# ON SMALL-HEIGHT ELEMENTS IN NUMBER FIELDS

LENNY FUKSHANSKY AND SEHUN JEONG

Abstract. Let $K$ be a number field of degree $d$ that contains elements of degree $m$ for some divisor $m$ of $d$. Then every ideal $I$ in the ring of integers $\mathcal{O}_K$ contains infinitely many elements of degree $m$. We prove a bound on the smallest height of such an element in $I$. As a corollary of our result in the case $m = d$, we obtain small-height primitive elements for $K$ in every ideal, an observation closely related to a 1998 conjecture of W. Ruppert. Our bound depends on the degree of the element, degree and discriminant of the number field, and the norm of the ideal. We investigate the optimality of our bound for quadratic number fields, proving that in that case dependence on the discriminant is sharp. This dependence differs from Ruppert's bound for quadratic fields without restriction to an ideal. Finally, in the case of a totally real field, we obtain a height bound for a totally positive primitive element in an ideal.

## 1. Introduction and statement of results

Let $K$ be a number field of degree $d := [K : \mathbb{Q}] \geq 1$. Let $\sigma_1, \dots, \sigma_d : K \hookrightarrow \mathbb{C}$ be the embeddings of $K$, ordered so that the first $r_1$ of them are real and the remaining $2r_2$ are conjugate pairs of complex embeddings so that $\sigma_{r_2+j} = \bar{\sigma}_j$ for

$$d = r_1 + 2r_2.$$

An element $\alpha \in K$ is called *primitive* if $K = \mathbb{Q}(\alpha)$. This is equivalent to the condition that $\deg_{\mathbb{Q}}(\alpha) = d$, and hence there are infinitely many primitive elements in $K$. A conjecture of Ruppert [7] asserts that there exists a primitive element $\alpha \in K$ such that

$$h(\alpha) \leq C_d |\Delta_K|^{\frac{1}{2d}},$$

where $h$ is the absolute Weil height, $\Delta_K$ is the discriminant of the number field $K$, and $C_d$ is a constant depending only on the degree $d$. Ruppert himself proved this conjecture for quadratic number fields and for totally real fields of prime degree. There has been quite a bit of later work on this conjecture; for instance, Vaaler and Widmer [9] proved the conjecture for number fields with at least one real embedding.

In this note, we consider a somewhat different, but related problem. Suppose that $m \mid d$ is such that $K$ contains elements of degree $m$ over $\mathbb{Q}$. Let $\mathcal{O}_K \subset K$ be the ring of integers of $K$ and let $I \subseteq \mathcal{O}_K$ be an ideal in this ring. It is not difficult to see that $I$ contains infinitely many elements of degree $m$. We want to produce an upper bound on the height of the "smallest" (with respect to height) such element in $I$; naturally, we would expect this bound to depend on $d$, $\Delta_K$ and the norm of the ideal $I$, which we denote by $\mathbb{N}_K(I)$.

---

2020 *Mathematics Subject Classification.* Primary: 11G50, 11R04, 11R11.
*Key words and phrases.* number field, small height, ideal, primitive element.
Fukshansky was partially supported by the Simons Foundation grant #519058.

**Theorem 1.1.** *Suppose that the number field $K$ of degree $d = r_1 + 2r_2$ as above contains an element $\alpha$ of degree $m \mid d$ with $q_1$ real algebraic conjugates and $q_2$ complex pairs of complex algebraic conjugates. Then there exists such an $\alpha \in I$ with*

$$h(\alpha) \leq \left( \frac{d(d-3)+2m+4}{4} \right) \left( \frac{2^{\frac{d+m}{2}-q_1}}{\pi^{q_2}} \right) \mathbb{N}_K(I) \sqrt{|\Delta_K|}.$$

We review the necessary notation and technical tools in Section 2 and prove Theorem 1.1 in Section 3. Our main tools are Minkowski embedding, height-bounds inequalities, Minkowski's Successive Minima Theorem and a lemma on non-vanishing of polynomials in the spirit of Alon's Combinatorial Nullstellensatz. An immediate corollary of our main result upon taking $m = d$, $q_1 = r_1$ and $q_2 = r_2$ is an upper bound on the height of the smallest primitive element in a given ideal $I$, in the spirit of Ruppert's conjecture.

**Corollary 1.2.** *Let the notation be as above. Then there exists $\alpha \in I$ such that $K = \mathbb{Q}(\alpha)$ and*

$$h(\alpha) \leq \frac{d(d^2-d+4)}{4} \left( \frac{4}{\pi} \right)^{r_2} \mathbb{N}_K(I) \sqrt{|\Delta_K|}.$$

We show that the dependence of our bound on $|\Delta_K|$ is optimal, at least in the case of quadratic fields. In particular, it follows that if $K = \mathbb{Q}(\alpha)$ is an imaginary quadratic field and $\alpha \in \mathcal{O}_K$, then $h(\alpha) \gg |\Delta_K|^{1/2}$. On the other hand, Ruppert's conjecture (proved by Ruppert himself [7] in the quadratic case) asserts that there exists such $\alpha \in K$ with $h(\alpha) \ll |\Delta_K|^{1/4}$. It is unclear whether the dependence of our bound on $\mathbb{N}_K(I)$ is optimal. We produce the following bound for quadratic number fields.

