A uniform relative Dobrowolski’s lower bound over abelian extensions.
Francesco Amoroso, Umberto Zannier

To cite this version:

HAL Id: hal-00424258
https://hal.archives-ouvertes.fr/hal-00424258
Submitted on 14 Oct 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
A uniform relative Dobrowolskis lower bound over abelian extensions.

Francesco AMOROSO and Umberto ZANNIER

June 21, 2009

Abstract. Let $L/K$ be an abelian extension of number fields. We prove an uniform lower bound for the height in $L^*$ outside roots of unity. This lower bound depends only on the degree $[L : K]$.

1 Introduction.

Let $h$ be the Weil height on $\mathbb{Q}$ and let $\mu$ the set of roots of units. Let $L$ be an abelian extension of the rational field. In a joint work with R. Dvornicich ([Am-Dv]) the first author proved that for any $\alpha \in L^* \setminus \mu$

$$h(\alpha) \geq \frac{\log 5}{12} \quad (1.1)$$

giving a positive answer to a question of E. Bombieri and the second author. This result was generalized by several authors replacing $\mathbb{Q}^*$ by more complicated group varieties (see [Ba], [Si], [Ba-Si], [Ami-Da]).

Later, in a joint paper ([Am-Za]), we proved a “relative” result, which combines the lower bound (1.1) with a celebrate result of Dobrowolski ([Do]). Let $L$ be an abelian extension of a number field $K$ and let $\alpha \in \mathbb{Q}^* \setminus \mu$. Then

$$h(\alpha) \geq \frac{c(K)}{D} \left( \frac{\log \log 5D}{\log 2D} \right)^{13},$$

where $D = [L(\alpha) : L]$ and where $c(K) > 0$ (see [Ra] for a generalization to elliptic curves). More recently, the first author and E. Delsinne ([Am-De]) refine the error term in this inequality and compute a lower bound for $c(K)$. As the proof of
the original paper suggested, this lower bound depends on the degree and on the discriminant of \( K \).

In this paper we are interested in uniform lower bounds for the height on an abelian extension of a number field \( K \). We define

\[
\gamma_{ab}(K) = \inf \{ h(\alpha) \text{ such that } \alpha \in L^* \setminus \mu, \ L/K \text{ abelian} \}.
\]

As a very special case of the result of [Am-Za], \( \gamma_{ab}(K) \geq c(K) \) and, by the results of [Am-De], \( c(K) \) is bounded from below by an explicit positive function depending on the degree and on the discriminant of \( K \). A question which has been raised explicitly by a number of mathematicians is whether \( \gamma_{ab}(K) \) may be bounded below in terms only of the degree of \( K \), namely the following:

**Problem 1.1** It is true that \( \gamma_{ab}(K) \geq f([K : \mathbb{Q}]) \) for some positive function \( f(\cdot) \)?

We give a positive answer to this question:

**Theorem 1.2** Let \( K \) be a number field of degree \( d \) over \( \mathbb{Q} \) and let \( \alpha \in \mathbb{Q}^* \setminus \mu \). Assume \( K(\alpha)/K \) abelian. Then

\[
h(\alpha) > 3^{-d^2 - 2d - 6}.
\]

In other words, \( \gamma_{ab}(K) > 3^{-d^2 - 2d - 6} \).

Let \( L \) be a dihedral extension of the rational field of degree \( 2n \). Then \( L \) is an abelian extension of its quadratic subfield fixed by the normal cyclic group of order \( n \). Thus

**Corollary 1.3** Let \( L \) be a dihedral extension of the rational field and let \( \alpha \in \mathbb{Q}^* \setminus \mu \). Then

\[
h(\alpha) \geq 3^{-14}.
\]

For further examples, results and conjectures, see section 5.

The proof of theorem 1.2 does not follow by a straightforward adaptation of the previous methods and requires several new arguments and tools: we shall need a finer use of ramification theory and especially a new descent argument to eliminate dependence on discriminants; this was totally absent in the quoted papers in this topic.

More precisely, here is a sketch of how these new arguments come into the proof.

