Lower bounds for the height and size of the ideal class group in CM-fields

Published version:

DOI:10.1007/s00605-002-0499-7

(Article begins on next page)

Monatsh. Math. 138, 85–94 (2003)
DOI 10.1007/s00605-002-0499-7

Monatshefte für
Mathematik
Printed in Austria

Lower Bounds for the Height and Size of the Ideal Class Group in CM-Fields

By

Francesco Amoroso[1] and **Roberto Dvornicich**[2]

[1] Université de Caen, France
[2] Università di Pisa, Italy

Received September 10, 2001; in revised form April 5, 2002
Published online November 18, 2002

Abstract. We prove that, under the assumption of the Generalized Riemann Hypothesis, the exponent of the ideal class group of a CM-field goes to infinity with its absolute discriminant. This gives a positive answer to a question raised by Louboutin and Okazaki [4].

2000 Mathematics Subject Classification: 11R29, 11R21
Key words: CM fields, class group

1. Introduction

In a recent talk given at the University of Caen, S. Louboutin conjectured that the exponent of the ideal class group of a CM field goes to infinity with its absolute discriminant. Subsequently, he has also succeeded to prove a weak version of his conjecture. Let K be a CM field, and denote by d_K, Δ_K and E_K the degree, the discriminant and the exponent of the ideal class group of K, respectively. Then Louboutin and Okazaki [4] proved that, restricting to the CM fields with given degree $d_K = d$, one has

$$E_K \gg_d \frac{\log|\Delta_K|}{\log\log|\Delta_K|}, \tag{1}$$

where the constant involved depends on d only.

In this paper we develop the methods introduced in [2] and we investigate further the links between lower bounds for the height and the class group of CM-fields; this will give, in particular, a complete positive answer to Louboutin's conjecture.

Consider first the simpler case of cyclotomic extensions. Let ζ_m be a primitive m-root of unity and denote by E_m the exponent of the ideal class group of the cyclotomic field $\mathbb{Q}(\zeta_m)$. Corollary 2 of [2] gives the lower bound

$$E_m \geqslant \frac{\log 5}{12} \times \frac{\phi(m)}{\log p},$$

where p is a rational prime which splits completely in $\mathbb{Q}(\zeta_m)$. It is well-known that p splits completely in $\mathbb{Q}(\zeta_m)$ if and only if $p \equiv 1 \pmod m$, and therefore, by a celebrated result of Linnik, there exists an effective and absolute constant $L > 0$ and a rational prime $p < m^L$ which splits completely in $\mathbb{Q}(\zeta_m)$. Using Mertens' inequality $\phi(m) \gg \frac{m}{\log\log m}$, one gets the lower bound

$$E_m \geqslant \frac{\log 5}{12L} \times \frac{\phi(m)}{\log m} \gg \frac{m}{(\log m)(\log\log m)}$$

that depends only on m.

Let now K be a complex abelian extension, and let d_K, Δ_K and E_K be as above. Then, again by Corollary 2 of [2],

$$E_K \geqslant \frac{\log 5}{12} \times \frac{d_K}{\log p}, \tag{2}$$

where p is a rational prime which splits completely in K. Using the Generalized Riemann Hypothesis, we can find (see [3]) a rational prime $p \ll (\log|\Delta_K|)^2$ which splits completely in K; hence

$$E_K \gg \frac{d_K}{\log\log|\Delta_K|},$$

where the implicit constant in $\gg$ is absolute and effectively computable. To obtain an estimate depending only on the degree d_K, or only on the discriminant Δ_K, it is enough to show that, if the exponent E_K is small, then Δ_K is bounded in terms of d_K. We shall use a result of Silverman (see Lemma 4.3) to prove that

$$E_K \gg \frac{\max\left\{d_K^{-1}\log|\Delta_K| - \log d_K, d_K\right\}}{\log\log|\Delta_K|}.$$

Therefore, E_K goes to infinity with $|\Delta_K|$. More precisely,

$$E_K \gg \max\left\{\frac{\sqrt{\log|\Delta_K|}}{\log\log|\Delta_K|}, \frac{d_K}{\log d_K}\right\}.$$

