Rev. Mat. Iberoam. 39 (2023), no. 1, 269–282
DOI 10.4171/RMI/1331

Minimal Mahler measures for generators of some fields

Artūras Dubickas

Abstract. We prove that for each odd integer $d \geq 3$ there are infinitely many number fields K of degree d such that each generator α of K has Mahler measure greater than or equal to $d^{-d}|\Delta_K|^{\frac{d+1}{d(2d-2)}}$, where Δ_K is the discriminant of the field K. This, combined with an earlier result of Vaaler and Widmer for composite d, answers negatively a question of Ruppert raised in 1998 about 'small' algebraic generators for every $d \geq 3$. We also show that for each $d \geq 2$ and any $\varepsilon > 0$, there exist infinitely many number fields K of degree d such that every algebraic integer generator α of K has Mahler measure greater than $(1-\varepsilon)|\Delta_K|^{1/d}$. On the other hand, every such field K contains an algebraic integer generator α with Mahler measure smaller that $|\Delta_K|^{1/d}$. This generalizes the corresponding bounds recently established by Eldredge and Petersen for $d = 3$.

1. Introduction

Throughout the paper, let K be a number field of degree $d \geq 2$, and let $\mathcal{O}_K$ be its ring of integers. Set

$$M(K) := \inf\{M(\alpha) : \alpha \in K,\ \mathbb{Q}(\alpha) = K\}$$

and

$$M(\mathcal{O}_K) := \inf\{M(\alpha) : \alpha \in \mathcal{O}_K,\ \mathbb{Q}(\alpha) = K\},$$

where $M(\alpha) = M(f)$ is the *Mahler measure* of the minimal polynomial $f \in \mathbb{Z}[x]$ of α. (Recall that for any $f(x) = a\prod_{i=1}^{d}(x-\alpha_i) \in \mathbb{C}[x]$, its Mahler measure is defined by $M(f) := |a|\prod_{i=1}^{d}\max\{1,|\alpha_i|\}$.) Note that the infima in the definitions of $M(K)$ and $M(\mathcal{O}_K)$ are attained. Indeed, by the inequalities

$$2^{-d}H(\alpha) \leq M(\alpha) \leq H(\alpha)\sqrt{d+1} \tag{1.1}$$

(see, e.g., [18]), where $H(\alpha)$ stands for the *naive height* (the maximal modulus of the coefficients of the minimal polynomial $f \in \mathbb{Z}[x]$ of α), there are only finitely many irreducible integer polynomials of degree d whose Mahler measures are bounded above by a constant.

2020 Mathematics Subject Classification: Primary 11R04; Secondary 11R18, 11C08.
Keywords: Mahler measure, discriminant, number field, monogenic field, generator.

Recall that for an algebraic integer α, with minimal monic polynomial $f \in \mathbb{Z}[x]$, and $K = \mathbb{Q}(\alpha)$, we have

$$\Delta(f) = g^2 \Delta_K. \tag{1.2}$$

Here, $\Delta(f)$ is the discriminant of the polynomial f, Δ_K is the discriminant of the field K, and $g = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is a positive integer which is the index of the $\mathbb{Z}$-module $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$ (see, e.g., Proposition 4.4.4 in [4] or Proposition 2.13 in [19]).

In [16], Mahler showed that

$$|\Delta(f)| \le d^d M(f)^{2d-2}$$

for any $f \in \mathbb{C}[x]$ of degree d. This inequality applied to the minimal polynomial f of $\alpha \in \mathcal{O}_K$ satisfying $K = \mathbb{Q}(\alpha)$ in tandem with (1.2) implies that

$$d^{-d/(2d-2)} |\Delta_K|^{1/(2d-2)} \le M(\mathcal{O}_K). \tag{1.3}$$

By a more general result of Silverman (Theorem 2 in [25]), we have

$$d^{-d/(2d-2)} |\Delta_K|^{1/(2d-2)} \le M(K). \tag{1.4}$$

Clearly, (1.4) implies (1.3) in view of $\mathcal{O}_K \subset K$. Since $M(\alpha) \ge 1$ for any algebraic number α, the bounds (1.3) and (1.4) are nontrivial for number fields K satisfying

$$|\Delta_K| > d^d.$$

In [23], Ruppert gave one more proof of the inequality

$$|\Delta_K|^{1/(2d-2)} \ll M(K),$$

which is a version of (1.4) with a different constant implied in $\ll$. (Here and below, the constants in $\ll$ depend on d only.) He also observed that for each $d \ge 2$, the exponent $1/(2d-2)$ in the power of $|\Delta_K|$ in (1.4) is best possible, namely,

$$M(K) \ll |\Delta_K|^{1/(2d-2)}$$

for *infinitely many* fields K of degree d. It is easy to see that this holds for $K = \mathbb{Q}(\alpha)$, where p and q are primes satisfying $p < q < 2p$ and $\alpha = (-q/p)^{1/d}$. (See also Proposition 1 in [22] due to Masser.)

In [23], Ruppert asked if for every $d \ge 2$ there is a constant $\kappa(d)$ such that for *every* number field K of degree $d \ge 2$,

$$M(K) \le \kappa(d) |\Delta_K|^{1/(2d-2)}. \tag{1.5}$$

(To be precise, he asked this in terms of the naive height, but the question is the same by (1.1).) The case $d = 2$ has been settled by Ruppert himself. He showed that the inequality $M(K) \ll |\Delta_K|^{1/2}$ holds for every imaginary quadratic field K, and that

$$M(K) \le M(\mathcal{O}_K) \ll |\Delta_K|^{1/2}$$

for every real quadratic field K. Later, in [3] it was shown that the inequalities

$$\frac{1}{2}|\Delta_K|^{1/2} \leq M(K) \leq |\Delta_K|^{1/2}$$

hold for all real quadratic fields K.