Let \( L/K \) be an abelian extension of number fields and let \( \wp \) be a prime ideal of \( K \) over a rational prime \( p \). Let \( q = N_{\wp} \). Assume that \( \wp \) is ramified in \( L \) and consider the subgroup

\[
H_\wp := \{ \sigma \in \text{Gal}(L/K) \text{ such that } \forall \gamma \in \mathcal{O}_L, \ \sigma \gamma^q \equiv \gamma^q \mod \wp \mathcal{O}_L \}.
\]
If $K_{p} = \mathbb{Q}_p$, then $L$ is locally contained in a cyclotomic extension of $\mathbb{Q}$ by the Kronecker-Weber theorem. Using this remark, we proved in [Am-Za], Lemma 3.2, that $H_{p}$ is non-empty. Here we need a generalization of this result, dropping the assumption $K_{p} = \mathbb{Q}_p$. This is done in section 2, using ramification theory. In Section 3 we prove a lower bound for the height of $\alpha \in L$, under the technical assumption $K(\alpha^{q}) = K(\alpha)$: this step follows similarly to the papers [Am-Dv] and [Am-Za] (see especially Lemma 3.2 therein).

However, to remove such annoying technical assumption in the most general case we need a totally new “kummerian” descent argument, which is developed in section 4.

Acknowledgments. We thank B. Anglès et G. Ranieri for reading a preliminary version of this paper. We also thank R. Dvornicich for helpful discussions.

2 Ramification

We recall some basic fact about higher ramification groups. Let $L/K$ be a normal extension of number fields with Galois group $G$. Let $\wp$ be a prime ideal of $K$ and let $\mathfrak{Q}$ be a prime ideal of $L$ over $\wp$. We consider the decomposition group $G_{-1} = G_{-1}(\mathfrak{Q}/\wp) = \{\sigma \in G \text{ such that } \sigma(\mathfrak{Q}) = \mathfrak{Q}\}$ and (for $k = 0, 1, \ldots$) the $k$-th ramification group $G_{k} = G_{k}(\mathfrak{Q}/\wp) = \{\sigma \in G \text{ such that } \forall \gamma \in \mathcal{O}_L, \sigma\gamma \equiv \gamma \mod \mathfrak{Q}^{k+1}\}$. Then $G \supseteq G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots$. Moreover, for all $k \geq 0$, $G_{k}$ is a normal subgroup of $G_{-1}$. Let $(p) = \wp \cap \mathbb{Z}$. Writing $e := |G_0| = e_0p^{a}$ with $(e_0, p) = 1$ we have $|G_0/G_1| = e_0$.

Let $\pi$ be a uniformizer at $\mathfrak{Q}$ (i.e. $\pi \in \mathfrak{Q} \setminus \mathfrak{Q}^2$). We consider the map

$$
\theta_0 : G_0/G_1 \to (\mathcal{O}_L/\mathfrak{Q})^*
$$

which sends $\sigma$ to the class of $\sigma(\pi)/\pi$. We also consider, for $k \geq 1$, the map

$$
\theta_k : G_k/G_{k+1} \to \mathfrak{Q}^k/\mathfrak{Q}^{k+1}
$$

which sends $\sigma$ to the class of $\sigma(\pi)/\pi - 1$. Then (cf [Co], proposition 10.1.14)

**Proposition 2.1** The maps $\theta_k$ are well-defined and injective. Moreover, they do not depend on the choice of the uniformizer $\pi$.

Let now assume that $G_{-1}$ is an abelian group. Then

**Proposition 2.2**

i) The image of $\theta_0$ is contained in $(\mathcal{O}_K/\wp)^*$. 

ii) For all $k \geq 1$, the image of $\theta_k$ is contained in a $\mathcal{O}_K/\wp$ vector space of dimension 1.
In particular

\[ |G_k/G_{k+1}| \leq N \varphi \]  

(2.2)

for \( k = 0, 1, \ldots \).

**Proof.** For i), see [Ca], corollary 2, page 136. For ii), a straightforward computation shows that the image of \( \theta_k \) is fixed by \( G_{-1} \). Indeed let \( \tau \in G_k, \sigma \in G_{-1} \) and \( \alpha := \tau \pi/\pi - 1 \). Let also \( \sigma(\pi) = x\pi \) with \( x \not\in \Omega \). Thus \( \sigma^{-1}(\pi) = \sigma^{-1}(x^{-1})\pi \) and

\[
\tau(\pi) = \sigma \tau \sigma^{-1}(\pi) = (\sigma \tau)(\sigma^{-1}(x^{-1})\pi) = \tau(x)^{-1}(\sigma \tau)(\pi) = \tau(x)^{-1}\sigma(\pi + \alpha \pi) = \tau(x)^{-1}x(1 + \sigma(\alpha))\pi.
\]

