TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 302, Number 2, August 1987

ON THE STICKELBERGER IDEAL AND THE RELATIVE CLASS NUMBER

TATSUO KIMURA AND KUNIAKI HORIE

ABSTRACT. Let k be any imaginary abelian field, R the integral group ring of $G = \mathrm{Gal}(k/\mathbb{Q})$, and S the Stickelberger ideal of k. Roughly speaking, the relative class number h^- of k is expressed as the index of S in a certain ideal A of R described by means of G and the complex conjugation of k; $c^-h^- = [A : S]$, with a rational number c^- in $\frac{1}{2}\mathbb{N} = \{n/2; n \in \mathbb{N}\}$, which can be described without h^- and is of lower than h^- if the conductor of k is sufficiently large (cf. [**6**, **9**, **10**]; see also [**5**]). We shall prove that $2c^-$, a natural number, divides $2([k: \mathbb{Q}]/2)^{[k: \mathbb{Q}]/2}$. In particular, if k varies through a sequence of imaginary abelian fields of degrees bounded, then c^- takes only a finite number of values. On the other hand, it will be shown that c^- can take any value in $\frac{1}{2}\mathbb{N}$ when k ranges over all imaginary abelian fields. In this connection, we shall also make a simple remark on the divisibility for the relative class number of cyclotomic fields.

Let $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ denote the rational integer ring, the rational number field, the real number field, and the complex number field, respectively. A finite abelian extension over $\mathbb{Q}$ contained in $\mathbb{C}$ will be called an abelian field. Let k be an imaginary abelian field, namely, an abelian field not contained in $\mathbb{R}$. We denote by $R(k)$ the group ring of the Galois group $G = \mathrm{Gal}(k/\mathbb{Q})$ over $\mathbb{Z}$ and by $s(H)$, for any subgroup H of G, the sum in $R(k)$ of all elements in H. Put

$$A(k) = \{\alpha \in R(k); (1 + j_k)\alpha = as(G) \text{ for some } a \in \mathbb{Z}\},$$

where j_k denotes the complex conjugation of k. Let h_k^- denote the relative class number of k (i.e., the so-called first factor of the class number of k), Q_k the unit index of k, g_k the number of distinct prime numbers ramified in k, and $S(k)$ the Stickelberger ideal of k in the sense of Iwasawa-Sinnott, which is an additive subgroup of $A(k)$ with finite index (for the definition of the Stickelberger ideal, see [**6**, **10**]). We define c_k^- as the ratio of the index $[A(k) : S(k)]$ to h_k^-:

$$c_k^- h_k^- = [A(k) : S(k)].$$

The product $Q_k c_k^-$ is known to be a natural number and is determined by Sinnott in various cases, for example, in the case $g_k = 1$ or 2 (cf. [**10**]). He has also shown in [**9**] that, if k is a cyclotomic field, then $c_k^- = 2^b$ where $b = 0$ or $2^{g_k - 1} - 1$ according as $g_k = 1$ or $g_k \geq 2$ (for the case $g_k = 1$, see [**6**]).

In this paper, we shall give an additional result concerning the range of c_k^-.

Received by the editors July 31, 1986.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R20, 11R29; Secondary 11N25, 11R18.

Key words and phrases. (Imaginary) abelian field, Stickelberger ideal, relative class number, analytic class number formula.

The main result of this paper has been announced in [**7**] without details.

THEOREM. *In general,* $2c_k^-$ *is a natural number dividing* $2([k:\mathbb{Q}]/2)^{[k:\mathbb{Q}]/2}$, *and the following assertions hold.*

(i) *If* $g_k = 1$, *then* $c_k^- = 1$.

(ii) *If* $g_k = 2$, *then* $c_k^- = \frac{1}{2}$ *or* 1; *and, for either* $c \in \{\frac{1}{2}, 1\}$, *there exist infinitely many imaginary abelian fields* K *with* $g_K = 2$ *and* $c_K^- = c$.

(iii) *If* $g_k = 3$, *then* $c_k^- = 2^t$ *for some rational integer* $t \geq -1$. *On the other hand, for any given rational integer* $t \geq -1$, *there exist infinitely many imaginary abelian fields* K *with* $g_K = 3$ *and* $c_K^- = 2^t$.

(iv) *For any given pair* (m, n) *of natural numbers with* $m \geq 4$, *there exist infinitely many imaginary abelian fields* K *satisfying* $g_K = m$ *and* $c_K^- = n/2$.

This is verified as a consequence of basic results in [**4** and **10**]. It might be of some interest that the proof of the Theorem also leads us to the following:

COROLLARY. *Let* n *be any natural number. For each* $x > 0$, *let* $\mathbf{c}(x)$ *denote the number of cyclotomic fields with conductor* $\leq x$ *and* $\tilde{\mathbf{c}}(x)$ *the number of cyclotomic fields* K *with conductor* $\leq x$ *such that* h_K^- *is divisible by* n. *Then the ratio* $\tilde{\mathbf{c}}(x)/\mathbf{c}(x)$ *coverges to* 1 *as* x *goes to infinity:*

$$\lim_{x\to\infty} \frac{\tilde{\mathbf{c}}(x)}{\mathbf{c}(x)} = 1.$$

We note here that the above corollary is a simple analogue of Gerth's asymptotic result for class number divisibility in cyclotomic fields and in their maximal real subfields (cf. Theorem 1 of [**3**]), which follows from the results of Cornell and Washington [**2**].

In conclusion, the second author wishes to thank Professor K. Iimura for introducing him to the study in this paper and is also grateful to his teacher, Professor M. Ishida, for valuable advice.

