A uniform relative Dobrowolski's lower bound over abelian extensions

A uniform relative Dobrowolskis lower bound over abelian extensions.

Francesco Amoroso and Umberto Zannier

Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139
Université de Caen, Campus II, BP 5186
14032 Caen Cedex, France

Scuola Normale Superiore
Piazza dei Cavalieri, 7
56126 Pisa, Italia

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 $[L : K]$.

Mathematics Subject Classification: 11G5O (Primary), 11Jxx (Secondary).

1 Introduction.

Let h be the Weil height on $\overline{\mathbb{Q}}$ and let $\boldsymbol{\mu}$ 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 $\alpha \in L^* \backslash \boldsymbol{\mu}$

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

giving a positive answer to a question of E. Bombieri and the second author. This result was generalized by several authors replacing $\overline{\mathbb{Q}}^*$ 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 $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$. 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

$$\gamma_{\mathrm{ab}}(K) = \inf\{h(\alpha) \text{ such that } \alpha \in L^* \backslash \boldsymbol{\mu},\ L/K \text{ abelian}\} .$$

As a very special case of the result of [Am-Za], $\gamma_{\mathrm{ab}}(K) \geq c(K)$ 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 explicitely 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* $\gamma_{\mathrm{ab}}(K) \geq f([K:\mathbb{Q}])$ *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 $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$. Assume $K(\alpha)/K$ abelian. Then*

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

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

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 $\alpha \in L^* \backslash \boldsymbol{\mu}$. 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 straighforward 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

$$H_\wp := \{\sigma \in \mathrm{Gal}(L/K) \text{ such that } \forall \gamma \in \mathcal{O}_L,\ \sigma\gamma^q \equiv \gamma^q \bmod \wp\mathcal{O}_L\} .$$

If $K_\wp = \mathbb{Q}_p$, 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 $H_\wp$ is non-trivial. Here we need a generalization of this result, dropping the assumption $K_\wp = \mathbb{Q}_p$. 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 $\mathfrak{L}$ be a prime ideal of L over $\wp$. We consider the decomposition group $G_{-1} = G_{-1}(\mathfrak{L}/\wp) = \{\sigma \in G \text{ such that } \sigma(\mathfrak{L}) = \mathfrak{L}\}$ and (for $k = 0, 1, \ldots$) the k-th ramification group

$$G_k = G_k(\mathfrak{L}/\wp) = \{\sigma \in G \text{ such that } \forall \gamma \in \mathcal{O}_L,\, \sigma\gamma \equiv \gamma \bmod \mathfrak{L}^{k+1}\} .$$

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 $e := |G_0| = e_0 p^a$ with $(e_0, p) = 1$ we have $|G_0/G_1| = e_0$.

Let π be a uniformizer at $\mathfrak{L}$ (*i. e.* $\pi \in \mathfrak{L}\backslash\mathfrak{L}^2$). We consider the map

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

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

$$\theta_k \colon G_k/G_{k+1} \to \mathfrak{L}^k/\mathfrak{L}^{k+1}$$

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

Proposition 2.1 *The maps θ_k are well-defined and injective. Moreover, they do not depend on the choice of the uniformizer π.*

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

Proposition 2.2

i) The image of θ_0 is contained in $(\mathcal{O}_K/\wp)^*$.

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

In particular

$$|G_k/G_{k+1}| \leq N\wp \tag{2.1}$$

for $k = 0, 1, \ldots$.

Proof. For i), see [Ca], corollary 2, page 136. For ii), a straightforward computation shows that the image of θ_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 $x \notin \mathfrak{Q}$. Thus $\sigma^{-1}(\pi) = \sigma^{-1}(x^{-1})\pi$ and

$$\begin{aligned}\tau(\pi) = \sigma\tau\sigma^{-1}(\pi) &= (\sigma\tau)(\sigma^{-1}(x^{-1})\pi) \\ &= \tau(x)^{-1}(\sigma\tau)(\pi) \\ &= \tau(x)^{-1}\sigma(\pi + \alpha\pi) \\ &= \tau(x)^{-1}x(1 + \sigma(\alpha))\pi \ .\end{aligned}$$