Since \( \tau \in G_k \) and \( x \not\in \Omega \), \( \tau(x)^{-1}x \equiv 1(\pi^{k+1}) \). Thus \( \alpha = \tau(\pi)/\pi - 1 \equiv \sigma(\alpha)(\pi^{k+1}) \). Since \( \theta_k(\tau) \) is the class of \( \alpha \) in \( \Omega^k/\Omega^{k+1} \), this last congruence proves that

\[
\theta_k(\tau) = \sigma(\theta_k(\tau)).
\]

(2.3)

Let now \( v_0, v \in \text{Im}(\theta_k) \) with \( v_0 \neq 0 \) (if \( G_k/G_{k+1} \) is trivial the result is clear). Since \( \Omega^k/\Omega^{k+1} \) is a vector space of dimension 1 over \( \mathcal{O}_L/\mathcal{O}_L \), we have \( v = \lambda v_0 \) for some \( \lambda \in \mathcal{O}_L/\mathcal{O}_L \). Equation (2.3) shows that \( \lambda \) is fixed by \( G_{-1} \). Since \( \text{Gal}(\mathcal{O}_L/\mathcal{O}_K/\varphi) \cong G_{-1}/G_0 \), we infer that \( \lambda \in \mathcal{O}_K/\varphi \). Thus \( \text{Im}(\theta_k) \) is contained in the \( \mathcal{O}_K/\varphi \)-vector space spanned by \( v_0 \).

\[ \square \]

**Proposition 2.3** Let \( L/K \) be an abelian extension of number fields with Galois group \( G \) and let \( \varphi \) be a prime ideal of \( K \), ramified in \( L \). Let \( q = N \varphi \). Then

\[
H_{\varphi} := \{ \sigma \in G \text{ such that } \forall \gamma \in \mathcal{O}_L, \sigma \gamma \equiv \gamma \text{ mod } \varphi \mathcal{O}_L \}
\]

is a non trivial subgroup of \( G \).

**Proof.** As before, let \( G_{-1} \) and \( G_k \) be the inertia group and the ramification groups of a prime \( \Omega \) over \( \varphi \) (since \( G \) is abelian, these groups do not depend on the choice of \( \Omega \)). Let \( e = |G_0| \) and \((p) = \varphi \cap \mathbb{Z} \). We write as before \( e = e_0 p^a \) with \((e_0, p) = 1 \). Assume first that \( \varphi \) is tamely ramified in \( L \). Thus \( e = e_0 = |G_0/G_1| \leq q \), by (2.2) of Proposition 2.2. Let \( \sigma \in G_0 \) and \( \gamma \in \mathcal{O}_L \); then

\[
(\sigma \gamma - \gamma)^q \in \Omega^q \subseteq \Omega^e
\]

and

\[
(\sigma \gamma - \gamma)^q \equiv \sigma \gamma^q - \gamma^q \text{ mod } p \mathcal{O}_L.
\]

This implies

\[
\sigma \gamma^q \equiv \gamma^q \text{ mod } \varphi \mathcal{O}_L.
\]
Thus $H_\wp \supset G_0$. On the other hand, $G_0$ is non-trivial because $\wp$ ramifies in $L$ by assumption.

Let now assume $p | e$. By Hasse-Arf theorem ([Se], §7, Th. 1', p.101)

$$\forall j \geq 1, \ G_j \neq G_{j+1} \implies \frac{1}{e} \sum_{i=1}^{j} |G_i| \in \mathbb{Z}.$$  

Let $k \geq 1$ such that $G_k \neq G_{k+1} = \{1\}$. We also define $h = 0$ if $G_k = G_1$ and otherwise we define $h \geq 1$ by

$$G_h \neq G_{h+1} = \cdots = G_k \neq G_{k+1} = \{1\}.$$  

Then

$$\frac{1}{e} \sum_{i=1}^{h} |G_i| \in \mathbb{Z} \quad \text{and} \quad \frac{1}{e} \sum_{i=1}^{k} |G_i| \in \mathbb{Z}.$$  

Thus $e$ divides

$$\sum_{i=h+1}^{k} |G_i| = (k-h)|G_k| = (k-h)|G_k/G_{k+1}|.$$  

Thus, by inequality (2.2) of Proposition 2.2 we have $e \leq kq$.

