J. Math. Soc. Japan
Vol. 59, No. 3 (2007) pp. 811–824

Primary components of the ideal class group of an Iwasawa-theoretical abelian number field

By Kuniaki HORIE

(Received Apr. 3, 2006)
(Revised Nov. 27, 2006)

Abstract. Let S be a non-empty finite set of prime numbers, and let F be an abelian extension over the rational field such that the Galois group of F over some subfield of F with finite degree is topologically isomorphic to the additive group of the direct product of the p-adic integer rings for all p in S. Let m be a positive integer that is neither congruent to 2 modulo 4 nor divisible by any prime number outside S but divisible by all prime numbers in S. Let Ω denote the composite of p^n-th cyclotomic fields for all p in S and all positive integers n. In our earlier paper [**3**], it is shown that there exist only finitely many prime numbers l for which the l-class group of F is nontrivial and the m-th cyclotomic field contains the decomposition field of l in Ω. We shall prove more precise results providing us with an effective upper bound for a prime number l such that the l-class group of F is nontrivial and that the m-th cyclotomic field contains the decomposition field of l in Ω.

Introduction.

An abelian extension over the rational number field $\boldsymbol{Q}$ in the complex number field $\boldsymbol{C}$ will be called an abelian number field. Let S be a non-empty finite set of prime numbers, let $\boldsymbol{Z}_p$ denote for each $p \in S$ the ring of p-adic integers, and let $\boldsymbol{Q}^S$ denote the abelian number field such that the Galois group $\mathrm{Gal}(\boldsymbol{Q}^S/\boldsymbol{Q})$ is topologically isomorphic to the additive group of the direct product of $\boldsymbol{Z}_p$ for all $p \in S$. Let F be any abelian number field which is a finite extension of $\boldsymbol{Q}^S$. As is well known, arithmetic properties of F have been studied with great success in virtue of Iwasawa theory (cf. Friedman [**1**], Washington [**6**], [**7**], etc.). Let Ω denote the composite of the cyclotomic fields $\boldsymbol{Q}(e^{2\pi i/p^n})$ for all $p \in S$ and all positive integers n. Take a positive integer m, with $m \not\equiv 2 \pmod 4$, which is divisible by all prime numbers in S and not divisible by any prime number outside S. It then follows that $\Omega = \boldsymbol{Q}^S(e^{2\pi i/m})$. For each prime number l, $\Omega^{(l)}$ will denote the decomposition field of l for the abelian extension $\Omega/\boldsymbol{Q}$. Given any abelian number field M, we let C_M denote the ideal class group of M and, for each prime number l, we let $C_M(l)$ denote the l-class group of M, i.e., the l-primary component of C_M.

After some initiative investigations of [**2**] partly based upon [**6**], using the algebraic interpretation by Leopoldt [**5**] of the analytic class number formula, we have shown in [**3**] that there exist only finitely many prime numbers l such that $C_F(l)$ is nontrivial and such that $\boldsymbol{Q}(e^{2\pi i/m})$ contains $\Omega^{(l)}$. Meanwhile, among others, the simplest case where $F = \boldsymbol{Q}^S$ with $|S| = 1$ is treated effectively by [**4**]. In the present paper, we shall pursue our arguments in [**2**], [**3**], [**4**] to prove some results actually giving us an explicit constant

2000 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R23, 11R27.
Key Words and Phrases. abelian number field, ideal class group, Iwasawa theory.

$\mathfrak{C} > 0$ such that $C_F(l)$ is trivial whenever

$$l \geq \mathfrak{C} \quad \text{and} \quad \Omega^{(l)} \subseteq \boldsymbol{Q}(e^{2\pi i/m}).$$

A few additional remarks, for instance, on the cardinality $|C_F|$ will also be made in connexion with distinguished results in [**1**], [**6**]. We shall devote the last part of the paper to indispensable corrections to [**3**], [**4**].

ACKNOWLEDGEMENTS. The author expresses his most sincere gratitude to the referee who read the paper in manuscript very carefully, and made very helpful comments on it, which included kind corrections of the author's several mistakes.

1. Statements of main results.

In this section, we shall state our main results, with giving definitions needed for the statements.

For each prime number p, put

$$\tilde{p} = p \quad \text{or} \quad \tilde{p} = 4$$

according as $p > 2$ or $p = 2$; for each positive integer u, let $[u]_p$ denote the p-part of u, that is, the highest power of p dividing u. We note that $\tilde{p} \leq [m]_p$ for each $p \in S$ and that a prime number $l \notin S$ satisfies $\Omega^{(l)} \subseteq \boldsymbol{Q}(e^{2\pi i/m})$ if and only if, for each $p \in S$, either $l^{\varphi(\tilde{p})} \not\equiv 1 \pmod{p[m]_p}$ or $[l-1]_2 = [m]_2$ with $p = 2$, where φ denotes the Euler function as usual. Naturally, there exists a unique abelian number field k of finite degree with $F = k\boldsymbol{Q}^S$ such that, for each $p \in S$, the p-part of the conductor of k divides $\tilde{p}$. We then find that $k \cap \boldsymbol{Q}^S = \boldsymbol{Q}$. Given any positive integer n, let D_n denote the absolute value of the discriminant of $\boldsymbol{Q}(e^{2\pi i/n})$, and let

$$\Xi(n) = (\varphi(n) - 1)^{(\varphi(n)-1)/2} \quad \text{or} \quad \Xi(n) = 1$$

according as $n \geq 3$ or $n \leq 2$. It is well known that

$$D_n \prod_{p|n} \left(\frac{p-1}{p^{(p-2)/(p-1)}} \right)^{\varphi(n)} = \varphi(n)^{\varphi(n)},$$

p ranging over the prime divisors of n. However the inequality

$$\frac{x-1}{x^{(x-2)/(x-1)}} \geq 1$$

holds for each real number $x \geq 2$. Hence we obtain $D_n \leq \varphi(n)^{\varphi(n)}$, which implies that

$$\frac{(\varphi(n)-1)^{\varphi(n)}}{D_n} \geq \left(1 - \frac{1}{\varphi(n)}\right)^{\varphi(n)}.$$

