at every prime in S, we provide an explicit search bound for finding a K-equivalence that are integral at all primes in S.

1. Introduction

The study of quadratic forms has played a central role in number theory since the foundational work of Gauss, Minkowski, and Siegel. A key problem in this area is determining when two quadratic forms are equivalent over a given ring or field and, further, whether such an equivalence can be constructed effectively. While the theory over local and global fields is well understood in principle, explicit algorithmic results, particularly those that unify local and global constraints, remain an active area of research.

A fundamental tool in the study of quadratic forms is the Cartan–Dieudonné theorem, which provides a structural decomposition of orthogonal transformations. Classically, this theorem states that every element of the orthogonal group of a non-degenerate quadratic form over a field of characteristic not equal to 2 can be written as a product of reflections. This decomposition not only illuminates the algebraic

Date: October 1, 2025.

structure of the orthogonal group but also serves as a powerful computational device, reducing questions about general isometries to simpler questions about reflections. In this paper, we refine the Cartan–Dieudonné decomposition for special orthogonal groups of binary quadratic forms over non-archimedean local fields of characteristic zero, showing that each group element can be expressed as a product of a pair of reflections with respect to vectors satisfying specific stable properties. This local result is particularly suited for applications in number theory, where control over the analytic properties of the reflecting vectors is essential.

Let us fix the following notation for our main result. Let K be a number field of degree r with ring of integers $\mathcal{O}$, and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$, lying over a rational prime p. Denote by $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$ the valuation ring of $K_\mathfrak{p}$, π a fixed uniformizer of $\mathcal{O}_\mathfrak{p}$, and $|\cdot|_\mathfrak{p}$ the normalized absolute value on $K_\mathfrak{p}$ satisfying $|\pi|_\mathfrak{p} = q^{-1}$, where $q = \#(\mathcal{O}_\mathfrak{p}/\pi\mathcal{O}_\mathfrak{p})$ is the cardinality of the residue field. Let e be the ramification index of $\mathfrak{p}$ over the rational prime p, so that $|p|_\mathfrak{p} = q^{-e}$.

For a quadratic form Q on a vector space V over $K_\mathfrak{p}$, we write $O_Q(K_\mathfrak{p})$ for the orthogonal group consisting all linear automorphs preserving Q, that is,

$$O_Q(K_\mathfrak{p}) := \{g \in \mathrm{GL}(V) : Q(gv) = Q(v) \text{ for all } v \in V\}.$$

The special orthogonal group is defined by

$$O_Q^+(K_\mathfrak{p}) := \{g \in O_Q(K_\mathfrak{p}) : \det(g) = 1\},$$

as a subgroup of $O_Q(K_\mathfrak{p})$ with index 2. Let B_Q be the bilinear form associated with Q. For a non-isotropic vector v, the reflection in the direction of v is the map

$$\sigma_v(x) := x - 2\frac{B_Q(x,v)}{Q(v)}v, \quad x \in V. \tag{1.1}$$

To state our main result on stability, we also define the $\mathfrak{p}$-adic sup-norm of vector $x = (x_1, \ldots, x_n)^t \in (K_\mathfrak{p})^n$ and matrix $M = (m_{ij}) \in \mathrm{Mat}_n(K_\mathfrak{p})$ by

$$\|x\|_\mathfrak{p} := \max_{1\le i\le n} |x_i|_\mathfrak{p}, \quad \text{and } \|M\|_\mathfrak{p} := \max_{1\le i,j\le n} |m_{ij}|_\mathfrak{p}.$$

Theorem 1.1. *Let $\lambda \in K_\mathfrak{p}$ be such that $|\lambda|_\mathfrak{p} \in \{1, q\}$, and define $A = \mathrm{diag}(1, \lambda)$. Then for any matrix $S \in O_A^+(K_\mathfrak{p})$, there exist vectors $\alpha, \xi \in (K_\mathfrak{p})^2$ satisfying*

(a) The $\mathfrak{p}$-adic sup-norms $\|\alpha\|_\mathfrak{p} = \|\xi\|_\mathfrak{p} = 1$.

(b) The matrix S can be decomposed into reflections $S = \sigma_\alpha\sigma_\xi$.

(c) For any $u, v \in (K_\mathfrak{p})^2$ such that $\|\alpha - u\|_\mathfrak{p} < |4|_\mathfrak{p} q^{-2e-2}$ and $\|\xi - v\|_\mathfrak{p} < |4|_\mathfrak{p} q^{-2e-2} \|S\|_\mathfrak{p}^{-2}$, we have the bound

$$\|S - \sigma_u \sigma_v\|_\mathfrak{p} \leq \left|\frac{1}{8}\right|_\mathfrak{p} \|S\|_\mathfrak{p}^4 q^{4e+4} \max\{\|\alpha - u\|_\mathfrak{p}, \|\xi - v\|_\mathfrak{p}\}. \tag{1.2}$$

Notice that Equation (1.2) expresses a precise stability property: if the reflecting vectors α, ξ are perturbed slightly to nearby vectors u, v, then the corresponding product of reflections $\sigma_u \sigma_v$ remains close to $S = \sigma_\alpha \sigma_\xi$, with the deviation bounded explicitly in terms of the perturbation size.

We also remark that our proof yields stronger results than stated. In fact, we obtain explicit formulas for the vectors α and ξ appearing in the construction. As these formulas require additional notation, we present here a simplified version of our theorem and refer to Section 5 for complete details.

While our main theorem is formulated for diagonal quadratic forms, the results extend naturally to general binary quadratic forms. By Proposition 6.1, any non-singular symmetric 2×2 matrix B over $K_\mathfrak{p}$ can be expressed as

$$B = k\, P^t A P$$

for some $k \in K_\mathfrak{p}^\times$, $P \in \mathrm{GL}_2(K_\mathfrak{p})$, and $A = \mathrm{diag}(1, \lambda)$. The conjugation relation

$$P^{-1} O_A^+(K_\mathfrak{p}) P = O_B^+(K_\mathfrak{p})$$

then allows us to transfer our results from diagonal to general forms.

There has been considerable interest in obtaining effective versions of the Cartan–Dieudonné theorem. Fukshansky [Fuk07] showed that every isometry of a regular bilinear space over a number field is a product of reflections defined by vectors of bounded height. Over the fields of real and complex numbers, the problem of a constructive decomposition has been studied in, for instance, [Uhl01, AGARA06, Ful11].

The technical difficulty over local fields is distinct. Over number fields, one can use the product formula to study $Q(v)\sigma_v$ instead of σ_v itself when estimating the height, as in [Fuk07, Lem. 5.1]. Over local fields, however, the term $Q(v)$ remains in the denominator, as Equation (1.1) shows. Thus, we require a lower bound for $|Q(v)|$ to control $\|\sigma_v\|$. In this paper, we obtain such bounds using explicit parametrizations

for isometries of binary quadratic forms. This approach, unfortunately, presents significant obstacles to generalization in higher dimensions.

Theorem 1.1 has an interesting application. Conway and Sloane posed the following question [CS99, Page. 402, Question (G4)]:

> (G4) "*If two quadratic forms are equivalent over $\mathbb{Z}_p$ for every prime p and also equivalent over $\mathbb{R}$, find an explicit rational equivalence whose denominator is prime to any given number.*"

This problem is first resolved by Siegel using the Cayley transformation in [Sie41], and [CGL21] clarified implicit steps in Siegel's argument by exhibiting the effective process of finding such equivalence. O'Meara in [O'M63, 101:7] gave an existential proof, generalizing the result to arbitrary number fields and their completions based on the weak approximation property on the special orthogonal group. Theorem 1.1 makes O'Meara's approach effective, therefore we can extend the result of [CGL21] to number fields, though only in dimension 2. The precise statement is given below, continuing with the notation of Theorem 1.1.

Theorem 1.2. *Pick finitely many distinct non-Archimedean absolute values $|\cdot|_{\mathfrak{p}_1}$, ..., $|\cdot|_{\mathfrak{p}_s}$ on K. Let $A, B \in \mathrm{GL}_2(K) \cap \mathrm{Sym}_2(K)$ be symmetric matrices that are equivalent over K via $\tau_0 \in \mathrm{GL}_2(K)$, and also equivalent over $\mathcal{O}_{\mathfrak{p}_1}, ..., \mathcal{O}_{\mathfrak{p}_s}$.*

(a) There exists a matrix $P \in \mathrm{GL}_2(K)$ and a scalar $k \in K$ such that $kP^tAP = \mathrm{diag}(1, \lambda)$, where $|\lambda|_{\mathfrak{p}_i} \in \{1, q_i\}$ for $i \in \{1, 2, ..., s\}$.

(b) Let $\{b_1, ..., b_r\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}$. Define constants

$$\epsilon = \min_{1 \le i \le s} \left\{ \frac{|8 \det(P)^5|_{\mathfrak{p}_i}}{\|\tau_0^{-1}\|_{\mathfrak{p}_i}^4 \|\tau_0\|_{\mathfrak{p}_i} \|P\|_{\mathfrak{p}_i}^{10} q_i^{4e_i+4}} \right\}$$

and

$$M_K = \sum_{j=1}^{r} \mathsf{H}(b_j), \quad \ell_i = \lceil \log_{N(\mathfrak{p}_i)}(1/\epsilon) \rceil + 1$$

for $i \in \{1, 2, ..., s\}$. Then there exists integral vectors $u, v \in \mathcal{O}^2$ with bounded height

$$\mathsf{H}(u), \mathsf{H}(v) < r M_K \prod_{i=1}^{s} N(\mathfrak{p}_i)^{\ell_i},$$

such that the matrix $\tau_0 P \sigma_u \sigma_v P^{-1} \in \mathrm{GL}_2(K \cap \mathcal{O}_{\mathfrak{p}_i})$ for $i \in \{1, 2, ..., s\}$, and A, B are equivalent via $\tau_0 P \sigma_u \sigma_v P^{-1}$.