Therefore, for any $\sigma \in G_{k-1}$ and for any $\gamma \in \mathcal{O}_L$

$$(\sigma \gamma - \gamma)^q \in \mathcal{O}^{kq} \subseteq \mathcal{O}^e.$$  

As before, this implies

$$\sigma \gamma^q \equiv \gamma^q \mod \wp \mathcal{O}_L.$$  

Thus $\{1\} \neq G_{k-1} \subseteq H \subseteq G_0$.

\[\square\]

### 3 A first lower bound

The following is Lemma 1 of [Am-Dv].

**Lemma 3.1** Let $L$ be a number field and let $\nu$ be a non-archimedean place of $L$. Then, for any $\alpha \in L^*$ there exists an algebraic integer $\beta \in L$ such that $\beta \alpha$ is also integer and

$$|\beta|_\nu = \max\{1, |\alpha|_\nu\}^{-1}.$$  

We now prove our main proposition:
Proposition 3.2. Let $K$ be a number field of degree $d$ over $\mathbb{Q}$. Let $\wp$ be a prime ideal of $K$. We denote $q = N\wp$. Let $\alpha \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ and assume that $K(\alpha)$ is an abelian extension of $K$. Assume further

$$K(\alpha) = K(\alpha^q).$$  \hspace{1cm} (3.4)

Then

$$h(\alpha) \geq \frac{\log(q^{1/d}/2)}{2q}.$$  \hspace{1cm} \text{(3.4)}

Proof. Let $(p) = \wp \cap \mathbb{Z}$ and let $e = e(\wp/p)$, $f = f(\wp/p)$, be resp. the ramification index and the inertial degree of $\wp$ over $p$.

A first case occurs when $\wp$ does not ramify in $L$; let then $\phi$ be the Frobenius automorphism of $\Omega/\wp$, where $\Omega$ is any prime of $L$ over $\wp$ (since $L/K$ is abelian, $\phi$ does not depend on the choice of $\Omega$).

Let $\nu$ be a place of $L := K(\alpha)$, normalized so to induce on $\mathbb{Q}$ one of the standard places. We shall estimate $|\alpha^q - \phi(\alpha)|_\nu$. Suppose to start with that $\nu|\wp$.

By Lemma 1, there exists an integer $\beta \in L$ such that $\alpha \beta$ is integer and $|\beta|_\nu = \max\{1, |\alpha|_\nu\}^{-1}$.

Then $(\alpha \beta)^q \equiv \phi(\alpha \beta) \mod \wp \mathcal{O}_L$ and $\beta^q \equiv \phi(\beta) \mod \wp \mathcal{O}_L$. We recall that $\forall \gamma \in \wp \mathcal{O}_L$ we have $|\gamma|_\nu \leq p^{-1/e}$. Using the ultrametric inequality, we deduce that

$$|\alpha^q - \phi(\alpha)|_\nu \leq |\beta|_\nu^{-q} \max\{1, |\alpha \beta|_\nu, |\alpha|_\nu, |\beta|_\nu, |\phi(\alpha)|_\nu\}$$

$$\leq \max(1, |\alpha|_\nu)^q p^{-1/e} \max(1, |\phi(\alpha)|_\nu).$$

Suppose now that $\nu$ is a finite place not dividing $\wp$. Then we have plainly

$$|\alpha^q - \phi(\alpha)|_\nu \leq \max(1, |\alpha|_\nu)^q \max(1, |\phi(\alpha)|_\nu).$$

Finally, if $\nu|\infty$, we have

$$|\alpha^q - \phi(\alpha)|_\nu \leq 2 \max(1, |\alpha|_\nu)^q \max(1, |\phi(\alpha)|_\nu).$$

