LOWER BOUNDS FOR HEIGHTS IN RELATIVE GALOIS EXTENSIONS

SHABNAM AKHTARI, KEVSER AKTAŞ, KIRSTI BIGGS, ALIA HAMIEH,
KATHLEEN PETERSEN, AND LOLA THOMPSON

ABSTRACT. The goal of this paper is to obtain lower bounds on the height of an algebraic number in a relative setting, extending previous work of Amoroso and Masser. Specifically, in our first theorem we obtain an effective bound for the height of an algebraic number α when the base field $\mathbb{K}$ is a number field and $\mathbb{K}(\alpha)/\mathbb{K}$ is Galois. Our second result establishes an explicit height bound for any non-zero element α which is not a root of unity in a Galois extension $\mathbb{F}/\mathbb{K}$, depending on the degree of $\mathbb{K}/\mathbb{Q}$ and the number of conjugates of α which are multiplicatively independent over $\mathbb{K}$. As a consequence, we obtain a height bound for such α that is independent of the multiplicative independence condition.

1. INTRODUCTION

Consider the non-constant polynomial

$$P(x) = c_d x^d + c_{d-1} x^{d-1} + \cdots + c_1 x + c_0 = c_d \prod_{i=1}^{d} (x - r_i).$$

The Mahler measure of $P(x)$ is defined as

$$M(P) = \exp\left(\int_0^1 \log |P(e^{2\pi i t})| \, dt \right),$$

the geometric mean of $|P(z)|$ for z on the unit circle. By Jensen's formula, this is equivalent to

$$M(P) = |c_d| \prod_{|r_i| \geq 1} |r_i|.$$

If $P(x)$ has integer coefficients, then $M(P) \geq 1$; by a result of Kronecker, $M(P) = 1$ exactly when $P(x)$ is a power of x times a product of cyclotomic polynomials.

Given an algebraic number α, we let $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ be its degree over $\mathbb{Q}$. We will use $M(\alpha)$ to denote the Mahler measure of the minimal polynomial of α over $\mathbb{Z}$. We will formulate our results in terms of the Weil height of α, defined to be

$$h(\alpha) = \tfrac{1}{d} \log M(\alpha).$$

In [16] Lehmer asked whether there are monic integer polynomials whose Mahler measure is arbitrarily close to 1. For the polynomial $L(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$ (now called Lehmer's polynomial), he calculated $M(L) = 1.176280818\ldots$, which is still the smallest value of $M(P) > 1$ known for $P \in \mathbb{Z}[x]$. Although he did not make a conjecture, the statement that there exists a constant $\delta > 0$ such that the Mahler measure of any polynomial in $\mathbb{Z}[x]$ is either 1 or is greater than $1 + \delta$ has become known as Lehmer's conjecture. In terms of height, Lehmer's conjecture states that there is a universal constant $c_0 > 0$ such that if α is a non-zero algebraic number of degree d which is not a root of unity then

$$h(\alpha) \geq \frac{c_0}{d}.$$

In 1971 Blanksby and Montgomery [8] and later Stewart [23] produced bounds for the Mahler measure of such algebraic numbers. These bounds inspired the work of Dobrowolski [12] who, in 1979, proved for $d \geq 2$ that

$$M(\alpha) > 1 + \frac{1}{1200}\Big(\frac{\log\log d}{\log d}\Big)^3.$$

Many of the best bounds are modifications of Dobrowolski's bound. The constants in these bounds have been improved over the years, but the dependence on the degree (for general polynomials) has remained. Of note, in 1996 Voutier [24] used elementary techniques to show that for $d \geq 2$, we have

$$(1) \qquad h(\alpha) > \frac{1}{4d}\Big(\frac{\log\log d}{\log d}\Big)^3.$$

(Dobrowolski's bound, when translated into a statement about Weil height, has a similar form.) Voutier also showed that for $d \geq 2$, we have

$$(2) \qquad h(\alpha) > \frac{2}{d\left(\log 3d\right)^3},$$

which gives a better lower bound than (1) for small values of d. For more details on the history of Lehmer's conjecture and related problems, see the excellent survey paper of Smyth [20].

Lehmer's conjecture has been proven in certain settings. Notably, Breusch [10] and Smyth [21] independently proved it for non-reciprocal polynomials. More recently, Borwein, Dobrowolski and Mossinghoff [9] proved it for many infinite families of polynomials, including polynomials with no cyclotomic factors and all odd coefficients. (Their result therefore proves Lehmer's conjecture for the Littlewood polynomials, namely those polynomials whose coefficients are ± 1.)

Results also exist concerning height bounds for α with certain properties. For example, Amoroso and David [1] have proven that there is an absolute constant c such that if $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, and α is not a root of unity, then $h(\alpha) \geq cd^{-1}$. This proves Lehmer's conjecture for such α. Moreover, if α is any non-zero algebraic number that lies in an abelian extension of $\mathbb{Q}$, then

Amoroso and Dvornicich [3] have shown that the height of α is greater than the constant $(\log 5)/12$.

Amoroso and Masser [4] improved upon the bounds in [1] for the case where $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. They showed that, for any ϵ, the height of α is bounded below by $c(\epsilon)d^{-\epsilon}$. Our first theorem is a generalization of this result to the case when α generates a Galois extension of an arbitrary number field.

Theorem 1. *Let $\epsilon > 0$ be given. Let α be a non-zero algebraic number, not a root of unity, such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 2$ and $\mathbb{K}(\alpha)/\mathbb{K}$ is Galois for some number field $\mathbb{K}$. Let δ be the degree of α over $\mathbb{K}$. Then there is an effectively computable constant $c(\epsilon, \mathbb{K}) > 0$ such that*

$$h(\alpha) \geq c(\epsilon, \mathbb{K})\delta^{-2\epsilon}.$$

Relative height bounds for α in a number field $\mathbb{K}$ which is abelian over $\mathbb{L}$ are given in [6] and [2]. These bounds are similar in shape to Dobrowolski's bound.

Theorem 1 determines bounds for $h(\alpha)$ when $\mathbb{K}(\alpha)/\mathbb{K}$ is Galois, and therefore when $\mathbb{Q}(\alpha)/\mathbb{K}$ is Galois. Our next theorem determines height bounds for any element α in a Galois extension $\mathbb{F}$ of $\mathbb{K}$ which is non-zero and not a root of unity. This is a generalization of Theorem 3.1 in [4].

