A lower bound for the height in abelian extensions

A lower bound for the height in abelian extensions

Francesco Amoroso

Dipartimento di Matematica, Università di Torino
Via Carlo Alberto 10, 10123 Torino, Italy

and

Roberto Dvornicich

Dipartimento di Matematica, Università di Pisa
Via F. Buonarroti 2, 56127 Pisa, Italy

We produce an absolute lower bound for the height of the algebraic numbers (different from zero and from the roots of unity) lying in an abelian extension of the rationals. The proof rests on elementary congruences in cyclotomic fields and on Kronecker-Weber theorem.

§1 Introduction.

Using Weil's height (the logarithmic and absolute height), the famous Lehmer problem [Le 1933] reads as follows: does there exist a positive constant c such that for any algebraic number α, $\alpha \neq 0$ and α not a root of unity, we have

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha):\mathbb{Q}]} \quad ? \tag{1}$$

This problem is still open, the best unconditional lower bound in this direction being a theorem of Dobrowolski [Do 1979]. However, in some special cases not only inequality (1) is true, but it can also be sharpened. Assume for instance that $\mathbb{L}$ is a "kroneckerian field" (i.e. either a totally real number field or a totally complex quadratic extension of such a field); then, as a special case of a more general result, Schinzel proved that

$$h(\alpha) \geq \frac{1}{2}\log\frac{1+\sqrt{5}}{2} \approx 0.2406 \tag{2}$$

if $\alpha \in \mathbb{L}^*$ *and* $|\alpha| \neq 1$ (apply [Sc 1973], Corollary $1'$, p. 386, to the linear polynomial $P(z) = z - \alpha$) . In particular, by Kronecker's theorem, this inequality hold if α is an algebraic integer different from zero and from the roots of unity. Although this additional assumption makes no harm if one is interested in proving inequality (1) (since the Weil's height of a non-integer α is trivially $\geq (\log 2)/[\mathbb{Q}(\alpha):\mathbb{Q}]$), it may happen that non-integers in kroneckerian fields have Weil's height smaller than $\frac{1}{2}\log\frac{1+\sqrt{5}}{2}$. For instance, the roots of the irreducible polynomial $2x^4 - 3x^2 + 2 \in \mathbb{Z}[x]$ belong to an abelian extension and have absolute value 1, hence their height is $\frac{\log 2}{4} \approx 0.1732$.

When the extension $\mathbb{L}/\mathbb{Q}$ is Galois, $\mathbb{L}$ is kroneckerian if and only if the complex conjugation lies in the center of the Galois group. In this situation there are other proofs of (2) (see for instance [La 1980] and [Fl 1994]) all of these relying on the following idea: $\beta = \alpha\overline{\alpha}$ is totally positive and $\neq 1$, otherwise all of its conjugates would have absolute value 1 and then, since α is an integer, it would be a root of unity. So the condition that α is an integer is essential for this kind of argument.

Assume further $\mathbb{L}/\mathbb{Q}$ abelian. In the paper quoted above [La 1980], Laurent uses the idea that the Frobenius automorphism relative to a prime ideal depends only on the underlying rational prime, to prove that $h(\alpha) \geq c(\mathbb{L})$ where $c(\mathbb{L})$ depends on the smallest non-ramified rational prime in $\mathbb{L}$ (although the proof is given explicitly only for integers, it can be easily adapted to the general case). In this paper we introduce a new idea which allows us to deal with ramified primes, thereby leading to an absolute lower bound for the height in abelian extensions. Our main result is the following:

Theorem.

Let $\mathbb{L}/\mathbb{Q}$ be an abelian extension and let $\alpha \in \mathbb{L}^*$, α not a root of unity. Then

$$h(\alpha) \geq \frac{\log 5}{12} \approx 0.1341.$$

We do not know what is the best possible lower bound, but certainly the constant $\frac{\log 5}{12}$ cannot be replaced by any number $> \frac{\log 7}{12}$ (see the example after the remarks following the proof of Corollary 2).

As a consequence of inequalities which hold also for non integers α, our method enables us to prove some results on lower bounds for the norm and the class group of abelian fields.