Moreover $x := \alpha^q - \phi(\alpha) \neq 0$, since $\alpha$ is not a root of unity. Indeed, if $x = 0$ then $qh(\alpha) = h(\alpha^q) = h(\phi(\alpha)) = h(\alpha)$, which implies $h(\alpha) = 0$. We apply the
product formula to $x$:

$$0 = \sum_{\nu|\infty} \frac{[L_{\nu} : Q_{\nu}]}{[L : Q]} \log |x|_{\nu} + \sum_{\nu | \wp} \frac{[L_{\nu} : Q_{\wp}]}{[L : Q]} \log |x|_{\nu} + \sum_{\nu|\infty} \frac{[L_{\nu} : Q_{\nu}]}{[L : Q]} \log |x|_{\nu}$$

$$\leq \sum_{\nu} \frac{[L_{\nu} : Q_{\nu}]}{[L : Q]} \left( q \log |\alpha|_{\nu} + \log \sigma(\alpha)|_{\nu} \right) - \frac{\log p}{e} \sum_{\nu | \wp} \frac{[L_{\nu} : Q_{\wp}]}{[L : Q]}$$

$$+ \sum_{\nu|\infty} \frac{[L_{\nu} : Q_{\nu}]}{[L : Q]} \log 2$$

$$= q h(\alpha) + h(\sigma(\alpha)) - \frac{[L_{\wp} : Q_{\wp}]}{e[L : Q]} \sum_{\nu | \wp} \frac{[L_{\nu} : Q_{\wp}]}{[L_{\wp} : Q_{\wp}]} + (\log 2) \sum_{\nu|\infty} \frac{[L_{\nu} : Q_{\nu}]}{[L : Q]}.$$

We recall that $h(\sigma(\alpha)) = h(\alpha)$. Moreover,

$$\sum_{\nu | \infty} \frac{[L_{\nu} : Q_{\nu}]}{[L : Q]} = 1, \quad \sum_{\nu | \wp} \frac{[L_{\nu} : Q_{\wp}]}{[L_{\wp} : Q_{\wp}]} = [L : K]$$

and $[L_{\wp} : Q_{\wp}] = ef$. Thus

$$0 \leq (q + 1)h(\alpha) + \log 2 - \frac{f}{d} \log p$$

i. e.

$$h(\alpha) \geq \frac{\log (q^{1/d}/2)}{q + 1} \geq \frac{\log (q^{1/d}/2)}{2q}.$$

Assume now that $\wp$ is ramified in $L$ and let $\sigma$ be a non trivial automorphism in the subgroup $H_{\wp}$ defined in Proposition 2.3. Let $\nu$ be a place of $L$ dividing $\wp$ and let $\beta$ as in the first part of the proof. We have $(\alpha \beta)^q \equiv \sigma(\alpha \beta)^q \mod \wp O_L$ and $\beta^q \equiv \sigma \beta^q \mod \wp O_L$. Using the ultrametric inequality, we find

$$|\alpha^q - \sigma(\alpha)^q|_{\nu} = |\beta|_{\nu}^{-q}|(\alpha \beta)^q - \sigma(\alpha \beta)^q + (\sigma \beta^q - \beta^q)\sigma(\alpha)|_{\nu} \leq p^{-1/e} \max(1, |\alpha|_{\nu})^q \max(1, |\sigma(\alpha)|_{\nu})^q.$$

Assume $\sigma(\alpha)^q = \alpha^q$. Since $\sigma(\alpha) \neq \alpha$ we have $K(\alpha^q) \subsetneq K(\alpha)$, which contradicts hypothesis (3.4).

Thus $x := \alpha^q - \sigma(\alpha)^q \neq 0$. Applying the product formula to $x$ as in the first part of the proof, we get

$$0 \leq 2qh(\alpha) + \log 2 - \frac{f}{d} \log p.$$

Therefore

$$h(\alpha) \geq \frac{\log (q^{1/d}/2)}{2q}.$$

\[\square\]
4 Radicals reduction

In this section we show that a slightly weaker version of Proposition 3.2 still holds without assuming (3.4). The proof of the main theorem will follow.

We need the following lemma (perhaps known, but for which we have no reference):

**Lemma 4.1** Let $B, k$ be integers with $B \geq 5$ and $k \geq 60 B \log B$. Then, for every subgroup $H$ of $(\mathbb{Z}/(k))^*$ of index $\leq B$, there are $h_1, h_2 \in H$ such that

$$2 < h_1 - h_2 \leq 60 B \log B.$$ 

**Proof.** Write an integer decomposition $k = k_1 k_2$ where $k_1$ is divisible only by primes $\leq B^5$ and where $k_2$ is coprime to any such prime. Then $\gcd(k_1, k_2) = 1$ and we have a decomposition $(\mathbb{Z}/(k))^* \cong (\mathbb{Z}/(k_1))^* \times (\mathbb{Z}/(k_2))^*$, say, where $G_1 = (\mathbb{Z}/(k_1))^* \times \{1\}$, $G_2 = \{1\} \times (\mathbb{Z}/(k_2))^*$. Further, for $i = 1, 2$ put $H_i := H \cap G_i$, so $[G_i : H_i] \leq B$.