Now, let us consider the case when K is a CM-field, *i.e.* an imaginary quadratic extension of a totally real field. As K need not to be abelian, we cannot apply inequality (2). However, the argument of Corollary 2 in [2] works also in this case, provided that one has some lower bound for the height of elements of K. Using the general estimate for the height given in [1], we can prove that for any $\varepsilon > 0$,

$$E_K \gg_\varepsilon \frac{\max\left\{d_K^{-1}\log|\Delta_K| - \log d_K, d_K^{1-\varepsilon}\right\}}{\log\log|\Delta_K|} \tag{3}$$

where the implicit constant in $\gg_\varepsilon$ depends only on ε and is effectively computable. Therefore, E_K goes again to infinity with $|\Delta_K|$. More precisely, if $\varepsilon < 1/2$ we have

$$\max\left\{d_K^{-1}\log|\Delta_K| - \log d_K, d_K^{1-\varepsilon}\right\} \gg_\varepsilon \max\{(\log|\Delta_K|)^{1/2-\varepsilon}, d_K^{1-\varepsilon}\};$$

thus, for any $\varepsilon' > 0$ the exponent E_K is bounded from below by a positive quantity depending on ε' times

$$\max\{(\log|\Delta_K|)^{1/2-\varepsilon'}, d_K^{1-\varepsilon'}\}.$$

It is to be remarked that our result (3) includes inequality (1) as a special case.

We shall deduce these bounds from a more general result concerning the size of the multiplicative relations in the class group of a CM-field. Let G be a group and let l be a positive integer. We define $\mathscr{M}_G(l)$ as the least integer A such that for all $g_1, \ldots, g_l \in G$ there exists $\underline{a} \in \mathbb{Z}^l \backslash \{0\}$ such that $g_1^{a_1} \cdots g_l^{a_l} = e$ and $\sum_j |a_j| \leqslant A$. Then we have:

Theorem 1.1. *Let $K/\mathbb{Q}$ be a CM-field and let G be the ideal class group of K. Let also l be a positive integer. Then, for any $\varepsilon > 0$ and under the assumption of the Generalized Riemann Hypothesis for the Dedekind zeta function of K, we have*

$$\mathscr{M}_G(l) \gg_\varepsilon \frac{\max\left\{d_K^{-1} \log|\Delta_K| - \log d_K, d_K^{1-\varepsilon}\right\}}{\log l + \log\log|\Delta_K|}.$$

Moreover, if $K/\mathbb{Q}$ is abelian, then the conclusion holds also for $\varepsilon = 0$.

This theorem gives some information on the invariants of the ideal class group of a CM field (we recall that the positive integers $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the invariants of a finite abelian group G if G is isomorphic to the direct product of cyclic groups of order $\lambda_1, \lambda_2, \ldots, \lambda_n$ with $\lambda_n | \lambda_{n-1} | \cdots | \lambda_1$).

Corollary 1.2. *Let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be the invariants of G and put $\lambda_{n+1} = 1$. Let also $\varepsilon > 0$ and $j \in \{1, \ldots, n+1\}$. Then, again under the assumption of the Generalized Riemann Hypothesis for the Dedekind zeta function of K*

$$\lambda_j \log\left(\frac{\lambda_1 \cdots \lambda_{j-1}}{\lambda_j^{j-1}} \log|\Delta_K|\right) \gg_\varepsilon \max\left\{d_K^{-1} \log|\Delta_K| - \log d_K, d_K^{1-\varepsilon}\right\}.$$

Moreover, if $K/\mathbb{Q}$ is abelian, then the above conclusions hold also for $\varepsilon = 0$.

By choosing $j = 1$ we find the announced lower bounds for the exponent. On the other hand, the choice $j = n+1$ gives a 'good' lower bound for the class number of a CM-field:

Corollary 1.3. *Let $\varepsilon \in (0, 1/2)$; then, still under the assumption of the Generalized Riemann Hypothesis for the Dedekind zeta function of K,*

$$\log h_K \gg_\varepsilon \max\left\{d_K^{-1} \log|\Delta_K| - \log d_K, d_K^{1-\varepsilon}\right\}.$$

Hence

$$\log h_K \gg_\varepsilon \max\{(\log|\Delta_K|)^{1/2-\varepsilon}, d_K^{1-\varepsilon}\}.$$

Moreover, if $K/\mathbb{Q}$ is abelian, then the above conclusions hold also for $\varepsilon = 0$.

