NORMAL BASES OF SMALL HEIGHT IN GALOIS NUMBER FIELDS

LENNY FUKSHANSKY AND SEHUN JEONG

ABSTRACT. Let K be a number field of degree d so that $K/\mathbb{Q}$ is a Galois extension. The *normal basis theorem* states that K has a $\mathbb{Q}$-basis consisting of algebraic conjugates, in fact K contains infinitely many such bases. We prove an effective version of this theorem, obtaining a normal basis for $K/\mathbb{Q}$ of bounded Weil height with an explicit bound in terms of the degree and discriminant of K. In the case when d is prime, we obtain a particularly good bound using a different method.

1. INTRODUCTION AND STATEMENT OF RESULTS

Let K be a number field of degree $d = [K : \mathbb{Q}] \geq 1$ and $\mathcal{O}_K$ its ring of integers. An element $\theta \in K$ is called *primitive* if $K = \mathbb{Q}(\theta)$. This is equivalent to the condition that $\deg_{\mathbb{Q}}(\theta) = d$, and hence, there are infinitely many primitive elements in K. A conjecture of Ruppert [13] (also see [14] for the convenient formulation we are using) asserts that there exists a primitive element $\theta \in K$ such that

$$(1) \qquad h(\theta) \leq c(d)|\Delta_K|^{\frac{1}{2d}},$$

where h is the absolute Weil height, Δ_K is the discriminant of the number field K, and $c(d)$ is a constant depending only on the degree d; we review all the necessary notation in Section 2. 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 [14] proved the conjecture for number fields with at least one real embedding (further results in the case of totally complex fields were just recently obtained in [1]). More generally, a slightly weaker bound is obtained by Pazuki and Widmer in [12, Lemma 7.1]:

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

where θ can be taken in $\mathcal{O}_K$. If θ is a primitive element, then $1, \theta, \ldots, \theta^{d-1}$ is a basis for K as a $\mathbb{Q}$-vector space. Hence, Ruppert's conjecture implies the existence of such a basis with

$$(3) \qquad \max_{0 \leq k \leq d-1} h(\theta^k) \leq c(d)^{d-1}|\Delta_K|^{\frac{d-1}{2d}}.$$

Consider the situation when $K/\mathbb{Q}$ is a Galois extension. In that case, there exists a *normal basis* for K over $\mathbb{Q}$, i.e. a basis consisting of algebraic conjugates $\beta_1, \ldots, \beta_d$; in fact, there are infinitely many such bases (this fact is known as the *normal basis theorem*, usually attributed to the works of Noether and Deuring, 1932). On the other hand, if β_1 is just an arbitrary primitive element for K, its

---

algebraic conjugates may be linearly dependent, and so not every primitive element gives rise to a normal basis. Indeed, it may happen for instance that the degree-d minimal polynomial of β_1 has zero coefficient in front of x^{d-1}, which implies that

$$\beta_1 + \cdots + \beta_d = 0.$$

It is then natural to ask for a normal basis of bounded height. The first simple observation about quadratic fields follows directly from Ruppert's bound.

Proposition 1.1. *Let $K/\mathbb{Q}$ be a quadratic extension. Then there exists a normal basis $\beta_1, \beta_2 \in K$ with*

$$h(\beta_i) \leq c(2)|\Delta_K|^{\frac{1}{4}},$$

for $i = 1, 2$, where $c(2)$ is as in (1).

We give a quick proof of this proposition in Section 2. Our first main result produces a general bound for any Galois extension $K/\mathbb{Q}$.

Theorem 1.2. *Let $K/\mathbb{Q}$ be a Galois extension of degree $d \geq 2$. There exists a normal basis $\beta_1, \ldots, \beta_d$ for K over $\mathbb{Q}$ so that*

$$h(\beta_i) \leq \frac{d^{4d}(d^2 - d + 2)^{4d-3}}{2} \left(\frac{d-1}{[(d-1)/2]} \right)^2 |\Delta_K|^{(d-1)(4d-3)},$$

for all $1 \leq i \leq d$.

Our argument for the proof of this theorem follows the standard proof of the *normal basis theorem*. We are using the Pazuki and Widmer bound (2), a polynomial non-vanishing principle (Lemma 2.4) along with some standard inequalities on height and Mahler measure to make this argument effective. We present our proof in Section 3. In the case when d is an odd prime, we can obtain a better bound using a completely different approach.

