J. Math. Soc. Japan
Vol. 57, No. 3, 2005

Triviality in ideal class groups of Iwasawa-theoretical abelian number fields

By Kuniaki HORIE

(Received Mar. 1, 2004)
(Revised Oct. 25, 2004)

Abstract. Let S be a non-empty finite set of prime numbers and, for each p in S, let $\boldsymbol{Z}_p$ denote the ring of p-adic integers. 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 $\boldsymbol{Z}_p$ for all p in S. We shall prove that each of certain arithmetic progressions contains only finitely many prime numbers l for which the l-class group of F is nontrivial. This result implies our conjecture in [**3**] that the set of prime numbers l for which the l-class group of F is trivial has natural density 1 in the set of all prime numbers.

Introduction.

Let $\boldsymbol{C}$ denote the field of complex numbers, $\boldsymbol{Q}$ the field of rational numbers, and $\boldsymbol{P}$ the set of all prime numbers. By a number field, we mean an algebraic extension of $\boldsymbol{Q}$ in $\boldsymbol{C}$, not necessarily finite over $\boldsymbol{Q}$. When k is any number field, we let C_k denote the ideal class group of k and, for each $l \in \boldsymbol{P}$, we let $C_k(l)$ denote the l-class group of k, namely, the l-primary component of C_k. A number field is called abelian if it is an abelian extension over $\boldsymbol{Q}$. We put, in $\boldsymbol{C}$,

$$\zeta_m = e^{2\pi i/m}$$

for each positive integer m.

Now, let S be a non-empty finite set of prime numbers:

$$S \subset \boldsymbol{P}, \quad 1 \leq |S| < \infty.$$

For each $p \in \boldsymbol{P}$, let $\boldsymbol{Z}_p$ denote the ring of p-adic integers, and let

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

according as $p > 2$ or $p = 2$. Let $\boldsymbol{Q}^S$ denote the abelian number field such that the Galois group $\mathrm{Gal}(\boldsymbol{Q}^S/\boldsymbol{Q})$ is isomorphic, as a profinite group, to the additive group of the direct product $\prod_{p \in S} \boldsymbol{Z}_p$. Let F be an abelian number field which is a finite extension of $\boldsymbol{Q}^S$. In this paper, we shall prove:

2000 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R23, 11R27.

Key Words and Phrases. abelian number field, ideal class group, Iwasawa theory, class number formula.

Theorem 1. *Let m_0 be any positive integer divisible by $\tilde{p}$ for every prime number p in S. Then there exist only finitely many prime numbers l such that $C_F(l)$ is nontrivial and that $\boldsymbol{Q}(\zeta_{m_0})$ contains the decomposition field of l for the abelian extension $\boldsymbol{Q}^S(\zeta_{m_0})/\boldsymbol{Q}$.*

Most of the paper consists of the proof of the above theorem including not a few preliminaries. To explain briefly the heart of the proof, let F^+ be the maximal real subfield of F, and C_F^- the kernel of the norm map of C_F into C_{F^+}; for each $l \in \boldsymbol{P}$, let $C_F^-(l)$ denote the l-primary component of C_F^-. Obviously, C_F^- is trivial if F itself is real. We have actually shown in [**3**] that, under the hypothesis of Theorem 1, there exist only finitely many prime numbers l such that $C_F^-(l)$ is nontrivial and such that $\boldsymbol{Q}(\zeta_{m_0})$ contains the decomposition field of l for $\boldsymbol{Q}^S(\zeta_{m_0})/\boldsymbol{Q}$ (for the basic case where $|S| = 1$, see Washington [**6**, IV]). With this fact in mind, we shall naturally concentrate on the study of primary subgroups of C_{F^+}, which is based on the algebraic interpretation by Leopoldt [**5**], involving circular units in F^+, of the analytic class number formula for subfields of F^+ with finite degrees. In the major part §§1–4 of the paper, conforming to the description of [**5**], we shall generalize or pursue many of our arguments in [**3**]. We shall prove Theorem 1 in §5 by means of results in [**3**], [**5**] and the preceding sections. Finally, in §6, some problems together with some additional facts will be mentioned in relation to Theorem 1.