Theorem 2. *Let $\mathbb{K}$ be a number field with degree τ over $\mathbb{Q}$. For any positive integer $r \geq 1$ and any $\epsilon > 0$ there is a positive effective constant $c(\epsilon, r, \tau)$ with the following property. Let $\mathbb{F}/\mathbb{K}$ be a Galois extension of relative degree η, and suppose $\alpha \in \mathbb{F}^*$ is not a root of unity. Assume that r conjugates of α over $\mathbb{K}$ are multiplicatively independent. Then*

$$h(\alpha) \geq c(\epsilon, r, \tau)\eta^{-\frac{1}{r+1}-\epsilon}.$$

Theorem 2 is proven in Section 5, where the explicit constants are presented. Taking $r = 1$, we have the following corollary as an immediate consequence.

Corollary 1.1. *For any $\epsilon > 0$ there is a positive effective constant $c(\epsilon, \tau)$ with the following property. Let $\mathbb{F}/\mathbb{K}$ be a Galois extension, with $[\mathbb{F} : \mathbb{K}] = \eta$, and suppose $\alpha \in \mathbb{F}^*$ is not a root of unity. Then*

$$h(\alpha) \geq c(\epsilon, \tau)\eta^{-\frac{1}{2}-\epsilon}.$$

The present paper closely follows and builds on the work of Amoroso and Masser in [4].

2. Preliminaries

In this section, we collect results that will be used in the proofs of Theorem 1 and Theorem 2.

2.1. **Finite linear groups.** We will require a bound on the size of finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ in the proof of Lemma 3.1. We now establish this bound, following the work of Serre [19].

Proposition 2.1 (Serre)**.** *Let A be an abelian variety, and let u be an automorphism of A of finite order. Let $n \geq 2$ be a positive integer such that $u \equiv 1 \mod n$. If $n = 2$, then $u^2 = 1$. Otherwise, we have $u = 1$.*

The proof of Lemma 3.1 will use the following well-known corollary to Proposition 2.1 (see also [4, Remark 2.3]).

Corollary 2.2. *Let H be a finite subgroup of $\mathrm{GL}_\rho(\mathbb{Z})$. The reduction modulo 3 homomorphism $\phi_3 : H \to \mathrm{GL}_\rho(\mathbb{Z}/3\mathbb{Z})$ is injective. As a result, the order of a finite subgroup of $\mathrm{GL}_\rho(\mathbb{Z})$ is less than 3^{ρ^2}.*

Proof. Let u be an element in $\ker(\phi_3) \subset H$. Then u has finite order and $u \equiv I_\rho \mod 3$, where I_ρ is the $\rho \times \rho$ identity matrix. By Proposition 2.1, we have $u = I_\rho$. This establishes that ϕ_3 is injective. We conclude that the order of H is at most $|\mathrm{GL}_\rho(\mathbb{Z}/3\mathbb{Z})|$, which is less than 3^{ρ^2}. $\square$

Remark 2.3. In an unpublished paper from 1995, Feit [13] shows that the maximal order of a finite subgroup of $\mathrm{GL}_\rho(\mathbb{Q})$ is $2^\rho \rho!$, except when $\rho = 2, 4, 6, 7, 8, 9, 10$. He further shows that for these exceptional cases, the maximal order is

$$12, 1152, 103680, 2903040, 696729600, 1393459200, 8360755200,$$

respectively. Therefore, the maximal order of a finite subgroup is at most $\frac{135}{2} 2^\rho \rho!$ for all ρ. See [7] for more information about these subgroups. Additionally, in 1997, Friedland showed in [14] that the orthogonal groups are the maximal subgroups for ρ large enough.

2.2. **Height of algebraic numbers.** We will use the following auxiliary height bounds in our proofs of Theorem 1 and Theorem 2.

The first is Corollary 1.6 of [5].

Proposition 2.4 (Amoroso-Viada)**.** *Let $\alpha_1, \ldots, \alpha_n$ be multiplicatively independent algebraic numbers in a number field $\mathbb{A}$ of degree $D = [\mathbb{A} : \mathbb{Q}]$. Then*

$$h(\alpha_1) \ldots h(\alpha_n) \geq D^{-1}(1050 n^5 \log 3D)^{-n^2(n+1)^2}.$$

The following result is Théorème 1.3 from [2].

Proposition 2.5 (Amoroso-Delsinne)**.** *Let α be a non-zero algebraic number which is not a root of unity. For every abelian extension $\mathbb{A}$ of $\mathbb{B}$, we have*

$$h(\alpha) \geq \frac{(g(\tau)\Delta)^{-c}}{D} \frac{(\log\log 5D)^3}{(\log 2D)^4},$$

where c is an absolute, strictly positive constant, Δ is the absolute value of the discriminant of $\mathbb{B}$ over $\mathbb{Q}$, $\tau = [\mathbb{B} : \mathbb{Q}]$, $D = [\mathbb{A}(\alpha) : \mathbb{A}]$, and $g(\tau) = 1$ if

there exists a tower of extensions

$$\mathbb{Q} = \mathbb{B}_0 \subset \mathbb{B}_1 \subset \cdots \subset \mathbb{B}_m = \mathbb{B}$$

with $\mathbb{B}_i/\mathbb{B}_{i-1}$ Galois for $i = 1, \ldots m$, and $g(\tau) = \tau!$ otherwise.

Remark 2.6. The constant c in Proposition 2.5 depends on a number of constants defined in [2], as well as on constants from papers of Friedlander [15] and Stark [22].

Finally, we will use Théorème 1.6 of [11], in which $\mathbb{Q}^{ab}$ denotes the maximal abelian extension of $\mathbb{Q}$, and $\mathbb{G}_m(\overline{\mathbb{Q}})$ denotes the multiplicative group of $\overline{\mathbb{Q}}$.

Proposition 2.7 (Delsinne). *For any positive integer n, there exists an effectively computable constant $c(n) > 0$ depending only on n for which the following property holds. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{G}_m^n(\overline{\mathbb{Q}})$. If*

$$\prod_{i=1}^{n} h(\alpha_i) \leq \left(c(n)[\mathbb{Q}^{ab}(\boldsymbol{\alpha}) : \mathbb{Q}^{ab}](\log(3[\mathbb{Q}^{ab}(\boldsymbol{\alpha}) : \mathbb{Q}^{ab}]))^{\kappa(n)} \right)^{-1},$$

where $\kappa(n) = 3n(2(n+1)^2(n+1)!)^n$, then $\boldsymbol{\alpha}$ is contained in a torsion subvariety B for which

$$(\deg B)^{1/\mathrm{codim}(B)} \leq c(n)[\mathbb{Q}^{ab}(\boldsymbol{\alpha}) : \mathbb{Q}^{ab}]^{\eta(n)}(\log(3[\mathbb{Q}^{ab}(\boldsymbol{\alpha}) : \mathbb{Q}^{ab}]))^{\mu(n)},$$

where

$$\eta(n) = (n-1)!\left(\sum_{i=0}^{n-3} \frac{1}{i!} + 1 \right) + n - 1$$

and $\mu(n) = 8m!(2(n+1)^2(n+1)!)^n$.

