SMALL INTEGRAL GENERATORS OF TOTALLY COMPLEX NUMBER FIELDS

SHABNAM AKHTARI, JEFFREY D. VAALER AND MARTIN WIDMER

Abstract. Let K be an algebraic number field and H the absolute Weil height. Write c_K for a certain positive constant that is an invariant of K. We consider the question: does K contain an algebraic integer α such that both $K = \mathbb{Q}(\alpha)$ and $H(\alpha) \le c_K$? If K has a real embedding then a positive answer was established in previous work. Here we obtain a positive answer if $\mathrm{Tor}\big(K^\times\big) \neq \{\pm 1\}$, and so K has only complex embeddings. We also show that if the answer is negative, then K is totally complex, $\mathrm{Tor}\big(K^\times\big) = \{\pm 1\}$, and K is a Galois extension of its maximal totally real subfield. Further, we show that if $\mu \in O_K$ is not totally real, then there exists α in O_K with $K = \mathbb{Q}(\alpha)$ and $H(\alpha) \le H(\mu)\, c_K$.

1. Introduction

Let K be an algebraic number field of degree $d = [K : \mathbb{Q}]$, and let Δ_K be the discriminant of K. We define the positive constant

$$c_K = \left(\frac{2}{\pi}\right)^{s/d} \big|\Delta_K\big|^{1/2d}, \tag{1.1}$$

where s is the number of complex places of K. We write $K^\times$ for the multiplicative group of nonzero elements of K, and

$$H : K^\times \to [1, \infty) \tag{1.2}$$

for the absolute, multiplicative Weil height defined in (3.2).

In [8, Question 2] W. Ruppert asked the following question:

Question 1.1. [Ruppert, 1998] *Does there exist a positive constant $A = A(d)$ such that if K is an algebraic number field of degree d over $\mathbb{Q}$, then there exists an element α in K such that*

$$K = \mathbb{Q}(\alpha), \quad \textit{and} \quad H(\alpha) \le A\big|\Delta_K\big|^{1/2d}\,?$$

Ruppert stated his question using the naive height. However, it follows from elementary inequalities for heights that the variant we have stated here is equivalent to the question originally asked by Ruppert. It is known that there exists always a generator whose height is at most $|\Delta_K|^{1/d}$, see, e.g., [12, Lemma 7.1].

In [8, Proposition 2] Ruppert obtained a positive answer to his question when $[K : \mathbb{Q}] = 2$. He also proved that if K is a real quadratic extension of $\mathbb{Q}$, then the generator α can be selected from the ring O_K of algebraic integers in K. In [10] the second and third named authors provided the following partial answer to Ruppert's question:

2010 *Mathematics Subject Classification.* 11H06, 11R29, 11R56.

Key words and phrases. height, integral generators, CM-fields, roots of unity.

Theorem 1.1. *Assume that K has an embedding into $\mathbb{R}$. Then there exists an algebraic integer α in O_K such that*

$$K = \mathbb{Q}(\alpha), \quad \text{and} \quad H(\alpha) \le c_K. \tag{1.3}$$

In Theorem 1.1 the generator α is an algebraic integer, a requirement that was *not* stated in Ruppert's question, while the height of α is bounded in a manner that was anticipated in Ruppert's question. Hence Theorem 1.1 generalizes Ruppert's earlier result to number fields K that have at least one real embedding.

Ruppert's question has also been answered in the affirmative for abelian number fields of sufficiently large degree [11, Theorem 1]. Moreover, it is known that the exponent $1/2d$ cannot be replaced by a smaller value, at least not if d is even [11, Theorem 2].

In this note we establish a positive answer to Ruppert's question for a new class of number fields.

Theorem 1.2. *Assume that K is a number field, and μ is an algebraic integer in O_K that is not totally real. Then there exists an algebraic integer α in O_K such that*

$$K = \mathbb{Q}(\alpha), \quad \text{and} \quad H(\alpha) \le H(\mu)\, c_K. \tag{1.4}$$

Let $\mathrm{Tor}\big(K^\times\big)$ denote the torsion subgroup of the multiplicative group $K^\times$. This group is known to be a finite, cyclic group of even order $2q_K$, where q_K is a positive divisor of Δ_K (see [5, Proposition 3.11]). The following simple corollary illustrates how Theorem 1.2 can be applied.

Corollary 1.1. *Assume that K is a number field such that*

$$\mathrm{Tor}\big(K^\times\big) \neq \{\pm 1\}.$$

Then there exists α in O_K such that

$$K = \mathbb{Q}(\alpha), \quad \text{and} \quad H(\alpha) \le c_K.$$

To derive Corollary 1.1 from Theorem 1.2 we select μ to be an element of the group $\mathrm{Tor}\big(K^\times\big)$ having order greater than or equal to 3. It follows that μ is a complex (and not real) root of unity and therefore $H(\mu) = 1$. In this example μ has no real conjugates over $\mathbb{Q}$ and therefore the field K containing μ is totally complex.