Since $\tau \in G_k$ and $x \notin \mathfrak{Q}$, $\tau(x)^{-1}x \equiv 1(\pi^{k+1})$. Thus $\alpha = \tau(\pi)/\pi - 1 \equiv \sigma(\alpha)(\pi^{k+1})$. Since $\theta_k(\tau)$ is the class of α in $\mathfrak{Q}^k/\mathfrak{Q}^{k+1}$, this last congruence proves that

$$\theta_k(\tau) = \sigma(\theta_k(\tau)) \ . \tag{2.2}$$

Let now $v_0, v \in \mathrm{Im}(\theta_k)$ with $v_0 \neq 0$ (if G_k/G_{k+1} is trivial the result is clear). Since $\mathfrak{Q}^k/\mathfrak{Q}^{k+1}$ is a vector space of dimension 1 over $\mathcal{O}_L/\mathfrak{Q}$, we have $v = \lambda v_0$ for some $\lambda \in \mathcal{O}_L/\mathfrak{Q}$. Equation (2.2) shows that λ is fixed by G_{-1}. Since $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{Q}/\mathcal{O}_K/\wp) \cong G_{-1}/G_0$, we infer that $\lambda \in \mathcal{O}_K/\wp$. Thus $\mathrm{Im}(\theta_k)$ is contained in the $\mathcal{O}_K/\wp$-vector space spanned by v_0.

□

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

$$H_\wp := \{\sigma \in G \text{ such that } \forall \gamma \in \mathcal{O}_L,\ \sigma\gamma^q \equiv \gamma^q \bmod \wp\mathcal{O}_L\}$$

is a non trivial subgroup of G.

Proof. As before, let G_{-1} and G_k be the decomposition group and the ramification groups of a prime $\mathfrak{Q}$ over $\wp$ (since G is abelian, these groups do not depend on the choice of $\mathfrak{Q}$). Let $e = |G_0|$ and $(p) = \wp \cap \mathbb{Z}$. We write as before $e = e_0 p^a$ with $(e_0, p) = 1$. Assume first that $\wp$ is tamely ramified in L. Thus $e = e_0 = |G_0/G_1| \leq q$, by (2.1) of Proposition 2.2. Let $\sigma \in G_0$ and $\gamma \in \mathcal{O}_L$; then

$$(\sigma\gamma - \gamma)^q \in \mathfrak{Q}^q \subseteq \mathfrak{Q}^e$$

and

$$(\sigma\gamma - \gamma)^q \equiv \sigma\gamma^q - \gamma^q \bmod p\mathcal{O}_L \ .$$

This implies

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

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)

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

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

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

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 (2.1) of Proposition 2.2 we have $e \leq kq$.

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

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

As before, this implies

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

Thus $\{\mathbf{1}\} \neq G_{k-1} \subseteq H_\wp \subseteq G_0$.

□

3 A first lower bound

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

Lemma 3.1 *Let L be a number field and let ν 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 $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ and assume that $K(\alpha)$ is an abelian extension of K. Assume further*

$$K(\alpha) = K(\alpha^q) \; . \tag{3.1}$$

Then

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

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 ϕ be the Frobenius automorphism of $\mathfrak{Q}/\wp$, where $\mathfrak{Q}$ is any prime of L over $\wp$ (since L/K is abelian, ϕ does not depend on the choice of $\mathfrak{Q}$).

Let ν 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 $(\alpha\beta)^q \equiv \phi(\alpha\beta) \bmod \wp\mathcal{O}_L$ and $\beta^q \equiv \phi(\beta) \bmod \wp\mathcal{O}_L$. 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

$$\begin{aligned} |\alpha^q - \phi(\alpha)|_\nu &= |\beta|_\nu^{-q} |(\alpha\beta)^q - \phi(\alpha\beta) + (\phi(\beta) - \beta^q)\phi(\alpha)|_\nu \\ &\leq |\beta|_\nu^{-q} \max\left(|(\alpha\beta)^q - \phi(\alpha\beta)|_\nu, |\beta^p - \phi(\beta)|_\nu |\phi(\alpha)|_\nu\right) \\ &\leq \max(1, |\alpha|_\nu)^q p^{-1/e} \max(1, |\phi(\alpha)|_\nu) \; . \end{aligned}$$