By the corollary to theorem 7 of [Ro-Sc], for any $x > 1$

$$\prod_{l \leq x} \left(1 - \frac{1}{l}\right) > \frac{e^{-\gamma}}{\log x} \left(1 - \frac{1}{(\log x)^2}\right)$$

where $\gamma$ is Euler’s constant and in the product $l$ runs through prime numbers. Since $B \geq 5$,

$$\frac{k_1}{\phi(k_1)} \leq \prod_{l \leq B^5} \left(1 - \frac{1}{l}\right)^{-1} < 5 e^{-\gamma} \left(1 - \frac{1}{(5 \log 5)^2}\right)^{-1} \log B < 10 \log B. \quad (4.5)$$

Let $s$ be the integer defined by

$$\frac{1}{3} |H_1| - 1 \leq s < \frac{1}{3} |H_1|.$$ 

We have $|H_1| \geq \phi(k_1)/B$, so by (4.5) and since $k_1 \geq 60 B \log B$,

$$s \geq \frac{\phi(k_1)}{3B} - 1 \geq \frac{k_1}{30 B \log B} - 1 \geq \frac{k_1}{60 B \log B}.$$ 

By the Pigeon-hole principle, there exist integers $x_1, \ldots, x_4$ whose class modulo $k_1$ is in $H_1$ and such that

$$x_1 < x_2 < x_3 < x_4$$

and

$$x_4 - x_1 < \frac{k_1}{s} \leq 60 B \log B.$$ 

Let $x = x_1$ and $t = x_4 - x_1$. Then $x, x + t \in H_1$ and $2 < t \leq 60 B \log B$.

Let now $l^a$ be a power of the prime $l$ dividing exactly $k_2$ and set $H(l) = H \cap (\mathbb{Z}/(l^a))^*$, where we view the group on the right as a subgroup of $G_2$, as before. Let $V(l)$ be the the kernel of the reduction $r: (\mathbb{Z}/(l^a))^* \to (\mathbb{Z}/(l))^*$ modulo
lies in $K$. Note that $\Gamma$ is a subgroup of $\text{Gal}(K(\alpha)/K)$. We let $L_\alpha := K(\alpha)^{\Gamma_\alpha}$ be its fixed field; note that $K(\alpha)/L_\alpha$ is Galois with group $\Gamma_\alpha$.

We need the following simple generalization of a classical lemma in Kummer’s theory.

**Lemma 4.2** Let $k$ be a positive integer, $\sigma \in \text{Gal}(K(\zeta_k)/K)$ and $\alpha \in \overline{\mathbb{Q}}$. We assume that $K(\alpha)/K$ is abelian. Then for any extension $\tilde{\sigma} \in \text{Gal}(K(\alpha, \zeta_k)/K)$ we have

$$\tilde{\sigma}\alpha^{\sigma} \in L_\alpha,$$

where $g = g_\sigma$ is defined by $\sigma\zeta_k = \zeta_k^{g_\sigma}$ and $g_\sigma \in [1, k)$.

**Proof.** Let $\tau \in \Gamma_\alpha$, then $\tau\alpha = \zeta_k^u\alpha$ for some $u \in \mathbb{Z}$. Put $\alpha' = \tilde{\sigma}\alpha$; note that $\alpha'$ lies in $K(\alpha)$ because it is a conjugate of $\alpha$ over $K$. Then, since $K(\alpha, \zeta_k)/K$ is also abelian (as a composite of abelian extensions of $K$), we have

$$\tau\alpha'/\alpha' = \tau\tilde{\sigma}\alpha/\tilde{\sigma}\alpha = \tilde{\sigma}(\tau\alpha/\alpha) = \sigma\zeta_k^u = \zeta_k^{ug_\sigma} = (\tau\alpha/\alpha)^{g_\sigma}.$$

Thus $\alpha'/\alpha^{g_\sigma}$ is fixed by $\tau$ for all $\tau \in \Gamma_\alpha$, and therefore it lies in $L_\alpha$. 

\[\square\]
Proposition 4.3 Let $K$ be a number field of degree $d$ over $\mathbb{Q}$ and let $\wp$ be a prime ideal of $K$. Let $q = N\wp$, $\alpha \in \overline{\mathbb{Q}}^* \setminus \mu$ and assume that $K(\alpha)$ is an abelian extension of $K$. Then
\[
h(\alpha) \geq \frac{\log (q^{1/d}/2)}{400d\log(3d)q}.
\]

Proof. We choose an integer $k > 180d\log(3d)$ such that any root of unity of the shape $\rho\alpha/\alpha$ for $\rho \in \Gamma_\alpha$ has order dividing $k$.

