ACTA ARITHMETICA
131.3 (2008)

The Mahler measure of dihedral extensions

by

John Garza (Austin, TX)

1. Introduction. Mahler's measure of a polynomial f, denoted by $M(f)$, is defined as the product of the absolute values of those roots of f that lie outside the unit disk, multiplied by the absolute value of the leading coefficient. If $f(x) = b\prod_{i=1}^{d}(x-\alpha_i)$, then $M(f) = |b|\prod_{i=1}^{d}\max\{1,|\alpha_i|\}$. If $f \in \mathbb{Z}[x]$, then $M(f) \geq 1$ and it is a result of Kronecker that for $f \in \mathbb{Z}[x]$, $M(f) = 1$ if and only if f is a product of a power of x and cyclotomic polynomials. In 1933, D. H. Lehmer [3] asked if for every $\varepsilon > 0$ there exists $f_\varepsilon \in \mathbb{Z}[x]$ such that $1 < M(f_\varepsilon) < 1+\varepsilon$. This is known as *Lehmer's question* and remains an open problem. For an algebraic number α, we let $m_{\alpha,\mathbb{Z}}$ be the minimal polynomial of α over $\mathbb{Z}$ and define $M(\alpha) \equiv M(m_{\alpha,\mathbb{Z}})$. It follows that for an algebraic number α that is not an integer, $M(\alpha) \geq 2$. An algebraic integer $\alpha \notin \mathbb{Z}$ is said to be reciprocal if $1/\alpha$ is a Galois conjugate of α. Chris Smyth [5] proved that amongst all nonreciprocal, nonzero algebraic integers the smallest Mahler measure is attained by the roots of $x^3 - x - 1$. A. Schinzel [4] proved that if f is monic of degree d satisfying $f(0) = \pm 1$, $f(\pm 1) \neq 0$, and all roots of f real, then

$$M(f) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{d/2}.$$

More recently F. Amoroso and R. Dvornicich [1] have extended the work of Schinzel [4] by establishing that for an algebraic number α, different from zero and the roots of unity, contained in an abelian Galois extension of $\mathbb{Q}$,

$$M(\alpha) \geq 5^{[\mathbb{Q}(\alpha):\mathbb{Q}]/12}.$$

In [2], F. Amoroso and U. Zannier establish the following: *Let* $\mathbb{K}$ *be any algebraic number field and let* $\mathbb{L}$ *be any abelian extension of* $\mathbb{K}$. *Then for*

2000 *Mathematics Subject Classification*: Primary 11R09; Secondary 11G50.
Key words and phrases: Mahler measure, dihedral Galois group.

any nonzero algebraic number α which is not a root of unity, we have

$$\log\left(\frac{M(\alpha)}{[\mathbb{Q}(\alpha):\mathbb{Q}]}\right) \geq \frac{C_2(\mathbb{K})}{D}\left(\frac{\log(2D)}{\log\log(5D)}\right)^{-13}$$

where $D = [\mathbb{L}(\alpha):\mathbb{L}]$ and $C_2(\mathbb{K})$ is a positive constant depending only on $\mathbb{K}$.

In this work, for $m \in \mathbb{N}$, $m \geq 3$, D_{2m} is a group with presentation $\langle \sigma, \tau \mid \sigma^m = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1}\rangle$. A group G is said to be *dihedral* if there exists $m \in \mathbb{N}$ with $m \geq 3$ such that $\mathrm{G} \approx \mathrm{D}_{2m}$. This article establishes the following.

THEOREM 1. *Amongst all polynomials in $\mathbb{Z}[x]$ whose splitting fields over $\mathbb{Q}$ are contained in dihedral Galois extensions of $\mathbb{Q}$, the lowest Mahler measure (other than 1) is attained by $x^3 - x - 1$.*

Since a finite dihedral extension of $\mathbb{Q}$ of degree $4m$, $m \geq 2$, is a quadratic extension of an abelian extension, by [2] we should expect, in principle, for such a result to exist. However, it is not known to the author if the constant $C_2(\mathbb{K})$ in Theorem 1 of [2] is strong enough to result in Theorem 1 provided here, and our Theorem 1 is attained by different methods than those found in [2].

Amongst the absolute values in a place v of an algebraic number field $\mathbb{K}$, two will play a role in the development of Theorem 1. If v is Archimedean, let $\|\cdot\|_v$ denote the unique absolute value in v which restricts to the usual Archimedean absolute value on $\mathbb{Q}$. If v is non-Archimedean and $v \mid p$, let $\|\cdot\|_v$ denote the unique absolute value in v restricting to the usual p-adic absolute value on $\mathbb{Q}$. For each place v of $\mathbb{K}$, let $\mathbb{K}_v$ and $\mathbb{Q}_v$ denote the completions of $\mathbb{K}$ and $\mathbb{Q}$ with respect to v, and define the local degree as $d_v \equiv [\mathbb{K}_v : \mathbb{Q}_v]$. Let $|\cdot|_v = \|\cdot\|_v^{d_v/d}$.

The absolute values $|\cdot|_v$ satisfy the product formula: if $\alpha \in \mathbb{K}^\times$, then $\prod_v |\alpha|_v = 1$. The absolute (logarithmic) *Weil height* of α is defined as $h(\alpha) = \sum_v \log^+ |\alpha|_v$ where the sum is over all places v of $\mathbb{K}$. Because of the way in which the absolute values $|\cdot|_v$ are normalized, the absolute Weil height of α does not depend on the field $\mathbb{K}$ in which α is contained. If α_i and α_j are algebraic integers, then $h(\alpha_i \cdot \alpha_j) \leq h(\alpha_i) + h(\alpha_j)$, and if α_i and α_j are Galois conjugates, then $h(\alpha_i) = h(\alpha_j)$. Also, if α is an algebraic integer, then $[\mathbb{Q}(\alpha):\mathbb{Q}]h(\alpha) = \log M(\alpha)$.

In this article, $\mathbb{K}/\mathbb{Q}$ will be a finite Galois extension. If $\alpha \in \mathbb{K}$, $\mathrm{H}_{\mathbb{Q}(\alpha)}$ will denote the subgroup of $\mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ fixing α. $\mathfrak{B}_1, \ldots, \mathfrak{B}_t$ (where $t \in \mathbb{N}$) will be the prime ideal divisors of $2\mathcal{O}_\mathbb{K}$, e their common ramification index, and f their common residue class degree. For $i \in \{1, \ldots, t\}$, let $\mathrm{Z}_{\mathfrak{B}_i}$ be the decomposition group of $\mathfrak{B}_i$. If 2 does not ramify in $\mathbb{K}$, then for $i \in \{1, \ldots, t\}$, $\Phi_{\mathfrak{B}_i}$ will denote the Frobenius automorphism of the extension $(\mathcal{O}_\mathbb{K}/\mathfrak{B}_i)/(\mathbb{Z}/2\mathbb{Z})$. Since $\mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ acts transitively by conjugation on

the $\mathrm{Z}_{\mathfrak{B}_i}$, it is sufficient for our purpose to explicitly consider only the higher ramification groups of $\mathfrak{B}_1$. We thus establish the following notations. Let G_0 be the inertia group of $\mathfrak{B}_1$, and for $i \in \mathbb{N}$, let G_i be the ith ramification group of $\mathfrak{B}_1$. We have $|\mathrm{G}_0| = e$, $\mathrm{G}_0 \trianglelefteq \mathrm{Z}_{\mathfrak{B}_1}$, $\mathrm{Z}_{\mathfrak{B}_1}/\mathrm{G}_0$ is cyclic of order f, $\mathrm{G}_1 \trianglelefteq \mathrm{G}_0$ is the unique Sylow-2 subgroup of G_0, $|\mathrm{G}_0/\mathrm{G}_1|$ divides $2^f - 1$, and for $i \in \mathbb{N}$, $\mathrm{G}_{i+1} \trianglelefteq \mathrm{G}_i$, and $\mathrm{G}_i/\mathrm{G}_{i+1}$ is of exponent 2. Also, $\mathrm{Z}_{\mathfrak{B}_1}/\mathrm{G}_0$ is the Galois group, $\mathrm{G}_{\mathfrak{B}_1}$, of the cyclic Galois extension $(\mathcal{O}_{\mathbb{K}}/\mathfrak{B}_1)/(\mathbb{Z}/2\mathbb{Z})$.

2. Outline of the proof of Theorem 1. This section provides an overview of the proof of Theorem 1. The first step, carried out in Section 3, is the consideration of dihedral Galois extensions of $\mathbb{Q}$ of degrees not divisible by 4. Lemma 1 establishes that we need not consider primitive elements of Galois extensions, and Lemma 2 concerns Galois extensions of $\mathbb{Q}$ of degree $2p$ where p is a prime number. Lemma 2 is used as the base case for an induction proof of Proposition 1 establishing $M(x^3-x-1)$ as a lower bound for the Mahler measures, different from 1, in dihedral Galois extensions of $\mathbb{Q}$ of degrees not divisible by 4. Section 3 concludes by pointing out that the Galois group of $x^3 - x - 1$ is dihedral.