Suppose now that ν 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 α 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:

$$\begin{aligned}
0 &= \sum_{\substack{\nu\nmid\infty\\ \nu\nmid\wp}} \frac{[L_\nu:\mathbb{Q}_\nu]}{[L:\mathbb{Q}]}\log|x|_\nu + \sum_{\nu\,|\,\wp}\frac{[L_\nu:\mathbb{Q}_p]}{[L:\mathbb{Q}]}\log|x|_\nu + \sum_{\nu\,|\,\infty}\frac{[L_\nu:\mathbb{Q}_\nu]}{[L:\mathbb{Q}]}\log|x|_\nu\\
&\le \sum_{\nu}\frac{[L_\nu:\mathbb{Q}_\nu]}{[L:\mathbb{Q}]}(q\log^+|\alpha|_\nu+\log^+|\phi(\alpha)|_\nu) - \frac{\log p}{e}\sum_{\nu\,|\,\wp}\frac{[L_\nu:\mathbb{Q}_p]}{[L:\mathbb{Q}]}\\
&\qquad + \sum_{\nu\,|\,\infty}\frac{[L_\nu:\mathbb{Q}_\nu]}{[L:\mathbb{Q}]}\log 2\\
&= qh(\alpha)+h(\phi(\alpha)) - \frac{[K_\wp:\mathbb{Q}_p]\log p}{e[L:\mathbb{Q}]}\sum_{\nu\,|\,\wp}\frac{[L_\nu:\mathbb{Q}_p]}{[K_\wp:\mathbb{Q}_p]} + (\log 2)\sum_{\nu\,|\,\infty}\frac{[L_\nu:\mathbb{Q}_\nu]}{[L:\mathbb{Q}]}\,.
\end{aligned}$$

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

$$\sum_{\nu\,|\,\infty}\frac{[L_\nu:\mathbb{Q}_\nu]}{[L:\mathbb{Q}]}=1, \qquad \sum_{\nu\,|\,\wp}\frac{[L_\nu:\mathbb{Q}_p]}{[K_\wp:\mathbb{Q}_p]}=[L:K]$$

and $[K_\wp:\mathbb{Q}_p]=ef$. Thus

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

i. e.

$$h(\alpha)\ge \frac{\log\left(q^{1/d}/2\right)}{q+1}\ge\frac{\log\left(q^{1/d}/2\right)}{2q}\,.$$

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

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

Assume $\sigma(\alpha)^q=\alpha^q$. Since $\sigma(\alpha)\neq\alpha$ we have $K(\alpha^q)\subsetneq K(\alpha)$, which contradicts hypothesis (3.1).

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

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

Therefore

$$h(\alpha)\ge\frac{\log\left(q^{1/d}/2\right)}{2q}\,.$$

□

4 Radicals reduction

In this section we show that a slightly weaker version of Proposition 3.2 still holds without assuming (3.1). 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 $k \geq 60B\log B$. Then, for every subgroup H of $(\mathbb{Z}/(k))^*$ of index $\leq B$, there are $h_1, h_2 \in H$ such that*

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

Proof. Write an integer decomposition $k = k_1k_2$ 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 $(\mathbb{Z}/(k))^* \cong (\mathbb{Z}/(k_1))^* \times (\mathbb{Z}/(k_2))^* = G_1G_2$, 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 γ is Euler's constant and in the product l runs through prime numbers. Since $B \geq 5$,

$$\frac{k_1}{\varphi(k_1)} = \prod_{l \leq B^5}\left(1 - \frac{1}{l}\right)^{-1} < 5e^{\gamma}\left(1 - \frac{1}{(5\log 5)^2}\right)^{-1}\log B < 10\log B\ , \qquad (4.1)$$

where φ is Euler's function. Let s be the integer defined by

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

We have $|H_1| \geq \varphi(k_1)/B$, so by (4.1) and since $k_1 \geq 60B\log B$,

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

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

$$x_1 < x_2 < x_3 < x_4 \quad \text{and} \quad x_4 - x_1 < \frac{k_1}{s} \leq 60B\log B\ .$$

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

Let now l^a be the 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 kernel of the reduction $r\colon (\mathbb{Z}/(l^a))^* \to (\mathbb{Z}/(l))^*$ modulo l.