Theorem 1.3. *Let $K/\mathbb{Q}$ be a Galois extension of prime degree $d \geq 3$. There exists an integral normal basis $\beta_1, \ldots, \beta_d$ for K over $\mathbb{Q}$ so that*

$$h(\beta_i) \leq |\Delta_K|^{1/2},$$

for all $1 \leq i \leq d$.

We prove Theorem 1.3 in Section 4. Our argument is based on a result of Dubickas [7] on linear independence of algebraic conjugates of prime degree and Minkowski's *successive minima theorem*.

It is worth mentioning that our approach in the proofs of Theorems 1.2 and 1.3 utilizes the Diophantine avoidance method, i.e., obtaining effective height-bounds for points *not* satisfying some algebraic conditions. Such avoidance ideas are naturally embedded in the proofs of some classical theorems in algebraic number theory, such as the *primitive element theorem* and the *normal basis theorem*. While most points do not satisfy any given polynomial equation, explicitly identifying such a point may require some work; it is the "searching for hay in a haystack" problem. We are ready to proceed.

2. Notation and heights

Throughout this paper, we work over a Galois number field K of degree $d \geq 2$ over $\mathbb{Q}$ and write $\mathcal{O}_K$ for its ring of integers. Let $\sigma_1, \ldots, \sigma_d : K \hookrightarrow \mathbb{C}$ be the embeddings of K. Since $K/\mathbb{Q}$ is Galois, K is either totally real or totally imaginary, meaning that either all of the embeddings are real or all of them are complex coming in conjugate pairs.

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 $v \nmid \infty$. Then archimedean places are in bijective correspondence with the embeddings so that for each $v \mid \infty$ there exists an index $1 \leq j \leq d$ with

$$|\alpha|_v = |\sigma_j(\alpha)|,$$

for each $\alpha \in K$, where $|\ |$ is the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$ (notice that each conjugate pair of complex embeddings induces the same place). With this normalization 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 numbers $\alpha \in K$ as

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

and notice that $h(\alpha) = \prod_{v|\infty} \max\{1, |\alpha|_v\}^{d_v/d}$ if $\alpha \in \mathcal{O}_K$. This height is absolute, meaning that it is the same when computed over any number field K containing α: this is due to the normalizing exponent $1/d$ in the definition. Hence, we can compute height for elements of $\overline{\mathbb{Q}}$.

We review some useful well-known properties of heights. The first can be found, for instance, as Lemma 2.1 of [9].

Lemma 2.1. *Let $\xi_1, \ldots, \xi_m \in \mathbb{Z}$ and $\alpha_1, \ldots, \alpha_m \in \overline{\mathbb{Q}}$ for $m \geq 1$. Then*

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

where $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ and $|\boldsymbol{\xi}| := \max\{|\xi_i| : 1 \leq i \leq m\}$.

Define *Mahler measure* of a polynomial $f(x) = \sum_{k=0}^d a_k x^k \in \mathbb{C}[x]$ of degree d with roots $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ to be

$$\mu(f) = |a_d| \prod_{k=1}^d \max\{1, |\alpha_k|\}.$$

The next lemma is Proposition 1.6.6 of [5].

Lemma 2.2. *Let $\alpha \in \overline{\mathbb{Q}}$ have degree d and let $f(x) \in \mathbb{Z}[x]$ be its minimal polynomial. Then*

$$\mu(f) = h(\alpha)^d.$$

Further, write $|f| = \max_{0 \le n \le d} |a_d|$, then Lemma 1.6.7 of [5] provides the following bound.

Lemma 2.3. *Write [ ] for the integer part function, then*

$$|f| \le \binom{d}{[d/2]} \mu(f),$$

for any $f(x) \in \mathbb{C}[x]$.

The next lemma quantifies the basic principle that a polynomial which is not identically zero cannot vanish "too much". Somewhat different formulations of this principle can be found in [6] (Lemma 1 on p. 261) as well as in the context of N. Alon's celebrated Combinatorial Nullstellensatz [2]. The following formulation, which is most convenient for our purposes follows easily from Lemma 2.2 of [8].