**Theorem 1.3.** *Let $D$ be a squarefree integer and let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field. Let $I \subseteq \mathcal{O}_K$ be an ideal with the canonical basis $\{a, b + g\delta\}$, as described in* (11)*, so $b < a$. Let*

$$h_{\min}(I) = \min \{ h(\alpha) : \alpha \in I, K = \mathbb{Q}(\alpha) \}.$$

*If $D \not\equiv 1 (\operatorname{mod} 4)$, then*

$$\sqrt{ag} < h_{\min}(I) \leq g \left( b + \sqrt{|\Delta_K|/2} \right),$$

*and additionally $h_{\min}(I) > g\sqrt{|\Delta_K|/2}$ if $D < 0$.*
*If $D \equiv 1 (\operatorname{mod} 4)$, then*

$$\sqrt{ag} < h_{\min}(I) \leq g \left( \frac{(2b+1) + \sqrt{|\Delta_K|}}{2} \right),$$

*and additionally $h_{\min}(I) > g\sqrt{|\Delta_K|}/2$ if $D < 0$.*

To compare the bounds of Theorem 1.3 to that of Corollary 1.2, notice that

$$bg < ag = \begin{cases} \mathbb{N}_K(I) & \text{if } D \not\equiv 1 (\operatorname{mod} 4), \\ 2\mathbb{N}_K(I) & \text{if } D \equiv 1 (\operatorname{mod} 4). \end{cases}$$

We review all the necessary notation and prove Theorem 1.3 in Section 4.

Now, suppose that $K$ is a *totally real* number field, meaning that all of its embeddings are real; this is equivalent to the condition that $r_1 = d$ and $r_2 = 0$. An element $\alpha \in K$ is called *totally positive* if all of its algebraic conjugates are positive, i.e. $\sigma_j(\alpha) > 0$ for all $1 \leq j \leq d$. For an ideal $I \subseteq \mathcal{O}_K$, we can define its semigroup of totally positive elements as

$$I^+ = \{\alpha \in I : \sigma_j(\alpha) > 0 \ \forall \ 1 \leq j \leq d\}.$$

The investigation of elements of bounded height in $I^+$ has been initiated in [5]. Here we use the results of [5] to prove a bound on the smallest height of a primitive element in $I^+$.

**Theorem 1.4.** *Let the notation be as above. Then there exists $\alpha \in I^+$ such that $K = \mathbb{Q}(\alpha)$ and*

$$h(\alpha) \leq 3^d d^{\frac{3d+2}{2}} \frac{d(d-1)}{2} \left( \mathbb{N}_K(I) \sqrt{|\Delta_K|} \right)^{d+1}.$$

We prove Theorem 1.4 in Section 5. We are now ready to proceed.

## 2. Notation and heights

Continuing to set up the notation, notice that the space $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$ can be viewed as a subspace of

$$\left\{ (\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : y_{r_2+j} = \bar{y}_j \ \forall \ 1 \leq j \leq r_2 \right\} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \subset \mathbb{C}^d,$$

where in the last containment each copy of $\mathbb{R}$ is identified with the real part of the corresponding copy of $\mathbb{C}$. Then $K_{\mathbb{R}}$ is a $d$-dimensional Euclidean space with the bilinear form induced by the trace form on $K$:

$$\langle \alpha, \beta \rangle := \mathrm{Tr}_K(\alpha \bar{\beta}) \in \mathbb{R},$$

for every $\alpha, \beta \in K$, where $\mathrm{Tr}_K$ is the number field trace on $K$. We also define the sup-norm on $K_{\mathbb{R}}$ by

$$|\boldsymbol{x}| := \max\{|x_1|, \dots, |x_d|\},$$

for any $\boldsymbol{x} \in K_{\mathbb{R}}$, where $|x_j|$ stands for the usual absolute value of $x_j$ on $\mathbb{C}$. Let $\Sigma_K = (\sigma_1, \dots, \sigma_d) : K \hookrightarrow K_{\mathbb{R}}$ be the Minkowski embedding, then for any ideal $I \subseteq \mathcal{O}_K$ the image $\Sigma_K(I)$ is a lattice of full rank in $K_{\mathbb{R}}$. We define the determinant of a full-rank lattice to be the absolute value of the determinant of any basis matrix for the lattice, then

