SMALL GENERATORS OF ABELIAN NUMBER FIELDS

MARTIN WIDMER

ABSTRACT. We show that for each abelian number field K of sufficiently large degree d there exists an element $\alpha \in K$ with $K = \mathbb{Q}(\alpha)$ and absolute Weil height $H(\alpha) \ll_d |\Delta_K|^{1/2d}$, where Δ_K denotes the discriminant of K. This answers a question of Ruppert from 1998 in the case of abelian extensions of sufficiently large degree. We also show that the exponent $1/2d$ is best-possible when d is even.

1. INTRODUCTION

In this article we answer Ruppert's question on small generators of number fields for abelian fields of sufficiently large degree. We also show that Ruppert's proposed bound is sharp when the degree is even.

Let K be a number field, and for $\alpha \in K$ let

$$H(\alpha) = \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{\frac{d_v}{[K:\mathbb{Q}]}}$$

be the absolute multiplicative Weil height of α. Here M_K denotes the set of places of K and for each place v we choose the unique representative $|\cdot|_v$ that either extends the usual Archimedean absolute value on $\mathbb{Q}$ or a usual p-adic absolute value on $\mathbb{Q}$, and $d_v = [K_v : \mathbb{Q}_v]$ denotes the local degree at v. By the product formula $H(\alpha)$ is independent of the number field K containing α, and thus $H(\cdot)$ is a well-defined function on the algebraic numbers $\overline{\mathbb{Q}}$. For an extension K/F of number fields we write

$$\delta(K/F) = \min\{H(\alpha); K = F(\alpha)\}.$$

Northcott's Theorem[1] implies that the above minimum exists, and thus $\delta(K/F)$ is well-defined. We write Δ_K for the discriminant of K. In 1998 Ruppert [11, Question 2] proposed the following question.

Question 1. *[Ruppert, 1998] Let $d > 1$ be an integer. Is it true that*

$$\delta(K/\mathbb{Q}) \ll_d |\Delta_K|^{\frac{1}{2d}} \tag{1.1}$$

for every number field K of degree d?

Ruppert showed that for $d = 2$ the answer is yes. In [13] an affirmative answer to Ruppert's question was given for all number fields K that have a real embedding, confirming (1.1) for all odd d. In the same article it was also shown that (1.1) holds, provided the Riemann-hypothesis for the Dedekind-zeta function of the Galois closure $K^{(G)}$ of $K/\mathbb{Q}$ holds true.

Pierce, Turnage-Butterbaugh and Wood [9, Theorem 8.2] have shown that (1.1) holds for 100% (when enumerated by modulus of their discriminant) of all number fields in

Date: March 25, 2024.

2010 *Mathematics Subject Classification.* Primary 11R04; 11G50 Secondary 11R29; 11R06.

Key words and phrases. Weil height, small generators, Ruppert's conjecture, abelian number fields, Linnik's Theorem.

[1] Northcott's Theorem states that given a positive integer d and a real number $X \geq 1$ there are only finitely many algebraic numbers α of degree d with $H(\alpha) \leq X$.

various families of degree d-extensions with prescribed Galois group and certain conditions on the ramification types[2].

Very recently Akhtari, Vaaler, and the author [1, Theorem 1.3] showed that (1.1) can only fail for totally complex fields K that are Galois over their maximal totally real subfield F. Hence, all these exceptional fields do have a subfield of index 2, namely the fixed field of the group generated by complex conjugation. This implies that, apart from the families of cyclic number fields [9, Theorem 3.3, (1)], the unconditional parts of the "almost all" result [9, Theorem 8.2] are superseded[3] by the recent pointwise result [1, Theorem 1.3].

Regarding cyclic, and more generally abelian, number fields, we have the following pointwise result.

Theorem 1. *Let L be the effectively computable constant from (3.16), and suppose $d \geq 4L$. Then, apart from finitely many exceptional fields, we have*

$$\delta(K/\mathbb{Q}) \leq (25|\Delta_K|)^{\frac{1}{2d}}$$

for each abelian number field K of degree d.

The proof is a combination of well-known facts, classical tools, and [13, Theorem 1.4], which yields (1.1) provided there exists a product of distinct degree one primes of size between $|\Delta_K|^{1/2}$ and $\gamma|\Delta_K|^{1/2}$ (for some $\gamma = \gamma_d > 1$).