Let us now give a consequence of the theorem. Take a real variable x, and let

$$\pi(x) = |\{l \mid l \in \boldsymbol{P},\ l \leq x\}|$$

as usual. Let $\boldsymbol{P}_F(x)$ denote the set of prime numbers $l \leq x$ for which $C_F(l)$ is trivial. Let m_0 be the same as in Theorem 1, and let $\boldsymbol{P}_0(x)$ denote the set of prime numbers $l \leq x$ such that $\boldsymbol{Q}(\zeta_{m_0})$ contains the decomposition field of l for $\boldsymbol{Q}^S(\zeta_{m_0})/\boldsymbol{Q}$. We then easily see that the decomposition field of a prime number $l \notin S$ for $\boldsymbol{Q}^S(\zeta_{m_0})/\boldsymbol{Q}$ is contained in $\boldsymbol{Q}(\zeta_{m_0})$ if and only if $l^{\varphi(\tilde{p})} \not\equiv 1 \pmod{\mu_p \tilde{p}}$ for any $p \in S$. Here φ denotes the Euler function and, for each $p \in S$, μ_p denotes the p-part of m_0, that is, the highest power of p dividing m_0. Hence Theorem 1, together with the prime number theorem for arithmetic progressions, shows that

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

However, for all $p \in S$, μ_p can be arbitrarily large independent of F. We thus obtain the following result conjectured in [**3**, §3]:

Theorem 2.

$$\lim_{x \to \infty} \frac{|\boldsymbol{P}_F(x)|}{\pi(x)} = 1.$$

Remark. Among a number of important results on subgroups of C_F provided by Iwasawa theory (see Friedman [**1**], Washington [**7**], etc.), it is known not only that $C_F(l)$

is finite for every l in $\boldsymbol{P} \setminus S$ but that, if F is imaginary, then there exist infinitely many l in $\boldsymbol{P}$ for which $C_F^-(l)$ is nontrivial (cf. [**6**, V]).

Throughout the paper, $\boldsymbol{R}$ will denote the field of real numbers, and $\boldsymbol{Z}$ the ring of (rational) integers. For any finite extension k'/k of number fields, we let $N_{k'/k}$ denote the norm map of k' into k. For each complex number $z \neq 0$, we let $\langle z \rangle$ denote the cyclic group generated by z in the multiplicative group $\boldsymbol{C}^\times = \boldsymbol{C} \setminus \{0\}$: $\langle z \rangle = \{z^a \mid a \in \boldsymbol{Z}\}$. All Dirichlet characters are assumed to be primitive.

Acknowledgement. The author expresses his heartfelt gratitude to the referee who carefully read the paper, kindly corrected some mistakes, and offered several invaluable suggestions (cf., for example, the proofs of Proposition 1).

1.

We shall first give several definitions, mainly following [**5**].

Let ψ be any (primitive) Dirichlet character, and let f_ψ denote the conductor of ψ. Then ψ defines a homomorphism ψ^* of $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{f_\psi})/\boldsymbol{Q})$ into $\boldsymbol{C}^\times$ such that, for each $u \in \boldsymbol{Z}$ relatively prime to f_ψ, $\psi(u)$ is the image under ψ^* of the automorphism in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{f_\psi})/\boldsymbol{Q})$ mapping ζ_{f_ψ} to $\zeta_{f_\psi}^u$. Let g_ψ denote the order of ψ, and let K_ψ denote the fixed field of $\mathrm{Ker}(\psi^*)$ in $\boldsymbol{Q}(\zeta_{f_\psi})$;

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

It follows that K_ψ is a cyclic extension over $\boldsymbol{Q}$ of degree g_ψ with conductor f_ψ.

We assume from now that ψ is even or, equivalently, K_ψ is real:

$$\psi(-1) = 1, \quad K_\psi \subset \boldsymbol{R}.$$

Let E_ψ denote the group of units ε of K_ψ such that $N_{K_\psi/k}(\varepsilon) = \pm 1$ for every proper subfield k of K_ψ. Note that

$$E_\psi \supseteq \langle -1 \rangle = \{\pm 1\}$$

and that every conjugate over $\boldsymbol{Q}$ of an element of E_ψ also belongs to E_ψ. If a unit ε in E_ψ belongs to a proper subfield k of K_ψ, then $\varepsilon^{2[K_\psi:k]} = N_{K_\psi/k}(\varepsilon)^2 = 1$ so that $\varepsilon^2 = 1$. Thus

$$K_\psi = \boldsymbol{Q}(\varepsilon) \qquad \text{for every } \varepsilon \text{ in } E_\psi \setminus \{\pm 1\}. \tag{1}$$

Remark 1. The elements of E_ψ are the proper $\widehat{\psi}$-relative units in the sense of Leopoldt (cf. [**5**, §4]), where $\widehat{\psi}$ denotes the rational irreducible character of Gal $(\boldsymbol{Q}(\zeta_{f_\psi})/\boldsymbol{Q})$ such that

$$\widehat{\psi}(\tau) = \sum_u \psi^*(\tau)^u \qquad \text{for all } \tau \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_{f_\psi})/\boldsymbol{Q}),$$

the sum taken over the positive integers $u \le g_\psi$ with $\gcd(u, g_\psi) = 1$.

