ON EFFECTIVE WITT DECOMPOSITION AND CARTAN-DIEUDONNÉ THEOREM

LENNY FUKSHANSKY

Abstract. Let K be a number field, and let F be a symmetric bilinear form in $2N$ variables over K. Let Z be a subspace of K^N. A classical theorem of Witt states that the bilinear space (Z,F) can be decomposed into an orthogonal sum of hyperbolic planes, singular, and anisotropic components. We prove the existence of such a decomposition of small height, where all bounds on height are explicit in terms of heights of F and Z. We also prove a special version of Siegel's Lemma for a bilinear space, which provides a small-height orthogonal decomposition into one-dimensional subspaces. Finally, we prove an effective version of Cartan-Dieudonné theorem. Namely, we show that every isometry σ of a regular bilinear space (Z,F) can be represented as a product of reflections of bounded heights with an explicit bound on heights in terms of heights of F, Z, and σ.

1. Introduction and notation

Let K be a number field, $N > 1$ an integer. Let

$$F(\boldsymbol{X},\boldsymbol{Y}) = \sum_{i=1}^{N}\sum_{j=1}^{N} f_{ij} X_i Y_j,$$

be a symmetric bilinear form in $2N$ variables with coefficients $f_{ij} = f_{ji}$ in K. We will write $F(\boldsymbol{X}) = F(\boldsymbol{X},\boldsymbol{X})$ for the associated quadratic form in N variables, and will also use F to denote the symmetric $N\times N$ matrix $(f_{ij})_{1\leq i,j\leq N}$. Let $Z \subseteq K^N$ be an L-dimensional subspace, $2 \leq L \leq N$, then F is also defined on Z, and we write (Z,F) for the bilinear space. Let M be the Witt index of (Z,F). With this basic notation we can recall the classical Witt decomposition theorem. We give a brief overview of required definitions and basic results on bilinear spaces in section 3.

Theorem 1.1. *Suppose that (Z,F) is a bilinear space as above. Then there exists an orthogonal decomposition of (Z,F) of the form*

$$Z = Z^{\perp} \perp \mathbb{H}_1 \perp \ \dots\ \perp \mathbb{H}_M \perp V, \tag{1}$$

where $Z^{\perp} = \{\boldsymbol{x} \in Z : F(\boldsymbol{x},\boldsymbol{z}) = 0\ \forall\ \boldsymbol{z} \in Z\}$ is the singular component, $\mathbb{H}_i$ are hyperbolic planes, and V is anisotropic component, which is uniquely determined up to isometry.

Theorem 1.1 can easily be obtained by combining Theorem 3.8 on p. 9 with Corollary 5.11 on p.17 of [10]. The first objective of this paper is to make this theorem effective, namely to prove that there exists a decomposition like (1) with hyperbolic planes, singular, and anisotropic components having relatively small

1991 *Mathematics Subject Classification.* Primary 11E12, 15A63; Secondary 11G50.
Key words and phrases. quadratic forms, heights.

height for an appropriately defined notion of height. By Northcott's theorem, there are only finitely many subspaces of fixed dimension over K whose height is bounded above by a given constant. Hence our result produces a "search bound" on components of Witt decomposition for a bilinear space (see [7] for a discussion of search bounds). This result is also related to the vast collection of results on small-height zeros of quadratic forms. The subject originates in a classical paper of Cassels, [2], where he proved that an isotropic rational quadratic form has a zero of relatively small height, producing an explicit bound on height in terms of the height of the quadratic form. Cassels' theorem has been extended and generalized in a number of different ways (see [13], [7] and [3] for more information on this). Our first main result can also be viewed in the context of those results; we will discuss this approach in more details in section 3.

Another direction we pursue here is investigation of the effective structure of the isometry group of a regular symmetric bilinear space (Z, F) over K. In [7] Masser proposes a version of the following question. Let F and G be two symmetric bilinear forms on K^N such that there exists $A \in GL_N(K)$ with $F(A\boldsymbol{X}, A\boldsymbol{Y}) = G(\boldsymbol{X}, \boldsymbol{Y})$. Can we prove that there exists such an A of bounded height, where the bound would be in terms of heights of F and G? In our context $F = G$, and so we can ask for an element of bounded height in the isometry group of the space (Z, F). This question is quite easy to answer (see Corollary 5.3 below), however one can consider the following generalization. Let $\mathcal{O}(Z, F)$ be the group of isometries of (Z, F). We recall a classical theorem of Cartan and Dieudonné (see Theorem 5.4 on p. 15 of [10] or Theorem 43:3 on p.102 of [8]). We review the required definitions in section 5.

Theorem 1.2. *Let (Z, F) be a regular symmetric bilinear space over K with $Z \subseteq K^N$ of dimension L, $1 \leq L \leq N$. Let $\sigma \in \mathcal{O}(Z, F)$. Then σ can be represented as a product of at most L reflections.*

The identity element of $\mathcal{O}(Z, F)$ is thought of here as the product of zero reflections. We will be interested in proving a slightly weaker effective version of this theorem, namely given a $\sigma \in \mathcal{O}(Z, F)$ we will prove that it can be represented as a product of at most $2L-1$ reflections of bounded height, where the bound on height is in terms of heights of F, Z, and σ.

We start with some notation. We write d for degree of K over $\mathbb{Q}$, O_K for its ring of integers, $\mathcal{D}_K$ for its discriminant, and $M(K)$ for its set of places. For each place $v \in M(K)$ we write K_v for the completion of K at v and let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree of K at v, so that for each $u \in M(\mathbb{Q})$

$$\sum_{v \in M(K), v|u} d_v = d. \tag{2}$$

For each place $v \in M(K)$ we define the absolute value $\| \ \|_v$ to be the unique absolute value on K_v that extends either the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$ if $v|\infty$, or the usual p-adic absolute value on $\mathbb{Q}_p$ if $v|p$, where p is a prime. We also define the second absolute value $| \ |_v$ for each place v by $|a|_v = \|a\|_v^{d_v/d}$ for all $a \in K$. Then for each non-zero $a \in K$ the *product formula* reads

$$\prod_{v \in M(K)} |a|_v = 1. \tag{3}$$

For each finite place $v \in M(K)$, $v \nmid \infty$, we define the *local ring of v-adic integers* $O_v = \{x \in K : |x|_v \leq 1\}$, whose unique maximal ideal is $P_v = \{x \in K : |x|_v < 1\}$. Then $O_K = \bigcap_{v \nmid \infty} O_v$. For each $v|\infty$ and each positive integer j, define as in [13]

$$r_v(j) = \begin{cases} \pi^{-1/2}\Gamma(j/2+1)^{1/j} & \text{if } v|\infty \text{ is real} \\ (2\pi)^{-1/2}\Gamma(j+1)^{1/2j} & \text{if } v|\infty \text{ is complex} \end{cases}$$

It will be useful to define a field constant

$$C_K(j) = 2|\mathcal{D}_K|^{1/2d} \prod_{v|\infty} r_v(j)^{d_v/d}, \tag{4}$$

We extend absolute values to vectors by defining the local heights. For each $v \in M(K)$ define a local height H_v on K_v^N by

$$H_v(\boldsymbol{x}) = \begin{cases} \max_{1\leq i\leq N} |x_i|_v & \text{if } v \nmid \infty \\ \left(\sum_{i=1}^N \|x_i\|_v^2\right)^{d_v/2d} & \text{if } v|\infty \end{cases}$$

for each $\boldsymbol{x} \in K_v^N$. We define the following global height function on K^N:

$$H(\boldsymbol{x}) = \prod_{v\in M(K)} H_v(\boldsymbol{x}), \tag{5}$$

for each $\boldsymbol{x} \in K^N$. We also define an *inhomogeneous* height function on vectors by

$$h(\boldsymbol{x}) = H(1, \boldsymbol{x}). \tag{6}$$

A basic property of heights that we will use states that for $m_1, ..., m_L \in \mathbb{Z}$ and $\boldsymbol{x}_1, ..., \boldsymbol{x}_L \in K^N$,

$$h\left(\sum_{i=1}^L m_i \boldsymbol{x}_i\right) \leq \left(\sum_{i=1}^L m_i^2\right)^{1/2} \prod_{i=1}^L h(\boldsymbol{x}_i). \tag{7}$$

We extend height to polynomials by viewing it as height function of the coefficient vector of a given polynomial. Hence for our quadratic form F, $H(F)$ is the height of the matrix $(f_{ij})_{1\leq i,j\leq N}$ viewed as a vector in K^{N^2}. In general, for an $M \times N$ matrix A we define $H(A)$ by viewing A as a vector in K^{MN}, same way as we defined height of F. This way we also have height defined on elements of the isometry group $\mathcal{O}(K^N, F)$, since they can be represented by $N \times N$ matrices, and each such matrix can be viewed as a vector in K^{N^2}. For each element σ of the isometry group $\mathcal{O}(Z, F)$ of a regular bilinear space we will select an extension $\hat{\sigma} \in \mathcal{O}(K^N, F)$ of minimal possible height, and will define $H(\sigma)$ to be $H(\hat{\sigma})$. We will explain how this is done in more details in section 5.