For abelian number fields a sufficient condition for the splitting of a prime p can be given in terms of a congruence condition modulo the conductor $\mathfrak{f}$ of K. The latter is related to the discriminant by Hasse's conductor-discriminant formula, and one can show that $\mathfrak{f} \leq |\Delta_K|^{2/d}$. Linnik's Theorem provides a prime p in the required residue class modulo $\mathfrak{f}$ and satisfying $p \leq \mathfrak{f}^L$, where L is an absolute constant (usually called Linnik's constant). This upper bound is sufficient as long as $d \geq 4L$. We also need $p > |\Delta_K|^{1/2}$ but a minor adjustment to the proof of Linnik's Theorem allows one to take care of this additional constraint.

For abelian fields of small degree better bounds for the least splitting prime p were obtained by Pollack [10] (see also [18] for an extension to certain non-abelian number fields). The proof is based on the observation that a lower bound on the number of ideals of bounded norm furnishes an upper bound on the smallest splitting prime. Unfortunately, it is unclear how to use this method to establish a splitting prime p in the required interval $|\Delta_K|^{1/2} < p \ll_d |\Delta_K|^{1/2}$.

The constant L in Theorem 1 is expressed in terms of the constants c, c_1, c_2, c_3 that arise from the three fundamental principles Linnik's Theorem is based upon (cf. Section 2). These four constants are all explicitly computable and are subject to further improvement. However, getting good values requires rather tedious computations, which come at the expense of clarity and simplicity of the proof. But even the strongest methods (as developed in [6] and [17]) would at very best lead to the bound $L = 5$, leaving the cases $2 < d < 20$ still open. Therefore, we have not attempted to present explicit values for c, c_1, c_2, and c_3.

---

[2]Some of their results are conditional on the strong Artin conjecture (but not the Riemann-hypothesis for the corresponding Dedekind-zeta function).

[3]The families of even degree considered in [9, Theorem 8.2] are (certain) d-extensions K with $\mathrm{Gal}(K^{(G)}/\mathbb{Q})$ isomorphic to either A_d, S_d, a cyclic group, or a simple group (the latter being conditional on the strong Artin conjecture). Each subgroup of A_d or S_d of index d is some A_{d-1} or S_{d-1} respectively, and there is neither a proper intermediate group between A_{d-1} and A_d nor between S_{d-1} and S_d. Hence, these fields K cannot have a subfield of index 2 if $d > 2$.

It is also worthwhile mentioning that the bound (1.1) is stable under taking composite fields with coprime discriminants. To see this let $\alpha_i \in K_i$ with

$$\delta(K_i/\mathbb{Q}) = H(\alpha_i) \ll_{d_i} |\Delta_{K_i}|^{\frac{1}{2d_i}} \quad (1 \le i \le 2).$$

There exists a generator $\alpha = m_1\alpha_1 + m_2\alpha_2$ of $K = K_1K_2$ with rational integers $0 \le m_i < d = [K : \mathbb{Q}]$ (see, e.g., [16, Lemma 3.3]). If $(\Delta_{K_1}, \Delta_{K_2}) = 1$ then it follows (cf. [8, Theorem 4.9]) that $d = d_1d_2$ and[4]

$$|\Delta_K| = |\Delta_{K_1}^{d_2}\Delta_{K_2}^{d_1}|,$$

and thus

$$\delta(K/\mathbb{Q}) \le H(\alpha) \ll_d |\Delta_{K_1}|^{\frac{1}{2d_1}}|\Delta_{K_2}|^{\frac{1}{2d_2}} = |\Delta_K|^{\frac{1}{2d}}.$$

Can the exponent $1/2d$ in (1.1) be improved? A well-known result of Silverman [12, Theorem 1.1] implies that

$$\delta(K/\mathbb{Q}) \gg_d |\Delta_K|^{\frac{1}{2d(d-1)}}. \tag{1.2}$$

Ruppert's [11, Theorem 1.1] shows that for $d = 2$ the reversed inequality holds true as well. This suggests the following strengthening of Question 1.1, also proposed by Ruppert [11, Question 1].

Question 2. *[Ruppert, 1998] Let $d > 1$ be an integer. Is it true that*

$$\delta(K/\mathbb{Q}) \ll_d |\Delta_K|^{\frac{1}{2d(d-1)}} \tag{1.3}$$

for every number field K of degree d?