The paper is organized as follows. In Section 2, we recall basic facts about absolute values on number fields and establish notation. Section 3 develops the theory of automorphs for diagonal binary quadratic forms, with particular attention to their decomposition into products of reflections. Section 4 proves an effective weak approximation result that allows us to construct global solutions with controlled height. Section 5 formulates a constructive Cartan–Dieudonné decomposition, which constitutes the main result of this paper. Finally, in Section 6 we present an application of this result, giving an effective procedure for finding an equivalence between two globally equivalent forms that are locally equivalent at a finite set of places.

2. Preliminaries

We begin with some foundational materials. A classical result of Ostrowski states that, up to equivalence, every non-trivial absolute value on $\mathbb{Q}$ is either the real absolute value or the p-adic absolute value of some prime p. Let K be a number field with ring of integers $\mathcal{O}$. Absolute values on K extend those on $\mathbb{Q}$ in two distinct ways.

First, for each (real or complex) embedding $\sigma : K \hookrightarrow \mathbb{C}$, we obtain an Archimedean absolute value on K by setting $|x|_\sigma = |\sigma(x)|$, where the right-hand-side denotes the usual absolute value on $\mathbb{C}$.

Second, fix a rational prime p. The ideal $(p) \subseteq \mathbb{Z}$ extends to an ideal in $\mathcal{O}$, which factors as

$$(p)\mathcal{O} = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i},$$

where the $\mathfrak{p}_i$'s are distinct prime ideal in $\mathcal{O}$, and the e_i are their ramification indices. Each $\mathfrak{p}_i$ gives rise to a discrete valuation $v_{\mathfrak{p}_i} : K^\times \to \mathbb{Z}$ defined as follows: for $x = a/b$ with $a, b \in \mathcal{O}$, set $v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(a) - v_{\mathfrak{p}_i}(b)$, where $v_{\mathfrak{p}_i} = n$ if $a \in \mathfrak{p}^n \backslash \mathfrak{p}^{n+1}$, and similarly for b. This valuation is well-defined because $\mathcal{O}$ is a Dedekind domain. The corresponding non-Archimedean absolute value on K is given by

$$|x|_{\mathfrak{p}_i} = \begin{cases} p^{-v_{\mathfrak{p}_i}(x) f_i}, & \text{if } x \neq 0, \\ 0, & \text{if } x = 0, \end{cases}$$

where $f_i = [\mathcal{O}/\mathfrak{p}_i : \mathbb{F}_p]$ is the inertia degree. This convention follows standard sources (see, e.g., [Neu99, Chapter. II, §5]). When the choice of $\mathfrak{p}_i$ is clear from the context,

we may write $q = p^{f_i}$, so the formula simplifies to $|x|_{\mathfrak{p}} = q^{-v_{\mathfrak{p}}(x)}$. Another frequently used immediate consequence is the ramification index e_i is equal to $v_{\mathfrak{p}_i}(p)$.

Absolute values on K arise from one of the constructions above. We denote the set of all absolute values on K by $M(K)$. For $v \in M(K)$, write $v|\infty$ if v arises from an embedding into $\mathbb{C}$, and write $v|p$ for some prime number p if v extends the p-adic absolute value.

For certain classes of elements in $K_{\mathfrak{p}}^{\times}$, square roots can be defined and distinguished via binomial expansion. The following result ensures the validity of such a definition.

Proposition 2.1. *Let K be a number field with ring of integers $\mathcal{O}$, and let $\mathfrak{p} \subseteq \mathcal{O}$ be a non-zero prime ideal dividing (p). Let e be the ramification index of $\mathfrak{p}$, and let $K_{\mathfrak{p}}$ and $\mathcal{O}_{\mathfrak{p}}$ be its completion and its valuation ring, respectively. Then:*

(a) If $p > 2$, the series $\sum_{n=0}^{\infty} \binom{1/2}{n} x^n$ converges in $K_{\mathfrak{p}}$ for all $x \in \mathfrak{p}^e\mathcal{O}_{\mathfrak{p}}$.

(b) If $p = 2$, the series converges for all $x \in \mathfrak{p}^{2e+1}\mathcal{O}_{\mathfrak{p}}$.

Moreover, the limit defines an element whose square is $1 + x$; that is:

$$\left(\sum_{n=0}^{\infty} \binom{1/2}{n} x^n\right)^2 = 1 + x.$$

Proof. To show convergence,we estimate the terms $|\binom{1/2}{n} x^n|_{\mathfrak{p}}$ as $n \to \infty$. For simplicity, we write $p^{f_i} = q$. When $\mathfrak{p}|(p)$ for prime $p > 2$, we know

$$\left|\binom{1/2}{n}\right|_{\mathfrak{p}} = \left|\frac{1/2(1/2-1)\cdots(1/2-n+1)}{n!}\right|_{\mathfrak{p}} \leq \left|\frac{1}{n!}\right|_{\mathfrak{p}} = q^{v_{\mathfrak{p}}(n!)}.$$

By Legendre's formula,

$$v_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor \leq \frac{n}{p-1},$$

so $v_{\mathfrak{p}}(n!) = e v_p(n!) \leq en/(p-1)$. Since $x \in \mathfrak{p}^e\mathcal{O}_{\mathfrak{p}}$, we have $|x|_{\mathfrak{p}} \leq 1/q^e$. Hence,

$$\lim_{n\to\infty} \left|\binom{1/2}{n} x^n\right|_{\mathfrak{p}} \leq \lim_{n\to\infty} q^{\frac{en}{p-1} - en} = 0.$$

The case of $p = 2$ is slightly different. We know

$$\left|\binom{1/2}{n}\right|_{\mathfrak{p}} = \left|\frac{1/2(1/2-1)\cdots(1/2-n+1)}{n!}\right|_{\mathfrak{p}} \leq \left|\frac{1}{n!}\frac{1}{2^n}\right|_{\mathfrak{p}} = q^{v_{\mathfrak{p}}(n!)} q^{v_{\mathfrak{p}}(2)n}.$$

Legendre's formula still gives $v_{\mathfrak{p}}(n!) = ev_2(n!) \leq en$, and by $e = v_{\mathfrak{p}}(2)$ we have $|\binom{1/2}{n}|_{\mathfrak{p}} \leq q^{en}q^{en} = q^{2en}$. On the other hand, $x \in \mathfrak{p}^{2e+1}\mathcal{O}_{\mathfrak{p}}$ implies $|x|_{\mathfrak{p}} \leq 1/q^{2e+1}$, and thus

$$\lim_{n\to\infty} \left| \binom{1/2}{n} x^n \right|_{\mathfrak{p}} = \lim_{n\to\infty} q^{2en-(2e-1)n} = 0.$$

Therefore, the series converges in both cases.

Finally, the square root relation is easily verified through Vandermonde's convolution:

$$\begin{aligned}\left((1+x)^{1/2}\right)^2 &= \left(\sum_{n=0}^{\infty} \binom{1/2}{n} x^n\right)\left(\sum_{n=0}^{\infty} \binom{1/2}{n} x^n\right) \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \binom{1/2}{k}\binom{1/2}{n-k}\right) x^n = \sum_{n=0}^{\infty} \binom{1}{n} x^n = 1 + x.\end{aligned}$$

□

This justifies the following definition:

Definition 2.2. Let K, $\mathcal{O}$, $\mathfrak{p}$, e, $K_{\mathfrak{p}}$, and $\mathcal{O}_{\mathfrak{p}}$ be as in Proposition 2.1. For all $x \in \mathfrak{p}^e\mathcal{O}_{\mathfrak{p}}$ if $p > 2$, and all $x \in \mathfrak{p}^{2e+1}\mathcal{O}_{\mathfrak{p}}$ if $p = 2$, we define the p-adic square root of $1 + x$ by the convergent power series

$$(1+x)_{\mathfrak{p}}^{1/2} = \sum_{n=0}^{\infty} \binom{1/2}{n} x^n.$$

The following three general facts will be used in the proof of Theorem 1.1, Lemma 5.3, and Theorem 1.2.

Lemma 2.3. *Let K be a field of characteristic 0 with a non-Archimedean absolute value $|\cdot|_{\mathfrak{p}}$. For matrices $M, N \in \mathrm{Mat}_n(K_{\mathfrak{p}})$, the following two statements hold.*

(a) $\|MN\|_{\mathfrak{p}} \leq \|M\|_{\mathfrak{p}}\|N\|_{\mathfrak{p}}$.
(b) If M is invertible, then $\|M^{-1}\|_{\mathfrak{p}} \leq \|M\|_{\mathfrak{p}}^{n-1}/|\det(M)|_{\mathfrak{p}}$.