Section 4 begins the analysis of dihedral Galois extensions of $\mathbb{Q}$ of degrees divisible by 4. We combine the structure of the $\mathrm{Z}_{\mathfrak{B}_i}$ as described in the introduction, assumptions allowed by the results of Smyth and Schinzel together with the Fundamental Theorem of Galois Theory to identify important allowable assumptions that are used in later sections.

Section 5 establishes Propositions 2 and 3 which constitute the fundamental method of drawing conclusions about the height of an algebraic number from information about the decomposition groups $\mathrm{Z}_{\mathfrak{B}_i}$. These Propositions are almost obvious to prove, but the language chosen for Proposition 2 along with the Archimedean results described by Lemmas 3, 4, and 5 allow for the exact nature of our Theorem 1.

Section 6 concerns algebraic integers of degrees ≥ 10 in dihedral Galois extensions of $\mathbb{Q}$. Proposition 4 establishes lower bounds for the height in the case that 2 does not ramify in $\mathbb{K}$. Proposition 5 establishes a lower bound for the height in the case that 2 ramifies in $\mathbb{K}$ with ramification index 2. This case is separated out from the cases in Proposition 7 as it will be used in Section 7. The cases of larger ramification index are covered jointly by Propositions 6 and 7. Proposition 7 is divided into five cases: $e \leq [\mathbb{Q}(\alpha) : \mathbb{Q}]/4$, $3e = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, $2e = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, $e = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, and $e = 2[\mathbb{Q}(\alpha) : \mathbb{Q}]$. These cases together with the assumptions allowed from previous sections establish Theorem 1 in the case of $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 10$.

Section 7 concerns the cases $[\mathbb{Q}(\alpha) : \mathbb{Q}] \in \{4, 6, 8\}$. This section once again uses the structure of $\mathrm{Z}_{\mathfrak{B}_i}$ to obtain lower bounds on the height. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}]h(\alpha) = \log M(\alpha)$, in order to achieve the desired lower bound of

$M(x^3 - x - 1)$ we must use Lemmas 3, 4 and 5 to obtain improved estimates for the quantity A defined by equation (1) in Proposition 2. Section 7 is thus complex in that we simultaneously consider possibilities for the angular and radial distribution of the conjugates of α together with the possibilities for the $\mathrm{Z}_{\mathfrak{B}_i}$.

3. Dihedral Galois groups of degrees not divisible by 4. As a necessary step, dihedral extensions of degrees not divisible by 4 are considered first. Let $m \in \mathbb{N}, m \geq 3$ and $\mathrm{G} = \langle\sigma\rangle \rtimes_{\varrho} \langle\tau\rangle \approx \mathrm{D}_{2m}$. The distinct elements of G are $1, \sigma, \sigma^2, \ldots, \sigma^{m-1}, \tau, \sigma\tau, \ldots, \sigma^{m-1}\tau$. Consequently, if a subgroup H of a dihedral group G is of order 3 or larger, then $\mathrm{H} \cap \langle\sigma\rangle \neq \{1\}$. For a reciprocal algebraic integer $\alpha \notin \mathbb{Z}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is even.

Let $\mathbb{K}$ be a non-totally real finite Galois extension of $\mathbb{Q}$ and fix an embedding η of $\mathbb{K}$ into $\mathbb{C}$. There exists $\xi \in \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ corresponding to complex conjugation with respect to η. Suppose that $\xi \in \mathrm{C}(\mathrm{Aut}(\mathbb{K}/\mathbb{Q}))$. Then, for all embeddings of $\mathbb{K}$ into $\mathbb{C}$, ξ corresponds to complex conjugation. The subfield of $\mathbb{K}$ fixed by ξ is thus totally real. Let $\alpha \in \mathcal{O}_{\mathbb{K}}$ be nonreal and different from the roots of unity. By the result of Kronecker, there exists a Galois conjugate γ of α such that $\beta \equiv \gamma \cdot \xi(\gamma) > 1$. $\mathbb{Q}(\beta)$ is totally real. Since $\xi \in \mathrm{C}(\mathrm{Aut}(\mathbb{K}/\mathbb{Q}))$, $2[\mathbb{Q}(\beta) : \mathbb{Q}] \leq [\mathbb{Q}(\gamma) : \mathbb{Q}]$, so $h(\beta) \leq 2h(\gamma)$. It follows that $M(\beta) \leq M(\alpha)$. By the result of Schinzel, $M(x^3 - x - 1) < M(\alpha)$. As a result, we only consider nonabelian algebraic integers. It is elementary to prove that the quotients of dihedral groups by normal subgroups are either abelian or dihedral. Consequently, by the Fundamental Theorem of Galois Theory, we only consider elements in dihedral extensions whose Galois closures are dihedral extensions of $\mathbb{Q}$.

Lemma 1 (Primitive elements in Galois extensions). *Let $\mathbb{K}/\mathbb{Q}$ be a nonabelian, non-totally real, finite Galois extension. Let $\omega \in \mathcal{O}_{\mathbb{K}}$ be a primitive element. Then there exists a nonprimitive element $\beta \in \mathcal{O}_{\mathbb{K}}^{\times}$, different from the roots of unity, such that $M(\beta) \leq M(\omega)$.*

Proof. The element ω is not a root of unity. Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and let $\xi \in \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ correspond to complex conjugation with respect to η. By the result of Kronecker, there exists a Galois conjugate γ of ω such that $\beta = \gamma \cdot \xi(\gamma) > 1$. Moreover, $h(\beta) \leq 2h(\omega)$. Since $\beta \in \mathbb{R}$ and $\mathbb{K}$ is not totally real, $[\mathbb{K} : \mathbb{Q}(\beta)] \geq 2$. Thus $[\mathbb{Q}(\beta) : \mathbb{Q}]h(\beta) \leq 2[\mathbb{Q}(\beta) : \mathbb{Q}]h(\omega) \leq [\mathbb{Q}(\omega) : \mathbb{Q}]h(\omega)$. ∎

Lemma 2 (Galois extensions of $\mathbb{Q}$ of degree $2p$). *Let $p \in \mathbb{N}$ be a prime. Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension of degree $2p$. If $\omega \in \mathcal{O}_{\mathbb{K}}^{\times}$ is not a root of 1 then $M(x^3 - x - 1) \leq M(\omega)$.*

Proof. If $p = 2$ then $\mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ is abelian. By Lemma 1 and the result of Schinzel, we can assume that $d \equiv [\mathbb{Q}(\omega) : \mathbb{Q}] \in \{1, 2, p\}$. If $d = 1$ then $\omega \in \mathbb{Z}$

and $M(\omega) \geq 2$. If $d = 2$, then ω is an abelian algebraic integer different from the roots of unity. If $d = p$ and $p \neq 2$, then the result of Smyth yields the assertion. ∎

PROPOSITION 1 (Dihedral Galois groups not divisible by 4). *Let $m \in \mathbb{N}$ be odd and $m \geq 3$. Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension with $\mathrm{G} \equiv \mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle \rtimes_\varrho \langle\tau\rangle \approx \mathrm{D}_{2m}$. If $\omega \in \mathcal{O}_\mathbb{K}^\times$ is not a root of 1, then $M(x^3-x-1) \leq M(\omega)$.*

Proof. By the result of Schinzel, we assume that $\mathbb{K}$ is not totally real. The proof will be by induction on the number of prime factors of $2m$, counting multiplicity. By Lemma 2, if m is a prime, $M(x^3-x-1) \leq M(\omega)$. Let $n \in \mathbb{N}$ be the number of prime factors of $2m$, counting multiplicity. Assume that for all $l \in \mathbb{N}, l \geq 3$ such that $2l$ has fewer than n prime factors, counting multiplicity, if $\mathbb{F}/\mathbb{Q}$ is a Galois extension such that $\mathrm{Aut}(\mathbb{F}/\mathbb{Q}) \approx \mathrm{D}_{2l} \approx \langle\beta\rangle \rtimes_\phi \langle\eta\rangle$ and $\gamma \in \mathcal{O}_\mathbb{F}^\times$ is not a root of 1, then $M(x^3 - x - 1) \leq M(\gamma)$. By Lemma 1, we can assume that ω is not a primitive element. If $[\mathbb{Q}(\omega) : \mathbb{Q}]$ is odd then, by the result of Smyth, $M(x^3 - x - 1) \leq M(\omega)$. If $[\mathbb{Q}(\omega) : \mathbb{Q}]$ is even, then $\mathrm{H}_{\mathbb{Q}(\omega)}$ contains a nontrivial subgroup of $\langle\sigma\rangle$. Consequently, by the Fundamental Theorem of Galois Theory, either $\omega \in \mathcal{O}_\mathbb{V}$ where $\mathbb{V}$ is a dihedral Galois extension of $\mathbb{Q}$ of order containing fewer than n prime factors (counting multiplicity) or ω is abelian. Hence, by the induction hypothesis, $M(x^3 - x - 1) \leq M(\omega)$. ∎

