A note on generators of number fields

Jeffrey D. Vaaler and Martin Widmer

Abstract. We establish upper bounds for the smallest height of a generator of a number field k over the rational field $\mathbb{Q}$. Our first bound applies to all number fields k having at least one real embedding. We also give a second conditional result for all number fields k such that the Dedekind zeta-function associated to the Galois closure of $k/\mathbb{Q}$ satisfies GRH. This provides a partial answer to a question of W. Ruppert.

1. Introduction

Let $\overline{\mathbb{Q}}$ denote an algebraic closure of the field $\mathbb{Q}$ of rational numbers, and for α in $\overline{\mathbb{Q}}$ let $H(\alpha)$ denote the absolute, multiplicative Weil height of α. If $k \subseteq \overline{\mathbb{Q}}$ is an algebraic number field, we consider the problem of showing that $k = \mathbb{Q}(\alpha)$, where the height of α can be estimated by invariants of k. In particular we are interested in showing that k is generated over $\mathbb{Q}$ by an element α that has relatively small height.

Let Δ_k denote the discriminant of the number field k. In [**5**, Question 2] W. Ruppert proposed the following more precise question.

Question 1.1. [Ruppert, 1998] *Does there exist a positive constant $B = B(d)$ 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*

$$k = \mathbb{Q}(\alpha), \quad \text{and} \quad H(\alpha) \le B\big|\Delta_k\big|^{1/2d}? \tag{1.1}$$

In fact Ruppert stated this question using the naive height of α, but elementary inequalities between the two heights imply that (1.1) is equivalent to the bound that Ruppert proposed. Ruppert himself gave a positive answer to Question 1.1 for $d = 2$ ([**5**, Proposition 2]), and also for totally real number fields k of prime degree ([**5**, Proposition 3]). The analogous question for function fields in positive characteristic has been answered positively by the second author in [**8**]. In this note we give a positive answer for all number fields k having at least one embedding into $\mathbb{R}$, and with a constant $B \le 1$ for all such k. Our argument is a simple application of Minkowski's first theorem in the geometry of numbers over the adele space $k_{\mathbb{A}}$ associated to k.

1991 *Mathematics Subject Classification.* Primary 11R04, 11G50; Secondary 11R06, 11R29.
Key words and phrases. Algebraic number theory, small height.
The first author was supported in part by NSA Grant #H98230-12-1-0254.
The second author was supported by an FWF grant #M1222-N13.

THEOREM 1.2. *Let k be an algebraic number field with degree d over $\mathbb{Q}$ and assume that k has at least one embedding into $\mathbb{R}$. Then there exists an element α in k such that*

$$k = \mathbb{Q}(\alpha), \quad \text{and} \quad H(\alpha) \le \Big(\frac{2}{\pi}\Big)^{s/d} \big|\Delta_k\big|^{1/2d}, \tag{1.2}$$

where s is the number of complex places of k.

If all the embeddings of k into $\mathbb{C}$ are complex then the situation is more complicated. In this case an alternative application of Minkowski's first theorem over $k_{\mathbb{A}}$ leads to a bound that depends on the existence of certain rational prime numbers p such that the principal ideal $\langle p \rangle$ in O_k has a prime ideal factor with residue class degree equal to 1. It is also necessary that a finite product of such rational primes be slightly larger than $|\Delta_k|^{\frac{1}{2}}$. In order to establish the existence of such rational primes, we must assume that the Dedekind zeta-function $\zeta_l(s)$ associated with the Galois closure l of the extension $k/\mathbb{Q}$ satisfies the Generalized Riemann Hypothesis. This leads to a bound for the height of a generator as anticipated by Ruppert in (1.1), and with $B = B(d)$ depending effectively on the degree d.

THEOREM 1.3. *For each integer $d \ge 2$ there exists an effectively computable positive number $B = B(d)$ having the following property. Let k be an algebraic number field with degree d over $\mathbb{Q}$, let l be the Galois closure of the extension $k/\mathbb{Q}$, and assume that the Dedekind zeta-function $\zeta_l(s)$ associated to l satisfies the Generalized Riemann Hypothesis. Then there exists an element α in k such that*

$$k = \mathbb{Q}(\alpha), \quad \text{and} \quad H(\alpha) \le B\big|\Delta_k\big|^{1/2d}. \tag{1.3}$$

We obtain this conditional result by applying an effective version of the Chebotarev density theorem proved by Lagarias and Odlyzko in [**3**].