Notations. For a natural number $m \geq 3$ we denote by ζ_m a primitive m-root of unity and we let $\mathbb{K}_m = \mathbb{Q}(\zeta_m)$ be the m-th cyclotomic field of degree $\phi(m)$ over $\mathbb{Q}$. Since $\mathbb{K}_m = \mathbb{K}_{2m}$ for odd m, we shall assume that $m \not\equiv 2 \pmod 4$.

§2 Congruences and proof of the main result.

Lemma 1.

Let $\mathbb{K}$ be a number field and let ν be a non-archimedean place of $\mathbb{K}$. Then, for any $\alpha \in \mathbb{K}^*$ there exists an algebraic integer β such that $\beta\alpha$ is also integer and

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

Proof. Let Σ_0 be the set of non-archimedean places w of $\mathbb{K}$ such that $\max\{1, |\alpha|_w\} > 1$.

Let $\Sigma = \Sigma_0 \cup \{\nu\}$ and choose an arbitrary non-archimedean place w_0. By the "strong approximation theorem" (see [CF], Chapter II, § 15, page 67), there exists $\beta \in \mathbb{K}$ such that $|\beta - \alpha^{-1}|_w < \max\{1, |\alpha|\}^{-1}$ for any $w \in \Sigma$ and $|\beta|_w \leq 1$ if $w \notin \Sigma \cup \{w_0\}$. Using the ultrametric inequality, we deduce that

$$|\beta|_w = \max\{1, |\alpha|_w\}^{-1}$$

for any $w \in \Sigma$ and $|\beta|_w \leq 1$ if $w \notin \Sigma \cup \{w_0\}$. Therefore, $|\beta|_w \leq 1$ and $|\alpha\beta|_w \leq 1$ for any finite place w (and so β and $\alpha\beta$ are both integers) and $|\beta|_\nu = \max\{1, |\alpha|_\nu\}^{-1}$, since $\nu \in \Sigma$.

□

Lemma 2.

Let p be a rational prime. Then there exists $\sigma = \sigma_p \in \mathrm{Gal}(\mathbb{K}_m/\mathbb{Q})$ with the following two properties.

1) If $p \nmid m$, then

$$p \mid (\gamma^p - \sigma\gamma)$$

for any integer $\gamma \in \mathbb{K}_m$.

2) If $p \mid m$, then

$$p \mid (\gamma^p - \sigma\gamma^p)$$

for any integer $\gamma \in \mathbb{K}_m$. Moreover, if $\sigma\gamma^p = \gamma^p$ for some $\gamma \in \mathbb{K}_m$, then there exists a root of unity $\zeta \in \mathbb{K}_m$ such that $\zeta\gamma$ is contained in a proper cyclotomic subextension of $\mathbb{K}_m$.

Proof. Assume first that $p \nmid m$. Let $\sigma \in \mathrm{Gal}(\mathbb{K}_m/\mathbb{Q})$ be defined by $\sigma\zeta_m = \zeta_m^p$. For any integer $\gamma \in \mathbb{K}_m$ we have $\gamma = f(\zeta_m)$ for some $f \in \mathbb{Z}[x]$; hence

$$\gamma^p \equiv f(\zeta_m^p) \equiv f(\sigma\zeta_m) \equiv \sigma\gamma \pmod{p}.$$

Assume now that $p|m$. The Galois group $\mathrm{Gal}(\mathbb{K}_m/\mathbb{K}_{m/p})$ is cyclic of order $k = p$ or $k = p-1$ depending on whether $p^2|m$ or not. Let σ be one of its generators; hence $\sigma\zeta_m = \zeta_p\zeta_m$ for some primitive p-root of unity ζ_p. For any integer $\gamma = f(\zeta_m) \in \mathbb{Z}[\zeta_m]$, we have

$$\gamma^p \equiv f(\zeta_m^p) \equiv f(\sigma\zeta_m^p) \equiv \sigma\gamma^p \pmod{p}.$$

Suppose finally that $\sigma\gamma^p = \gamma^p$: then $\sigma\gamma = \zeta_p^u\gamma$ for some integer u. It follows that $\sigma(\gamma/\zeta_m^u) = \gamma/\zeta_m^u$, hence γ/ζ_m^u belongs to the fixed field $\mathbb{K}_{m/p}$, as desired.

□

Proposition 1.