However, Vaaler and the author [14, Theorem 1.2] have shown that there exist infinitely many number fields K of degree d with

$$\delta(K/\mathbb{Q}) \ge |\Delta_K|^{\gamma} \tag{1.4}$$

whenever

$$\gamma < \begin{cases} 1/((b+1)d) : & \text{if } b \le 3, \\ 1/(2(b+1)d) + 1/(b^2(b+1)d) : & \text{otherwise.} \end{cases} \tag{1.5}$$

Here $b = b(d) > 1$ denotes the smallest divisor of d. This provides a negative answer to Question 2 when d is composite.

A negative answer was also given [14, Theorem 1.3] for prime $d > 3$, conditional on a weak form of a folklore conjecture about the distribution of number fields. Very recently Dubickas [3, Theorem 1] showed unconditionally that for odd d one can take

$$\gamma = \frac{d+1}{2d^2(d-1)}, \tag{1.6}$$

hence showing that Ruppert's Question 2 has a negative answer also for prime $d > 2$. While the bound (1.5) is better for composite d than (1.6) Dubickas provides an explicit family of fields whereas there is no such description for the fields in [14, Theorem 1.2 and Corollary 4.1].

Our next result shows that for even d the exponent $1/2d$ in (1.1) cannot be replaced by any smaller value. Furthermore, it improves the exponents γ in (1.5) and (1.6) when d is composite and $b \ne 3$, and it provides an explicit description of the fields K. On the other hand the method in [14] (cf. [14, Corollary 4.2]) also provides density statements which we do not recover here.

[4] In fact, $d = d_1d_2$ implies that already $\alpha = \alpha_1 + \alpha_2$ is a generator of K, as was shown by Isaac (cf. [15, Theorem 1.3]).

Theorem 2. *Let m and $n > 1$ be positive integers, and set $d = mn$. Then there are infinitely many number fields K of degree d such that*

$$\frac{1}{\sqrt{2d}}|\Delta_K|^{\frac{1}{2d(n-1)}} \le \delta(K/\mathbb{Q}) \le (2d)^2|\Delta_K|^{\frac{1}{2d(n-1)}}.$$

More precisely, the above bounds hold for each $K = \mathbb{Q}(2^{1/m}, (p/q)^{1/n})$ where p and q are primes satisfying $m < p < q < 2p$.

The aforementioned optimality of the exponent $1/2d$ in (1.1) for even d follows from the lower bound by taking $n = 2$. Theorem 2 is a simple consequence of an observation of Ruppert (and independently of Masser), and a standard height inequality of Silverman.

In [14] it was proposed to determine the cluster points[5] of the set

$$\left\{\frac{\log \delta(K/\mathbb{Q})}{\log|\Delta_K|}; [K:\mathbb{Q}] = d\right\}.$$

Ruppert [11] has shown that $1/(2d(d-1))$ is the smallest cluster point, and for $d = 3$ Dubickas has recently shown that $1/9$ is a cluster point. Theorem 2 shows that $1/2d(n-1)$ is a cluster point for every divisor $n > 1$ of d.

ACKNOWLEDGEMENTS

It is my pleasure to thank Glyn Harman, for pointing out that a lower bound as in Lemma 3 can be derived by an easy adaptation of the usual proof of Linnik's theorem, and to Marc Technau, for showing that Lemma 2 follows easily from [7, Proposition 18.5]. I am also grateful to Shabnam Akhtari and Jeffrey Vaaler for many fruitful and interesting discussions on Ruppert's questions and beyond. I also would like to thank the reviewer for many helpful comments that improved the exposition of this article.