1. For each natural number m, let $\mathbb{K}_m$ denote the cyclotomic field of mth roots of unity. Let k be an abelian field. Let $\mathfrak{S}(k)$ denote the group ring of $\mathrm{Gal}(k/\mathbb{Q})$ over $\mathbb{Q}$, so that the group ring $R(k)$ of $\mathrm{Gal}(k/\mathbb{Q})$ over $\mathbb{Z}$ is a lattice in the $\mathbb{Q}$-vector space $\mathfrak{S}(k)$. We write f_k and $\bar{f}_k$, respectively, for the conductor of k and for the product of all prime numbers ramified in k. Let p be any prime number and t the rational integer ≥ 0 such that p^t is the highest power dividing f_k. Then there exists a unique prime ideal $\mathfrak{p}$ of $\mathbb{K}_{p^t}$ dividing p, which is unramified in $\mathbb{K}_{f_k}$. We define $(\frac{k}{p})$ to be the restriction to k of the Frobenius automorphism of $\mathfrak{p}$ for the extension $\mathbb{K}_{f_k}/\mathbb{K}_{p^t}$. Let $T(p,k)$ denote the inertia group of p for $k/\mathbb{Q}$ and let, in $\mathfrak{S}(k)$,

$$(p,k)^* = \frac{s(T(p,k))}{|T(p,k)|}\left(\frac{k}{p}\right)^{-1}.$$

Here, for any finite set H, $|H|$ denotes the cardinality of H. We note that, if p is unramified in k, then $(p,k)^* = (\frac{k}{p})^{-1}$ and $(\frac{k}{p})$ is nothing but the Frobenius automorphism of p for $k/\mathbb{Q}$. Let n be any natural number dividing $\bar{f}_k$ and let $T(n,k)$ denote the compositum in $\mathrm{Gal}(k/\mathbb{Q})$ of the inertia groups $T(q,k)$ as q varies through the prime numbers dividing n. We then also put

$$(n,k)^* = \prod_q (q,k)^*, \qquad \left(\frac{k}{n}\right) = \prod_q \left(\frac{k}{q}\right)$$

in $\mathfrak{S}(k)$. Regarding $\mathfrak{S}(k)$ as an $R(k)$-module in the obvious manner, we define $U(n,k)$ to be the $R(k)$-submodule in $\mathfrak{S}(k)$ generated by the elements

$$s(T(u,k)) \prod_{v \mid n/u} (1-(v,k)^*)$$

for all natural numbers u dividing n, with v in the above product ranging over the prime numbers that divide n/u. It is known that $U(n,k)$ becomes a lattice in $\mathfrak{S}(k)$. In particular, $U(1,k) = R(k)$.

In general, let X and Y be any lattices in a finite dimensional vector space V over $\mathbb{Q}$. Then there exists a $\mathbb{Q}$-linear automorphism τ of V such that $\tau(X) = Y$. We denote by $(X:Y)$ the absolute value of the determinant of τ, which does not depend on the choice of τ. Note that, if $X \supseteq Y$, then $(X:Y)$ is equal to the index $[X:Y]$.

Let α be any element in $\mathfrak{S}(k)$ and m a natural number dividing n, so that $\alpha U(m,k)$ and $\alpha U(n,k)$ are lattices in $\alpha\mathfrak{S}(k)$. It follows from [**10**] that $(\alpha U(m,k):\alpha U(n,k))$ is a natural number. Now, let k be imaginary and let

$$e_k^- = \tfrac{1}{2}(1-j_k), \qquad U(k) = U(\bar{f}_k, k).$$

Theorem 2.1 of [**10**] then states that

$$c_k^- = (1/Q_k)(e_k^- R(k) : e_k^- U(k)).$$

Moreover we have the following

PROPOSITION 1. *For any imaginary abelian field k, $(e_k^- R(k) : e_k^- U(k))$ is a divisor of $([k:\mathbb{Q}]/2)^{[k:\mathbb{Q}]/2}$.*

PROOF. We start the proof with the identity

$$\sum_{u \mid \bar{f}_k} (u,k)^* \prod_{v \mid \bar{f}_k/u} (1-(v,k)^*) = 1$$

in $\mathfrak{S}(k)$, where the sum is taken over the natural numbers u dividing $\bar{f}_k$, with v ranging over the prime divisors of $\bar{f}_k/u$. Note, in the above, that

$$(u,k)^* = \frac{s(T(u,k))}{|T(u,k)|}\left(\frac{k}{u}\right)^{-1}.$$

Further, if $[k:\mathbb{Q}]/|T(u,k)|$ is odd, then $j_k \in T(u,k)$ and so $e_k^- s(T(u,k)) = 0$. Consequently, we obtain the following element in $e_k^- U(k)$:

$$\frac{[k:\mathbb{Q}]}{2} e_k^- = \sum_{u \mid \bar{f}_k} \frac{[k:\mathbb{Q}]}{2|T(u,k)|}\left(\frac{k}{u}\right)^{-1} e_k^- s(T(u,k)) \prod_{v \mid \bar{f}_k/u} (1-(v,k)^*).$$

Since $U(k)$ is an $R(k)$-module, it follows that

$$\frac{[k:\mathbb{Q}]}{2} e_k^- R(k) \subseteq e_k^- U(k).$$

On the other hand,

$$(e_k^- R(k) : e_k^- U(k))\left(e_k^- U(k) : \frac{[k:\mathbb{Q}]}{2} e_k^- R(k)\right)$$
$$= \left(e_k^- R(k) : \frac{[k:\mathbb{Q}]}{2} e_k^- R(k)\right) = \left(\frac{[k:\mathbb{Q}]}{2}\right)^{[k:\mathbb{Q}]/2}.$$

Hence we have

$$(e_k^- R(k) : e_k^- U(k))\,|\left(\frac{[k:\mathbb{Q}]}{2}\right)^{[k:\mathbb{Q}]/2}.$$

REMARK 1. Let k be an abelian field, α any element in $\mathfrak{S}(k)$, n a natural number dividing $\bar{f}_k$, and m a natural number dividing n. Then an argument similar to the above shows that $(\alpha U(m,k)\colon \alpha U(n,k)) \mid |T(n/m,k)|^r$, where r is the rank of $\alpha R(k)$ over $\mathbb{Z}$.

2. We shall show some lemmas for the proof of the Theorem.

LEMMA 1 (CF. [**4**, **10**]). *Let k be an imaginary abelian field in which only one prime number is ramified. Then $Q_k = 1$, $(e_k^- R(k) : e_k^- U(k)) = 1$, and so $c_k^- = 1$.*

By a character of a finite abelian group H, we mean a homomorphism of H into the multiplicative group $\mathbb{C}^\times$ of $\mathbb{C}$. For an abelian field k, each character ψ of $\mathrm{Gal}(k/\mathbb{Q})$ can be extended to a $\mathbb{Q}$-algebra homomorphism $\mathfrak{S}(k) \to \mathbb{C}$ in the usual way. Then ψ induces a primitive Dirichlet character χ satisfying $\chi(n) = \psi((n,k)^*)$ for every prime number n. We call such a character χ a (primitive Dirichlet) character associated with k. Let $\mathfrak{X}_k$ denote the (group of) primitive Dirichlet characters associated with k and $\mathfrak{X}_k^-$ the odd characters in $\mathfrak{X}_k$:

$$\mathfrak{X}_k^- = \{\chi \in \mathfrak{X}_k;\ \chi(-1) = -1\}.$$

By definition, $\mathfrak{X}_k^-$ is not empty if and only if k is imaginary. When this is the case, $\mathfrak{X}_k$ is the disjoint union of $\mathfrak{X}_k^-$ and $\mathfrak{X}_{k^+}$, where k^+ denotes the maximal real subfield of k.