$$\det(\Sigma_K(I)) = \mathbb{N}_K(I) |\Delta_K|^{1/2}, \tag{1}$$

as follows, for instance, from Corollary 2.4 of [2]. More generally, for a lattice $L \subset K_{\mathbb{R}}$ of rank $m \leq d$ with a basis $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$, the determinant of $L$ is given by

$$\det(L) = \|\boldsymbol{x}_1 \wedge \dots \wedge \boldsymbol{x}_m\| = \det(X^\top X)^{1/2}, \tag{2}$$

where $X = (\boldsymbol{x}_1 \ \dots \ \boldsymbol{x}_m)$ is the corresponding basis matrix, $\| \ \|$ is the Euclidean norm on vectors over $K_{\mathbb{R}}$ and $\wedge$ stands for the wedge-product of vectors: the wedge product $\boldsymbol{x}_1 \wedge \dots \wedge \boldsymbol{x}_m$ is identified with the vector of Grassmann coordinates of the matrix $X$ under the lexicographic embedding into $\mathbb{C}^{\binom{d}{m}}$. The second equality in (2) is a consequence of the Laplace identity (see [8], p.15). We have the following useful technical lemma, which is a direct consequence of Lemma 8A on p.28 of [8].

**Lemma 2.1.** *Let $L = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_m\}$ be as above. Let $V \subset K_{\mathbb{R}}$ be a $k$-dimensional rational subspace with a basis $\boldsymbol{y}_1, \dots, \boldsymbol{y}_k$ consisting of vectors with integer relatively prime coordinates. If $L \cap V \neq \{\boldsymbol{0}\}$, then it is a lattice and*

$$\det(L \cap V) \leq \det(L)\|\boldsymbol{y}_1 \wedge \cdots \wedge \boldsymbol{y}_k\|.$$

Next we normalize absolute values and introduce the standard height function. Let us write $M(K)$ for the set of places of $K$. For each $v \in M(K)$ let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree, then for each $u \in M(\mathbb{Q})$, $\sum_{v|u} d_v = d$. We select the absolute values so that $|\ |_v$ extends the usual archimedean absolute value on $\mathbb{Q}$ when $v \mid \infty$, or the usual $p$-adic absolute value on $\mathbb{Q}$ when $v \nmid \infty$. With this choice, the product formula reads

$$\prod_{v \in M(K)} |\alpha|_v^{d_v} = 1,$$

for each nonzero $\alpha \in K$. We define the multiplicative Weil height on algebraic vectors $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in K^n$ as

$$h(\boldsymbol{\alpha}) = \prod_{v \in M(K)} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}^{\frac{d_v}{d}},$$

for all $n \geq 1$. This height is absolute, meaning that it is the same when computed over any number field $K$ containing $\alpha_1, \dots, \alpha_n$: this is due to the normalizing exponent $1/d$ in the definition. Hence we can compute height for points defined over $\overline{\mathbb{Q}}$.

We will need a few technical lemmas. The first is a well-known property of heights, which can be found, for instance, as Lemma 2.1 of [4].

**Lemma 2.2.** *Let $\xi_1, \dots, \xi_m \in \overline{\mathbb{Q}}$ and $\boldsymbol{x}, \dots, \boldsymbol{x}_m \in \overline{\mathbb{Q}}^n$ for $m, n \geq 1$. Then*

$$h\left(\sum_{j=1}^m \xi_j \boldsymbol{x}_j\right) \leq m h(\boldsymbol{\xi}) \prod_{j=1}^m h(\boldsymbol{x}_j),$$

*where $\boldsymbol{\xi} = (\xi_1, \dots, \xi_m)$.*

Next is Lemma 4.1 of [5]: while in that paper the lemma is stated for totally real fields, its proof holds verbatim for any number field with our definition of Minkowski embedding $\Sigma_K$.

**Lemma 2.3.** *For any $\alpha \in \mathcal{O}_K$,*

$$1 \leq h(\alpha) \leq |\Sigma_K(\alpha)|,$$

*where $|\ |$ stands for the sup-norm on $K_{\mathbb{R}}$, as above.*

We also revisit the important principle that a polynomial that is not identically zero cannot vanish "too much". There are several versions of this principle in the literature, including Alon's celebrated Combinatorial Nullstellensatz [1]. The following formulation, which is most convenient for our purposes follows easily from Theorem 4.2 of [4].

**Lemma 2.4.** *Let $F$ be a field, $n \geq 1$ and integer and $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in F^n$ be linearly independent vectors, $1 \leq m \leq n$. Let $P(\boldsymbol{x}) := P(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ be a* *polynomial which is not identically zero with* $m := \deg P \geq 1$. *Let* $S_1, \dots, S_m \subset F$ *be sets with cardinalities* $|S_j| \geq m+1$ *for every* $j$. *Then there exists a point*

$$\boldsymbol{\xi} = (\xi_1, \dots, \xi_m) \in S_1 \times \cdots \times S_m,$$

*such that* $P\left(\sum_{j=1}^{m} \xi_j \boldsymbol{v}_i\right) \neq 0$.