In fact, we may take $c(n) = (2n^2)^n \exp\left(64n^2 n! \left(2(n+1)^2(n+1)! \right)^{2n} \right)$.

Notice that if $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent, then $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ cannot be contained in a torsion subvariety. This simple observation yields the following corollary to Proposition 2.7.

Corollary 2.8. *Let n be a positive integer, and let $\alpha_1, \ldots, \alpha_n$ be multiplicatively independent algebraic numbers. Then there exists an effectively computable constant $c(n) > 0$ depending only on n for which*

$$\prod_{i=1}^{n} h(\alpha_i) > \left(c(n)[\mathbb{Q}^{ab}(\boldsymbol{\alpha}) : \mathbb{Q}^{ab}](\log(3[\mathbb{Q}^{ab}(\boldsymbol{\alpha}) : \mathbb{Q}^{ab}]))^{\kappa(n)} \right)^{-1},$$

where $\kappa(n) = 3n(2(n+1)^2(n+1)!)^n$.

2.3. **Estimates for** $\phi(n)/n$**.** We will make use of the following lower bound for Euler's totient function, which is a slightly weaker version of [18, Theorem 15].

Proposition 2.9. *For all natural numbers* $n \geq 3$, *we have*

$$\frac{\phi(n)}{n} > \frac{1}{\exp\left(\gamma\right)\log\log n + \frac{3}{\log\log n}},$$

where γ *is Euler's constant.*

The following lower bound for $\phi(n)^{1+\epsilon}/n$ will be useful in making the lower bound constants explicit in the proofs of both of our main theorems.

Lemma 2.10. *For any* $\epsilon > 0$, *there is an effective constant* $C(\epsilon)$ *such that*

$$\frac{\phi(n)^{1+\epsilon}}{n} \geq C(\epsilon)$$

for all $n \geq 3$. *Specifically, one can take*

$$C(\epsilon) = \left(\frac{(\log\log 3)\left(\exp(2)\frac{\epsilon}{2+2\epsilon}\right)^{\sqrt{\frac{\epsilon}{2+2\epsilon}}+1}}{\exp\left(\gamma\right) + 3^{\frac{1}{1+\epsilon}}\left(\exp(2)\frac{\epsilon}{2+2\epsilon}\right)^{\sqrt{\frac{\epsilon}{2+2\epsilon}}+1}} \right)^{1+\epsilon}.$$

Proof. By Proposition 2.9, for all $n \geq 3$ we have

$$\frac{\phi(n)}{n} > \frac{\log\log n}{\exp\left(\gamma\right)\left(\log\log n\right)^2 + 3}.$$

We use the fact that $\log x \leq \frac{x^\theta}{\exp(1)\theta}$ for any $\theta > 0$ to replace the power of $\log\log n$ in the denominator and conclude that

$$\frac{\phi(n)}{n} > \frac{\log\log 3}{\exp\left(\gamma\right)\frac{n^{2\theta^2}}{(\exp(1)\theta)^{2\theta+2}} + 3}.$$

Hence,

$$\frac{\phi(n)}{n^{1-2\theta^2}} \geq \frac{\log\log 3}{\frac{\exp(\gamma)}{(\exp(1)\theta)^{2\theta+2}} + \frac{3}{n^{2\theta^2}}} \geq \frac{\log\log 3}{\frac{\exp(\gamma)}{(\exp(1)\theta)^{2\theta+2}} + \frac{3}{3^{2\theta^2}}},$$

which implies that

$$\frac{\phi(n)^{1+\frac{2\theta^2}{1-2\theta^2}}}{n} \geq \left(\frac{\log\log 3}{\frac{\exp(\gamma)}{(\exp(1)\theta)^{2\theta+2}} + 3^{1-2\theta^2}} \right)^{1+\frac{2\theta^2}{1-2\theta^2}}.$$

Choosing θ such that $2\theta^2 = \frac{\epsilon}{1+\epsilon}$ completes the proof.   □

Remark 2.11. Our lemma holds for all $n \geq 3$. By Mertens' theorem (see, for example, [17, Theorem 3.15]), $\phi(n)/n \sim 1/(\exp(\gamma)\log\log n)$ as $n \to \infty$. Using this, one can obtain sharper lower bounds for n "sufficiently large."

3. Some Useful Lemmas

In this section we prove two lemmas that will be useful in the proof of Theorem 1.

Lemma 3.1. *Let $\mathbb{F}/\mathbb{K}$ be a Galois extension. Assume that $\alpha \in \mathbb{F}^*$ is not a root of unity, let $\alpha_1, \ldots, \alpha_\delta$ be the conjugates of α over $\mathbb{K}$, and let ρ be the multiplicative rank of this set of conjugates. Let e be the order of the group of roots of unity in $\mathbb{F}$, so that $\mathbb{Q}(\zeta_e) \subset \mathbb{F}$. Then there exists a subfield $\mathbb{L}$ of $\mathbb{F}$ which is Galois over $\mathbb{K}$ of relative degree $[\mathbb{L} : \mathbb{K}] = n \leq n(\rho) < 3^{\rho^2}$, and $\alpha^e \in \mathbb{L}$.*

Proof. Let $\beta_i = \alpha_i^e$, and $\mathbb{L} = \mathbb{K}(\beta_1, \ldots, \beta_\delta) \subseteq \mathbb{F}$. Then, by construction, $\mathbb{L}$ is Galois over $\mathbb{K}$ and $\alpha^e \in \mathbb{L}$. Consider the multiplicative group

$$\mathcal{M} = \{\beta_1^{a_1} \cdot \cdots \cdot \beta_\delta^{a_\delta} : a_i \in \mathbb{Z}\},$$

which is a $\mathbb{Z}$-module that is multiplicatively spanned by $\{\beta_1, \beta_2, \ldots, \beta_\delta\}$. First, we will show that $\mathcal{M}$ is a free $\mathbb{Z}$-module of rank ρ. It is enough to show that $\mathcal{M}$ is torsion-free as the fact that ρ is the multiplicative rank of $\{\alpha_1, \ldots, \alpha_\delta\}$ implies that it is also the multiplicative rank of $\{\beta_1, \ldots, \beta_\delta\}$. Assume for the sake of contradiction that there exists an $x \in \mathcal{M}$ such that $x \neq 1$ and $x^n = 1$ for some positive integer $n > 1$. Then $x = \beta_1^{a_1} \cdot \cdots \cdot \beta_\delta^{a_\delta}$ for some $a_1, \ldots, a_\delta \in \mathbb{Z}$. Since $x^n = 1$, we get

$$\left(\beta_1^{a_1} \cdot \cdots \cdot \beta_\delta^{a_\delta}\right)^n = \left(\alpha_1^{a_1} \cdot \cdots \cdot \alpha_\delta^{a_\delta}\right)^{ne} = 1.$$

Hence, $y = \alpha_1^{a_1} \cdot \cdots \cdot \alpha_\delta^{a_\delta}$ is a root of unity. Since $y \in \mathbb{F}$ and e is the order of the group of roots of unity in $\mathbb{F}$, it follows that $x = y^e = 1$, contrary to our assumption.