Let $p \geq 3$ be a prime number and let $\alpha \in \mathbb{K}_m^*$, α not a root of unity. Then

$$h(\alpha) \geq \begin{cases} \frac{\log(p/2)}{p+1}, & \textit{if } p \nmid m; \\ \frac{\log(p/2)}{2p}, & \textit{otherwise.} \end{cases}$$

Proof.

Let $\mathbb{K} = \mathbb{K}_m$ and let ν be a place of $\mathbb{K}$ dividing p (with $|p|_\nu = 1/p$). By Lemma 1, there exists an integer $\beta \in \mathbb{K}$ such that $\alpha\beta$ is integer and

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

Let $\sigma = \sigma_p$ the homomorphism given by Lemma 2. Assume first that $p \nmid m$; then

$$|(\alpha\beta)^p - \sigma(\alpha\beta)|_\nu \leq \frac{1}{p} \quad \text{and} \quad |\beta^p - \sigma\beta|_\nu \leq \frac{1}{p}.$$

Using the ultrametric inequality, we deduce that

$$\begin{aligned} |\alpha^p - \sigma\alpha|_\nu &= |\beta|_\nu^{-p} |(\alpha\beta)^p - \sigma(\alpha\beta) + (\sigma\beta - \beta^p)\sigma\alpha|_\nu \\ &\leq |\beta|_\nu^{-p} \max\big(|(\alpha\beta)^p - \sigma(\alpha\beta)|_\nu, |\beta^p - \sigma\beta|_\nu |\sigma\alpha|_\nu\big) \\ &\leq \frac{1}{p} \max(1, |\alpha|_\nu)^p \max(1, |\sigma\alpha|_\nu). \end{aligned}$$

Moreover $\alpha^p \neq \sigma\alpha$, since α is not a root of unity $\big($see for instance [Do], Lemma 2 i)$\big)$. We now apply the product formula to $\gamma = \alpha^p - \sigma\alpha$.

$$\begin{aligned} 0 &= \sum_{\substack{\nu \nmid \infty \\ \nu \nmid p}} \frac{[\mathbb{K}_\nu : \mathbb{Q}_\nu]}{[\mathbb{K} : \mathbb{Q}]} \log|\gamma|_\nu + \sum_{\nu \mid p} \frac{[\mathbb{K}_\nu : \mathbb{Q}_\nu]}{[\mathbb{K} : \mathbb{Q}]} \log|\gamma|_\nu + \sum_{\nu \mid \infty} \frac{[\mathbb{K}_\nu : \mathbb{Q}_\nu]}{[\mathbb{K} : \mathbb{Q}]} \log|\gamma|_\nu \\ &\leq \sum_{\nu \nmid \infty} \frac{[\mathbb{K}_\nu : \mathbb{Q}_\nu]}{[\mathbb{K} : \mathbb{Q}]} (p \log^+ |\alpha|_\nu + \log^+ |\sigma\alpha|_\nu) - \sum_{\nu \mid p} \frac{[\mathbb{K}_\nu : \mathbb{Q}_\nu]}{[\mathbb{K} : \mathbb{Q}]} \log p \\ &\qquad + \sum_{\nu \mid \infty} \frac{[\mathbb{K}_\nu : \mathbb{Q}_\nu]}{[\mathbb{K} : \mathbb{Q}]} (p \log^+ |\alpha|_\nu + \log^+ |\sigma\alpha|_\nu + \log 2) \\ &= p h(\alpha) + h(\sigma\alpha) - \log p + \log 2 \\ &= (p+1) h(\alpha) - \log(p/2). \end{aligned}$$

Therefore,

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

Assume now that $p \mid m$: again by Lemma 2, we have

$$|(\alpha\beta)^p - \sigma(\alpha\beta)^p|_\nu \leq \frac{1}{p} \quad \text{and} \quad |\beta^p - \sigma\beta^p|_\nu \leq \frac{1}{p}.$$