2. PRIMES OF A GIVEN RESIDUE CLASS IN SHORT INTERVALS

For $x \ge 1$ and coprime positive integers a and $q \ge 2$ let

$$\pi(x;q,a) = \sum_{\substack{p\le x\\ p\equiv a \pmod q}} 1,$$
$$\psi(x;q,a) = \sum_{\substack{n\le x\\ n\equiv a \pmod q}} \Lambda(n),$$

where in the first sum p denotes a prime, and in the second sum $\Lambda(\cdot)$ denotes the von Mangoldt function. Noting that

$$\psi(x;q,a) = \sum_{\substack{p\le x\\ p\equiv a \pmod q}} \left\lfloor \frac{\log x}{\log p}\right\rfloor \log p,$$

and splitting the sum in $p \le \sqrt{x}$ and $p > \sqrt{x}$ gives the inequalities

$$\frac{1}{2}\log x\left(\pi(x;q,a) - \pi(\sqrt{x};q,a)\right) \le \psi(x;q,a) \le \log x\left(\pi(x;q,a) + \pi(\sqrt{x};q,a)\right).$$

[5] What the authors in [14] meant by "cluster point of the set $\left\{\frac{\log\delta(K/\mathbb{Q})}{\log|\Delta_K|}; [K:\mathbb{Q}] = d\right\}$" is a real number η such that for each $\varepsilon > 0$ there are infinitely many number fields K of degree d with $\left|\frac{\log\delta(K/\mathbb{Q})}{\log|\Delta_K|} - \eta\right| < \varepsilon$.

This in turn yields for $y > x \geq 2$

$$\pi(y;q,a) - \pi(x;q,a) \geq \frac{\psi(y;q,a)}{\log y} - \frac{2\psi(x;q,a)}{\log x} + O\left(\frac{\sqrt{y}}{\log y}\right), \tag{2.7}$$

where the implicit constant in the O-term is absolute.

As explained in Section 3, to prove Theorem 1 it suffices to prove a positive lower bound for

$$\pi(y;q,a) - \pi(x;q,a),$$

when $y = \gamma x$ for some absolute $\gamma > 1$ and x is of size $q^{d/4}$.

Such a lower bound can be deduced by an easy adaptation of the usual proof of Linnik's theorem, provided d is sufficiently big. We follow Iwaniec-Kowalski [7] which itself borrows significantly from Graham's work [5, 4]. However, to keep track of the constants which determine the threshold $4L$ for the degree in Theorem 1 we need to give some background.

Following [7] we write $s = \sigma + it$ and $L_q(s)$ for the product of all Dirichlet L-functions associated to Dirichlet characters χ modulo q

$$L_q(s) = \prod_{\chi \pmod q} L(s,\chi).$$

For $\frac{1}{2} \leq \alpha \leq 1$, and $T \geq 1$ we write

$$N_q(\alpha, T)$$

for the number of zeros of $L_q(s)$, counted with multiplicity, with real part $\alpha < \sigma \leq 1$, and modulus of the imaginary part $|t| \leq T$.

The proof of Linnik's Theorem rests on the following three principles which we quote from [7][6].

Principle 1 (The zero-free region)**.** *There is an effectively computable positive constant c_1 such that $L_q(s)$ has at most one zero in the region*

$$\sigma \geq 1 - c_1/2\log q, \quad |t| \leq q.$$

The exceptional zero, if it exists, is real and simple, and it is for a real, non-principal character.

Principle 2 (The log-free zero-density estimate)**.** *There are effectively computable positive constants c, c_2 such that for any $\frac{1}{2} \leq \alpha \leq 1$*

$$N_q(\alpha, q) \leq c q^{2c_2(1-\alpha)}.$$

Principle 3 (The exceptional zero repulsion)**.** *There is an effectively computable positive constant c_3 such that if the exceptional zero β_1 from Principle 1 exists, say $L(\beta_1, \chi_1) = 0$ with*

$$1 - c_1/2\log q \leq \beta_1 < 1,$$

then the function $L_q(s)$ has no other zeros in the region

$$\sigma \geq 1 - c_3 \frac{|\log(1-\beta_1)|}{2\log q}, \quad |t| \leq q.$$

For the effectively computable constants from Principle 1, 2, and 3 we assume (as we can) throughout this section that

$$c, c_2 > 1 > c_1, c_3 > 0.$$

[6] In [7] the authors state these principles for more general ranges $|t| \leq T$ but only apply them with $T = q$. The authors [7, Section 18.1, p. 429] remark that for q sufficiently large and $T \leq \log q$ one can choose $c_1 = 1/10, c_2 = 3, c_3 = 1/2$ (they provide no value for c). However, following [7] we choose $T = q$, and thus these values may not be eligible in our setting.