Next, let σ be any generator of $\mathrm{Gal}(K_\psi/\boldsymbol{Q})$, and let α run through $\boldsymbol{Z}[\zeta_{g_\psi}]$. For each α, there uniquely exist integers $a_1, \cdots, a_{\varphi(g_\psi)}$ satisfying

$$\alpha = \sum_{j=1}^{\varphi(g_\psi)} a_j \zeta_{g_\psi}^{j-1},$$

so we define

$$\alpha_\sigma = \sum_{j=1}^{\varphi(g_\psi)} a_j \sigma^{j-1}$$

in $\boldsymbol{Z}[\mathrm{Gal}(K_\psi/\boldsymbol{Q})]$, the group ring of $\mathrm{Gal}(K_\psi/\boldsymbol{Q})$ over $\boldsymbol{Z}$. It follows that $\varepsilon^{\alpha_\sigma}$ always belongs to E_ψ as ε runs through E_ψ. The map $(\alpha, \varepsilon^2) \mapsto \varepsilon^{2\alpha_\sigma}$ then defines an action of the Dedekind domain $\boldsymbol{Z}[\zeta_{g_\psi}]$ on the abelian group $E_\psi^2 = \{\varepsilon^2 \mid \varepsilon \in E_\psi\}$, since the definition of E_ψ implies that ε^2 is annihilated by

$$\sum_{u=1}^{g_\psi/n} \sigma^{(u-1)n}$$

for all positive divisors n of g_ψ smaller than g_ψ, and since the g_ψ-th cyclotomic polynomial in an indeterminate y is the monic greatest common divisor in $\boldsymbol{Z}[y]$ of

$$\sum_{u=1}^{g_\psi/n} y^{(u-1)n} = \frac{y^{g_\psi} - 1}{y^n - 1}$$

for all positive divisors n of g_ψ smaller than g_ψ. At the same time, the quotient group $E_\psi/\langle -1 \rangle$ is made into a unitary $\boldsymbol{Z}[\zeta_{g_\psi}]$-module by the map $(\alpha, \{\pm\varepsilon\}) \mapsto \{\pm\varepsilon^{\alpha_\sigma}\}$, and the map $\varepsilon^2 \mapsto \{\pm\varepsilon\}$ defines a $\boldsymbol{Z}[\zeta_{g_\psi}]$-isomorphism

$$\iota_\psi : E_\psi^2 \xrightarrow{\sim} E_\psi/\langle -1 \rangle.$$

Henceforth, we assume further that the even Dirichlet character ψ is nonprincipal. It is verified in [**5**, §§5–6] that the $\boldsymbol{Z}[\zeta_{g_\psi}]$-modules E_ψ^2, $E_\psi/\langle -1 \rangle$ are isomorphic to a nonzero ideal of $\boldsymbol{Z}[\zeta_{g_\psi}]$. Now we let

$$\theta_\psi = \prod_b \left(\zeta_{2f_\psi}^b - \zeta_{2f_\psi}^{-b} \right),$$

with the product taken over the integers b satisfying

$$\psi(b) = 1, \quad 2 \nmid b, \quad 0 < b < \frac{f_\psi}{\gcd(2, f_\psi)}.$$

Note that the number of such integers b is $\varphi(f_\psi)/2g_\psi$. Take an automorphism $\boldsymbol{s}_\psi$ in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{f_\psi})/\boldsymbol{Q})$ for which

$$\psi^*(\boldsymbol{s}_\psi) = \zeta_{g_\psi},$$

so that the restriction $\boldsymbol{s}_\psi|K_\psi$ is a generator of the cyclic group $\mathrm{Gal}(K_\psi/\boldsymbol{Q})$. Fix an extension $\boldsymbol{\sigma}(\psi)$ of $\boldsymbol{s}_\psi$ in $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{2f_\psi})/\boldsymbol{Q})$, and put

$$\Delta(\psi) = \prod_p \left(1 - \boldsymbol{\sigma}(\psi)^{g_\psi/p}\right)$$

in $\boldsymbol{Z}[\mathrm{Gal}(\boldsymbol{Q}(\zeta_{2f_\psi})/\boldsymbol{Q})]$, where p ranges over the prime divisors of g_ψ. Considering $\boldsymbol{Q}(\zeta_{2f_\psi})^\times$ to be a module over $\boldsymbol{Z}[\mathrm{Gal}(\boldsymbol{Q}(\zeta_{2f_\psi})/\boldsymbol{Q})]$ in the obvious manner, we then let

$$\eta_\psi = \theta_\psi^{\Delta(\psi)}.$$

This belongs to E_ψ; because the real number $\theta_\psi^{1-\boldsymbol{\sigma}(\psi)}$ is a unit of K_ψ, θ_ψ^2 is the product of $(-1)^{\varphi(f_\psi)/2g_\psi}$ and the norm of $1-\zeta_{f_\psi}$ for $\boldsymbol{Q}(\zeta_{f_\psi})/K_\psi$, and

$$N_{K_\psi/k}\left(\theta_\psi^2\right)^{\Delta(\psi)} = 1$$

for each subfield k of K_ψ with $[K_\psi : k] \in \boldsymbol{P}$. We also easily see that the class $\{\pm\eta_\psi\}$ in $E_\psi/\langle -1\rangle$ as well as η_ψ^2 in E_ψ^2 does not depend on the choice of $\boldsymbol{s}_\psi$ or $\boldsymbol{\sigma}(\psi)$ but depends only on ψ.