These bounds for h_K must be compared with [5], Theorem 2, p. 279 and with [8], Theorem 2, p. 136.

2. Analytic Results

Throughout the paper $c_1, c_2, \ldots$ will be positive absolute constants which are effectively computable.

Let K be any number field and let $x > 1$. We denote by $\pi'_K(x)$ the number of primes $P \subseteq \mathcal{O}_K$ of degree 1, non-ramified over $\mathbb{Q}$, and such that $|N_{\mathbb{Q}}^K P| \leqslant x$. The following lemma is an easy corollary of a very special case of the effective version of the Čebotarev Density Theorem proved by Lagarias and Odlyzko (see [3]).

Lemma 2.1. *If the Generalized Riemann Hypothesis holds for the Dedekind zeta function of K, then for every* $x \geqslant c_1(\log|\Delta_K|)^2(\log\log|\Delta_K|)^4$,

$$\pi'_K(x) \geqslant c_2\frac{x}{\log x}.$$

Proof. Applying Theorem 1.1 of [3] (with $L = K$), we get the following estimate for the cardinality $\pi_K(x)$ of the primes $P \subseteq \mathcal{O}_K$ of norm $\leqslant x$,

$$\pi_K(x) \geqslant \mathrm{Li}(x) - c_3\big((\sqrt{x}+1)\log|\Delta_K| + d_K\log x\big).$$

Using the well-known lower bound $\log|\Delta_K| \geqslant c_4 d_K$, the asymptotic equality $\mathrm{Li}(x) \sim \frac{x}{\log x}$ and our assumption on x, we get

$$\pi_K(x) \geqslant c_5\frac{x}{\log x}.$$

If p is a rational prime ramified in K, then p divides $|\Delta_K|$. Since in K there are at most d_K primes over p, we obtain

$$\#\{P \subseteq \mathcal{O}_K,\ P \text{ ramified over } \mathbb{Z}\} \leqslant d_K\frac{\log|\Delta_K|}{\log 2} \leqslant c_6(\log|\Delta_K|)^2 \leqslant c_7\frac{x}{(\log x)^4}.$$

Moreover, if P has degree >1 and norm $\leqslant x$, then the rational prime p under P satisfies $p \leqslant \sqrt{x}$. Hence

$$\#\{P \subseteq \mathcal{O}_K,\ P \text{ of degree} > 1,\ N_{\mathbb{Q}}^K P \leqslant x\} \leqslant d_K\pi(\sqrt{x}) \leqslant c_8\frac{x}{(\log x)^2}.$$

Now Lemma 2.1 easily follows. □

3. Algebraic Results

Lemma 3.1. *Let K be a number field, let p be a rational prime and P be an ideal prime above p such that* $e(P|p) = e_P$, $f(P|p) = f_P$. *Let L be the normal closure of K in* $\overline{\mathbb{Q}}$. *Then*

$$|\{\sigma(P\mathcal{O}_L)|\sigma \in \mathrm{Gal}(L/\mathbb{Q})\}| \geqslant \frac{d_K}{e_Pf_P}.$$

Proof. Let $d = d_K$ and $[L:K] = s$, so that $[L:\mathbb{Q}] = ds$. Since $L/\mathbb{Q}$ is normal, the factorization into prime ideals of $p\mathcal{O}_L$ can be written as

$$p\mathcal{O}_L = (Q_1,\ldots,Q_r)^e$$

where all Q_i have the same inertial degree f and $ref = ds$. By the multiplicativity of the ramification index and of the inertial degree in towers, we have, possibly after a renumbering of $Q_1,\ldots,Q_r$,

$$(P\mathcal{O}_L)^{e_P} = (Q_1,\ldots,Q_h)^e$$

where $\frac{hef}{e_Pf_P} = s$. The Galois group $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the set $\{Q_1,\ldots,Q_r\}$, hence the number of conjugates of P is not less that $\frac{r}{h} = \frac{d}{e_Pf_P}$. □

We recall that a CM-field is an imaginary quadratic extension of a totally real field. If K is a CM-field, we denote by K^+ the totally real field $K \cap \mathbb{R}$.