Whenever $\varphi(n) \geq 2$, the right hand side of the above inequality is at least equal to $1/4$ since, for a real variable $\xi > 1$, $(1-1/\xi)^{\xi}$ is an increasing function. Hence, taking account of the fact that $D_2 = D_1 = 1$, we always have

$$\frac{\Xi(n)}{\sqrt{D_n}} > \frac{1}{2\sqrt{\varphi(n)}}. \tag{1}$$

Now, for any abelian number field M, we denote by M^+ the maximal real subfield of M, so that $M = M^+$ if M is real. We see particularly that

$$F^+ = k^+\boldsymbol{Q}^S, \quad k^+ \cap \boldsymbol{Q}^S = \boldsymbol{Q}.$$

Let u_0 be the least common multiple of m and the exponent of $\mathrm{Gal}(k/\boldsymbol{Q})$; let n_0 be the least common multiple of m and the exponent of $\mathrm{Gal}(k^+/\boldsymbol{Q})$. It is obvious that $u_0 = 2n_0$ or $u_0 = n_0$. Let $d = \prod_{p\in S}([n_0]_p/p)$, and let $\boldsymbol{Q}^*$ denote the unique subfield of $\boldsymbol{Q}^S$ with degree d. Then $k^+\boldsymbol{Q}^*$ is the unique intermediate field of F^+/k^+ with degree d over k^+. We write h^* for the class number of $k^+\boldsymbol{Q}^*$. Let λ_0 be the number of distinct prime divisors of n_0, and v the product of prime numbers ramified in k^+ or belonging to S. We put

$$J = \frac{2^{\lambda_0-2}\varphi(2v)\varphi(n_0)^3\Xi(n_0)\sum_{p\in S}\varphi(p-1)}{(\log 2)D_{n_0}^{(\varphi(n_0)-1)/(2\varphi(n_0))}}.$$

We further put

$$w = \max_{p\in S}\frac{(p-1)\varphi(\tilde{p})[m]_p^{1/\varphi(p-1)}}{p}, \quad \kappa = \left(\frac{1}{\pi}+\frac{1}{s}\right)\max_{p\in S}\frac{d\prod_{q\in S}\tilde{q}}{[d]_p\tilde{p}},$$
$$\Lambda = \log\left(J\big(\varphi(2v)n_0w(t\kappa)^{1/\sum_{p\in S}\varphi(p-1)}\big)^{1/\varphi(n_0)}\right).$$

Here s denotes the minimum of $\tilde{p}$ for all prime divisors p of v, and t the maximal divisor of the conductor of k^+ relatively prime to m. In view of (1), we easily have $\Lambda > 1$.

THEOREM 1. *Assume that F is real: $F^+ = F$, $k^+ = k$. Let l be a prime number such that $\Omega^{(l)} \subseteq \boldsymbol{Q}(e^{2\pi i/m})$, l does not divide $u_0h^*t = n_0h^*t$, and*

$$l \geq \left(J\Lambda\left(1+\frac{\log\Lambda}{\Lambda-1}\right)\right)^{\varphi(n_0)}.$$

Then $C_F(l)$, the l-class group of F, is trivial.

Next, let $\boldsymbol{Q}'$ be the subfield of $\boldsymbol{Q}^S$ with degree $m^2/\prod_{p\in S}p$. We write h^- for the relative class number of $k\boldsymbol{Q}'$, namely, the positive integer defined as the ratio of the class number of $k\boldsymbol{Q}'$ to that of $(k\boldsymbol{Q}')^+ = k^+\boldsymbol{Q}'$. We put $m' = \prod_{p\in S}[u_0]_p$, and write t' for the

maximal divisor of the conductor of k relatively prime to m. Denoting by r the minimum of $[m]_p$ for all $p \in S$, we put

$$\delta = \max_{p \in S} \frac{p^{1/\varphi([m]_p)}(\log[m]_p + c)}{[m]_p}, \qquad \text{with } \ c = \frac{\pi}{r \sin(\pi/r)} - \log \frac{\pi}{2}.$$

Note that $c > 1 - \log(\pi/2) > 1/2$. For each abelian number field M, we let $\mathfrak{N}_M$ denote the norm map $C_M \to C_{M^+}$, and let $C_M^-(l)$ denote, for each prime number l, the l-primary component of the kernel of the group homomorphism $\mathfrak{N}_M$.

THEOREM 2. *Assume that F is imaginary. Let l be a prime number such that $\Omega^{(l)} \subseteq \boldsymbol{Q}(e^{2\pi i/m})$, l does not divide mh^-, and*

$$l \geq \left(\frac{\delta t' m' \prod_{p \in S} \tilde{p}}{2\pi} \right)^{\varphi(u_0)}.$$

Then $C_F^-(l)$ is trivial.