REMARK 2. Unless g_ψ is 2 or a power of an odd prime, η_ψ itself depends only on ψ.

Let H_ψ denote the subgroup of E_ψ generated by -1 and by all conjugates of η_ψ over $\boldsymbol{Q}$. It then follows from the class number formula for K_ψ that the index of H_ψ in E_ψ is finite (cf. [**5**, §8]). We write h_ψ for the index:

$$h_\psi = (E_\psi : H_\psi) < \infty.$$

On the other hand, H_ψ^2 becomes a cyclic $\boldsymbol{Z}[\zeta_{g_\psi}]$-submodule of E_ψ^2 generated by η_ψ^2, the quotient group $H_\psi/\langle -1\rangle$ becomes a cyclic $\boldsymbol{Z}[\zeta_{g_\psi}]$-submodule of $E_\psi/\langle -1\rangle$ generated by $\{\pm\eta_\psi\}$ so that the quotient group E_ψ/H_ψ becomes a $\boldsymbol{Z}[\zeta_{g_\psi}]$-module, and ι_ψ induces $\boldsymbol{Z}[\zeta_{g_\psi}]$-isomorphisms

$$H_\psi^2 \xrightarrow{\sim} H_\psi/\langle -1\rangle, \quad E_\psi^2/H_\psi^2 \xrightarrow{\sim} E_\psi/H_\psi.$$

Thus the $\boldsymbol{Z}[\zeta_{g_\psi}]$-modules H_ψ^2, $H_\psi/\langle -1\rangle$ are isomorphic to $\boldsymbol{Z}[\zeta_{g_\psi}]$.

2.

The purpose of this section is to prove some preliminary results for the proof of Theorem 1. Let χ be a nonprincipal even Dirichlet character, which will be fixed throughout the section:

$$\chi(-1)=1, \quad g_\chi \geq 2, \quad f_\chi \geq 5.$$

We shall put, for simplicity,

$$f=f_\chi, \quad g=g_\chi$$

in the proofs of our assertions.

Proposition 1. *Let l be a prime number not dividing g_χ, σ a generator of* $\mathrm{Gal}(K_\chi/\boldsymbol{Q})$, *and k an extension in $\boldsymbol{Q}(\zeta_{g_\chi})$ of the decomposition field of l for $\boldsymbol{Q}(\zeta_{g_\chi})/\boldsymbol{Q}$. Then l divides h_χ if and only if there exists a prime ideal $\mathfrak{l}$ of k dividing l such that the absolute value $\left|\eta_\chi^{\alpha_\sigma}\right|$ is an l-th power in E_χ for any element α of the integral ideal $l\mathfrak{l}^{-1}$ of k.*

Proof. Let d be the degree of $\boldsymbol{Q}(\zeta_g)$ over k:

$$d=[\boldsymbol{Q}(\zeta_g):k], \quad g=g_\chi.$$

Let $\mathfrak{o}$ be the ring of algebraic integers in k. Then $1, \zeta_g, \cdots, \zeta_g^{d-1}$ form a free basis of the $\mathfrak{o}$-module $\boldsymbol{Z}[\zeta_g]$;

$$\boldsymbol{Z}[\zeta_g]=\mathfrak{o} \oplus \mathfrak{o}\zeta_g \oplus \cdots \oplus \mathfrak{o}\zeta_g^{d-1}.$$

Assume first that l divides h_χ. Since the finite $\boldsymbol{Z}[\zeta_g]$-module E_χ/H_χ is isomorphic, as an $\mathfrak{o}$-module, to the direct sum $\bigoplus_{\mathfrak{a}\in\mathscr{S}}(\mathfrak{o}/\mathfrak{a})$ for some finite set $\mathscr{S}$ of nonzero ideals of $\mathfrak{o}$, there are a prime ideal $\mathfrak{l}$ of k dividing l and an injective $\mathfrak{o}$-module homomorphism $\mathfrak{o}/\mathfrak{l} \to E_\chi/H_\chi$. Hence there exists a unit ε in $E_\chi \setminus H_\chi$ such that every β in $\mathfrak{l}$ satisfies $\varepsilon^{\beta_\sigma} \in H_\chi$, namely, $\varepsilon^{2\beta_\sigma} \in H_\chi^2$. In particular,

$$\varepsilon^{2l}=\eta_\chi^{2\omega_\sigma} \tag{2}$$

with some ω in $\boldsymbol{Z}[\zeta_g]$, which is expressed uniquely in the form

$$\omega=\sum_{j=1}^{d}\gamma_j\zeta_g^{j-1} \qquad \text{with } \gamma_1, \cdots, \gamma_d \in \mathfrak{o}.$$