Lemma 3.2. *Let K be a CM-field, let p be a rational prime, and assume that P is a prime of K above p such that $e(P|p) = f(P|p) = 1$. Then $\bar{P} \neq P$.*

Proof. Let $Q = P \cap K^+$. Then the factorization of $Q\mathcal{O}_K$ is of type $Q = PP'$, where $P' \neq P$. On the other hand, P and P' are conjugate under the Galois group $\mathrm{Gal}(K/K^+)$. Since this Galois group consists of the identity and of the complex conjugation, we have $P' = \bar{P}$. □

CM-fields are characterized by the following property: let $\alpha \in K$ and assume that $|\alpha| = 1$; then for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have $|\sigma\alpha| = 1$. This property will play a central role in the sequel. The link between primes of small norm and algebraic numbers of small height in CM-fields is given by the following proposition, which generalizes Corollary 2 of [2].

Proposition 3.3. *Let K be a CM-field and let $P_1, \dots, P_k \subseteq \mathcal{O}_K$ be primes of degree 1 and not ramified over $\mathbb{Q}$. Assume that $P_i \neq P_j$ and $P_i \neq \bar{P}_j$ for $i \neq j$. Let also $a_1, \dots, a_k$ be integers such that $P_1^{a_1} \cdots P_l^{a_k} = (\gamma)$ is a principal ideal and let $\alpha = \gamma/\bar{\gamma}$. Then:*

$$d_K h(\alpha) = \sum_{j=1}^{k} |a_j| \log N_{\mathbb{Q}}^{K} P_j.$$

Moreover, if $(a_1, \dots, a_l) \neq (0, \dots, 0)$ and if the rational primes $P_1 \cap \mathbb{Z}, \dots, P_k \cap \mathbb{Z}$ are all distinct, then α is a generator of K over $\mathbb{Q}$.

Proof. Since $P_j \neq \bar{P}_j$ by Lemma 3.2, the prime ideals $P_1, \dots, P_k, \bar{P}_1, \dots, \bar{P}_k$ are distinct. For $j = 1, \dots, k$ let v_j be the place relative to P_j and $\bar{v}_j$ be the place relative to $\bar{P}_j$. Then

$$|\alpha|_{v_j}^{n_{v_j}} = (N_{\mathbb{Q}}^{K} P_j)^{-a_j} \quad \text{and} \quad |\alpha|_{\bar{v}_j}^{n_{\bar{v}_j}} = (N_{\mathbb{Q}}^{K} P_j)^{a_j}.$$

Hence, $\log\max\{|\alpha|_{v_j}^{n_{v_j}}, 1\} + \log\max\{|\alpha|_{\bar{v}_j}^{n_{\bar{v}_j}}, 1\} = |a_j| \log N_{\mathbb{Q}}^{K} P_j$. Moreover $|\alpha| = 1$, hence $|\alpha|_v = 1$ for any archimedean place v, since K is a CM-field. Therefore,

$$dh(\alpha) = \sum_{\substack{v \in M_K \\ v|\infty}} \log\max\{|\alpha|_v^{n_v}, 1\}|\} + \sum_{\substack{v \in M_K \\ v\nmid\infty}} \log\max\{|\alpha|_v^{n_v}, 1\}|\} = \sum_{j=1}^{k} |a_j| \log N_{\mathbb{Q}}^{K} P_j.$$

We now assume that the rational primes $P_1 \cap \mathbb{Z}, \dots, P_k \cap \mathbb{Z}$ are all distinct and we show that α is a generator of K over $\mathbb{Q}$. Since $\alpha \in K$, it is enough to show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geqslant d_K$. Let L be the normal closure of K in $\overline{\mathbb{Q}}$ and assume $a_1 \neq 0$; by Lemma 3.1, $P_1\mathcal{O}_L$ has at least d_K distinct conjugate ideals $\sigma_1(P_1\mathcal{O}_L), \dots, \sigma_{d_K}(P_1\mathcal{O}_L)$. Assume that, for some $i, j \in \{1, \dots, d_K\}$, we have $\sigma_i(\alpha) = \sigma_j(\alpha)$. Then

$$\begin{aligned}\sigma_i(P_1\mathcal{O}_L)^{a_1}\sigma_i(\bar{P}_1\mathcal{O}_L)^{-a_1} \cdots \sigma_i(P_k\mathcal{O}_L)^{a_k}\sigma_i(\bar{P}_k\mathcal{O}_L)^{-a_k} \\ = \sigma_j(P_1\mathcal{O}_L)^{a_1}\sigma_j(\bar{P}_1\mathcal{O}_L)^{-a_1} \cdots \sigma_j(\bar{P}_k\mathcal{O}_L)^{a_k}\sigma_j(\bar{P}_k\mathcal{O}_L)^{-a_k}.\end{aligned}$$

