Bulletin of the London Mathematical Society Advance Access published March 22, 2010

Bull. London Math. Soc. Page 1 of 10
doi:10.1112/blms/bdq008

A uniform relative Dobrowolski's lower bound over abelian extensions

Francesco Amoroso and Umberto Zannier

Abstract

Let L/K be an abelian extension of number fields. We prove a 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 $\overline{\mathbb{Q}}$ and let $\boldsymbol{\mu}$ be the set of roots of units. Let L be an abelian extension of the rational field. In a joint work with Dvornicich [2] the first author, for any $\alpha \in L^* \setminus \boldsymbol{\mu}$, proved that

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

giving a positive answer to a question of Bombieri and the second author. This result was generalized by several authors replacing $\overline{\mathbb{Q}}^*$ by more complicated group varieties (see [4, 5, 9, 14]).

Later, in a joint paper [3], we proved a 'relative' result, which combines the lower bound (1.1) with a celebrated result of Dobrowolski [8]. Let L be an abelian extension of a number field K and let $\alpha \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}$. Then

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

where $D = [L(\alpha) : L]$ and where $c(K) > 0$ (see [10] for a generalization to elliptic curves). More recently, the first author and Delsinne [1] have refined the error term in this inequality and computed 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

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

As a very special case of the result of [3], we have $\gamma_{\mathrm{ab}}(K) \geqslant c(K)$ and, by the results of [1], we have $c(K)$ 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 $\gamma_{\mathrm{ab}}(K)$ may be bounded below in terms *only* of the degree of K, namely the following.

Problem 1.1. Is it true that $\gamma_{\mathrm{ab}}(K) \geqslant f([K:\mathbb{Q}])$ for some positive function $f(\cdot)$?

We give a positive answer to this question.

Received 21 June 2009; revised 23 November 2009.

2000 *Mathematics Subject Classification* 11G50 (primary), 11Jxx (secondary).

THEOREM 1.2. *Let K be a number field of degree d over $\mathbb{Q}$ and let $\alpha \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}$. Assume that $K(\alpha)/K$ is 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 we have the following corollary.

COROLLARY 1.3. *Let L be a dihedral extension of the rational field and let $\alpha \in L^* \setminus \boldsymbol{\mu}$. Then*

$$h(\alpha) \geqslant 3^{-14}.$$

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

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

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 [**3**, 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 follows from the papers [**2**, **3**] (see especially Lemma 3.2 therein).

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

2. *Ramification*

We recall some basic facts 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 kth ramification group

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

Then $G \supseteq G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \ldots$ Moreover, for all $k \geqslant 0$, we have that 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 $\mathfrak{Q}$ (that is, $\pi \in \mathfrak{Q} \setminus \mathfrak{Q}^2$). We consider the map

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

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

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

which sends σ to the class of $\sigma(\pi)/\pi - 1$. Then (cf. [7, Proposition 10.1.14]) we have the following proposition.

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 us now assume that G_{-1} is an abelian group. Then we have the following proposition.

PROPOSITION 2.2. (i) *The image of θ_0 is contained in $(\mathcal{O}_K/\wp)^*$.*
(ii) *For all $k \geqslant 1$, the image of θ_k is contained in a $\mathcal{O}_K/\wp$ vector space of dimension 1. In particular*

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

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

Proof. For (i), see [6, Corollary 2, p. 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 $\alpha := \tau\pi/\pi - 1$. Also let $\sigma(\pi) = x\pi$ 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 $x \notin \mathfrak{Q}$, it follows that $\tau(x)^{-1}x \equiv 1(\pi^{k+1})$. 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

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

Now let $v_0, v \in \mathrm{Im}(\theta_k)$ with $v_0 \neq 0$ (if G_k/G_{k+1} is trivial, then 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 $e = e_0 = |G_0/G_1| \leqslant q$, 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 us now assume $p\,|\,e$. By the Hasse–Arf theorem (see [**12**, § 7, Theorem 1′, p. 101]) we have

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

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

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

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 $e \leqslant kq$.

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 [**2**].

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 $\alpha \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}$ and assume that $K(\alpha)$ is an abelian extension of K. Assume further*

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

Then

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

Proof. Let $(p) = \wp \cap \mathbb{Z}$ and let $e = e(\wp/p)$ and $f = f(\wp/p)$ be respectively 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 as to induce on $\mathbb{Q}$ one of the standard places. We shall estimate $|\alpha^q - \phi(\alpha)|_\nu$. Suppose to start with that $\nu \mid \wp$.

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 $|\gamma|_\nu \leqslant p^{-1/e}$. Using the ultrametric inequality, we deduce that

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

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

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

Finally, if $\nu \mid \infty$, then we have

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

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 that $h(\alpha) = 0$. We apply the product formula to x as follows:

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

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

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

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

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

that is

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

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 be 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 that

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

Assume that $\sigma(\alpha)^q = \alpha^q$. 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

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

Therefore, we have

$$h(\alpha) \geqslant \frac{\log\left(q^{1/d}/2\right)}{2q}. \qquad \square$$

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

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

Proof. Write an integer decomposition $k = k_1k_2$, where k_1 is divisible only by primes bounded by 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 $i = 1,2$ consider $H_i := H \cap G_i$, and hence $[G_i : H_i] \leqslant B$.