The polynomial $x^3 - x - 1$. Let $\mathbb{K}$ be the splitting field of the polynomial $f(x) = x^3 - x - 1$. Then $\mathbb{K}/\mathbb{Q}$ is a Galois extension and $[\mathbb{K} : \mathbb{Q}] \in \{3, 6\}$. The discriminant of f is -23, $(-23)^{1/2} \in \mathbb{K}$, and $[\mathbb{Q}(-23)^{1/2} : \mathbb{Q}] = 2$. Hence, $2 \,|\, [\mathbb{K} : \mathbb{Q}]$ and thus $[\mathbb{K} : \mathbb{Q}] = 6$. Consequently, $\mathrm{Aut}\big(\mathbb{K}/\mathbb{Q}\big) \approx S_3 \approx \mathbb{Z}/(3\mathbb{Z}) \rtimes_\varrho \mathbb{Z}/2\mathbb{Z}$. We thus know, by Proposition 1, that amongst all polynomials in $\mathbb{Z}[x]$ whose splitting fields are contained in dihedral Galois extensions of $\mathbb{Q}$ of degree not divisible by 4, $x^3 - x - 1$ has the smallest Mahler measure (other than 1).

4. Subgroups of dihedral groups. By Section 3, we restrict to consideration of dihedral Galois groups of orders divisible by 4. The subgroups of such groups will be used in the proof of Theorem 1 and the purpose of this section is to identify relevant properties of these subgroups. If $m \in \mathbb{N}$, $m \geq 2$ and $\mathbb{K}/\mathbb{Q}$ is a Galois extension such that $\mathrm{G} = \mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle \rtimes_\varrho \langle\tau\rangle \approx \mathrm{D}_{2\cdot 2m}$, then the distinct elements of G are $1, \sigma, \sigma^2, \ldots, \sigma^{2m-1}, \tau, \sigma\tau, \ldots, \sigma^{2m-1}\tau$. It follows that if $\mathrm{H} \leq \mathrm{G}$ and $|\mathrm{H}| \geq 3$ then $\mathrm{H} \cap \langle\sigma\rangle \neq \{1\}$. The elements of G of order 2 are σ^m and $\sigma^i\tau$ for $i \in \{0, \ldots, 2m-1\}$, and the center of G is $\langle\sigma^m\rangle$. If $\mathrm{H} \trianglelefteq \langle\sigma\rangle$, then H is characteristic in $\langle\sigma\rangle \trianglelefteq \mathrm{G}$ so that $\mathrm{H} \triangleleft \mathrm{G}$. For $i \in \{0, \ldots, 2m-1\}$, $\mathrm{N_G}(\langle\sigma^i\tau\rangle) = \langle\sigma^m, \sigma^i\tau\rangle$ and $[\mathrm{N_G}(\langle\sigma^i\tau\rangle) : \langle\sigma^i\tau\rangle] = 2$. The cyclic subgroups of G are the subgroups of $\langle\sigma\rangle$ and $\langle\sigma^i\tau\rangle$ for $i \in \{0, \ldots, 2m-1\}$. If $\mathrm{H} < \mathrm{G}$ is such that there exist $i \in \{0, \ldots, 2m-1\}$

and $\sigma^i\tau \in \mathrm{H}$, then $[\mathrm{N_G(H)} : \mathrm{H}] = 2$ so that either $[\mathrm{G} : \mathrm{H}] = 2$ or $\mathrm{H} \not\trianglelefteq \mathrm{G}$. As a result, if $\mathrm{G}_0 \not\subseteq \langle\sigma\rangle$, then $f \leq 2$, and if $f \geq 3$, then $\mathrm{G}_0 \trianglelefteq \langle\sigma\rangle$ and $ef \leq 2m$.

Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and let $\xi \in \mathrm{G}$ correspond to complex conjugation with respect to η. By Section 3, assume $\xi \notin \mathrm{C(G)}$. If $\alpha \in \mathcal{O}_{\mathbb{K}}$ is reciprocal such that $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$, we can assume, by Lemma 1, the above remarks, and the Fundamental Theorem of Galois Theory, that there exists $i \in \{0, \ldots, 2m-1\}$ such that $\mathrm{H}_{\mathbb{Q}(\alpha)} = \langle\sigma^i\tau\rangle$. Consequently, $\mathrm{N_G}(\mathrm{H}_{\mathbb{Q}(\alpha)}) = \langle \mathrm{H}_{\mathbb{Q}(\alpha)}, \sigma^m\rangle$ and $[\mathrm{N_G}(\mathrm{H}_{\mathbb{Q}(\alpha)}) : \mathrm{H}_{\mathbb{Q}(\alpha)}] = 2$. It then follows from the Fundamental Theorem of Galois Theory that $\sigma^m(\alpha) = 1/\alpha$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2m$, and that the only Galois conjugates of α in $\mathbb{Q}(\alpha)$ are α and $1/\alpha$. Since $\xi \notin \mathrm{C(G)}$, we can deduce, using Galois theory and the above remarks, that α can have at most two Galois conjugates on the Archimedean unit circle. Suppose there exists $j \in \mathbb{N}$ such that $\mathbb{Q}(\alpha^{2^{j-1}}) = \mathbb{Q}(\alpha)$ but $\mathbb{Q}(\alpha^{2^j}) \subsetneq \mathbb{Q}(\alpha)$. Then $-\alpha^{2^{j-1}}$ is a Galois conjugate of $\alpha^{2^{j-1}}$ and $\mathrm{H}_{\mathbb{Q}(\alpha^{2^{j-1}})} = \mathrm{H}_{\mathbb{Q}(\alpha)}$. Since $\alpha^{2^{j-1}}$ and $1/\alpha^{2^{j-1}}$ are the only Galois conjugates of $\alpha^{2^{j-1}}$ in $\mathbb{Q}(\alpha^{2^{j-1}})$, we have a contradiction. Consequently, for a Galois conjugate γ of α ($\gamma \neq \alpha$) and for all $j \in \mathbb{N}$, $\gamma^{2^j} \neq \alpha^{2^j}$.

5. Dedekind's theory and Mahler measure. Propositions 2 and 3 below allow for the use of Dedekind's theory in the analysis of the Mahler measure of algebraic integers. In Proposition 2, we will use the fact that if $\mathbb{K}$ is an algebraic number field and $\alpha \in \mathcal{O}_{\mathbb{K}}^{\times}$, then, for all non-Archimedean places v, $|\alpha|_v \leq 1$ and $h(\alpha) = \sum_{v|\infty} \log^+ |\alpha|_v$. We recall the useful fact that if $\mathfrak{D}_1, \ldots, \mathfrak{D}_t$ are distinct prime ideals of $\mathcal{O}_{\mathbb{K}}$ then $\mathfrak{D}_1 \cdots \mathfrak{D}_t = \mathfrak{D}_1 \cap \cdots \cap \mathfrak{D}_t$.

PROPOSITION 2. *Let $m, n \in \mathbb{N}$. Let $\omega \in \overline{\mathbb{Q}}^{\times}$ be an algebraic integer and let $\omega_1, \ldots, \omega_n$ be n distinct Galois conjugates of ω. For each $k \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$ let $c_k \in \mathbb{Z} - \{0\}$ and let $b_{j,k} \in \mathbb{N} \cup \{0\}$ be such that $\sum_{j=1}^{n} \sum_{k=1}^{m} b_{j,k} \geq 1$. Define*

$$\delta \equiv \sum_{k=1}^{m} c_k \prod_{j=1}^{n} \omega_j^{b_{j,k}}, \qquad M_j \equiv \max\{b_{j,k} \mid 1 \leq k \leq m\},$$

$$M \equiv \sum_{j=1}^{n} M_j, \quad s \equiv \prod_{v \nmid \infty} |\delta|_v, \quad L \equiv \sum_{k=1}^{m} |c_k|.$$

For each place $v \mid \infty$, let $a_v \in \mathbb{R}$ be defined via

$$\|\delta\|_v = a_v \prod_{j=1}^{n} \max\{1, \|\omega_j^{M_j}\|_v\}$$

and let

$$A \equiv \prod_{v|\infty} a_v^{d_v/d}. \tag{1}$$

If $\delta \neq 0$, then

$$sA \leq 1, \quad A \leq L \quad \textit{and} \quad Mh(\omega) = \log(1/sA).$$

Proof. By the triangle inequality, we have $a_v \leq L$ for all $v \mid \infty$, so that $A \leq L$.