Using the ultrametric inequality, we find

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

Moreover, we can assume $\alpha^p \neq \sigma\alpha^p$. Otherwise, again by Lemma 2, there exists a root of unity $\zeta \in \mathbb{K}$ such that $\zeta\alpha$ is contained in a proper cyclotomic subextension of $\mathbb{K}$; hence $h(\alpha) = h(\zeta\alpha)$ and, by induction, $h(\zeta\alpha) \geq \frac{\log(p/2)}{2p}$. Applying the product formula to $\gamma = \alpha^p - \sigma\alpha^p$ as in the first part of the proof, we get

$$0 \leq ph(\alpha) + ph(\sigma\alpha) - \log p + \log 2 = 2ph(\alpha) - \log(p/2).$$

Therefore, in this case,

$$h(\alpha) \geq \frac{\log(p/2)}{2p}.$$

□

The previous proposition gives, *via* Kronecker-Weber's theorem, the lower bound

$$h(\alpha) \geq \frac{\log(5/2)}{10} \approx 0.09163$$

for the height of a non-zero algebraic number α (α not a root of unity) lying in an abelian extension. To reach the better lower bound announced in the introduction, we study the special case $p = 2$:

Lemma 3.

Let $\sigma = \sigma_2$ be as before, and let $\gamma \in \mathbb{K}_m$ be an integer.

1) If $4 \nmid m$, then

$$4 \mid (\gamma^4 - \sigma\gamma^2).$$

2) If $4 \mid m$, then

$$4 \mid (\gamma^2 - \sigma\gamma^2).$$

Proof. The first assertion immediately follows from Lemma 2, since

$$\gamma^4 - \sigma\gamma^2 = (\gamma^2 - \sigma\gamma) \cdot \big((-\gamma)^2 - \sigma(-\gamma)\big).$$

For the second, let $\gamma = \sum_i a_i\zeta_m^i$ be an integer of $\mathbb{K}_m$. Then $\sigma\gamma = \sum_i (-1)^i a_i \zeta_m^i$, hence $\sigma\gamma - \gamma$ and $\sigma\gamma + \gamma$ are both divisible by 2, so $\sigma\gamma^2 - \gamma^2$ is divisible by 4.

□

Proposition 2.

Let $\alpha \in \mathbb{K}_m^*$. We have:

1) If $4 \mid m$ and there is no root of unity $\zeta \in \mathbb{K}_m$ such that $\alpha\zeta$ is not contained in any proper cyclotomic subextension of $\mathbb{K}_m$, then

$$h(\alpha) \geq \frac{\log 2}{4}.$$

2) If $4 \nmid m$ and α is not a root of unity, then

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

Proof. Assume first that $4 \mid m$ and $\alpha\zeta$ is not contained in any proper cyclotomic subextension of $\mathbb{K}_m$ for any root of unity $\zeta \in \mathbb{K}_m$. Then the proof of the inequality $h(\alpha) \geq \frac{\log 2}{4}$ can be obtained as the proof of the inequality $h(\alpha) \geq \frac{\log(p/2)}{2p}$ in Proposition 1, simply replacing the relation $p \mid (\gamma^p - \sigma\gamma^p)$ by the stronger relation $4 \mid (\gamma^2 - \sigma\gamma^2)$.

Assume now that $4 \nmid m$ and α is not a root of unity. Then the argument of the first part of the proof of Proposition 1 gives (replacing the relation $p \mid (\gamma^p - \sigma\gamma^p)$ by $4 \mid (\gamma^4 - \sigma\gamma^2)$):

$$h(\alpha) \geq \frac{2\log 2 - \frac{2}{D}\sum_{v|\infty} \log^+ |\alpha^4 - \sigma\alpha^2|_v}{6},$$

where $D = \phi(m)$. Similarly, considering $\alpha^8 - \sigma\alpha^4$ one obtains

$$h(\alpha) \geq \frac{3\log 2 - \frac{2}{D}\sum_{v|\infty} \log^+ |\alpha^8 - \sigma\alpha^4|_v}{12}.$$

If $|\alpha| \neq 1$, the result of Schinzel [Sc 1973] quoted in the introduction gives the better lower bound

$$h(\alpha) \geq \frac{1}{2}\log\frac{\sqrt{5}+1}{2}.$$

Therefore we can assume $|\alpha| = 1$ (and hence $|\alpha|_v = 1$ for all $v|\infty$). Putting $\sigma\alpha^2 = \alpha^4 e^{it}$ and $|1 - e^{it}|_v = |1 - e^{it_v}|$, we get

$$h(\alpha) \geq \frac{1}{12}\max\{\frac{2}{D}\sum_{v|\infty}(4\log 2 - 2\log^+\sqrt{2 - 2\cos t_v}), \frac{2}{D}\sum_{v|\infty}(3\log 2 - \log^+\sqrt{4 - 4\cos^2 t_v})\}.$$

Let $x_v = \cos t_v$; to conclude the proof we quote the following lemma:

Lemma 4.