A lower bound for the height of a generator, somewhat analogous to the upper bounds (1.2) and (1.3), can be derived from a result of Silverman. More precisely, it follows from [**6**, Theorem 2] that for $2 \le d$ there exists a positive constant $b = b(d)$ such that if $k/\mathbb{Q}$ is an extension of degree d and α is an element of k with $k = \mathbb{Q}(\alpha)$, then

$$b\big|\Delta_k\big|^{1/2d(d-1)} \le H(\alpha). \tag{1.4}$$

A related problem concerning the existence of a vector space basis for the extension $k/\mathbb{Q}$ of relatively small projective height has been treated by Roy and Thunder [**4**].

2. Preliminaries

We suppose that r is the number of real places of k and s is the number of complex places of k, so that $r + 2s = d$. Then we define the field constant

$$c_k = \Big(\frac{2}{\pi}\Big)^{s/d} \big|\Delta_k\big|^{1/2d}. \tag{2.1}$$

We have

$$\Big(\frac{2}{\pi}\Big)^{\frac{1}{2}} \le \Big(\frac{2}{\pi}\Big)^{s/d} \le 1,$$

so that this factor is of no significance for our purposes here. However, the constant c_k occurs naturally in a basic formula for the Haar measure of certain subsets of the adele ring $k_{\mathbb{A}}$ associated to k. At each place v of k we let k_v denote the completion of

k with respect to an absolute value from v, and we write $d_v = d_v(k/\mathbb{Q}) = [k_v : \mathbb{Q}_v]$ for the local degree at v. Let $\| \ \|_v$ be the unique absolute value at the place v which extends either the usual Euclidean absolute value on $\mathbb{Q}$, or the usual p-adic absolute value on $\mathbb{Q}$. We also define a second absolute value $| \ |_v$ from the place v by setting

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

At each place v we define $O_v \subseteq k_v$ by

$$O_v = \begin{cases} \{\xi \in k_v : |\xi|_v < 1\} & \text{if } v|\infty, \\ \{\xi \in k_v : |\xi|_v \leq 1\} & \text{if } v \nmid \infty. \end{cases}$$

It follows that

$$\prod_v O_v \subseteq k_{\mathbb{A}},$$

and from the product formula we get

$$k \cap \prod_v O_v = \{0\}.$$

At each place v of k we select a Haar measure β_v defined on the Borel subsets of k_v and normalized as follows. If v is a real place then β_v is the ordinary Lebesgue measure, and if v is a complex place then β_v is the Lebesgue measure on $\mathbb{C}$ multiplied by 2. If v is a non-archimedean place then we require that

$$\beta_v(O_v) = |\mathcal{D}_v|_v^{d/2},$$

where $\mathcal{D}_v$ is the local different of k at v. Now let S be a finite subset of places of k containing all the archimedean places, and let

$$k_{\mathbb{A}}(S) = \prod_{v \in S} k_v \times \prod_{v \notin S} O_v$$

be the corresponding open subgroup of the additive group of $k_{\mathbb{A}}$. We write β for the unique Haar measure on the Borel subsets of $k_{\mathbb{A}}$ such that the restriction of β to each open subgroup $k_{\mathbb{A}}(S)$ is the product measure

$$\prod_v \beta_v.$$

The Haar measure β, normalized in this way, has the property that it induces a Haar measure β' on the Borel subsets of the compact quotient group $k_{\mathbb{A}}/k$ such that

$$\beta'\big(k_{\mathbb{A}}/k\big) = 1.$$

Using the basic identity

$$\prod_{v \nmid \infty} |\mathcal{D}_v|_v^{-d} = |\Delta_k|, \tag{2.2}$$

we find that

$$\beta\Big(\prod_v O_v\Big) = 2^d \Big(\frac{\pi}{2}\Big)^s \big|\Delta_k\big|^{-1/2} = 2^d c_k^{-d}. \tag{2.3}$$

Suppose more generally that $\gamma = (\gamma_v)$ is an element of the multiplicative group $k_{\mathbb{A}}^{\times}$ of ideles associated to k. Then at each place v of k we have

$$\gamma_v O_v = \begin{cases} \{\xi \in k_v : |\xi|_v < |\gamma_v|_v\} & \text{if } v|\infty, \\ \{\xi \in k_v : |\xi|_v \leq |\gamma_v|_v\} & \text{if } v \nmid \infty. \end{cases}$$