## 3. Proof of Theorem 1.1

Suppose that the number field $K$ has elements of degree $m$ for some $1 < m < d$, then $m$ must be a divisor of $d$. In this case, there must exist elements of degree $m$ in every ideal $I \subset \mathcal{O}_K$. Indeed, for every $\alpha \in K$ there exists a $t_\alpha \in \mathbb{Z}$ such that $t_\alpha \alpha \in \mathcal{O}_K$ and then $\mathbb{N}_K(I) t_\alpha \alpha \in I$, while $\deg(\mathbb{N}_K(I) t_\alpha \alpha) = \deg(\alpha)$ since $\mathbb{N}_K(I) t_\alpha \in \mathbb{Z}$. Fix an ideal $I \subset \mathcal{O}_K$ and let $\alpha \in I$ have degree $m$, then $\alpha$ has precisely $m$ distinct algebraic conjugates. In other words, precisely $m$ of the coordinates of the vector $\Sigma_K(\alpha)$ are distinct, meaning that $\alpha$ satisfies a system of $d-m$ equations

$$\sigma_{i_k}(\alpha) = \sigma_{j_k}(\alpha), \ \forall\ 1 \leq k \leq d-m, \tag{3}$$

for some collection of distinct indices $\{i_1, \dots, i_{d-m}\} \subset \{1, \dots, d\}$ and possibly repeating indices

$$\{j_1, \dots, j_{d-m}\} \subset \{1, \dots, d\} \setminus \{i_1, \dots, i_{d-m}\}.$$

For this choice of indices,

$$V = \{\boldsymbol{x} \in K_{\mathbb{R}} : x_{i_k} = x_{j_k}\ \forall\ 1 \leq k \leq d-m\}$$

be an $m$-dimensional subspace of $K_{\mathbb{R}}$. Then $L_K(I,V) := \Sigma_K(I) \cap V$ is a lattice of full rank in $V$, since for every $\Sigma(\alpha) \in V$,

$$\Sigma_K(\mathbb{N}_K(I) t_\alpha \alpha) = \mathbb{N}_K(I) t_\alpha \Sigma_K(\alpha) \in L_K(I,V).$$

For each $1 \leq k \leq d-m$ define $J_k = \{i : \sigma_i(\alpha) = \sigma_{i_k}(\alpha)\}$. Write $\boldsymbol{e}_i$ for the $i$-th standard basis vector, and notice that the collection of distinct vectors among

$$\left\{\boldsymbol{e}_{j_k} + \sum_{i \in J_k} \boldsymbol{e}_i : 1 \leq k \leq d-m\right\} \cup \{\boldsymbol{e}_\ell : \ell \in \{1, \dots, d\} \setminus \{i_1, j_1, \dots, i_{d-m}, j_{d-m}\}\}$$

forms an integral relatively prime basis for $V$. For example, if $d = 5$, $m = 3$ and the system (3) looks like

$$\sigma_1(\alpha) = \sigma_2(\alpha),\ \sigma_3(\alpha) = \sigma_2(\alpha),$$

then $\{i_1, i_2\} = \{1, 3\}$, $\{j_1, j_2\} = \{2, 2\}$, $J_1 = J_2 = \{1, 3\}$, and

$$\{\boldsymbol{e}_2 + \boldsymbol{e}_1 + \boldsymbol{e}_3, \boldsymbol{e}_4, \boldsymbol{e}_5\}$$

is a basis for $V$.

Let us write $\boldsymbol{y}_1, \dots, \boldsymbol{y}_m$ for these basis vectors and $G(V)$ for their wedge product, viewed as a vector in $\mathbb{C}^{\binom{d}{m}}$. Then Lemma 2.1 implies that

$$\det(L_K(I,V)) \leq \det(\Sigma_K(I)) \|G(V)\|. \tag{4}$$

Now, Lemma 5F(i) of [8] implies that

$$\|G(V)\| \leq \prod_{i=1}^{m} \|\boldsymbol{y}_i\|,$$

and if some $\boldsymbol{y}_i$ is a sum of, say, $t \geq 2$ distinct standard basis vectors, then

$$\|\boldsymbol{y}_i\| = \sqrt{t} \leq 2^{\frac{t-1}{2}}.$$

For instance, in our example above, $\|\boldsymbol{e}_2 + \boldsymbol{e}_1 + \boldsymbol{e}_3\| = \sqrt{3} < 2^{\frac{3-1}{2}} = 2$. Combining these observations with (4) and (1), we see that

$$\det(L_K(I,V)) \leq 2^{\frac{d-m}{2}} \mathbb{N}_K(I) |\Delta_K|^{1/2}. \tag{5}$$