Lemma 2.4. *Let K be a number field as above and $P(\boldsymbol{x}) \in K[x_1, \dots, x_n]$ be a polynomial of degree m in n variables which is not identically 0. There exists a point $\boldsymbol{\xi} \in \mathbb{Z}^n$ such that $P(\boldsymbol{\xi}) \ne 0$ and*

$$|\boldsymbol{\xi}| \le \frac{m+2}{2}.$$

In case K is totally real, we define the Minkowski embedding $\Sigma_K = (\sigma_1, \dots, \sigma_d) : K \hookrightarrow \mathbb{R}^d$, then for any ideal $I \subseteq \mathcal{O}_K$ the image $\Sigma_K(I)$ is a lattice of full rank in $\mathbb{R}^d$. 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

$$(4) \qquad\qquad \det(\Sigma_K(I)) = \mathbb{N}_K(I)|\Delta_K|^{1/2},$$

where $\mathbb{N}_K(I) := |\mathcal{O}_K/I|$ is the norm of I, as follows, for instance, from Corollary 2.4 of [4]. The following property is Lemma 4.1 of [10].

Lemma 2.5. *For any $\alpha \in \mathcal{O}_K$,*

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

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

We finish this section with a proof of Ruppert's bound on the height of a normal basis in the quadratic case.

Proof of Proposition 1.1. Let $K = \mathbb{Q}(\sqrt{D})$ for a nonzero squarefree integer $D \ne 1$. A result of Ruppert [13] guarantees the existence of a primitive element $\theta \in K$ satisfying (1), i.e.

$$h(\theta) \le c(2)|\Delta_K|^{\frac{1}{4}},$$

for an absolute constant $c(2)$. Then $\theta = a + b\sqrt{D}$ for some $a, b \in \mathbb{Q}$. Suppose that $a = 0$ and $b = m/n$ for some relatively prime integers m, n, then the minimal polynomial of θ is $f(x) = n^2 x^2 - Dm^2$ and, by Lemma 2.2, we have

$$h(\theta) = \mu(f)^{1/2} = |n| \max\{1, |m||\sqrt{D}|/|n|\} \ge |\sqrt{D}| = c|\Delta_K|^{1/2},$$

for an absolute constant c. This implies that we must have $a \ne 0$, in which case $a \pm b\sqrt{D}$ is the desired normal basis. $\square$

3. Proof of Theorem 1.2

We follow the standard proof of the *normal basis theorem*, e.g. [3, Theorem 28], making it effective. Let $G = \{\sigma_1, \ldots, \sigma_d\}$ be the Galois group of $K/\mathbb{Q}$ with σ_1 being the identity, where we are identifying elements of G with the embeddings of K into $\mathbb{C}$. Let $\alpha \in \mathcal{O}_K$ be a primitive element, $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α and define

$$g(x) = \frac{f(x)}{(x - \alpha)f'(\alpha)}.$$

Let $D(x) = \det(\sigma_i \sigma_j(g(x)))$. This is a nonzero polynomial with integer coefficients and

$$\deg(D(x)) = d(d - 1).$$

We want to choose $\alpha \in \mathcal{O}_K$ so that $D(\alpha) \neq 0$. Let $\theta \in \mathcal{O}_K$ be a primitive element satisfying (2), then $1, \theta, \ldots, \theta^{d-1} \in \mathcal{O}_K$ is a basis for K over $\mathbb{Q}$ with

(5)
$$\max_{0 \leq k \leq d-1} h(\theta^k) \leq |\Delta_K|^{\frac{d-1}{d}}.$$

For a given vector $\boldsymbol{\xi} = (\xi_0, \ldots, \xi_{d-1}) \in \mathbb{Z}^d$, define

(6)
$$\alpha_{\boldsymbol{\xi}} = \sum_{k=0}^{d-1} \xi_k \theta^k \in \mathcal{O}_K.$$

Then $D(\alpha_{\boldsymbol{\xi}})$ is a polynomial in d variables $\xi_0, \ldots, \xi_{d-1}$ of degree $d(d-1)$, which is not identically zero. Then Lemma 2.4 guarantees the existence of an integer vector $\boldsymbol{\xi} \in \mathbb{Z}^d$ so that $D(\alpha_{\boldsymbol{\xi}}) \neq 0$ with

$$|\boldsymbol{\xi}| \leq \frac{d(d-1) + 2}{2}.$$

Combining this observation with Lemma 2.1, (5) and (6), we obtain an element $\alpha_{\boldsymbol{\xi}} \in K$ so that $D(\alpha_{\boldsymbol{\xi}}) \neq 0$ with