Note that $\text{Gal}(K(\zeta_k)/K)$ may be seen as a subgroup of $(\mathbb{Z}/k)^*$ of index $\leq [K : \mathbb{Q}] = d$. We choose $B = 3d \geq 6$ in Lemma 4.1. Since $k \geq 180d\log(3d)$, the assumptions of this lemma are satisfied. We thus see that there exist $\sigma_1, \sigma_2 \in \text{Gal}(K(\zeta_k)/K)$ such that
\[
2 < g_{\sigma_2} - g_{\sigma_1} < 180d\log(3d).
\]
We define $g = g_{\sigma_2} - g_{\sigma_1}$. By Lemma 4.2 we have
\[
\tilde{\sigma}_2(\alpha) = c\alpha^g\tilde{\sigma}_1(\alpha) \tag{4.6}
\]
with $c \in L_\alpha$. We recall that
\[
2 < g < 180d\log(3d). \tag{4.7}
\]
We want to apply Proposition 3.2 to $c$. To do that we need that $c \not\in \mu$ and that $K(c) = K(c^\theta)$. Let us verify these requirements.

• $c \not\in \mu$. Assume the contrary. Then, by (4.6),
\[
gh(\alpha) = h(\alpha^g) = h(\tilde{\sigma}_2(\alpha))/\tilde{\sigma}_1(\alpha)) \leq 2h(\alpha).
\]
Since $g > 2$ we get $\alpha \in \mu$. Contradiction.

• $K(c) = K(c^\theta)$. Assume the contrary. Note that $K(c)/K(c^\theta)$ is Galois, as a subextension of the abelian extension $K(\alpha)/K$. Then, let $\tau$ be a non-trivial element of $\text{Gal}(K(c)/K(c^\theta))$. We have $\tau(c) = \theta c$ for some nontrivial root of unity $\theta$.

Denote by $\tilde{\tau} \in \text{Gal}(K(\alpha)/K)$ an arbitrary extension of $\tau$ and set $\eta := \tilde{\tau}(\alpha)/\alpha$. Now, apply (4.6) and its conjugate by $\tilde{\tau}$, taking into account that we are working in an abelian extension of $K$. We obtain $\tilde{\sigma}_2(\eta) = \theta\eta^g\tilde{\sigma}_1(\eta)$. Hence $gh(\eta) \leq 2h(\eta)$ which implies $h(\eta) = 0$. Hence $\eta \in \mu$. But then $\tilde{\tau} \in \Gamma_\alpha$ by definition. Since however $c \in L_\alpha$ and since $\Gamma_\alpha$ fixes $L_\alpha$ we have a contradiction because $\theta \neq 1$.

The hypotheses of Proposition 3.2 are therefore fulfilled. We get the lower bound
\[
h(c) \geq \frac{\log (q^{1/d}/2)}{2q}.
\]
By (4.6) and by the upper bound $g < 180d\log(3d)$ (see (4.7)) we have

$$h(c) \leq (g + 2)h(\alpha) \leq 182d\log(3d)h(\alpha).$$

Thus

$$h(\alpha) \geq \frac{\log (q^{1/d}/2)}{400d\log(3d)q}.$$ 

\[\square \]

**Proof of theorem 1.2.** Let $p$ be a prime number such that $3^d \leq p < 2 \cdot 3^d$ and let $\wp$ be a prime of $K$ over $p$. Let $q = N\wp$. Then

$$3^d \leq p \leq q \leq p^d < 3^{d^2+d}.$$ 

Thus, by proposition 4.3,

$$h(\alpha) > \frac{\log(3/2)}{400d\log(3d) \cdot 3^{d^2+d}} \geq 3^{-d^2-2d-6},$$

since $\log(3/2) \geq 1/3$ and $400d\log(3d) \leq 3^{d+5}$. 

\[\square \]

5 \hspace{1em} **Further remarks**

In this section we denote by $c_1, c_2, c_3, c_4$ absolute positive constants.