Let $\mathfrak{L}$ be the ideal of $\boldsymbol{Z}[\zeta_g]$ generated by $\mathfrak{l}$. Then, as an $\mathfrak{o}$-module, $\mathfrak{L}$ coincides with $\mathfrak{l} \oplus \mathfrak{l}\zeta_g \oplus \cdots \oplus \mathfrak{l}\zeta_g^{d-1}$ and, by the hypothesis of the proposition, $\mathfrak{L}$ is the only prime ideal of $\boldsymbol{Q}(\zeta_g)$ dividing $\mathfrak{l}$. Let us consider the case $\omega \in \mathfrak{L}$. In this case, $\gamma_1, \cdots, \gamma_d$ belong to $\mathfrak{l}$. As

$\mathfrak{l}$ is unramified for $k/\boldsymbol{Q}$, there exists an algebraic integer β' in $l\mathfrak{l}^{-1}$ satisfying $1-\beta' \in \mathfrak{l}$. We note that $\beta'\gamma_1 l^{-1}, \cdots, \beta'\gamma_d l^{-1}$ belong to $\mathfrak{o}$. On the other hand, (2) gives

$$\varepsilon^{2l\beta'_\sigma} = \eta_\chi^{2(\sum_{j=1}^d \beta'\gamma_j\zeta_g^{j-1})_\sigma}.$$

Consequently,

$$\varepsilon^2 = \varepsilon^{2(1-\beta'+\beta')_\sigma} = \varepsilon^{2(1-\beta')_\sigma}\eta_\chi^{2(\sum_{j=1}^d \beta'\gamma_j l^{-1}\zeta_g^{j-1})_\sigma} \in H_\chi^2.$$

This is a contradiction, however. Thus the case $\omega \in \mathfrak{L}$ does not occur. Let $\mathfrak{G} = \mathrm{Gal}(\boldsymbol{Q}(\zeta_g)/k)$. Then

$$\omega^\tau \notin \mathfrak{L} \qquad \text{for any } \tau \text{ in } \mathfrak{G}, \tag{3}$$

since $\mathfrak{L}$ is invariant under τ. We next define a square matrix Y of degree d with coefficients in $\mathfrak{o}$ by

$$Y\begin{pmatrix} 1 \\ \zeta_g \\ \vdots \\ \zeta_g^{d-1} \end{pmatrix} = \omega \begin{pmatrix} 1 \\ \zeta_g \\ \vdots \\ \zeta_g^{d-1} \end{pmatrix}.$$

Clearly,

$$Y\begin{pmatrix} 1 \\ \zeta_g^\tau \\ \vdots \\ \zeta_g^{(d-1)\tau} \end{pmatrix} = \omega^\tau \begin{pmatrix} 1 \\ \zeta_g^\tau \\ \vdots \\ \zeta_g^{(d-1)\tau} \end{pmatrix} \qquad \text{for all } \tau \text{ in } \mathfrak{G},$$

so that

$$\det(Y) = \prod_{\tau\in\mathfrak{G}} \omega^\tau.$$

Hence it follows from (3) that

$$\det(Y) \notin \mathfrak{l}, \quad \text{i.e.,} \quad 1-\beta''\det(Y) \in \mathfrak{l} \ \text{ for some } \beta'' \text{ in } \mathfrak{o}.$$

Now let α be any element of $l\mathfrak{l}^{-1}$. We then find that

$$\eta_\chi^{\alpha_\sigma} = \eta_\chi^{(\det(Y))_\sigma(\alpha\beta'')_\sigma}\eta_\chi^{(\alpha(1-\beta''\det(Y)))_\sigma}.$$

Furthermore, from (2), we obtain $\eta_\chi^{2(\omega\zeta_g^{j-1})_\sigma} = \varepsilon^{2l(\zeta_g^{j-1})_\sigma}$ as j runs through $\{1, \cdots, d\}$, and hence, by the definition of Y,

$$\eta_\chi^{2(\det(Y))_\sigma} = \varepsilon^{2l(\sum_{j=1}^{d} \partial_j \zeta_g^{j-1})_\sigma},$$

with ∂_j denoting the $(j,1)$-cofactor of Y. Since l divides $\alpha(1-\beta'' \det(Y))$, it follows that $\eta_\chi^{2\alpha_\sigma}$ is a $2l$-th power in E_χ^2, namely, $\left|\eta_\chi^{\alpha_\sigma}\right|$ is an l-th power in E_χ.