In [23], Ruppert also established the inequality

$$M(\mathcal{O}_K) \ll |\Delta_K|^{1/2}$$

for all totally real number fields K of prime degree d. Then, in [26], Vaaler and Widmer proved the inequality

$$M(K) \ll |\Delta_K|^{1/2}$$

for all not totally complex number fields K of degree d, and also for all number fields K of degree d under assumption of the generalized Riemann hypothesis. In [27], they also showed that for each composite d there is a constant $\gamma(d)$, which is given explicitly and is strictly greater than $1/(2d-2)$, such that for each positive number ε there exist infinitely many number fields K of degree d such that

$$M(K) > |\Delta_K|^{\gamma(d)-\varepsilon}. \tag{1.6}$$

This answers Ruppert's question related to $\kappa(d)$ in (1.5) negatively for each composite d. For $d = 5$, the answer is also negative by a combination of the results of Vaaler and Widmer [27] and Bhargava [2]. (See the end of Section 1 in [27].)

The next theorem implies that the answer to Ruppert's question is negative for each prime number $d \geq 3$ too.

Theorem 1. *Let $d \geq 3$ be an odd integer. Then, for infinitely many number fields K of degree d we have*

$$M(K) \geq d^{-d}|\Delta_K|^{\frac{d+1}{d(2d-2)}}. \tag{1.7}$$

In particular, Theorem 1 answers Ruppert's question negatively for $d = 3$ (as the authors say in [27] their method sheds no light on the cubic case), gives a much simpler proof for $d = 5$ (without involving deep methods of [2]), and, combined with the results of [27], answers Ruppert's question negatively for each $d \geq 3$.

We remark that for d odd, but not a prime number, the exponent $\gamma(d)$ obtained in [27] is greater than the exponent $(d+1)/(d(2d-2))$ in (1.7), so inequality (1.6) is stronger than (1.7) for those d. The constant d^{-d} can be improved by a slightly more technical argument, but this constant is not very important in the estimate (1.7) (the important one is the exponent of $|\Delta_K|$), so we have chosen it for the sake of simplicity.

The related quantity $M(\mathcal{O}_K)$ for cubic fields has been recently investigated, see [8], by Eldredge and Petersen. In particular, they showed that there are infinitely many cubic number fields K such that

$$\frac{1}{30}|\Delta_K|^{1/3} < M(\mathcal{O}_K) < \frac{4}{3}|\Delta_K|^{1/3}. \tag{1.8}$$

This implies that the exponent $1/(2d-2)$ of $|\Delta_K|$ in (1.3) is not sharp for some cubic fields (as $1/(2d-2) = 1/4 < 1/3$ for $d = 3$). The proof of the lower bound in (1.8) is based on application of the so-called Minkowski embedding, which to each $\alpha \in K$, where K is a field with signature (s, t), assigns the vector

$$\big(\sigma_1(\alpha), \dots, \sigma_s(\alpha), \Re(\sigma_{s+1}(\alpha)), \Im(\sigma_{s+1}(\alpha)), \dots, \Re(\sigma_{s+t}(\alpha)), \Im(\sigma_{s+t}(\alpha))\big)$$

in $\mathbb{R}^{s+2t} = \mathbb{R}^d$. Here, $\sigma_1, \dots, \sigma_s$ are the s real embeddings of K, and $\sigma_{s+j}, \overline{\sigma_{s+j}}$, for $j = 1, \dots, t$, are the t pairs of complex conjugate embeddings. The Euclidean norm of such vector has been recently investigated in [6] and [7]. In [8], the authors perform the Gram–Schmidt algorithm to determine an orthogonal basis consisting of certain vectors of a cubic field K and then derive the lower bound in (1.8) (see Section 3.1 in [8]).

In this paper, by a different method, we generalize the inequalities (1.8) to arbitrary integer $d \geq 2$.

Theorem 2. *For each $\varepsilon > 0$ and each integer $d \geq 2$, there are infinitely many number fields K of degree d such that*

$$(1 - \varepsilon)|\Delta_K|^{1/d} < M(\mathcal{O}_K) < |\Delta_K|^{1/d}.$$

This implies that for any $d \geq 3$, the exponent $1/(2d-2)$ of $|\Delta_K|$ in (1.3) is not sharp for infinitely many fields of degree d. Note that in the cubic case the constants $1 - \varepsilon$ and 1 in Theorem 2 are better than those in (1.8) (respectively, $1/30$ and $4/3$). In terms of [27], Section 5, our Theorem 2 implies that $1/d$ is a cluster point of the set

$$\Big\{\frac{\log M(\mathcal{O}_K)}{\log|\Delta_K|} \; : \; [K:\mathbb{Q}] = d\Big\},$$

which means that for any $\varepsilon > 0$ there are infinitely many number fields K of degree d such that

$$\Big|\frac{1}{d} - \frac{\log M(\mathcal{O}_K)}{\log|\Delta_K|}\Big| < \varepsilon.$$

In fact, the fields K which we consider in Theorems 1 and 2 are the same. So, combining both theorems for $d = 3$, we obtain

$$\frac{1}{27}|\Delta_K|^{1/3} \leq M(K) \leq M(\mathcal{O}_K) < |\Delta_K|^{1/3}.$$

Accordingly, $1/3$ is a cluster point of the set

$$\Big\{\frac{\log M(K)}{\log|\Delta_K|} \; : \; [K:\mathbb{Q}] = 3\Big\}.$$

In the next section we give some results on monogenic fields of the form $\mathbb{Q}(a^{1/d})$, where $d \geq 2$ is an integer and a runs over the prime numbers. In Section 3 we prove several auxiliary results, and then complete the proofs of Theorems 1 and 2 in Sections 4 and 5, respectively.