Proof. Clear. □

Lemma 2.4. *Let K be a number field with a non-Archimedean absolute value $|\cdot|_{\mathfrak{p}}$, and let M lies in $\mathrm{GL}_2(K_{\mathfrak{p}})$. If $\det(M) = \pm 1$, then $\|M\|_{\mathfrak{p}} \geq 1$.*

Proof. To be explicit, write

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Thus, we have $|ad - bc|_{\mathfrak{p}} = |\det(M)|_{\mathfrak{p}} = |\pm 1|_p = 1$. The ultrametric triangle inequality of the $\mathfrak{p}$-adic absolute value then yields

$$1 = |ad - bc|_{\mathfrak{p}} \leq \max\{|a|_{\mathfrak{p}}|d|_{\mathfrak{p}}, |b|_{\mathfrak{p}}|c|_{\mathfrak{p}}\} \leq \|M\|_{\mathfrak{p}}^2.$$

That implies $\|M\|_{\mathfrak{p}} \geq 1$, as we want. □

Lemma 2.5. *Let K be a field of characteristic 0 with a non-Archimedean absolute value $|\cdot|_{\mathfrak{p}}$. Let $K_{\mathfrak{p}}$ be the corresponding completion, and $\mathcal{O}_{\mathfrak{p}}$ be its valuation ring. For matrices $M \in \mathrm{GL}_n(K_{\mathfrak{p}})$ and $N \in \mathrm{GL}_n(\mathcal{O}_{\mathfrak{p}})$. If $\|M - N\|_{\mathfrak{p}} < 1$, then $M \in \mathrm{GL}_n(\mathcal{O}_{\mathfrak{p}})$.*

Proof. Since $\|M - N\|_{\mathfrak{p}} < 1$, we have $|m_{ij} - n_{ij}|_{\mathfrak{p}} < 1$ for all $1 \leq i, j \leq n$. Since $N \in \mathrm{GL}_n(\mathcal{O}_{\mathfrak{p}})$, we know $|n_{ij}|_{\mathfrak{p}} \leq 1$. Hence,

$$|m_{ij}|_{\mathfrak{p}} = |n_{ij} + (m_{ij} - n_{ij})|_{\mathfrak{p}} \leq \max\{|n_{ij}|_{\mathfrak{p}}, |m_{ij} - n_{ij}|_{\mathfrak{p}}\} \leq 1,$$

which implies $m_{ij} \in \mathcal{O}_{\mathfrak{p}}$ for all i, j.

It remains to show that $|\det(M)|_{\mathfrak{p}} = 1$. This follows from the fact that the determinant function $\det : \mathrm{GL}_n(K_{\mathfrak{p}}) \to K_{\mathfrak{p}}$ is continuous under the matrix $\mathfrak{p}$-adic sup norm. To show this, we observe

$$\begin{aligned} |\det(M) - \det(N)|_{\mathfrak{p}} &= \left| \sum_{\sigma \in S_n} \prod_{i=1}^{n} (m_{i,\sigma(i)} - n_{i,\sigma(i)}) \right|_p \\ &\leq \max_{\sigma \in S_n} \left| \prod_{i=1}^{n} (m_{i,\sigma(i)} - n_{i,\sigma(i)}) \right|_{\mathfrak{p}} \leq \left(\max_{1 \leq i,j \leq n} |m_{ij} - n_{ij}|_{\mathfrak{p}} \right)^n < 1. \end{aligned}$$

Therefore, $|\det(M)|_{\mathfrak{p}} = \max\{|\det(N)|_{\mathfrak{p}}, |\det(M) - \det(N)|_{\mathfrak{p}}\} = 1$, implying that $M \in \mathrm{GL}_n(\mathcal{O}_{\mathfrak{p}})$. □

3. Form of Automorphs

In this section, we revisit the notion of orthogonal groups of a quadratic form introduced in Section 1, now working in coordinates and representing quadratic forms by symmetric matrices. This equivalent formulation allows us to write down explicit formulas for reflections in dimension 2.

Definition 3.1. Let K be a field of characteristic 0, and let $A \in \mathrm{GL}_2(K)$ be a symmetric matrix. A matrix $S \in \mathrm{GL}_2(K)$ is called an A-automorph over K, denoted $S \in O_A(K)$, if $S^t A S = A$, where S^t denotes the transpose of S. The set of proper A-automorphs over K, denoted $O_A^+(K)$, consists of those $S \in O_A(K)$ with $\det(S) = 1$.

An important class of elements in $O_A(K) \backslash O_A^+(K)$ is given by reflections with respect to A. When the matrix A has a particularly simple form, the reflections can be explicitly expressed as follows.

Definition 3.2. Let K be a field of characteristic 0. Define a matrix $A = \mathrm{diag}(1, \lambda) \in \mathrm{GL}_2(K)$. For vector $(m, n)^t \in (K^\times)^2$, define the matrix $\sigma_{(m,n)^t} \in \mathrm{GL}_2(K)$ by

$$\sigma_{(m,n)^t} = \frac{1}{m^2 + \lambda n^2} \begin{pmatrix} -m^2 + \lambda n^2 & -2\lambda mn \\ -2mn & m^2 - \lambda n^2 \end{pmatrix}.$$

We refer to $\sigma_{(m,n)^t}$ as the reflection (with respect to A) along the direction of the vector $(m, n)^t$.

It follows immediately from Definition 3.2 that the reflection matrix $\sigma_{(m,n)^t}$ is invariant under multiplication: for all $k \in K^\times$, we have $\sigma_{(m,n)^t} = \sigma_{k(m,n)^t}$. Furthermore, each reflection is involutive: $\sigma^2_{(m,n)^t} = I$ for all non-zero vectors $(m, n) \in (K^\times)^2$.

The elements of $O_A^+(K)$ can also be explicitly described.

Proposition 3.3. *Let K be a field of characteristic 0. Define $A = \mathrm{diag}(1, \lambda) \in \mathrm{GL}_2(K)$. Then any element in $O_A^+(K)$ is of the form*

$$S = \begin{pmatrix} a & -c\lambda \\ c & a \end{pmatrix},$$

for some $c \in K$ such that $1 - \lambda c^2$ is a square in K, and $a \in K$ satisfying $a^2 = 1 - \lambda c^2$.

Proof. Fix an arbitrary matrix $S \in O_A^+(K)$, and write $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then the condition $S^t A S = A$ yields the system:

$$\begin{cases} a^2 + c^2\lambda = 1, & (3.1) \\ ab + \lambda cd = 0, & (3.2) \\ b^2 + d^2\lambda = \lambda. & (3.3) \end{cases}$$

Treating c as a parameter and solving the system, we find that Equation (3.1) and (3.3) hold only if $a^2 = d^2 = 1 - \lambda c^2$ and $b^2 = c^2\lambda^2$. To satisfy Equation (3.2), we observe if $a = d$ then $b = -c\lambda$ and $\det(S) = 1$; if $a = -d$ then $b = c\lambda$ and $\det(S) = -1$. Since we require $S \in O_A^+(K)$, only the first case $a = d$ is possible. □

4. Effective Weak Approximation

A central tool for proving our main result is an effective version of the weak approximation theorem. This result enables us to find an integral element in a number field K that approximates prescribed values at finitely many non-Archimedean absolute values, using only a finite search. The finiteness of searching is guaranteed by two key notions that measure the "size" of elements in K: height and norm. We introduce these concepts below.

For an element $x \in K$, the height of x (with respect to K) is defined as

$$\mathsf{H}(x) = \max_{v|\infty} |x|_v.$$

This notion naturally extends to vectors $x = (x_1, ..., x_n)^t \in K^n$ by $\mathsf{H}(x) = \max_{1\le i\le n} \mathsf{H}(x_i)$. The field norm of x, denoted $N(x) = N_{K/\mathbb{Q}}(x)$, is given by

$$N(x) = \prod_{\sigma: K\hookrightarrow\mathbb{C}} \sigma(x).$$

With a slight abuse of notation, for non-zero ideal $\mathfrak{a}$ of $\mathcal{O}$ we use $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$ to denote the norm of $\mathfrak{a}$.

Let K be a number field with degree d, with integral basis $x_1, ..., x_d$. Then K has d embeddings, among which r_1 are real and $2r_2$ are complex. We enumerate te embeddings as $\sigma_1, ..., \sigma_{r_1}$, and $\tau_1, ..., \tau_{2r_2}$, where τ_i is the conjugate of τ_{r_2+i} for $i \in \{1, 2, ..., r_2\}$. We can embed K into $\mathbb{R}^d$ by the Minkowski embedding

$$\sigma : K \to \mathbb{R}^d : x \mapsto \Big(\sigma_1(x), ..., \sigma_{r_1}(x), \Re\tau_1(x), ..., \Re\tau_{r_2}(x), \Im\tau_1(x), ..., \Im\tau_{r_2}(x)\Big).$$

Under this embedding, $\mathcal{O}_K$ becomes a full-rank lattice (i.e. a discrete, finitely generated abelian group) in $\mathbb{R}^d$ with $\mathbb{Z}$-basis $\{\sigma(x_1), ..., \sigma(x_d)\}$. Any non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ is likewise embedded as a full-rank sublattice of $\sigma(\mathcal{O}_K)$, with index $[\sigma(\mathcal{O}_K) : \sigma(\mathfrak{a})] = N(\mathfrak{a})$. We now introduce a standard tool for producing bases of such sublattices.

Definition 4.1. A square matrix $H \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$ with $\det(H) \neq 0$ is in Hermite normal form if:

(1) The matrix H is upper triangular.
(2) The diagonal entries $h_{ii} > 0$ for all $i \in \{1, ..., d\}$.
(3) The off diagonal entries satisfy $0 \leq h_{ij} < h_{ii}$ for all $j \neq i$.