Since $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ acts on $\mathcal{M}$ by permuting the α_i, this action defines an injective homomorphism from $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ to $\mathrm{GL}_\rho(\mathbb{Z})$. This implies that the finite group $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is isomorphic to a finite subgroup of $\mathrm{GL}_\rho(\mathbb{Z})$. By Corollary 2.2 the order of a finite subgroup of $\mathrm{GL}_\rho(\mathbb{Z})$ is bounded by $n(\rho)$ which is at most 3^{ρ^2}. We conclude that $[\mathbb{L} : \mathbb{K}] \leq n(\rho) < 3^{\rho^2}$. $\qquad\square$

Lemma 3.2. *Let $\epsilon > 0$ be given. Let $\mathbb{K}$ be a number field. Assume that α is a non-zero algebraic number, not a root of unity, such that $\mathbb{K}(\alpha)/\mathbb{K}$ is Galois. Let δ be the degree of α over $\mathbb{K}$. Further, let e be the order of the group of roots of unity in $\mathbb{K}(\alpha)$, f be the order of the group of roots of unity in $\mathbb{K}$, $\tau = [\mathbb{K} : \mathbb{Q}]$, and let ρ be the multiplicative rank of the conjugates of α over $\mathbb{K}$. Then*

$$[\mathbb{K}(\alpha) : \mathbb{K}(\zeta_e)] \leq \delta^\epsilon C_4(\mathbb{K}, \epsilon),$$

with $C_4(\mathbb{K}, \epsilon) = \frac{1}{C(\epsilon)} n(\rho) f \tau^{1+\epsilon}$. We have $C(\epsilon)$ as in Lemma 2.10 unless $e/f \in \{1, 2\}$ in which case we take $C(\epsilon) = 1/2$.

Proof. We begin by obtaining a few inequalities, proving (3) and (4) below. By the second isomorphism theorem, we have

$$[\mathbb{K}(\zeta_e) : \mathbb{K}] = [\mathbb{Q}(\zeta_e) : \mathbb{K} \cap \mathbb{Q}(\zeta_e)] = \frac{[\mathbb{Q}(\zeta_e) : \mathbb{Q}(\zeta_f)]}{[\mathbb{K} \cap \mathbb{Q}(\zeta_e) : \mathbb{Q}(\zeta_f)]}$$

$$= \frac{\phi(e)/\phi(f)}{[\mathbb{K} \cap \mathbb{Q}(\zeta_e) : \mathbb{Q}(\zeta_f)]}.$$

Since $[\mathbb{K} \cap \mathbb{Q}(\zeta_e) : \mathbb{Q}(\zeta_f)] \leq [\mathbb{K} : \mathbb{Q}(\zeta_f)]$, we conclude that

$$[\mathbb{K}(\zeta_e) : \mathbb{K}] \geq \frac{\phi(e)/\phi(f)}{[\mathbb{K} : \mathbb{Q}(\zeta_f)]}.$$

It follows from the fact that ϕ is multiplicative that

$$(3) \qquad [\mathbb{K}(\zeta_e) : \mathbb{K}] \geq \frac{\phi(e)/\phi(f)}{[\mathbb{K} : \mathbb{Q}(\zeta_f)]} \geq \frac{\phi(\frac{e}{f})}{[\mathbb{K} : \mathbb{Q}(\zeta_f)]}.$$

Next, we will show

$$(4) \qquad \frac{\frac{e}{f}}{\phi(\frac{e}{f})} \leq \frac{[\mathbb{K} : \mathbb{Q}(\zeta_f)]^\epsilon}{C(\epsilon)} \delta^\epsilon.$$

By Lemma 2.10, if $e/f \geq 3$ we have the upper bound

$$\frac{\frac{e}{f}}{\phi(\frac{e}{f})} \leq \frac{1}{C(\epsilon)} \left(\phi(\tfrac{e}{f}) \right)^\epsilon.$$

If $e/f \in \{1, 2\}$, we can take $C(\epsilon) = 1/2$ and this is still satisfied. Again appealing to the multiplicativity of ϕ, we have
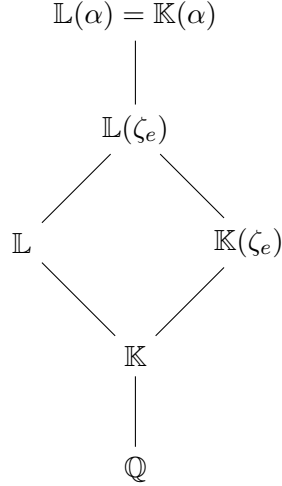
$$\phi(\tfrac{e}{f}) \leq \frac{\phi(e)}{\phi(f)} = [\mathbb{Q}(\zeta_e) : \mathbb{Q}(\zeta_f)] \leq [\mathbb{K}(\zeta_e) : \mathbb{K}][\mathbb{K} : \mathbb{Q}(\zeta_f)] \leq \delta[\mathbb{K} : \mathbb{Q}(\zeta_f)].$$

Hence, (4) follows by combining these two inequalities.