We also define another height on matrices, which is the same as height function on subspaces of K^N. Let $V \subseteq K^N$ be a subspace of dimension J, $1 \leq J \leq N$. Choose a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_J$ for V, and write $X = (\boldsymbol{x}_1 \ ... \ \boldsymbol{x}_J)$ for the corresponding $N \times J$ basis matrix. Then

$$V = \{X\boldsymbol{t} : \boldsymbol{t} \in K^J\}.$$

On the other hand, there exists an $(N-J) \times N$ matrix A with entries in K such that

$$V = \{\boldsymbol{x} \in K^N : A\boldsymbol{x} = 0\}.$$

Let $\mathcal{I}$ be the collection of all subsets I of $\{1, ..., N\}$ of cardinality J. For each $I \in \mathcal{I}$ let I' be its complement, i.e. $I' = \{1, ..., N\} \setminus I$, and let $\mathcal{I}' = \{I' : I \in \mathcal{I}\}$. Then

$$|\mathcal{I}| = \binom{N}{J} = \binom{N}{N-J} = |\mathcal{I}'|.$$

For each $I \in \mathcal{I}$, write X_I for the $J \times J$ submatrix of X consisting of all those rows of X which are indexed by I, and ${}_{I'}A$ for the $(N-J) \times (N-J)$ submatrix of A consisting of all those columns of A which are indexed by I'. By the duality principle of Brill-Gordan [4] (also see Theorem 1 on p. 294 of [5]), there exists a non-zero constant $\gamma \in K$ such that

$$\det(X_I) = (-1)^{\varepsilon(I)} \gamma \det({}_{I'}A), \tag{8}$$

where $\varepsilon(I) = \sum_{i \in I} i$. Define the vectors of *Grassmann coordinates* of X and A respectively to be

$$Gr(X) = (\det(X_I))_{I \in \mathcal{I}} \in K^{|I|},\ \ Gr(A) = (\det({}_{I'}A))_{I' \in \mathcal{I}'} \in K^{|I'|}.$$

Define

$$\mathcal{H}(X) = H(Gr(X)),\ \ \mathcal{H}(A) = H(Gr(A)),$$

and so by (8) and (3)

$$\mathcal{H}(X) = \mathcal{H}(A).$$

Define height of V denoted by $H(V)$ to be this common value. Hence the height of a matrix is the height of its row (or column) space, which is equal to the height of its nullspace. Also notice that $Gr(X)$ can be identified with $\boldsymbol{x}_1 \wedge\ ...\ \wedge \boldsymbol{x}_J$, where $\wedge$ stands for the wedge product, viewed under the cannonical lexicographic embedding into $K^{\binom{N}{J}}$. Therefore we can also write

$$H(V) = H(\boldsymbol{x}_1 \wedge\ ...\ \wedge \boldsymbol{x}_J).$$

This definition is legitimate, since it does not depend on the choice of the basis for V: let $\boldsymbol{y}_1, ..., \boldsymbol{y}_J$ be another basis for V over K, then there exists $C \in GL_N(K)$ such that $\boldsymbol{y}_i = C\boldsymbol{x}_i$ for each $1 \leq i \leq J$, and so

$$\begin{aligned} H(\boldsymbol{y}_1 \wedge\ ...\ \wedge \boldsymbol{y}_J) &= H(C\boldsymbol{x}_1 \wedge\ ...\ \wedge C\boldsymbol{x}_J) \\ &= \left(\prod_{v \in M(K)} |\det(C)|_v \right) H(\boldsymbol{x}_1 \wedge\ ...\ \wedge \boldsymbol{x}_J) \\ &= H(\boldsymbol{x}_1 \wedge\ ...\ \wedge \boldsymbol{x}_J), \end{aligned}$$

by the product formula. We are now ready to state our main results. First is an effective version of Witt's decomposition Theorem 1.1.

Theorem 1.3. *Let F be a symmetric bilinear form on K^N. Let $Z \subseteq K^N$ be a subspace of dimension L, $2 \leq L \leq N$, and Witt index $M \geq 1$. Let F have rank r on Z, $1 \leq r \leq L$. There exists an orthogonal decomposition of the bilinear space (Z, F) of the form (1) with*

$$H(Z^{\perp}) \leq C_K(r)^r H(F)^{r/2} H(Z), \tag{9}$$

and

$$\max\{H(\mathbb{H}_i), H(V)\} \leq \mathcal{A}_K(N, L, M) \left\{ H(F)^{\frac{L+2M}{4}} H(Z) \right\}^{\frac{(M+1)(M+2)}{2}}, \tag{10}$$

for each $1 \leq i \leq M$*, where*

$$\mathcal{A}_K(N,L,M) = \left\{ \left(2^{2M+1} C_K(L)^2\right)^L \left(N|\mathcal{D}_K|^{1/d}\right)^{M+5L} \right\}^{\frac{M(M+3)}{8}}. \tag{11}$$

Next is an effective version of Cartan-Dieudonné Theorem 1.2.

Theorem 1.4. *Let* (Z,F) *be a regular symmetric bilinear space over* K *with* $Z \subseteq K^N$ *of dimension* L*,* $1 \leq L \leq N$*,* $N \geq 2$*. Let* $\sigma \in \mathcal{O}(Z,F)$*. Then either* σ *is the identity, or there exist an integer* $1 \leq l \leq 2L-1$ *and reflections* $\tau_1,...,\tau_l \in \mathcal{O}(Z,F)$ *such that*

$$\sigma = \tau_1 \circ \cdots \circ \tau_l, \tag{12}$$

and for each $1 \leq i \leq l$*,*

$$H(\tau_i) \leq \left\{ \left(2N^2 |\mathcal{D}_K|^{\frac{1}{2d}}\right)^{\frac{L^2}{2}} H(F)^{\frac{L}{3}} H(Z)^{\frac{L}{2}} H(\sigma) \right\}^{5^{L-1}}. \tag{13}$$

This paper is structured as follows. In section 2 we discuss a related problem of producing an orthogonal basis of small height for a bilinear space. This can actually be viewed as a version of Siegel's Lemma for a bilinear space, and provides a decomposition of a bilinear space into an orthogonal sum of one-dimensional subspaces of small height - a result of independent interest. In section 3 we recall some basic lemmas on the properties of bilinear spaces, review a result of Vaaler on a maximal totally isotropic subspace of a bilinear space of small height, and prove an effective decomposition lemma for a bilinear space into a singular and regular components of small height. In section 4 we prove Theorem 1.3. In section 5 we develop some notation and preliminary lemmas on the effective structure of the isometry group. In particular, we prove two simple lemmas of independent interest: one on the existence of a small-height isometry of a bilinear space, and the other on the bound for the height of the invariant subspace of an isometry. We use these lemmas in section 6 to prove Theorem 1.4.

2. Siegel's Lemma for a bilinear space

In this section we prove a certain analogue of Siegel's Lemma for a bilinear space. First we recall the Bombieri-Vaaler formulation of a general Siegel's Lemma.

Theorem 2.1 ([1]). *Let* U *be a* J*-dimensional subspace of* K^N*,* $J < N$*. Then there exists a basis* $\boldsymbol{x}_1,...,\boldsymbol{x}_J \in K^N$ *for* U *such that*

$$\prod_{i=1}^J H(\boldsymbol{x}_i) \leq \prod_{i=1}^J h(\boldsymbol{x}_i) \leq \left\{ N|\mathcal{D}_K|^{1/d} \right\}^{J/2} H(U). \tag{14}$$

We will also need the following simple technical lemmas.