As $\mathfrak{N}_F$ is surjective by class field theory (in the case where F is imaginary), it turns out that, for each prime number l, $C_F(l)$ is trivial if and only if both $C_{F^+}(l)$ and $C_F^-(l)$ are trivial. Thus we obtain the following result from the above two theorems.

THEOREM 3. *Assume that F is imaginary. Let l be a prime number such that $\Omega^{(l)} \subseteq \boldsymbol{Q}(e^{2\pi i/m})$, l does not divide $n_0 h^* t h^-$, and*

$$l \geq \max \left(\left(J\Lambda \left(1 + \frac{\log \Lambda}{\Lambda - 1} \right) \right)^{\varphi(n_0)}, \ \left(\frac{\delta t' m' \prod_{p \in S} \tilde{p}}{2\pi} \right)^{\varphi(u_0)} \right).$$

Then $C_F(l)$ is trivial.

2. Proofs of main results.

In this section, we shall prove the first two theorems stated in the preceding section.

Given any primitive Dirichlet character χ, we denote by g_χ the order of χ, denote by f_χ the conductor of χ, put $\zeta_\chi = e^{2\pi i/f_\chi}$, and define χ^* to be the homomorphism of $\mathrm{Gal}(\boldsymbol{Q}(\zeta_\chi)/\boldsymbol{Q})$ into the multiplicative group $\boldsymbol{C}^\times = \boldsymbol{C} \setminus \{0\}$ such that, for each integer u relatively prime to f_χ, $\chi(u)$ is the image under χ^* of the automorphism in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_\chi)/\boldsymbol{Q})$ sending ζ_χ to ζ_χ^u. Let K_χ denote the fixed field in $\boldsymbol{Q}(\zeta_\chi)$ of the kernel of χ^*:

$$\mathrm{Gal}(\boldsymbol{Q}(\zeta_\chi)/K_\chi) = \mathrm{Ker}(\chi^*).$$

Then K_χ is a cyclic extension over $\boldsymbol{Q}$ of degree g_χ with conductor f_χ.

Next, suppose that $\chi(-1) = 1$, namely, K_χ is real and that χ is not principal. Let E_χ denote the group of units ε in K_χ such that, for every proper subfield L of K_χ, the norm of ε for K_χ/L is 1 or -1. Let

$$\theta_\chi = \prod_a \left(e^{\pi i a/f_\chi} - e^{-\pi i a/f_\chi}\right),$$

with the product taken over the odd integers a satisfying

$$\chi(a) = 1, \quad 0 < a < \frac{f_\chi}{\gcd(2, f_\chi)}.$$

Let $\mathfrak{R}_\chi$ denote the group ring of $\mathrm{Gal}(\boldsymbol{Q}(e^{\pi i/f_\chi})/\boldsymbol{Q})$ over the ring $\boldsymbol{Z}$ of (rational) integers. Take an automorphism σ of $\boldsymbol{Q}(e^{\pi i/f_\chi})$ for which the restriction $\sigma|\boldsymbol{Q}(\zeta_\chi)$ satisfies $\chi^*(\sigma|\boldsymbol{Q}(\zeta_\chi)) = e^{2\pi i/g_\chi}$, and put

$$\Delta = \prod_p (1 - \sigma^{g_\chi/p}) \qquad \text{in } \mathfrak{R}_\chi,$$

where p ranges over all prime divisors of g_χ. Considering the multiplicative group $\boldsymbol{Q}(e^{\pi i/f_\chi})^\times$ to be an $\mathfrak{R}_\chi$-module in the usual manner, let

$$\eta = \theta_\chi^\Delta,$$

and let H_χ denote the $\mathfrak{R}_\chi$-submodule of $\boldsymbol{Q}(e^{\pi i/f_\chi})^\times$ generated by η and -1. Note here that H_χ depends only on χ because η^2, an element of K_χ, does not depend on the choice of σ. It is known that H_χ is a subgroup of E_χ with finite index (cf. [**5**, Section 8]). We denote by h_χ the index of H_χ in E_χ:

$$h_\chi = (E_\chi : H_\chi).$$

Now, to prove Theorem 1, the following result is essential.

PROPOSITION 1. *Assume F to be real. Let l be a prime number not dividing $n_0 h^* t$ such that $\Omega^{(l)} \subseteq \boldsymbol{Q}(e^{2\pi i/m})$ and that $C_F(l)$ is not trivial. Then there exists a real number $x_0 > 1$ for which*

$$\frac{x_0^{\varphi(n_0)}}{\varphi(2v) n_0 w} < l < \left(J\left(\log x_0 + \frac{\log(t\kappa)}{\varphi(n_0)\sum_{p\in S}\varphi(p-1)}\right)\right)^{\varphi(n_0)}.$$

PROOF. Let $\mathfrak{X}$ be a set of nonprincipal primitive Dirichlet characters such that $K_\chi \subset F$ for each χ in $\mathfrak{X}$ and that, for any nonprincipal primitive Dirichlet character ψ with $K_\psi \subset F$, there exists just one Dirichlet character χ in $\mathfrak{X}$ satisfying $K_\chi = K_\psi$. For each subfield L of F, let $\mathfrak{X}(L)$ denote the set of Dirichlet characters χ in $\mathfrak{X}$ with $K_\chi \subseteq L$. Since $C_F(l)$ is not trivial, there exists a subfield K' of F of finite degree with class number divisible by l; $l \mid |C_{K'}|$. Since l does not divide $h^*[K'k\boldsymbol{Q}^* : \boldsymbol{Q}]$ by the hypothesis on l, we know from [**5**, Satz 21] that

$$\prod_{\chi\in\mathfrak{X}(K')}[h_\chi]_l = |C_{K'}(l)| > 1$$

and that

$$\prod_{\chi\in\mathfrak{X}(k\boldsymbol{Q}^*)}[h_\chi]_l = [h^*]_l = 1. \tag{2}$$

In particular, there exists a Dirichlet character ψ in $\mathfrak{X}(K')$ with $l \mid h_\psi$.