We say that the real number β_1 is an exceptional zero of $L_q(s)$ if there exists a real character χ_1 modulo q for which $L(\beta_1, \chi_1) = 0$, and $\beta_1 = 1 - \delta_1$ with

$$0 < \delta_1 \le \frac{c_1}{2\log q}.$$

Let

$$\eta = \begin{cases} c_3 \frac{|\log(2\delta_1 \log q)|}{2\log q} & \text{if the exceptional zero } \beta_1 \text{ does exist,} \\ \frac{c_1}{2\log q} & \text{if } \beta_1 \text{ does not exist.} \end{cases} \tag{2.8}$$

We will use [7, Proposition 18.5] which we state as a lemma.

Lemma 1. [7, Proposition 18.5] *Let c, c_1, c_2, c_3 be the absolute constants from Principles 1, 2, 3. Let*

$$\lambda = \chi_1(a)\frac{x^{\beta_1 - 1}}{\beta_1}$$

if the exceptional zero β_1 does exist and $\lambda = 0$ if β_1 does not exist. Then for $x \ge q^{4c_2}$ we have

$$\psi(x; q, a) = \frac{x}{\phi(q)}\left\{1 - \lambda + \theta c x^{-\eta/2} + O\left(\frac{\log q}{q}\right)\right\}$$

where η is as in (2.8) and $|\theta| \le 4$, and the implied constant is absolute.

Next we consider the quantity[7] ν from [7, (18.90)], but we allow an additional real parameter U, and we set

$$\nu = \max\left\{4c_2, \frac{4}{c_1}, \frac{4}{c_3}, \frac{4\log(2Uc)}{c_3|\log c_1|}\right\}. \tag{2.9}$$

Lemma 2. *Suppose the exceptional zero β_1 of $L_q(s)$ exists, let $U \ge 1$, and let $\gamma \ge 5$. Further, suppose that $x \ge q^{\nu}$. Then*

$$\psi(\gamma x; q, a) - 3\psi(x; q, a) \ge \frac{x}{\phi(q)}\left\{\left[\frac{4(\gamma-3)}{3c_1} - \frac{4(\gamma+3)}{Uc_1} - \frac{(\gamma-3)}{\log q}\right]\delta_1 \log q + O\left(\frac{\gamma \log q}{q}\right)\right\},$$

where the implied constant is absolute.

Proof. Let c, c_1, c_2 and c_3 be the absolute constants from Principles 1, 2, 3, and let η be as in (2.8). Applying Lemma 1 we get

$$\begin{aligned}\psi(\gamma x; q, a) - 3\psi(x; q, a) =& \frac{\gamma x}{\phi(q)}\left\{1 - \chi_1(a)\frac{(\gamma x)^{\beta_1 - 1}}{\beta_1} + \theta_1 c(\gamma x)^{-\eta/2} + O\left(\frac{\log q}{q}\right)\right\} \\ &- \frac{3x}{\phi(q)}\left\{1 - \chi_1(a)\frac{x^{\beta_1-1}}{\beta_1} + \theta_2 c x^{-\eta/2} + O\left(\frac{\log q}{q}\right)\right\} \\ =& \frac{x}{\phi(q)}\left\{(\gamma - 3) - (\gamma^{\beta_1} - 3)\chi_1(a)\frac{x^{\beta_1-1}}{\beta_1} + (\theta_1\gamma^{1-\eta/2} - 3\theta_2)cx^{-\eta/2} + O\left(\frac{\gamma\log q}{q}\right)\right\}\end{aligned}$$

for some $|\theta_i| \le 4$. Since $\gamma \ge 5$ we have $\left|\gamma^{\beta_1} - 3\right| \le \gamma - 3$, and since $|\theta_i| \le 4$ we get $|\theta_1\gamma^{1-\eta/2} - 3\theta_2| \le 4(\gamma + 3)$. Hence,

$$\psi(\gamma x; q, a) - 3\psi(x; q, a) \ge \frac{x}{\phi(q)}\left\{(\gamma - 3)\left(1 - |\chi_1(a)|\frac{x^{\beta_1-1}}{\beta_1}\right) - 4(\gamma+3)cx^{-\eta/2} + O\left(\frac{\gamma\log q}{q}\right)\right\}. \tag{2.10}$$

[7] We have additionally included the term $4/c_3$ as $\nu \ge 4/c_3$ is used in [7] without mentioning.