Lemma 4.2. *Let $\Lambda' \subseteq \Lambda \subseteq \mathbb{R}^d$ be full-rank lattices. For every column vector basis matrix $B \in \mathrm{GL}_d(\mathbb{R})$ of Λ, there exists a basis matrix B' of Λ' such that $B' = BH$, where H is a matrix in Hermite normal form.*

Proof. Let B be a basis matrix of Λ, and B_0 be any basis matrix of Λ'. Since Λ' is a sublattice of Λ, every element in Λ' is a $\mathbb{Z}$-linear combination of the column vectors of B. Therefore, we can write $B_0 = BV$ for some integral matrix V with full rank. Basic matrix theory gives the fact that every rational matrix with full rank can be transformed into Hermite normal form by a finite sequence of elementary column operations. Due to unimodularity of those operations, there exists a unimodular matrix U such that $H := VU$ is in Hermite normal form. It suffices to show that $BH = BVU = B_0U$ is also a basis matrix of Λ'. To prove this claim, we observe that for vectors $y = B_0Ux$ where $x \in \mathbb{R}^d$, x is integral if and only if Ux is integral. But x is integral means y is in the lattice generated by B_0U, and Ux is integral means y is in the lattice generated by B_0. That implies B_0 and B_0U generates the same lattice, completing the proof. □

Lemma 4.2 helps us to prove the next result, which can be seen as an effective version of the Weak Approximation Theorem. A version of this result was first established in [CGL21, Lem. 2.3] for $\mathbb{Q}$ and its completions $\mathbb{Q}_p$. Here we adapt their method to general number fields, thereby obtaining the following generalization.

Lemma 4.3. *Let K be a number field of degree r, and let $\mathcal{O}$ be its ring of integers. Take $\{b_1, ..., b_r\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}$. Define $\mathfrak{p}_1, ..., \mathfrak{p}_s$ to be non-zero prime ideals of $\mathcal{O}$, each corresponding to a non-Archimedean absolute value $|\cdot|_{\mathfrak{p}_i}$ on K. Fix a real number $0 < \epsilon \leq 1$, and suppose that for each $\mathfrak{p}_i$, a number $x_i \in \mathcal{O}_{\mathfrak{p}_i}$ is given. Then there exists $z \in \mathcal{O}$ such that for each $1 \leq i \leq s$,*

$$|z - x_i|_{\mathfrak{p}_i} < \epsilon, \quad \text{and} \quad 0 \leq \mathsf{H}(z) < rM_K \prod_{i=1}^{s} N(\mathfrak{p}_i)^{\ell_i},$$

where

$$\ell_i = \left\lceil \log_{N(\mathfrak{p}_i)} \left(\frac{1}{\epsilon} \right) \right\rceil + 1, \quad \text{and} \quad M_K = \sum_{i=1}^{r} \mathsf{H}(b_i).$$

Proof. Since $\mathcal{O}$ is dense in $\mathcal{O}_{\mathfrak{p}_i}$, for each i we may find $z_i \in \mathcal{O}$ such that $|x_i - z_i|_{\mathfrak{p}_i} < \epsilon$. Define an ideal $\mathfrak{a}$ of $\mathcal{O}$ by $\mathfrak{a} = \prod_{i=1}^{s} \mathfrak{p}_i^{\ell_i}$. By the Chinese Remainder Theorem, there exists a coset $z_0 + \mathfrak{a}$ of $\mathfrak{a}$ such that for all $z' \in z_0 + \mathfrak{a}$, we have

$$z' \equiv z_i \mod \mathfrak{p}_i^{\ell_i} \text{ for all } i.$$

This implies $|z' - z_i|_{\mathfrak{p}_i} \leq N(\mathfrak{p}_i)^{-\ell_i} < \epsilon$, and so

$$|z' - x_i|_{\mathfrak{p}_i} \leq \max\{|z' - z_i|_{\mathfrak{p}_i}, |z_i - x_i|_{\mathfrak{p}_i}\} < \epsilon,$$

as we want.

Next, the goal is to find one element in the coset $z_0 + \mathfrak{a}$ with bounded height. To do this, we embed K into $\mathbb{R}^r$ by the Minkowski embedding σ. Let $B = [\sigma(b_1)\ \sigma(b_2)\ ...\ \sigma(b_r)]$ be the basis matrix of the full-rank lattice $\sigma(\mathcal{O})$. By Lemma 4.2 there exists a basis B' of $\sigma(\mathfrak{a})$ such that $B' = BH$, where $H = (h_{ij})$ is in Hermite normal form. Because $\det(B) = \mathrm{vol}(\mathbb{R}^r/\sigma(\mathcal{O}))$ and $\det(B') = \mathrm{vol}(\mathbb{R}^r/\sigma(\mathfrak{a})) = N(\mathfrak{a})\mathrm{vol}(\mathbb{R}^r/\sigma(\mathcal{O}))$, we conclude $\det(H) = N(\mathfrak{a})$. Since H is an integral upper triangular matrix, we have $|h_{ii}| \leq \det(H)$ for $1 \leq i \leq r$. Since off-diagonal entries in matrices of Hermite normal form are strictly less than their diagonal entries, we further conclude that $|h_{ij}| \leq \det(H)$ for all $1 \leq i, j \leq r$. Thus, if we write $\{b_1', ..., b_r'\}$ as the integral basis of $\mathfrak{a}$ generated by B', we can bound the height of the b_i''s by

$$\mathsf{H}(b_i') = \mathsf{H}\left(\sum_{j=1}^{r} h_{ij} b_j\right) \leq \sum_{j=1}^{r} |h_{ij}| \mathsf{H}(b_j) < \sum_{j=1}^{r} |h_{ii}| \mathsf{H}(b_j) \leq M_K N(\mathfrak{a}).$$

Since every coset of $\mathfrak{a}$ must have one of its representative be mapped by σ into the region

$$A = \left\{ \sum_{i=1}^{r} a_i \sigma(b_i') : 0 \leq a_i < 1 \text{ for } i = 1, ..., r \right\},$$

there exists $z \in z_0 + \mathfrak{a}$ such that $\sigma(z) \in A$. Thus

$$\mathsf{H}(z) < \sum_{i=1}^{r} \mathsf{H}(b_i') \leq r M_K N(\mathfrak{a}),$$

as we want. □

It is worth noting that the bound $\mathsf{H}(z) < r M_K \prod_{i=1}^{s} N(\mathfrak{p}_i)^{\ell_i}$ is indeed an effective search bound for $z \in \mathcal{O}$. That is, there are only finitely many elements in $\mathcal{O}$ whose height is bounded above by a fixed finite constant. This assertion is formalized in the following proposition.

Proposition 4.4. *Let K be a number field with ring of integers $\mathcal{O}$. Let m be a positive real number. Then the set $\{x \in \mathcal{O} : \mathsf{H}(x) < m\}$ is finite and can be determined effectively.*

This proposition is a special case of Northcott's Theorem (see, e.g., [Zan09, Thm. 3.7]), which asserts that the set of algebraic numbers of bounded degree and bounded logarithmic Weil height is finite. In our case, since the elements of $\mathcal{O}$ are algebraic integers of fixed degree, it suffices to note that for any $x \in \mathcal{O}$, the logarithmic Weil height $h(x)$ satisfies

$$h(x) \leq \log \mathsf{H}(x),$$

where $\mathsf{H}(x)$ is the Archimedean height defined above. Therefore, the finiteness of the set $\{x \in \mathcal{O} : \mathsf{H}(x) < m\}$ follows immediately from Northcott's Theorem. For the effectiveness of Northcott's Theorem, see, for example, [Ser97, Chapter. 2, § 5].

5. Proof fo Theorem 1.1

To prove Theorem 1.1, we will first establish three preparatory lemmas. The proposition will then follow as a consequence.

Lemma 5.1. *Let $\lambda, d \in K_{\mathfrak{p}}$ be such that $|d|_{\mathfrak{p}} = 1/q^{e+1}$ and $|\lambda|_{\mathfrak{p}} \in \{1, q\}$. Define $A = \operatorname{diag}(1, \lambda)$, and let $a, c \in K_{\mathfrak{p}}$ satisfy $a^2 + \lambda c^2 = 1$. Consider the matrix*

$$S = \begin{pmatrix} a & -c\lambda \\ c & a \end{pmatrix} \in O_A^+(K_{\mathfrak{p}}).$$

Then:

(a) The element $1-\lambda d^2$ is a square element in $K_{\mathfrak{p}}$, and its square root $(1-\lambda d^2)^{1/2}$ is well-defined.

(b) Define vectors $\beta, \eta \in (K_{\mathfrak{p}})^2$ as

$$\beta = \begin{pmatrix} -1 + (1 - \lambda d^2)^{1/2} \\ d \end{pmatrix}, \quad \eta = \begin{pmatrix} -1 + a(1 - \lambda d^2)^{1/2} + \lambda cd \\ da - c(1 - \lambda d^2)^{1/2} \end{pmatrix}.$$

Then S can be written as the product of two reflections: $S = \sigma_\beta \sigma_\eta$.

Proof.

(a) Since $|d|_{\mathfrak{p}} = 1/q^{e+1}$ and $|\lambda|_{\mathfrak{p}} \leq q$, we have $|\lambda d^2|_{\mathfrak{p}} \leq 1/q^{2e+1}$, so $\lambda d^2 \in \mathfrak{p}^{2e+1}\mathcal{O}_{\mathfrak{p}}$. By Definition 2.2, the binomial series for $(1-\lambda d^2)^{1/2}$ converges in $K_{\mathfrak{p}}$, which confirms that $1-\lambda d^2$ is indeed a square in $K_{\mathfrak{p}}$.