Next, for any subset R of S, let $\mathfrak{X}^R$ denote the set of Dirichlet characters χ in $\mathfrak{X}$ for which

$$\bigl\{p \in S \mid [f_\chi]_p = \tilde{p}[g_\chi]_p,\ [g_\chi]_p \geq [m]_p\bigr\} = R.$$

Obviously, $\mathfrak{X}$ is the disjoint union of $\mathfrak{X}^R$ for all subsets R of S. Hence there exists a unique subset R_0 of S such that ψ belongs to $\mathfrak{X}^{R_0}$. We note that $[f_\chi]_q \leq \tilde{q}[g_\chi]_q$ for every χ in $\mathfrak{X}$ and every prime number q. Therefore, a Dirichlet character χ in $\mathfrak{X}$ belongs to $\mathfrak{X}^\varnothing$ if and only if

$$[f_\chi]_p < \tilde{p}[g_\chi]_p \quad \text{or} \quad [f_\chi]_p = \tilde{p}[g_\chi]_p < \tilde{p}[m]_p$$

for every $p \in S$. As the first inequality above implies that $p[f_\chi]_p$ divides the product of $\tilde{p}$ and the exponent of $\mathrm{Gal}(k/\boldsymbol{Q})$, we see that any $\chi \in \mathfrak{X}^\varnothing$ satisfies $p[f_\chi]_p \leq \tilde{p}[n_0]_p$ for every $p \in S$. This fact gives $\mathfrak{X}^\varnothing \subseteq \mathfrak{X}(k\boldsymbol{Q}^*)$. Hence we obtain $R_0 \neq \varnothing$ from (2). It further follows that $[f_\psi]_p \geq \tilde{p}[m]_p$ for all $p \in R_0$. Hence f_ψ is not a prime number. Let us define a positive integer n_ψ by

$$n_\psi = g_\psi \prod_{p\in R_0}\frac{[m]_p}{[g_\psi]_p}.$$

Clearly, n_ψ divides g_ψ and is divisible by all prime divisors of g_ψ. Also, n_ψ divides n_0 since $[g_\psi]_p$ divides the exponent of $\mathrm{Gal}(k/\boldsymbol{Q})$ for every $p \in S \setminus R_0$ with $[f_\psi]_p < \tilde{p}[g_\psi]_p$. The hypothesis on l implies that $\boldsymbol{Q}(e^{2\pi i/n_\psi})$ contains the decomposition field of l for $\boldsymbol{Q}(e^{2\pi i/g_\psi})/\boldsymbol{Q}$ as well as that l does not divide $f_\psi g_\psi$. Therefore, by Proposition 2 of [**3**],

$$l < \sqrt{D_{n_\psi}}\left(\frac{2^{\lambda(\psi)-2}\varphi(f_\psi)\varphi(n_\psi)^2\Xi(n_\psi)}{(\log 2)g_\psi\sqrt{D_{n_\psi}}}\log\left(\frac{f_\psi}{\pi}+1\right)\right)^{\varphi(n_\psi)} \tag{3}$$

where $\lambda(\psi)$ denotes the number of distinct prime divisors of g_ψ; furthermore, by Proposition 4 of [**3**],

$$l > \frac{g_\psi}{\varphi(f_\psi)n_\psi}\left(\prod_{p\in R_0}\frac{p^{\varphi(p-1)}[f_\psi]_p}{((p-1)\varphi(\tilde{p}))^{\varphi(p-1)}[n_\psi]_p}\right)^{1/A} \tag{4}$$

where $A = \sum_{p \in R_0} \varphi(p-1)$ (for the corrections of Propositions 3, 4 of [**3**], see **3** of Section 4).

Now, the relation $n_\psi \mid n_0$ induces

$$\lambda(\psi) \le \lambda_0, \quad \varphi(n_\psi) \mid \varphi(n_0). \tag{5}$$

We know however that, for any integer $u \ge 3$,

$$\frac{\Xi(u)^{\varphi(u)}}{D_u^{(\varphi(u)-1)/2}} = \left(\left(1 - \frac{1}{\varphi(u)}\right)^{\varphi(u)} \prod_{p \mid u} \left(\frac{p-1}{p^{(p-2)/(p-1)}} \right)^{\varphi(u)} \right)^{(\varphi(u)-1)/2},$$

with p ranging over the prime divisors of u, and that the function $(1-1/\xi)^\xi$ of a real variable $\xi > 1$ is increasing. Therefore

$$\frac{\Xi(n_\psi)^{\varphi(n_\psi)}}{D_{n_\psi}^{(\varphi(n_\psi)-1)/2}} \le \frac{\Xi(n_0)^{\varphi(n_0)}}{D_{n_0}^{(\varphi(n_0)-1)/2}}. \tag{6}$$