By the product formula, $\sum_v \log|\delta|_v = 0$. Since $\sum_{v\nmid\infty} \log|\delta|_v = \log s$, we have $\sum_{v\mid\infty} \log|\delta|_v = -\log s$. At this point, we remember that $\|\cdot\|^{d_v/d} = |\cdot|_v$. Fix $v \mid \infty$. Then $\|\delta\|_v = |\delta|^{d/d_v} = a_v \prod_{j=1}^n \max\{1, \|\omega_j\|_v^{M_j}\}$. Consequently,

$$\log|\delta|_v = (d_v/d)\Big(\log a_v + \sum_{j=1}^n M_j \log^+ \|\omega_j\|_v\Big).$$

Summing over all the Archimedean places, we obtain

$$\sum_{v\mid\infty} \log|\delta|_v = \sum_{v\mid\infty} \log a_v^{d_v/d} + \sum_{v\mid\infty}\sum_{j=1}^n M_j \log^+ |\omega_j|_v.$$

Using the Galois action on places gives

$$\log(1/s) = \log A + M \sum_{v\mid\infty} \log^+ |\omega_j|_v.$$

Since $h(\omega_i) = h(\omega_j)$ for all $i, j \in \{1, \dots, n\}$, we obtain $\log(1/sA) = Mh(\omega)$. ∎

Proposition 3. *Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension. Let $\omega \in \mathcal{O}_\mathbb{K}^\times$. Let $p \in \mathbb{N}$ be prime. Let $\mathfrak{D}_1, \dots, \mathfrak{D}_t$ be the distinct prime ideal divisors of $p\mathcal{O}_\mathbb{K}$. Let e be the common ramification index of the $\mathfrak{D}_i$. Let $a_1, \dots, a_t \in \mathbb{N} \cup \{0\}$. If $\omega \in \prod_{i=1}^t \mathfrak{D}_i^{a_i}$, then*

$$\sum_{v\mid p} \log|\omega|_v \leq (-\log p) \cdot \left(\frac{1}{et}\right) \cdot \Big(\sum_{i=1}^t a_i\Big).$$

Proof. There exists a one-to-one correspondence between the prime ideal divisors of $p\mathcal{O}_\mathbb{K}$ and the places of $\mathbb{K}$ extending the unique place of $\mathbb{Q}$ containing the usual p-adic absolute value. We have $p\mathcal{O}_\mathbb{K} = \mathfrak{D}_1^e \cdots \mathfrak{D}_t^e$. For $i \in \{1, \dots, t\}$ let $v_{\mathfrak{D}_i}$ be the exponential valuation associated to $\mathfrak{D}_i$. Then $v_{\mathfrak{D}_i}(p) = e$. Let v_i denote the place of $\mathbb{K}$ defined by $\phi \in v_i$ if and only if there exists $\varrho \in (0,1)$ such that for all $\gamma \in \mathbb{K}^\times$, $\phi(\gamma) = \varrho^{v_{\mathfrak{D}_i}(\gamma)}$. Let $\|\cdot\|_{v_i}$ be the unique absolute value in v_i such that $\|p\|_{v_i} = 1/p$. The ϱ associated to $\|\cdot\|_{v_i}$ is $1/\sqrt[e]{p}$. The local degrees are all equal and their sum is $[\mathbb{K}:\mathbb{Q}]$. Consequently, each local degree is $[\mathbb{K}:\mathbb{Q}]/t$ and the ϱ associated to $|\cdot|_{v_i}$ is $1/\sqrt[et]{p}$. Let $\pi_i \in \mathfrak{D}_i$ be such that $|\pi_i|_{v_i}$ is a generator of the valuation group of $|\cdot|_{v_i}$. Then $v_{\mathfrak{D}_i}(\pi_i) = 1$ and $|\pi_i|_{v_i} = 1/\sqrt[et]{p}$. For all $i \in \{1, \dots, t\}$ we have $|\omega|_{v_i} \leq |\pi_i|_{v_i}^{a_i}$. As a result, $\prod_{v\mid p} |\omega|_v \leq \prod_{i=1}^t (1/\sqrt[et]{p})^{a_i}$. ∎

LEMMA 3. *Let $\|\cdot\|_\infty$ be the usual Archimedean absolute value on $\mathbb{C}$. Let $z = re^{i\theta} \in \mathbb{C}$ be such that $\theta \in [-\pi/3, \pi/3]$. Then $\|z-1\|_\infty \le \max\{1, \|z\|_\infty\}$.*

Proof. If $\|z\|_\infty \le 1$ the conclusion is trivial. Assume $\|z\|_\infty > 1$. We have $re^{i\theta} = r\cos\theta + ir\sin\theta$, $\operatorname{Re} z > 0.5$ and $|\operatorname{Re}(z-1)| < |\operatorname{Re} z|$. As $\operatorname{Im}(z-1) = \operatorname{Im} z$,

$$\|z-1\|_\infty^2 = (\operatorname{Re}(z-1))^2 + (\operatorname{Im} z)^2 \le (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2 = \|z\|_\infty^2. \ \blacksquare$$

LEMMA 4. *Let $\|\cdot\|_\infty$ be the usual Archimedean absolute value on $\mathbb{C}$. Let $z = re^{i\theta}$ be such that $\theta \in [\pi/2, 3\pi/2]$. Then*

$$\|z-1\|_\infty \le \sqrt{2}\cdot\sqrt{1-\cos\theta}\cdot\max\{1, \|z\|_\infty\}. \tag{2}$$

Proof. If $\|z\|_\infty \le 1$, the conclusion is trivial. Assume $\|z\|_\infty > 1$. Let $a = \tan\theta$. Then $\cos\theta = -1/\sqrt{a^2+1}$. We have $z = \operatorname{Re} z + i(a\operatorname{Re} z)$ and $\|z\|_\infty^2 = (a^2+1)(\operatorname{Re} z)^2$. Inequality (2) is equivalent to

$$0 \le (a^2+1)(2+\sqrt{a^2+1})(\operatorname{Re} z)^2 + 2\sqrt{a^2+1}\cdot\operatorname{Re} z - \sqrt{a^2+1}.$$

Let $A = (a^2+1)(\sqrt{a^2+1}+2)$, $B = 2\sqrt{a^2+1}$, $C = -\sqrt{a^2+1}$, and $f(x) = Ax^2 + Bx + C$. Then $f(-1/\sqrt{a^2+1}) = 0$, $f(0) < 0$ and $f(1) \ge 0$. By the Intermediate Value Theorem it follows that if $\operatorname{Re} z \le -1/\sqrt{a^2+1} = \cos\theta$, then

$$\|z-1\|_\infty \le \sqrt{2 + \frac{2}{\sqrt{a^2+1}}}\cdot\|z\|_\infty.$$

Since $\|z\|_\infty \ge 1$, $\operatorname{Re} z \le -1/\sqrt{a^2+1}$ and we have inequality (2). $\blacksquare$

LEMMA 5. *Let $\|\cdot\|_\infty$ be the usual Archimedean absolute value on $\mathbb{C}$. Let $z = re^{i\theta}$ be such that $\theta \in [\pi/3, \pi/2] \cup [-\pi/2, -\pi/3]$. Then inequality* (2) *holds.*

Proof. If $\|z\|_\infty \le 1$ the conclusion is trivial. Assume $\|z\|_\infty \ge 1$. Let $a = \tan\theta$. Then $\cos\theta = 1/\sqrt{a^2+1}$. We have $z = \operatorname{Re} z + i(a\operatorname{Re} z)$, $\|z\|_\infty^2 = (a^2+1)(\operatorname{Re} z)^2$, and $\|z-1\|_\infty^2 = (a^2+1)(\operatorname{Re} z)^2 - 2\operatorname{Re} z + 1$. Inequality (2) is thus equivalent to

$$0 \le (a^2+1)(\sqrt{a^2+1}-2)(\operatorname{Re} z)^2 + 2\sqrt{a^2+1}\cdot\operatorname{Re} z - \sqrt{a^2+1}.$$

Let $A = (a^2+1)(\sqrt{a^2+1}-2)$, $B = 2\sqrt{a^2+1}$, $C = -\sqrt{a^2+1}$, and $f(x) = Ax^2 + Bx + C$. Then $f(1/\sqrt{a^2+1}) = f(\cos\theta) = 0$. Since $\theta \in [\pi/3, \pi/2] \cup [-\pi/2, -\pi/3]$, we have $a^2 \ge 3$ and therefore $A \ge 0$. Since $B > 0$, for $\operatorname{Re} z \ge \cos\theta = 1/\sqrt{a^2+1}$, $f(\operatorname{Re} z) \ge 0$. $\blacksquare$

Lemmas 3, 4, and 5 each have symmetric versions where $z+1$ is considered as opposed to $z-1$. These symmetric versions have the same proofs and will be used in Propositions 9 and 10.