Now following [7, p. 441] we get

$$1-|\chi_1(a)|\frac{x^{\beta_1-1}}{\beta_1}\geq 1-\frac{x^{-\delta_1}}{\beta_1}\geq \beta_1-q^{-\nu\delta_1}=1-q^{-\nu\delta_1}-\delta_1\geq \frac{\nu\delta_1\log q}{1+\nu\delta_1\log q}-\delta_1\geq \frac{\nu\delta_1\log q}{1+\frac{\nu c_1}{2}}-\delta_1$$

$$\geq \frac{4\delta_1}{3c_1}\log q-\delta_1. \tag{2.11}$$

Furthermore, following [7, p. 441] and using that $\nu c_3/4\geq 1$, we get

$$x^{-\eta/2}\leq q^{-\nu\eta/2}=(2\delta_1\log q)^{\nu c_3/4}\leq (2\delta_1\log q)c_1^{\nu c_3/4-1}\leq \frac{\delta_1}{Ucc_1}\log q. \tag{2.12}$$

Finally, plugging (2.11) and (2.12) into (2.10) yields

$$\psi(\gamma x;q,a)-3\psi(x;q,a)\geq \frac{x}{\phi(q)}\left\{\left[\frac{4(\gamma-3)}{3c_1}-\frac{4(\gamma+3)}{Uc_1}-\frac{(\gamma-3)}{\log q}\right]\delta_1\log q+O\left(\frac{\gamma\log q}{q}\right)\right\}.$$

□

Lemma 3. *Let $5\leq\gamma\leq\sqrt{x}$, let $U>3\left(\frac{\gamma+3}{\gamma-3}\right)$, and let*

$$L_U=\max\left\{4c_2,\frac{4}{c_3},\frac{4\log(2Uc)}{c_1},\frac{4\log(2Uc)}{c_3|\log c_1|}\right\}. \tag{2.13}$$

There exists q_0 such that for $q\geq q_0$ and $x\geq q^{L_U}$

$$\pi(\gamma x;q,a)-\pi(x;q,a)\gg_{\gamma,U,c_1,q_0}\frac{x}{\phi(q)\sqrt{q}\log\gamma x}.$$

Proof. From (2.7), and using that $q\leq x^{1/L_U}\leq x^{1/4}$, we see that it suffices to show that

$$\frac{\psi(\gamma x;q,a)}{\log\gamma x}-\frac{2\psi(x;q,a)}{\log x}\gg_{\gamma,U,c_1,q_0}\frac{x}{\phi(q)\sqrt{q}\log\gamma x}. \tag{2.14}$$

Since $\gamma\leq\sqrt{x}$ we have

$$\frac{\psi(\gamma x;q,a)}{\log\gamma x}-\frac{2\psi(x;q,a)}{\log x}\geq\frac{1}{\log\gamma x}\left(\psi(\gamma x;q,a)-3\psi(x;q,a)\right). \tag{2.15}$$

First suppose the exceptional zero β_1 of $L_q(s)$ exists. Then (2.14) follows immediately from (2.15) and Lemma 2 upon noticing that $\delta_1\log q\gg q^{-1/2}$ by Siegel's Theorem[8].

Next suppose the exceptional zero β_1 does not exists so that $\eta=c_1/(2\log q)$. Applying Lemma 1, and using that $x\geq q^{\frac{4\log(2Uc)}{c_1}}$, yields

$$\begin{aligned}\psi(\gamma x;q,a)-3\psi(x;q,a)=&\frac{x}{\phi(q)}\left\{(\gamma-3)+(\theta_1\gamma^{1-\eta/2}-3\theta_2)cx^{-\eta/2}+O\left(\frac{\gamma\log q}{q}\right)\right\}\\ \geq&\frac{x}{\phi(q)}\left\{(\gamma-3)-4(\gamma+3)cx^{-\eta/2}+O\left(\frac{\gamma\log q}{q}\right)\right\}\\ \geq&\frac{x}{\phi(q)}\left\{(\gamma-3)-\frac{2(\gamma+3)}{U}+O\left(\frac{\gamma\log q}{q}\right)\right\}\gg_{\gamma,U,q_0}\frac{x}{\phi(q)\sqrt{q}}.\end{aligned}$$

This in conjunction with (2.15) proves (2.14). □

[8]Siegel's Theorem states that for every $\varepsilon>0$ there exists $c_\varepsilon>0$ such that $\delta_1\geq c_\varepsilon q^{-\varepsilon}$.