By the corollary to Theorem 7 of [**11**], for any $x > 1$, we have

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

where γ is Euler's constant and in the product l runs through prime numbers. Since $B \geqslant 5$, it follows that

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

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

$$\tfrac{1}{3}|H_1| - 1 \leqslant s < \tfrac{1}{3}|H_1|.$$

We have $|H_1| \geqslant \varphi(k_1)/B$, and hence by (4.1) and since $k_1 \geqslant 60B\log B$, it follows that

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

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

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

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

Now let 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 $r : (\mathbb{Z}/(l^a))^* \to (\mathbb{Z}/(l))^*$ modulo l. Remark that the index $b = [(\mathbb{Z}/(l^a))^* : H(l)] \leqslant B$. 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 $r(H(l)) = \{u^b \mid u \in \mathbb{F}_l^*\}$. The curve $X^b - Y^b = t$ over $\mathbb{F}_l$ has a plane projective closure which is non-singular, because $0 < t < l$, and whose genus is $g \leqslant (B-1)(B-2)/2$. 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 $B \geqslant 5$, this lower bound is greater than $l - 2g\sqrt{l} - 3B \geqslant B^5 - B^2B^{5/2} - 3B > 0$. Hence there is x_l so that the images of both x_l and $x_l + t$ lie in the reduction of $H(l)$ and hence in $H(l)$, which contains the kernel of reduction.

Finally, it suffices to pick by 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 consider $h_1 := h_2 + t$. □

We introduce the following notation. 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 kth 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 $u \in \mathbb{Z}$. Consider $\alpha' = \tilde{\sigma}\alpha$; 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 $q = N\wp$, $\alpha \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}$ and assume that $K(\alpha)$ is an abelian extension of K. Then*

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

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 at most $[K : \mathbb{Q}] = d$. We choose $B = 3d \geqslant 6$ in Lemma 4.1. Since $k \geqslant 180d\log(3d)$, 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. For this purpose we need to check that (i) $c \notin \boldsymbol{\mu}$ and that (ii) $K(c) = K(c^q)$. Let us verify these requirements.

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

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

Since $g > 2$, we get $\alpha \in \boldsymbol{\mu}$, which is a contradiction.

(ii) $K(c) = K(c^q)$: 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 non-trivial 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 $gh(\eta) \leqslant 2h(\eta)$ which implies that $h(\eta) = 0$. Hence $\eta \in \boldsymbol{\mu}$; but then $\tilde{\tau} \in \Gamma_\alpha$ by definition. However, since $c \in L_\alpha$ 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

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

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

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

Thus

$$h(\alpha) \geqslant \frac{\log(q^{1/d}/2)}{364d\log(3d)q}. \qquad \square$$

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

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

Thus, by proposition 4.3, we have

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

since $\log(3/2) \geqslant 1/3$ and $364d\log(3d) \leqslant 3^{d+5}$. $\square$

5. *Further remarks*

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

(a) The ‘natural’ generalization of Lehmer’s conjecture, namely

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

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, we have

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

Therefore

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

This proves the following proposition.

PROPOSITION 5.1. *We have*

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

(b) For *cyclotomic* extensions of a number field K of degree d, we can deduce from the main results of [**1**, **3**] a lower bound for the height sharper than Theorem 1.2.

PROPOSITION 5.2. *Let ζ be a root of unity and let $\alpha \in K(\zeta)^* \setminus \boldsymbol{\mu}$. Then*

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

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 [**1**] there exists an absolute constant $c_2 > 0$ such that

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

(c) The example of (a) 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 $\alpha \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}$ such that $\alpha^n \in K$ for some positive integer n. Then, if $K(\alpha)/K$ is abelian, we have*

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

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 [**13**, 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 [**1**], we have

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

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

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

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

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

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

References

1. 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, MathSciNet, 2007) 1–24.
2. F. AMOROSO and R. DVORNICICH, 'A lower bound for the height in Abelian extensions', *J. Number Theory* 80 (2000) 260–272.
3. F. AMOROSO and U. ZANNIER, 'A relative Dobrowolski's lower bound over abelian extensions', *Ann. Scuola Norm. Super Pisa Cl. Sci.* (4) 29 (2000) 711–727.
4. M. BAKER, 'Lower bounds for the canonical height on elliptic curves over abelian extensions', *Int. Math. Res. Not.* 29 (2003) 1571–1589.
5. M. BAKER and J. SILVERMAN, 'Lower bound for the canonical height on abelian varieties over abelian extensions', *Math. Res. Lett.* 11 (2004) 377–396.
6. J. W. S. CASSELS, *Local fields*, London Mathematical Society Student Texts 3 (Cambridge University Press, Cambridge, 1986).
7. H. COHEN, *Advanced topics in computational number theory*, Graduate Texts in Mathematics 193 (Springer, New York, 2000).
8. E. DOBROWOLSKI, 'On a question of Lehmer and the number of irreducible factors of a polynomial', *Acta Arith.* 34 (1979) 391–401.
9. A. PACHECO and S. DAVID, 'Abelian Lehmer problem for Drinfeld modules', *Int. J. Number Theory* 4 (2008), no. 6, 1043–1067.
10. 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.
11. J. B. ROSSER and L. SCHOENFELD, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math.* 6 (1962) 64–94.
12. J. P. SERRE, *Corps locaux* (Hermann, Paris, 1968), 245pp.
13. A. SCHINZEL, 'Abelian binomials, power residues and exponential congruences', *Acta Arith.* 32 (1977) 245–274.
14. J. SILVERMAN, 'A lower bound for the canonical height on elliptic curves over abelian extensions', *J. Number Theory* 104 (2004) 353–372.

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

Umberto Zannier
Scuola Normale Superiore
Piazza dei Cavalieri, 7
56126 Pisa
Italy