6. $[\mathbb{Q}(\alpha):\mathbb{Q}] \geq 10$

PROPOSITION 4. *Let $m \in \mathbb{N}$, $m \geq 2$. Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension such that $\mathrm{G} \equiv \mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle \rtimes_{\varrho} \langle\tau\rangle \approx \mathrm{D}_{2\cdot 2m}$. Let $\alpha \in \mathcal{O}_{\mathbb{K}}$ be reciprocal such that $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$. If 2 does not ramify in $\mathbb{K}$, then $h(\alpha) \geq \frac{1}{24}\log 2$. If 2 does not ramify in $\mathbb{K}$ and $f \leq 2$, then $h(\alpha) \geq \frac{1}{6}\log 2$.*

Proof. If $f \leq 2$, then $\alpha - \alpha^4 \in 2\mathcal{O}_{\mathbb{K}}$. Since α is a unit, $1-\alpha^3 \in 2\mathcal{O}_{\mathbb{K}}$. By the difference of squares formula, $1-\alpha^6 \in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{6}\log 2$. If $f \geq 3$ then $\Phi_{\mathfrak{B}_1} \in \langle\sigma\rangle$ and $[\mathrm{G} : \mathrm{C}_{\mathrm{G}}(\Phi_{\mathfrak{B}_1})] \leq 2$. Since G acts transitively by conjugation on the set of Frobenius automorphisms of the $\mathfrak{B}_i$, we may suppose that $\Phi_{\mathfrak{B}_1} = \cdots = \Phi_{\mathfrak{B}_{t/2}}$. As a result, $\Phi_{\mathfrak{B}_1}(\alpha) - \alpha^2 \in \mathfrak{B}_1 \cdots \mathfrak{B}_{t/2}$. Since α is not a root of unity and by the difference of squares formula, $0 \neq \Phi_{\mathfrak{B}_1}(\alpha^4) - \alpha^8 \in \mathfrak{B}_1^3 \cdots \mathfrak{B}_{t/2}^3$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{24}\log 2$. ∎

PROPOSITION 5. *Let $m \in \mathbb{N}$, $m \geq 2$. Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension such that $\mathrm{G} \equiv \mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle \rtimes_{\varrho} \langle\tau\rangle \approx \mathrm{D}_{2\cdot 2m}$. Let $\alpha \in \mathcal{O}_{\mathbb{K}}$ be reciprocal such that $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$. If 2 ramifies in $\mathbb{K}$ and $e = 2$, then $h(\alpha) \geq \frac{1}{12}\log 2$.*

Proof. Suppose that there exists $i \in \{0,\ldots,2m-1\}$ such that $\mathrm{G}_0 = \langle\sigma^i\tau\rangle$. By Section 3, $f = 1$ or $f = 2$ and $\alpha - \alpha^4 \in \mathfrak{B}_1 \cdots \mathfrak{B}_t$. Since α is a unit, $1-\alpha^3 \in \mathfrak{B}_1 \cdots \mathfrak{B}_t$. By the difference of squares formula, $1-\alpha^{12} \in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{12}\log 2$.

If $e = 2$ and there does not exist $i \in \{0,\ldots,2m-1\}$ such that $\mathrm{G}_0 = \langle\sigma^i\tau\rangle$, then $\mathrm{G}_0 = \mathrm{G}_1 = \langle\sigma^m\rangle$. Since G acts transitively by conjugation on the inertia groups of the $\mathfrak{B}_i$ and $\sigma^m \in \mathrm{C}(\mathrm{G})$, we have $\alpha - \sigma^m(\alpha) \in \mathfrak{B}_1^2 \cdots \mathfrak{B}_t^2 = 2\mathcal{O}_{\mathbb{K}}$. By Section 3 and the difference of squares formula, $0 \neq \alpha^2 - \sigma^m(\alpha^2) \in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{4}\log 2$. ∎

PROPOSITION 6. *Let $\mathbb{K}/\mathbb{Q}$ be a finite Galois extension. Let $\mathrm{G} = \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$. Let $\gamma \in \mathrm{G}$ be such that $\gamma \neq 1$ and $\langle\gamma\rangle \trianglelefteq \mathrm{G}$. Let $\mathfrak{B}$ be a prime ideal divisor of $2\mathcal{O}_{\mathbb{K}}$. Suppose that 2 ramifies in $\mathbb{K}$ and let e be the ramification index of $\mathfrak{B}$. Suppose that $\langle\gamma\rangle$ is in the nth ramification group of $\mathfrak{B}$. Let $r \in \mathbb{N} \cup \{0\}$ be minimal such that $(n+1)\cdot 2^r \geq e$. Let $\alpha \in \mathcal{O}_{\mathbb{K}}$ be such that $0 \neq \gamma(\alpha^{2^{r+1}}) - \alpha^{2^{r+1}}$. Then $h(\alpha) \geq \frac{1}{2^{r+2}}\log 2$.*

Proof. Since G acts transitively by conjugation on the ramification groups of the $\mathfrak{B}_i$, $\langle\gamma\rangle$ is in the nth ramification group of each of the $\mathfrak{B}_i$. Consequently, $\gamma(\alpha) - \alpha \in \mathfrak{B}_1^{n+1} \cdots \mathfrak{B}_t^{n+1}$. By the difference of squares formula, $0 \neq \gamma(\alpha^{2^{r+1}}) - \alpha^{2^{r+1}} \in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{2^{r+2}}\log 2$. ∎

PROPOSITION 7. *Let $m \in \mathbb{N}$, $m \geq 5$. Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension such that $\mathrm{G} \equiv \mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle \rtimes_{\varrho} \langle\tau\rangle \approx \mathrm{D}_{2\cdot 2m}$. Let $\alpha \in \mathcal{O}_{\mathbb{K}}$ be reciprocal such*

that $\mathbb{K}$ *is the Galois closure of* $\mathbb{Q}(\alpha)$*. If* 2 *ramifies in* $\mathbb{K}$ *with ramification index greater than* 2*, then*

$$M(\alpha) \geq M(x^3 - x - 1). \tag{3}$$

Proof. Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and recall the last paragraph of Section 4.

Case 1: $e \leq [\mathbb{Q}(\alpha) : \mathbb{Q}]/4$. By considering the distinct elements of G, there exists $i \in \{1, \ldots, 2m-1\}$ such that $\sigma^i \in \mathrm{G}_0$. Let $r \in \mathbb{N}$ be smallest such that $2^r \geq e$. Then $2^r < 2e \leq [\mathbb{Q}(\alpha) : \mathbb{Q}]/2$. As a result, $2^{r+2} \leq 2[\mathbb{Q}(\alpha) : \mathbb{Q}]$. By Proposition 6, $h(\alpha) \geq \frac{1}{2^{r+2}} \log 2$, and (3) follows.

Case 2: $3e = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is even, it follows that $2 \,|\, e$. Suppose that $\sigma^m \in \mathrm{G}_1$ and let $r \in \mathbb{N}$ be smallest such that $2^r \geq e$. Then $2^{r+1} < 4e = (4/3) \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Since $\sigma^m(\alpha) = 1/\alpha$ and α is a unit, it follows that $\alpha^2 - 1 \in \mathfrak{B}_1^2 \cdots \mathfrak{B}_t^2$. By the difference of squares formula and since α is not a root of unity, $0 \neq \alpha^{2^{r+1}} - 1 \in \mathfrak{B}_1^{2e} \cdots \mathfrak{B}_t^{2e}$. By Propositions 2 and 3 and since $2^{r+1} < (4/3)[\mathbb{Q}(\alpha) : \mathbb{Q}]$, we have $h(\alpha) \geq 3 \log 2/(4[\mathbb{Q}(\alpha) : \mathbb{Q}])$, and (3) follows again.

Suppose that $\sigma^m \notin \mathrm{G}_1$. Then, from Section 3, $e = 6$ and so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 18$. Since $e = 6$, there exists $j \in \{1, \ldots, 2m-1\}$ such that $\sigma^j \in \mathrm{G}_0$. It follows that $0 \neq \alpha - \sigma^j(\alpha) \in \mathfrak{B}_1 \cdots \mathfrak{B}_t$. From the difference of squares formula and Section 3, $0 \neq \alpha^{16} - \sigma^j(\alpha^{16}) \in \mathfrak{B}_1^{2e} \cdots \mathfrak{B}_t^{2e}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{32} \log 2$, and (3) follows.

Case 3: $2e = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Let $r \in \mathbb{N}$ be minimal such that $2^r \geq e$. Then $2^{r+1} < 4e$. If σ^m acts as the Frobenius automorphism on the $\mathfrak{B}_i$, then $e = 6$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 12$. As a result, $\sigma^4(\alpha) - \alpha \in \mathfrak{B}_1 \cdots \mathfrak{B}_t$. By the difference of squares formula, $\sigma^4(\alpha^{16}) - \alpha^{16} \in \mathfrak{B}_1^{14} \cdots \mathfrak{B}_t^{14}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{24} \log 2$, which yields (3).