Let $S$ be the set of $d-m$ pairs of indices $(i_k, j_k)$ for which (3) holds, and define a polynomial

$$P_S(x_1, \dots, x_d) = \prod_{\substack{a \neq b \\ (a,b) \notin S}} (x_a - x_b) \in K[x_1, \dots, x_d]. \tag{6}$$

This polynomial has degree $\binom{d}{2} - |S| = \frac{d(d-3)+2m}{2}$ and we see that if $\Sigma_K(\alpha) \in L_K(I,V)$ is such that

$$P_S\left(\Sigma_K(\alpha)\right) \neq 0,$$

then $\alpha \in I$ has degree $m$. Since such $\Sigma_K(\alpha) \in L_K(I,V)$ must exist, the polynomial $P_S$ does not vanish identically on the lattice $L_K(I,V)$.

Notice that in equation (3), embeddings on different sides of the equality are either both real or both complex for each given $k$. Further, if $\sigma_{i_k}(\alpha) = \sigma_{j_k}(\alpha)$ for some $k$, then $\bar{\sigma}_{i_k}(\alpha) = \bar{\sigma}_{j_k}(\alpha)$, thus equations corresponding to complex embeddings in (3) come in conjugate pairs. Let $s_1$ be the number of equations with real embeddings in (3) and $s_2$ be the number of conjugate pairs of equations with complex embeddings. Then

$$d - m = s_1 + 2s_2,$$

and every $\alpha \in K$ that satisfies (3) has $q_1 = r_1 - s_1$ distinct real algebraic conjugates and $q_2 = r_2 - s_2$ distinct complex conjugate pairs of complex algebraic conjugates. Define the set

$$U = \left\{ \boldsymbol{x} \in V : |\boldsymbol{x}| \leq 1 \right\},$$

which is the Cartesian product of $q_1$ intervals $[-1,1]$ and $q_2$ circles of radius 1. Hence, $U$ is a convex $\mathbf{0}$-symmetric set with $m$-dimensional volume

$$\operatorname{Vol}_m(U) = 2^{q_1} \pi^{q_2}.$$

Let $\lambda_1, \dots, \lambda_m$ be the successive minima of $U$ with respect to the lattice $L_K(I,V)$ in $V$. Let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in L_K(I,V)$ be vectors corresponding to these successive minima, respectively. Then, by Minkowski's Successive Minima Theorem (see, for instance [6], Section 9.1, Theorem 1) combined with (5), we have

$$\prod_{j=1}^m |\boldsymbol{v}_j| = \prod_{j=1}^m \lambda_j \leq \frac{2^m \det(L_K(I,V))}{\operatorname{Vol}_m(U)} \leq \left( \frac{2^{\frac{d+m}{2} - q_1}}{\pi^{q_2}} \right) \mathbb{N}_K(I) |\Delta_K|^{1/2}. \tag{7}$$

Also, notice that if $\boldsymbol{x} \in \Sigma_K(I)$ then $\boldsymbol{x} = (\sigma_1(\alpha), \dots, \sigma_d(\alpha))$ for some $\alpha \in I$. Then

$$1 = \prod_{v \in M(K)} |\alpha|_v^{d_v} = \prod_{v \nmid \infty} |\alpha|_v^{d_v} \times \prod_{j=1}^d |\sigma_j(\alpha)| \leq \prod_{j=1}^d |\sigma_j(\alpha)|,$$

since $\alpha \in \mathcal{O}_K$, and so $|\alpha|_v \leq 1$ for each $v \nmid \infty$. This implies that

$$|\boldsymbol{x}| = \max_{1 \leq j \leq d} |\sigma_j(\alpha)| \geq 1. \tag{8}$$

Now, let $c := \frac{d(d-3)+2m}{2}$ and define $T_1 := \{-[c/2]-1,\dots,[c/2]+1\}$, where $[\ ]$ stands for integer part. Then $|T_1| \geq c+1$ and for every $\boldsymbol{\xi} \in T := T_1^m$, $|\boldsymbol{\xi}| \leq c/2+1$. Lemma 2.4 guarantees that there exists $\boldsymbol{\xi} \in T$ such that the polynomial $P_S$ does not vanish at the point

$$\boldsymbol{v}(\boldsymbol{\xi}) := \sum_{j=1}^{m} \xi_j \boldsymbol{v}_j \in L_K(I,V).$$

Notice that

$$|\boldsymbol{v}(\boldsymbol{\xi})| \leq m \left( \max_{1\leq j\leq m} |\xi_j| \right) \left( \max_{1\leq j\leq m} |\boldsymbol{v}_j| \right) \leq \left( \frac{d(d-3)+2m+4}{4} \right) \prod_{j=1}^{d} |\boldsymbol{v}_j|, \tag{9}$$

by (8). Let $\alpha \in I$ be such that $\Sigma_K(\alpha) = \boldsymbol{v}(\boldsymbol{\xi})$. Then, combining (9) with (7) and Lemma 2.3 yields Theorem 1.1.