Let $x_1, \ldots, x_k \in (-1, 1)$ and consider the following real functions:

$$f(x) = 4\log 2 - 2\log^+\sqrt{2 - 2x}, \quad g(x) = 3\log 2 - \log^+\sqrt{4 - 4x^2}.$$

Then

$$\frac{1}{k}\max\left\{\sum_{j=1}^{k} f(x_j), \sum_{j=1}^{k} g(x_j)\right\} \geq \log 5.$$

Proof. Let

$$I_1 = \left\{x \mid -1 < x \leq -\frac{\sqrt{3}}{2}\right\}, \quad I_2 = \left\{x \mid -\frac{\sqrt{3}}{2} < x \leq \frac{1}{2}\right\}, \quad I_3 = \left\{x \mid \frac{1}{2} < x < 1\right\}.$$

We have

$$\begin{cases} f(x) \geq 2\log 2, & \text{if } x \in I_1; \\ f(x) = 4\log 2, & \text{if } x \in I_3; \end{cases} \qquad \begin{cases} g(x) = 3\log 2, & \text{if } x \in I_1; \\ g(x) \geq 3\log 2 - \log\sqrt{3}, & \text{if } x \in I_3; \end{cases}.$$

Moreover, f and g are convex functions in I_2. Hence,

$$\frac{1}{k}\sum_j f(x_j) \geq \frac{k_1}{k}\cdot 2\log 2 + \frac{k_2}{k}\cdot f\left(\frac{1}{k_2}\sum_{x_j\in I_2} x_j\right) + \frac{k_3}{k}\cdot 4\log 2;$$
$$\frac{1}{k}\sum_j g(x_j) \geq \frac{k_1}{k}\cdot 3\log 2 + \frac{k_2}{k}\cdot g\left(\frac{1}{k_2}\sum_{x_j\in I_2} x_j\right) + \frac{k_3}{k}\cdot (3\log 2 - \log\sqrt{3}),$$

where k_l denotes the number of j for which $x_j \in I_l$. Let

$$F(x_0; y_1, y_2, y_3) = y_1\cdot 2\log 2 + y_2\cdot f(x_0) + y_3\cdot 4\log 2,$$
$$G(x_0; y_1, y_2, y_3) = y_1\cdot 3\log 2 + y_2\cdot g(x_0) + y_3\cdot (3\log 2 - \log\sqrt{3}).$$

We infer that

$$\frac{1}{k}\max\left\{\sum_{j=1}^{k} f(x_j), \sum_{j=1}^{k} g(x_j)\right\} \geq \min_{\substack{x_0\in I_2 \\ y_1+y_2+y_3=1}} \max\{F(x_0; y_1, y_2, y_3), G(x_0; y_1, y_2, y_3)\}$$
$$= \log 5.$$

□

We now combine propositions 1 and 2. We observe that, for primes $p \geq 13$, we have

$$\frac{\log(p/2)}{p+1} < \frac{\log 5}{12} < \frac{\log(11/2)}{12} < \frac{\log(5/2)}{6} < \frac{\log(7/2)}{8} < \frac{\log 2}{4}.$$

Therefore, we define

$$c(m) = \begin{cases} \frac{\log(7/2)}{8}, & \text{if } 7 \nmid m; \\ \frac{\log(5/2)}{6}, & \text{if } 7 \mid m \text{ and } 5 \nmid m; \\ \frac{\log(11/2)}{12}, & \text{if } 35 \mid m \text{ and } 11 \nmid m; \\ \frac{\log 5}{12}, & \text{if } 385 \mid m. \end{cases}$$

Theorem 1.