Another implication of Theorem 1.2 is an affirmative answer to Question 1.1 (with $A = 2$, say) whenever the field K contains a non-quadratic algebraic integer of the form $n^{1/m}$ with integers $m \ge n \ge 2$. In Theorem 1.2 we may take $\mu = n^{1/m}$, for which we have $H(\mu) \le 2$.

The constructive method used in the proof of Theorem 1.2 enables us to obtain a result in which we identify a class of number fields which might not have a small integral generator.

Theorem 1.3. *Let $\mathcal{H} \ge 1$ and assume that K is a number field such that*

$$\mathcal{H} c_K < \min\big\{H(\alpha) : \alpha \in O_K \text{ and } K = \mathbb{Q}(\alpha)\big\}. \tag{1.5}$$

Let $F \subseteq K$ be the maximal, totally real subfield of K. Then K is totally complex, K/F is Galois, and every $\mu \in O_K$ with $H(\mu) \le \mathcal{H}$ is contained in F.

For a number field K that satisfies the hypotheses of Theorem 1.3, a representation for the Galois group $\mathrm{Aut}(K/F)$ is provided in (5.5). We also note that the restriction of complex conjugation to K belongs to $\mathrm{Aut}(K/F)$ and is an automorphism of order 2. This implies that $k = K \cap \mathbb{R}$ is the unique real subfield of K with $[K : k] = 2$ and $F \subseteq k \subseteq K$. A more general form of these remarks follows from (5.2) and (5.3) in the proof of Theorem 1.3.

Taking $\mathcal{H} = 1$ in Theorem 1.3, we conclude that if K is a number field such that

$$c_K < \min\big\{H(\alpha) : \alpha \in O_K \text{ and } K = \mathbb{Q}(\alpha)\big\}, \tag{1.6}$$

then K is totally complex, K is Galois over its maximal totally real subfield F, and $\mathrm{Tor}\big(K^\times\big) = \{\pm 1\}$. Next we record some examples of fields K that satisfy the inequality (1.5) in Theorem 1.3 with $\mathcal{H} = 1$.

In Section 2 we provide some examples which motivate our new results. In Section 3 we prove some auxiliary lemmas. The proof of our main results Theorem 1.2 and Theorem 1.3 are completed in Sections 4 and 5, respectively.

2. Examples

2.1. **Imaginary quadratic fields.** Let m be a squarefree, negative integer and let $L = \mathbb{Q}\big(\sqrt{m}\big)$ be the imaginary quadratic field generated by $\sqrt{m}$. An integral basis for the ring O_L is well known (see [1, Theorem 7.1.1]). We also recall (see [1, Theorem 7.1.2]) that

$$\Delta_L = \begin{cases} m & \text{if } m \equiv 1 \pmod 4, \\ 4m & \text{if } m \not\equiv 1 \pmod 4. \end{cases} \tag{2.1}$$

It is now a simple matter to minimize the height over elements of O_L that generate the field L by constructing their minimal polynomials (see [8, Section 2] for more details). If $m \equiv 1 \pmod 4$ we find that

$$\min\big\{H(\alpha) : \alpha \in O_L \text{ and } L = \mathbb{Q}(\alpha)\big\} = \tfrac{1}{2}\big(1 + |\Delta_L|\big)^{\frac{1}{2}}, \tag{2.2}$$

and if $m \not\equiv 1 \pmod 4$ then

$$\min\big\{H(\alpha) : \alpha \in O_L \text{ and } L = \mathbb{Q}(\alpha)\big\} = \tfrac{1}{2}|\Delta_L|^{\frac{1}{2}}. \tag{2.3}$$

Among the imaginary quadratic fields L, only the fields

$$L = \mathbb{Q}\big(\sqrt{-3}\big) \quad \text{and} \quad L = \mathbb{Q}\big(\sqrt{-1}\big)$$

satisfy the condition $\mathrm{Tor}\big(L^\times\big) \neq \{\pm 1\}$. These fields are both generated by a root of unity and therefore the minimal height of an algebraic integer that generates the field is 1. This conclusion also follows from (2.1), (2.2), and (2.3).