## 4. Quadratic fields

In this section we review the necessary notation and prove Theorem 1.3. First notice that for any number field $K$ and $\alpha \in \mathcal{O}_K$,

$$h(\alpha) = \prod_{v|\infty} \max\{1, |\alpha|_v\}^{\frac{d_v}{d}} \geq \left( \prod_{v|\infty} |\alpha|_v^{d_v} \right)^{\frac{1}{d}} = \left( \prod_{j=1}^{d} |\sigma_j(\alpha)| \right)^{\frac{1}{d}} = \mathbb{N}_K(\alpha)^{\frac{1}{d}}.$$

Now let $D$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field. Let $I \subseteq \mathcal{O}_K$ be an ideal. Then there exists a unique integral basis $a, b+g\delta$ for $I$, called the canonical basis, where

$$\delta = \begin{cases} -\sqrt{D} & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \not\equiv 1 (\operatorname{mod} 4) \\ \frac{1-\sqrt{D}}{2} & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \equiv 1 (\operatorname{mod} 4), \end{cases} \tag{10}$$

and $a, b, g \in \mathbb{Z}_{\geq 0}$ such that

$$b < a,\ \ g \mid a, b,\ \text{ and } ag \mid \mathbb{N}_K(b+g\delta), \tag{11}$$

see Section 6.3 of [3] for further details. The embeddings $\sigma_1, \sigma_2 : K \to \mathbb{C}$ are given by

$$\sigma_1(x+y\sqrt{D}) = x+y\sqrt{D},\ \ \sigma_2(x+y\sqrt{D}) = x-y\sqrt{D}$$

for each $x+y\sqrt{D} \in K$, where $D$ being positive or negative is determined by whether $K$ is a real or an imaginary quadratic field, respectively. The number field norm on $K$ is given by

$$\mathbb{N}_K(x+y\sqrt{D}) = \sigma_1(x+y\sqrt{D})\sigma_2(x+y\sqrt{D}) = \left(x+y\sqrt{D}\right)\left(x-y\sqrt{D}\right).$$

The discriminant of $K$ is

$$\Delta_K = \begin{cases} 4D & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \not\equiv 1 (\operatorname{mod} 4) \\ D & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \equiv 1 (\operatorname{mod} 4), \end{cases} \tag{12}$$

and the norm of the ideal $I$ as above is

$$\mathbb{N}_K(I) = \begin{cases} ag & \text{if } D \not\equiv 1 (\operatorname{mod} 4), \\ ag/2 & \text{if } D \equiv 1 (\operatorname{mod} 4). \end{cases} \tag{13}$$

Observe that an ideal $I$ as above can be written as $I = gJ$ for the corresponding ideal $J = \frac{1}{g} I \subseteq \mathcal{O}_K$, since $g \mid a, b$. Hence we start by restricting our consideration to ideals with $g = 1$. Then the bound of Corollary 1.2 in the case of a quadratic field can be written as

$$\sqrt{\mathbb{N}_K(\alpha)} \leq h(\alpha) \ll_d a\sqrt{|D|}. \tag{14}$$

We will show that in this case the power on $\sqrt{D}$ cannot in general be reduced. First observe that an element $\alpha \in I$ is primitive if and only if it is of the form

$$\alpha = xa + y(b + \delta)$$

with $x, y \in \mathbb{Z}$ and $y \neq 0$.

*Case 1:* Suppose $D \in \mathbb{Z}$ is squarefree, $D \not\equiv 1 \pmod 4$ and $K = \mathbb{Q}(\sqrt{D})$. Then $K$ is a real quadratic if $D > 0$ and $K$ is an imaginary quadratic if $D < 0$. Take an ideal

$$I = \operatorname{span}_{\mathbb{Z}}\{a, b - \sqrt{D}\} \subset \mathcal{O}_K$$

with $a \mid \mathbb{N}_K(b - \sqrt{D}) = |b^2 - D|$. Then

$$\begin{aligned} \mathbb{N}_K(\alpha) &= \left|\left(xa + y(b - \sqrt{D})\right)\left(xa + y(b + \sqrt{D})\right)\right| \\ &= \left|x^2a^2 + 2xyab + y^2(b^2 - D)\right| = a\left|x^2a + 2xyb + y^2\left(\frac{b^2 - D}{a}\right)\right| > a, \end{aligned} \tag{15}$$

where $(b^2 - D)/a \in \mathbb{Z}$. Further,

$$\mathbb{N}_K(\alpha) = \left|x^2a^2 + 2xyab + y^2(b^2 - D)\right| = \left|(xa + yb)^2 - y^2D\right| > |D|, \tag{16}$$