LEMMA 2. *Let k be an imaginary abelian field such that exactly two prime numbers p and q $(> p)$ are ramified in k. Then the following assertions hold.*

(i) *$(e_k^- R(k) : e_k^- U(k)) = 1$ or 2; and further, if $(e_k^- R(k) : e_k^- U(k)) = 2$, then $Q_k = 2$.*

(ii) *$c_k^- = 1$ if j_k is not contained in $T(2,k)$ (e.g., if $p > 2$).*

(iii) *$c_k^- = \frac{1}{2}$ if j_k is contained in $T(2,k)$ (so that $p = 2$) but not in $T(q,k)$ and if the highest power of 2 dividing $|T(q,k)|$ is equal to that dividing $q-1$.*

PROOF. Theorem 5.1 of [**10**] implies the first part of (i), and also states that $(e_k^- R(k) : e_k^- U(k)) = 2$ if and only if j_k is neither in $T(p,k)$ nor in $T(q,k)$. Let K be the cyclotomic field of f_kth roots of unity: $K = \mathbb{K}_{f_k}$. Since $\mathrm{Gal}(K/\mathbb{Q}) = T(p,K) \times T(q,K)$, j_K is uniquely decomposed as

$$j_K = j_p j_q, \qquad j_p \in T(p,K),\ j_q \in T(q,K).$$

Taking the restriction map $\rho\colon \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(k/\mathbb{Q})$, we then have

$$j_k = \rho(j_p)\rho(j_q), \qquad \rho(j_p) \in T(p,k),\ \rho(j_q) \in T(q,k).$$

Now, assume that $(e_k^- R(k) : e_k^- U(k)) = 2$ and $p > 2$. Then $j_k \notin T(q,k)$, i.e., $\rho(j_p) \neq 1$; $T(p,K)$ is a cyclic group, and it follows that j_p, the only element of order 2 in $T(p,K)$, is not in the kernel of the surjective homomorphism $\rho\,|\,T(p,K) : T(p,K) \to T(p,k)$. Hence the ratio $|T(p,K)|/|T(p,k)|$ is an odd integer. A similar argument shows that $|T(q,K)|/|T(q,k)|$ is also an odd integer. On the other hand,

$j_k \notin T(p,k) \cup T(q,k)$ implies $\rho(j_p) \notin T(p,k) \cap T(q,k)$ and $\rho(j_q) \notin T(p,k) \cap T(q,k)$. Since $\rho(j_p)$, $\rho(j_q)$, and j_k are the elements in $\mathrm{Gal}(k/\mathbb{Q})$ of order 2, it follows that $|T(p,k) \cap T(q,k)|$ is odd, and consequently that the integer

$$\frac{\varphi(f_k)}{[k:\mathbb{Q}]} = \frac{|T(p,K)|}{|T(p,k)|}\frac{|T(q,K)|}{|T(q,k)|}|T(p,k) \cap T(q,k)|$$

is odd, where φ denotes the Euler function. The assumption of Satz 26 in [**4**] is thus satisfied for k, so that we have $Q_k = 2$. Assume next that $(e_k^- R(k) : e_k^- U(k)) = 2$ and $p = 2$. Let t be the natural number such that $2^t \parallel f_k$. As in the above case, we can see that the ratio

$$\frac{\varphi(f_k)}{[k\mathbb{K}_{2^t}:\mathbb{Q}]} = \frac{|T(q,K)|}{|T(q,k)|}$$

is an odd integer. Furthermore, since $j_k \notin T(q,k)$, the inertia field of q for $k/\mathbb{Q}$ is imaginary and, hence, there exists a character in $\mathfrak{X}_k^-$ with conductor a power of 2. We then obtain $Q_k = 2$ again from Satz 26 of [**4**]. The proof of (i) is now completed.

Because of (i), $c_k^- = 1$ if $(e_k^- R(k) : e_k^- U(k)) = 2$. Hence, for the proof of (ii), we may assume that $(e_k^- R(k) : e_k^- U(k)) = 1$ or, equivalently, $j_k \in T(p,k) \cup T(q,k)$ as well as that $j_k \notin T(2,k)$. In such a case, there exists a prime of k^+ ramified in k and lying above an odd prime $\in \{p,q\}$. Note that k does not contain $\sqrt{-1}$ since any prime of k^+ above an odd prime is unramified in $k^+(\sqrt{-1})$. Then Satz 22 of [**4**] shows $Q_k = 1$, so that $c_k^- = 1$ (see also Satz 19 of [**4**]).

To prove (iii), let u be the natural number such that $2^u \parallel (q-1)$, i.e., $2^u \parallel |T(q,K)|$. Assume that $j_k \in T(2,k) \backslash T(q,k)$ and $2^u \parallel |T(q,k)|$. Then $(e_k^- R(k) : e_k^- U(k)) = 1$ and, as in the proof of (i), $\varphi(f_k)/[k\mathbb{K}_{2^t} : \mathbb{Q}]$ becomes an odd integer, where t is the natural number such that $2^t \parallel f_k$. Furthermore, it follows that there exists a character in $\mathfrak{X}_k^-$ with conductor a power of 2. The assumption of Satz 26 of [**4**] is now satisfied for k. Therefore we can conclude that $Q_k = 2$ and $c_k^- = \frac{1}{2}$.

Thus we have proved all assertions of the lemma.

REMARK 2. As Iwasawa has shown, $c_k^- = 1$ for every cyclotomic field k with $g_k = 2$ (cf. [**9**, **10**], (ii) of the above lemma). On the other hand, if $k = \mathbb{Q}(\sqrt{-1}, \sqrt{-2q})$ or $\mathbb{Q}(\sqrt{-2}, \sqrt{-2q})$ with q a prime number $\equiv -1 \pmod 4$, then $c_k^- = \frac{1}{2}$ by (iii) of Lemma 2.

LEMMA 3. *Let k be an imaginary abelian field in which only a prime number p is ramified, and k' a real abelian field with conductor prime to p. Then, for the compositum $K = kk'$, $Q_K = 1$.*

PROOF. Rewriting the assumption in terms of Dirichlet characters, we can deduce the lemma from Satz 22 of [**4**].