Now we will proceed to prove the bound for $[\mathbb{K}(\alpha) : \mathbb{K}(\zeta_e)]$ stated in the lemma. By Lemma 3.1 there is a subfield $\mathbb{L}$ of $\mathbb{K}(\alpha)$ which is Galois over $\mathbb{K}$, contains α^e and

$$(5) \qquad [\mathbb{L} : \mathbb{K}] = n \leq n(\rho).$$

Thus, we have $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{K}(\alpha)$, so $\mathbb{K}(\alpha) = \mathbb{L}(\alpha)$.

$$\mathbb{L}(\alpha) = \mathbb{K}(\alpha)$$

$$\mathbb{L}(\zeta_e)$$

$$\mathbb{L} \qquad \mathbb{K}(\zeta_e)$$

$$\mathbb{K}$$

$$\mathbb{Q}$$

Let $e' = [\mathbb{L}(\alpha) : \mathbb{L}]$. Since the minimal polynomial for α over $\mathbb{L}$ divides $x^e - \alpha^e$, we conclude that $e' \leq e$. Using multiple applications of the tower law, we have

$$[\mathbb{K}(\alpha) : \mathbb{K}(\zeta_e)] = [\mathbb{L}(\alpha) : \mathbb{L}(\zeta_e)][\mathbb{L}(\zeta_e) : \mathbb{K}(\zeta_e)]$$

$$= [\mathbb{L}(\zeta_e) : \mathbb{K}(\zeta_e)]\frac{[\mathbb{L}(\alpha) : \mathbb{L}]}{[\mathbb{L}(\zeta_e) : \mathbb{L}]}$$

$$= e'\frac{[\mathbb{L}(\zeta_e) : \mathbb{K}(\zeta_e)]}{[\mathbb{L}(\zeta_e) : \mathbb{L}]} = e'\frac{[\mathbb{L} : \mathbb{K}]}{[\mathbb{K}(\zeta_e) : \mathbb{K}]}.$$

By (5), we see that

$$[\mathbb{K}(\alpha) : \mathbb{K}(\zeta_e)] \leq e'\frac{n(\rho)}{[\mathbb{K}(\zeta_e) : \mathbb{K}]}.$$

Using (3) we have

$$[\mathbb{K}(\alpha) : \mathbb{K}(\zeta_e)] \leq e'\frac{n(\rho)}{[\mathbb{K}(\zeta_e) : \mathbb{K}]} \leq \frac{e'}{\phi(\frac{e}{f})}n(\rho)[\mathbb{K} : \mathbb{Q}(\zeta_f)].$$

Since $e' \leq e$, we conclude that $e' \leq \frac{e}{f}f$, and hence

$$[\mathbb{K}(\alpha) : \mathbb{K}(\zeta_e)] \leq \frac{\frac{e}{f}}{\phi(\frac{e}{f})}n(\rho)f[\mathbb{K} : \mathbb{Q}(\zeta_f)].$$

Combining this bound with (4) shows that

$$[\mathbb{K}(\alpha) : \mathbb{K}(\zeta_e)] \leq \frac{1}{C(\epsilon)}\delta^\epsilon n(\rho)f[\mathbb{K} : \mathbb{Q}(\zeta_f)]^{1+\epsilon} \leq \delta^\epsilon C_4(\mathbb{K}, \epsilon)$$

with $C_4(\mathbb{K}, \epsilon) = \frac{1}{C(\epsilon)}n(\rho)f\tau^{1+\epsilon}$, as needed.

$\square$

4. Proof Of Theorem 1

In this section, we present the proof of Theorem 1, which generalizes Theorem 3.3 of [4].

Proof. Let $\epsilon > 0$ be given, let r be the smallest integer greater than $1/\epsilon$, and let $\tau = [\mathbb{K} : \mathbb{Q}]$. First consider the case when $r > \delta$, so that

$$\delta \leq r - 1 \leq \tfrac{1}{\epsilon} < r.$$

We will show that $h(\alpha) \gg_{\tau,\epsilon} 1$. For $d \geq 2$, using equation (2), we obtain

$$h(\alpha) \geq \frac{2}{d(\log 3d)^3}.$$

The function $f_1(x) = \frac{2}{x(\log 3x)^3}$ is decreasing for $x \geq 1$. Since $\mathbb{Q}(\alpha) \subset \mathbb{K}(\alpha)$ we have

$$d = [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{K}(\alpha) : \mathbb{Q}] = [\mathbb{K}(\alpha) : \mathbb{K}][\mathbb{K} : \mathbb{Q}] = \delta\tau \leq \tau/\epsilon.$$

Therefore,

$$h(\alpha) \geq f_1(\tau/\epsilon) = \frac{2}{\tau/\epsilon(\log 3\tau/\epsilon)^3}.$$

We can often improve upon this lower bound. Using equation (1) for $d \geq 2$ yields

$$h(\alpha) \geq \frac{1}{4d}\left(\frac{\log\log d}{\log d}\right)^3.$$

Let $g_1(x) = \frac{1}{4x}\left(\frac{\log\log x}{\log x}\right)^3$. The function $g_1(x)$ is positive for all $x \geq 3$ and decreasing for $x \geq 7$. For $x = 3, 4, 5, 6$, we see that $g_1(x)$ achieves its minimum at $g_1(3) = 0.00005227953369\ldots$. For $d \geq 7$, since $d \leq \tau/\epsilon$, we have

$$h(\alpha) \geq g_1(\tau/\epsilon).$$

There exists $a \in (184, 185)$ such that for $x \leq a$ we have $f_1(x) > g_1(x)$, but for $x \geq a$, $g_1(x) > f_1(x)$. (In fact, $a = 184.615\ldots$.) We also note that $f_1(6) > g_1(3)$. We conclude that when $r > \delta$, we have $h(\alpha) \geq C_1(\epsilon, \tau)$, where

$$C_1(\epsilon, \tau) = \begin{cases} f_1(6), & \text{if } 3 \leq d \leq 6 \text{ and } \tau/\epsilon < 6, \\ f_1(\tau/\epsilon), & \text{if } 3 \leq d \leq 6 \text{ and } \tau/\epsilon \geq 6, \text{ or if } d \geq 7 \text{ and } \tau/\epsilon \leq a, \\ g_1(\tau/\epsilon), & \text{if } d \geq 7 \text{ and } \tau/\epsilon \geq a. \end{cases}$$

For $d = 2$, we can use $C_1 = f_1(2)$, and for $d = 1$ we can use $C_1 = \log 2$.

We may now assume that $r \leq \delta$. Let ρ be the multiplicative rank of the conjugates of α over $\mathbb{K}$.

First, consider the case when $\rho \geq r$. (That is, r of the conjugates of α over $\mathbb{K}$ are multiplicatively independent.) By Proposition 2.4, with $D = [\mathbb{K}(\alpha) : \mathbb{Q}] = \delta\tau$, we have

$$h(\alpha)^r \geq (\delta\tau)^{-1}(1050r^5\log(3\delta\tau))^{-r^2(r+1)^2}$$

using the fact that the Weil heights of conjugate algebraic numbers are equal. Since $r > \frac{1}{\epsilon}$, it follows that $-\frac{1}{r} > -\epsilon$, so $(\delta\tau)^{-\frac{1}{r}} > (\delta\tau)^{-\epsilon}$. Therefore, upon taking the rth roots, with $f_2(\delta, \tau, r) = (1050r^5 \log(3\delta\tau))^{-r(r+1)^2}$ we have

$$(6) \qquad h(\alpha) > \delta^{-\epsilon}\tau^{-\epsilon}f_2(\delta, \tau, r).$$