If $L = \mathbb{Q}\big(\sqrt{m}\big)$ satisfies $\mathrm{Tor}\big(L^\times\big) = \{\pm 1\}$ then it follows from our previous remarks that the minimum height of an integral generator is greater than 1. As the value of the minimal height is given by (2.2) or by (2.3), it is easy to verify that

$$c_L = \left(\frac{2}{\pi}\right)^{1/2} \big|\Delta_L\big|^{1/4} < \min\big\{H(\alpha) : \alpha \in O_L \text{ and } L = \mathbb{Q}(\alpha)\big\}$$

in both cases. This shows that for imaginary quadratic fields L the inequality (1.5) with $\mathcal{H} = 1$ holds if and only if L satisfies $\mathrm{Tor}\big(L^\times\big) = \{\pm 1\}$.

2.2. **A quartic number field.** While for quadratic number fields K, the inequality (1.6) holds if and only if K is totally complex Galois extension of $\mathbb{Q}$ and $\mathrm{Tor}\big(K^\times\big) = \{\pm 1\}$, for number fields of degree greater than 2, this equivalence no longer holds. The following is an example of a totally complex quartic number field K that is a Galois extension of a totally real number field, with $\mathrm{Tor}\big(K^\times\big) = \{\pm 1\}$ for which (1.6) does not hold. Let α be an algebraic integer that satisfies

$$\alpha^2 = \sqrt{3} - 2 < 0,$$

and $K = \mathbb{Q}(\alpha)$. The quartic field K has discriminant (see [4, Theorem 1])

$$\Delta_K = 2^8 3^2.$$

On the other hand,

$$H(\alpha) = H(\sqrt{3}-2)^{1/2} = (\sqrt{3}+2)^{1/4} < (2/\pi)^{1/2}(2^8 3^2)^{1/8} = c_K.$$

Assume that $\mathrm{Tor}\big(K^\times\big) \neq \{\pm 1\}$. Since 2 and 3 are the only primes that ramify in K we conclude that

$$\tfrac{1}{2}\big(\sqrt{-3}-1\big) \in K \quad \text{or} \quad \sqrt{-1} \in K.$$

But since $\sqrt{3} \in K$, we get $\sqrt{-1} \in K$ in either case, and thus also $\sqrt{2-\sqrt{3}} \in K$. However, the algebraic number $\sqrt{2-\sqrt{3}}$ is totally real of degree 4, and therefore it cannot belong to the totally complex quartic field K. This contradiction confirms that $\mathrm{Tor}\big(K^\times\big) = \{\pm 1\}$.

2.3. **A family of** CM**-fields.** We recall that K is a CM-field if K has only complex embeddings and there exists a totally real subfield $k \subseteq K$ such that K/k is a quadratic extension. There are well known characterizations of CM-fields due to Blanksby and Loxton [2] and Shimura [9, Proposition 5.11]. It follows that if K is a CM-field that satisfies the hypotheses of Theorem 1.3 then the maximal totally real subfield F that occurs in the statement of Theorem 1.3 is equal to k.

Next we give a family of examples of CM-fields of degree $d = 2N \geq 4$ that satisfy (1.6). First we pick a totally real field F of degree N. Let $\{\omega_1, \ldots, \omega_N\}$ be a $\mathbb{Z}$-basis of O_F. Let n be a positive, squarefree integer, set $M = \mathbb{Q}(\sqrt{-n})$, and let $1, \xi$ be a $\mathbb{Z}$-basis of O_M. Assume that Δ_F and Δ_M are coprime, and set $K = FM = F(\sqrt{-n})$. This implies that

$$\{\omega_1, \ldots, \omega_N, \omega_1\xi, \ldots, \omega_N\xi\}$$

is a $\mathbb{Z}$-basis of O_K, and

$$|\Delta_K| = \Delta_F^2 |\Delta_M|^N \leq \Delta_F^2 (4n)^N.$$

In particular, every $\alpha \in O_K$ with $K = \mathbb{Q}(\alpha)$ can be written in the form

$$\alpha = \tfrac{1}{2}\big(\omega + \omega'\sqrt{-n}\big),$$

where ω and $\omega' \neq 0$ are in O_F. Using that F is totally real, and writing τ for an embedding in $\mathrm{Hom}(K, \mathbb{C})$, we find

$$\begin{aligned} H(\alpha) &\geq \prod_{\tau \in \mathrm{Hom}(K,\mathbb{C})} |\tau(\alpha)|^{1/d} = \tfrac{1}{2} \prod_{\tau \in \mathrm{Hom}(K,\mathbb{C})} \big|\tau(\omega) + \tau(\omega')\tau(\sqrt{-n})\big|^{1/d} \\ &\geq \tfrac{1}{2}\sqrt{n} \prod_{\tau \in \mathrm{Hom}(K,\mathbb{C})} \big|\tau(\omega')\big|^{1/d} \geq \tfrac{1}{2}\sqrt{n}. \end{aligned}$$

Hence K satisfies (1.5) with $\mathcal{H} = 1$ for all sufficiently large n.