(b) Using the general formula for reflections from Definition 3.2, the reflection matrices are computed as:

$$\sigma_\beta = \begin{pmatrix} (1-\lambda d^2)^{1/2} & d\lambda \\ d & -(1-\lambda d^2)^{1/2} \end{pmatrix}, \quad \sigma_\eta = \begin{pmatrix} a(1-\lambda d^2)^{1/2} + \lambda cd & \lambda da - \lambda c(1-\lambda d^2)^{1/2} \\ da - c(1-\lambda d^2)^{1/2} & -a(1-\lambda d^2)^{1/2} + \lambda cd \end{pmatrix}.$$

A direct matrix multiplication verifies $S = \sigma_\beta \sigma_\eta$.

□

Lemma 5.2. *Let $\lambda \in K_{\mathfrak{p}}$ satisfy $|\lambda|_{\mathfrak{p}} = q$, and let $a, c \in K_{\mathfrak{p}}$ be such that $a^2 + \lambda c^2 = 1$. Define the matrix*

$$S = \begin{pmatrix} a & -c\lambda \\ c & a \end{pmatrix}.$$

Then for any $d \in K_{\mathfrak{p}}$, any $\xi \in \{k\eta : k \in K_{\mathfrak{p}}, \|k\eta\|_{\mathfrak{p}} = 1\}$, where $\eta \in (K_{\mathfrak{p}})^2$ was defined in Lemma 5.1 (b), and any $\gamma \in (K_{\mathfrak{p}})^2$ with $\|\xi - \gamma\|_{\mathfrak{p}} < 1$, we have

$$\|\sigma_\xi - \sigma_\gamma\|_{\mathfrak{p}} \leq \left|\frac{1}{8}\right|_{\mathfrak{p}} \|S\|_{\mathfrak{p}}^4 q^{4e+4} \|\xi - \gamma\|_{\mathfrak{p}}.$$

Proof. For the sake of clarity, we write $\xi = (\xi_1, \xi_2)^t = k(\eta_1, \eta_2)^t$ and $\gamma = (\gamma_1, \gamma_2)^t$. For any matrix M denote by $M(i,j)$ its (i,j)-entry. The condition $\|\xi - \gamma\|_{\mathfrak{p}} < 1$ gives us $\|\gamma\|_{\mathfrak{p}} = \|\xi\|_{\mathfrak{p}} = 1$, because

$$1 = \|\xi\|_{\mathfrak{p}} = \|\gamma + (\xi - \gamma)\|_{\mathfrak{p}} \leq \max\{\|\gamma\|_{\mathfrak{p}}, \|\xi - \gamma\|_{\mathfrak{p}}\}$$

implies $\|\gamma\|_{\mathfrak{p}} \geq 1$, and

$$\|\gamma\|_{\mathfrak{p}} = \|\xi + (\gamma - \xi)\|_{\mathfrak{p}} \leq \max\{\|\xi\|_{\mathfrak{p}}, \|\gamma - \xi\|_{\mathfrak{p}}\} = 1$$

implies $\|\gamma\|_{\mathfrak{p}} \leq 1$.

Since we equip the matrices with sup-norm, we estimate $\|\sigma_\xi - \sigma_\gamma\|_{\mathfrak{p}}$ by computing each entry's $\mathfrak{p}$-absolute value. Using the general formula for reflections in Definition 3.2, we have

$$\sigma_\xi(1,1) - \sigma_\gamma(1,1) = \frac{2\lambda(\xi_2\gamma_1 + \xi_1\gamma_2)(\xi_2\gamma_1 - \xi_1\gamma_2)}{(\xi_1^2 + \lambda\xi_2^2)(\gamma_1^2 + \lambda\gamma_2^2)}.$$

Because $\|\xi\|_\mathfrak{p} = \|\gamma\|_\mathfrak{p} = 1$, the numerator satisfies $|\xi_2\gamma_1+\xi_1\gamma_2|_\mathfrak{p} \leq \max\{|\xi_2\gamma_1|_\mathfrak{p}, |\xi_1\gamma_2|_\mathfrak{p}\} \leq 1$, and $|\xi_2\gamma_1-\xi_1\gamma_2|_\mathfrak{p} = |\xi_2(\gamma_1-\xi_1)+\xi_1(\xi_2-\gamma_2)|_\mathfrak{p} \leq \max\{|\xi_2|_\mathfrak{p}, |\xi_1|_\mathfrak{p}\}\|\xi-\gamma\|_\mathfrak{p} \leq \|\xi-\gamma\|_\mathfrak{p}$. Hence we know

$$|\sigma_\xi(1,1) - \sigma_\gamma(1,1)|_\mathfrak{p} \leq \frac{|2\lambda|_\mathfrak{p}\|\xi-\gamma\|_\mathfrak{p}}{|\xi_1^2+\lambda\xi_2^2|_\mathfrak{p}|\gamma_1^2+\lambda\gamma_2^2|_\mathfrak{p}},$$

To bound this expression, we seek a lower bound for the denominator. Because $|\lambda|_\mathfrak{p} = q$, we know $v_\mathfrak{p}(\xi_1^2)$ and $v_\mathfrak{p}(\lambda\xi_2^2)$ differ in parity. Thus $|\xi_1^2|_\mathfrak{p} \neq |\lambda\xi_2^2|_\mathfrak{p}$, implying $|\xi_1^2+\lambda\xi_2^2|_\mathfrak{p} = \max\{|\xi_1^2|_\mathfrak{p}, |\lambda\xi_2^2|_\mathfrak{p}\} \geq 1$. Similar argument shows $|\gamma_1^2+\lambda\gamma_2^2|_\mathfrak{p} \geq 1$. Therefore, we obtain $|\sigma_\xi(1,1) - \sigma_\gamma(1,1)|_\mathfrak{p} \leq q|2|_\mathfrak{p}\|\xi-\gamma\|_\mathfrak{p}$.

We have identical bound for the $(2,1)$-entry:

$$|\sigma_\xi(2,1) - \sigma_\gamma(2,1)|_\mathfrak{p} = \left|\frac{2(\gamma_2\xi_1-\gamma_1\xi_2)(\xi_1\gamma_1-\lambda\xi_2\gamma_2)}{(\xi_1^2+\lambda\xi_2^2)(\gamma_1^2+\lambda\gamma_2^2)}\right|_\mathfrak{p} \leq q|2|_\mathfrak{p}\|\xi-\gamma\|_\mathfrak{p}.$$

Moreover, from the general formula of reflection in Definition 3.2, we observe $\sigma_\xi(1,2)-\sigma_\gamma(1,2) = \lambda(\sigma_\xi(2,1) - \sigma_\gamma(2,1))$ and $\sigma_\xi(2,2) - \sigma_\gamma(2,2) = -(\sigma_\xi(1,1) - \sigma_\gamma(1,1))$. So we finally conclude

$$\|\sigma_\xi - \sigma_\gamma\|_\mathfrak{p} = |\sigma_\xi(1,2) - \sigma_\gamma(1,2)|_\mathfrak{p} \leq q^2|2|_\mathfrak{p}\|\xi-\gamma\|_\mathfrak{p}.$$

□

Lemma 5.3. *Let $\lambda \in K_\mathfrak{p}$ satisfy $|\lambda|_\mathfrak{p} = 1$. Let $a, c \in K_\mathfrak{p}$ and $S \in \mathrm{GL}_2(K_\mathfrak{p})$ be as in Lemma 5.2. Then there exists $d \in K_\mathfrak{p}$ with $|d|_\mathfrak{p} = 1/q^{e+1}$, such that for any $\xi \in \{k\eta : k \in K_\mathfrak{p}, \|k\eta\|_\mathfrak{p} = 1\}$ where $\eta \in (K_\mathfrak{p})^2$ was defined in Lemma 5.1 (b), and any $\gamma \in (K_\mathfrak{p})^2$ with $\|\xi-\gamma\|_\mathfrak{p} < |4|_\mathfrak{p}q^{-2e-2}\|S\|_\mathfrak{p}^{-2}$, we have*

$$\|\sigma_\xi - \sigma_\gamma\|_\mathfrak{p} \leq \left|\frac{1}{8}\right|_\mathfrak{p}\|S\|_\mathfrak{p}^4 q^{4e+4}\|\xi-\gamma\|_\mathfrak{p}.$$

Proof. By lemma 2.4, $\det(S) = 1$ implies $\|S\|_\mathfrak{p} \geq 1$. Thus the norm of $\xi-\gamma$ can be bounded by

$$\|\xi-\gamma\|_\mathfrak{p} < |4|_\mathfrak{p}q^{-2e-2}\|S\|_\mathfrak{p}^{-2} < 1.$$

By similar argument in Lemma 5.2, we still have $\|\gamma\|_\mathfrak{p} = \|\xi\|_\mathfrak{p} = 1$.

Continuing the notation from the proof of Lemma 5.2, we write $\xi = (\xi_1, \xi_2)^t = k(\eta_1, \eta_2)^t$ and $\gamma = (\gamma_1, \gamma_2)^t$. We also let $M(i,j)$ denote the (i,j)-entry of the matrix M. As before, we bound the sup-norm of $\sigma_\xi - \sigma_\gamma$ by formulating upper bounds for

each entry one by one. Using the general formula for reflections in Definition 3.2, we have

$$|\sigma_\xi(1,1)-\sigma_\gamma(1,1)|_\mathfrak{p}=\left|\frac{2\lambda(\xi_2\gamma_1+\xi_1\gamma_2)(\xi_2\gamma_1-\xi_1\gamma_2)}{(\xi_1^2+\lambda\xi_2^2)(\gamma_1^2+\lambda\gamma_2^2)}\right|_\mathfrak{p}\leq\frac{|2\lambda|_\mathfrak{p}\|\xi-\gamma\|_\mathfrak{p}}{|\xi_1^2+\lambda\xi_2^2|_\mathfrak{p}|\gamma_1^2+\lambda\gamma_2^2|_\mathfrak{p}}.$$

Thus, we seek a lower bound for the denominator. Using formula of η in Lemma 5.1 and the fact $\xi=k\eta$, a direct computation shows $\xi_1^2+\lambda\xi_2^2=-2k\xi_1=-2k^2\eta_1$. So we will bound $|\xi_1^2+\lambda\xi_2^2|_\mathfrak{p}$ by obtaining lower bounds for $|k|_\mathfrak{p}$ and $|\eta_1|_\mathfrak{p}$ separately.