It follows that

$$\prod_v \gamma_v O_v \subseteq k_{\mathbb{A}},$$

and

$$\begin{aligned} \beta\Big(\prod_v \gamma_v O_v\Big) &= \prod_v \beta_v(\gamma_v O_v) \\ &= \prod_v \Big(\|\gamma_v\|_v^{d_v} \beta_v(O_v)\Big) \\ &= 2^d c_k^{-d} \Big(\prod_v |\gamma_v|_v\Big)^d. \end{aligned} \tag{2.4}$$

If

$$\prod_v |\gamma_v|_v \leq 1,$$

then from the product formula we get

$$k \cap \prod_v \gamma_v O_v = \{0\}.$$

On the other hand, if

$$c_k < \prod_v |\gamma_v|_v, \tag{2.5}$$

then there exists a nonzero point α in

$$k \cap \prod_v \gamma_v O_v.$$

That is, $\alpha \neq 0$ belongs to k and satisfies the system of inequalities

$$|\alpha|_v < |\gamma_v|_v \quad \text{if} \quad v|\infty, \tag{2.6}$$

and

$$|\alpha|_v \leq |\gamma_v|_v \quad \text{if} \quad v \nmid \infty. \tag{2.7}$$

The existence of α follows immediately from the adelic version of Minkowski's first theorem, (see [**2**, Theorem 3] for a more detailed account of geometry of numbers over adeles spaces.)

3. Proof of Theorem 1.2

If the number field k has an embedding into $\mathbb{R}$, then there exists an archimedean place w of k such that $k_w = \mathbb{R}$ and $[k_w : \mathbb{Q}_\infty] = 1$. Let ρ be a real parameter such that $c_k < \rho$. We select $\gamma = (\gamma_v)$ in $k_{\mathbb{A}}^{\times}$ so that

$$|\gamma_v|_v = \begin{cases} 1 & \text{if } v|\infty \text{ and } v \neq w, \\ \rho & \text{if } v = w, \\ 1 & \text{if } v \nmid \infty. \end{cases}$$

Because $c_k < \rho$ we have

$$c_k < \rho = \prod_v |\gamma_v|_v,$$

and this verifies (2.5). Hence there exists a point $\alpha \neq 0$ in

$$k \cap \prod_v \gamma_v O_v. \tag{3.1}$$

If w is the *only* archimedean place of k then

$$[k : \mathbb{Q}] = [k_w : \mathbb{Q}_\infty] = 1,$$

and the statement of the theorem is trivial. Hence we may assume that k has at least two archimedean places. Then (2.6) and (2.7) imply that α satisfies the inequalities

$$1 < |\alpha|_w < \rho, \quad \text{and} \quad H(\alpha) \leq \prod_v \max\{1, |\gamma_v|_v\} = \rho. \tag{3.2}$$

Let $\mathbb{Q}(\alpha) = k' \subseteq k$, and let u be an infinite place of k' such that $w|u$. Because α belongs to k', the map $v \mapsto \|\alpha\|_v$ is constant on the set of places v of k such that $v|u$. It follows from our choice of $\gamma = (\gamma_v)$ that w is the only place of k that lies over u. Then we have

$$[k : k'] = [k_w : k'_u] \leq [k_w : \mathbb{Q}_\infty] = 1,$$

and therefore $k = k' = \mathbb{Q}(\alpha)$. The inequality on the right of (3.2) shows that $H(\alpha) \leq \rho$ must hold for every positive number ρ such that $c_k < \rho$. Since the set of points in k with height bounded by a constant is finite, we conclude that $H(\alpha) \leq c_k$. This proves Theorem 1.2.

We note that for the collection of algebraic number fields k having an embedding into $\mathbb{R}$, Ruppert's Question 1.1 has a positive answer with $B = 1$. In particular, for this collection of number fields the constant B is independent of the degree of k over $\mathbb{Q}$.