Since $r - 1 \leq \frac{1}{\epsilon}$, it follows that $r \leq 1 + \frac{1}{\epsilon}$ so

$$f_2(\delta, \tau, r) \geq \left(1050(1 + \tfrac{1}{\epsilon})^5 \log(3\delta\tau)\right)^{-(1+\frac{1}{\epsilon})(2+\frac{1}{\epsilon})^2}.$$

Using the inequality $\log(x) \leq \frac{1}{\epsilon_1 \exp(1)}x^{\epsilon_1}$, which holds for any $\epsilon_1 > 0$, we see that

$$f_2(\delta, \tau, r) \geq \left(1050(1 + \tfrac{1}{\epsilon})^5 \frac{1}{\epsilon_1 \exp(1)}(3\delta\tau)^{\epsilon_1}\right)^{-(1+\frac{1}{\epsilon})(2+\frac{1}{\epsilon})^2}.$$

Taking $\epsilon_1 = \epsilon/(1 + \frac{1}{\epsilon})(2 + \frac{1}{\epsilon})^2$ we have

$$f_2(\delta, \tau, r) \geq \left(\frac{1050}{\epsilon \exp(1)}(1 + \tfrac{1}{\epsilon})^6(2 + \tfrac{1}{\epsilon})^2\right)^{-(1+\frac{1}{\epsilon})(2+\frac{1}{\epsilon})^2}(3\delta\tau)^{-\epsilon}.$$

We conclude, from (6), that $h(\alpha) \geq C_2(\epsilon, \tau)\delta^{-2\epsilon}$, where

$$C_2(\epsilon, \tau) = \tau^{-2\epsilon}3^{-\epsilon}\left(\frac{1050}{\epsilon \exp(1)}(1 + \tfrac{1}{\epsilon})^6(2 + \tfrac{1}{\epsilon})^2\right)^{-(1+\frac{1}{\epsilon})(2+\frac{1}{\epsilon})^2}.$$

Now we may assume that $r \leq \delta$ and $\rho \leq r - 1$. First, let us establish some notation. Let e be the order of the group of roots of unity in $\mathbb{K}(\alpha)$, let f be the order of the group of roots of unity in $\mathbb{K}$, and let $D = [\mathbb{K}(\alpha) : \mathbb{K}(\zeta_e)]$. By Proposition 2.5, taking $\mathbb{A} = \mathbb{K}(\zeta_e)$ and $\mathbb{B} = \mathbb{K}$, we conclude that there is an absolute positive constant c such that

$$h(\alpha) \geq \frac{(g(\tau)\Delta)^{-c}}{D}\frac{(\log\log 5D)^3}{(\log 2D)^4},$$

where Δ is the absolute value of the discriminant of $\mathbb{K}$ over $\mathbb{Q}$ and $g(\tau) = 1$ if there exists a tower of successive Galois extensions $\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_m = \mathbb{K}$, and $g(\tau) = \tau!$ otherwise.

Notice that the function $f(x) = \frac{1}{x}\frac{(\log\log 5x)^3}{(\log 2x)^4}$ is decreasing for all $x \geq 1$. By Lemma 3.2 we have

$$D = [\mathbb{K}(\alpha) : \mathbb{K}(\zeta_e)] \leq \delta^{\epsilon}C_4(\mathbb{K}, \epsilon)$$

with $C_4(\mathbb{K}, \epsilon) = \frac{1}{C(\epsilon)}n(\rho)f\tau^{1+\epsilon}$. Therefore,

$$h(\alpha) \geq \frac{(g(\tau)\Delta)^{-c}}{C_4(\mathbb{K}, \epsilon)\delta^{\epsilon}}\frac{\left(\log\log(5C_4(\mathbb{K}, \epsilon)\delta^{\epsilon})\right)^3}{\left(\log(2C_4(\mathbb{K}, \epsilon)\delta^{\epsilon})\right)^4}.$$

It remains to show that this is $\gg_{\rho, \mathbb{K}} \delta^{-2\epsilon}$. The constant $C(\epsilon)$ from Lemma 2.10 is easily seen to be positive and less than 1, which implies that $C_4(\mathbb{K}, \epsilon) \geq 1$. Moreover, for all $y \geq 1$, we have

$$\frac{y \left(\log \log 5y\right)^3}{\left(\log 2y\right)^4} \geq \frac{1}{4}.$$

Since $C_4(\mathbb{K}, \epsilon)\delta^\epsilon \geq 1$, we conclude that

$$\frac{\left(\log \log(5C_4(\mathbb{K}, \epsilon)\delta^\epsilon)\right)^3}{\left(\log(2C_4(\mathbb{K}, \epsilon)\delta^\epsilon)\right)^4} \geq \frac{1}{4C_4(\mathbb{K}, \epsilon)\delta^\epsilon}.$$

We have shown that

$$h(\alpha) \geq \delta^{-2\epsilon} C_5(\mathbb{K}, \epsilon),$$

where $C_5(\mathbb{K}, \epsilon) = \frac{(g(\tau)\Delta)^{-c}C(\epsilon)^2}{4(n(\rho)f\tau^{1+\epsilon})^2}$ and $C(\epsilon)$ is the constant from Lemma 2.10. Since we are assuming that $\rho \leq r - 1 < 1/\epsilon$, then $n(\rho) < 3^{\rho^2} < 3^{(1/\epsilon)^2}$. Thus, we have

$$h(\alpha) \geq \delta^{-2\epsilon} C_3(\mathbb{K}, \epsilon),$$

where $C_3(\mathbb{K}, \epsilon) = \frac{(g(\tau)\Delta)^{-c}C(\epsilon)^2}{4(3^{(1/\epsilon)^2}f\tau^{1+\epsilon})^2}$.

$\square$

Remark 4.1. Recall that, if $\mathbb{Q}(\alpha)/\mathbb{K}$ is Galois, then since $\mathbb{K} \subset \mathbb{Q}(\alpha)$, it follows that $\mathbb{K}(\alpha) = \mathbb{Q}(\alpha)$. Therefore, this theorem also applies to the case where $\mathbb{Q}(\alpha)/\mathbb{K}$ is Galois.

5. Proof of Theorem 2

We prove Theorem 2 below.

Proof. Let $\alpha_1, \ldots, \alpha_\delta$ be the conjugates of α over $\mathbb{K}$, and let ρ be their multiplicative rank. As a result, $\delta \leq \eta$. Since we assume that r conjugates of α over $\mathbb{K}$ are multiplicatively independent, we know that $\rho \geq r$.