LEMMA 4. *Let k be an imaginary abelian field, p a prime number ramified in k, and r a natural number dividing $\tilde{f}_k/p$. Suppose that j_k lies in $T(p,k)$. Then $e_k^- U(r,k) = e_k^- U(rp,k)$, so that $(e_k^- U(r,k) : e_k^- U(rp,k)) = 1$.*

PROOF. As $j_k \in T(p,k)$ implies $e_k^- s(T(p,k)) = 0$, this lemma follows immediately from the definitions of $U(r,k)$ and $U(rp,k)$.

LEMMA 5. *Let k be an imaginary abelian field such that* $\mathrm{Gal}(k/\mathbb{Q})$ *is the direct product of inertia groups, for $k/\mathbb{Q}$, of all prime numbers ramified in k. Then*

(i) *For a natural number r dividing $\bar{f}_k$, $(e_k^- R(k) : e_k^- U(r,k)) = 1$ unless j_k lies in $T(r,k)$.*

(ii) *If j_k lies in $T(p,k)$ for some prime number p, then $(e_k^- R(k) : e_k^- U(k)) = 1$, $Q_k = 1$.*

PROOF. The arguments in [**9**, §§5, 6] provide the proof of (i). Assume now that there exists a prime number p for which $j_k \in T(p,k)$. Since $j_k \notin T(\bar{f}_k/p, k)$, it follows from (i) that $(e_k^- R(k) : e_k^- U(\bar{f}_k/p, k)) = 1$. Furthermore, by Lemma 4, $(e_k^- U(\bar{f}_k/p, k) : e_k^- U(k)) = 1$. Therefore

$$(e_k^- R(k) : e_k^- U(k)) = (e_k^- R(k) : e_k^- U(\bar{f}_k/p, k))(e_k^- U(\bar{f}_k/p, k) : e_k^- U(k)) = 1.$$

It is easy to see $Q_k = 1$ from Lemma 3. Thus (ii) of the lemma is proved.

REMARK 3. Let k be as in Lemma 5. The proof of the Theorem in [**9**] implies that, if j_k is not in $T(r,k)$ for any natural number r dividing $\bar{f}_k$ and less than $\bar{f}_k$, then $(e_k^- R(k) : e_k^- U(k)) = 2^a$, where $a = 0$ or $2^{g_k - 2}$ according as $g_k = 1$ or > 1.

LEMMA 6. *Let k be an imaginary abelian field in which exactly three distinct prime numbers are ramified. Then $(e_k^- R(k) : e_k^- U(k)) = 2^t$ for some rational integer t with $0 \leq t \leq [k : \mathbb{Q}]/2$.*

PROOF. Let l be any odd prime, L the highest power of l dividing $(e_k^- R(k) : e_k^- U(k))$, and k' the maximal subfield in k of l-power degree. Theorem 5.2 of [**10**] then states that

$$L = \prod_{\chi} (R(k') : U(m_\chi, k'))$$

where the product is taken over the characters χ in $\mathfrak{X}_k^-$ of order prime to l and, for each such χ, m_χ denotes the product of prime numbers p ramified in k' such that $\chi(p) = 1$. However, in the above, each χ is not principal, so that the number of prime numbers dividing m_χ is less than 3. Therefore $L = 1$ by Proposition 5.2 of [**10**]. This means that $(e_k^- R(k) : e_k^- U(k)) = 2^t$ for some rational integer $t \geq 0$.

Now, let p_1, p_2, p_3 be the prime numbers ramified in k. For simplicity, we put $G = \mathrm{Gal}(k/\mathbb{Q})$, $T = T(p_2, k)$, and

$$d_1 = (e_k^- U(p_1, k) : e_k^- U(p_1 p_2, k)),$$
$$d_2 = (e_k^- U(p_1 p_2, k) : e_k^- U(k)).$$

Then, again by Proposition 5.2 of [**10**], $(e_k^- R(k) : e_k^- U(k)) = d_1 d_2$. Lemma 4 says that, if $j_k \in T$, then $d_1 = 1$; while we see easily that, even if $j_k \notin T$, d_1 divides $|T|^{[G:T]/2} = (|T|^{1/|T|})^{[k:\mathbb{Q}]/2}$ (cf. [**10**, **5**]). Since d_1 is a power of 2, it follows that $d_1 = 1$ also when $|T|$ is odd. Furthermore, note that $|T|^{1/|T|} \leq 2^{1/2}$ if $|T|$ is even. We have therefore $d_1 \leq 2^{[k:\mathbb{Q}]/4}$. Similarly, we also have $d_2 \leq 2^{[k:\mathbb{Q}]/4}$. Consequently

$$2^t = (e_k^- R(k) : e_k^- U(k)) \leq 2^{[k:\mathbb{Q}]/2}.$$

This completes the proof of Lemma 6.

LEMMA 7. *Let k and K be imaginary abelian fields, with k contained in K. Then Q_k divides Q_K if the 2-power degree roots of unity in K are also contained in k. Furthermore, $Q_k = Q_K$ if $[K: k]$ is odd.*

PROOF. See [**10**, §7] as well as [**4**].

For any natural number n and any abelian field k, we let $Z(n, k)$ denote the compositum in $\mathrm{Gal}(k/\mathbb{Q})$ of the decomposition groups, for $k/\mathbb{Q}$, of all prime numbers dividing n.

LEMMA 8. *Let k be an imaginary abelian field, r a natural number dividing $\bar{f}_k$, and p a prime number dividing $\bar{f}_k/r$. Suppose that $T(p, k)$ is disjoint from the compositum of $\{1, j_k\}$ and $Z(r, k)$ in $\mathrm{Gal}(k/\mathbb{Q})$. Then $(e_k^- U(r, k) : e_k^- U(rp, k)) = 1$.*

PROOF. The assumption implies that the $R(k)$-module $e_k^- U(r, k)$ is free over $T(p, k)$. Then the arguments in [**9**, §5] lead us to the conclusion of this lemma.