4. A general strategy

In this section we consider an alternative argument using Minkowski's first theorem, but with a different choice of $\gamma = (\gamma_v)$. In view of Theorem 1.2 we are mainly interested in the case where k has no real embedding, but the argument we develop here applies to all number fields k. Let P be a finite set of rational prime numbers. Assume that for each prime p in P there exists a place v of k such that

$$v|p \quad \text{and} \quad f_v(k/\mathbb{Q}) = 1, \tag{4.1}$$

where $f_v(k/\mathbb{Q})$ is the residue class degree of the place v (or alternatively, the residue class degree of the associated prime ideal

$$\mathfrak{p} = \{\xi \in O_k : |\xi|_v < 1\},$$

where O_k is the ring of algebraic integers in k.) Then let S be a set of non-archimedean places of k selected so that S contains exactly one place v of k for each prime number p in P, and the places v in S satisfy (4.1). Obviously we have $|P| = |S|$.

Recall that if v is a finite place, then the positive integer $d_v(k/\mathbb{Q})$ factors as

$$d_v(k/\mathbb{Q}) = e_v(k/\mathbb{Q}) f_v(k/\mathbb{Q}), \tag{4.2}$$

where $e_v = e_v(k/\mathbb{Q})$ is the index of ramification and $f_v = f_v(k/\mathbb{Q})$ is the local residue class degree. If $v|p$ then we write π_v for an element that generates the unique maximal ideal in the integral domain O_v. We find that

$$\|\pi_v\|_v^{e_v} = p^{-1}, \quad \text{and} \quad |\pi_v|_v = p^{-f_v/d}. \tag{4.3}$$

Next we select $\gamma = (\gamma_v)$ in $k_{\mathbb{A}}^{\times}$ so that

$$\gamma_v = \begin{cases} \pi_v^{-1} & \text{if } v \text{ belongs to } S, \\ 1 & \text{if } v \text{ does not belong to } S. \end{cases} \tag{4.4}$$

Using (2.4) and (4.3) we find that

$$\beta\Big(\prod_v \gamma_v O_v\Big) = \Big(2c_k^{-1} \prod_{v\in S} |\pi_v^{-1}|_v\Big)^d = \big(2c_k^{-1}\big)^d \prod_{p\in P} p. \tag{4.5}$$

We now assume that P is selected so that

$$c_k < \Big(\prod_{p\in P} p\Big)^{1/d}. \tag{4.6}$$

By the adelic form of Minkowski's first theorem there exists a nonzero point α in the set

$$k \cap \prod_v \gamma_v O_v. \tag{4.7}$$

THEOREM 4.1. *Let P be a finite set of rational primes satisfying the above conditions, and in particular satisfying the inequality* (4.6)*. Then for each nonzero point α contained in the set* (4.7)*, we have*

$$\mathbb{Q}(\alpha) = k, \quad \textit{and} \quad H(\alpha) \le \Big(\prod_{p\in P} p\Big)^{1/d}. \tag{4.8}$$

PROOF. A nonzero point α contained in the set (4.7) satisfies the inequality

$$|\alpha|_v < 1$$

at each infinite place v of k. Hence it must satisfy

$$1 < |\alpha|_w \le |\pi_w|_w^{-1} \tag{4.9}$$

for at least one place w from the set S. Because the multiplicative value group of $|\ |_w$ on $k^{\times}$ is given by

$$\big\{|\pi_w|_w^m : m \in \mathbb{Z}\big\},$$

the inequality (4.9) implies that

$$|\alpha|_w = |\pi_w|_w^{-1} = q^{1/d}, \tag{4.10}$$

where q is the unique prime number in P such that $w|q$. Also, the height of α satisfies the bound

$$H(\alpha) = \prod_v \max\{1, |\alpha|_v\} \le \prod_{v\in S} \max\{1, |\pi_v|_v^{-1}\} = \Big(\prod_{p\in P} p\Big)^{1/d}. \tag{4.11}$$

This verifies the inequality on the right of (4.8).