3. Lemmas

Let K is an algebraic number field. We use

$$|\ |:\mathbb{C}\to[0,\infty)\quad\text{and}\quad\rho:\mathbb{C}\to\mathbb{C},$$

for the standard absolute value on $\mathbb{C}$ and complex conjugation, respectively. At each place v of K we write K_v for the completion of K with respect to an absolute value from v. Then $\|\ \|_v$ is the unique absolute value from v that extends either the usual Euclidean absolute value on $\mathbb{Q}_\infty$ or the unique p-adic absolute value on $\mathbb{Q}_p$. We write $d=[K:\mathbb{Q}]$ for the degree of K and $d_v=[K_v:\mathbb{Q}_v]$ for the local degree at the place v. Then we define a second absolute value from v by

$$|\ |_v=\|\ \|_v^{d_v/d}. \tag{3.1}$$

It follows that the absolute, multiplicative Weil height of α in $K^\times$ is the map (1.2) defined by (see [3, section 1.5.7])

$$H(\alpha)=\prod_v\max\big\{1,|\alpha|_v\big\}. \tag{3.2}$$

We also write $W_\infty(K/\mathbb{Q})$ for the set of archimedean places of K. If v is a real place of K then $\sigma_v:K\to\mathbb{C}$ is the embedding associated to v by

$$\|\beta\|_v=\big|\sigma_v(\beta)\big|\quad\text{for each }\beta\text{ in }K. \tag{3.3}$$

If w is a complex place of K then

$$\sigma_w:K\to\mathbb{C}\quad\text{and}\quad\rho\sigma_w:K\to\mathbb{C}$$

are the two distinct embeddings associated to w by the identity

$$\|\beta\|_w=\big|\sigma_w(\beta)\big|=\big|\rho\sigma_w(\beta)\big|\quad\text{for each }\beta\text{ in }K. \tag{3.4}$$

We write more simply $\mathrm{Hom}(K,\mathbb{C})$ for the collection of all d distinct embeddings of K into $\mathbb{C}$. If $\alpha\neq0$ belongs to the ring O_K of algebraic integers in K then from (3.1), (3.3), and (3.4), we obtain the identity

$$H(\alpha)^d=\prod_{v|\infty}\max\big\{1,\|\alpha\|_v^{d_v}\big\}=\prod_{\tau\in\mathrm{Hom}(K,\mathbb{C})}\max\big\{1,|\tau\alpha|\big\}.$$

The following result is a version of Minkowski's basic theorem on lattice points in convex bodies. A proof is given in [6, Chapter I, Theorem 5.3].

Theorem 3.1. *For each embedding τ in $\mathrm{Hom}(K,\mathbb{C})$ let $b(\tau)$ be a positive real number. Assume that $b(\rho\tau)=b(\tau)$ for each τ in $\mathrm{Hom}(K,\mathbb{C})$, and*

$$(c_K)^d<\prod_{\tau\in\mathrm{Hom}(K,\mathbb{C})}b(\tau), \tag{3.5}$$

where c_K is defined in (1.1). Then there exists $\xi\neq0$ in O_K such that

$$|\tau\xi|<b(\tau)\quad\textit{for all }\tau\textit{ in }\mathrm{Hom}(K,\mathbb{C}).$$

The next lemma is a simple application of Minkowski's theorem.

Lemma 3.1. *Assume that the field K has at least two archimedean places. Let w be an archimedean place of K. For each archimedean place $v\neq w$ let $0<B_v\le1$. Then there exists a nonzero algebraic integer $\xi^{(w)}$ in O_K such that*

$$\big|\xi^{(w)}\big|_v<B_v\quad\textit{if }v|\infty\textit{ and }v\neq w, \tag{3.6}$$

and

$$\left|\xi^{(w)}\right|_w \le c_K \prod_{\substack{v|\infty \\ v\neq w}} B_v^{-1}. \tag{3.7}$$

Furthermore, we have $H\big(\xi^{(w)}\big) = \left|\xi^{(w)}\right|_w$.