Lemma 2.2. *Let* U_1 *and* U_2 *be subspaces of* K^N*. Then*

$$H(U_1 \cap U_2) \leq H(U_1) H(U_2).$$

This well known fact is an immediate corollary of Theorem 1 of [12].

Lemma 2.3. *Let X be a $J \times N$ matrix over K with row vectors $\boldsymbol{x}_1, ..., \boldsymbol{x}_J$, and let F be a symmetric bilinear form in N variables over K, as above (we also write F for its $N \times N$ coefficient matrix). Then*

$$\mathcal{H}(XF) \leq H(F)^J \prod_{i=1}^{J} H(\boldsymbol{x}_i).$$

Proof. By Lemma 4.7 of [9]

$$\mathcal{H}(XF) = H(\boldsymbol{x}_1^t F \wedge \ \dots \ \wedge \boldsymbol{x}_J^t F) \leq \prod_{i=1}^{J} H(\boldsymbol{x}_i^t F). \tag{15}$$

For each $1 \leq i \leq J$,

$$\boldsymbol{x}_i^t F = \left(\sum_{j=1}^{N} f_{j1} x_{ij}, ..., \sum_{j=1}^{N} f_{jN} x_{ij} \right),$$

and so for $v \nmid \infty$,

$$H_v(\boldsymbol{x}_i^t F) \leq H_v(F) H_v(\boldsymbol{x}_i), \tag{16}$$

and for $v | \infty$, by Cauchy-Schwarz inequality

$$\begin{aligned} H_v(\boldsymbol{x}_i^t F) &= \left\{ \sum_{k=1}^{N} \left\| \sum_{j=1}^{N} f_{jk} x_{ij} \right\|^2 \right\}^{d_v/2d} \\ &\leq \left\{ \sum_{k=1}^{N} \left(\sum_{j=1}^{N} \|f_{jk}\|_v^2 \right) \left(\sum_{j=1}^{N} \|x_{ij}\|_v^2 \right) \right\}^{d_v/2d} = H_v(F) H_v(\boldsymbol{x}_i). \end{aligned} \tag{17}$$

Therefore for each $1 \leq i \leq J$,

$$H(\boldsymbol{x}_i^t F) \leq H(\boldsymbol{x}_i) H(F). \tag{18}$$

The lemma follows by combining (15) with (18). □

Next we will use Theorem 2.1 to produce a small-height orthogonal basis for a subspace of a bilinear space. Specifically, we prove the following theorem.

Theorem 2.4. *Let U be a J-dimensional subspace of (K^N, F), $J < N$. Then there exists a basis $\boldsymbol{x}_1, ..., \boldsymbol{x}_J \in K^N$ for U such that $F(\boldsymbol{x}_i, \boldsymbol{x}_j) = 0$ for all $i \neq j$, and*

$$\prod_{i=1}^{J} H(\boldsymbol{x}_i) \leq (N|\mathcal{D}_K|)^{\frac{J^2+J-2}{4}} H(F)^{\frac{J(J+1)}{2}} H(U)^J. \tag{19}$$

Proof. We argue by induction on J. First suppose that $J = 1$, then pick any $\boldsymbol{0} \neq \boldsymbol{x}_1 \in U$, and observe that $H(\boldsymbol{x}_1) = H(U)$. Now assume that $J > 1$ and the theorem is true for all $1 \leq j < J$. Let $\boldsymbol{0} \neq \boldsymbol{x}_1 \in U$ be a vector guaranteed by Theorem 2.1 so that

$$H(\boldsymbol{x}_1) \leq \left\{ N |\mathcal{D}_K|^{1/d} \right\}^{1/2} H(U)^{1/J}. \tag{20}$$

First assume that $\boldsymbol{x}_1$ is a non-singular point in U. Then

$$U_1 = \{\boldsymbol{y} \in U : \boldsymbol{x}_1^t F \boldsymbol{y} = 0\} = \{\boldsymbol{x}_1\}^{\perp} \cap U,$$

has dimension $J-1$; here $\{\boldsymbol{x}_1\}^{\perp} = \{\boldsymbol{y} \in K^N : \boldsymbol{x}_1^t F \boldsymbol{y} = 0\}$. Then by Lemma 2.2, Lemma 2.3, and (20) we obtain
(21)

$$H(U_1) \leq H(\boldsymbol{x}_1^t F) H(U) \leq H(F) H(\boldsymbol{x}_1) H(U) \leq \left(N |\mathcal{D}_K|^{1/d} \right)^{1/2} H(F) H(U)^{\frac{J+1}{J}}.$$

Since $\dim_K(U_1) = J-1$, the induction hypothesis implies that there exists a basis $\boldsymbol{x}_2, ..., \boldsymbol{x}_J$ for U_1 such that $F(\boldsymbol{x}_i, \boldsymbol{x}_j) = 0$ for all $2 \leq i \neq j \leq J$, and

$$\begin{aligned} \prod_{i=2}^{J} H(\boldsymbol{x}_i) &\leq \left(N |\mathcal{D}_K|^{1/d} \right)^{\frac{J^2-J-2}{4}} H(F)^{\frac{J(J-1)}{2}} H(U_1)^{J-1} \\ &\leq \left(N |\mathcal{D}_K|^{1/d} \right)^{\frac{J^2+J-4}{4}} H(F)^{\frac{J^2+J-2}{2}} H(U)^{\frac{J^2-1}{J}}, \end{aligned} \tag{22}$$

where the last inequality follows by (21). Combining (20) and (22) we see that $\boldsymbol{x}_1, ..., \boldsymbol{x}_J$ is a basis for U satisfying (19) such that $F(\boldsymbol{x}_i, \boldsymbol{x}_j) = 0$ for all $1 \leq i \neq j \leq J$.

Now assume that $\boldsymbol{x}_1$ is a singular point in U. Since $\boldsymbol{x}_1 \neq 0$, it must be true that $x_{1j} \neq 0$ for some $1 \leq j \leq N$. Let

$$U_1 = U \cap \{\boldsymbol{x} \in K^N : x_j = 0\},$$

then $\boldsymbol{x}_1 \notin U_1$, $U = K\boldsymbol{x}_1 \perp U_1$, and

$$H(U_1) \leq H(U), \tag{23}$$

by Lemma 2.2. Since $\dim_K(U_1) = J-1$, we can apply induction hypothesis to U_1, and proceed the same way as in the non-singular case above. Since the upper bound of (23) is smaller than that of (21), the result follows. □

Notice that Theorem 2.4 can be reformulated by saying that there exists a decomposition of the bilinear space (U, F) into an orthogonal sum of one-dimensional subspaces, the product of heights of which is bounded above by (19). Therefore Theorem 2.4 can also be viewed as a result on effective orthogonal decomposition of a bilinear space, which is the subject of this paper.

3. Small zeros of quadratic forms

Let F be a symmetric bilinear form in $2N$ variables over K, as above. Let $Z \subseteq K^N$ be a subspace of dimension $2 \leq L \leq N$. We write (Z, F) for the bilinear space on Z with the bilinear form F restricted to Z. In this section we review some basic results on bilinear spaces and setup the notation that will later be used in the proof of Theorem 1.3.

We start by giving a brief overview of required notation (see Chapter 1 of [10] for a detailed introduction into the subject). A totally isotropic subspace W of (Z, F) is a subspace such that for all $\boldsymbol{x}, \boldsymbol{y} \in W$, $F(\boldsymbol{x}, \boldsymbol{y}) = 0$. All maximal totally isotropic subspaces of (Z, F) have the same dimension. It is called the Witt index of (Z, F) and we denote it by M. A subspace U of (Z, F) is anisotropic if $F(\boldsymbol{x}) \neq 0$ for all $\boldsymbol{0} \neq \boldsymbol{x} \in U$. A subspace U of (Z, F) is called regular if for each $\boldsymbol{0} \neq \boldsymbol{x} \in U$ there exists $\boldsymbol{y} \in U$ so that $F(\boldsymbol{x}, \boldsymbol{y}) \neq 0$. For each subspace U of (Z, F) we define $U^{\perp} = \{\boldsymbol{x} \in Z : F(\boldsymbol{x}, \boldsymbol{y}) = 0 \ \forall \ \boldsymbol{y} \in U\}$. If two subspaces U_1 and U_2 of (Z, F) are orthogonal, we write $U_1 \perp U_2$ for their orthogonal sum. If U is a regular subspace of (Z,F), then $Z = U \perp U^\perp$ and $U \cap U^\perp = \{\mathbf{0}\}$.