Let $\alpha \in \mathbb{K}_m^*$. Then:

1) If α is not a root of unity,

$$h(\alpha) \geq c(m);$$

2) If $4|m$ and there is no root of unity $\zeta \in \mathbb{K}_m$ such that $\alpha\zeta$ is contained in a proper cyclotomic subextension of $\mathbb{K}_m$, we have the stronger lower bound

$$h(\alpha) \geq \frac{\log 2}{4}.$$

In particular we find, *via* Kronecker-Weber's theorem, the result announced in the introduction.

§3 Corollaries.

Now we state some corollaries of our main theorem. We start by giving a lower bound for the norm of an algebraic integer:

Corollary 1.

Let $\gamma \neq 0$ be an integer lying in an abelian extension $\mathbb{L}$ of $\mathbb{Q}$. Then, if $\gamma/\overline{\gamma}$ is not a root of unity,

$$\frac{\log |\mathrm{N}_{\mathbb{Q}}^{\mathbb{L}}\gamma|}{[\mathbb{L}:\mathbb{Q}]} \geq \frac{\log 5}{12}.$$

Moreover the constant $\frac{\log 5}{12}$ can be replaced by $c(m)$ if $\mathbb{L} = \mathbb{K}_m$ and by $\frac{\log 2}{4}$ if $\mathbb{L} = \mathbb{K}_m$ and if there is no root of unity $\zeta \in \mathbb{K}_m$ such that $\alpha\zeta$ is contained in a proper cyclotomic subextension of $\mathbb{K}_m$.

Proof. Let $\alpha = \overline{\gamma}/\gamma$. By the product formula,

$$\begin{aligned} h(\alpha) &= \sum_{\nu\nmid\infty} \frac{[\mathbb{L}_\nu : \mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]} \log^+ |\alpha|_\nu \leq -\sum_{\nu\nmid\infty} \frac{[\mathbb{L}_\nu : \mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]} \log |\gamma|_\nu \\ &= \sum_{\nu|\infty} \frac{[\mathbb{L}_\nu : \mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]} \log |\gamma|_\nu \quad = \frac{\log |\mathrm{N}_{\mathbb{Q}}^{\mathbb{L}}\gamma|}{[\mathbb{L}:\mathbb{Q}]}. \end{aligned}$$

Now, apply Theorem 1.

□

Let β be a non-reciprocal algebraic number (i.e. such that β^{-1} is not a conjugate of β) of degree D. Smyth [Sm 1971], by using tools from complex analysis, proved that the height of β is $\geq \frac{\log \theta_0}{D} \approx \frac{0.2811}{D}$, where θ_0 is the smallest Pisot's number, *i.e.* the real root of the polynomial $x^3 - x - 1$. This result is optimal since $h(\theta_0) = \frac{\log \theta_0}{3}$. Corollary 1 allows us to reobtain, although in a slightly weaker form, Smyth's result:

Theorem (Smyth).

Let β be a non-reciprocal algebraic number of degree D. Then we have

$$h(\beta) \geq \frac{c}{D}$$

with $c = \frac{\log(7/2)}{8} \approx 0.1565$.

Proof. We may assume that β is an algebraic integer (since otherwise $h(\beta) \geq \frac{\log 2}{D}$). Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of β and let $p \neq 7$ be a prime number $\geq 2D+3$. Let also $\gamma = f(\zeta_p)$. We start by proving that $\gamma/\overline{\gamma}$ is not a root of unity. Assume the contrary. Then there exists an integer j such that $f(\zeta_p) = \pm\zeta_p^j f(\zeta_p^{-1})$; hence

$$\zeta_p^D f(\zeta_p) = \pm\zeta_p^j f^*(\zeta_p),$$

where $f^*(x) = x^D f(x^{-1})$ is the reciprocal polynomial of f. Without loss of generality, we can assume $-1 \leq j \leq p-2$. By assumption on β, the polynomial

$$g(x) = x^{\max\{D-j,0\}} f(x) \pm x^{\max\{j-D,0\}} f^*(x)$$

is not zero; on the other hand $g(\zeta_p) = 0$ and g has degree bounded by

$$D + |D-j| \leq \max\{2D+1, p-2\} < p-1,$$

a contradiction. The hypothesis of Corollary 1 is therefore satisfied and we find:

$$\frac{\log |\mathrm{N}_{\mathbb{Q}}^{\mathbb{K}_p} f(\zeta_p)|}{p-1} \geq \frac{\log(7/2)}{8}.$$