LEMMA 9. *Let t be any natural number. Let p be a prime number $\equiv 1 \pmod{2(t+1)}$; let q_1 and q_2 be distinct prime numbers $\equiv 1 \pmod{p}$. Furthermore let k be a compsitum of the real cyclic field[1] of degree $t+1$ with conductor p, an imaginary cyclic field with conductor q_1, and an imaginary cyclic field with conductor q_2. Then $(e_k^- R(k) : e_k^- U(k)) = 2^{t+1}$, $Q_k = 2$, so that $c_k^- = 2^t$.*

PROOF. Let k' be the (real) cyclic field of degree $t+1$ with conductor p and k'' the maximal subfield of k with conductor $q_1 q_2$; $k = k'k''$. It then follows from Lemma 7 that $Q_k = 2$, since $k \not\ni \sqrt{-1}$ and since $Q_{k''} = 2$ by Satz 26 of [**4**]. It also follows that

$$j_k \in T(q_1 q_2, k) = Z(q_1 q_2, k), \qquad j_k \notin T(q_1, k) \cup T(q_2, k),$$
$$T(p, k) \cap Z(q_1 q_2, k) = 1.$$

Hence, by Proposition 5.2 of [**10**] and Lemma 8,

$$\begin{aligned}(e_k^- R(k) : e_k^- U(k)) &= (e_k^- R(k) : e_k^- U(q_1 q_2, k))(e_k^- U(q_1 q_2, k) : e_k^- U(k)) \\ &= 2^{[\mathrm{Gal}(k/\mathbb{Q}) : Z(q_1 q_2, k)]} = 2^{[k' : \mathbb{Q}]} = 2^{t+1}.\end{aligned}$$

Thus Lemma 9 is proved.

3. Let us now begin to prove our Theorem.

PROOF OF THEOREM. Let k be an imaginary abelian field. Since $Q_k = 1$ or 2, Proposition 1 shows that $2c_k^-$ is a natural number dividing $2([k : \mathbb{Q}]/2)^{[k:\mathbb{Q}]/2}$. The assertion (i) of the Theorem is an immediate consequence of Theorem 5.1 in [**10**] and Satz 23 in [**4**] (see Lemma 1). The assertion (ii) follows from Lemma 2 and Remark 2. The first part of (iii) follows from Lemma 6. Now, let $K = \mathbb{Q}(\sqrt{-2p}, \sqrt{q})$, where p and q are distinct prime numbers $\equiv -1 \pmod 4$. Then Satz 26 of [**4**] shows $Q_K = 2$. Since $j_K \in T(2, K) \cap T(p, K)$, $(e_K^- R(K) : e_K^- U(K)) = 1$ by Proposition 5.2 of [**10**] and Lemma 4, so that $c_K^- = \frac{1}{2}$. This fact, Lemma 5, and Lemma 9 verify the second part of (iii). The assertion (iv) will be obtained from the following lemmas (in particular, Lemmas 11, 12), Proposition 2, and above-mentioned Remark 2.

[1] An abelian field k will be called a cyclic field if $\mathrm{Gal}(k/\mathbb{Q})$ is a cyclic group.

LEMMA 10. *Let K be an imaginary abelian field. Assume that K is a compositum of its subfield k and k'; $K = kk'$, and that all prime numbers ramified in k are completely decomposed in k'. If furthermore k is real, then*

$$(e_K^- R(K) : e_K^- U(\bar{f}_k, K)) = (R(k) : U(k))^{[K:k]/2}.$$

PROOF. It follows from the assumption that f_k is prime to $f_{k'}$. Hence $\mathrm{Gal}(K/\mathbb{Q})$ is the direct product of $T(\bar{f}_k, K) \cong \mathrm{Gal}(k/\mathbb{Q})$ and $T(\bar{f}_{k'}, K) \cong \mathrm{Gal}(k'/\mathbb{Q})$, so that we have a canonical $\mathbb{Q}$-linear isomorphism $\eta\colon \mathfrak{S}(K) \xrightarrow{\sim} \mathfrak{S}(k) \otimes_{\mathbb{Q}} \mathfrak{S}(k')$. Since $Z(\bar{f}_k, K) = T(\bar{f}_k, K)$, η induces $U(\bar{f}_k, K) \cong U(k) \otimes_{\mathbb{Z}} R(k')$ as well as $R(K) \cong R(k) \otimes_{\mathbb{Z}} R(k')$. Therefore, if k is real, then η also induces

$$e_K^- R(K) \cong R(k) \otimes_{\mathbb{Z}} e_{k'}^- R(k'), \qquad e_K^- U(\bar{f}_k, K) \cong U(k) \otimes_{\mathbb{Z}} e_{k'}^- R(k').$$

The lemma now follows from these isomorphisms.

LEMMA 11. *Let n be any natural number and p_1, p_2, p_3 three distinct prime numbers $\equiv 1 \pmod{4n}$. For each $i \in \{1,2,3\}$, let k_i be a real cyclic field of degree divisible by n with conductor a power of p_i and take an element σ_i of order n in $T(p_i, k_1k_2k_3)$. Furthermore let $K = k(\sqrt{-1})$, where k is the abelian field consisting of all elements in $k_1k_2k_3$ fixed by $\sigma_1\sigma_2\sigma_3$. Then $Q_K = 1$, $(e_K^- R(K) : e_K^- U(K)) = n$, so that $c_K^- = n$.*

PROOF. Note that all prime numbers ramified in k (i.e., p_1, p_2, and p_3) are decomposed in $\mathbb{Q}(\sqrt{-1})$. It then follows from Lemma 10 that $(e_K^- R(K) : e_K^- U(K)) = (R(k) : U(k))$. On the other hand, $\mathrm{Gal}(k_1k_2k_3/k) \cap T(r, k_1k_2k_3) = \{1\}$ for all natural numbers r dividing $p_1p_2p_3$ and less than $p_1p_2p_3$. Hence, by Theorem 5.4 of[**10**], $(R(k) : U(k)) = [k_1k_2k_3 : k] = n$. Thus we have $(e_K^- R(K) : e_K^- U(K)) = n$. We also have $Q_K = 1$ by Lemma 3.