Two vectors $\boldsymbol{x}, \boldsymbol{y} \in Z$ are called a hyperbolic pair if $F(\boldsymbol{x}) = F(\boldsymbol{y}) = 0$, $F(\boldsymbol{x}, \boldsymbol{y}) = 1$; the subspace $\mathbb{H}(\boldsymbol{x}, \boldsymbol{y}) = \operatorname{span}_K\{\boldsymbol{x}, \boldsymbol{y}\}$ is regular and is called a hyperbolic plane. An orthogonal sum of hyperbolic planes is called a hyperbolic space. Every hyperbolic space is regular.

We now state a result of Vaaler [13] (see also [11]) on the existence of a maximal totally isotropic subspace of (Z,F) of small height, which we later use in the proof of Theorem 1.3.

Theorem 3.1 ([13])**.** *Let $M \geq 1$ be the Witt index of (Z,F) over K. Then there exists a subspace W of (Z,F) of dimension M such that $F(\boldsymbol{x}) = 0$ for all $\boldsymbol{x} \in W$ and*

$$H(W) \leq \{2^{2M+1} C_K (L-M)^2 H(F)\}^{(L-M)/2} H(Z). \tag{24}$$

Notice that subspace W of Theorem 3.1 is indeed maximal totally isotropic. Maximality is by construction. Also, for each $\boldsymbol{x}, \boldsymbol{y} \in W$, $\boldsymbol{x} + \boldsymbol{y} \in W$, hence

$$0 = F(\boldsymbol{x} + \boldsymbol{y}) = F(\boldsymbol{x}) + F(\boldsymbol{y}) + 2F(\boldsymbol{x}, \boldsymbol{y}) = 2F(\boldsymbol{x}, \boldsymbol{y}).$$

A consequence of a related theorem of Vaaler is the following simple decomposition lemma in case when (Z,F) is not a regular space.

Lemma 3.2. *Let F have rank r on Z, and assume that $1 \leq r < L$. Then the bilinear space (Z,F) can be represented as*

$$Z = Z^\perp \perp W, \tag{25}$$

where W is a regular subspace of Z, with

$$H(Z^\perp) \leq C_K(r)^r H(F)^{r/2} H(Z), \tag{26}$$

and

$$H(W) \leq \left\{ N |\mathcal{D}_K|^{1/d} \right\}^{L/2} H(Z). \tag{27}$$

Proof. The fact that $Z^\perp$ satisfies (26) is guaranteed by Theorem 2 of [14]. Now let $\boldsymbol{z}_1, ..., \boldsymbol{z}_L$ be the basis for Z guranteed by Theorem 2.1, then

$$\prod_{i=1}^{L} H(\boldsymbol{z}_i) \leq \left\{ N |\mathcal{D}_K|^{1/d} \right\}^{L/2} H(Z). \tag{28}$$

Notice that $\dim_K(Z^\perp) = L - r$. We can now pick r vectors $\boldsymbol{z}_{i_1}, ..., \boldsymbol{z}_{i_r}$ from our basis for Z such that

$$\operatorname{span}_K\{Z^\perp, \boldsymbol{z}_{i_1}, ..., \boldsymbol{z}_{i_r}\} = Z.$$

Let $W = \operatorname{span}_K\{\boldsymbol{z}_{i_1}, ..., \boldsymbol{z}_{i_r}\}$, then $Z = Z^\perp \oplus W$. This implies, by Theorem 3.8 on p. 9 of [10], that $Z = Z^\perp \perp W$, W is regular and unique up to isometry. Also, combining Lemma 4.7 of [9] with (28), we obtain

$$H(W) = H(\boldsymbol{z}_{i_1} \wedge \ ... \ \wedge \boldsymbol{z}_{i_r}) \leq \prod_{j=1}^{r} H(\boldsymbol{z}_{i_j}) \leq \left\{ N |\mathcal{D}_K|^{1/d} \right\}^{L/2} H(Z).$$

This finishes the proof. $\square$

Notice that we can immediately deduce a version of Cassels' theorem on small zeros of quadratic form F over K from Theorem 3.1. Namely, if F is isotropic over K, then there exists $\boldsymbol{0} \neq \boldsymbol{x} \in \mathcal{V}_K(F) = \{\boldsymbol{t} \in K^N : F(\boldsymbol{t}) = 0\}$ such that

$$H(\boldsymbol{x}) \ll_{K,N} H(F)^{\frac{N-1}{2}}. \tag{29}$$

The exponent $\frac{N-1}{2}$ on $H(F)$ is proved to be best possible. In fact, if $\mathcal{V}_K(F)$ contains a *nonsingular* point, then by Corollary 1.2 of [3] there exists such a point satisfying (29). A similar statement about singular points of small height in $\mathcal{V}_K(F)$ can be deduced from Lemma 3.2.

Corollary 3.3. *Suppose that $\mathcal{V}_K(F) = \{\boldsymbol{t} \in K^N : F(\boldsymbol{t}) = 0\}$ contains a singular point $\boldsymbol{x} \neq \boldsymbol{0}$, so $1 \leq r = \mathrm{rk}(F) < N$. Then there exists such a point $\boldsymbol{x}$ with*

$$H(\boldsymbol{x}) \leq \sqrt{N}|\mathcal{D}_K|^{1/2d} C_K(r)^{\frac{r}{N-r}} H(F)^{\frac{r}{2(N-r)}}. \tag{30}$$

Proof. Let Z of Lemma 3.2 be K^N, then $H(Z) = 1$, $L = N$, and $\dim_K(Z^{\perp}) = N - r$. Clearly $Z^{\perp} \subseteq \mathcal{V}_K(F)$, and all points of $Z^{\perp}$ are singular in $\mathcal{V}_K(F)$. By Theorem 2.1, there must exist $\boldsymbol{0} \neq \boldsymbol{x} \in Z^{\perp}$ such that

$$H(\boldsymbol{x}) \leq \sqrt{N}|\mathcal{D}_K|^{1/2d} H(Z^{\perp})^{1/(N-r)} \leq \sqrt{N}|\mathcal{D}_K|^{1/2d} C_K(r)^{\frac{r}{N-r}} H(F)^{\frac{r}{2(N-r)}},$$

where the last inequality follows by (26). □

Notice that Corollary 3.3 suggests that in this context the singular case can be simpler than the nonsingular one. This unusual phenomenon has already been observed in [6] and [3]. We are now ready to prove Theorem 1.3.

4. Proof of Theorem 1.3

We first prove a version of our theorem for a regular bilinear space. We remark that everywhere in our arguments, if $m < n$, then $\sum_{i=n}^{m}$ is taken to mean 0 and $\prod_{i=n}^{m}$ is taken to mean 1.