Next, without assuming $l \mid h_\chi$, let α' be any algebraic integer in $l\mathfrak{l}^{-1}$ such that l is relatively prime to $\alpha' l^{-1}\mathfrak{l}$, and assume that $\left|\eta_\chi^{\alpha'_\sigma}\right|$ is an l-th power in E_χ. Then

$$H_\chi^{2\alpha'_\sigma} = \left\{\eta_\chi^{2\alpha'_\sigma \gamma_\sigma} \mid \gamma \in \boldsymbol{Z}[\zeta_g]\right\} \subseteq E_\chi^{2l}.$$

We also know that

$$\left(E_\chi^2 : H_\chi^2\right) = h_\chi, \quad \left(E_\chi^2 : E_\chi^{2l}\right) = l^{\varphi(g)}, \quad \left(H_\chi^2 : H_\chi^{2\alpha'_\sigma}\right) = \left|N_{\boldsymbol{Q}(\zeta_g)/\boldsymbol{Q}}(\alpha')\right|.$$

Let d' be the degree of $\boldsymbol{Q}(\zeta_g)$ over the decomposition field of l for $\boldsymbol{Q}(\zeta_g)/\boldsymbol{Q}$. As l does not divide g, our choice of α' implies that $l^{\varphi(g)-d'}$ is the l-part of $N_{\boldsymbol{Q}(\zeta_g)/\boldsymbol{Q}}(\alpha')$. Hence $l^{d'}$ must divide h_χ. The proposition is thus completely proved. □

The above proof may be a natural generalization of the proof of [**3**, Lemma 2] combined with [**3**, Remark 2]. The following simple proof of Proposition 1 is due to the referee.

Another Proof of Proposition 1. We first assume that $k = \boldsymbol{Q}(\zeta_g)$. Let $\mathscr{O} = \boldsymbol{Z}[\zeta_g]$. Then we have the following commutative diagram of $\mathscr{O}$-modules for some integral ideal $\mathscr{I}$ of $\boldsymbol{Q}(\zeta_g)$ and some $\beta \in \mathscr{I}$:

$$\begin{array}{ccc} E_\chi^2 & \xrightarrow{\sim} & \mathscr{I} \\ \uparrow & & \uparrow \\ H_\chi^2 & \xrightarrow{\sim} & \beta\mathscr{O}, \end{array}$$

where the vertical maps are the natural inclusions. Since $E_\chi/H_\chi \simeq E_\chi^2/H_\chi^2 \simeq \mathscr{I}/\beta\mathscr{O} \simeq \mathscr{O}/\beta\mathscr{I}^{-1}$, $l \mid h_\chi$ is equivalent to that there exists a prime ideal $\mathscr{L}$ of $\mathscr{O}$ dividing l such that $\beta\mathscr{I}^{-1} \subseteq \mathscr{L}$, which is also equivalent to $l\mathscr{L}^{-1} \subseteq l\mathscr{I}\beta^{-1}$. Furthermore we note that $H_\chi^2 = (E_\chi^2)^{\beta\mathscr{I}^{-1}}$. Here, for each $\mathscr{O}$-submodule Ω of E_χ^2 and each integral ideal $\mathscr{J}$ of $\boldsymbol{Q}(\zeta_g)$, $\Omega^{\mathscr{J}}$ denotes the $\mathscr{O}$-submodule of E_χ^2 generated by all $\varepsilon^{\gamma_\sigma}$, $(\gamma, \varepsilon) \in \mathscr{J} \times \Omega$.

Assume that $l \mid h_\chi$, i.e., $\beta\mathscr{I}^{-1} \subseteq \mathscr{L}$ with some prime ideal $\mathscr{L}$ of $\mathscr{O}$ dividing l. It follows from the above diagram that there exist a positive $s \in \boldsymbol{Z}$, $\varepsilon_1, \ldots, \varepsilon_s \in E_\chi$, and $\gamma_1, \ldots, \gamma_s \in \beta\mathscr{I}^{-1}$ such that $\eta_\chi^2 = \varepsilon_1^{2(\gamma_1)_\sigma} \cdots \varepsilon_s^{2(\gamma_s)_\sigma}$. Hence

$$\eta_\chi^{2\alpha_\sigma} = \varepsilon_1^{2(\alpha\gamma_1)_\sigma} \cdots \varepsilon_s^{2(\alpha\gamma_s)_\sigma} \in E_\chi^{2l} \qquad \text{for } \alpha \in l\mathscr{L}^{-1}$$

because $\alpha\gamma_1, \dots, \alpha\gamma_s \in l\mathscr{L}^{-1}\beta\mathscr{I}^{-1} \subseteq l\mathscr{O}$ by $l\mathscr{L}^{-1} \subseteq l\mathscr{I}\beta^{-1}$. Therefore $\left|\eta_\chi^{\alpha_\sigma}\right| \in E_\chi^l$ holds for $\alpha \in l\mathscr{L}^{-1}$.