If $\sigma^m \in \mathrm{G}_1$ then $\alpha - \sigma^m(\alpha) = \alpha - 1/\alpha \in \mathfrak{B}_1^2 \cdots \mathfrak{B}_t^2$. Since α is an integer, $\alpha^2 - 1 \in \mathfrak{B}_1^2 \cdots \mathfrak{B}_t^2$. By the difference of squares formula, $\alpha^{2^{r+1}} - 1 \in 4\mathcal{O}_{\mathbb{K}}$. If $f = 1$, then $\alpha^2 - \alpha \in \mathfrak{B}_1 \cdots \mathfrak{B}_t$. Since α is a unit, $\alpha - 1 \in \mathfrak{B}_1 \cdots \mathfrak{B}_t$. By the difference of squares formula, $\alpha^{2^{r+1}} - 1 \in 4\mathcal{O}_{\mathbb{K}}$. In either case, (3) follows from Propositions 2 and 3. Since $|\mathrm{G}_0/\mathrm{G}_1|$ divides $2^f - 1$, we are thus left with $f = 2$ and $e = 3$, which implies that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6 < 10$.

Case 4: $e = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Then $f \in \{1, 2\}$. Let $r \in \mathbb{N}$ be minimal such that $2^r \geq 2e$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 10$ and is even, if $f = 1$, then G is a 2-group, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 16$ and $\alpha - \alpha^2 \in \mathfrak{B}_1 \cdots \mathfrak{B}_t$. Since α is a unit, $1 - \alpha \in \mathfrak{B}_1 \cdots \mathfrak{B}_t$. By the difference of squares formula, $1 - \alpha^{2[\mathbb{Q}(\alpha):\mathbb{Q}]} \in \mathfrak{B}_1^{2e} \cdots \mathfrak{B}_t^{2e}$. From Propositions 2 and 3, $h(\alpha) \geq \log 2/(2[\mathbb{Q}(\alpha) : \mathbb{Q}])$, proving (3).

If $f = 2$ then the only odd prime power possibly dividing e is 3, and $t = 1$. If $f = 2$ and $3 \nmid e$ then G is a 2-group, $e \geq 16$, $\sigma^m \in \mathrm{G}_3$ and

$\alpha - \sigma^m(\alpha) = \alpha - 1/\alpha \in \mathfrak{B}_1^4$. Since α is an integer, $\alpha^2 - 1 \in \mathfrak{B}_1^4$. By the difference of squares formula, $\alpha^{[\mathbb{Q}(\alpha):\mathbb{Q}]} - 1 \in \mathfrak{B}_1^{2e}$. By Propositions 2 and 3, $h(\alpha) \geq \log 2/[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and (3) holds.

If $f = 2$ and $3 \,|\, e$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 12$ and there exists $s \in \mathbb{N}$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s \cdot 3$. In this case, $\sigma^m \in \mathrm{G}_1$ and $\alpha - \sigma^m(\alpha) = \alpha - 1/\alpha \in \mathfrak{B}_1^2$. Since α is a unit, $\alpha^2 - 1 \in \mathfrak{B}_1^2$. Suppose that $e = 12$. By the difference of squares formula, $\alpha^{32} - 1 \in \mathfrak{B}_1^{28}$. By Propositions 2 and 3 we deduce $h(\alpha) \geq \frac{1}{24} \log 2$ and so (3) holds.

If $e \geq 24$ then $\sigma^m \in \mathfrak{B}_1^3$ and $\alpha - \sigma^m(\alpha) = \alpha - 1/\alpha \in \mathfrak{B}_1^3$. Since α is an integer, $\alpha^2 - 1 = (\alpha + 1)(\alpha - 1) \in \mathfrak{B}_1^3$. Since $\mathfrak{B}_1$ is a prime ideal divisor of $2\mathcal{O}_{\mathbb{K}}$, we can assume that $\alpha + 1 \in \mathfrak{B}_1^2$. By the difference of squares formula, $\alpha^{2^{s+1}} - 1 \in \mathfrak{B}_1^{2^{s+2}}$ and $\alpha^{2^{s+2}} - 1 \in \mathfrak{B}_1^{2e}$. Since $2^{s+2} = 4[\mathbb{Q}(\alpha) : \mathbb{Q}]/3$ it follows from Propositions 2 and 3 that $h(\alpha) \geq 3 \log 2/(4[\mathbb{Q}(\alpha) : \mathbb{Q}])$, and we obtain (3).

Case 5: $e = 2[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Then $f = 1$, $t = 1$, G is a 2-group, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 16$. Consequently, $\sigma^m \in \mathrm{G}_3$ and $\alpha - \sigma^m(\alpha) = \alpha - 1/\alpha \in \mathfrak{B}_1^4$. Since α is an integer, $\alpha^2 - 1 \in \mathfrak{B}_1^4$. By the difference of squares formula, $\alpha^{2[\mathbb{Q}(\alpha):\mathbb{Q}]} - 1 \in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha) \geq \log 2/(2[\mathbb{Q}(\alpha) : \mathbb{Q}])$, and (3) follows. ∎

7. $[\mathbb{Q}(\alpha) : \mathbb{Q}] \in \{4, 6, 8\}$

Proposition 8 ($[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$). *Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension such that $\mathrm{G} \equiv \mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle \rtimes_{\varrho} \langle\tau\rangle \approx \mathrm{D}_{2\cdot 4}$. Let $\alpha \in \mathcal{O}_{\mathbb{K}}$ be reciprocal such that $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$. Then inequality* (3) *holds.*

Proof. The element α is not a root of unity. Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and let $\xi \in \mathrm{G}$ correspond to complex conjugation with respect to η. By the result of Schinzel, we suppose that $\mathbb{K}$ is not totally real and, by Section 4, that $\xi \notin \mathrm{C}(\mathrm{G})$. Suppose that α does not have a real Galois conjugate. By the theorem of Kronecker, we can assume that α has a Galois conjugate γ such that $\beta = \gamma \cdot \xi(\gamma) > 1$. Recall the last paragraph of Section 3. Since $\sigma^2(\beta) = 1/\beta$, $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. We can deduce that $M(\alpha) = M(\beta)$. It follows that we may assume α to be real and positive. In this case, $M(\alpha) = \alpha$.

Case 1: 2 *does not ramify in* $\mathbb{K}$. By Proposition 4, we assume that $f = 4$. Thus, $2\mathcal{O}_{\mathbb{K}} = \mathfrak{B}_1\mathfrak{B}_2$ and $\Phi^2_{\mathfrak{B}_1} = \Phi^2_{\mathfrak{B}_2} = \sigma^2$. As a result, $\sigma^2(\alpha) - \alpha^4 = 1/\alpha - \alpha^4 \in 2\mathcal{O}_{\mathbb{K}}$. Since α is an integer, $1 - \alpha^5 \in 2\mathcal{O}_{\mathbb{K}}$. By the difference of squares formula, $1 - \alpha^{10} \in 4\mathcal{O}_{\mathbb{K}}$. Let $\delta \equiv 1 - \alpha^{10}$ and let A be as defined in (1). By Lemma 3, $A \leq \sqrt{2}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{10} \log(4/\sqrt{2})$, and (3) holds.

Case 2: 2 *ramifies in* $\mathbb{K}$. If $e = 2$ and $\sigma^2 \in \mathrm{G}_1$ then $\alpha - \sigma^2(\alpha) = \alpha - 1/\alpha \in 2\mathcal{O}_{\mathbb{K}}$. Since α is an integer, $\alpha^2 - 1 \in 2\mathcal{O}_{\mathbb{K}}$. By the difference of

squares formula, $\alpha^4 - 1 \in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{4}\log 2$, proving (3).

If $e = 2$ and $f \leq 2$, then $\alpha^4 - \alpha \in \mathfrak{B}_1 \cdots \mathfrak{B}_t$. Since α is a unit and the $\mathfrak{B}_i$ are prime, $\alpha^3 - 1 \in \mathfrak{B}_1 \cdots \mathfrak{B}_t$. By the difference of squares formula, $\alpha^{12} - 1 \in 4\mathcal{O}_{\mathbb{K}}$. Let $\delta \equiv \alpha^{12} - 1$ and let A be as defined in (1). By Lemma 3, $A \leq \sqrt{2}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{12}\log(4/\sqrt{2})$, and (3) follows.

If $e = 4$, then $\sigma^2 \in \mathrm{G}_1$ and $\alpha - \sigma^2(\alpha) = \alpha - 1/\alpha \in \mathfrak{B}_1^2 \cdots \mathfrak{B}_t^2$. Since α is an integer, $\alpha^2 - 1 \in \mathfrak{B}_1^2 \cdots \mathfrak{B}_t^2$. By the difference of squares formula, $\alpha^8 - 1 \in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{8}\log 2$, so (3) holds.