Theorem 4.1. *Let F be a symmetric bilinear form on K^N. Let $Z \subseteq K^N$ be a subspace of dimension L, $2 \leq L \leq N$, such that the bilinear space (Z, F) is regular, i.e. $Z^{\perp} = \{\boldsymbol{0}\}$. Let $M \geq 1$ be the Witt index of (Z, F). There exists an orthogonal decomposition of (Z, F) of the form*

$$Z = \mathbb{H}_1 \perp \dots \perp \mathbb{H}_M \perp V, \tag{31}$$

where $\mathbb{H}_i$ are hyperbolic planes, V is anisotropic component, and

$$\max\{H(\mathbb{H}_i), H(V)\} \leq A_K(N, L, M) \left\{ H(F)^{\frac{L+2M}{4}} H(Z) \right\}^{\frac{(M+1)(M+2)}{2}}, \tag{32}$$

for each $1 \leq i \leq M$, where

$$A_K(N, L, M) = \left\{ \left(2^{2M+1} C_K(L)^2\right)^L \left(N|\mathcal{D}_K|^{1/d}\right)^{M+L} \right\}^{\frac{M(M+3)}{8}}. \tag{33}$$

Proof. Let W be a maximal totally isotropic subspace of (Z, F) satisfying (24) and let $\boldsymbol{x}_1, \dots, \boldsymbol{x}_M$ be the basis for W guaranteed by Theorem 2.1. Notice that $F(\boldsymbol{x}_i, \boldsymbol{x}_j) = 0$ for all $1 \leq i, j \leq M$, since W is a totally isotropic subspace. Let $\boldsymbol{y}_1, \dots, \boldsymbol{y}_L$ be the basis for Z guaranteed by Theorem 2.1, ordered so that

$$H(\boldsymbol{y}_1) \leq H(\boldsymbol{y}_2) \leq \dots \leq H(\boldsymbol{y}_L).$$

For each $1 \leq i \leq M$ let j_i be the smallest index such that $F(\boldsymbol{x}_i, \boldsymbol{y}_{j_i}) \neq 0$. Such j_i exists for each i since otherwise $\boldsymbol{x}_i$ would be a singular point, contradicting regularity of (Z,F). By reordering $\boldsymbol{x}_1,...,\boldsymbol{x}_M$ if necessary, we can assume without loss of generality that

$$1 \leq j_M \leq j_{M-1} \leq ... \leq j_1 \leq L.$$

Moreover, for each $1 \leq i \leq M$, $j_i \leq L-i+1$, since

$$\operatorname{span}_K\{\boldsymbol{y}_1,...,\boldsymbol{y}_{L-i+1}\} \nsubseteq \operatorname{span}_K\{\boldsymbol{x}_1,...,\boldsymbol{x}_i\}^{\perp},$$

and so $H(\boldsymbol{y}_{j_i}) \leq H(\boldsymbol{y}_{L-i+1})$ by our ordering of $\boldsymbol{y}_1,...,\boldsymbol{y}_L$. Therefore, by (14)

$$\begin{aligned} \prod_{i=1}^M H(\boldsymbol{x}_i)H(\boldsymbol{y}_{j_i}) &\leq \prod_{i=1}^M H(\boldsymbol{x}_i)H(\boldsymbol{y}_{L-i+1}) \\ &= \left(\prod_{i=1}^M H(\boldsymbol{x}_i)\right)\left(\prod_{i=1}^M H(\boldsymbol{y}_{L-i+1})\right) \\ &\leq \left\{N|\mathcal{D}_K|^{1/d}\right\}^{\frac{M+L}{2}} H(W)H(Z). \end{aligned} \tag{34}$$

In particular, for some $1 \leq i \leq M$, we must have

$$H(\boldsymbol{x}_i)H(\boldsymbol{y}_{j_i}) \leq \left\{N|\mathcal{D}_K|^{1/d}\right\}^{\frac{M+L}{2M}} (H(W)H(Z))^{\frac{1}{M}}. \tag{35}$$

Define $\mathbb{H}_1 = \operatorname{span}_K\{\boldsymbol{x}_i, \boldsymbol{y}_{j_i}\}$ for this choice of i. Since $F(\boldsymbol{x}_i) = 0$ and $F(\boldsymbol{x}_i, \boldsymbol{y}_{j_i}) \neq 0$, $\mathbb{H}_1$ is a regular subspace of Z with Witt index equal to one, hence it is a hyperbolic plane. Notice that by combining (35) and (24), we have

$$H(\mathbb{H}_1) \leq H(\boldsymbol{x}_i)H(\boldsymbol{y}_{j_i}) \leq B_K(N,L,M)H(F)^{\frac{L-M}{2M}}H(Z)^{\frac{2}{M}}, \tag{36}$$

where

$$B_K(N,L,M) = \left\{\left(2^{2M+1}C_K(L-M)^2\right)^{L-M}\left(N|\mathcal{D}_K|^{1/d}\right)^{M+L}\right\}^{\frac{1}{2M}}. \tag{37}$$

Define

$$Z_1 = \mathbb{H}_1^{\perp} = \{\boldsymbol{z} \in K^N : F(\boldsymbol{z},\boldsymbol{x}) = 0 \ \forall\ \boldsymbol{x} \in \mathbb{H}_1\} \cap Z,$$

so $\dim_K(Z_1) = L-2$, and $Z = \mathbb{H}_1 \perp Z_1$. Notice that by combining Lemma 2.2, Lemma 2.3, and (36), we have

$$H(Z_1) \leq H(\mathbb{H}_1)H(Z)H(F)^2 \leq B_K(N,L,M)H(F)^{\frac{L+3M}{2M}}H(Z)^{\frac{M+2}{M}}. \tag{38}$$

We continue by induction on M. If $M=1$, we are done. If $M \geq 2$, assume that the theorem holds for a bilinear space of Witt index smaller than M, in particular it holds for (Z_1,F), a bilinear space of dimension $L-2$ and Witt index $M-1$. Then there exists a decomposition

$$Z_1 = \mathbb{H}_2 \perp \ ... \ \perp \mathbb{H}_M \perp V, \tag{39}$$

where V, the anisotropic component of Z_1 is the same as that of Z, and combining the induction hypothesis with (38) and (37), for each $2 \leq i \leq M$ we obtain

$$\begin{aligned}
\max\{H(\mathbb{H}_i), H(V)\} &\leq A_K(N, L-2, M-1)\left\{H(F)^{\frac{L+2M-4}{4}} H(Z_1)\right\}^{\frac{M(M+1)}{2}} \\
&\leq A_K(N, L-2, M-1) B_K(N, L, M)^{\frac{M(M+1)}{2}} \times \\
&\times \left\{H(F)^{\frac{L+2M-4}{4}+\frac{L+3M}{2M}} H(Z)^{\frac{M+2}{M}}\right\}^{\frac{M(M+1)}{2}} \\
&\leq A_K(N, L, M)\left\{H(F)^{\frac{L+2M}{4}} H(Z)\right\}^{\frac{(M+1)(M+2)}{2}}. \qquad (40)
\end{aligned}$$

This finishes the proof. □

Proof of Theorem 1.3. If (Z, F) is regular, then $Z^{\perp} = \{\mathbf{0}\}$, and we are done by Theorem 4.1. Let r be rank of F on Z, and assume that $1 \leq r < L$. By Lemma 3.2, there exists a decomposition of Z of the form (25) with $H(Z^{\perp})$ and $H(W)$ bounded as in (26) and (27) respectively. Now W is a regular subspace of Z, so we can apply Theorem 4.1 to the bilinear space (W, F). The result follows. □

5. Isometries of a bilinear space

In this section we develop the preliminaries needed for the proof of Theorem 1.4. We start with some definitions and then prove a few technical lemmas. Let F be a symmetric bilinear form as above, and let Z be an L-dimensional subspace of K^N, $1 \leq L \leq N$, $N \geq 2$, such that the bilinear space (Z, F) is regular, and thus $K^N = Z \perp Z^{\perp_{K^N}}$, where $Z^{\perp_{K^N}} = \{\boldsymbol{x} \in K^N : F(\boldsymbol{x}, \boldsymbol{z}) = 0 \ \forall\ \boldsymbol{z} \in Z\}$. Let $\mathcal{O}(Z, F)$ be the group of isometries of (Z, F), and write id_Z for its identity element. Also let $-id_Z$ be the element of $\mathcal{O}(Z, F)$ that takes $\boldsymbol{x}$ to $-\boldsymbol{x}$ for each $\boldsymbol{x} \in Z$. Each element σ of the isometry group $\mathcal{O}(K^N, F)$ is uniquely represented by an $N \times N$ matrix $A \in GL_N(K)$, and so we can define $H(\sigma) = H(A)$, where $H(A)$ is defined by viewing A as a vector in K^{N^2} as we did in section 1.

Notice that each $\sigma \in \mathcal{O}(Z, F)$ can be extended to an isometry of $\hat{\sigma} \in \mathcal{O}(K^N, F)$ by selecting an isometry $\sigma' \in \mathcal{O}(Z^{\perp_{K^N}}, F)$. For each $\sigma \in \mathcal{O}(Z, F)$ choose such an extension $\hat{\sigma} : K^N \to K^N$ so that $H(\hat{\sigma})$ is minimal, and define $H(\sigma) = H(\hat{\sigma})$ for this choice of $\hat{\sigma}$. This definition of height in particular insures that for each $\sigma \in \mathcal{O}(Z, F)$

$$H(\sigma) = H(-\sigma), \qquad (41)$$

where $-\sigma = -id_Z \circ \sigma$. Moreover, if A is the matrix of $\hat{\sigma}$, then

$$\det(A) = \det(\hat{\sigma}) = \det\left(\hat{\sigma}\ |_Z\right) \det\left(\hat{\sigma}\ |_{Z^{\perp_{K^N}}}\right) = \det(\sigma)\det(\sigma') = \pm 1. \qquad (42)$$

We will also refer to this matrix A as the matrix of σ.