On the other hand, denoting by $\beta_1, \dots, \beta_D$ the conjugates of β,

$$|\mathrm{N}_{\mathbb{Q}}^{\mathbb{K}_p} f(\zeta_p)| = \left|\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(\beta)} \frac{\beta^p - 1}{\beta - 1}\right| \leq |\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(\beta)}(\beta^p - 1)| \leq 2^D \prod_{j=1}^{D} \max\{|\beta_j|^p, 1\}.$$

Hence

$$\log |\mathrm{N}_{\mathbb{Q}}^{\mathbb{K}_p} f(\zeta_p)| \leq D\big(\log 2 + p h(\beta)\big).$$

Taking into account the previous lower bound for this norm we find

$$D h(\beta) \geq \left(1 - \frac{1}{p}\right) \frac{\log(7/2)}{8} - \frac{D \log 2}{p}.$$

Now, we let $p \to +\infty$.

□

We remark that in the preceding proof we have used only the first bound given in Proposition 1, namely the lower bound $h(\alpha) \geq \frac{\log(7/2)}{8}$ for a non-root of unity $\alpha \in \mathbb{K}_p^*$ with $p \neq 7$.

Next we state a result about the class group of abelian extensions of $\mathbb{Q}$.

Corollary 2.

Let $\mathbb{L}$ be an abelian extension of $\mathbb{Q}$ of degree D and let p be a rational prime (possibly ramified); let also denote by f its inertal degree. Assume that p splits completely in a quadratic imaginary extension $\mathbb{K}$ of $\mathbb{Q}$ contained in $\mathbb{L}$ and denote by δ the order of a prime over p in the class group of $\mathbb{L}$. Then

$$\frac{f\delta \log p}{D} \geq \frac{\log 5}{12}.$$

Moreover the constant $\frac{\log 5}{12}$ can be replaced by $c(m)$ if $\mathbb{L} = \mathbb{K}_m$ and by $\frac{\log 2}{4}$ if $\mathbb{L} = \mathbb{K}_m$ and if $4|m$ and $f = 1$.

Proof. Let $\wp$ be a prime of $\mathbb{L}$ over p and let δ be its order in the class group of $\mathbb{L}$. Hence $\wp^\delta = (\gamma)$ for some integer $\gamma \in \mathbb{L}$. Let $\mathbb{L}^+$ the maximal real subfield of $\mathbb{L}$; since $\mathbb{K}\mathbb{L}^+ = \mathbb{L}$, we have :

$$\wp \neq \overline{\wp}.$$

Therefore, denoting by ν the finite place of $\mathbb{L}$ corresponding to $\wp$,

$$h(\gamma/\overline{\gamma}) = \frac{[\mathbb{L}_\nu : \mathbb{Q}_\nu]}{D} \log |\gamma|_\nu = \frac{f\delta \log p}{D} > 0.$$

Now, applying Theorem 1, we find $\frac{f\delta \log p}{D} \geq \frac{\log 5}{12}$ and $\frac{f\delta \log p}{D} \geq c(m)$ if $\mathbb{L} = \mathbb{K}_m$.

Assume now $f = 1$ and $\mathbb{L} = \mathbb{K}_m$ for some m divisible by 4. Let $\zeta \in \mathbb{K}_m$ be a root of unity and let $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ be such that $\sigma(\zeta\gamma/\overline{\gamma}) = \zeta\gamma/\overline{\gamma}$. Then we have the equality of ideals $(\sigma\gamma)(\overline{\gamma}) = (\gamma)(\sigma\overline{\gamma})$; since $(\gamma) \neq (\overline{\gamma})$, it follows from unique factorization that $(\sigma\gamma) = (\gamma)$ and hence σ must be the identity. So $\alpha = \zeta\gamma/\overline{\gamma}$ is not contained in any proper subextension of $\mathbb{K}_m$ and the second part of Theorem 1 applies.

□

Remarks.

1) The condition about the splitting of p is necessary: the prime $p = 157$ has inertial degree 1 in the maximal real subfield $\mathbb{K}_{79}^+$ and $\frac{\log 157}{(79-1)/2} \approx 0.1296 < \frac{\log 5}{12}$, but (at least assuming GRH) $\mathbb{K}_{79}^+$ has class number one (see [Wa], Tables, p. 352).