LEMMA 12. *Let n be any odd integer ≥ 3; let p_1, p_2, p_3 be three distinct prime numbers such that $p_1 \equiv 3 \pmod 8$, $(-2/p_2) = (-2/p_3) = 1$, $p_1 \equiv p_2 \equiv p_3 \equiv 1 \pmod n$. For each $i \in \{1,2,3\}$, let k_i be the cyclic field of degree n with conductor p_i and let σ_i be a generator of $T(p_i, k_1k_2k_3)$. Put $K = k(\sqrt{-2}, \sqrt{p_1})$, where k is the subfield of $k_1k_2k_3$ consisting of all elements in $k_1k_2k_3$ fixed by $\sigma_1\sigma_2\sigma_3$. Then $Q_K = 2$, $(e_K^- R(K) : e_K^- U(K)) = n$, and hence $c_K^- = n/2$.*

PROOF. Let $F = \mathbb{Q}(\sqrt{-2}, \sqrt{p_1})$, so that $Q_F = 2$ and $(e_F^- R(F) : e_F^- U(F)) = 1$ (cf. Remark 2). Theorem 5.2 of [**10**] then shows that $(e_K^- R(K) : e_K^- U(K))$ is odd. Let l be any prime number dividing $(e_K^- R(K) : e_K^- U(K))$ and k' the maximal subfield in K of l-power degree. Obviously, k' is also the maximal subfield of k of l-power degree. The choice of p_1, p_2, p_3 implies that the odd Dirichlet character associated with $\mathbb{Q}(\sqrt{-2})$ is a unique element χ in $\mathfrak{X}_K^-$ satisfying $\chi(p_1) = \chi(p_2) = \chi(p_3) = 1$. Hence, by Proposition 5.2 and Theorem 5.2 of [**10**], the highest power of l dividing $(e_K^- R(K) : e_K^- U(K))$ is equal to that dividing $(R(k) : U(k))$. Consequently $(e_K^- R(K) : e_K^- U(K)) = (R(k) : U(k))$. It also follows from Theorem 5.4 of [**10**] that $(R(k) : U(k)) = n$. Thus we have $(e_K^- R(K) : e_K^- U(K)) = n$. It remains to see $Q_K = 2$, but this follows from $Q_F = 2$ and Lemma 7.

LEMMA 13. *Let k be an imaginary abelian field, l a prime number such that the l-primary part of $\mathrm{Gal}(k/\mathbb{Q})$ is cyclic, and p a prime number ramified in k such*

that $|T(p,k)|$ *is a power of* l. *Then* $(e_k^- U(r,k) : e_k^- U(rp,k)) = 1$ *for every natural number* r *dividing* $\bar{f}_k/p$.

PROOF. This follows from Lemma 5.1 and Theorem 5.3 of [**10**].

PROPOSITION 2. *Let* k *be an imaginary abelian field,* m *a natural number, and* l *a prime number not dividing* $[k:\mathbb{Q}]$. *Then there exist infinitely many imaginary abelian fields* K *containing* k *such that* $[K:k] = l$, $g_K = g_k + m$, $Q_K = Q_k$,

$$(e_K^- R(K) : e_K^- U(K)) = (e_k^- R(k) : e_k^- U(k)),$$

and hence $c_K^- = c_k^-$.

PROOF. By the Tschebotareff density theorem, there exist infinitely many m-tuples $(q_1,\dots,q_m)$ of distinct prime numbers $\equiv 1 \pmod{l}$ for which no prime number ramified in k is an lth power residue $(\mathrm{mod}\, q_1\cdots q_m)$. Take such a m-tuple $(q_1,\dots,q_m)$. Let K be a compositum of k and a cyclic field of degree l with conductor $q_1\cdots q_m$. Then $[K:k] = l$, $\bar{f}_K = \bar{f}_k q_1\cdots q_m$, $g_K = g_k + m$. Since the l-primary part of $\mathrm{Gal}(K/\mathbb{Q})$ is of order l and since $|T(q_1,K)| = \cdots = |T(q_m,K)| = l$, it follows from Lemma 13 that

$$(1)\qquad (e_K^- U(\bar{f}_k,K) : e_K^- U(K)) = \prod_{i=1}^{m} (e_K^- U(\bar{f}_k q_1\cdots q_{i-1},K) : e_K^- U(\bar{f}_k q_1\cdots q_i,K)) = 1.$$

Next, let χ be any character in $\mathfrak{X}_K$ but not in $\mathfrak{X}_k$, so that the conductor of χ is divisible by $q_1\cdots q_m$. As $[k:\mathbb{Q}]$ is prime to l, the choice of $q_1,\dots,q_m$ then implies that $\chi(p) \neq 1$ for any prime number p ramified in k. Hence we have, by Theorem 5.2 of [**10**], $(e_K^- R(K) : e_K^- U(\bar{f}_k,K)) = (e_k^- R(k) : e_k^- U(k))$. This and (1) induce $(e_K^- R(K) : e_K^- U(K)) = (e_k^- R(k) : e_k^- U(k))$. Further, noting that $[K:k] = l$ is odd, we obtain $Q_K = Q_k$ from Lemma 7. Consequently $c_K^- = c_k^-$, and the proposition is proved.

4. To prove the corollary, we prepare the following lemma.

LEMMA 14. *Let* K/F *be an extension of imaginary abelian fields, with* F *containing an imaginary root of unity. Then* $[A(F) : S(F)] | [A(K) : S(K)]$.

PROOF. For any imaginary abelian field k, let

$$R(k)^- = \{\alpha \in R(k); j_k\alpha = -\alpha\} = (1 - j_k)R(k),$$
$$S(k)^- = S(k) \cap R(k)^-, \qquad e_k^+ = \tfrac{1}{2}(1 + j_k).$$

Since $R(k)^- \subseteq A(k)$ and $e_k^+ A(k) = \frac{1}{2}s(\mathrm{Gal}(k/\mathbb{Q}))\mathbb{Z}$, it follows from Lemma 6.1 of [**9**] that

$$\begin{aligned}[A(k) : S(k)] &= [A(k) \cap R(k)^- : S(k)^-][e_k^+ A(k) : e_k^+ S(k)] \\ &= [R(k)^- : S(k)^-][\tfrac{1}{2}s(\mathrm{Gal}(k/\mathbb{Q}))\mathbb{Z} : e_k^+ S(k)].\end{aligned}$$

Hence $[A(k) : S(k)] = [R(k)^- : S(k)^-]$ if and only if there exists $\alpha \in S(k)$ such that $e_k^+\alpha = \frac{1}{2}s(\mathrm{Gal}(k/\mathbb{Q}))$.

Now, let F' be an imaginary cyclotomic field contained in F. Then Theorem 3.1 of [**9**] and Theorem 2.1 of [**10**] imply that $[A(F') : S(F')] = [R(F')^- : S(F')^-]$, so that

$$e^+_{F'}\beta = \tfrac{1}{2}s(\mathrm{Gal}(F'/\mathbb{Q}))$$

for some $\beta \in S(F')$. Applying to both sides the corestriction map $\iota\colon R(F') \to R(F)$, we have

$$e^+_F\iota(\beta) = \tfrac{1}{2}s(\mathrm{Gal}(F/\mathbb{Q})), \qquad \iota(\beta) \in S(F).$$

Therefore $[A(F) : S(F)] = [R(F)^- : S(F)^-]$. We have similarly $[A(K) : S(K)] = [R(K)^- : S(K)^-]$. Furthermore the restriction map $R(K) \to R(F)$ induces a surjective homomorphism $R(K)^-/S(K)^- \to R(F)^-/S(F)^-$. In particular, $[R(F)^- : S(F)^-]$ is a divisor of $[R(K)^- : S(K)^-]$, namely, $[A(F) : S(F)]$ is that of $[A(K) : S(K)]$.