Proof. Let $\varepsilon > 0$. If $v \neq w$ is a real place of K and

$$\sigma_v : K \to \mathbb{C}$$

is the associated embedding, we set

$$b\big(\sigma_v\big) = B_v^d.$$

Similarly, if $v \neq w$ is a complex place of K and the associated embeddings are

$$\sigma_v : K \to \mathbb{C} \quad \text{and} \quad \rho\sigma_v : K \to \mathbb{C},$$

we set

$$b\big(\sigma_v\big) = b\big(\rho\sigma_v\big) = B_v^{d/2}.$$

If w is a real place we define

$$b\big(\sigma_w\big) = \Big((1+\varepsilon)c_K \prod_{\substack{v|\infty \\ v\neq w}} B_v^{-1}\Big)^d,$$

and if w is a complex place we define

$$b\big(\sigma_w\big) = b\big(\rho\sigma_w\big) = \Big((1+\varepsilon)(c_K \prod_{\substack{v|\infty \\ v\neq w}} B_v^{-1})\Big)^{d/2}.$$

Then it follows in all cases that

$$\prod_{\tau\in \mathrm{Hom}(K,\mathbb{C})} b(\tau) = \left((1+\varepsilon)c_K\right)^d. \tag{3.8}$$

The identity (3.8) implies that the positive real numbers $b(\tau)$ satisfy the hypothesis (3.5) in the statement of Theorem 3.1. Then it follows from the conclusion of Theorem 3.1 that there exists an algebraic integer $\xi^{(w)} \neq 0$ in O_K such that

$$\left|\tau\xi^{(w)}\right| < b(\tau) \quad \text{for all } \tau \text{ in } \mathrm{Hom}(K,\mathbb{C}).$$

We have shown that for every positive value of ε there exists a nonzero algebraic integer $\xi^{(w)}$ in O_K such that

$$\left|\xi^{(w)}\right|_v < B_v \quad \text{if } v|\infty \text{ and } v \neq w, \tag{3.9}$$

and

$$\left|\xi^{(w)}\right|_w < (1+\varepsilon)c_K \prod_{\substack{v|\infty \\ v\neq w}} B_v^{-1}. \tag{3.10}$$

Using that $B_v \le 1$ whenever $v \mid \infty$ and $v \neq w$, and that $\xi^{(w)}$ is a nonzero algebraic integer, we conclude from the product formula that $\left|\xi^{(w)}\right|_w > 1$. Thus (3.2) gives

$$H\big(\xi^{(w)}\big) = \left|\xi^{(w)}\right|_w.$$

It follows from Northcott's theorem in [7] that the set of nonzero algebraic integers $\xi^{(w)}$ in O_K that satisfy (3.9) and (3.10) with $\varepsilon = 1$ is finite. And we have shown that

this finite set is not empty for every positive value of ε. Therefore the statement of the lemma follows. □

Lemma 3.2. *Assume that the field K is totally complex and has at least two archimedean places. Let w be an archimedean place of K and let $\xi^{(w)}$ be a nonzero element of O_K that satisfies*

$$|\xi^{(w)}|_v < 1 \quad \text{if } v|\infty \text{ and } v \neq w. \tag{3.11}$$

Write

$$\sigma_w : K \to \mathbb{C} \quad \text{and} \quad \rho\sigma_w : K \to \mathbb{C}$$

for the embeddings of K into $\mathbb{C}$ that satisfy the identity (3.4)*. Assume that the field*

$$k = \mathbb{Q}(\xi^{(w)})$$

is a proper subfield of K. Then we have

$$\big[K : k\big] = 2. \tag{3.12}$$

Moreover, the subfield k satisfies

$$\sigma_w(k) = \sigma_w(K) \cap \mathbb{R}. \tag{3.13}$$

And the restriction of complex conjugation

$$\rho : \sigma_w(K) \to \sigma_w(K) \tag{3.14}$$

is an automorphism that fixes the subfield $\sigma_w(k)$.

Proof. Since $\xi^{(w)}$ is a nonzero algebraic integer it follows from (3.11) and the product formula that

$$1 < |\xi^{(w)}|_w.$$

Let x be the unique archimedean place of the proper subfield k that satisfies $w|x$. Write K_w for the completion of K at the place w and k_x for the completion of k at the place x. Then we get

$$1 < |\xi^{(w)}|_w = |\xi^{(w)}|_x.$$

If $v \neq w$ is a second archimedean place of K that also satisfies $v|x$, we find that

$$1 < |\xi^{(w)}|_x = |\xi^{(w)}|_v$$

which contradicts (3.11). We conclude that w is the *unique* place of K that satisfies $w|x$. Because the global degree of the extension K/k is the sum of local degrees over the completion k_x, we conclude that

$$2 \le [K : k] = \big[K_w : k_x\big] \le [\mathbb{C} : \mathbb{R}] = 2. \tag{3.15}$$

This verifies (3.12).