To bound $|k|_\mathfrak{p}$, we first claim that $\|\eta\|_\mathfrak{p}\leq\|S\|_\mathfrak{p}$. This follows by showing that each of the five terms appearing in η_1 and η_2 has $\mathfrak{p}$-adic absolute value no greater than some entry of S. The term $|-1|_\mathfrak{p}\leq\|S\|_\mathfrak{p}$ because

$$1=|a^2+\lambda c^2|_\mathfrak{p}\leq\max\{|a^2|_\mathfrak{p},|\lambda c^2|_\mathfrak{p}\},$$

implying that either $|a|_\mathfrak{p}\geq 1$ or $|\lambda c|_\mathfrak{p}\geq 1$. The term $|a(1-\lambda d^2)^{1/2}|_\mathfrak{p}=|a|_\mathfrak{p}$, because $|d|_\mathfrak{p}=1/q^{e+1}$ implies $|(1-\lambda d^2)^{1/2}|_\mathfrak{p}=1$. The term $|\lambda cd|_\mathfrak{p}$ is less than $|-c\lambda|_\mathfrak{p}$, $|da|_\mathfrak{p}$ less than $|a|_\mathfrak{p}$, and $|c(1-\lambda d^2)^{1/2}|_\mathfrak{p}$ no greater than $|c|_\mathfrak{p}$. So indeed we have $\|\eta\|_\mathfrak{p}\leq\|S\|_\mathfrak{p}$. Together with our assumption $\|k\eta\|_\mathfrak{p}=1$, we deduce $\|kS\|_\mathfrak{p}\geq 1$, so the bound of $|k|_\mathfrak{p}$ is

$$|k|_\mathfrak{p}\geq\frac{1}{\|S\|_\mathfrak{p}}.$$

Now the main task falls on analyzing $|\eta_1|_\mathfrak{p}$. Write $|c|_\mathfrak{p}=q^m$ for $m\in\mathbb{Z}$. As long as $m\neq -e-1$, d can be any element with absolute value $|d|_\mathfrak{p}=1/q^{e+1}$. Therefore we may fix a uniformizer π of $K_\mathfrak{p}$, and take $d=\pi^{e+1}$. In the case of $m=-e-1$, d will either be c or $-c$, and the sign will be chosen later. We now determine the values of $|\eta_1|_\mathfrak{p}$ by performing a case analysis on the possible values of m.

When $m>0$, then $|a|_\mathfrak{p}=q^m$ and $|(1-\lambda d^2)^{1/2}|_\mathfrak{p}=1$. Therefore,

$$|\eta_1|_\mathfrak{p}=|-1+a(1-\lambda d^2)^{1/2}+\lambda cd|_\mathfrak{p}=\max\{1,q^m,q^{m-e-1}\}=q^m.$$

When $m=-e-1$, we know $|\lambda c^2|_\mathfrak{p}=1/q^{2e+2}$ is small enough to define the binomial expansion for $(1-\lambda c^2)^{1/2}$ by the requirement of Definition 2.2. If $a=(1-\lambda c^2)^{1/2}$ we set $d=-c$, and $|\eta_1|_\mathfrak{p}=|-2\lambda d^2|_\mathfrak{p}=|2|_\mathfrak{p}q^{-2e-2}$; when $a=-(1-\lambda c^2)^{1/2}$ we set $d=c$, and $|\eta_1|_\mathfrak{p}=|-2+2\lambda d^2|_\mathfrak{p}=|2|_\mathfrak{p}$.

When $-e\leq m\leq 0$, the binomial expansion cannot be applied on a. However, if we set $g=-1+\lambda cd$ and $h=a(1-\lambda d^2)^{1/2}$, we immediately observe $(g+h)(g-h)=\lambda(c-d)^2\neq 0$. Since $|c|_\mathfrak{p}=q^m>q^{-e-1}=|d|_\mathfrak{p}$, we know $|c-d|_\mathfrak{p}=|c|_\mathfrak{p}=q^m$. Since

$|(1-\lambda d^2)^{1/2}|_{\mathfrak{p}} = 1$ and $|a|_{\mathfrak{p}} = \sqrt{\max\{|1|_{\mathfrak{p}}, |-\lambda c^2|_{\mathfrak{p}}\}} \leq 1$, $g-h$ can also be bounded by

$$|g-h|_{\mathfrak{p}} \leq \max\{|-1|_{\mathfrak{p}}, |\lambda cd|_{\mathfrak{p}}, |a(1-\lambda d^2)^{1/2}|_{\mathfrak{p}}\} = 1.$$

Thus we can estimate the norm of $\eta_1 = g+h$ by

$$|\eta_1|_{\mathfrak{p}} = |g+h|_{\mathfrak{p}} = \frac{|\lambda(c-d)^2|_{\mathfrak{p}}}{|g-h|_{\mathfrak{p}}} = \frac{q^{2m}}{|g-h|_{\mathfrak{p}}} \geq q^{2m}.$$

When $m < -e-1$, we use binomial expansion on both $(1-\lambda d^2)^{1/2}$ and $(1-\lambda c^2)^{1/2}$. In the binomial series, lower-order terms has strictly larger $\mathfrak{p}$-adic absolute values than the higher-order terms. Hence, by the ultrametric triangle inequality we can ignore all higher-order terms when evaluating $|\eta_1|_{\mathfrak{p}}$. If $a = (1-\lambda c^2)^{1/2}$, then we have

$$\begin{aligned} |-1+a(1-\lambda d^2)^{1/2}|_{\mathfrak{p}} &= \left| -1 + \sum_{n=0}^{\infty} \binom{1/2}{n} (-\lambda c^2)^n \sum_{n=0}^{\infty} \binom{1/2}{n} (-\lambda d^2)^n \right|_{\mathfrak{p}} \\ &= |-1/2\lambda d^2 - 1/2\lambda c^2|_{\mathfrak{p}} = |1/2\lambda d^2|_{\mathfrak{p}} = |1/2|_{\mathfrak{p}} q^{-2e-2}. \end{aligned}$$

If $a = -(1-\lambda c^2)^{1/2}$, then

$$|-1+a(1-\lambda d^2)^{1/2}|_{\mathfrak{p}} = |-2+1/2\lambda d^2 + 1/2\lambda c^2|_{\mathfrak{p}} = |2|_{\mathfrak{p}} \geq q^{-e}.$$

In either case we have

$$|-1+a(1-\lambda d^2)^{1/2}|_{\mathfrak{p}} \geq q^{-2e-2} > |\lambda cd|_{\mathfrak{p}}.$$

Hence we know

$$|\eta_1|_{\mathfrak{p}} = |-1+a(1-\lambda d^2)^{1/2} + \lambda cd|_{\mathfrak{p}} \geq \max\{|1/2|_{\mathfrak{p}} q^{-2e-2}, |\lambda cd|_{\mathfrak{p}}\} = |1/2|_{\mathfrak{p}} q^{-2e-2}.$$

To sum up, we have

$$|\eta_1|_{\mathfrak{p}} \geq \begin{cases} q^m & m > 0, \\ q^{2m} & -e \leq m \leq 0, \\ |2|_{\mathfrak{p}} q^{-2e-2} & m = -e-1, \\ |1/2|_{\mathfrak{p}} q^{-2e-2} & m < -e-1. \end{cases}$$

Therefore, we finally obtain

$$|\xi_1^2+\lambda\xi_2^2|_{\mathfrak{p}} = |-2k^2\eta_1|_{\mathfrak{p}} \geq \begin{cases} |2|_{\mathfrak{p}} q^m/\|S\|_{\mathfrak{p}}^2, & m>0, \\ |2|_{\mathfrak{p}} q^{2m}/\|S\|_{\mathfrak{p}}^2, & -e\leq m\leq 0, \\ |4|_{\mathfrak{p}} q^{-2e-2}/\|S\|_{\mathfrak{p}}^2, & m=-e-1, \\ q^{-2e-2}/\|S\|_{\mathfrak{p}}^2, & m<-e-1. \end{cases}$$

A uniform bound is therefore

$$|\xi_1^2+\lambda\xi_2^2|_{\mathfrak{p}} \geq \frac{|4|_{\mathfrak{p}} q^{-2e-2}}{\|S\|_{\mathfrak{p}}^2}.$$

To obtain a lower bound for $|\gamma_1^2+\lambda\gamma_2^2|_{\mathfrak{p}}$, we observe

$$\begin{aligned} |\gamma_1^2+\lambda\gamma_2^2|_{\mathfrak{p}} &= \Big|\Big(\xi_1+(\gamma_1-\xi_1)\Big)^2+\lambda\Big(\xi_2+(\gamma_2-\xi_2)\Big)^2\Big|_{\mathfrak{p}} \\ &= |(\xi_1^2+\lambda\xi_2^2)+(\gamma_1-\xi_1)^2+\lambda(\gamma_2-\xi_2)^2+2\xi_1(\gamma_1-\xi_1)+2\lambda\xi_2(\gamma_2-\xi_2)|_{\mathfrak{p}}. \end{aligned}$$