Case 1 ($\rho > r$)**:** If the multiplicative rank of the conjugates of α over $\mathbb{K}$ is strictly larger than r, we know that there exists a subset

$$\{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{r+1}}\} \subset \{\alpha_1, \alpha_2, \ldots, \alpha_\delta\}$$

such that $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{r+1}}$ are distinct and multiplicatively independent. By Proposition 2.4,

$$h(\alpha_{i_1})h(\alpha_{i_2}) \cdots h(\alpha_{i_{r+1}}) \geq D^{-1} \left(1050(r + 1)^5 \log(3D)\right)^{-(r+1)^2(r+2)^2},$$

where $D = [\mathbb{Q}(\alpha_{i_1}, \ldots, \alpha_{i_{r+1}}) : \mathbb{Q}]$. Since the α_i are all conjugates, they all have the same height, so the left hand side of this inequality is $h(\alpha)^{r+1}$. In addition,

$$D = [\mathbb{Q}(\alpha_{i_1}, \ldots, \alpha_{i_{r+1}}) : \mathbb{Q}] \leq [\mathbb{F} : \mathbb{Q}] = [\mathbb{F} : \mathbb{K}][\mathbb{K} : \mathbb{Q}] = \eta\tau.$$

Upon taking $(r + 1)^{\text{st}}$ roots, it follows that

$$h(\alpha) \geq \tau^{-\frac{1}{r+1}} \eta^{-\frac{1}{r+1}} \left(1050(r + 1)^5 \log(3\tau\eta)\right)^{-(r+1)(r+2)^2}.$$

Recall that $\log x \leq \frac{1}{\epsilon_1 \exp(1)} x^{\epsilon_1}$ for any $\epsilon_1 > 0$. By applying this inequality with $\epsilon_1 = \frac{\epsilon}{(r+1)(r+2)^2}$, we get an explicit lower bound for $h(\alpha)$ in the desired form,

$$h(\alpha) \geq C_1(\epsilon, r, \tau) \eta^{-\frac{1}{r+1} - \epsilon},$$

where

$$C_1(\epsilon, r, \tau) = 3^{-\epsilon} \left(\frac{1050(r+1)^6(r+2)^2}{\epsilon \exp(1)} \right)^{-(r+1)(r+2)^2} \tau^{-\frac{1}{r+1} - \epsilon}.$$

Case 2 ($\rho = r$)**:** Let $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_r}$ be multiplicatively independent conjugates of α over $\mathbb{K}$. We denote by e the order of the group of roots of unity in $\mathbb{F}$ so that $\mathbb{Q}(\zeta_e) \subset \mathbb{F}$. By Lemma 3.1 we know that there exists a subfield $\mathbb{L}$ of $\mathbb{F}$ which is Galois over $\mathbb{K}$ such that $\alpha^e \in \mathbb{L}$ and $[\mathbb{L} : \mathbb{K}] = n \leq n(r) < 3^{r^2}$. By (1), we have

$$h(\alpha^e) \geq \frac{1}{4[\mathbb{Q}(\alpha^e) : \mathbb{Q}]} \left(\frac{\log\log([\mathbb{Q}(\alpha^e) : \mathbb{Q}])}{\log([\mathbb{Q}(\alpha^e) : \mathbb{Q}])} \right)^3,$$

provided $\alpha^e \notin \mathbb{Q}$. Now,

$$[\mathbb{Q}(\alpha^e) : \mathbb{Q}] \leq [\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{Q}] \leq n(r)\tau.$$

As in the proof of Theorem 1, we can use the properties of the function $g_1(x)$ previously defined to obtain

$$(7) \qquad h(\alpha) = \frac{1}{e} h(\alpha^e) \geq \frac{1}{e} \frac{1}{4n(r)\tau} \left(\frac{\log\log(n(r)\tau)}{\log(n(r)\tau)} \right)^3$$

whenever $[\mathbb{Q}(\alpha^e) : \mathbb{Q}] \geq 7$. When $n(r)\tau \leq 184$, this can be improved by using $f_1(x)$ in place of $g_1(x)$, as before, and similarly, we use $f_1(x)$ when $3 \leq [\mathbb{Q}(\alpha^e) : \mathbb{Q}] \leq 6$. For $[\mathbb{Q}(\alpha^e) : \mathbb{Q}] = 2$, we have $h(\alpha) \geq \frac{1}{e} f_1(2)$, and for $[\mathbb{Q}(\alpha^e) : \mathbb{Q}] = 1$ we have $h(\alpha) \geq \frac{1}{e} \log 2$. For the remainder of the proof, we focus on the case given in equation (7), and trust the reader to make the appropriate substitutions.

On the other hand, Corollary 2.8 implies that with $\boldsymbol{\alpha} = (\alpha_{i_1}, \ldots, \alpha_{i_r})$ we have

$$h(\boldsymbol{\alpha})^r > \left(c_2(r)[\mathbb{Q}^{\mathrm{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\mathrm{ab}}] \left(\log\left(3[\mathbb{Q}^{\mathrm{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\mathrm{ab}}] \right) \right)^{\kappa_2(r)} \right)^{-1},$$

where $\kappa_2(r) = 3r \left(2(r+1)^2(r+1)! \right)^r$ and

$$c_2(r) = (2r^2)^r \exp\left(64r^2 r! \left(2(r+1)^2(r+1)! \right)^{2r} \right).$$

Using the bound

$$[\mathbb{Q}^{\mathrm{ab}}(\boldsymbol{\alpha}) : \mathbb{Q}^{\mathrm{ab}}] \leq [\mathbb{Q}(\zeta_e)(\boldsymbol{\alpha}) : \mathbb{Q}(\zeta_e)] \leq [\mathbb{F} : \mathbb{Q}(\zeta_e)] = \frac{[\mathbb{F} : \mathbb{Q}]}{[\mathbb{Q}(\zeta_e) : \mathbb{Q}]} = \frac{\tau\eta}{\phi(e)},$$

we conclude that

$$(8) \qquad h(\alpha)^r > \left(c_2(r) \frac{\tau\eta}{\phi(e)} \left(\log \left(3 \frac{\tau\eta}{\phi(e)} \right) \right)^{\kappa_2(r)} \right)^{-1}.$$

Combining equations (7) and (8) yields

$$h(\alpha)^{r+1} > C_1(r, \tau, e)\eta^{-1} \left(\log(3\tfrac{\tau\eta}{\phi(e)}) \right)^{-\kappa_2(r)},$$

where $C_1(r, \tau, e) = c_2(r)^{-1} \left(\frac{\log\log(n(r)\tau)}{\log(n(r)\tau)} \right)^3 \frac{1}{4n(r)\tau^2} \frac{\phi(e)}{e}$. We now apply the inequality $\log x \le \frac{1}{\epsilon_1 \exp(1)} x^{\epsilon_1}$ with $\epsilon_1 = \epsilon/\kappa_2(r)$ and $x = 3\frac{\tau\eta}{\phi(e)}$ and conclude that

$$h(\alpha)^{r+1} > C_1(r, \tau, e)\eta^{-1} \left(\frac{\kappa_2(r)}{\epsilon \exp(1)} \right)^{-\kappa_2(r)} \left(3\frac{\tau\eta}{\phi(e)} \right)^{-\epsilon}.$$