Conversely we assume that there exists a prime ideal $\mathscr{L}$ of $\mathscr{O}$ above l such that $\left|\eta_\chi^{\alpha_\sigma}\right| \in E_\chi^l$ for any $\alpha \in l\mathscr{L}^{-1}$. Since η_χ^2 generates H_χ^2 over $\mathscr{O}$, this implies $(H_\chi^2)^{l\mathscr{L}^{-1}} \subseteq E_\chi^{2l}$. Then it follows from the above diagram that $l\mathscr{L}^{-1}\beta\mathscr{O} \subseteq l\mathscr{I}$, which implies $\beta\mathscr{I}^{-1} \subseteq \mathscr{L}$. Hence we have $l \mid h_\chi$.

The proposition for general k is derived from that for the case $k = \boldsymbol{Q}(\zeta_g)$: Let $\mathfrak{o}$ be the integer ring of k, and let Λ be the set of prime ideals of $\mathfrak{o}$ above l. The implication

$$l \mid h_\chi \implies \exists \mathfrak{l} \in \Lambda, \forall \alpha \in l\mathfrak{l}^{-1}, \ \left|\eta_\chi^{\alpha_\sigma}\right| \in E_\chi^l$$

follows from the case $k = \boldsymbol{Q}(\zeta_g)$, because $\mathscr{L} \cap \mathfrak{o} \in \Lambda$ for any prime ideal $\mathscr{L}$ of $\mathscr{O}$ above l and $l(\mathscr{L} \cap \mathfrak{o})^{-1} = l\mathscr{L}^{-1} \cap \mathfrak{o}$ by the assumption on k. Another implication also follows; because $\mathfrak{l}\mathscr{O}$ is a prime ideal of $\mathscr{O}$ for any $\mathfrak{l} \in \Lambda$ by the assumption on k, and the statement that $\left|\eta_\chi^{\alpha_\sigma}\right| \in E_\chi^l$ for all $\alpha \in l\mathfrak{l}^{-1}$ implies that $\left|\eta_\chi^{\alpha_\sigma}\right| \in E_\chi^l$ for all α in $l(\mathfrak{l}\mathscr{O})^{-1} = (l\mathfrak{l}^{-1})\mathscr{O}$. $\square$

Given any algebraic number z, we denote by $\|z\|$ the maximum of the absolute values of all conjugates of z over $\boldsymbol{Q}$. It follows that, for any algebraic numbers z_1, z_2, and for any non-negative integer a,

$$\|z_1 z_2\| \leq \|z_1\| \cdot \|z_2\|, \quad \|z_1^a\| = \|z_1\|^a.$$

LEMMA 1. *Let u be a positive integer and ε an element of $E_\chi \setminus \{\pm 1\}$. If ε is a u-th power in E_χ, then*

$$2^u < \|\varepsilon\|$$

except in the case $f_\chi \in \{9\} \cup \boldsymbol{P}$.

PROOF. Assume not only that $\varepsilon = \varepsilon_0^u$ with some ε_0 in E_χ but also that $2^u \geq \|\varepsilon\|$. It suffices to prove that $f = f_\chi$ is either 9 or a prime number. Since the above assumption implies that

$$\varepsilon_0^2 \neq 1, \quad \|\varepsilon_0\| \leq 2,$$

(1) yields $K_\chi = \boldsymbol{Q}(\varepsilon_0)$ and, by the theorem of Kronecker [**4**, II], $\varepsilon_0 = \delta + \delta^{-1}$ holds for some root δ of unity. Therefore we obtain $\boldsymbol{Q}(\zeta_f) = \boldsymbol{Q}(\delta)$, so that $\zeta_f + \zeta_f^{-1}$ belongs to $E_\chi \setminus \{\pm 1\}$. Furthermore, $\zeta_{2^a} + \zeta_{2^a}^{-1}$ is not a unit for any non-negative integer a. Hence there exists an odd prime p dividing f. In the case $p^2 \mid f$,

$$\boldsymbol{Q}(\zeta_{f/p} + \zeta_{f/p}^{-1}) \subset \boldsymbol{Q}(\zeta_f + \zeta_f^{-1}) = K_\chi, \quad N_{K_\chi/\boldsymbol{Q}(\zeta_{f/p} + \zeta_{f/p}^{-1})}(\zeta_f + \zeta_f^{-1}) = \zeta_{f/p} + \zeta_{f/p}^{-1},$$