A crucial observation in the proof of Theorem 1 is that, for any algebraic generator α of the field $K = \mathbb{Q}(a^{1/d})$ of degree d, either α itself or its reciprocal α^{-1} can be written as a $\mathbb{Q}$-linear form in $1, a^{1/d}, \dots, a^{m/d}$ with $m \geq [d/2]$ and a nonzero coefficient for $a^{m/d}$.

Accordingly, the Mahler measure of $M(\alpha)$ (or $M(\alpha^{-1})$ which equals $M(\alpha)$) turns out to be 'large' and gives the exponent of $|\Delta_K|$ in (1.7) at least

$$\frac{m}{d(d-1)} \geq \frac{[d/2]}{d(d-1)},$$

which is $(d+1)/(d(2d-2))$ for d odd and $1/(2d-2)$ for d even. Thus, our approach gives no improvement of (1.4) for d even.

2. Monogenic fields of the form $\mathbb{Q}(a^{1/d})$

Recall that the field K is called *monogenic* if it contains an algebraic integer α such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. In particular, if for $\alpha = a^{1/d}$, where $a \in \mathbb{N}$, with minimal polynomial

$$f(x) = x^d - a,$$

the field $K = \mathbb{Q}(\alpha) = \mathbb{Q}(a^{1/d})$ is monogenic and $\mathcal{O}_K = \mathbb{Z}[\alpha]$ then, by $|\Delta(f)| = d^d a^{d-1}$ (see, e.g., Example 1.3.7 in [21]) and (1.2) with $g = 1$, we must have

$$|\Delta_K| = d^d a^{d-1}. \tag{2.1}$$

We first prove the next lemma.

Lemma 3. *For each $d \geq 2$, there are infinitely many prime numbers a for which the field $K = \mathbb{Q}(a^{1/d})$ is monogenic, $|\Delta_K| = d^d a^{d-1}$, and $\mathcal{O}_K = \mathbb{Z}[a^{1/d}]$.*

Proof. In Theorem 1.1 of [10], Gassert showed that the field $K = \mathbb{Q}(a^{1/d})$ is monogenic for $d \geq 2$ and squarefree integer a if p^2 does not divide $a^p - a$ for all primes p dividing d. (As observed in [5], it should be an additional assumption that $x^d - a$ is irreducible over $\mathbb{Q}$.) The same statement asserting that $1, a^{1/d}, \dots, a^{(d-1)/d}$ is an integral basis of K was also recently proved independently in Corollary 1.3 of [13]. (See also [12, 14, 15] for some related work.)

In Proposition 2.5 of [10], Gassert also observed that the condition

$$p^2 \mid (a^p - a)$$

is satisfied only if a belongs to one of p distinct equivalence classes modulo p^2, namely,

$$0, 1, 2^p, 3^p, \dots, (p-1)^p.$$

In particular, for each prime p dividing d and each squarefree integer $a > 1$ of the form

$$a = p^2 u + u_p, \tag{2.2}$$

where $u \in \mathbb{N}$ and $u_p \in \{0, 1, \dots, p^2 - 1\}$ satisfies $u_p \not\equiv i^p \pmod{p^2}$ for each $i = 0, 1, \dots, p-1$ and, in addition, $u_p \neq p, 2p, \dots, (p-1)p$, we have

$$p^2 \nmid (a^p - a).$$

Note that there are p^2 equivalence classes for possible u_p, and we remove $p + p - 1 = 2p - 1$ of them, which is less than p^2. Consequently, we can select any of

$$p^2 - (2p - 1) = (p - 1)^2$$

remaining possibilities in the set $\{0, 1, \dots, p^2 - 1\}$ as u_p.

Put

$$Q := \prod_{p|d} p.$$

Then, by the Chinese remainder theorem, there exists $v \in \mathbb{N}$ such that for each $a = Q^2 s + v$, $s = 1, 2, \dots$, satisfying (2.2) for every prime $p \mid d$, we have $p^2 \nmid (a^p - a)$. Furthermore, by the choice of u_p, we have $\gcd(p, u_p) = 1$, and hence

$$\gcd(Q^2, v) = 1.$$

So, by Dirichlet's theorem on arithmetic progressions, there are infinitely many prime numbers a of the form

$$a = Q^2 s + v, \tag{2.3}$$

with $s \in \mathbb{N}$.

This completes the proof of the lemma for each of those (infinitely many) prime numbers a by Theorem 1.1 in [10] or Corollary 1.3 in [13], the irreducibility of $x^d - a$ (see, e.g., [24], p. 92) and (2.1). ∎

In [1], Bardestani showed that for each prime number d there are 'many' prime numbers a (with lower density at least $1 - 1/d$ among all primes) for which the field $K = \mathbb{Q}(a^{1/d})$ is monogenic. In this context, Lemma 3 implies the following generalization of the main result of [1].