Remark that the index $b = [(\mathbb{Z}/(l^a))^* : H(l)] \leq B$. Since $[(\mathbb{Z}/(l^a))^* : V(l)] = l - 1$ and $l > B$, we have $V(l) \subseteq H(l)$. Thus $r(H(l))$ has index b in $\mathbb{F}_l^*$ and $r(H(l)) = \{u^b \,|\, u \in \mathbb{F}_l^*\}$. The curve $X^b - Y^b = t$ over $\mathbb{F}_l$ has a plane projective closure which is nonsingular, because $0 < t < l$, and whose genus is $g \leq (B-1)(B-2)/2$. By a celebrated theorem of Weil (but more elementary methods amply suffice for this case) the curve has then at least $l + 1 - 2g\sqrt{l}$ projective points. Hence at least $l + 1 - 2g\sqrt{l} - 3b$ of them lie in the affine piece and have $XY \neq 0$; in turn, since $B \geq 5$, this lower bound is $> l - 2g\sqrt{l} - 3B \geq B^5 - B^2 B^{5/2} - 3B > 0$. Hence there is x_l so that the images of both $x_l, x_l + t$ lie in the reduction of $H(l)$ and hence in $H(l)$, which contains the kernel of reduction.

Finally, it suffices to pick with the Chinese Theorem an h_2 congruent to x modulo k_1 and to x_l modulo l^a, for each l dividing k_2, and to put $h_1 := h_2 + t$.

□

We introduce the following notations. Let $\alpha \in \overline{\mathbb{Q}}$ such that $K(\alpha)/K$ is a Galois extension. We define

$$\Gamma_\alpha := \{\rho \in \mathrm{Gal}(K(\alpha)/K) \ : \ \rho(\alpha)/\alpha \in \boldsymbol{\mu}\}.$$

Note that Γ_α is a subgroup of $\mathrm{Gal}(K(\alpha)/K)$. We let $L_\alpha := K(\alpha)^{\Gamma_\alpha}$ be its fixed field; note that $K(\alpha)/L_\alpha$ is Galois with group Γ_α.

We need the following simple generalization of a classical lemma in Kummer's theory. Given an integer k we let ζ_k be a primitive k-th root of unity.

Lemma 4.2 *Let $\alpha \in \overline{\mathbb{Q}}$ and let k be a positive integer such that any root of unity of the shape $\rho(\alpha)/\alpha$ for $\rho \in \Gamma_\alpha$ has order dividing k. Let $\sigma \in \mathrm{Gal}(K(\zeta_k)/K)$ and assume that $K(\alpha)/K$ is abelian. Then for any extension $\tilde{\sigma} \in \mathrm{Gal}(K(\alpha, \zeta_k)/K)$ we have*

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

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

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

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

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

□

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 $q = N\wp$, $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ and assume that $K(\alpha)$ is an abelian extension of K. Then*

$$h(\alpha) \geq \frac{\log\left(q^{1/d}/2\right)}{364d\log(3d)q} .$$

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 $\mathrm{Gal}(K(\zeta_k)/K)$ 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 σ_1, $\sigma_2 \in \mathrm{Gal}(K(\zeta_k)/K)$ 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

$$\tilde{\sigma}_2(\alpha) = c\,\alpha^g \tilde{\sigma}_1(\alpha) \tag{4.2}$$

with $c \in L_\alpha$. We recall that

$$2 < g < 180d\log(3d) . \tag{4.3}$$

We want to apply Proposition 3.2 to c. To do that we need that $c \notin \boldsymbol{\mu}$ and that $K(c) = K(c^q)$. Let us verify these requirements.

- $c \notin \boldsymbol{\mu}$. Assume the contrary. Then, by (4.2),

  $$gh(\alpha) = h(\alpha^g) = h(\tilde{\sigma}_2(\alpha)/\tilde{\sigma}_1(\alpha)) \leq 2h(\alpha) .$$

  Since $g > 2$ we get $\alpha \in \boldsymbol{\mu}$. Contradiction.