(7)
$$h(\alpha_{\boldsymbol{\xi}}) \leq \frac{d(d^2 - d + 2)}{2}|\Delta_K|^{d-1}.$$

For this choice of $\alpha_{\boldsymbol{\xi}}$, define $\beta = g(\alpha_{\boldsymbol{\xi}})$. Then, by the argument in the proof of [3, Theorem 28],

$$\beta_j = \sigma_j(\beta), \ 1 \leq j \leq d$$

is a normal basis for K.

We now want to estimate the height of β. Let us write $\alpha_{\boldsymbol{\xi}}^j = \sigma_j(\alpha_{\boldsymbol{\xi}})$ and notice that for each $1 \leq j \leq d$,

$$g_j(x) = \sigma_j(g(x)) = \frac{f(x)}{(x - \alpha_{\boldsymbol{\xi}}^j)f'(\alpha_{\boldsymbol{\xi}}^j)}$$

has degree $d - 1$, roots $\alpha_{\boldsymbol{\xi}}^i$ for all $i \neq j$, and leading coefficient $1/f'(\alpha_{\boldsymbol{\xi}}^j)$. Then, by Lemma 2.3,

$$|g_j| \leq \binom{d-1}{[(d-1)/2]} \mu(g_j) = \binom{d-1}{[(d-1)/2]} \frac{h(\alpha_{\boldsymbol{\xi}})^d}{|f'(\alpha_{\boldsymbol{\xi}}^j)| \max\{1, |\alpha_{\boldsymbol{\xi}}^j|\}}.$$

Then, for each $1 \leq j \leq d$,

$$|\beta_j| \leq d|g_j| \max\{1, |\alpha_{\boldsymbol{\xi}}^j|\}^{d-1} \leq d\binom{d-1}{[(d-1)/2]} \frac{h(\alpha_{\boldsymbol{\xi}})^d \max\{1, |\alpha_{\boldsymbol{\xi}}^j|\}^{d-2}}{|f'(\alpha_{\boldsymbol{\xi}}^j)|}.$$

This implies that

$$\max\{1,|\beta_j|\} \leq \frac{1}{|f'(\alpha_{\boldsymbol{\xi}}^j)|} \max\left\{|f'(\alpha_{\boldsymbol{\xi}}^j)|, d\binom{d-1}{[(d-1)/2]}h(\alpha_{\boldsymbol{\xi}})^d \max\{1,|\alpha_{\boldsymbol{\xi}}^j|\}^{d-2}\right\}$$

$$(8) \qquad \leq d\binom{d-1}{[(d-1)/2]}h(\alpha_{\boldsymbol{\xi}})^d \frac{1}{|f'(\alpha_{\boldsymbol{\xi}}^j)|}\max\{1,|f'(\alpha_{\boldsymbol{\xi}}^j)|\}\max\{1,|\alpha_{\boldsymbol{\xi}}^j|\}^{d-2}.$$

Notice that the coefficients of $f'(\alpha_{\boldsymbol{\xi}})g(x)$, while not necessarily rational integers, are algebraic integers, as is $\alpha_{\boldsymbol{\xi}}$. Therefore, for any $v \nmid \infty$,

$$|f'(\alpha_{\boldsymbol{\xi}})|_v |g|_v \leq 1,$$

where we write $|g|_v$ for the maximum of absolute values $|\ |_v$ of the coefficients of $g(x)$. This implies that for every $v \nmid \infty$,

$$\max\{1,|\beta|_v\} \leq \max\{1,|g|_v\}\max\{1,|\alpha_{\boldsymbol{\xi}}|_v\}^{d-1}$$

$$(9) \qquad \leq \frac{1}{|f'(\alpha_{\boldsymbol{\xi}})|_v}\max\{1,|f'(\alpha_{\boldsymbol{\xi}})|_v\}\max\{1,|\alpha_{\boldsymbol{\xi}}|_v\}^{d-1}.$$