It also follows from the equality in (3.15) that the completion k_x is isomorphic to $\mathbb{R}$. We conclude that

$$\sigma_w\big(k\big) \subseteq \mathbb{R}, \quad \text{and} \quad \sigma_w\big(k\big) \subseteq \sigma_w(K) \cap \mathbb{R} \subseteq \sigma_w(K). \tag{3.16}$$

Because K/k is a quadratic extension it follows from the two containments on the right of (3.16) that either

$$\sigma_w\big(k\big) = \sigma_w(K) \cap \mathbb{R} \quad \text{or} \quad \sigma_w(K) \cap \mathbb{R} = \sigma_w(K). \tag{3.17}$$

As K is totally complex the equality on the right of (3.17) is clearly impossible, and we conclude that the equality on the left of (3.17) must hold. This verifies the equality in (3.13). It also shows that the restriction of complex conjugation to

$\sigma_w(K)$, fixes the real subfield $\sigma_w\big(k\big)$. The field extension $\sigma_w(K)/\sigma_w\big(k\big)$ is quadratic and therefore Galois. We conclude that ρ in (3.14) is indeed an automorphism. □

In the statement of Lemma 3.2 the map $\rho : \mathbb{C} \to \mathbb{C}$ is restricted in (3.14) to the various embeddings of K into $\mathbb{C}$. We record a variant in which K is fixed and the group $\mathrm{Aut}\big(K/k\big)$ is identified.

Corollary 3.1. *Let K be an algebraic number field that satisfies the hypotheses of* Lemma 3.2. *For each archimedean place w of K let $\xi^{(w)}$ be a nonzero element of O_K that satisfies* (3.11) *from* Lemma 3.2, *and suppose*

$$k^{(w)} = \mathbb{Q}\big(\xi^{(w)}\big)$$

is a proper subfield of K. Then $K/k^{(w)}$ is a Galois extension of order 2 *and*

$$\mathrm{Aut}\big(K/k^{(w)}\big) = \langle \sigma_w^{-1}\rho\sigma_w \rangle.$$

Proof. It follows from Lemma 3.2 that $K/k^{(w)}$ is an extension of degree 2. And it follows from (3.14) that

$$\sigma_w^{-1}\rho\sigma_w : K \to K \tag{3.18}$$

is an automorphism that fixes the subfield $k^{(w)} \subseteq K$. We conclude that $K/k^{(w)}$ is a Galois extension and $\mathrm{Aut}\big(K/k^{(w)}\big)$ is generated by the nontrivial automorphism (3.18). □

Next we prove an elementary lemma from Galois theory.

Lemma 3.3. *Let L be an algebraic number field and let*

$$\big\{\ell_1, \ell_2, \cdots, \ell_J\big\}$$

be a finite collection of subfields of L. Assume that L/ℓ_j is a Galois extension for each $j = 1, 2, \ldots, J$. If

$$F = \ell_1 \cap \ell_2 \cap \cdots \cap \ell_J$$

then L/F is a Galois extension. Moreover, let

$$H_j = \mathrm{Aut}(L/\ell_j) \subseteq \mathrm{Aut}(L/F) \quad \textit{for } j = 1, 2, \ldots, J,$$

be the subgroups attached to the extensions L/ℓ_j. And let

$$G = \langle H_1, H_2, \cdots, H_J \rangle \subseteq \mathrm{Aut}(L/F)$$

be the group generated by the collection of subgroups $H_1, H_2, \ldots, H_J$. Then we have

$$G = \mathrm{Aut}(L/F). \tag{3.19}$$

Proof. Since the characteristic of F is zero the extension L/F is separable. Suppose α is an element of L satisfying $L = F(\alpha)$. Then let $P(x)$ be the monic polynomial

$$P(x) = \prod_{\gamma \in G} \big(x - \gamma(\alpha)\big).$$

It follows that $P(\alpha) = 0$. Since $G \subseteq \mathrm{Aut}(L/F)$ each root $\gamma(\alpha)$ belongs to L.

Let φ be an automorphism in G. Then we have

$$\begin{aligned} \varphi\big(P(x)\big) &= \prod_{\gamma \in G} \big(x - \varphi\big(\gamma(\alpha)\big)\big) \\ &= \prod_{\gamma \in G} \big(x - \gamma(\alpha)\big) = P(x). \end{aligned} \tag{3.20}$$

From (3.20) we conclude that each coefficient of $P(x)$ is fixed by the automorphisms in each of the groups H_j for $j = 1, 2, \ldots, J$. Therefore each coefficient belongs to the field

$$\ell_1 \cap \ell_2 \cap \cdots \cap \ell_J = F.$$

We conclude that $P(x)$ is in $F[x]$ and L is the splitting field of P over F. It follows that L/F is a Galois extension and $\#G = \deg P \geq [L : F] = \#\operatorname{Aut}(L/F)$. This implies that $G = \operatorname{Aut}(L/F)$. □

4. Proof of Theorem 1.2

If K has an embedding into $\mathbb{R}$ then the inequality (1.4) follows from (1.3) in the statement of Theorem 1.1. Therefore we assume throughout the remainder of the proof that K is totally complex.