Since $P_1 \cap \mathbb{Z}, \dots, P_k \cap \mathbb{Z}$ are all distinct, we must have

$$\sigma_i(P_1\mathcal{O}_L)^{a_1}\sigma_i(\bar{P}_1\mathcal{O}_L)^{-a_1} = \sigma_j(P_1\mathcal{O}_L)^{a_1}\sigma_j(\bar{P}_1\mathcal{O}_L)^{-a_1}.$$

Since $P_1 \neq \bar{P}_1$ by Lemma 3.2, the ideals $\sigma_i(P_1\mathcal{O}_L)^{a_1}$ and $\sigma_i(\bar{P}_1\mathcal{O}_L)^{a_1}$ are coprime; by unique factorization of the ideals in $\mathcal{O}_L$, we get $\sigma_i(P_1\mathcal{O}_L)^{a_1} = \sigma_j(P_1\mathcal{O}_L)^{a_1}$, whence $\sigma_i(P_1\mathcal{O}_L) = \sigma_j(P_1\mathcal{O}_L)$ and $i=j$. It follows that α has at least d_K distinct conjugates in $\overline{\mathbb{Q}}$, whence $[\mathbb{Q}(\alpha):\mathbb{Q}] \geqslant d_K$, as claimed. This completes the proof of the proposition. □

4. Diophantine Results

We now state three "diophantine results" concerning lower bounds for the Weil absolute logarithmic height $h(\cdot)$, that we shall need later for the proof of our main result.

Lemma 4.3. *Let K be a number field. Then, for any generator α of K we have*:

$$h(\alpha) \geqslant \frac{d_K^{-1}\log|\Delta_K| - \log d_K}{2(d_K-1)}.$$

Proof. The lemma is a special case of Theorem 2 of [6]. It is also an easy consequence of the inequality $|\Delta_K| \leqslant |\mathrm{disc}(\alpha)|$ (see [7]) and of Hadamard's inequality. □

The next two lower bounds for the height are respectively the main result of [2] (Theorem at p. 261) and of [1] (Theorem 1.6, p. 148).

Theorem 4.4. *Let $K/\mathbb{Q}$ be an abelian extension and let $\alpha \in K^*$, α not a root of unity. Then*

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

Theorem 4.5. *Let $K/\mathbb{Q}$ be any number field and let $\alpha_1,\dots,\alpha_m \in K^*$ multiplicatively independent. Then*

$$\big(h(\alpha_1)\cdots h(\alpha_m)\big)^{1/m} \geqslant c_9(m) d_K^{-1/m}\log(3d_K)^{-k(m)}$$

where $c_9(m)$ and $k(m)$ are positive constant depending only on m.

5. Size of the Ideal Class Group in CM-Fields

We now prove Theorem 1.1.

I) We start by proving that

$$\mathcal{M}_G(l) \geqslant c_{10}\frac{d_K^{-1}\log|\Delta_K| - \log d_K}{\log l + \log\log|\Delta_K|} \tag{4}$$

for some positive absolute constant c_{10}. We choose

$$x = c_{11} l d_K \log(l d_K) + c_1(\log|\Delta_K|)^2(\log\log|\Delta_K|)^4,$$

where c_{11} is such that $c_2 x(\log x)^{-1} \geqslant l d_K$. Since there at most d_K distinct primes in K over a rational prime, by Lemma 2.1 we can find l distinct rational primes $p_1,\dots,p_l \leqslant x$ and l primes ideals $P_1,\dots,P_l \subseteq \mathcal{O}_K$ such that $P_i \cap \mathbb{Z} = (p_i)$ and $e(P_i|p_i) = f(P_i|p_i) = 1$ for $i=1,\dots,l$. Let g_i be the class of P_i in G and assume that there exists a non-trivial multiplicative relation

$$g_1^{a_1}\cdots g_l^{a_l}=1$$

with a_i integers. Let $A=\sum_i |a_i|$; by assumption, $P_1^{a_1}\cdots P_l^{a_l}=(\gamma)$ is a principal ideal. Let $\alpha=\gamma/\bar{\gamma}$; by Proposition 3.3, α is a generator of K over $\mathbb{Q}$ and

$$d_K h(\alpha)=\sum_{i=1}^{l}|a_i|\log N_{\mathbb{Q}}^{K}P_i\leqslant A\log x.$$