Corollary 4. *For each $d \geq 2$, we have*

$$\liminf_{x\to\infty} \frac{\#\{p \leq x : \mathbb{Q}(p^{1/d}) \text{ is monogenic}\}}{\pi(x)} \geq \frac{\varphi(\mathrm{rad}(d))}{\mathrm{rad}(d)},$$

where p denotes the prime numbers, $\pi(x)$ is the prime counting function, φ is the Euler totient function, and $\mathrm{rad}(d)$ *stands for the radical of d (i.e., the product of its distinct prime divisors).*

Proof. Set $Q = \mathrm{rad}(d)$ and write each prime number a greater than Q^2 in the form

$$a = Q^2 s + w,$$

where $s = 1, 2, \dots$ and $w \in \{0, 1, \dots, Q^2 - 1\}$. Clearly, there are $\varphi(Q^2)$ choices for w. By the construction of v as in (2.3) and Lemma 3, there are at least $\prod_{p|d}(p-1)^2$ choices for w when for the corresponding prime number a the field $\mathbb{Q}(a^{1/d})$ is monogenic. Since

$$\frac{\prod_{p|d}(p-1)^2}{\varphi(Q^2)} = \frac{\prod_{p|d}(p-1)^2}{Q\prod_{p|d}(p-1)} = \frac{\prod_{p|d}(p-1)}{Q} = \frac{\varphi(Q)}{Q} = \frac{\varphi(\mathrm{rad}(d))}{\mathrm{rad}(d)},$$

we get the inequality for the lower density as claimed. ∎

3. Auxiliary results

The following lemma will be used in proving an upper bound for $M(\mathcal{O}_K)$ in Theorem 2.

Lemma 5. *For each $d \geq 2$ and each sufficiently large $a \in \mathbb{N}$, which is not a pth power of an integer for some prime number p dividing d, the number*

$$\alpha := a^{1/d} - \lfloor a^{1/d} \rfloor \tag{3.1}$$

is an algebraic integer of degree d and has Mahler measure less than $da^{(d-1)/d}$.

Proof. Set $t := \lfloor a^{1/d} \rfloor$. The minimal polynomial of $a^{1/d} = \alpha + t$ over $\mathbb{Q}$ is

$$f(x) = x^d - a.$$

Indeed, $f(a^{1/d}) = 0$ and f is irreducible by Capelli's theorem (see, e.g., [24], p. 92). Thus, $\alpha = a^{1/d} - t$ is an algebraic integer of degree d over $\mathbb{Q}$, and the d conjugates of α over $\mathbb{Q}$ are

$$\alpha_j = a^{1/d} e^{2\pi i (j-1)/d} - t,$$

where $j = 1, \dots, d$.

Note that $\alpha = \alpha_1 \in (0, 1)$, and $|\alpha_2|, \dots, |\alpha_d| > 1$ for each sufficiently large a. Hence, in view of $0 < t < a^{1/d}$, we obtain

$$\begin{aligned} M(\alpha) &= \prod_{j=2}^{d} |\alpha_j| = \prod_{j=1}^{d-1} \left| a^{1/d} e^{2\pi i j/d} - t \right| = \frac{|a - t^d|}{|a^{1/d} - t|} \\ &= a^{(d-1)/d} + a^{(d-2)/d} t + \dots + t^{d-1} < d a^{(d-1)/d}, \end{aligned}$$

which completes the proof of the lemma. ∎

We also record the following simple inequality.

Lemma 6. *For any real numbers $y_1, \dots, y_k \geq 1$ we have*

$$y_1 + \dots + y_k \leq k - 1 + y_1 \cdots y_k.$$

Proof. Set $z_j := y_j - 1$ for $j = 1, \dots, k$. Then, $z_j \geq 0$ for each j. From the inequality

$$(1 + z_1) \cdots (1 + z_k) \geq 1 + z_1 + \dots + z_k$$

we derive that $y_1 \cdots y_k = (1 + z_1) \cdots (1 + z_k)$ is greater than or equal to $1 + z_1 + \dots + z_k = y_1 + \dots + y_k - k + 1$, which is the inequality of the lemma. ∎

The next lemma will be used in the proof of Theorem 1 and in the proof of the lower bound for $M(\mathcal{O}_K)$ in Theorem 2.

Lemma 7. *Let $d \geq 3$, $m \in \{1, 2, \dots, d-1\}$, $\zeta = e^{2\pi i/d}$ and $F = \mathbb{Q}(\zeta)$. Then, for any integers $k_1, \dots, k_{m+1}$ satisfying $1 \leq k_1 < \dots < k_{m+1} \leq d$, the linear system*

$$X_1 \zeta^{(k_1 - 1) j} + \dots + X_{m+1} \zeta^{(k_{m+1} - 1) j} = \delta_j, \quad j = 0, \dots, m, \tag{3.2}$$

where $\delta_0 = \cdots = \delta_{m-1} = 0$ *and* $\delta_m = 1$, *has a unique nonzero solution* $X_1, \dots, X_{m+1} \in F$. *Moreover, we have* $d^m X_j \in \mathcal{O}_F$ *and*

$$|X_j| \le \frac{1}{\big(2\sin(\frac{\pi}{d})\big)^m}$$

for $j = 1, \dots, m+1$.