If $e = 8$, then $\sigma^2 \in \mathrm{G}_2$ and $\alpha - 1/\alpha \in \mathfrak{B}_1^3$. Since α is an integer, $\alpha^2 - 1 = (\alpha + 1)(\alpha - 1) \in \mathfrak{B}_1^3$. Since $\mathfrak{B}_1$ is a prime ideal divisor of $2\mathcal{O}_{\mathbb{K}}$, $\alpha - 1 \in \mathfrak{B}_1^2$. By the difference of squares formula, $\alpha^8 - 1 \in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{8}\log 2$, proving (3). ∎

Proposition 9 ($[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$). *Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension such that $\mathrm{G} \equiv \mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle \rtimes_{\varrho} \langle\tau\rangle \approx \mathrm{D}_{2\cdot 6}$. Let $\alpha \in \mathcal{O}_{\mathbb{K}}$ be reciprocal such that $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$. Then inequality* (3) *holds.*

Proof. Let $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding and let $\xi \in \mathrm{G}$ correspond to complex conjugation with respect to η. By the result of Schinzel, we can assume that $\mathbb{K}$ is not totally real and, by Section 3, that $\xi \notin \mathrm{C}(\mathrm{G})$. Recall the last paragraph of Section 4.

Case 1: 2 *ramifies in* $\mathbb{K}$. By Proposition 5, we assume $e \geq 3$.

If $e = 4$, then $\sigma^3 \in \mathrm{G}_1$ and, by Proposition 6, $h(\alpha) \geq \frac{1}{8}\log 2$, so (3) holds.

If $e = 3$, then $\sigma^2 \in \mathrm{G}_0$ and $\sigma^2(\alpha) - \alpha \in \mathfrak{B}_1 \cdots \mathfrak{B}_t$. By the difference of squares formula and Section 3, $0 \neq \sigma^2(\alpha^8) - \alpha^8 \in \mathfrak{B}_1^7 \cdots \mathfrak{B}_t^7$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{12}\log 2$, yielding (3).

If $e = 6$ then $f = 2$ and there exists a unique prime ideal divisor $\mathfrak{B}_1$ of $2\mathcal{O}_{\mathbb{K}}$. If $\sigma^3 \in \mathrm{G}_1$, $\alpha - \sigma^3(\alpha) = \alpha - 1/\alpha \in \mathfrak{B}_1^2$. Since α is an integer, $\alpha^2 - 1 \in \mathfrak{B}_1^2$. By the difference of squares formula, $\alpha^{16} - 1 \in \mathfrak{B}_1^{14}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{12}\log 2$, giving (3). If $e = 6$ and $\sigma^3 \notin \mathrm{G}_1$, then $\mathrm{G}_0 \approx \mathrm{D}_{2\cdot 3}$. By Section 3, we can assume that $\tau \in \mathrm{G}_1$ and $\tau \notin \mathrm{H}_{\mathbb{Q}(\alpha)}$. Thus, $0 \neq \alpha - \tau(\alpha) \in \mathfrak{B}_1^2$. By the difference of squares formula and Section 3, $0 \neq \alpha^8 - \tau(\alpha^8) \in \mathfrak{B}_1^{14}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{12}\log 2$, which proves (3).

Case 2: 2 *does not ramify in* $\mathbb{K}$. By Proposition 4, we assume that $f \geq 3$. If $f = 3$ then $\alpha - \alpha^8 \in 2\mathcal{O}_{\mathbb{K}}$. Since α is a unit and the $\mathfrak{B}_i$ are prime ideal divisors of $2\mathcal{O}_{\mathbb{K}}$, $1 \pm \alpha^7 \in 2\mathcal{O}_{\mathbb{K}}$. By the difference of squares formula, $1 - \alpha^{14} \in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha) \geq \frac{1}{14}\log 2$, which proves (3). If $f = 6$, then $2\mathcal{O}_{\mathbb{K}} = \mathfrak{B}_1\mathfrak{B}_2$ and $\Phi^3_{\mathfrak{B}_1} = \Phi^3_{\mathfrak{B}_2} = \sigma^3$. Since α is an integer and

$\sigma^3(\alpha) = 1/\alpha$, and the $\mathfrak{B}_i$ are prime ideal divisors of $2\mathcal{O}_{\mathbb{K}}$, it follows from $\Phi^3_{\mathfrak{B}_1}(\alpha) - \alpha^{2^3} = 1/\alpha - \alpha^8 \in 2\mathcal{O}_{\mathbb{K}}$ that $1 \pm \alpha^9 \in 2\mathcal{O}_{\mathbb{K}}$.

Assume that α is not real and is outside the Archimedean unit circle. Since α is reciprocal of degree 6, α has either two Galois conjugates on the Archimedean unit circle, or two Galois conjugates that are real and none on the Archimedean unit circle.

Case 2(a): *No real Galois conjugates.* Suppose that α has no real Galois conjugates. Let $\gamma \equiv \alpha^9$. By considering $-\gamma, -\overline{\gamma}$, and $\overline{\gamma}$ if necessary, assume that γ is in the first quadrant. By the Fundamental Theorem of Galois Theory, there exists a subfield $\mathbb{F}$ of $\mathbb{Q}(\gamma)$ that is quadratic over $\mathbb{Q}$. Let g_1, g_2, g_3 be a complete set of distinct coset representatives of $\mathrm{H}_{\mathbb{Q}(\gamma)}$ in $\mathrm{H}_{\mathbb{F}}$. Since $h(g_1(\alpha)g_2(\alpha)g_3(\alpha)) \le 3h(\alpha)$, $3[\mathbb{Q}(g_1(\alpha)g_2(\alpha)g_3(\alpha)) : \mathbb{Q}] \le [\mathbb{Q}(\alpha) : \mathbb{Q}]$, 2 does not ramify, and $g_1(\alpha)g_2(\alpha)g_3(\alpha)$ is an abelian integer of degree less than or equal to 2, we assume that $g_1(\gamma)g_2(\gamma)g_3(\gamma) = (g_1(\alpha)g_2(\alpha)g_3(\alpha))^9 = \pm 1$. It then follows that $\gamma_u \equiv \gamma/\overline{\gamma}$ is a Galois conjugate of γ on the Archimedean unit circle. Consequently, the argument of either γ_u or $\overline{\gamma}_u$ is twice that of γ. Let $\delta_1 \equiv \gamma - 1$ and let A_1 be defined as in (1). If γ is in the sector $[0, 17.75\pi/48]$, then, by Lemmas 4 and 5,

$$A_1 \le \sqrt[6]{2 - 2\cos(35.5\pi/48)} \cdot \sqrt[3]{2 - 2\cos(17.75\pi/48)}.$$

By Propositions 2 and 3, $h(\alpha) \ge \frac{1}{9}\log(2/A_1)$, proving (3).

Let $\delta_2 \equiv \gamma + 1$ and let A_2 be defined as in (1). If γ is in the sector $[17.75\pi/48, \pi/2]$, then by the symmetric version of Lemma 4 and since γ_u is on the Archimedean unit circle,

$$A_2 \le \sqrt[6]{2 + 2\cos(35.5\pi/48)} \cdot \sqrt[3]{2 + 2\cos(17.75\pi/48)}.$$

By Propositions 2 and 3, $h(\alpha) \ge \frac{1}{9}\log(2/A_2)$, giving (3). This completes the proof of Case 2(a).

Case 2(b): *Real Galois conjugates.* Suppose now that $\gamma \equiv \alpha^9$ has a real Galois conjugate β. One can assume that $\beta \le 1.33^{9/2}$. Let γ_3 be a Galois conjugate of γ that is not real. By considering $-\gamma_3, -\overline{\gamma}_3$, and $\overline{\gamma}_3$ if necessary, we can assume that γ_3 is in the first quadrant. Let $\delta \equiv \gamma - 1$ and let A be defined as in (1). Suppose γ_3 is in the sector $[0, \pi/3]$. By Lemma 3, $A \le 2^{1/3}$. By Propositions 2 and 3, $h(\alpha) \ge \frac{1}{9}\log(2/A)$, so (3) holds.

Suppose $\beta < 0$ and γ_3 is in the sector $[\pi/3, \pi/2]$. Let $\delta \equiv \gamma + 1$ and let A be defined as in (1). By the symmetric version of Lemma 3, $A \le 3^{1/3}(1 + 1/\beta)^{1/3}$. By Propositions 2 and 3, $h(\alpha) \ge \frac{1}{9}\log(2/A)$, giving (3).