Because of $\|\xi-\gamma\|_{\mathfrak{p}} < |4|_{\mathfrak{p}} q^{-2e-2}\|S\|_{\mathfrak{p}}^{-2}$, all correction terms have norm strictly less than the leading term $\xi_1^2+\lambda\xi_2^2$. So

$$|\gamma_1^2+\lambda\gamma_2^2|_{\mathfrak{p}} = |\xi_1^2+\lambda\xi_2^2|_{\mathfrak{p}} \geq \frac{|4|_{\mathfrak{p}} q^{-2e-2}}{\|S\|_{\mathfrak{p}}^2}.$$

Therefore, we can finally estimate

$$|\sigma_\xi(1,1)-\sigma_\gamma(1,1)|_{\mathfrak{p}} = \left|\frac{2\lambda(\xi_2\gamma_1+\xi_1\gamma_2)(\xi_2\gamma_1-\xi_1\gamma_2)}{(\xi_1^2+\lambda\xi_2^2)(\gamma_1^2+\lambda\gamma_2^2)}\right|_{\mathfrak{p}} \leq \frac{\|\xi-\gamma\|_{\mathfrak{p}}}{|8|_{\mathfrak{p}}\|S\|_{\mathfrak{p}}^{-4} q^{-4e-4}},$$

and

$$|\sigma_\xi(2,1)-\sigma_\gamma(2,1)|_{\mathfrak{p}} = \left|\frac{2(\gamma_2\xi_1-\gamma_1\xi_2)(\xi_1\gamma_1-\lambda\xi_2\gamma_2)}{(\xi_1^2+\lambda\xi_2^2)(\gamma_1^2+\lambda\gamma_2^2)}\right|_{\mathfrak{p}} \leq \frac{\|\xi-\gamma\|_{\mathfrak{p}}}{|8|_{\mathfrak{p}}\|S\|_{\mathfrak{p}}^{-4} q^{-4e-4}}.$$

From the general formula of reflection in Definition 3.2, we observe $\sigma_\xi(1,2)-\sigma_\gamma(1,2) = \lambda(\sigma_\xi(2,1)-\sigma_\gamma(2,1))$ and $\sigma_\xi(2,2)-\sigma_\gamma(2,2) = -(\sigma_\xi(1,1)-\sigma_\gamma(1,1))$. So the $(1,2)$ and $(2,2)$-entry yields the same bound for $\|\sigma_\xi-\sigma_\gamma\|_{\mathfrak{p}}$, and we can finally conclude

$$\|\sigma_\xi-\sigma_\gamma\|_{\mathfrak{p}} \leq \left|\frac{1}{8}\right|_{\mathfrak{p}} \|S\|_{\mathfrak{p}}^4 q^{4e+4}\|\xi-\gamma\|_{\mathfrak{p}}.$$

□

With the preceding lemmas established, we are now in a position to complete the proof of one of our main results, Theorem 1.1.

Proof of Theorem 1.1. Let $|\lambda|_{\mathfrak{p}} \in \{1, q\}$, and $S \in O_A^+(K_{\mathfrak{p}})$ be arbitrary. By Proposition 3.3, S has the form described in Lemma 5.1. Applying Lemma 5.1, we may write $S = \sigma_\alpha \sigma_\xi$, where the vectors α and ξ has been normalized so that $\|\alpha\|_{\mathfrak{p}} = \|\xi\|_{\mathfrak{p}} = 1$.

Now, let $u, v \in (K_{\mathfrak{p}})^2$ satisfy $\|\alpha - u\|_{\mathfrak{p}} < |4|_{\mathfrak{p}} q^{-2e-2}$ and $\|\xi - v\|_{\mathfrak{p}} < |4|_{\mathfrak{p}} q^{-2e-2} \|S\|_{\mathfrak{p}}^{-2}$. The bound in the case $|\lambda|_{\mathfrak{p}} = q$, as given by Lemma 5.2, is weaker than the bound for $|\lambda|_{\mathfrak{p}} = 1$ provided by Lemma 5.3. Therefore, we consistently use the bound from Lemma 5.3 to ensure correctness. Specifically, Lemma 5.3 yields

$$\|\sigma_\xi - \sigma_v\|_{\mathfrak{p}} \leq \left|\frac{1}{8}\right|_{\mathfrak{p}} \|S\|_{\mathfrak{p}}^4 q^{4e+4} \|\xi - v\|_{\mathfrak{p}},$$

and by choosing $a = 1$ and $c = 0$, it also implies

$$\|\sigma_\alpha - \sigma_u\|_{\mathfrak{p}} \leq \left|\frac{1}{8}\right|_{\mathfrak{p}} q^{4e+4} \|\alpha - u\|_{\mathfrak{p}}.$$

Therefore,

$$\begin{aligned}
\|S - \sigma_u \sigma_v\|_{\mathfrak{p}} &= \|\sigma_\alpha(\sigma_\xi - \sigma_v) + (\sigma_\alpha - \sigma_u)\sigma_\xi - (\sigma_\alpha - \sigma_u)(\sigma_\xi - \sigma_v)\|_{\mathfrak{p}} \\
&\leq \max\left\{ \left|\frac{1}{8}\right|_{\mathfrak{p}} \|S\|_{\mathfrak{p}}^4 q^{4e+4} \|\sigma_\alpha\|_{\mathfrak{p}} \|\xi - v\|_{\mathfrak{p}}, \left|\frac{1}{8}\right|_{\mathfrak{p}} q^{4e+4} \|\sigma_\xi\|_{\mathfrak{p}} \|\alpha - u\|_{\mathfrak{p}}, \right. \\
&\qquad \left. \left|\frac{1}{64}\right|_{\mathfrak{p}} \|S\|_{\mathfrak{p}}^4 q^{8e+8} \|\alpha - u\|_{\mathfrak{p}} \|\xi - v\|_{\mathfrak{p}} \right\}.
\end{aligned}$$

Next, we know $\sigma_\beta = \sigma_\alpha$ because scalar multiplication does not change the expression of reflection matrix. Thus by the formula of σ_β in Part (b) of Lemma 5.1, we have

$$\|\sigma_\alpha\|_{\mathfrak{p}} = \max\{(1 - \lambda d^2)^{1/2}, d, d\lambda\} = \max\left\{1, \frac{1}{q^{e+1}}, \frac{1}{q^e}\right\} = 1.$$

Together with our assumption of $\|\alpha - u\|_{\mathfrak{p}} < |4|_{\mathfrak{p}} q^{-2e-2} < 1$ and the fact $|1/8|_{\mathfrak{p}} \leq q^{3e} < q^{4e+4}$, they imply that the third term in the maximum above is strictly smaller than the first:

$$\begin{aligned}
\left|\frac{1}{64}\right|_{\mathfrak{p}} \|S\|_{\mathfrak{p}}^4 q^{8e+8} \|\alpha - u\|_{\mathfrak{p}} \|\xi - v\|_{\mathfrak{p}} &< \left|\frac{1}{8}\right|_{\mathfrak{p}} \|S\|_{\mathfrak{p}}^4 q^{4e+4} \|\alpha - u\|_{\mathfrak{p}} \|\xi - v\|_{\mathfrak{p}} \\
&\leq \left|\frac{1}{8}\right|_{\mathfrak{p}} \|S\|_{\mathfrak{p}}^4 q^{4e+4} \|\sigma_\alpha\|_{\mathfrak{p}} \|\xi - v\|_{\mathfrak{p}}.
\end{aligned}$$

Finally, since reflection matrices are involutive ($\sigma_\alpha = \sigma_\alpha^{-1}$), Lemma 2.3implies

$$\|\sigma_\xi\|_\mathfrak{p} = \|\sigma_\alpha S\|_\mathfrak{p} \leq \|\sigma_\alpha\|_\mathfrak{p}\|S\|_\mathfrak{p} = \|S\|_\mathfrak{p}.$$

Combining all the bounds, we arrive at

$$\begin{aligned}\|S - \sigma_u\sigma_v\|_\mathfrak{p} &\leq \max\left\{\left|\frac{1}{8}\right|_\mathfrak{p}\|S\|_\mathfrak{p}^4 q^{4e+4}\|\sigma_\alpha\|_\mathfrak{p}\|\xi - v\|_\mathfrak{p}, \left|\frac{1}{8}\right|_\mathfrak{p} q^{4e+4}\|\sigma_\xi\|_\mathfrak{p}\|\alpha - u\|_\mathfrak{p}\right\} \\ &\leq \left|\frac{1}{8}\right|_\mathfrak{p}\|S\|_\mathfrak{p}^4 q^{4e+4}\max\{\|\alpha - u\|_\mathfrak{p}, \|\xi - v\|_\mathfrak{p}\}.\end{aligned}$$

□

6. Proof of Theorem 1.2

From Theorem 1.1, we can derive a effective weak approximation for elements of $O_A^+(K)$.

Proposition 6.1. *Let K be a number field of degree r. Let $B \in \mathrm{GL}_2(K)$ be any symmetric matrix. Let $\mathfrak{p}_1, ..., \mathfrak{p}_s$ be non-zero prime ideals of $\mathcal{O}$, with ramification index e_i and uniformizer $|\pi_i|_{\mathfrak{p}_i} = 1/q_i$. Pick $T_i \in O_B^+(K_{\mathfrak{p}_i})$ for $i \in \{1, 2, ..., s\}$.*

(a) There exists a matrix $P \in \mathrm{GL}_2(K)$ and scalar $k \in K$ such that $kP^tBP = A = \mathrm{diag}(1, \lambda)$, where $|\lambda|_{\mathfrak{p}_i} \in \{1, q_i\}$ for $i \in \{1, 2, ..., s\}$.