2) In the last part of Corollary 2 we cannot avoid the hypothesis $f = 1$. Consider for instance the cyclotomic field $\mathbb{L} = \mathbb{K}_{84}$. Then $p = 7$ splits as the product of 2 principal primes with ramification index 6 and inertial degree $f = 2$. Moreover 7 splits completely in $\mathbb{Q}(\sqrt{-3})$, but we have $\frac{2\log 7}{\phi(84)} < \frac{\log 2}{4}$.

Corollary 2 is almost optimal. Consider the cyclotomic field $\mathbb{K}_{21}$ of class number one; the prime $p = 7$ splits as the product of 2 primes with ramification index 6 and inertial degree 1. We have $\frac{\log 7}{\phi(21)} = \frac{\log 7}{12} \approx 0.1621$ and $c(21) = \frac{\log(5/2)}{6} \approx 0.1527$. This produces the best example we know of an algebraic number of "small" height lying in an abelian extension: $\alpha = \gamma/\overline{\gamma}$, where (γ) is a prime of $\mathbb{K}_{21}$ over $p = 7$, has height

$$h(\alpha) = \frac{\log 7}{12}.$$

The complete list of cyclotomic fields having class number one is well-known (see [MM 1976]):

$\mathbb{K}_m$ *has class number one if and only if* m *is one of the following twenty-nine numbers:*

$$3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.$$

As an application of Corollary 2, we can show in a totally elementary way, that for any "reasonably" small m (say $m \leq 10^4$) which does not belong to the previous list, the field $\mathbb{K}_m$ has class number > 1. Let $p(m, 1)$ be the smallest prime satisfying $p \equiv 1 \pmod{m}$. A simple computation (done by a small personal computer) shows that if $m \leq 10^4$ does not belong to the previous list of twenty-nine numbers and if $m \neq 23, 31, 39, 56, 72$, then

$$\frac{\log p(m,1)}{\phi(m)} < \begin{cases} \frac{\log 2}{4}, & \text{if } 4 \mid m; \\ c(m), & \text{otherwise,} \end{cases}$$

and therefore $\mathbb{K}_m$ has class number > 1. The case $m = 23$ can be treated directly; for $m = 31$ we remark that the prime 2 is unramified in $\mathbb{K}_{31}$ and splits as a product of six primes having inertial degree 5. Since

$$\frac{5 \log 2}{30} = \frac{\log 2}{6} < \frac{\log(7/2)}{8},$$

we find that also $\mathbb{K}_{31}$ has class number > 1. The cases $m = 39$, $m = 56$ and $m = 72$ can be settled in a similar way, by considering the splitting of $p = 13$, $p = 2$ and $p = 3$, respectively.

To prove the "only if" part of the quoted result on the class number of cyclotomic field, we need a non-trivial upper bound for $p(m, 1)$, say $\log p(m, 1) < 0.13 \cdot \phi(m)$ for $m > m_0$, for a "reasonable" and explicit absolute constant m_0. For large m, a much stronger inequality is known: a celebrate (and deep) result of Linnick assert that $p(m, 1) < m^L$ where L is an effective constant.

REFERENCES

[CF 1967] J. W. S. Cassels and A. Fröhlich. – Algebraic number theory; Proceedings of an instructional conference organized by the London Mathematical Society, Academic Press, London–New-York, (1967).

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

[Fl 1994] V. Flammang. – "Mesures de polynômes. Application au diamètre transfini entier"; Thèse. Université de Metz.

[La 1980] M. Laurent. – "Sur la mesure de Mahler de certaines classes d'entiers algébriques"; unpublished (1980).

[Le 1933] D.H. Lehmer. – “Factorization of certain cyclotomic functions”; Ann. of Math., **34** (1933), 461–479.

[MM 1976] J.M. Masley, H.L Montgomery.–“Cyclotomic fields with unique factorization”; J. Reine Angew. Math. 286/287 (1976), 248–256.

[Sc 1973] 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), 329–361.

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

[Wa 1982] L.C. Washington. – “Introduction to Cyclotomic Fields”; Springer–Verlag, New York (1982).