Remark that

$$\log x\leqslant c_{12}(\log l+\log d_K+\log\log|\Delta_K|)\leqslant c_{13}(\log l+\log\log|\Delta_K|),$$

since $\log|\Delta_K|\geqslant c_4 d_K$. Hence, by Lemma 4.3,

$$\frac{d_K^{-1}\log|\Delta_K|-\log d_K}{2(d_K-1)}\leqslant c_{13}A\frac{\log l+\log\log|\Delta_K|}{d_K}.$$

We get

$$A\geqslant c_{10}\frac{d_K^{-1}\log|\Delta_K|-\log d_K}{\log l+\log\log|\Delta_K|}.$$

II) We now prove that if $K/\mathbb{Q}$ is abelian, then

$$\mathscr{M}_G(l)\geqslant c_{14}\frac{d_K}{\log l+\log\log|\Delta_K|}\tag{5}$$

for some positive absolute constant c_{14}. We choose

$$x=c_{15}l\log l+c_1(\log|\Delta_K|)^2(\log\log|\Delta_K|)^4$$

where c_{15} is such that $c_2x(\log x)^{-1}\geqslant 2l$. By Lemma 2.1 we can find l primes ideals $P_1,\dots,P_l\subseteq\mathcal{O}_K$ of degree 1 and not ramified over $\mathbb{Q}$, such that

$$P_i\neq P_j\quad\text{and}\quad P_i\neq\bar{P}_j$$

for $i\neq j$. Let g_i be the class of P_i in G and assume that there exists a non-trivial multiplicative relation

$$g_1^{a_1}\cdots g_l^{a_l}=e$$

with a_i integers. Let $A=\sum_i |a_i|$; by assumption, $P_1^{a_1}\cdots P_l^{a_l}=(\gamma)$ is a principal ideal. Let $\alpha=\gamma/\bar{\gamma}$; by Proposition 3.3,

$$d_K h(\alpha)=\sum_{i=1}^{l}|a_i|\log N_{\mathbb{Q}}^{K}P_i\leqslant A\log x\leqslant c_{16}A(\log l+\log\log|\Delta_K|).$$

Hence, by Theorem 4.4,

$$c_{16}A(\log l+\log\log|\Delta_K|)\geqslant\frac{d_K\log 5}{12}.$$

We get

$$A\geqslant c_{14}\frac{d_K}{\log l+\log\log|\Delta_K|}.$$

III) We finally prove that for any $\varepsilon > 0$ we have

$$\mathscr{M}_G(l) \geqslant c_{17}(\varepsilon) \frac{d_K^{1-\varepsilon}}{\log l + \log\log|\Delta_K|} \tag{6}$$

for some positive constant $c_{17}(\varepsilon)$. Let $m = [1/\varepsilon] + 1$ and choose

$$x = c_{18} lm \log(lm) + c_1 (\log|\Delta_K|)^2 (\log\log|\Delta_K|)^4,$$

where c_{18} is such that $c_2 x (\log x)^{-1} \geqslant 2lm$. By Lemma 2.1 we can find $l \times m$ prime ideals $P_{ij} \subseteq \mathscr{O}_K (i = 1, \dots, l;\ j = 1, \dots, m)$ of degree 1 and not ramified over $\mathbb{Q}$, such that

$$P_{i_1 j_1} \neq P_{i_2 j_2} \quad \text{and} \quad P_{i_1 j_1} \neq \bar{P}_{i_2 j_2}$$

for $(i_1, j_1) \neq (i_2, j_2)$. Let g_{ij} be the class of P_{ij} in G and assume that for $j = 1, \dots, m$ there exists a non-trivial multiplicative relation

$$g_{1j}^{a_{1j}} \cdots g_{lj}^{a_{lj}} = e$$

with a_{ij} integers. Let $A = \max_j \sum_i |a_{ij}|$; by assumption, $P_{1j}^{a_{1j}} \cdots P_{lj}^{a_{lj}} = (\gamma_j)$ is a principal ideal. Let $\alpha_j = \gamma_j / \bar{\gamma}_j$; by Proposition 3.3,

$$d_K h(\alpha_j) = \sum_{i=1}^{l} |a_{ij}| \log N_{\mathbb{Q}}^K P_{ij} \leqslant A \log x \leqslant c_{19} A (\log l + \log m + \log\log|\Delta_K|).$$