if $D < 0$. On the other hand,

$$\begin{aligned} h(\alpha) &= \prod_{v \in M(K)} \max\{1, |\alpha|_v\}^{\frac{d_v}{2}} = \prod_{v|\infty} \max\{1, |\alpha|_v\}^{\frac{d_v}{2}} = \left(\prod_{j=1}^{2} \max\{1, |\sigma_i(\alpha)|\}\right)^{\frac{1}{2}} \\ &\leq \frac{1}{2}\left(\max\{1, |\sigma_1(\alpha)|\} + \max\{1, |\sigma_2(\alpha)|\right) \leq \frac{1}{2}\left(2 \cdot \max\{|\sigma_1(\alpha)|, |\sigma_2(\alpha)|\}\right) \\ &= \max\{|\sigma_1(\alpha)|, |\sigma_2(\alpha)|\} = \max\left\{\left|(xa + yb) - y\sqrt{D}\right|, \left|(xa + yb) + y\sqrt{D}\right|\right\} \\ &\leq |x|a + |y|b + |y|\sqrt{|D|}. \end{aligned}$$

Taking the minimum over all primitive elements $\alpha \in I$, we see that

$$\begin{aligned} \min\{h(\alpha) : \alpha \in I, K = \mathbb{Q}(\alpha)\} &\leq \min\{|x|a + |y|b + |y|\sqrt{|D|} : x, y \in \mathbb{Z}, y \neq 0\} \\ &\leq b + \sqrt{|D|}, \end{aligned} \tag{17}$$

where the last inequality is obtained by taking $x = 0$, $y = 1$. Putting together (14), (15), (16) and (17), we obtain the $D \not\equiv 1 (\bmod 4)$ case of Theorem 1.3 in case $g = 1$.

*Case 2:* Suppose $D \in \mathbb{Z}$ is squarefree, $D \equiv 1 \pmod 4$ and $K = \mathbb{Q}(\sqrt{D})$. Again, $K$ is a real quadratic if $D > 0$ and $K$ is an imaginary quadratic if $D < 0$. Take an ideal

$$I = \operatorname{span}_{\mathbb{Z}}\left\{a, b + \frac{1 - \sqrt{D}}{2}\right\} \subset \mathcal{O}_K$$

with $a \mid \mathbb{N}_K\left(\frac{(2b+1)-\sqrt{D}}{2}\right) = \frac{|(2b+1)^2-D|}{4} = \left|b^2+b-\frac{D-1}{4}\right|$. Then

$$\begin{aligned} \mathbb{N}_K(\alpha) &= \left|\left(xa+y\left(b+\frac{1-\sqrt{D}}{2}\right)\right)\left(xa+y\left(b+\frac{1+\sqrt{D}}{2}\right)\right)\right| \\ &= \left|x^2a^2+(2b+1)axy+y^2\left(b^2+b-\frac{D-1}{4}\right)\right| \\ &= a\left|x^2a+(2b+1)xy+\frac{y^2}{a}\left(b^2+b-\frac{D-1}{4}\right)\right| > a, \qquad (18) \end{aligned}$$

where $\frac{1}{a}\left(b^2+b-\frac{D-1}{4}\right) \in \mathbb{Z}$. Further,

$$\mathbb{N}_K(\alpha) = \left|x^2a^2+(2b+1)axy+y^2(b^2+b+1/4)-y^2D/4\right| > |D|/4, \qquad (19)$$

if $D < 0$. On the other hand,

$$\begin{aligned} h(\alpha) &\leq \max\{|\sigma_1(\alpha)|, |\sigma_2(\alpha)|\} \\ &= \max\left\{\left|xa+y\left(b+\frac{1-\sqrt{D}}{2}\right)\right|, \left|xa+y\left(b+\frac{1+\sqrt{D}}{2}\right)\right|\right\} \\ &\leq |x|a+\frac{|y|(2b+1)}{2}+\frac{|y|\sqrt{|D|}}{2}. \end{aligned}$$

Taking the minimum over all primitive elements $\alpha \in I$, we see that

$$\min\{h(\alpha) : \alpha \in I, K = \mathbb{Q}(\alpha)\} \leq \frac{(2b+1)+\sqrt{|D|}}{2}, \qquad (20)$$

where the inequality is obtained by taking $x = 0$, $y = 1$. Putting together (14), (18), (19) and (20), we obtain the $D \equiv 1 (\mathrm{mod}\, 4)$ case of Theorem 1.3 in case $g = 1$.