5.1

The “natural” generalisation of Lehmer’s conjecture, namely

$$\gamma_{ab}(K) \geq \frac{c}{[K : \mathbb{Q}]},$$

for some positive constant $c$, is false. Let $K_n = \mathbb{Q}(\zeta_n)$ and $L_n = K_n(2^{1/n})$; then $L_n/K_n$ is cyclic and

$$h(2^{1/n}) = \frac{\log 2}{n}.$$ 

Let $n(x)$ be the product of all primes up to $x > 1$ and define $d(x) := [K_{n(x)} : \mathbb{Q}] = \varphi(n(x))$. Then, by elementary analytic number theory,

$$n(x) \geq c_1 d(x) \log \log 3d(x).$$

Therefore

$$\gamma_{ab}(K_{n(x)}) \leq \frac{\log 2}{c_1 d(x) \log \log 3d(x)}.$$ 

This prove

**Proposition 5.1**

$$\liminf_{[K : \mathbb{Q}] \to \infty} \gamma_{ab}(K)[K : \mathbb{Q}] \log \log [K : \mathbb{Q}] < \infty.$$ 

11
5.2

For cyclotomic extensions of a number field $K$ of degree $d$, we can deduce from the main results of [Am-Za] and [Am-De] a lower bound for the height sharper than theorem 1.2.

**Proposition 5.2** Let $\zeta$ be a root of unity and let $\alpha \in K(\zeta)^* \setminus \mu$. Then

$$h(\alpha) \geq \frac{c_2 (\log \log 5d)^3}{d(\log 2d)^4}.$$ 

**Proof.** By Galois’ Theory, $K(\zeta)$ is an extension of $\mathbb{Q}(\zeta)$ of degree bounded by $d$. Since $\mathbb{Q}(\zeta)$ is an abelian extension of $\mathbb{Q}$, by the refined inequality of [Am-De] there exists an absolute constant $c_2 > 0$ such that

$$h(\alpha) \geq \frac{c_2 (\log \log 5d)^3}{d(\log 2d)^4}.$$ 

$\square$

5.3

The example of subsection 5.1 cannot be substantially improved by “taking roots” in a fixed field $K$.

**Proposition 5.3** Let $K$ be a number field of degree $d$. Let $\alpha \in \mathbb{Q}^* \setminus \mu$ such that $\alpha^n \in K$ for some positive integer $n$. Then, if $K(\alpha)/K$ is abelian,

$$h(\alpha) \geq \frac{c_3 (\log \log 5d)^2}{d(\log 2d)^4}.$$ 

**Proof.**

Let $\mu_n \cap K^* = \mu_r$; thus $r$ is the number of $n$-roots of unity contained in $K$. Since $K(\alpha)/K$ is abelian, the extension $K(\alpha, \zeta)/K$ is also abelian. By a theorem of Schinzel ([Sc], theorem 2), there exists $\gamma \in K$ such that

$$\alpha^{nr} = \gamma^n.$$

Let $\delta = [K : \mathbb{Q}(\zeta_r)] = d/\varphi(r)$. Since $\mathbb{Q}(\zeta_r)$ is an abelian extension of $\mathbb{Q}$, by the quoted result of [Am-De]

$$h(\gamma) \geq \frac{c_2 (\log \log 5\delta)^3}{\delta(\log 2\delta)^4} \geq \frac{c_2 (\log \log 5d)^3}{\delta(\log 2d)^4}.$$ 

By elementary analytic number theory, $r \leq c_4 \varphi(r) \log \log 3 \varphi(r) \leq c_4 \varphi(r) \log 5d$. Thus

$$h(\alpha) = \frac{h(\gamma)}{r} \geq \frac{c_3 (\log \log 5d)^2}{d(\log 2d)^4}.$$ 

$\square$
5.4

The examples and results above suggest the following conjecture.

**Conjecture 5.4** Let $K$ be a number field of degree $d$. Then, for any $\varepsilon > 0$ there exists $c_\varepsilon > 0$ having the following property. Let $\alpha \in \overline{\mathbb{Q}}^\times \setminus \mu$ such that $K(\alpha)/K$ is an abelian extension. Then

$$h(\alpha) \geq c_\varepsilon d^{-1-\varepsilon}.$$ 

**References**