Therefore

$$\big(h(\alpha_1) \cdots h(\alpha_m)\big)^{1/m} \leqslant c_{19} A \frac{\log l + \log m + \log\log|\Delta_K|}{d_K}.$$

Moreover, $\alpha_1, \dots, \alpha_m$ are multiplicatively independent (in fact, if $\alpha_1^{e_1} \cdots \alpha_m^{e_1} = 1$, then, again by Proposition 3.3, $0 = \sum_j |e_j| \sum_i |a_{ij}| \log N_{\mathbb{Q}}^K P_{ij}$ and hence $e_1 = \cdots = e_m = 0$). We can apply Theorem 4.5, obtaining

$$c_{19} A \frac{\log l + \log m + \log\log|\Delta_K|}{d_K} \geqslant c_9(m) d_K^{-1/m} \log(3d_K)^{-k(m)}.$$

By the choice of m, this yields

$$A \geqslant \frac{c_9(m) d_K^{1-1/m} \log(3d_K)^{-k(m)}}{c_{19}(\log l + \log m + \log\log|\Delta_K|)} \geqslant c_{17}(\varepsilon) \frac{d_K^{1-\varepsilon}}{\log l + \log\log|\Delta_K|}.$$

The conclusion of Theorem 1.1 follows from (4), (5) and (6). □

For the proof of Corollary 1.2 we need the following lemma.

Lemma 5.1. *Let G be a finite group of exponent E and order m. Then*

(i) $\mathscr{M}_G(1) = E$;
(ii) $\mathscr{M}_G(m) \leqslant 2$;
(iii) *Assume that G is abelian. If λ divides $o(G)$ then $\mathscr{M}_G(o(G/G_\lambda)) \leqslant 2\lambda$, where $G_\lambda = \{g \in G | g^\lambda = 1\}$.*

Proof. (i) is clear. As to (ii), let $g_1, \ldots, g_m \in G$. If $g_i = 1$ for some i, we have an obvious non-trivial multiplicative relation. Otherwise there exists i, j such that $i \neq j$ and $g_i g_j^{-1} = 1$. In any case there exists a non-trivial multiplicative relation $g_1^{a_1} \cdots g_m^{a_m} = 1$ with $\sum_j |a_j| \leqslant 2$. Finally, we have trivially

$$\mathscr{M}_G(o(G/G_\lambda)) \leqslant \lambda\, \mathscr{M}_{G/G_\lambda}(o(G/G_\lambda))$$

and hence (iii) follows from (ii). □

Proof of Corollary 1.2. We apply Lemma 5.1 (iii) by choosing $\lambda = \lambda_j$. Since $o(G_{\lambda_j}) = \lambda_j^j \lambda_{j+1} \cdots \lambda_n$, we obtain:

$$\mathscr{M}_G(\lambda_1 \cdots \lambda_{j-1}/\lambda_j^{j-1}) \leqslant 2\lambda_j.$$

By theorem 1.1 we have

$$2\lambda_j \geqslant c_{20}(\varepsilon) \frac{\max\left\{d_K^{-1}\log|\Delta_K| - \log d_K, d_K^{1-\varepsilon}\right\}}{\log(\lambda_1 \cdots \lambda_{j-1}/\lambda_j^{j-1}) + \log\log|\Delta_K|}$$

for some $c_{20}(\varepsilon) > 0$ depending only on ε. Therefore

$$\lambda_j \log\left(\frac{\lambda_1 \cdots \lambda_{j-1}}{\lambda_j^{j-1}} \log|\Delta_K|\right) \geqslant \frac{c_{20}(\varepsilon)}{2} \max\left\{d_K^{-1}\log|\Delta_K| - \log d_K, d_K^{1-\varepsilon}\right\}.$$