*Proof of Theorem 1.3.* Let $I$ be an ideal with the canonical basis $\{a, b+g\delta\}$ and $J = \frac{1}{g}I$. Then for any $\alpha \in J$ and the corresponding $g\alpha \in I$,

$$h(g\alpha) = \left(\prod_{j=1}^{2}\max\{1, |\sigma_i(g\alpha)|\}\right)^{\frac{1}{2}} \leq g\left(\prod_{j=1}^{2}\max\{1, |\sigma_i(\alpha)|\}\right)^{\frac{1}{2}} = gh(\alpha).$$

Further, $\mathbb{N}_K(I) = g\mathbb{N}_K(J)$. Take $\alpha \in J$ be a primitive element of bounded height as obtained above in Cases 1 and 2, then $g\alpha \in I$ is also a primitive element and the result follows. □

## 5. Proof of Theorem 1.4

The argument here is similar to the proof of Theorem 1.1 in Section 3 above, however instead of the Successive Minima Theorem we use a result from [5]. Specifically, Theorem 1.3 of [5] asserts that there exist $\mathbb{Q}$-linearly independent elements $\beta_1, \dots, \beta_d \in I^+$ such that

$$\prod_{j=1}^{d} h(\beta_j) \leq \left(3d\sqrt{d}\right)^d \left(\mathbb{N}_K(I)\sqrt{|\Delta_K|}\right)^{d+1}. \qquad (21)$$

Notice that for any integers $\xi_1, \dots, \xi_d \geq 0$, we have

$$\alpha(\boldsymbol{\xi}) := \sum_{j=1}^{d} \xi_j \beta_j \in I^+,$$

where $\boldsymbol{\xi} = (\xi_1, \dots, \xi_d)$. As in Section 3, let $m = \frac{d(d-1)}{2}$ and define the set $T_1 := \{0, \dots, m\}$, so that $|T_1| = m+1$ and for each $\boldsymbol{\xi} \in T := T_1^d$, $|\boldsymbol{\xi}| \leq m$. Again, Lemma 2.4 guarantees that there exists $\boldsymbol{\xi}^* \in T$ such that the polynomial

$$P(x_1, \dots, x_d) = \prod_{j \neq k} (x_j - x_k) \in K[x_1, \dots, x_d]$$

of degree $\binom{d}{2} = \frac{d(d-1)}{2}$ does not vanish at the point

$$\Sigma_K\left(\alpha(\boldsymbol{\xi}^*)\right) = \left( \sum_{j=1}^{d} \xi_j^* \sigma_1(\beta_j), \dots, \sum_{j=1}^{d} \xi_j^* \sigma_d(\beta_j) \right).$$

This means that $\alpha(\boldsymbol{\xi}^*) \in I^+$ is a primitive element. Now, combining Lemma 2.2 with (21), we obtain:

$$\begin{aligned} h(\alpha(\boldsymbol{\xi}^*)) &= h\left( \sum_{j=1}^{d} \xi_j^* \beta_j \right) \leq d h(\boldsymbol{\xi}^*) \prod_{j=1}^{d} h(\beta_j) \\ &\leq 3^d d^{\frac{3d+2}{2}} \frac{d(d-1)}{2} \left( \mathbb{N}_K(I) \sqrt{|\Delta_K|} \right)^{d+1}, \end{aligned} \tag{22}$$

since $\boldsymbol{\xi}^* \in \mathbb{Z}^d$, and so $h(\boldsymbol{x}^*) \leq |\boldsymbol{\xi}^*| \leq \frac{d(d-1)}{2}$. This yields Theorem 1.4.

## References


[1] N. Alon. Combinatorial Nullstellensatz. *Combin. Probab. Comput.*, 8 (1999), no. 1-2, pp. 7–29.
[2] E. Bayer Fluckiger. Upper bounds for Euclidean minima of algebraic number fields. *J. Number Theory*, 121 (2006), no. 2, pp. 305–323.
[3] D. A. Buell. Binary Quadratic Forms. Springer-Verlag, 1989.
[4] L. Fukshansky. Algebraic points of small height missing a union of varieties. *J. Number Theory*, 130 (2010), no. 10, pp. 2099–2118.
[5] L. Fukshansky and S. Wang. Positive semigroups in lattices and totally real number fields. *Adv. Geom.*, 22 (2022), no. 4, pp. 503–512.
[6] P. M. Gruber and C. G. Lekkerkerker. Geometry of Numbers. North-Holland Publishing Co., 1987.
[7] W. M. Ruppert. Small generators of number fields. *Manuscripta Math.*, 96 (1998), no. 1, pp. 17–22.
[8] W. M. Schmidt. Diophantine approximations and Diophantine equations. Lecture Notes in Mathematics, 1467. Springer-Verlag, Berlin, 1991.
[9] J. D. Vaaler and M. Widmer. A note on generators of number fields. Diophantine methods, lattices, and arithmetic theory of quadratic forms, *Contemp. Math.*, 587 (2013), Amer. Math. Soc., Providence, RI, pp. 201–211.



Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711
*Email address*: `lenny@cmc.edu`

Institute of Mathematical Sciences, Claremont Graduate University, Claremont, CA 91711
*Email address*: `sehun.jeong@cgu.edu`