We also have

$$\frac{f_\psi}{\pi} + 1 \le \left(\frac{1}{\pi} + \frac{1}{s} \right) f_\psi \le t\kappa \prod_{p \in R_0} [f_\psi]_p, \tag{7}$$

because $f_\psi \ge s$, $[f_\psi]_p \le [t]_p$ for each prime number p outside S, $[f_\psi]_p \le [n_0]_p \tilde{p}/p$ for each prime p in $S \setminus R_0$, and $R_0 \ne \varnothing$. Further, the integer $\varphi(f_\psi)/g_\psi$ divides $\varphi(2v)$:

$$\frac{\varphi(f_\psi)}{g_\psi} \;\Big|\; \varphi(2v). \tag{8}$$

Indeed, for each prime number p, $\varphi([f_\psi]_p)$ divides $\varphi(\tilde{p}[g_\psi]_p) = \varphi(\tilde{p})[g_\psi]_p$. We now let

$$x_0 = \left(\prod_{p \in R_0} [f_\psi]_p \right)^{1/(\varphi(n_0)A)},$$

so that

$$x_0 > 1, \quad \prod_{p \in R_0} [f_\psi]_p \le x_0^{\varphi(n_0) \sum_{p \in S} \varphi(p-1)}.$$

Since

$$\frac{2^{\lambda_0 - 2} \varphi(2v) \varphi(n_0)^2}{\log 2} \log \left(\frac{f_\psi}{\pi} + 1 \right) > 1,$$

it then follows from (3), (5), (6), (7), and (8) that

$$\begin{aligned} l &< \frac{\Xi(n_\psi)^{\varphi(n_\psi)}}{D_{n_\psi}^{(\varphi(n_\psi)-1)/2}}\left(\frac{2^{\lambda_0-2}\varphi(2v)\varphi(n_0)^2}{\log 2}\log\left(\frac{f_\psi}{\pi}+1\right)\right)^{\varphi(n_\psi)} \\ &\le \frac{\Xi(n_0)^{\varphi(n_0)}}{D_{n_0}^{(\varphi(n_0)-1)/2}}\left(\frac{2^{\lambda_0-2}\varphi(2v)\varphi(n_0)^2}{\log 2}\log\left(t\kappa x_0^{\varphi(n_0)\sum_{p\in S}\varphi(p-1)}\right)\right)^{\varphi(n_0)}. \end{aligned}$$

Thus

$$l < \left(J\left(\log x_0 + \frac{\log(t\kappa)}{\varphi(n_0)\sum_{p\in S}\varphi(p-1)}\right)\right)^{\varphi(n_0)}.$$

On the other hand,

$$\begin{aligned} &\log\left(\left(\prod_{p\in R_0}\frac{p^{\varphi(p-1)}}{((p-1)\varphi(\tilde{p}))^{\varphi(p-1)}[m]_p}\right)^{1/A}\right) \\ &\quad= \frac{\sum_{p\in R_0}\varphi(p-1)\log\left(p/((p-1)\varphi(\tilde{p})[m]_p^{1/\varphi(p-1)})\right)}{\sum_{p\in R_0}\varphi(p-1)} \\ &\quad\ge \min_{p\in R_0}\left(\log\frac{p}{(p-1)\varphi(\tilde{p})[m]_p^{1/\varphi(p-1)}}\right) \ge \log\frac{1}{w}, \end{aligned}$$

whence, by the fact that $[n_\psi]_p = [m]_p$ for every $p \in R_0$, we obtain

$$\left(\prod_{p\in R_0}\frac{p^{\varphi(p-1)}[f_\psi]_p}{((p-1)\varphi(\tilde{p}))^{\varphi(p-1)}[n_\psi]_p}\right)^{1/A} \ge \frac{x_0^{\varphi(n_0)}}{w}.$$

This, together with (4) and (8), yields

$$l > \frac{x_0^{\varphi(n_0)}}{\varphi(2v)n_0 w}.$$ □

Once Proposition 1 is verified, we can proceed to:

PROOF OF THEOREM 1. For simplicity, let

$$\alpha_1 = (\varphi(2v)n_0 w)^{1/\varphi(n_0)}J, \quad \alpha_2 = \frac{\log(t\kappa)}{\varphi(n_0)\sum_{p\in S}\varphi(p-1)},$$

$$\beta = \Lambda\left(1+\frac{\log\Lambda}{\Lambda-1}\right).$$

As is already seen, $\Lambda > 1$ so that $\beta > 1$. Since

$$\Lambda = \log \alpha_1 + \alpha_2, \quad \log \beta < \log \Lambda + \frac{\log \Lambda}{\Lambda - 1} = \frac{\Lambda \log \Lambda}{\Lambda - 1},$$

and since the function $\xi - \log \xi$ of a real variable $\xi \geq 1$ is increasing, we see that, for each real number x with $x/\alpha_1 \geq \beta$,

$$\begin{aligned} x - \alpha_1 \log x - \alpha_1 \alpha_2 &= \alpha_1 \left(\frac{x}{\alpha_1} - \log \frac{x}{\alpha_1} - \Lambda \right) \geq \alpha_1 (\beta - \log \beta - \Lambda) \\ &> \alpha_1 \left(\Lambda \left(1 + \frac{\log \Lambda}{\Lambda - 1} \right) - \frac{\Lambda \log \Lambda}{\Lambda - 1} - \Lambda \right) = 0. \end{aligned}$$