If K is a complex quadratic field then we have $K = \mathbb{Q}(\mu)$ because μ is not totally real. Since $c_K \geq 1$ it follows that (1.4) holds with $\alpha = \mu$.

For the remainder of the proof we assume that the totally complex number field K has degree at least 4, and so has at least two archimedean places. Let w be an archimedean place of K such that $\sigma_w(\mu) \notin \mathbb{R}$.

We apply Lemma 3.1 with the choices $B_v = \max\{1, |\mu|_v\}^{-1}$ (for $v|\infty, v \neq w$) to get a nonzero algebraic integer $\xi^{(w)}$ in O_K that satisfies the inequalities (3.6) and (3.7) in Lemma 3.1. Consider the subfield

$$\mathbb{Q}\big(\xi^{(w)}\big) \subseteq K. \tag{4.1}$$

Using (3.7) we find that

$$H\big(\xi^{(w)}\big) = \big|\xi^{(w)}\big|_w \leq c_K \prod_{\substack{v|\infty \\ v\neq w}} \max\{1, |\mu|_v\} \leq c_K H(\mu).$$

If there is equality in the containment (4.1) then (1.4) holds with $\alpha = \xi^{(w)}$.

Now suppose $\mathbb{Q}\big(\xi^{(w)}\big)$ is a proper subfield of K. It follows from (3.13) that $\sigma_w(\xi^{(w)}) \in \mathbb{R}$. Consider the nonzero algebraic integer $\alpha = \mu\xi^{(w)}$, and set

$$k = \mathbb{Q}(\alpha) \subseteq K.$$

We note that

$$|\alpha|_v = |\mu|_v |\xi^{(w)}|_v < \frac{|\mu|_v}{\max\{1, |\mu|_v\}} \leq 1 \quad \text{if } v|\infty \text{ and } v \neq w.$$

Since $\sigma_w(\xi^{(w)}) \in \mathbb{R}$ and $\sigma_w(\mu) \notin \mathbb{R}$ we conclude that $\sigma_w(\alpha) = \sigma_w(\mu)\sigma_w(\xi^{(w)}) \notin \mathbb{R}$. Therefore Lemma 3.2, applied to α instead of $\xi^{(w)}$, gives $k = K$. Finally, using that $|\alpha|_v \leq 1$ for all places v with $v \neq w$, we get

$$\begin{aligned} H(\alpha) = |\alpha|_w = |\mu|_w |\xi^{(w)}|_w &\leq |\mu|_w c_K \prod_{\substack{v|\infty \\ v\neq w}} \max\{1, |\mu|_v\} \\ &\leq c_K \prod_{v|\infty} \max\{1, |\mu|_v\} = c_K H(\mu). \end{aligned}$$

5. Proof of Theorem 1.3

If K has a real embedding then it follows from Theorem 1.1 that the inequality (1.5) is false.

Now suppose that K has only complex embeddings and there exists $\mu \in O_K$ such that $H(\mu) \le \mathcal{H}$ and $\mu \notin F$. It follows that μ is not totally real. And Theorem 1.2 implies that there exists α in O_K such that

$$K = \mathbb{Q}(\alpha), \quad \text{and} \quad H(\alpha) \le H(\mu)c_K \le \mathcal{H}c_K. \tag{5.1}$$

But the inequality (5.1) contradicts the hypothesis (1.5) in the statement of Theorem 1.3. We conclude that the hypothesis (1.5) implies that K is totally complex and that every $\mu \in O_K$ with $H(\mu) \le \mathcal{H}$ lies in F. It remains to prove that (1.5) also implies that K/F is a Galois extension.

If the totally complex field K has exactly one archimedean place then K is an imaginary quadratic extension of $\mathbb{Q}$. In this case it is easy to prove that $F = \mathbb{Q}$ and $K/\mathbb{Q}$ is Galois. For the remainder of the proof, we assume that K has at least two archimedean places, that satisfy

$$\{\alpha \in O_K : H(\alpha) \le \mathcal{H}\} \subseteq F,$$

and satisfy the inequality (1.5). Therefore K satisfies the hypotheses of Lemma 3.1 and Lemma 3.2. For each archimedean place w of K we select a nonzero $\xi^{(w)} \in O_K$ that satisfies the inequalities (3.6) and (3.7) in the statement of Lemma 3.1 for the choices $B_v = 1$ (for $v \mid \infty$, $v \ne w$). It follows from Lemma 3.1 that $H(\xi^{(w)}) \le c_K \le c_K\mathcal{H}$. Therefore the hypothesis (1.5) implies that

$$k^{(w)} = \mathbb{Q}\big(\xi^{(w)}\big) \tag{5.2}$$

is a proper subfield of K. Hence, it follows from Corollary 3.1 that $K/k^{(w)}$ is a Galois extension of order 2 and

$$\mathrm{Aut}\big(K/k^{(w)}\big) = \langle \sigma_w^{-1}\rho\sigma_w \rangle. \tag{5.3}$$