REMARK 4. For any extension K/F of imaginary abelian fields, we can see at least that $[A(F) : S(F)] \mid 2[A(K) : S(K)]$.

PROOF OF COROLLARY. As in the statement of the Corollary, let n be any natural number; for each $x > 0$, let $\mathbf{c}(x)$ denote the number of cyclotomic fields with conductor $\leq x$ and $\tilde{\mathbf{c}}(x)$ the number of cyclotomic fields K with $f_K \leq x$ such that h_K^- is divisible by n. We note that

$$\mathbf{c}(x) = \tfrac{3}{4}x + O(1), \quad \text{as } x \to \infty.$$

Let p be any prime number and let C_p denote the set of cyclotomic fields with conductor divisible by p and by three distinct prime numbers $\equiv 1 \pmod{16np}$. Take a cyclotomic field k in C_p such that f_k/p is a product of three distinct prime numbers $\equiv 1 \pmod{16np}$. Theorem 5.4 of [**10**] and Lemmas 3, 10 then show, as in the proof of Lemma 11, that there exists an imaginary subfield k' of k for which $k' \supseteq \mathbb{K}_{2p}$, $Q_{k'} = 1$, $8n \mid (e^-_{k'}R(k') : e^-_{k'}U(k'))$, and hence $8n \mid [A(k') : S(k')]$. On the other hand, by [**9, 10**], $[A(k) : S(k)] = 8h_k^-$. It therefore follows from Lemma 14 that $n \mid h_k^-$. Furthermore, for any cyclotomic field K containing k, $h_k^- \mid h_K^-$ by Lemma 5 of [**8**], so that $n \mid h_K^-$. Consequently, $n \mid h_K^-$ always holds whenever K is a cyclotomic field in C_p. For each $x > 0$, let $\mathbf{d}_p(x)$ denote the number of cyclotomic fields, not lying in C_p, with conductor divisible by p and not larger than x. Obviously $\mathbf{d}_p(x)$ does not exceed the number of natural numbers $\leq x/p$ divisible by at most two distinct rational primes $\equiv 1 \pmod{16np}$. Hence, by means of asymptotic formulae in analytic number theory, we can see that

$$\mathbf{d}_p(x) = O\left(\frac{x(\log\log x)^2}{(\log x)^{1/\varphi(16np)}}\right) \tag{2}$$

as $x \to \infty$ (see, e.g., [**3**]).

Now, for any $x > 0$ and any $y > 0$, let $\mathbf{c}(x, y)$ denote the number of cyclotomic fields K with $f_K \leq x$ such that $q \mid f_K$ for some prime number $q \leq y$; let $\tilde{\mathbf{c}}(x, y)$ denote the number of cyclotomic fields K such that $n \mid h_K^-$, $f_K \leq x$, and $q \mid f_K$ for some prime number $q \leq y$. According to the above argument,

$$\mathbf{c}(x, y) - \tilde{\mathbf{c}}(x, y) \leq \sum_{p \leq y} \mathbf{d}_p(x),$$

where p ranges over the rational primes $\leq y$; so that

$$\mathbf{c}(x) - \tilde{\mathbf{c}}(x) \leq \mathbf{c}(x) - \tilde{\mathbf{c}}(x,y) \leq \mathbf{c}(x) - \mathbf{c}(x,y) + \sum_{p \leq y} \mathbf{d}_p(x).$$

Since

$$\mathbf{c}(x) - \mathbf{c}(x,y) = O\left(\mathbf{c}(x) \prod_{p \leq y} \left(1 - \frac{1}{p}\right)\right), \quad \text{for } x > 0 \text{ and } y > 0,$$

it then follows from (2) that

$$\limsup_{x \to \infty} \frac{\mathbf{c}(x) - \tilde{\mathbf{c}}(x)}{\mathbf{c}(x)} = O\left(\prod_{p \leq y} \left(1 - \frac{1}{p}\right)\right) = O\left(\frac{1}{\log y}\right), \quad \text{for } y > 0.$$

This completes the proof.

REMARK 5. The above proof is essentially based upon the analytic class number formula for abelian fields.

We have used, in the proof of the Corollary, a simple fact on the divisibility for the relative class number of a cyclotomic field. Let us add in passing a similar but somewhat stronger fact as follows:

PROPOSITION 3. *Let K be a cyclotomic field with conductor divisible by distinct prime numbers p and q. Suppose that $q > 2$ and that the order a of q* (mod pu) *is odd, where $u = 1$ or 2 according as $p > 2$ or $p = 2$ (so that $2a$ divides $u(p-1)$). Then ph_K^- is divisible by $\{(q-1)/2\}^{u(p-1)/2a}$. If, furthermore, $q \not\equiv 1$* (mod p) *or $q \equiv 1$* (mod p^2u), *then h_K^- is divisible by $\{(q-1)/2\}^{u(p-1)/2a}$.*

PROOF. Indeed class field theory (together with genus theory and the ambiguous class number formula) provides an algebraic proof of the proposition (see, e.g., [**1**]) but, in the following, we deduce the proposition from some consequences, in [**4**, **8**, **9**], of the analytic class number formula.