For each $\boldsymbol{x} \in Z$ such that $F(\boldsymbol{x}) \neq 0$ we can define an element of $\mathcal{O}(Z, F)$, $\tau_{\boldsymbol{x}} : Z \longrightarrow Z$, given by

$$\tau_{\boldsymbol{x}}(\boldsymbol{y}) = \boldsymbol{y} - \frac{2F(\boldsymbol{x}, \boldsymbol{y})}{F(\boldsymbol{x})}\boldsymbol{x}, \qquad (43)$$

which is a *reflection* in the hyperplane $\{\boldsymbol{x}\}^{\perp} = \{\boldsymbol{z} \in Z : F(\boldsymbol{x}, \boldsymbol{z}) = 0\}$. It is not difficult to see that the matrix of such a reflection is of the form $(\tau_{ij}(\boldsymbol{x}))_{1 \leq i,j \leq N}$, where

$$\tau_{ij}(\boldsymbol{x}) = \begin{cases} 1 - \frac{2}{F(\boldsymbol{x})} \sum_{k=1}^N f_{ik} x_i x_k & \text{if } i = j \\ -\frac{2}{F(\boldsymbol{x})} \sum_{k=1}^N f_{jk} x_i x_k & \text{if } i \neq j \end{cases}$$

For each reflection $\tau_{\boldsymbol{x}}$, $\det(\tau_{\boldsymbol{x}}) = -1$. We say that σ is a *rotation* if $\det(\sigma) = +1$.

Lemma 5.1. *Let $\boldsymbol{x} \in Z$ be anisotropic and $\tau_{\boldsymbol{x}} \in \mathcal{O}(Z, F)$ be the corresponding reflection. Then*

$$H(\tau_{\boldsymbol{x}}) \leq N^3(N+2) H(F) H(\boldsymbol{x})^2. \tag{44}$$

Proof. By the product formula, $H(\tau_{\boldsymbol{x}}) = H(F(\boldsymbol{x})\tau_{\boldsymbol{x}})$. If $v \in M(K)$ is such that $v \nmid \infty$, then for each $1 \leq i = j \leq N$

$$\begin{aligned} |F(\boldsymbol{x})\tau_{ij}(\boldsymbol{x})|_v &= \left| F(\boldsymbol{x}) - 2 \sum_{k=1}^N f_{jk} x_i x_k \right|_v \\ &= \left| \sum_{l=1}^N \sum_{m=1}^N f_{lm} x_l x_m - 2 \sum_{k=1}^N f_{jk} x_i x_k \right|_v \leq H_v(F) H_v(\boldsymbol{x})^2, \end{aligned} \tag{45}$$

since $|2|_v \leq 1$, and similarly when $i \neq j$, so $H_v(F(\boldsymbol{x})\tau_{\boldsymbol{x}}) \leq H_v(F) H_v(\boldsymbol{x})^2$.
If $v | \infty$, then for each $1 \leq i = j \leq N$

$$\begin{aligned} \|F(\boldsymbol{x})\tau_{ij}(\boldsymbol{x})\|_v &\leq \sum_{l=1}^N \sum_{m=1}^N \|f_{lm} x_l x_m\|_v + 2 \sum_{k=1}^N \|f_{jk} x_i x_k\|_v \\ &\leq N(N+2) \max_{1 \leq l,m \leq N} \|f_{lm} x_l x_m\|_v \\ &\leq N(N+2) \left\{ H_v(F) H_v(\boldsymbol{x})^2 \right\}^{d/d_v}, \end{aligned} \tag{46}$$

and similarly when $i \neq j$, therefore $H_v(F(\boldsymbol{x})\tau_{\boldsymbol{x}}) \leq \left\{ N^3(N+2) \right\}^{d_v/d} H_v(F) H_v(\boldsymbol{x})^2$. The result follows by taking a product over all places of K. □

Lemma 5.2. *Let $\sigma \in \mathcal{O}(Z, F)$. There exists an anisotropic vector $\boldsymbol{y}$ in Z such that $\sigma(\boldsymbol{y}) \pm \boldsymbol{y}$ is also anisotropic for some choice of $\pm$, and*

$$H(\boldsymbol{y}) \leq h(\boldsymbol{y}) \leq 2\sqrt{L} \left\{ N |\mathcal{D}_K|^{\frac{1}{d}} \right\}^{\frac{L+2}{4}} H(Z)^{\frac{L+2}{2L}}. \tag{47}$$

Proof. If $L = 1$, then $Z = K\boldsymbol{y}$ for some $\boldsymbol{0} \neq \boldsymbol{y} \in K^N$, and since (Z, F) is regular, $F(\boldsymbol{y}) \neq 0$, $H(\boldsymbol{y}) = H(Z)$, $\mathcal{O}(Z, F) = \{id_Z\}$, and clearly $id_Z(\boldsymbol{y}) + \boldsymbol{y} = 2\boldsymbol{y}$ is also anisotropic. Hence assume $L \geq 2$. Let $\boldsymbol{x}_1, ..., \boldsymbol{x}_L$ be a basis for Z which satisfies (14), ordered so that

$$h(\boldsymbol{x}_1) \leq h(\boldsymbol{x}_2) \leq \cdots \leq h(\boldsymbol{x}_L),$$

Let m be the the smallest index such that the restriction of F to

$$U = \operatorname{span}_K \{\boldsymbol{x}_1, ..., \boldsymbol{x}_m\}$$

is not identically zero. Since (Z, F) is regular, we must have $1 \leq m \leq \left[\frac{L}{2}\right] + 1$, and therefore, by (14)

$$\prod_{i=1}^m h(\boldsymbol{x}_i) \leq \left\{ N |\mathcal{D}_K|^{\frac{1}{d}} \right\}^{\frac{m}{2}} H(Z)^{\frac{m}{L}} \leq \left\{ N |\mathcal{D}_K|^{\frac{1}{d}} \right\}^{\frac{L+2}{4}} H(Z)^{\frac{L+2}{2L}}. \tag{48}$$

Notice that for every vector $\boldsymbol{x} \in Z$,

$$F(\sigma(\boldsymbol{x}) - \boldsymbol{x}) + F(\sigma(\boldsymbol{x}) + \boldsymbol{x}) = 4F(\boldsymbol{x}).$$

Since F is not identically zero on U, it must therefore be true that at least one of $F \circ (\sigma \pm id_Z)$ is not identically zero on U. Assume for instance that $F \circ (\sigma - id_Z)$ is not identically zero on U. Then the homogeneous polynomial of degree four in m variables

$$P(a_1, ..., a_m) = F\left(\sum_{i=1}^m a_i \boldsymbol{x}_i\right) F\left(\sigma\left(\sum_{i=1}^m a_i \boldsymbol{x}_i\right) - \sum_{i=1}^m a_i \boldsymbol{x}_i\right) \in K[a_1, ..., a_m]$$

is not identically zero on U. Therefore there exist $\beta_1, ..., \beta_m \in \{-2, -1, 0, 1, 2\}$ such that $P(\beta_1, ..., \beta_m) \neq 0$. Let $\boldsymbol{y} = \sum_{i=1}^m \beta_i \boldsymbol{x}_i$ for this choice of $\beta_1, ..., \beta_m$, then $\boldsymbol{y} \in U$ is precisely the vector we are looking for. Combining (7) and (48) we obtain

$$H(\boldsymbol{y}) \leq h(\boldsymbol{y}) \leq \sqrt{\frac{4(L+2)}{2}} \prod_{i=1}^m h(\boldsymbol{x}_i) \leq 2\sqrt{L} \left\{N |\mathcal{D}_K|^{\frac{1}{d}}\right\}^{\frac{L+2}{4}} H(Z)^{\frac{L+2}{2L}},$$

since $L \geq 2$. This completes the proof. □

An immediate consequence of Lemma 5.1 and Lemma 5.2 is the following statement on the existence of isometries of (Z, F) of small height. This is related to a question of Masser in [7] (see the discussion on this in the introduction - section 1).