Next we define the subfield

$$\widetilde{F} = \bigcap_{w|\infty} k^{(w)} \subseteq K. \tag{5.4}$$

Then it follows from Lemma 3.3 that $K/\widetilde{F}$ is a Galois extension and

$$\mathrm{Aut}(K/\widetilde{F}) = \langle \sigma_w^{-1}\rho\sigma_w : w|\infty \text{ is a place of } K \rangle. \tag{5.5}$$

If α belongs to $\widetilde{F}$ then it follows from (5.4) that α belongs to $k^{(w)}$ at each archimedean place w of K. And it follows from (3.13) that

$$\sigma_w(\alpha) \in \sigma_w\big(k^{(w)}\big) \subseteq \mathbb{R}$$

at each archimedean place w of K. We conclude that $\widetilde{F}$ is totally real.

Finally, let β be an element of K that is totally real. Then at each archimedean place w of K we have both $\sigma_w(\beta) \in \sigma_w(K)$ and $\sigma_w(\beta) \in \mathbb{R}$. Applying (3.13) we find that

$$\sigma_w(\beta) \in \sigma_w(K) \cap \mathbb{R} = \sigma_w\big(k^{(w)}\big) \tag{5.6}$$

at each archimedean place w of K. We conclude from (5.6) that

$$\beta \in \bigcap_{w|\infty} k^{(w)} = \widetilde{F},$$

and therefore $\widetilde{F} = F$ is the maximal totally real subfield in K.

Acknowledgements

The authors are grateful to the anonymous referees for the careful reading and helpful suggestions.

We thank Dr. Michael Mossinghoff for insightful conversation about this project. We are grateful to Professor Hendrik Lenstra for pointing out an error in an earlier version of this manuscript.

The authors acknowledge support from the Max Planck Institute for Mathematics in Bonn and support from the Institute for Advanced Study in Princeton.

Shabnam Akhtari's research was partially supported by the National Science Foundation Awards DMS-2001281 and DMS-2327098.

References

[1] Ş. Alaca and K. S. Williams, Introductory Algebraic Number Theory, Cambridge U. Press, New York, 2004.
[2] P. E. Blanksby and J. H. Loxton, A note on the characterization of CM-fields, J. Austral. Math. Soc. (Series A) 26: 26–30, 1978.
[3] E. Bombieri and W. Gubler, Heights in Diophantine Geometry, Cambridge U. Press, New York, 2006.
[4] J. G. Huard and B. K. Spearman and K. S. Williams, Integral bases for quartic fields with quadratic subfields, J. Number Theory, 51: 87–102, 1995.
[5] W. Narkieweicz, Elementary and Analytic Theory of Algebraic Numbers, 3rd ed., Springer, 2004.
[6] J. Neukirch, Algebraic Number Theory, Springer-Verlag, New York, 1999.
[7] D. G. Northcott. An inequality on the theory of arithmetic on algebraic varieties. Proc. Cambridge Philos. Soc., 45: 502–509, 1949.
[8] W. Ruppert, Small generators of number fields, Manuscripta Math., 96(1): 17–22, 1998.
[9] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions Princeton University Press, Princeton, NJ, 1971.
[10] J. D. Vaaler and M. Widmer, A note on generators of number fields, In Diophantine Methods, Lattices and the Arithmetic Theory of Quadratic Forms, Vol. 587 of Contemp. Math. 201–211, Amer. Math. Soc., Providence, RI 2013.
[11] M. Widmer, Small generators of abelian number fields, Forum Math., 37: 629–636, 2025.
[12] F. Pazuki and M. Widmer, Bertini and Northcott, Res. Number Theory, 7: 2021, no. 1, art. 12, 18 pp.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802 USA
Email address: akhtari@psu.edu

Department of Mathematics, University of Texas, Austin, TX 78712 USA
Email address: vaaler@math.utexas.edu

Graz University of Technology, Institute of Analysis and Number Theory, Steyrergasse 30/II, 8010 Graz, Austria
Email address: martin.widmer@tugraz.at