Next we assume that $\mathbb{Q}(\alpha) = k' \subseteq k$. Let u be a place of k' such that $u|q$ and $w|u$. Then the ramification indices satisfy the identity

$$e_w(k/\mathbb{Q}) = e_w(k/k')e_u(k'/\mathbb{Q}). \tag{4.12}$$

And we can write (4.10) as

$$\log \|\alpha\|_w = \frac{\log q}{e_w(k/\mathbb{Q})}. \tag{4.13}$$

As α belongs to k', we also get

$$\log \|\alpha\|_w = \log \|\alpha\|_u = \frac{m \log q}{e_u(k'/\mathbb{Q})} \tag{4.14}$$

for some positive integer m. Combining (4.13) and (4.14) leads to the identity

$$m e_w(k/\mathbb{Q}) = e_u(k'/\mathbb{Q}). \tag{4.15}$$

Then (4.12) and (4.15) imply that $m = 1$ and

$$e_w(k/k') = 1. \tag{4.16}$$

Again because α belongs to the subfield k', the map $v \mapsto \|\alpha\|_v$ is constant on the collection of places v of k such that $v|u$. By our construction of S there is only one place v in S such that $v|q$ and $1 < |\alpha|_v$. Hence the collection of places v of k such that $v|u$ consists of exactly the place w. Using the hypothesis

$$f_w(k/\mathbb{Q}) = f_w(k/k') f_u(k'/\mathbb{Q}) = 1 \tag{4.17}$$

and (4.16), this implies that

$$[k : k'] = [k_w : k'_u] = e_w(k/k') f_w(k/k') = 1.$$

We have shown that $\mathbb{Q}(\alpha) = k' = k$. □

5. Application of Chebotarev's density theorem and GRH

Let L/K be a normal extension of algebraic number fields, and let C denote a conjugacy class in the Galois group $\mathrm{Aut}(L/K)$. Let $\mathfrak{p}$ denote a prime ideal in the ring O_K of algebraic integers in K. If $\mathfrak{p}$ is unramified in L, we use the Artin symbol

$$\left[\frac{L/K}{\mathfrak{p}}\right]$$

attached to $\mathfrak{p}$ to denote the conjugacy class of Frobenius automorphisms that correspond to prime ideals $\mathfrak{P}$ in O_L such that $\mathfrak{P}|\mathfrak{p}$. Then for $2 \le x$ we write $\pi_C(x; L/K)$ for the cardinality of the set of prime ideals $\mathfrak{p}$ in O_K such that $\mathfrak{p}$ is unramified in L,

$$\left[\frac{L/K}{\mathfrak{p}}\right] = C,$$

and

$$\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p}) \le x.$$

In its most basic form the Chebotarev density theorem (see [**7**]) asserts that

$$\lim_{x\to\infty} \frac{\pi_C(x; L/K)}{\mathrm{Li}(x)} = \frac{|C|}{[L : K]}, \tag{5.1}$$

where $|C|$ is the cardinality of the conjugacy class C, and

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\, \mathrm{d}t$$

is the logarithmic integral.

For our purposes it is useful to have an explicit estimate for the rate of convergence in (5.1). And it is important that the estimate apply for relatively small

values of the parameter x. Such an explicit, but conditional, estimate is given by a well known result of Lagarias and Odlyzko [**3**, Theorem 1.1], which we now describe. Let $\zeta_L(s)$ denote the Dedekind zeta-function associated to the number field L, where $s = \sigma + it$. We assume that $\zeta_L(s)$ satisfies the Generalized Riemann Hypothesis. Then [**3**, Theorem 1.1] implies that there exists an absolute and effectively computable constant $c_1 \geq 1$, such that, if $2 \leq x$ then

$$\left|\pi_C(x; L/K) - \frac{|C|}{[L:K]}\operatorname{Li}(x)\right| \leq c_1 x^{\frac{1}{2}}\big(\log|\Delta_L| + [L:\mathbb{Q}]\log x\big). \tag{5.2}$$

Let k be an algebraic number field of degree d over $\mathbb{Q}$. We apply the estimate (5.2) with L equal to the Galois closure of the extension $k/\mathbb{Q}$, and with $K = \mathbb{Q}$. Using the conjugacy class $C = \{1\}$, this will establish the existence of a rational prime number p that can be used to satisfy the hypotheses of Theorem 4.1.