Observe that $\max\{1,|\alpha_{\boldsymbol{\xi}}|_v\} = 1$ for $v \nmid \infty$, since $\alpha_{\boldsymbol{\xi}} \in \mathcal{O}_K$. Now, we combine (8) and (9) and take a product. Using the product formula, we obtain a bound
(10)

$$h(\beta) = \left\{\prod_{v \in M(K)} \max\{1,|\beta|_v\}^{d_v}\right\}^{\frac{1}{d}} \leq d\binom{d-1}{[(d-1)/2]}h(\alpha_{\boldsymbol{\xi}})^d h(\alpha_{\boldsymbol{\xi}})^{d-2}h(f'(\alpha_{\boldsymbol{\xi}})).$$

Notice that $f'(x)$ is a polynomial of degree $d-1$ with integer coefficients and

$$|f'| \leq d|f| \leq d\binom{d-1}{[(d-1)/2]}\mu(f) = d\binom{d-1}{[(d-1)/2]}h(\alpha_{\boldsymbol{\xi}})^d,$$

by Lemmas 2.2 and 2.3, since $f(x)$ is the minimal polynomial of $\alpha_{\boldsymbol{\xi}}$. This inequality implies that

$$h(f'(\alpha_{\boldsymbol{\xi}})) = \left\{\prod_{v|\infty}\max\{1,|f'(\alpha_{\boldsymbol{\xi}})|_v\}^{d_v} \times \prod_{v\nmid\infty}\max\{1,|f'(\alpha_{\boldsymbol{\xi}})|_v\}^{d_v}\right\}^{\frac{1}{d}}$$

$$(11) \qquad \leq d|f'|h(\alpha_{\boldsymbol{\xi}})^{d-1} \leq d^2\binom{d-1}{[(d-1)/2]}h(\alpha_{\boldsymbol{\xi}})^{2d-1}.$$

Combining (10) with (11) and (7), we obtain

$$h(\beta) \leq d^3\binom{d-1}{[(d-1)/2]}^2 h(\alpha_{\boldsymbol{\xi}})^{4d-3}$$

$$(12) \qquad \leq \frac{d^{4d}(d^2-d+2)^{4d-3}}{2}\binom{d-1}{[(d-1)/2]}^2 |\Delta_K|^{(d-1)(4d-3)}.$$

Since $h(\beta_j) = h(\beta)$ for every $1 \leq j \leq d$, this completes the proof.

Remark 3.1. Notice that in our proof of Theorem 1.2, we used the weaker bound (2) instead of the conjectured bound (1), which has been established in the case of real Galois fields. Using that stronger bound would slightly improve the constant depending on d and divide the exponent on $|\Delta_K|$ by 2 in the inequality (12).

4. PROOF OF THEOREM 1.3

Since we are assuming that $K/\mathbb{Q}$ is a Galois extension of prime degree $d \geq 3$, K must be a totally real number field and so $d_v = 1$ for every archimedean place v. Let $L_K = \Sigma_K(\mathcal{O}_K)$ be the full-rank lattice in $\mathbb{R}^d$, then each element $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in L_K$ where the coordinates $\alpha_1, \ldots, \alpha_d$ are algebraic conjugates. Since α_i's are algebraic integers, we have $|\alpha_i|_v \leq 1$ for every $1 \leq i \leq d$ and $v \nmid \infty$, hence, by product formula, for each $\boldsymbol{\alpha} \in L_K$,

$$|\boldsymbol{\alpha}| = \max\{|\alpha_1|, \ldots, |\alpha_d|\} \geq \left(\prod_{i=1}^{d} |\alpha_i|\right)^{\frac{1}{d}} = \left(\prod_{v|\infty} |\alpha_1|_v\right)^{\frac{1}{d}}$$

$$(13) \qquad \geq \left(\prod_{v \in M(K)} |\alpha_1|_v^{d_v}\right)^{\frac{1}{d}} = 1.$$

We want to find an element $\boldsymbol{\alpha} \in L_K$ whose coordinates are linearly independent over $\mathbb{Q}$. We will use the following special case of a result of A. Dubickas, which we state specifically over $\mathbb{Q}$.

Theorem 4.1 ([7], Theorem 1). *Let d be prime and $c_1, \ldots, c_d \in \mathbb{Q}$. Then*

$$c_1 \alpha_1 + \cdots + c_d \alpha_d \in \mathbb{Q}$$

if and only if $c_1 = \cdots = c_d$.