This simplifies to

$$h(\alpha)^{r+1} > C_2(\epsilon, r, \tau, e)\eta^{-1-\epsilon}$$

with $C_2(\epsilon, r, \tau, e) = \left(\frac{\log\log(n(r)\tau)}{\log(n(r)\tau)} \right)^3 \left(\frac{\kappa_2(r)}{\epsilon \exp(1)} \right)^{-\kappa_2(r)} \frac{\phi(e)^{1+\epsilon}/e}{4n(r)c_2(r)3^\epsilon \tau^{2+\epsilon}}$. By Lemma 2.10, $\phi(e)^{1+\epsilon}/e \ge C(\epsilon)$, so that we can replace $C_2(\epsilon, r, \tau, e)$ in the inequality by

$$C_3(\epsilon, r, \tau) = \left(\frac{\log\log(n(r)\tau)}{\log(n(r)\tau)} \right)^3 \left(\frac{\kappa_2(r)}{\epsilon \exp(1)} \right)^{-\kappa_2(r)} \frac{C(\epsilon)}{4n(r)c_2(r)3^\epsilon \tau^{2+\epsilon}},$$

and upon taking $(r+1)^{\mathrm{st}}$ roots we have

$$h(\alpha) > C_3(\epsilon, r, \tau)^{\frac{1}{r+1}} \eta^{-\frac{1}{r+1} - \frac{\epsilon}{r+1}}.$$

Using the fact that $\eta^{-\epsilon/(r+1)} \ge \eta^{-\epsilon}$ we get the bound

$$h(\alpha) > C_3(\epsilon, r, \tau)^{\frac{1}{r+1}} \eta^{-\frac{1}{r+1} - \epsilon}.$$

$\square$

Acknowledgements

References

[1] F. Amoroso and S. David. Le problème de Lehmer en dimension supérieure. *J. Reine Angew. Math.*, 513:145–179, 1999.

[2] F. Amoroso and E. Delsinne. Une minoration relative explicite pour la hauteur dans une extension d'une extension abélienne. In *Diophantine geometry*, volume 4 of *CRM Series*, pages 1–24. Ed. Norm., Pisa, 2007.

[3] F. Amoroso and R. Dvornicich. A lower bound for the height in abelian extensions. *J. Number Theory*, 80(2):260–272, 2000.

[4] F. Amoroso and D. Masser. Lower bounds for the height in Galois extensions. *Bull. London Math. Soc.*, 48(6):1008–1012, 2016.

[5] F. Amoroso and E. Viada. Small points on rational subvarieties of tori. *Comment. Math. Helv.*, 87(2):355–383, 2012.

[6] F. Amoroso and U. Zannier. A relative Dobrowolski lower bound over abelian extensions. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 29(3):711–727, 2000.

[7] N. Berry, A. Dubickas, N. D. Elkies, B. Poonen, and C. Smyth. The conjugate dimension of algebraic numbers. *Q. J. Math.*, 55(3):237–252, 2004.

[8] P. E. Blanksby and H. L. Montgomery. Algebraic integers near the unit circle. *Acta Arith.*, 18:355–369, 1971.

[9] P. Borwein, E. Dobrowolski, and M. J. Mossinghoff. Lehmer's problem for polynomials with odd coefficients. *Ann. of Math. (2)*, 166(2):347–366, 2007.

[10] R. Breusch. On the distribution of the roots of a polynomial with integral coefficients. *Proc. Amer. Math. Soc.*, 2:939–941, 1951.

[11] E. Delsinne. Le problème de Lehmer relatif en dimension supérieure. *Ann. Sci. Éc. Norm. Supér. (4)*, 42(6):981–1028, 2009.

[12] E. Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta Arith.*, 34(4):391–401, 1979.

[13] W. Feit. The orders of finite linear groups. *preprint*, 1995.

[14] S. Friedland. The maximal orders of finite subgroups in $\mathrm{GL}_n(\mathbf{Q})$. *Proc. Amer. Math. Soc.*, 125(12):3519–3526, 1997.

[15] J. B. Friedlander. Estimates for prime ideals. *J. Number Theory*, 12(1):101–105, 1980.

[16] D. H. Lehmer, Factorization of certain cyclotomic functions. *Ann. of Math. (2)* 34: 461–479, 1933.

[17] P. Pollack. *Not always buried deep: a second course in elementary number theory.* Amer. Math. Soc., 2009.

[18] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.

[19] J. P. Serre. Rigidité du foncteur de Jacobi d'échelon $n \geq 3$, Appendix to A. Grothendieck, Techniques de construction en géométrie analytique, X. Construction de l'espace de Teichmüller. *Appendice à l'exposé* 17 *du séminaire Cartan*, (17), 1960-61.

[20] C. Smyth. The Mahler measure of algebraic numbers: a survey. In *Number theory and polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, pages 322–349. Cambridge Univ. Press, Cambridge, 2008.

[21] C. J. Smyth. On the product of the conjugates outside the unit circle of an algebraic integer. *Bull. London Math. Soc.*, 3:169–175, 1971.

[22] H. M. Stark. Some effective cases of the Brauer-Siegel theorem. *Invent. Math.*, 23:135–152, 1974.

[23] C. L. Stewart. Algebraic integers whose conjugates lie near the unit circle. *Bull. Soc. Math. France*, 106(2):169–176, 1978.

[24] P. Voutier. An effective lower bound for the height of algebraic numbers. *Acta Arith.*, 74(1):81–95, 1996.

Department of Mathematics, University of Oregon, Eugene, Oregon 97402 USA

  E-mail address: akhtari@uoregon.edu

Department of Mathematics Education, Gazi University, Ankara, 06500, Turkey

  E-mail address: kevseraktas@gazi.edu.tr

School of Mathematics, University of Bristol, University Walk, Clifton, Bristol, BS8 1TW, United Kingdom

  E-mail address: kirsti.biggs@bristol.ac.uk

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, T1K3M4 Canada

  E-mail address: alia.hamieh@uleth.ca

Department of Mathematics, Florida State University, Tallahassee, Florida 32306 USA

  E-mail address: petersen@math.fsu.edu

Department of Mathematics, Oberlin College, Oberlin, OH 44074 USA

  E-mail address: lola.thompson@oberlin.edu