Now, contrary to the conclusion of the theorem, suppose that $C_F(l)$ is not trivial. Then, by Proposition 1,

$$\left(\frac{x_0 J}{\alpha_1} \right)^{\varphi(n_0)} < (J(\log x_0 + \alpha_2))^{\varphi(n_0)}, \quad \text{i.e.,} \quad x_0 - \alpha_1 \log x_0 - \alpha_1 \alpha_2 < 0,$$

x_0 being the same as in the proposition. Thus we have $x_0/\alpha_1 < \beta$, i.e., $x_0 < \alpha_1 \beta$. Threfore, for some real number x',

$$x_0 < x' < \alpha_1 \beta, \quad x' - \alpha_1 \log x' - \alpha_1 \alpha_2 = 0,$$

so that

$$J(\log x_0 + \alpha_2) < J(\log x' + \alpha_2) = \frac{J x'}{\alpha_1} < J\beta.$$

Proposition 1 implies however that $l < (J(\log x_0 + \alpha_2))^{\varphi(n_0)}$. We are thus led to a contradiction $l < (J\beta)^{\varphi(n_0)}$. Hence the theorem is proved. □

Next, let us give:

Proof of Theorem 2. Note first that m divides m' and that m' equals m if and only if, for each $p \in S$, the p-part of the exponent of $\mathrm{Gal}(k/\boldsymbol{Q})$ divides m. Since m'/m is not divisible by any prime number outside S, we may assume that $m' = m$.

For each positive integer n, let $\mathfrak{Y}_n$ denote the set of primitive Dirichlet characters χ with $\chi(-1) = -1$ such that K_χ is contained in the composite of k and the subfield of $\boldsymbol{Q}^S$ of degree n. Let Σ be the finite set of algebraic integers in the form

$$(1 - e^{2\pi i/u}) \sum_{a=1}^{\varphi(\tilde{u})/2} \frac{e^{2\pi i y_a/u}}{1 - e^{2\pi i f_{\chi,u} z_a/u}} \sum_{b=1}^{f_{\chi,u}} \chi(j_{a,b}) e^{2\pi i z_a b/u}. \tag{9}$$

Here u ranges over the integers >1 dividing m such that $\gcd(u, m/u) = 1$, $\tilde{u}$ denotes the product of $\tilde{p}$ for all distinct prime divisors p of u, χ runs through $\mathfrak{Y}_{m/u}$, $f_{\chi,u}$ denotes the maximal divisor of f_χ relatively prime to u, each y_a runs through $\boldsymbol{Z}$, each $j_{a,b}$ runs through $\boldsymbol{Z}$, and each z_a ranges over all integers relatively prime to u. Furthermore, we then denote by $g_{\chi,u}$ the maximal divisor of g_χ relatively prime to u, whence $ug_{\chi,u}$ is the least common multiple of u and g_χ by the assumption $m = m'$; we also let

$$\gamma_u = p^{1/\varphi(u)} \quad \text{or} \quad \gamma_u = 1$$

according as $u = [m]_p$ for some $p \in S$ or u is not a prime-power.

Now, in view of Theorem 1 of [**2**], it suffices to prove that every nonzero element of Σ is relatively prime to l (cf. [**4**, Section 2] as well). Noting that an element of Σ in the form (9) belongs to

$$\boldsymbol{Q}(e^{2\pi i/u}, e^{2\pi i/g_\chi}) = \boldsymbol{Q}(e^{2\pi i/(ug_{\chi,u})}),$$

let N be the norm for $\boldsymbol{Q}(e^{2\pi i/(ug_{\chi,u})})/\boldsymbol{Q}$ of that element of Σ. Put $\rho = e^{2\pi i/u}$ for simplicity. Let U_0 be the set of positive integers $< ug_{\chi,u}$ relatively prime to $ug_{\chi,u}$, U_1 the set of positive integers $< u$ relatively prime to u, and U_2 the set of all positive integers $< u/2$. Then

$$\begin{aligned}
|N| &\le \gamma_u^{\varphi(ug_{\chi,u})} \prod_{n\in U_0} \Bigg(\sum_{a=1}^{\varphi(\tilde{u})/2} \frac{f_{\chi,u}}{|1-\rho^{f_{\chi,u}z_a n}|} \Bigg) \\
&\le \gamma_u^{\varphi(ug_{\chi,u})} \Bigg(\frac{1}{\varphi(ug_{\chi,u})} \sum_{n\in U_0} \sum_{a=1}^{\varphi(\tilde{u})/2} \frac{f_{\chi,u}}{|1-\rho^{f_{\chi,u}z_a n}|} \Bigg)^{\varphi(ug_{\chi,u})} \\
&= \Bigg(\frac{\gamma_u \varphi(\tilde{u}) f_{\chi,u}}{2\varphi(u)} \sum_{n\in U_1} \frac{1}{|1-\rho^n|} \Bigg)^{\varphi(ug_{\chi,u})},
\end{aligned}$$

$$\begin{aligned}
\sum_{n\in U_1} \frac{1}{|1-\rho^n|} &= \sum_{n\in U_1} \frac{1}{2\sin(\pi n/u)} \le 2\Bigg(\sum_{n\in U_2} \frac{1}{2\sin(\pi n/u)} \Bigg) \\
&< 2\Bigg(\frac{1}{2\sin(\pi/u)} + \sum_{n\in U_2\setminus\{1\}} \frac{u}{\pi} \int_{\pi(n-1)/u}^{\pi n/u} \frac{dx}{2\sin x} \Bigg) \\
&< \frac{1}{\sin(\pi/u)} + \frac{u}{\pi} \int_{\pi/u}^{\pi/2} \frac{dx}{\sin x} = \frac{u}{\pi} \Bigg(\frac{\pi/u}{\sin(\pi/u)} + \log \frac{1}{\tan(\pi/(2u))} \Bigg) \\
&< \frac{u}{\pi} \Bigg(\frac{\pi/r}{\sin(\pi/r)} + \log \frac{2u}{\pi} \Bigg) = \frac{u(\log u + c)}{\pi}.
\end{aligned}$$