Proof. Fix any $k_1 < \cdots < k_{m+1}$ satisfying the assumptions of the lemma. The $(m+1) \times (m+1)$ determinant $\|\zeta^{(k_l-1)j}\|$, where $l = 1, \dots, m+1$ and $j = 0, \dots, m$, is the Vandermonde determinant, so it is nonzero. Consequently, by Cramer's rule, the linear system (3.2) has a unique solution $X_1, \dots, X_{m+1}$, where $X_j \in F$ for each $j = 1, \dots, m+1$. Evidently, in view of $\delta_m = 1$, at least one X_j is nonzero.

In fact, setting

$$g(x) := (x - \zeta^{k_1-1})(x - \zeta^{k_2-1}) \cdots (x - \zeta^{k_{m+1}-1}),$$

we can express X_j explicitly by the formula

$$X_j = \frac{1}{g'(\zeta^{k_j-1})} = \frac{1}{\prod_{s \ne j}(\zeta^{k_j-1} - \zeta^{k_s-1})}$$

(see, for instance, Problem 67 in Chapter 6 of [20]). Hence, as $\zeta^d = 1$, each X_j can be written as ζ^c, with $c \in \{0, \dots, d-1\}$, multiplied by a product of m factors of the form $(\zeta^b - 1)^{-1}$, with not necessarily distinct $b \in \{1, \dots, d-1\}$. Note that $\zeta^b - 1$ is a root of

$$\frac{(x+1)^d - 1}{x} = x^{d-1} + \binom{d}{1} x^{d-2} + \binom{d}{2} x^{d-3} + \cdots + \binom{d}{2} x + d.$$

Consequently, $d(\zeta^b - 1)^{-1} \in \mathcal{O}_F$, which implies $d^m X_j \in \mathcal{O}_F$ for each $j = 1, \dots, m+1$. Also, $|\zeta^b - 1| = 2\sin(\frac{\pi b}{d}) \ge 2\sin(\frac{\pi}{d})$, which yields the upper bound on $|X_j|$ as claimed. ∎

Finally, by Theorem 10.2 in [9], the following is true.

Lemma 8. *If* α *is an algebraic number of degree* d *with conjugates* $\alpha_1, \dots, \alpha_d$, *and* $T \in \mathbb{N}$ *is the leading coefficient of its minimal polynomial in* $\mathbb{Z}[x]$, *then* $T \prod_{j \in I} \alpha_j$ *is an algebraic integer for each* $I \subseteq \{1, \dots, d\}$.

4. Proof of Theorem 1

Let $d \ge 3$ be an odd integer. Consider the field $K = \mathbb{Q}(a^{1/d})$, where a is one of the prime numbers satisfying the conditions of Lemma 3. (Corollary 4 implies that there are 'many' such prime numbers a in terms of density.) In view of (2.1), we have

$$|\Delta_K|^{\frac{d+1}{d(2d-2)}} = d^{\frac{d+1}{2d-2}} a^{\frac{d+1}{2d}},$$

so for the proof of (1.7) it suffices to show that

$$M(\alpha) \ge d^{-d + \frac{d+1}{2d-2}} a^{\frac{d+1}{2d}} \tag{4.1}$$

for any $\alpha \in K$ of degree d.

Write

$$\alpha = b_0 + b_1 a^{1/d} + \cdots + b_m a^{m/d}, \tag{4.2}$$

where $m \in \{1, \ldots, d-1\}$, $b_0, \ldots, b_m \in \mathbb{Q}$ and $b_m \neq 0$. Without loss of generality we may assume that

$$m \geq \frac{d+1}{2}. \tag{4.3}$$

Indeed, in the case $m < (d+1)/2$ we have $m \leq (d-1)/2$. So, using $M(\alpha) = M(\alpha^{-1})$, we can simply replace α by its reciprocal

$$\alpha^{-1} = c_0 + c_1 a^{1/d} + \cdots + c_s a^{s/d},$$

where $s \in \{1, \ldots, d-1\}$, $c_0, \ldots, c_s \in \mathbb{Q}$, $c_s \neq 0$ and $s \geq (d+1)/2$. To see this, just observe that, by the linear independence of $1, a^{1/d}, \ldots, a^{(d-1)/d}$ over $\mathbb{Q}$, from

$$0 = \alpha\alpha^{-1} - 1 = b_0 c_0 - 1 + (b_0 c_1 + b_1 c_0) a^{1/d} + \cdots + b_m c_s a^{(m+s)/d}$$

and $b_m c_s \neq 0$, it follows that $m + s \geq d$. Hence,

$$s \geq d - m \geq d - \frac{d-1}{2} = \frac{d+1}{2}.$$

Assume that the leading coefficient of the minimal polynomial of α (in $\mathbb{Z}[x]$) defined in (4.2) with m satisfying (4.3) is $T \in \mathbb{N}$. The d distinct conjugates of α are of the form

$$\alpha_j = \sum_{k=0}^{m} b_k a^{k/d} \zeta^{(j-1)k}, \quad j = 1, \ldots, d, \tag{4.4}$$

where $\zeta = e^{2\pi i/d}$. Select $X_1, \ldots, X_{m+1} \in F$ as in Lemma 7 applied to

$$(k_1, k_2, \ldots, k_{m+1}) = (1, 2, \ldots, m+1).$$

Then, by (3.2) and (4.4), it follows that

$$X_1\alpha_1 + \cdots + X_{m+1}\alpha_{m+1} = b_m a^{m/d}.$$

By Lemma 7, we have $d^m X_j \in \mathcal{O}_F$ for $j = 1, \ldots, m+1$. Also, $T\alpha_j$ is an algebraic integer for every j by Lemma 8. Thus, each product $d^m T X_j \alpha_j$ is an algebraic integer, and so must be their sum

$$d^m T(X_1\alpha_1 + \cdots + X_{m+1}\alpha_{m+1}) = d^m T b_m a^{m/d}. \tag{4.5}$$