Suppose $\beta > 0$ and γ_3 is in the sector $[\pi/3, \pi/2]$. Let $\delta \equiv \gamma - 1$ and let A be defined as in (1). Then $A \le 2^{1/3}(1 - 1/\beta)^{1/3}$. By Propositions 2 and 3, $h(\alpha) \ge \frac{1}{9}\log(2/A)$, which proves (3). ∎

PROPOSITION 10 ($[\mathbb{Q}(\alpha):\mathbb{Q}]=8$). *Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension such that $\mathrm{G}\equiv\mathrm{Aut}(\mathbb{K}/\mathbb{Q})=\langle\sigma\rangle\rtimes_{\varrho}\langle\tau\rangle\approx\mathrm{D}_{2\cdot 8}$. Let $\alpha\in\mathcal{O}_{\mathbb{K}}$ be reciprocal such that $\mathbb{K}$ is the Galois closure of $\mathbb{Q}(\alpha)$. Then inequality* (3) *holds.*

Proof. Let $\eta:\mathbb{K}\hookrightarrow\mathbb{C}$ be an embedding and let $\xi\in\mathrm{G}$ correspond to complex conjugation with respect to η. By the result of Schinzel, we can assume that $\mathbb{K}$ is not totally real, and by Section 3, that $\xi\notin\mathrm{C}(\mathrm{G})$. Recall the last paragraph of Section 4.

CASE 1: 2 *ramifies in* $\mathbb{K}$. By Proposition 5, we assume $e\geq 4$.

If $e=4$, then $\sigma^4\in\mathrm{G}_1$ and $\alpha-1/\alpha\in\mathfrak{B}_1^2\cdots\mathfrak{B}_t^2$. Since α is an integer, $\alpha^2-1\in\mathfrak{B}_1^2\cdots\mathfrak{B}_t^2$. By the difference of squares formula, $\alpha^8-1\in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha)\geq\frac{1}{8}\log 2$, which gives (3).

If $e=8$, then $\sigma^4\in\mathrm{G}_2$ and $\alpha-1/\alpha\in\mathfrak{B}_1^3\cdots\mathfrak{B}_t^3$. Since α is an integer, $\alpha^2-1=(\alpha+1)(\alpha-1)\in\mathfrak{B}_1^3\cdots\mathfrak{B}_t^3$. Since the $\mathfrak{B}_i$ are prime ideal divisors of $2\mathcal{O}_{\mathbb{K}}$, one and hence both of $\alpha\pm 1$ are in $\mathfrak{B}_1^2\cdots\mathfrak{B}_t^2$. By the difference of squares formula, $\alpha^8-1\in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha)\geq\frac{1}{8}\log 2$, and (3) follows.

If $e=16$, then $\sigma^4\in\mathrm{G}_3$ and $\alpha-\sigma^4(\alpha)=\alpha-1/\alpha\in\mathfrak{B}_1^4\cdots\mathfrak{B}_t^4$. Since α is an integer, $\alpha^2-1\in\mathfrak{B}_1^4\cdots\mathfrak{B}_t^4$. By the difference of squares formula, $\alpha^{16}-1\in 4\mathcal{O}_{\mathbb{K}}$. By Propositions 2 and 3, $h(\alpha)\geq\frac{1}{16}\log 2$, proving (3).

CASE 2: 2 *does not ramify in* $\mathbb{K}$. By Proposition 4, we assume that $f\geq 4$ so that $\Phi_{\mathfrak{B}_1}\in\langle\sigma\rangle$, $[\mathrm{G}:\mathrm{C}_{\mathrm{G}}(\Phi_{\mathfrak{B}_1})]=2$. We may assume $\Phi_{\mathfrak{B}_1}=\cdots=\Phi_{\mathfrak{B}_{t/2}}$. Thus, $\alpha^2-\Phi_{\mathfrak{B}_1}(\alpha)\in\mathfrak{B}_1\cdots\mathfrak{B}_{t/2}$. By the difference of squares formula, $\alpha^8-\Phi_{\mathfrak{B}_1}(\alpha^4)\in\mathfrak{B}_1^3\cdots\mathfrak{B}_{t/2}^3$ and $\alpha^{16}-\Phi_{\mathfrak{B}_1}(\alpha^8)\in\mathfrak{B}_1^4\cdots\mathfrak{B}_{t/2}^4$. Let $\gamma\equiv\alpha^8/\Phi_{\mathfrak{B}_1}(\alpha^4)$. Then, since α is a unit, $\gamma-1\in\mathfrak{B}_1^3\cdots\mathfrak{B}_{t/2}^3$ and $\gamma^2-1\in\mathfrak{B}_1^4\cdots\mathfrak{B}_{t/2}^4$.

It follows from the result of Kronecker that γ is not a root of unity. Since $\sigma^4(\gamma)=1/\gamma$, $[\mathbb{Q}(\alpha):\mathbb{Q}]\geq 8$. Let $\delta_1\equiv\gamma-1$ and $\delta_2\equiv\gamma^2-1$ and let A_1 and A_2 be defined as in (1). Since $[\mathbb{Q}(\alpha):\mathbb{Q}]=8$, by Propositions 2 and 3, $\log M(\alpha)\geq\frac{2}{3}\log(\sqrt{8}/A_1)$ and $\log M(\alpha)\geq\frac{1}{3}\log(4/A_2)$.

Suppose that $[\mathbb{Q}(\gamma):\mathbb{Q}]=8$ and that γ has a real Galois conjugate. Then $A_1\leq 2^{3/4}$ and (3) holds. Suppose that $[\mathbb{Q}(\gamma):\mathbb{Q}]=16$ and that α has a real Galois conjugate; then $\mathbb{K}$ is totally real. Thus, in either case, we can assume that γ has no real Galois conjugates. If $[\mathbb{Q}(\gamma):\mathbb{Q}]=16$ and γ has a Galois conjugate on the Archimedean unit circle then $\xi\in\mathrm{C}(\mathrm{G})$ from Section 3. By Section 3, if $[\mathbb{Q}(\gamma):\mathbb{Q}]=8$, there can exist at most two Galois conjugates of γ on the Archimedean unit circle, in which case there would exist two real Galois conjugates. Consequently, we can assume that γ has no Galois conjugates on the Archimedean unit circle. As a result, the Galois conjugates of γ can be grouped together in sets of four, $\gamma, 1/\gamma, \overline{\gamma}, 1/\overline{\gamma}$.

If half the Galois conjugates of γ lie in the sector $[3\pi/4, 5\pi/4]$ then half the Galois conjugates of γ^2 lie in the sector $[-\pi/2, \pi/2]$. By Lemma 5, $A_2 \le 2^{3/4}$, which implies (3).

We consequently assume that at most $1/4$ of the Galois conjugates of γ lie in the sector $[3\pi/4, 5\pi/4]$. If $1/4$ of the Galois conjugates of γ lie in $[5\pi/6, 7\pi/6]$, then $1/4$ of the Galois conjugates of γ^2 lie in $[-\pi/3, \pi/3]$. By Lemma 3, $A_2 \le 2^{3/4}$, and (3) follows.

If all the Galois conjugates of γ lie in the sector $[-3\pi/4, 3\pi/4]$, it follows from Lemmas 3–5 that $A_1 \le \sqrt{2+\sqrt{2}}$, which yields (3). We consequently assume that $3/4$ of the Galois conjugates of γ are in $[-3\pi/4, 3\pi/4]$ and $1/4$ are in $[3\pi/4, 5\pi/6] \cup [7\pi/6, 5\pi/4]$. Suppose that $1/4$ of the Galois conjugates of γ are in $[-2\pi/3, 2\pi/3]$. In this case, by Lemmas 3–5, $A_1 \le \sqrt[4]{2+\sqrt{2}} \cdot \sqrt[8]{2+\sqrt{3}} \cdot \sqrt[8]{3}$, and (3) holds.

We consequently assume that $3/4$ of the Galois conjugates of γ lie in the sectors $[2\pi/3, 3\pi/4] \cup [-3\pi/4, -2\pi/3]$ and that the other $1/4$ lie in $[3\pi/4, 5\pi/6] \cup [7\pi/6, 5\pi/4]$. Consequently, $1/4$ of the Galois conjugates of γ^2 lie in $[3\pi/2, 5\pi/3] \cup [7\pi/3, 5\pi/2]$ and all of them lie in $[-2\pi/3, 2\pi/3]$ from which it follows that $A_2 \le 3^{3/8} 2^{1/8}$, giving (3). ∎

Proof of Theorem 1. By the results of Smyth and Schinzel and Propositions 1, 4, 5, and 7, we assume that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \in \{4, 6, 8\}$. Theorem 1 then follows from the results of Smyth and Schinzel together with Propositions 8–10. ∎

References

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

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

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

[4] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. 24 (1973), 385–399; Addendum, ibid. 26 (1973), 329–331.

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

Department of Mathematics
The University of Texas at Austin
1 University Station, C1200
Austin, TX 78712, U.S.A.
E-mail: jgarza@math.utexas.edu

Received on 7.11.2006
and in revised form on 2.1.2008 (5316)