Hence

$$|N| < \left(\frac{\gamma_u f_{\chi,u}\varphi(\tilde{u})u(\log u + c)}{2\pi\varphi(u)}\right)^{\varphi(ug_{\chi,u})} = \left(\frac{f_{\chi,u}\gamma_u\tilde{u}(\log u + c)}{2\pi}\right)^{\varphi(ug_{\chi,u})}.$$

In addition,

$$ug_{\chi,u} \mid u_0, \quad \gamma_u\tilde{u}(\log u + c) > 3^{3/2}\left(\log 3 + \frac{1}{2}\right) > 2\pi,$$

and the ratio $t'm\tilde{m}/(u\tilde{u})$ is an integer divisible by $f_{\chi,u}$. We thus obtain

$$|N| < \left(\frac{t'm\tilde{m}\gamma_u(\log u + c)}{2\pi u}\right)^{\varphi(u_0)}.$$

On the other hand, the function $(\log\xi + c)/\xi$ of a real variable $\xi \geq e^{1-c}$ is decreasing. The definition of δ therefore yields

$$|N| < \left(\frac{t'm\tilde{m}\delta}{2\pi}\right)^{\varphi(u_0)}.$$

Hence, by the hypothesis on l, we can deduce that all nonzero elements of Σ are relatively prime to l. □

3. Additional results.

Based upon some results in Section 1 and in [**1**], [**3**], [**6**], we shall add below simple remarks mainly on the cardinality of C_F.

Let $\bar{S}$ denote the set of positive integers $\not\equiv 2 \pmod 4$ not divisible by any prime number outside S but divisible by all prime numbers in S:

$$\bar{S} = \{u \in \boldsymbol{Z} \mid \ u > 0, \ \ u \not\equiv 2 \pmod 4, \ \ \boldsymbol{Q}^S(e^{2\pi i/u}) = \Omega\}.$$

In particular, m belongs to $\bar{S}$. At first, suppose F to be imaginary, so that k is also imaginary. Let p be any prime number in S, and let k_∞ denote the basic $\boldsymbol{Z}_p$-extension over k, namely, the intermediate field of F/k such that $\mathrm{Gal}(k_\infty/k)$ is topologically isomorphic to the additive group of $\boldsymbol{Z}_p$. Then, by Corollary 3 of [**6**, Section V], there exist infinitely many prime numbers l for which $C^-_{k_\infty}(l)$ is not trivial. However, for any prime number l outside S, the natural homomorphism $C_{k_\infty}(l) \to C_F(l)$ is injective and maps $C^-_{k_\infty}(l)$ into $C^-_F(l)$. Corollary 3 of [**6**, Section V] thus implies that there are infinitely many prime numbers l for which $C^-_F(l)$ is not trivial. Furthermore, the composite of $\boldsymbol{Q}(e^{2\pi i/u})$ for all $u \in \bar{S}$ coincides with Ω. Hence, from Theorem 2, we obtain the following result.

Proposition 2. *If F is imaginary, then for any $u \in \bar{S}$, there exist an example of m and a prime number l such that $\Omega^{(l)} \not\subseteq \boldsymbol{Q}(e^{2\pi i/u})$, $\Omega^{(l)} \subseteq \boldsymbol{Q}(e^{2\pi i/m})$, $C^-_F(l)$ is not trivial, and either $l \mid h^-$ or*

$$l < \left(\frac{\delta t' m' \prod_{p\in S} \tilde{p}}{2\pi}\right)^{\varphi(u_0)}.$$

REMARK. In the proposition, one can choose the example of m to be a multiple of u; moreover, the condition $\Omega^{(l)} \not\subseteq \boldsymbol{Q}(e^{2\pi i/u})$ implies that $l^{\varphi(\tilde{p})} \equiv 1 \pmod{p[u]_p}$ for some $p \in S$ whence $l > \min_{q\in S}(q[u]_q)^{1/\varphi(\tilde{q})}$.

Certainly, as above, C_F is infinite whenever F is imaginary, but we have not find any real example of F for which the statement $|C_F| = \infty$ is proved or disproved. Let C'_F denote the direct sum in C_F of $C_F(l)$ for all prime numbers l outside S;

$$C_F = C'_F \oplus \left(\bigoplus_{p\in S} C_F(p)\right).$$

In any case, the assertion (A) in the main theorem of [**1**] guarantees the finiteness of $C_F(l)$ for every prime number l outside S. Therefore, Theorem 1 of [**3**] or Theorem 1 of Section 1 yields at least:

PROPOSITION 3. *Assume that F is real. Then C'_F is finite if and only if there exists an element u' of $\bar{S}$ with the property that $C_F(l)$ is trivial for any prime number l satisfying $\Omega^{(l)} \not\subseteq \boldsymbol{Q}(e^{2\pi i/u'})$.*

We conclude this section with:

REMARK. If F is real, then Greenberg's conjecture on $\boldsymbol{Z}_l$-extensions for prime numbers l implies that $C_F(p)$ is trivial for all $p \in S$, namely, that $C_F = C'_F$.

4. Corrections to [3], [4].

Finally, we shall correct some mistakes in [**3**], [**4**]. The first and second corrections are due to one of the referee's comments on the present paper. The last correction is necessary to justify the proof of Theorem 1.