Corollary 5.3. *There exists a reflection $\tau \in \mathcal{O}(Z, F)$ with*

$$H(\tau) \leq 4LN^{\frac{L+8}{2}} (N+2) |\mathcal{D}_K|^{\frac{L+2}{2d}} H(F) H(Z)^{\frac{L+2}{L}}. \tag{49}$$

Proof. Let $\boldsymbol{x}$ be an anisotropic point in Z guaranteed by Lemma 5.2. Let $\tau = \tau_{\boldsymbol{x}}$. The result follows by combining (44) with (47). □

Lemma 5.4. *Let $A \in GL_N(K)$ be such that* $\det(A) = \pm 1$, *and write I_N for the $N \times N$ identity matrix. Then*

$$H(A \pm I_N) \leq 2H(A). \tag{50}$$

Proof. Let $\boldsymbol{a}_1, ..., \boldsymbol{a}_N$ be row vectors of A. Then for each $v \in M(K)$

$$\prod_{i=1}^N H_v(\boldsymbol{a}_i) \geq \begin{cases} |\det(A)|_v = 1 & \text{if } v \nmid \infty \\ \|\det(A)\|_v = 1 & \text{if } v | \infty \end{cases}$$

by Hadamard's inequality. Therefore, if $v \nmid \infty$, we have

$$H_v(A) = \max_{1 \leq i \leq N} \{H_v(\boldsymbol{a}_i)\} \geq 1,$$

and so

$$H_v(A \pm I_N) \leq \max\{1, H_v(A)\} = H_v(A). \tag{51}$$

If $v | \infty$,

$$\begin{aligned} 1 \leq \left(\prod_{i=1}^N H_v(\boldsymbol{a}_i)^{\frac{d}{d_v}}\right)^{\frac{1}{N}} &\leq \frac{1}{N} \sum_{i=1}^N H_v(\boldsymbol{a}_i)^{\frac{d}{d_v}} \\ &\leq \frac{1}{\sqrt{N}} \left(\sum_{i=1}^N H_v(\boldsymbol{a}_i)^{\frac{2d}{d_v}}\right)^{\frac{1}{2}} = \frac{1}{\sqrt{N}} H_v(A)^{\frac{d}{d_v}}, \end{aligned}$$

where the last inequality follows by Cauchy-Schwarz. Hence $H_v(A)^{\frac{d}{d_v}} \geq \sqrt{N}$, and so, by the triangle inequality,

$$H_v(A \pm I_N)^{\frac{d}{d_v}} \leq H_v(A)^{\frac{d}{d_v}} + H_v(I_N)^{\frac{d}{d_v}} \leq H_v(A)^{\frac{d}{d_v}} + \sqrt{N} \leq 2H_v(A)^{\frac{d}{d_v}}. \tag{52}$$

The result follows by combining (51) with (52) and taking a product over all places of K. □

The following simple corollary of Lemma 5.4 provides a bound on the height of the invariant subspace of an isometry, which is an object of interest in the algebraic theory of quadratic forms.

Corollary 5.5. *Let $\sigma \in \mathcal{O}(Z,F)$. Let U be the invariant subspace of σ, i.e. $U = \{\boldsymbol{z} \in Z : \sigma(\boldsymbol{z}) = \boldsymbol{z}\}$. Let $J = \dim_K(U) \leq L$. Then*

$$H(U) \leq \{2H(\sigma)\}^{N-J}\, H(Z), \tag{53}$$

Proof. Write A for the $N \times N$ matrix of σ, and I_N for the $N \times N$ identity matrix. Notice that $U = \{\boldsymbol{z} \in Z : (A - I_N)\boldsymbol{z} = \boldsymbol{0}\}$. Let B be a submatrix of $A - I_N$ which consists of $N - J$ linearly independent rows of $A - I_N$. Hence rows of B are of the form $\boldsymbol{a}_{i_1} - \boldsymbol{e}_{i_1}, ..., \boldsymbol{a}_{i_{N-J}} - \boldsymbol{e}_{i_{N-J}}$ for some $i_1, ..., i_{N-J} \in \{1, ..., N\}$. Then, by Lemma 4.7 of [9]

$$\begin{aligned} \mathcal{H}(B) &= H\left((\boldsymbol{a}_{i_1} - \boldsymbol{e}_{i_1}) \wedge \ ... \ \wedge (\boldsymbol{a}_{i_{N-J}} - \boldsymbol{e}_{i_{N-J}})\right) \\ &\leq \prod_{j=1}^{N-J} H(\boldsymbol{a}_{i_j} - \boldsymbol{e}_{i_j}) \leq H(A - I_N)^{N-J} \leq (2H(A))^{N-J}, \end{aligned} \tag{54}$$

where the last inequality follows by Lemma 5.4. Combining (54) with Lemma 2.2, we obtain

$$H(U) \leq \mathcal{H}(B) H(Z) \leq \{2H(A)\}^{N-J} H(Z).$$

The finishes the proof, since $H(\sigma) = H(A)$ by definition. □

The following lemma bounds the height of a product of two matrices.

Lemma 5.6. *Let A and B be two $N \times N$ matrices with entries in K. Then*

$$H(AB) \leq H(A)H(B). \tag{55}$$

Proof. Write $A = (\boldsymbol{a}_1 \dots \boldsymbol{a}_N)^t$, i. e. $\boldsymbol{a}_1^t, \dots, \boldsymbol{a}_N^t$ are row vectors of A. Then we can think of

$$AB = (\boldsymbol{a}_1^t B, \dots, \boldsymbol{a}_N^t B)^t$$

as a vector in K^{N^2}. Hence for each $v \in M(K)$ such that $v \nmid \infty$

$$H_v(AB) = \max_{1 \leq i \leq N} \{H_v(\boldsymbol{a}_i^t B)\} \leq H_v(B) \max_{1 \leq i \leq N} \{H_v(\boldsymbol{a}_i)\} = H_v(A) H_v(B),$$

by (16). For each $v | \infty$, we have

$$H_v(AB) = \left\{ \sum_{i=1}^N H_v(\boldsymbol{a}_i^t B)^{\frac{2d}{d_v}} \right\}^{\frac{d_v}{2d}} \leq H_v(B) \left\{ \sum_{i=1}^N H_v(\boldsymbol{a}_i)^{\frac{2d}{d_v}} \right\}^{\frac{d_v}{2d}} = H_v(A) H_v(B),$$

by (17). The conclusion follows by taking a product. □

6. Effective version of Cartan-Dieudonné theorem

In this section we will prove Theorem 1.4. Let all the notation be as in section 5. We argue by induction on L. When $L = 1$, $Z = K\boldsymbol{x}$ for some anisotropic vector $\boldsymbol{x} \in K^N$, since (Z, F) is regular. Then $\sigma = \pm id_Z$, where $-id_Z = \tau_{\boldsymbol{x}}$, and $H(\sigma) = \sqrt{N}$ by (41).