3. Proof of Theorem 1

We will apply Theorem 4.1 from [13]. Here we state only a special case, sufficient for our purposes.

Theorem 3. [13, Theorem 4.1] *Let K be a number field of degree d, and let $p > |\Delta_K|^{1/2}$ be a prime that splits completely in K. Then there exists $\alpha \in K$ with $K = \mathbb{Q}(\alpha)$ and $H(\alpha) \le p^{1/d}$.*

If K is an abelian number field of conductor $\mathfrak{f}$ then any prime $p \equiv 1 \pmod{\mathfrak{f}}$ splits completely in K (cf. [8, Theorem 8.1]). Thus, to prove Theorem 1 it suffices to show that, apart from finitely many exceptional fields, there exists a prime $p \equiv 1 \pmod{\mathfrak{f}}$ with $|\Delta_K|^{1/2} < p \le 5|\Delta_K|^{1/2}$. Let $c, c_2 > 1 > c_1, c_3 > 0$ be the absolute constants from Principles 1, 2, 3. We apply Lemma 3 with $\gamma = 5$, $U = 13$, $a = 1$, and $q = \mathfrak{f}$ to conclude that if $\mathfrak{f}$ is sufficiently large then there exists a prime p that splits completely in K and satisfies $x < p \le 5x$, provided $x \ge \mathfrak{f}^L$ where

$$L = L_{13} = \max\left\{4c_2, \frac{4}{c_3}, \frac{4\log(26c)}{c_1}, \frac{4\log(26c)}{c_3|\log c_1|}\right\}. \tag{3.16}$$

We note that $\mathfrak{f} \le |\Delta_K|^{2/d}$ (see [2, Lemma 9.2.1]). Since $d \ge 4L$ the hypothesis $x \ge \mathfrak{f}^L$ holds for $x = |\Delta_K|^{1/2}$, and thus we conclude that there exists a splitting prime p with $|\Delta_K|^{1/2} < p \le 5|\Delta_K|^{1/2}$ whenever $\mathfrak{f}$ is sufficiently large. Thus Theorem 3 yields a sufficiently small generator for these fields. Finally, as there are only finitely many abelian fields of degree d with conductor below a given bound the proof of Theorem 1 is complete.

4. Proof of Theorem 2

Theorem 2 is an immediate consequence of the following proposition.

Proposition 1. *Let m and $n > 1$ be positive integers, let F be a number field of degree $m = [F : \mathbb{Q}]$, and set $d = mn$.*
(1) Let K be a field extension of F of degree $n = [K : F]$. Then we have

$$\delta(K/\mathbb{Q}) \ge (n^m|\Delta_F|)^{-\frac{1}{2m(n-1)}}\,|\Delta_K|^{\frac{1}{2d(n-1)}}.$$

(2) Let $K = F((p/q)^{1/n})$ where p and q are primes, p is unramified in F and $p < q < 2p$. Then $[K : F] = n$ and

$$\delta(K/\mathbb{Q}) \le 2^{1+\frac{1}{2n}} d^2 \delta(F/\mathbb{Q})|\Delta_K|^{\frac{1}{2d(n-1)}}.$$

Proof. By a result of Silverman [12, Theorem 2] we have

$$H(\alpha) \ge n^{-\frac{1}{2(n-1)}} N_{F/\mathbb{Q}}(D(K/F))^{\frac{1}{2d(n-1)}}$$

whenever $K = F(\alpha)$. Here $D_{K/F}$ denotes the relative discriminant of K/F and $N_{F/\mathbb{Q}}(\cdot)$ is the norm from F to $\mathbb{Q}$. Since $N_{F/\mathbb{Q}}(D(K/F)) = |\Delta_F|^{-n}|\Delta_K|$ the first part follows immediately.