Again by Lemma 5 of [**8**], we may assume that $K = \mathbb{K}_{upq}$. Let l be any prime number dividing $(q-1)/2$, and e the natural number such that $l^e \parallel (q-1)/2$. It suffices to show that

$$l^{eu(p-1)/2a-\delta} \mid h_K^- \tag{3}$$

where

$$\begin{aligned} \delta &= 1, \quad \text{if } l = p,\ e = 1, \text{ and hence } a = 1, \\ &= 0, \quad \text{otherwise.} \end{aligned}$$

For each character χ in $\mathfrak{X}_K$, we let

$$\Theta(\chi) = \frac{-1}{2upq} \sum_x \chi(x)x,$$

the sum taken over the natural numbers $x \leq upq$ prime to pq. Let $\mathfrak{X}$ be the set of odd primitive Dirichlet characters with conductor upq. Then the analytic class number formula implies

$$h_K^- = h_{\mathbb{K}_{up}}^- h_{\mathbb{K}_q}^- \prod_{\chi \in \mathfrak{X}} \Theta(\chi). \tag{4}$$

Each $\Theta(\chi)$ in the above is known to be an algebraic integer (cf. [**4**, §28]). Let Φ be the set of odd primitive Dirichlet characters of order dividing $u(p-1)/a$ with conductor up. We note that $\phi(q) = 1$ for every ϕ in Φ. Let Ψ_t denote, for each natural number $t \leq e$, the set of even primitive Dirichlet characters of order l^t with conductor q. Take any ϕ in Φ and any ψ in Ψ_t so that $\phi\psi$ belongs to $\mathfrak{X}$. As in [**4**, §28], simple calculations show that

$$\Theta(\phi\psi) = \sum_{(x,y)} \phi(qx)\psi(upy),$$

$$\Theta(\phi) = \sum_{(x,y)} \phi(qx) - \frac{q-1}{up} B(\phi).$$

Here, in both sums, (x, y) ranges over the pairs of natural numbers such that $x < up/2$, $y < q/2$, and $y/q < x/up$; and further

$$B(\phi) = \sum_{x'} \phi(x')x',$$

the sum taken over all natural numbers $x' < up/2$. On the other hand, $\Theta(\phi) = 0$ since $\phi(q) = 1$ (cf. Lemma 2.1 of [**9**]). Therefore

$$\Theta(\phi\psi) = \sum_{(x,y)} \phi(qx)(\psi(upy) - 1) + \frac{q-1}{up} B(\phi),$$

with $((q-1)/up)B(\phi)$ an algebraic integer in $\mathbb{K}_{p-1}$. If follows from this that

$$\Theta(\phi\psi) \equiv \frac{q-1}{up} B(\phi) \pmod{\mathfrak{l}}, \tag{5}$$

where $\mathfrak{l}$ is a unique prime ideal of $\mathbb{K}_{l^t}$ dividing l. Hence, if

$$\frac{q-1}{up} B(\phi) \equiv 0 \pmod{l} \tag{6}$$

holds, then $\Theta(\phi\psi) \equiv 0 \pmod{\mathfrak{l}}$ so that

$$\prod_{\psi' \in \Psi_t} \Theta(\phi\psi') \equiv 0 \pmod{l}. \tag{7}$$

Now, assume that ϕ is of order less than $\varphi(up) = u(p-1)$. In such a case, $p > 2$ and, by [**4**, §31], $B(\phi) \equiv 0 \pmod{p}$, which implies (6) and therefore (7). Thus we obtain that

$$\prod_{\phi'} \left(\prod_{\psi' \in \Psi_t} \Theta(\phi'\psi') \right) \equiv 0 \pmod{l^{u(p-1)/2a}}, \qquad \text{if } a > 1, \tag{8}$$

$$\equiv 0 \pmod{l^{u(p-1)/2-\varphi(p-1)}}, \qquad \text{if } a = 1,$$

where ϕ' ranges over all characters in Φ of order less than $u(p-1)$.

Assume next that ϕ is of order $u(p-1)$, so that $a = 1$. In the case where $l \neq p$ or $e \geq 2$, (6) is easily verified and so is (7). Thus we have

$$\prod_{\phi''} \left(\prod_{\psi' \in \Psi_t} \Theta(\phi''\psi') \right) \equiv 0 \pmod{l^{\varphi(p-1)}}, \tag{9}$$

where ϕ'' ranges over the characters in Φ of order $p-1$. In the case wher $l = p$, $e = 1$, and hence $t = 1$; it follows from [4, §31] that $B(\phi) \equiv 0 \pmod{p/\mathfrak{B}}$ for some prime ideal $\mathfrak{B}$ of $\mathbb{K}_{p-1}$ dividing p. Therefore, by (5), $\Theta(\phi\psi) \equiv 0 \pmod{\mathfrak{p}/\mathfrak{B}^*}$, where $\mathfrak{p} = \mathfrak{l}$ and $\mathfrak{B}^*$ is a unique prime ideal of $\mathbb{K}_{p(p-1)}$ dividing $\mathfrak{B}$. Taking the norm for $\mathbb{K}_{p(p-1)}/\mathbb{Q}$ of the above, we have

$$\prod_{\phi''} \prod_{\psi' \in \Psi_1} \Theta(\phi''\psi') \equiv 0 \pmod{p^{\varphi(p-1)-1}}, \tag{10}$$

with ϕ'' running over the characters in Φ of order $p-1$.

Since the disjoint union $\bigcup_{t=1}^{e}\{\phi'\psi'; \phi' \in \Phi, \psi' \in \Psi_t\}$ is contained in $\mathfrak{X}$, (3) follows from (4), (8), (9), and (10). The proposition is thus proved.

REMARK 6. Class field theory also shows that there exists a subgroup H of the ideal class group of K such that H is isomorphic as a group to $(\mathbb{Z}/((q-1)/2)\mathbb{Z})^{u(p-1)/2a-1}$ and such that $\alpha^{j\kappa} = \alpha^{-1}$ for all α in H.

REFERENCES

1. G. Cornell, *Abhyankar's lemma and the class group*, Number Theory (Carbondale 1979), edited by M. Nathanson, Lecture Notes in Math., vol. 751, Springer, 1979, pp. 82–88.
2. G. Cornell and L. C. Washington, *Class numbers of cyclotomic fields*, J. Number Theory **21** (1985), 260–274.
3. F. Gerth III, *Asymptotic results for class number divisibility in cyclotomic fields*, Canad. Math. Bull. **26** (1983), 464–472.
4. H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.
5. K. Horie, *On the index of the Stickelberger ideal and the cyclotomic regulator*, J. Number Theory **20** (1985), 238–253.
6. K. Iwasawa, *A class number formula for cyclotomic fields*, Ann. of Math. **76** (1962), 171–179.
7. T. Kimura and K. Horie, *On the Stickelberger ideal and the relative class number*, Proc. Japan Acad. **58A** (1982), 170–171.
8. J. Masley and H. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976), 248–256.
9. W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. **108** (1978), 107–134.
10. ——, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980), 181–234.

THE INSTITUTE OF MATHEMATICS, UNIVERSITY OF TSUKUBA, NIIHARIGUN, IBARAKI 305, JAPAN

DEPARTMENT OF MATHEMATICS, TOKYO METROPOLITAN UNIVERSITY, SETAGAYA-KU, TOKYO 158, JAPAN