We claim that $d^m T b_m$ is a nonzero integer. Indeed, we know that this is a nonzero rational number, say $d^m T b_m = D_0/D$, where $D_0 \in \mathbb{Z}$, $D \in \mathbb{N}$ and $\gcd(D_0, D) = 1$. Assume that $D > 1$. Then, as $D_0 a^{m/d}/D$ and $a^{(d-m)/d}$ both are algebraic integers, so is their product $D_0 a/D$. But a is a prime, so $D = a$ is the only possibility. However, then $D_0 a^{m/d}/D = D_0 a^{(m-d)/d}$ is not an algebraic integer, since $m - d < 0$ and a is a prime number which does not divide D_0, a contradiction.

Consequently, using the upper bound on $|X_j|$ from Lemma 7 and (4.5), we get

$$a^{m/d} \le d^m T|b_m|a^{m/d} \le \frac{(m+1)\,d^m\,T\,\max_{1\le j\le m+1}|\alpha_j|}{\big(2\sin(\frac{\pi}{d})\big)^m},$$

which implies

$$M(\alpha) = T\prod_{j=1}^{d}\max(1,|\alpha_j|) \ge T \max_{1\le j\le m+1}|\alpha_j| \ge \frac{\big(2\sin(\frac{\pi}{d})\big)^m a^{m/d}}{(m+1)\,d^m}. \tag{4.6}$$

Recall that $m \ge (d+1)/2$ by (4.3) and $m \le d-1$. Clearly, if $m > (d+1)/2$, then (4.6) immediately implies (4.1) for each sufficiently large a. Assume that $m = (d+1)/2$. Then, (4.6) becomes

$$M(\alpha) \ge \frac{\big(2\sin(\frac{\pi}{d})\big)^{\frac{d+1}{2}} a^{\frac{d+1}{2d}}}{\frac{d+3}{2}\,d^{\frac{d+1}{2}}}.$$

Now, in order to complete the proof of (4.1) for $m = (d+1)/2$, it remains to verify that

$$\frac{\big(2\sin(\frac{\pi}{d})\big)^{\frac{d+1}{2}}}{\frac{d+3}{2}\,d^{\frac{d+1}{2}}} \ge d^{-d+\frac{d+1}{2d-2}} \tag{4.7}$$

for $d \ge 3$ odd. Indeed, for each $d \ge 7$ we have

$$\frac{\big(2\sin(\frac{\pi}{d})\big)^{\frac{d+1}{2}}}{\frac{d+3}{2}\,d^{\frac{d+1}{2}}} \ge \frac{\big(2\sin(\frac{\pi}{d})\big)^{\frac{d+1}{2}}}{d^{\frac{d+3}{2}}} > \frac{\big(\frac{4}{d}\big)^{\frac{d+1}{2}}}{d^{\frac{d+3}{2}}} = \frac{2^{d+1}}{d^{d+2}} > d^{-d+\frac{d+1}{2d-2}}.$$

For $d = 3$ and $d = 5$, the inequality (4.7) is verified directly. (In fact, for $d = 3$ we have equality in (4.7).)

5. Proof of Theorem 2

Consider the field $K = \mathbb{Q}(a^{1/d})$, where $d \ge 2$ and a is one of sufficiently large prime numbers satisfying the conditions of Lemma 3. Then, by Lemma 5, the Mahler measure of $\alpha \in \mathcal{O}_K$ of degree d defined as in (3.1) is less than $da^{(d-1)/d}$. Since $da^{(d-1)/d} = |\Delta_K|^{1/d}$, this yields $M(\alpha) < |\Delta_K|^{1/d}$, and hence

$$M(\mathcal{O}_K) < |\Delta_K|^{1/d}$$

for each of those fields K.

To prove the desired lower bound on $M(\mathcal{O}_K)$ in Theorem 2, we assume that the number $\alpha \in \mathcal{O}_K$ is of degree d. Then, due to the fact that the field $K = \mathbb{Q}(a^{1/d})$ is monogenic and $\mathcal{O}_K = \mathbb{Z}[a^{1/d}]$, we can write

$$\alpha = a_0 + a_1 a^{1/d} + \cdots + a_m a^{m/d}, \tag{5.1}$$

where $m \in \{1, \dots, d-1\}$, $a_0, a_1, \dots, a_m \in \mathbb{Z}$ and $a_m \neq 0$. Accordingly, the d distinct conjugates of α over $\mathbb{Q}$ can be written as

$$\alpha_j = \sum_{k=0}^{m} a_k a^{k/d} \zeta^{(j-1)k}, \quad j = 1, \dots, d, \tag{5.2}$$

with $\zeta = e^{2\pi i/d}$.

Fix any ε in the interval $(0, 1)$ and recall that a is one of the sufficiently large prime numbers satisfying the conditions of Lemma 3. In all what follows we will consider three cases, $m = d-1$, $m \in \{2, \dots, d-2\}$, $m = 1$, and show that in each of these cases the inequality

$$M(\alpha) > (1-\varepsilon)\, d a^{(d-1)/d} = (1-\varepsilon)\, |\Delta_K|^{1/d} \tag{5.3}$$

holds for all α as defined in (5.1).