For the second part we start with an observation of Ruppert [11]: let $\alpha = (p/q)^{1/n}$ and set $M = \mathbb{Q}(\alpha)$. Then $H(\alpha) = q^{1/n}$ and $(pq)^{n-1}|\Delta_M$. Thus $(q^2/2)^{n-1} \le |\Delta_M|$, and hence $H(\alpha) \le 2^{1/2n}|\Delta_M|^{1/2n(n-1)}$. Next let $\beta \in F$ be such that $F = \mathbb{Q}(\beta)$. Hence, $K = \mathbb{Q}(\alpha, \beta)$. There are integers $0 \le a, b < d$ such that with $\gamma = a\alpha + b\beta$ we have $K = \mathbb{Q}(\gamma)$ (see, e.g., [16, Lemma 3.3]). As p is unramified in F and totally ramified in M we conclude that $[MF : F] = [M : \mathbb{Q}]$, hence $[K : F] = n$. By standard properties of the height we get $H(\gamma) \le 2d^2 H(\alpha)H(\beta)$. Choosing the β with minimal height we conclude

$$\delta(K/\mathbb{Q}) \le 2^{1+\frac{1}{2n}} d^2 \delta(F/\mathbb{Q})|\Delta_M|^{\frac{1}{2n(n-1)}}. \tag{4.17}$$

Finally, noticing that $[K : M] = m$ and thus $\Delta_M^m | \Delta_K$ the second claim follows from (4.17). □

Theorem 2 follows now easily from Proposition 1. Let $F = \mathbb{Q}(2^{1/m})$ so that $[F : \mathbb{Q}] = m$, $\delta(F/\mathbb{Q}) \leq 2^{1/m}$, and $|\Delta_F| \leq (2m)^m$. Moreover, no prime $p > m$ ramifies in F. The lower bound follows from part (1). The upper bound follows from part (2) upon noticing that $2^{1+\frac{1}{2n}} d^2 \delta(F/\mathbb{Q}) < (2d)^2$, where for $m = 1$ we have used that $\delta(F/\mathbb{Q}) = 1$. This completes the proof of Theorem 2.

REFERENCES

1. S. Akhtari, J. D. Vaaler, and M. Widmer, *Small generators of number fields, II*, submitted (2023).
2. H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, 2000.
3. A. Dubickas, *Minimal Mahler measures for generators of some fields*, Rev. Math. Iberoam. **39, no. 1** (2023), 269–282.
4. S. Graham, *An asymptotic estimate related to Selberg's sieve*, J. Number Theory **10** (1978), 83–94.
5. _____, *On Linnik's constant*, Acta Arith. **XXXIX (4)** (1981), 163–179.
6. R. Heath-Brown, *Zero-free regions for dirichlet l-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. **64** (1991), no. 3.
7. H. Iwaniec and E. Kowalski, *Analytic number theory*, vol. 53, American Mathematical Soc., 2004.
8. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1990.
9. L. B. Pierce, C. Turnage-Butterbaugh, and M. Matchett Wood, *An effective Chebotarev density theorem for families of number fields, with an application to l-torsion in class groups*, Invent. Math. **219, no.2** (2020), 701–778.
10. P. Pollack, *The smallest prime that splits completely in an abelian number field*, Proc. Amer. Math. Soc. **142** (2014), 1925–1934.
11. W. Ruppert, *Small generators of number fields*, Manuscripta math. **96** (1998), 17–22.
12. J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
13. J. D. Vaaler and M. Widmer, *On small generators of number fields*, Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms, Contemporary Mathematics, vol. 587, Amer. Math. Soc., Providence, RI, 2013 (2013).
14. _____, *Number fields without small generators*, Math. Proc. Cam. Philos. Soc. **159, no.3** (2015), 379–385.
15. S. H. Weintraub, *Observations on primitive, normal, and subnormal elements of field extensions*, Monatsh. Math. **162** (2011), :239–244.
16. M. Widmer, *Counting primitive points of bounded height*, Trans. Amer. Math. Soc. **362** (2010), 4793–4829.
17. T. Xylouris, *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression, Dissertation for the degree of Doctor of Mathematics and Natural Sciences at the University of Bonn*, Bonner Math. Schriften, 404 (2011).
18. M. Milinovich Z. Ge and P. Pollack, *A note on the least prime that splits completely in a nonabelian Galois number field*, Math. Z. **292** (2019), 183–192.

DEPARTMENT OF MATHEMATICS, ROYAL HOLLOWAY, UNIVERSITY OF LONDON, TW20 0EX EGHAM, UK

E-mail address: martin.widmer@rhul.ac.uk