1. The clause "if and only if $l^{\varphi(\tilde{p})} \not\equiv 1 \pmod{\mu_p\tilde{p}}$ for any $p \in S$" in the 11th line from the bottom on [**3**, p. 828] should be "if and only if, for each $p \in S$, either $l^{\varphi(\tilde{p})} \not\equiv 1 \pmod{p\mu_p}$ or $\mu_p \parallel l-1$ with $p = 2$". Accordingly, when 2 belongs to S, the 7th line from the bottom on [**3**, p. 828] should be

$$\liminf_{x\to\infty} \frac{|\boldsymbol{P}_F(x)|}{\pi(x)} \geq \lim_{x\to\infty} \frac{|\boldsymbol{P}_0(x)|}{\pi(x)} = \left(1 - \frac{3}{\mu_2}\right) \prod_{p\in S\setminus\{2\}} \left(1 - \frac{1}{\mu_p}\right).$$

2. Quite similarly to the above, the condition "$l^{\varphi(q)} \not\equiv 1 \pmod{qp^\nu}$" in [**4**, Theorems 1, 2 and Proposition], line 11 on [**4**, p. 376], lines 16, 21 on [**4**, p. 390], and line 17 on [**4**, p. 392] must be changed into the condition that "either $l^{\varphi(q)} \not\equiv 1 \pmod{p^{\nu+1}}$ or $2^\nu \parallel l-1$ with $p = 2$". Along with this, line 15 on [**4**, p. 393] should be changed, for example, into

$$\geq \lim_{x\to\infty} \frac{\left|\{l \in P(x) \mid \ l^{\varphi(q)} \not\equiv 1 \pmod{p^{\nu+1}}\}\right|}{\pi(x)} = 1 - \frac{q^2}{p^{\nu+2}}.$$

3. In [**3**, Proposition 3], we should additionally assume that "n is divisible by all prime divisors of g_χ". Indeed, without such a hypothesis, we can not always define $b_{\boldsymbol{x},u,j}$ for $(\boldsymbol{x}, u, j) \in \mathscr{F}$ and $b_{\boldsymbol{w},u}$ for $(\boldsymbol{w}, u) \in \mathfrak{B} \times I$ in the proof of [**3**, Proposition 3] (cf. [**3**, pp. 844, 850]) while the hypothesis guarantees the definitions of all $b_{\boldsymbol{x},u,j}$ and all $b_{\boldsymbol{w},u}$. Furthermore, the proof of [**3**, Proposition 4] is based upon [**3**, Proposition 3]. We must therefore replace [**3**, Proposition 4] by the following:

PROPOSITION 4. *Let l be a prime number, n be a positive divisor of g_χ divisible by all prime divisors of g_χ such that $\boldsymbol{Q}(\zeta_n)$ contains the decomposition field of l for $\boldsymbol{Q}(\zeta_{g_\chi})/\boldsymbol{Q}$, and R be a finite subset of $\boldsymbol{P}$ such that every p in R satisfies $\tilde{p} \mid n$ and $f(p) = \tilde{p}g(p)$. Suppose that*

$$l \mid h_\chi, \quad l \nmid f_\chi g_\chi, \quad R \neq \varnothing.$$

Then

$$l > \frac{g_\chi}{\varphi(f_\chi)n} \left(\prod_{p\in R} \frac{p^{\varphi(p-1)} f(p)}{((p-1)\varphi(\tilde{p}))^{\varphi(p-1)} \nu_p} \right)^{1/\sum_{p\in R}\varphi(p-1)}$$

where, for each p in R, ν_p denotes the p-part of n.

On the other hand, as for the proof of [**3**, Theorem 1], [**3**, Proposition 3] is used only to prove [**3**, Proposition 4], and [**3**, Proposition 4] only to prove [**3**, Proposition 5]. Since n_ψ is divisible by all prime divisors of g_ψ (cf. [**3**, p. 854]), we can use the above Proposition 4 instead of [**3**, Proposition 4] in the proof of [**3**, Proposition 5] (cf. [**3**, p. 855]). Similarly, for our proof of Theorem 1, we can do the same in the proof of Proposition 1 (cf. (4)). In passing, "G_1 containing" in lines 12, 13 of [**3**, p. 849] should be "the group generated in G_1 by".

References

[1] E. Friedman, Ideal class groups in basic $\boldsymbol{Z}_{p_1} \times \cdots \times \boldsymbol{Z}_{p_s}$-extensions of abelian number fields, Invent. Math., **65** (1981/82), 425–440.

[2] K. Horie, Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field, J. London Math. Soc. (2), **66** (2002), 257–275.

[3] K. Horie, Triviality in ideal class groups of Iwasawa-theoretical abelian number fields, J. Math. Soc. Japan, **57** (2005), 827–857.

[4] K. Horie, The ideal class group of the basic $\boldsymbol{Z}_p$-extension over an imaginary quadratic field, Tohoku Math. J., **57** (2005), 375–394.

[5] H. W. Leopoldt, Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper, Abh. Deutsch. Acad. Wiss. Berlin, Kl. Math. Nat., 1953, **2**, Akademie-Verlag, Berlin, 1954.

[6] L. C. Washington, Class numbers and $\boldsymbol{Z}_p$-extensions, Math. Ann., **214** (1975), 177–193.

[7] L. C. Washington, Introduction to Cyclotomic Fields, Second Edition (GTM, 83), Springer-Verlag, New York, 1996.

Kuniaki Horie
Department of Mathematics
Tokai University
1117, Kitakaname, Hiratsuka
Kanagawa 259-1292
Japan