Then assume $L > 1$. Write A for the $N \times N$ matrix of σ, and I_N for the $N \times N$ identity matrix, so in particular $H(\sigma) = H(A)$. Notice that for each $\boldsymbol{x} \in Z$,

$$F(\sigma(\boldsymbol{x}) - \boldsymbol{x}, \sigma(\boldsymbol{x}) + \boldsymbol{x}) = 0. \tag{56}$$

Let $\boldsymbol{x} \in Z$ be the anisotropic vector guaranteed by Lemma 5.2 with $\sigma(\boldsymbol{x}) \pm \boldsymbol{x}$ also anisotropic. For this choice of $\pm$, $\tau_{\sigma(\boldsymbol{x})\pm\boldsymbol{x}}$ fixes $\sigma(\boldsymbol{x}) \mp \boldsymbol{x}$ and maps $\sigma(\boldsymbol{x}) \pm \boldsymbol{x}$ to $-(\sigma(\boldsymbol{x}) \pm \boldsymbol{x})$. Then $2\sigma(\boldsymbol{x}) = (\sigma(\boldsymbol{x})) + (\sigma(\boldsymbol{x}) - \boldsymbol{x})$ will be mapped to $(\sigma(\boldsymbol{x}) \mp \boldsymbol{x}) - (\sigma(\boldsymbol{x}) \pm \boldsymbol{x}) = \mp 2\boldsymbol{x}$. We can therefore observe that if $\sigma(\boldsymbol{x}) - \boldsymbol{x}$ is anisotropic, then

$$\sigma' = \tau_{\sigma(\boldsymbol{x})-\boldsymbol{x}} \circ \sigma \tag{57}$$

fixes $\boldsymbol{x}$. If, on the other hand, $\sigma(\boldsymbol{x}) + \boldsymbol{x}$ is anisotropic, then

$$\sigma' = \tau_{\sigma(\boldsymbol{x})+\boldsymbol{x}} \circ \tau_{\sigma(\boldsymbol{x})} \circ \sigma \tag{58}$$

fixes $\boldsymbol{x}$. In any case, σ' defined either by (57) or (58) is an isometry of the $(L-1)$-dimensional regular bilinear space $(\{\boldsymbol{x}\}^\perp, F)$, where $\{\boldsymbol{x}\}^\perp = \{\boldsymbol{z} \in Z : F(\boldsymbol{x}, \boldsymbol{z}) = 0\}$. Then, by the induction hypothesis,

$$\sigma' = \tau_1 \circ \cdots \circ \tau_l,$$

for some reflections $\tau_1, ..., \tau_l$ with $1 \le l \le 2L - 3$ and

$$H(\tau_i) \le \left\{ \left(2N^2 |\mathcal{D}_K|^{\frac{1}{2d}}\right)^{\frac{(L-1)^2}{2}} H(F)^{\frac{L-1}{3}} H\left(\{\boldsymbol{x}\}^\perp\right)^{\frac{L-1}{2}} H(\sigma') \right\}^{5^{L-2}}, \tag{59}$$

for each $1 \le i \le l$, and so

$$\sigma = \sigma'' \circ \tau_1 \circ \cdots \circ \tau_l, \tag{60}$$

for the same $\tau_1, ..., \tau_l$ and $\sigma'' = \tau_{\sigma(\boldsymbol{x})-\boldsymbol{x}}$ or $\sigma'' = \tau_{\sigma(\boldsymbol{x})+\boldsymbol{x}} \circ \tau_{\sigma(\boldsymbol{x})}$, depending on which of $\sigma(\boldsymbol{x}) \pm \boldsymbol{x}$ is anisotropic, so σ is a product of at most $2L - 1$ reflections. Next we are going to produce bounds on their heights. Combining Lemma 5.1 with an argument identical to the proof of Lemma 2.3 and Lemma 5.2, we obtain

$$H(\tau_{\sigma(\boldsymbol{x})}) \le 4LN^{\frac{L+8}{2}} (N+2) |\mathcal{D}_K|^{\frac{L+2}{2d}} H(F) H(Z)^{\frac{L+2}{L}} H(\sigma)^2. \tag{61}$$

Therefore $\tau_{\sigma(\boldsymbol{x})}$ satisfies (13). Also by Lemma 5.1,

$$H(\tau_{\sigma(\boldsymbol{x})\pm\boldsymbol{x}}) \le N^3 (N+2) H(F) H(\sigma(\boldsymbol{x}) \pm \boldsymbol{x})^2. \tag{62}$$

Notice that $\sigma(\boldsymbol{x}) \pm \boldsymbol{x} = (A \pm I_N)\boldsymbol{x}$. Then, once again, by an argument identical to the proof of Lemma 2.3

$$H(\sigma(\boldsymbol{x}) \pm \boldsymbol{x}) \le H(\boldsymbol{x}) H(A \pm I_N) \le 2\sqrt{L} \left\{ N |\mathcal{D}_K|^{\frac{1}{d}} \right\}^{\frac{L+2}{4}} H(Z)^{\frac{L+2}{2L}} H(A \pm I_N), \tag{63}$$

where the last inequality follows by (47). Combining (63) with Lemma 5.4, we obtain

$$H(\sigma(\boldsymbol{x}) \pm \boldsymbol{x}) \le 4\sqrt{L} \left\{ N |\mathcal{D}_K|^{\frac{1}{d}} \right\}^{\frac{L+2}{4}} H(Z)^{\frac{L+2}{2L}} H(A). \tag{64}$$

Combining (62) and (64), we obtain

$$H(\tau_{\sigma(\boldsymbol{x})\pm \boldsymbol{x}}) \leq 16LN^{\frac{L+8}{2}}(N+2)|\mathcal{D}_K|^{\frac{L+2}{2d}} H(F)H(Z)^{\frac{L+2}{L}} H(\sigma)^2, \tag{65}$$

hence $\tau_{\sigma(\boldsymbol{x})\pm \boldsymbol{x}}$ satisfies (13). By combining (57), (58), (41), Lemma 5.6, (61), and (65), we have

$$H(\sigma') \leq 64L^2N^{L+8}(N+2)^2|\mathcal{D}_K|^{\frac{L+2}{d}} H(F)^2 H(Z)^{\frac{2L+4}{L}} H(\sigma)^5. \tag{66}$$

By Lemma 2.2, Lemma 2.3, and (47)

$$H\left(\{\boldsymbol{x}\}^{\perp}\right) \leq H(F)H(\boldsymbol{x})H(Z) \leq 2\sqrt{L}\left\{N|\mathcal{D}_K|^{\frac{1}{d}}\right\}^{\frac{L+2}{4}} H(F)H(Z)^{\frac{3L+2}{2L}}. \tag{67}$$

Then bound (13) follows upon combining (59) with (66) and (67) while keeping in mind that $2 \leq L \leq N$ and $N+2 \leq 2N$. This completes the proof.

Aknowledgement. I would like to express my deep gratitude to Professor Damien Roy for pointing me in the direction of these problems, as well as for his extremely helpful suggestions that allowed to improve the bounds and simplify the arguments in this paper.

References

[1] E. Bombieri and J. D. Vaaler. On Siegel's lemma. *Invent. Math.*, 73(1):11–32, 1983.

[2] J. W. S. Cassels. Bounds for the least solutions of homogeneous quadratic equations. *Proc. Cambridge Philos. Soc.*, 51:262–264, 1955.

[3] L. Fukshansky. Small zeros of quadratic forms with linear conditions. *J. Number Theory*, 108(1):29–43, 2004.

[4] P. Gordan. Uber den grossten gemeinsamen factor. *Math. Ann.*, 7:443–448, 1873.

[5] W. V. D. Hodge and D. Pedoe. *Methods of Algebraic Geometry, Volume 1.* Cambridge Univ. Press, 1947.

[6] D. W. Masser. How to solve a quadratic equation in rationals. *Bull. London Math. Soc.*, 30(1):24–28, 1998.

[7] D. W. Masser. Search bounds for Diophantine equations. *A panorama of number theory or the view from Baker's garden (Zurich, 1999)*, pages 247–259, 2002.

[8] O. T. O'Meara. *Introduction to Quadratic Forms. Second Printing, Corrected.* Springer-Verlag, 1971.

[9] D. Roy and J. L. Thunder. An absolute Siegel's lemma. *J. Reine Angew. Math.*, 476:1–26, 1996.

[10] W. Scharlau. *Quadratic and Hermitian Forms.* Springer-Verlag, 1985.

[11] H. P. Schlickewei and W. M. Schmidt. Quadratic geometry of numbers. *Trans. Amer. Math. Soc.*, 301(2):679–690, 1987.

[12] T. Struppeck and J. D. Vaaler. Inequalities for heights of algebraic subspaces and the Thue-Siegel principle. *Analytic number theory (Allerton Park, IL, 1989), Progr. Math.*, 85:493–528, 1990.

[13] J. D. Vaaler. Small zeros of quadratic forms over number fields. *Trans. Amer. Math. Soc.*, 302:281–296, 1987.

[14] J. D. Vaaler. Small zeros of quadratic forms over number fields II. *Trans. Amer. Math. Soc.*, 302:671–686, 1989.

Department of Mathematics, Mailstop 3368, Texas A&M University, College Station, Texas 77843-3368

E-mail address: `lenny@math.tamu.edu`