Hence, this theorem implies that if $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in L_K$ is such that

$$(14) \qquad \alpha_1 + \cdots + \alpha_d \neq 0,$$

then $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$ are linearly independent over $\mathbb{Q}$, thus form a normal basis for $K/\mathbb{Q}$. Let

$$\mathcal{C} = \left\{\boldsymbol{x} \in \mathbb{R}^d : |\boldsymbol{x}| \leq 1\right\}$$

be the cube of side-length 2 centered at the origin in $\mathbb{R}^d$, then $\mathrm{Vol}_d(\mathcal{C}) = 2^d$. Write $\lambda_1, \ldots, \lambda_d$ for the successive minima of $\mathcal{C}$ with respect to our lattice L_K, then Minkowski's *successive minima theorem* provides the bound

$$(15) \qquad \prod_{i=1}^{d} \lambda_i \leq \frac{2^d \det(L_K)}{\mathrm{Vol}_d(\mathcal{C})} = \sqrt{|\Delta_K|},$$

by (4), and

$$(16) \qquad 1 \leq \lambda_1 \leq \cdots \leq \lambda_d,$$

by (13). Let $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_d \in L_K$ be the linearly independent points corresponding to $\lambda_1, \ldots, \lambda_d$, then at least one of these vectors satisfies condition (14), since

$$\{\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in L_K : \alpha_1 + \cdots + \alpha_d = 0\}$$

is a sublattice of rank $d-1$. Let us write $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_d)$ for the $\boldsymbol{\alpha}_i$ satisfying (14), then $\beta_1, \ldots, \beta_d \in \mathcal{O}_K$ is a normal basis for $K/\mathbb{Q}$ and (15) combined with (16) impliy that

$$(17) \qquad \max\{|\beta_1|, \ldots, |\beta_d|\} \leq |\Delta_K|^{1/2}.$$

Combining (17) with Lemma 2.5, we obtain

$$h(\beta_i) \leq |\Delta_K|^{1/2},$$

for each $1 \leq i \leq d$. This completes the proof.

Acknowledgements: We wish to thank Professor Adebisi Agboola for a valuable suggestion that led us to consider an effective version of the *normal basis theorem*.

Data availability statement: Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

References

[1] S. Akhtari, J. D. Vaaler and M. Widmer. Small integral generators of totally complex number fields. *Proc. Amer. Math. Soc.*, to appear (2025).

[2] N. Alon. Combinatorial Nullstellensatz. *Combin. Probab. Comput.*, 8 (1999), no. 1-2, pp. 7–29.

[3] E. Artin. Galois Theory. Second edition. University of Notre Dame Press, 1944.

[4] E. Bayer Fluckiger. Upper bounds for Euclidean minima of algebraic number fields. *J. Number Theory*, 121 (2006), no. 2, pp. 305–323.

[5] E. Bombieri and W. Gubler. Heights in Diophantine Geometry. Cambridge University Press, 2006.

[6] J. W. S. Cassels. An Introduction to the Geometry of Numbers. Springer-Verlag, 1959.

[7] A. Dubickas. On the degree of a linear form in conjugates of an algebraic number. *Illinois J. Math.*, 46(2):571–585, 2002.

[8] L. Fukshansky. Integral points of small height outside of a hypersurface. *Monatsh. Math.*, 147 (2006), no. 1, pp. 25–41.

[9] L. Fukshansky. Algebraic points of small height missing a union of varieties. *J. Number Theory*, 130 (2010), no. 10, pp. 2099–2118.

[10] L. Fukshansky and S. Wang. Positive semigroups in lattices and totally real number fields. *Adv. Geom.*, 22 (2022), no. 4, pp. 503–512.

[11] P. M. Gruber and C. G. Lekkerkerker. Geometry of Numbers. North-Holland Publishing Co., 1987.

[12] F. Pazuki and M. Widmer. Bertini and Northcott. *Res. Number Theory*, 7 (2021), Paper no. 12, 18 pp.

[13] W. M. Ruppert. Small generators of number fields. *Manuscripta Math.*, 96 (1998), no. 1, pp. 17–22.

[14] 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

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711

Email address: Sehun.Jeong@ClaremontMcKenna.edu