LEMMA 5.1. *Let k be an algebraic number field of degree $d \geq 2$ over $\mathbb{Q}$, and let l be the Galois closure of the extension $k/\mathbb{Q}$. Assume that the Dedekind zeta-function $\zeta_l(s)$ associated to l satisfies the Generalized Riemann Hypothesis, and let C be a conjugacy class in the Galois group* $\operatorname{Aut}(l/\mathbb{Q})$. *If*

$$(15)^{20}c_1^{20}(d!)^{60} \leq |\Delta_k|, \tag{5.3}$$

then we have

$$1 \leq \pi_C\big(2|\Delta_k|^{\frac{1}{2}}; l/\mathbb{Q}\big) - \pi_C\big(|\Delta_k|^{\frac{1}{2}}; l/\mathbb{Q}\big). \tag{5.4}$$

PROOF. As l is the Galois closure of $k/\mathbb{Q}$ we find that $[l:\mathbb{Q}] \leq d!$, and

$$\log|\Delta_l| \leq 2(d!)^2\log|\Delta_k|. \tag{5.5}$$

The inequality (5.5) follows because a rational prime that ramifies in l must also ramify in k. Then by [**1**, Theorem B.2.12.] the order to which a rational prime divides Δ_l is bounded from above by $2[l:\mathbb{Q}]^2$. We apply these observations to the inequality (5.2) with $L = l$ and $K = \mathbb{Q}$. It follows that for $2 \leq x$ we have

$$\left|\pi_C(x; l/\mathbb{Q}) - \frac{|C|}{[l:\mathbb{Q}]}\operatorname{Li}(x)\right| \leq 2c_1(d!)^2 x^{\frac{1}{2}}\big(\log|\Delta_k| + \log x\big). \tag{5.6}$$

If the nonnegative integer on the right of (5.4) is zero, then (5.6) implies that

$$\operatorname{Li}\big(2|\Delta_k|^{\frac{1}{2}}\big) - \operatorname{Li}\big(|\Delta_k|^{\frac{1}{2}}\big) \leq 10c_1(d!)^3|\Delta_k|^{\frac{1}{4}}\log|\Delta_k|. \tag{5.7}$$

Therefore we get

$$\frac{2|\Delta_k|^{\frac{1}{2}}}{3\log|\Delta_k|} \leq \frac{|\Delta_k|^{\frac{1}{2}}}{\log 2|\Delta_k|^{\frac{1}{2}}} \leq \int_{|\Delta_k|^{\frac{1}{2}}}^{2|\Delta_k|^{\frac{1}{2}}} \frac{1}{\log t}\,\mathrm{d}t \leq 10c_1(d!)^3|\Delta_k|^{\frac{1}{4}}\log|\Delta_k|,$$

and then

$$|\Delta_k|^{\frac{1}{2}} \leq 15c_1(d!)^3|\Delta_k|^{\frac{1}{4}}\big(\log|\Delta_k|\big)^2. \tag{5.8}$$

It is now obvious that (5.8) is false if $|\Delta_k|$ is sufficiently large. An elementary calculation shows that (5.8) is false if $|\Delta_k|$ satisfies the inequality (5.3). Therefore (5.3) implies that the nonnegative integer on the right of (5.4) is positive. □

6. Proof of Theorem 1.3

We assume that the number field k satisfies the hypotheses of Theorem 1.3, and we also assume that

$$(15)^{20}c_1^{20}(d!)^{60} \le |\Delta_k|.$$

We apply Lemma 5.1 with the conjugacy class $C = \{1\}$. It follows that there exists a rational prime number p such that $\langle p\rangle$ splits completely in O_l and

$$|\Delta_k|^{\frac{1}{2}} < p \le 2|\Delta_k|^{\frac{1}{2}}.$$

Then $\langle p\rangle$ splits completely in O_k, and therefore the residue class degrees of all prime ideal factors of $\langle p\rangle$ in O_k are equal to 1. As each prime ideal factor corresponds to a non-archimedean place of k, we find that the hypotheses of Theorem 4.1 are satisfied with $P = \{p\}$. We conclude that there exists an element α in k such that $k = \mathbb{Q}(\alpha)$, and

$$H(\alpha) \le p^{1/d} \le 2|\Delta_k|^{1/2d}. \tag{6.1}$$

By Hermite's theorem there are only finitely many algebraic number fields k having degree d and satisfying the inequality

$$|\Delta_k| < (15)^{20}c_1^{20}(d!)^{60}. \tag{6.2}$$

As these can be effectively determined, there exists an effectively computable positive number $B = B(d) \ge 2$ such that the conclusion (1.3) holds for each field k having degree d and satisfying (6.2). In view of (6.1), the conclusion (1.3) holds for all fields k of degree d.