We first examine the case $m = d-1$. From (5.2) it follows that

$$\alpha_1 + \zeta\alpha_2 + \dots + \zeta^{d-1}\alpha_d = \sum_{j=1}^{d} \zeta^{j-1} \sum_{k=0}^{d-1} a_k a^{k/d} \zeta^{(j-1)k} = \sum_{k=0}^{d-1} a_k a^{k/d} \sum_{j=1}^{d} \zeta^{(j-1)(k+1)}.$$

Note that the sum $\sum_{j=1}^{d} \zeta^{(j-1)(k+1)}$ equals d for $k = d-1$, while for $k \in \{0, 1, \dots, d-2\}$ it vanishes:

$$\sum_{j=1}^{d} \zeta^{(j-1)(k+1)} = \frac{1-\zeta^{d(k+1)}}{1-\zeta^{k+1}} = 0.$$

Consequently,

$$\alpha_1 + \zeta\alpha_2 + \dots + \zeta^{d-1}\alpha_d = d a_{d-1} a^{(d-1)/d},$$

and hence

$$d a^{(d-1)/d} \le d |a_{d-1}| a^{(d-1)/d} = \Big| \sum_{j=1}^{d} \alpha_j \zeta^{j-1} \Big| \le \sum_{j=1}^{d} |\alpha_j|.$$

Suppose there are k indices $j \in \{1, \dots, d\}$ for which $|\alpha_j| \ge 1$. Then, $k \ge 1$ and the product of those $|\alpha_j|$ is $M(\alpha)$. Estimating the sum of those $|\alpha_j|$ by $k - 1 + M(\alpha)$ (see Lemma 6) and each of the $d-k$ remaining $|\alpha_j|$ by 1, we derive that

$$d a^{(d-1)/d} \le \sum_{j=1}^{d} |\alpha_j| \le k - 1 + M(\alpha) + d - k = d - 1 + M(\alpha).$$

This yields

$$M(\alpha) \ge d a^{(d-1)/d} - d + 1,$$

which implies (5.3) for each sufficiently large a.

We now turn to the case when $2 \le m \le d-2$ (which occurs only for $d \ge 4$). We claim that then there is a constant $C(d)$ that depends on d only such that at most m of the conjugates of α lie in the disc

$$|z| < C(d) a^{m/d}. \tag{5.4}$$

Indeed, suppose $\alpha_{k_1}, \dots, \alpha_{k_{m+1}}$, where $1 \le k_1 < \dots < k_{m+1} \le d$, all lie in $|z| < C(d)\, a^{m/d}$. Select $X_1, \dots, X_{m+1} \in F$ as in Lemma 7. Then, by (3.2) and (5.2), it follows that

$$X_1 \alpha_{k_1} + \dots + X_{m+1} \alpha_{k_{m+1}} = a_m\, a^{m/d}.$$

From $|a_m| \ge 1$ and Lemma 7 we derive that at least one of the numbers $|\alpha_{k_1}|, \dots, |\alpha_{k_{m+1}}|$ is greater than or equal to

$$\frac{a^{m/d}}{(m+1) \max_{1 \le j \le m+1} |X_j|} \ge \frac{\big(2 \sin(\frac{\pi}{d})\big)^m a^{m/d}}{(m+1)}.$$

This proves (5.4) with the constant

$$C(d) = \max_{2 \le m \le d-2} \frac{\big(2 \sin(\frac{\pi}{d})\big)^m}{(m+1)}.$$

Now, by (5.4), at least $d - m$ conjugates of α have absolute values at least $C(d)\, a^{m/d}$. Consequently,

$$M(\alpha) \ge C(d)^{d-m}\, a^{(d-m)m/d},$$

which implies (5.3) in view of $(d-m)m > d - 1$.

It remains to investigate the case $m = 1$. Fix $\delta \in (0, 1)$ satisfying

$$(1-\delta)^{d-1} = 1 - \varepsilon \tag{5.5}$$

and put

$$\tau := 2\delta \sin\Big(\frac{\pi}{d}\Big). \tag{5.6}$$

Without loss of generality we may assume that

$$|\alpha_j| < \tau a^{1/d} \tag{5.7}$$

for some $j \in \{1, \dots, d\}$. Indeed, otherwise $|\alpha_j| \ge \tau a^{1/d}$ for all j, which implies $M(\alpha) \ge \tau^d a$, which is better than (5.3) for each sufficiently large a.

Using (5.2) with $m = 1$, for any

$$k \in J := \{1, \dots, d\} \setminus \{j\}$$

we obtain

$$\alpha_j - \alpha_k = a_1\, a^{1/d} (\zeta^{j-1} - \zeta^{k-1}).$$

Combining this with (5.6), (5.7) and $|a_1| \ge 1$ we deduce that

$$2\delta \sin\Big(\frac{\pi}{d}\Big) a^{1/d} + |\alpha_k| > |\alpha_j - \alpha_k| \ge 2\Big|\sin\Big(\frac{\pi(j-k)}{d}\Big)\Big|\, a^{1/d}.$$