(b) For any real number $\epsilon < \min_{1\leq i\leq s}\{|4|_{\mathfrak{p}_i} q_i^{-2e_i-2}\|P^{-1}T_iP\|_{\mathfrak{p}_i}^{-2}\}$, there exists a proper B-automorph

$$T \in \left\{P\sigma_u\sigma_v P^{-1}\middle| 0 \leq \mathsf{H}(u), \mathsf{H}(v) < rM_K\prod_{i=1}^{s} N(\mathfrak{p}_i)^{\ell_i}\right\} \subseteq O_B^+(K),$$

where M_K and ℓ_i are constants defined in Lemma 4.3, such that

$$\|T - T_i\|_{\mathfrak{p}_i} < \frac{\|P\|_{\mathfrak{p}_i}^{10}}{|8\det(P)^5|_{\mathfrak{p}_i}}\|T_i\|_{\mathfrak{p}_i}^4 q_i^{4e_i+4}\epsilon$$

for all $i \in \{1, 2, ..., s\}$.

Proof.

(a) Since every nonsingular symmetric bilinear form over a field of characteristic $\neq 2$ is diagonalizable, we may assume that B is diagonal, and write $B = \mathrm{diag}(\mu_1, \mu_2)$. By the weak approximation theorem, for each $1 \leq i \leq s$ there exists $\theta_i \in K$ such that $|\theta_i - \pi_i|_{\mathfrak{p}_i} < 1/q_i$ and $|\theta_i - 1|_{\mathfrak{p}_j} < 1$ for all $j \neq i$.

Therefore, θ_i serves as a uniformizer for $\mathfrak{p}_i$ while taking trivial absolute value at all other primes $\mathfrak{p}_j$. Define

$$k = \mu_1^{-1}, \quad \kappa = \prod_{i=1}^{s} \theta_i^{-\lceil v_{\mathfrak{p}_i}(\mu_2)/2 \rceil}, \quad \text{and } P = \operatorname{diag}(1, \kappa).$$

Then these choices satisfy the required condition.

(b) For $i \in \{1, 2, ..., s\}$, we define $S_i = P^{-1} T_i P \in O_A^+(K_{\mathfrak{p}_i})$. Since all the S_i's are proper A-automorphs, we can apply Theorem 1.1 to decompose them as $S_i = \sigma_{\alpha_i}\sigma_{\xi_i}$, where $\|\alpha_i\|_{\mathfrak{p}_i} = \|\xi_i\|_{\mathfrak{p}_i} = 1$. By Lemma 4.3, we can find $u, v \in \mathcal{O}^2$ such that $\|\alpha_i - u\|_{\mathfrak{p}_i}, \|\xi_i - v\| + \mathfrak{p}_i < \epsilon$ and $0 \leq \mathsf{H}(u), \mathsf{H}(v) < rM_K \prod_{i=1}^{s} N(\mathfrak{p}_i)^{\ell_i}$. Apply Theorem 1.1 again, we obtain

$$\begin{aligned}
\|P\sigma_u\sigma_v P^{-1} - T_i\|_{\mathfrak{p}_i} &\leq \|P\|_{\mathfrak{p}_i}\|P^{-1}\|_{\mathfrak{p}_i}\|\sigma_u\sigma_v - S_i\|_{\mathfrak{p}_i} \\
&< \|P\|_{\mathfrak{p}_i}\|P^{-1}\|_{\mathfrak{p}_i}\left|\frac{1}{8}\right|_{\mathfrak{p}_i}\|P^{-1}T_iP\|_{\mathfrak{p}_i}^4 q_i^{4e_i+4}\epsilon \\
&\leq \|P\|_{\mathfrak{p}_i}^5\|P^{-1}\|_{\mathfrak{p}_i}^5\left|\frac{1}{8}\right|_{\mathfrak{p}_i}\|T_i\|_{\mathfrak{p}_i}^4 q_i^{4e_i+4}\epsilon \\
&\leq \frac{\|P\|_{\mathfrak{p}_i}^{10}}{|8\det(P)^5|_{\mathfrak{p}_i}}\|T_i\|_{\mathfrak{p}_i}^4 q_i^{4e_i+4}\epsilon.
\end{aligned}$$

Taking $T = P\sigma_u\sigma_v P^{-1}$, the proof is completed.

□

The preparatory result obtained above now allow us to establish our second main theorem, Theorem 1.2.

Proof of Therorem 1.2.

(a) Already proved in Part (a) of Proposition 6.1.

(b) Since A and B are equivalent over $\mathcal{O}_{\mathfrak{p}_i}$, there exists $\tau_i \in \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}_i})$ such that $A = \tau_i^t B \tau_i$ for $i \in \{1, 2, ..., s\}$. Although the τ_i's cannot be written explicitly, their norm must be $\|\tau_i\|_{\mathfrak{p}_i} = 1$, as they are invertible, and all of their entries are in the valuation ring $\mathcal{O}_{\mathfrak{p}_i}$. We also know $\tau_0^{-1}\tau_i \in O_A(K_{\mathfrak{p}_i})$. Write them as T_i. If any T_i is not proper, then by [O'M63, 91:4], we can redefine $T_i = T_i R_i$ for some $R_i \in O_A(K_{\mathfrak{p}_i}) \backslash O_A^+(K_{\mathfrak{p}_i})$ with $\|R_i\|_{\mathfrak{p}_i} = 1$. Hence, we may assume $T_i \in O_A^+(K_{\mathfrak{p}_i})$ for both $i \in \{1, 2, ..., s\}$.

By Lemma 2.3, the norm of T_i can be bounded above by

$$\|T_i\|_{\mathfrak{p}_i} = \|\tau_0^{-1}\tau_i\|_{\mathfrak{p}_i} \leq \|\tau_0^{-1}\|_{\mathfrak{p}_i}\|\tau_i\|_{\mathfrak{p}_i} = \|\tau_0^{-1}\|_{\mathfrak{p}_i}.$$

By Proposition 6.1, there exists a matrix $T = P\sigma_u\sigma_v P^{-1} \in O_Q^+(K)$ such that for $i \in \{1, 2, ..., s\}$,

$$\begin{aligned}\|P\sigma_u\sigma_v P^{-1} - T_i\|_{\mathfrak{p}_i} &\leq \frac{\|P\|_{\mathfrak{p}_i}^{10}}{|8\det(P)^5|_{\mathfrak{p}_i}}\|T_i\|_{\mathfrak{p}_i}^4 q_i^{4e_i+4}\epsilon \\ &\leq \frac{\|\tau_0^{-1}\|_{\mathfrak{p}_i}^4\|P\|_{\mathfrak{p}_i}^{10}q_i^{4e_i+4}}{|8\det(P)^5|_{\mathfrak{p}_i}} \cdot \epsilon < \frac{1}{\|\tau_0\|_{\mathfrak{p}_i}}.\end{aligned}$$

This implies $\|\tau_0 P\sigma_u\sigma_v P^{-1} - \tau_0 T_i\|_{\mathfrak{p}_i} < 1$, where $\tau_0 T_i = \tau_i \in \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}_i})$ by definition. Therefore, by Lemma 2.5, we conclude that $\tau_0 P\sigma_u\sigma_v P^{-1} \in \mathrm{GL}_2(K) \cap \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}_i})$ for $i \in \{1, 2, ..., s\}$, as desired.

□

References

[AGARA06] G. Aragón-González, J. L. Aragón, and M. A. Rodríguez-Andrade, *The decomposition of an orthogonal transformation as a product of reflections*, J. Math. Phys. **47** (2006), no. 1, 013509, 10. MR 2201806

[CGL21] W. K. Chan, H. Gao, and H. Li, *Explicit result on equivalence of rational quadratic forms avoiding primes*, J. Number Theory **225** (2021), 281–293. MR 4235262

[CS99] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, third ed., Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999. MR 1662447

[Fuk07] L. Fukshansky, *On effective Witt decomposition and the Cartan-Dieudonné theorem*, Canad. J. Math. **59** (2007), no. 6, 1284–1300. MR 2363067

[Ful11] C. Fuller, *A constructive proof of the Cartan-Dieudonné-Scherk theorem in the real or complex case*, J. Pure Appl. Algebra **215** (2011), no. 5, 1116–1126. MR 2747244

[Neu99] J. Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999. MR 1697859

[O'M63] O. T. O'Meara, *Introduction to quadratic forms*, Die Grundlehren der mathematischen Wissenschaften, vol. Band 117, Springer-Verlag, Berlin-Göttingen-Heidelberg; Academic Press, Inc., Publishers, New York, 1963. MR 152507

[Ser97] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. MR 1757192

[Sie41] C. L. Siegel, *Equivalence of quadratic forms*, Amer. J. Math. **63** (1941), 658–680. MR 5506

[Uhl01] F. Uhlig, *Constructive ways for generating (generalized) real orthogonal matrices as products of (generalized) symmetries*, Proceedings of the Eighth Conference of the International Linear Algebra Society (Barcelona, 1999), vol. 332/334, 2001, pp. 459–467. MR 1839445

[Zan09] U. Zannier, *Lecture notes on Diophantine analysis*, Appunti. Scuola Normale Superiore di Pisa (Nuova Serie), vol. 8, Edizioni della Normale, Pisa, 2009. MR 2517762

Department of Mathematics and Computer Science, Wesleyan University
Email address: zfan@wesleyan.edu

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