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

  Denote by $\tilde{\tau} \in \mathrm{Gal}(K(\alpha)/K)$ an arbitrary extension of τ and set $\eta := \tilde{\tau}(\alpha)/\alpha$. Now, apply (4.2) 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 $\eta \in \boldsymbol{\mu}$. But then $\tilde{\tau} \in \Gamma_\alpha$ by definition. Since however $c \in L_\alpha$ and since Γ_α fixes L_α we have a contradiction because $\theta \neq 1$.

The hypotheses of Proposition 3.2 are therefore fulfilled. We get the lower bound

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

By (4.2) and by the upper bound $g < 180d\log(3d)$ (see (4.3)) we have

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

Thus

$$h(\alpha) \geq \frac{\log\left(q^{1/d}/2\right)}{364d\log(3d)q}\ .$$

□

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,

$$h(\alpha) > \frac{\log(3/2)}{364d\log(3d)\cdot 3^{d^2+d}} \geq 3^{-d^2-2d-6}\ ,$$

since $\log(3/2) \geq 1/3$ and $364d\log(3d) \leq 3^{d+5}$.

□

5 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

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

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

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

This prove

Proposition 5.1

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

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 ζ be a root of unity and let $\alpha \in K(\zeta)^* \backslash \boldsymbol{\mu}$. 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

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

□

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 $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ 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 $\boldsymbol{\mu}_n \cap K^* = \boldsymbol{\mu}_r$; thus r is the number of n-roots of unity contained in K. Since $K(\alpha)/K$ is abelian, the extension $K(\alpha, \zeta_n)/K$ 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, $r \leq c_4\varphi(r)\log\log 3\varphi(r) \leq c_4\varphi(r)\log\log 5d$. Thus

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

□

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 $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ such that $K(\alpha)/K$ is an abelian extension. Then*

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

References

[Am-Dv] F. Amoroso and R. Dvornicich. – "A Lower Bound for the Height in Abelian Extensions." *J. Number Theory* **80** (2000), no 2, 260–272.

[Am-Za] F. Amoroso and U. Zannier. – "A relative Dobrowolski's lower bound over abelian extensions." *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **29** (2000), no. 3, 711–727.

[Am-De] F. Amoroso and E. Delsinne. – "Une minoration relative explicite pour la hauteur dans une extension d'une extension ablienne". Diophantine geometry, CRM Series, 4, Ed. Norm., Pisa, 2007, 1–24

[Ami-Da] A. Pacheco and S. David – "Abelian Lehmer problem for Drinfeld modules". *Journal de théorie des Nombres de Bordeaux.* To appear.

[Ba] M. Baker – "Lower bounds for the canonical height on elliptic curves over abelian extensions". *Int. Math. Res. Not.* **29** (2003), 1571–1589.

[Ba-Si] M. Baker and J. Silverman, "Lower bound for the canonical height on abelian varieties over abelian extensions". *Math. Res. Lett.* **11** (2004), no. 2-3, 377–396.

[Ca] J. W. S. Cassels – "Local fields". London Mathematical Society Student Texts, **3**. Cambridge University Press, Cambridge, 1986.

[Co] H. Cohen– "Advanced topics in computational number theory". Graduate Texts in Mathematics, **193**. Springer-Verlag, New York, 2000.

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

[Ra] N. Ratazzi – "Théorème de Dobrowolski-Laurent pour les extensions abéliennes sur une courbe elliptique à multiplication complexe". *Int. Math. Res. Not.*, **58** (2004), 3121–3152.

[Ro-Sc] J. B. Rosser and L. Schoenfeld. "Approximate formulas for some functions of prime numbers"., Ill. J. Math., **6**, 64–94 (1962).

[Se] J. P. Serre – "Corps locaux". Hermann, Paris, 1968. 245 pp.

[Sc] A. Schinzel – "Abelian binomials, power residues and exponential congruences". *Acta Arith.* **32** (1977), no. 3, 245–274.

[Si] J. Silverman – "A lower bound for the canonical height on elliptic curves over abelian extensions". *J. Number Theory* **104** (2004), no. 2, 353–372.