Since

$$\sin\Big(\frac{\pi}{d}\Big) \le \Big|\sin\Big(\frac{\pi(j-k)}{d}\Big)\Big|$$

for $k \in J$, this further implies

$$|\alpha_k| > 2(1-\delta)\left|\sin\left(\frac{\pi(j-k)}{d}\right)\right| a^{1/d}$$

for each of those k. Consequently,

$$M(\alpha) \geq \prod_{k\in J} |\alpha_j| > 2^{d-1}(1-\delta)^{d-1} a^{(d-1)/d} \prod_{k\in J}\left|\sin\left(\frac{\pi(j-k)}{d}\right)\right|.$$

Observe that

$$\prod_{k\in J}\left|\sin\left(\frac{\pi(j-k)}{d}\right)\right| = \prod_{k=1}^{d-1}\sin\left(\frac{\pi k}{d}\right) = \frac{d}{2^{d-1}},$$

where the last identity can be found, e.g., in 1.392 of [11], p. 41. (See also [17] for its several proofs.) Therefore,

$$M(\alpha) > (1-\delta)^{d-1} d a^{(d-1)/d},$$

which yields (5.3) by (5.5).

Acknowledgements. I thank the referees for pointing out some inacurracies.

References

[1] Bardestani, M.: A density of a family of monogenic number fields. Preprint 2014, arXiv: 1202.2047v2.

[2] Bhargava, M.: The density of discriminants of quintic rings and fields. *Ann. of Math. (2)* **172** (2010), no. 3, 1559–1591.

[3] Cochrane, T., Dissnayake, R. M. S., Donohoue, N., Ishak, M. I. M., Pigno, V., Pinner, C. and Spencer, C.: Minimal Mahler measure in real quadratic fields. *Exp. Math.* **25** (2016), no. 2, 107–115.

[4] Cohen, H.: *Advanced topics in computational number theory*. Graduate Texts in Mathematics 193, Springer, New York, 2000.

[5] El Fadil, L.: A note on monogeneity of pure number fields. Preprint 2021, arXiv: 2106.00004.

[6] Dubickas, A.: Algebraic integers with small absolute size. *Quaest. Math.* **40** (2017), no. 5, 627–644.

[7] Dubickas, A., Sha, M. and Shparlinski, I. E.: On distances in lattices from algebraic number fields. *Moscow Math. J.* **17** (2017), no. 2, 239–268.

[8] Eldredge, L. and Petersen, K.: Minimal Mahler measure in cubic number fields. *Int. J. Number Theory* **18** (2022), no. 10, 2157–2169.

[9] Fel'dman, N. I.: *Approximation of algebraic numbers*. (Russian). Moskov. Gos. Univ., Moscow, 1981.

[10] Gassert, T. A.: A note on monogeneity of power maps. *Albanian J. Math.* **11** (2017), no. 1, 3–12.

[11] Gradshteyn, I. S. and Ryzhik, I. M.: *Table of integrals, series, and products*. Seventh edition. Academic Press, San Diego, 2007.

[12] Jakhar, A., Khanduja, S. K. and Sangwan, N.: On integral basis of pure number fields. *Mathematika* **67** (2021), no. 1, 187–195.

[13] Jakhar, A., Khanduja, S. K. and Sangwan, N.: On the discriminant of pure number fields. *Colloq. Math.* **167** (2022), no. 1, 149–157.

[14] Jakhar, A. and Sangwan, N.: Integral basis of pure prime degree number fields. *Indian J. Pure Appl. Math.* **50** (2019), no. 2, 309–314.

[15] Jones, L.: Monogenic polynomials with non-squarefree discriminant. *Proc. Amer. Math. Soc.* **148** (2020), no. 4, 1527–1533.

[16] Mahler, K.: An inequality for the discriminant of a polynomial. *Michigan Math. J.* **11** (1964), 257–262.

[17] Math.stackexchange.com, Question 8385.

[18] Mignotte, M. and Glesser, P.: On the smallest divisor of a polynomial. *J. Symbolic Comput.* **17** (1994), no. 3, 277–282.

[19] Narkiewicz, W.: *Elementary and analytic theory of algebraic numbers*. Third edition. Springer Monographs in Mathematics, Springer, Berlin, 2004.

[20] Pólya, G. and Szegő, G.: *Problems and theorems in analysis. II. Theory of functions, zeros, polynomials, determinants, number theory, geometry*. Classics in Mathematics, Springer, Berlin, 1998.

[21] Prasolov, V. V.: *Polynomials*. Algorithms and Computation in Mathematics 11, Springer, Berlin, 2010.

[22] Roy, D. and Thunder, J. L.: A note on Siegel's lemma over number fields. *Monatsh. Math.* **120** (1995), no. 3-4, 307–318.

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

[24] Schinzel, A.: *Polynomials with special regard to reducibility*. Encyclopedia of Mathematics and its Applications 77, Cambridge University Press, Cambridge, 2000.

[25] Silverman, J. H.: Lower bounds for height functions. *Duke Math. J.* **51** (1984), no. 2, 395–403.

[26] Vaaler, J. D. and Widmer, M.: A note on generators of number fields. In *Diophantine methods, lattices, and arithmetic theory of quadratic forms*, pp. 201–211. Contemp. Math. 587, American Mathematical Society, Providence, RI, 2013.

[27] Vaaler, J. D. and Widmer, M.: Number fields without small generators. *Math. Proc. Cambridge Philos. Soc.* **159** (2015), no. 3, 379–385.

Received May 13, 2021; revised October 18, 2021. Published online January 4, 2022.

Artūras Dubickas
Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University,
Naugarduko 24, 03225 Vilnius, Lithuania;
arturas.dubickas@mif.vu.lt