To prove the last assertion, remark that

$$\log\left(\frac{\lambda_1 \cdots \lambda_{j-1}}{\lambda_j^{j-1}} \log|\Delta_K|\right) \leqslant \log(\lambda_1 \cdots \lambda_{j-1}) + \log\log|\Delta_K|$$

and apply the inequality between the arithmetic and geometric mean. □

Remark. One could also prove Corollary 1.2 directly by using the effective version of the Cebotarev Density Theorem [3] in its full strength. We give a sketch of the argument in the simplest case when K is abelian. Let $H(K)$ be the Hilbert class field of K and let G be its Galois group over K, which we identify with the ideal class group of K. Let $L = L_j$ be the fixed field of G_{λ_j}; then L is an abelian unramified extension of K with Galois group G/G_{λ_j} and $|\Delta_L| = |\Delta_K|^{[L:K]}$. As in Lemma 2.1 we can find a prime ideal P of K such that

i) the class of P, viewed as an element of G, is in G_{λ_j}
ii) P is of degree 1 and non-ramified over $\mathbb{Q}$;
iii) the norm of P satisfies

$$|N_{\mathbb{Q}}^K P| \leqslant c_{21}(\log|\Delta_L|)^2(\log\log|\Delta_L|)^4.$$

Since the class of P is in G_{λ_j}, we have that $P^{\lambda_j} = (\gamma)$ is a principal ideal. By Proposition 3.3, $\alpha = \gamma/\bar{\gamma}$ is a generator of K with height

$$d_K h(\alpha) = \lambda_j \log N_{\mathbb{Q}}^K P.$$

A fortiori α is not a root of unity. Also remark that

$$\log|\Delta_L| = [L:K]\log|\Delta_K| = o(G/G_{\lambda_j})\log|\Delta_K| = \frac{\lambda_1 \cdots \lambda_{j-1}}{\lambda_j^{j-1}} \log|\Delta_K|.$$

Hence

$$d_K h(\alpha) \leqslant c_{22}\lambda_j \log\left(\frac{\lambda_1 \cdots \lambda_{j-1}}{\lambda_j^{j-1}} \log|\Delta_K|\right).$$

On the other hand, using Lemma 4.3 and Theorem 4.4,

$$d_K h(\alpha) \geqslant c_{23} \max\left\{d_K^{-1} \log|\Delta_K| - \log d_K, d_K\right\}.$$

Combining the upper and the lower bounds, we obtain the desired conclusion.

Acknowledgement. We are grateful to S. Louboutin who suggested us to look at this problem. We are indebted to A. M. Odlyzko for the reference to his explicit Čebotarev Density Theorem in the proof of Lemma 2.1. We are also indebted to B. Anglès for a useful discussion about Lemma 3.2.

References

[1] Amoroso F, David S (1999) Le problème de Lehmer en dimension supérieure. J reine angew Math **513**: 145–179
[2] Amoroso F, Dvornicich R (2000) A lower bound for the height in abelian extensions. J Number Theory **80**(2): 260–272
[3] Lagarias JC, Odlyzko AM (1977) Effective Versions of the Čebotarev Density Theorem. In: Froehlich A (ed) Algebraic Number Fields, pp 409–444 (Durham Symposium). London: Academic Press
[4] Louboutin S, Okazaki R (2001) Exponents of the ideal class groups of CM-fields. Preprint I.M.L. http://iml.univ-mrs.fr/editions/preprint2001/preprint2001.html
[5] Odlyzko AM (1975) Some analytic estimates of class numbers and discriminants. Invent Math **29**: 275–286
[6] Silverman JH (1984) Lower bounds for height functions. Duke Math J **51**: 395–403
[7] Simon D (2002) The index of nonmonic polynomials. Indag Math (to appear)
[8] Stark HM (1974) Some effective cases of the Brauer-Siegel theorem. Invent Math **23**: 135–152

Authors' addresses: F. Amoroso, Laboratoire SDAD, CNRS FRE 2271, Département de Mathématiques, Université de Caen, Campus II, BP 5186, 14032 Caen Cédex, France; R. Dvornicich, Dipartimento di Matematica, Università di Pisa, Via F. Buonarroti 2, 56127 Pisa, Italy