7. The field $\mathbb{Q}\big(\sqrt{-163}\big)$

Theorem 4.1 can be used to establish the existence of a generator α of $k/\mathbb{Q}$ with relatively small height. The bound obviously depends on identifying a finite set P of rational prime numbers that satisfies the hypotheses of that result. It may be of interest to observe that there are nontrivial examples where the bound obtained by applying Theorem 4.1 is sharp. In particular this is so for the imaginary quadratic field $\mathbb{Q}\big(\sqrt{-163}\big)$.

Lemma 7.1. *Let $d \le -1$ be a square free integer, let*

$$f(x) = ax^2 + bx + c$$

be a polynomial in $\mathbb{Z}[x]$ with

$$1 \le a, \quad 1 \le c, \quad \gcd(a,b,c) = 1, \quad \text{and} \quad b^2 - 4ac = de^2,$$

where e is a nonzero integer. If α is a root of f, then $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$ and

$$H(\alpha) = \max\{a,c\}^{\frac{1}{2}}. \tag{7.1}$$

Proof. That $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$ is obvious. For the remainder of the proof we work in $\mathbb{Q}(\sqrt{d})$ embedded in $\mathbb{C}$. Then complex conjugation is the unique nontrivial automorphism of $\mathbb{Q}(\sqrt{d})$, and the distinct roots of f are α and $\overline{\alpha}$. Hence the Mahler measure of f is

$$M(f) = a\max\{1,|\alpha|\}\max\{1,|\overline{\alpha}|\} = a\max\{1,\alpha\overline{\alpha}\} = \max\{a,c\}.$$

Because f is the unique irreducible polynomial in $\mathbb{Z}[x]$ with positive leading coefficient and a root at α, the Mahler measure is also given by

$$M(f) = H(\alpha)H(\overline{\alpha}) = H(\alpha)^2.$$

The result follows by combining these identities. □

A rational prime p will satisfy the hypotheses (4.1) for the field $\mathbb{Q}(\sqrt{-163})$ if and only if either p is odd and -163 is a quadratic residue modulo p, or $p = 163$. The smallest odd prime number p such that -163 is a quadratic residue modulo p is 41. We have $\Delta_k = -163$ and therefore

$$c_k = 2.850\cdots < \sqrt{41} = 6.403\cdots .$$

We conclude that Theorem 4.1 applies with $P = \{41\}$, and asserts that $\mathbb{Q}(\sqrt{-163})$ has a generator α such that

$$H(\alpha) \le \sqrt{41}.$$

Now let α' be a root of the polynomial $x^2 + x + 41$, which has discriminant -163. Clearly α' generates the imaginary quadratic field $\mathbb{Q}\big(\sqrt{-163}\big)$. Then by Lemma 7.1 we have

$$H\big(\alpha'\big) = \sqrt{41}.$$

The set of polynomials $f(x) = ax^2 + bx + c$ in $\mathbb{Z}[x]$ such that

$$1 \le a, \quad 1 \le c, \quad \gcd(a, b, c) = 1, \quad \text{and} \quad b^2 - 4ac = (-163)e^2,$$

where e is a nonzero integer, and

$$\max\{a, c\} \le 41, \tag{7.2}$$

is obviously finite. It is then a simple matter, using Lemma 7.1, to check that the the field $\mathbb{Q}\big(\sqrt{-163}\big)$ does not have a generator with height strictly smaller than $\sqrt{41}$. Therefore the inequality obtained in Theorem 4.1 for this field is sharp.

References

1. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
2. E. Bombieri and J. D. Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), 11–32.
3. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem. Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 409-464*, Academic Press Inc., New York, 1977.
4. D. Roy and J. L. Thunder, *Bases of number fields with small height*, Rocky Mountain J. Math. **26, no.3** (1996), 1089–1098.
5. W. Ruppert, *Small generators of number fields*, Manuscripta math. **96** (1998), 17–22.
6. J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
7. N. Tschebotareff, *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. **95** (1926), 191–228.
8. M. Widmer, *Small generators of function fields*, J. Théor. Nombres Bordeaux **22** (2010), 544–551.

Department of Mathematics, University of Texas at Austin, 1 University Station C1200, Austin, Texas 78712

E-mail address: vaaler@math.utexas.edu

Department for Analysis and Computational Number Theory, Graz University of Technology, 8010 Graz, Austria

E-mail address: widmer@math.tugraz.at