the relation $\zeta_{f/p} + \zeta_{f/p}^{-1} = \pm 1$ implies that $f/p = 3$ or 6, and consequently we have $f = 9$. Thus, in the rest of the proof, we may suppose that f is not divisible by the square of any odd prime. As $\boldsymbol{Q}(\zeta_f+\zeta_f^{-1})/\boldsymbol{Q}$ is a cyclic extension, f belongs to $\{p, 4p, pq\}$, with some odd prime q other than p. However, in view of $\zeta_{4p}+\zeta_{4p}^{-1}=\zeta_{4p}(1-\zeta_p^{(p-1)/2})$, we have $f\neq 4p$. Let us finally consider the case $f=pq$. We may suppose $p<q$. It follows that

$$\zeta_p\zeta_q+\zeta_p^{-1}\zeta_q^{-1}\in E_\chi, \quad N_{K_\chi/\boldsymbol{Q}(\zeta_q+\zeta_q^{-1})}\left(\zeta_p\zeta_q+\zeta_p^{-1}\zeta_q^{-1}\right)=\frac{\zeta_q^p+\zeta_q^{-p}}{\zeta_q+\zeta_q^{-1}}.$$

Therefore,

$$\zeta_q^{2p}+1=\pm\left(\zeta_q^{p+1}+\zeta_q^{p-1}\right);$$

but this is impossible, because $q\geq 5$ and, if $2p>q-1$, then $1\leq 2p-q\leq q-4$. □

Remark. Let ψ_0 be the Dirichlet character of order 3 with conductor 9 such that $\psi_0(2)=\zeta_3^2$. In the case $f_\chi=9$,

$$\chi=\psi_0 \ \text{ or } \ \psi_0^2, \quad K_\chi=\boldsymbol{Q}\left(\cos\frac{\pi}{9}\right),$$

E_χ is the unit group of $\boldsymbol{Q}(\cos(\pi/9))$, and a unit ε in E_χ satisfies $\|\varepsilon\|\leq 2$ if and only if ε or $-\varepsilon$ is conjugate to $\eta_{\psi_0}=-2\cos(4\pi/9)$ over $\boldsymbol{Q}$. Moreover, in the present case, the class number formula shows that h_χ coincides with the class number of $\boldsymbol{Q}(\cos(\pi/9))$, which is known to equal 1: $h_\chi=1$.

For each Dirichlet character ψ, we let $\lambda(\psi)$ denote the number of distinct prime divisors of g_ψ.

Lemma 2.

$$\max\left(\|\eta_\chi\|, \|\eta_\chi^{-1}\|\right)<\left(\frac{f_\chi}{\pi}+1\right)^{2^{\lambda(\chi)-2}\varphi(f_\chi)/g_\chi}.$$

Proof. Let p be a prime number dividing g, and r an integer such that $\zeta_{2f}^{\boldsymbol{\sigma}(\chi)^{-g/p}}=\zeta_{2f}^r$. Then

$$\left\|\left(\zeta_{2f}-\zeta_{2f}^{-1}\right)^{1-\boldsymbol{\sigma}(\chi)^{g/p}}\right\|=\left\|\left(\zeta_f-1\right)^{\boldsymbol{\sigma}(\chi)^{-g/p}-1}\right\|$$

and, for each integer j relatively prime to f,

$$\left|\left(\zeta_f^j-1\right)^{\boldsymbol{\sigma}(\chi)^{-g/p}-1}\right|=\left|\frac{\sin(\pi jr/f)}{\sin(\pi j/f)}\right|.$$

Therefore, when m ranges over the positive integers less than $f/2$ relatively prime to f,

$$\left\|\left(\zeta_{2f}-\zeta_{2f}^{-1}\right)^{1-\boldsymbol{\sigma}(\chi)^{g/p}}\right\| \leq \max_m \left|\frac{\sin(\pi mr/f)}{\sin(\pi m/f)}\right|$$
$$= \max_m \left|\frac{\sin(\pi m(r-1)/f)}{\tan(\pi m/f)} + \cos\frac{\pi m(r-1)}{f}\right| < \max_m \left(\frac{f}{\pi m}+1\right).$$

We thus obtain

$$\left\|\left(\zeta_{2f}-\zeta_{2f}^{-1}\right)^{1-\boldsymbol{\sigma}(\chi)^{g/p}}\right\| < \frac{f}{\pi}+1.$$

Similarly, we have

$$\left\|\left(\zeta_{2f}-\zeta_{2f}^{-1}\right)^{\boldsymbol{\sigma}(\chi)^{g/p}-1}\right\| < \frac{f}{\pi}+1.$$

The lemma now follows from the definition of η_χ. □

For each positive integer m, we let D_m denote the absolute value of the discriminant of $\boldsymbol{Q}(\zeta_m)$. We also let

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

according as $m \geq 3$ or $m \leq 2$.

Proposition 2. *Let l be a prime number not dividing g_χ, and n a positive divisor of g_χ such that $\boldsymbol{Q}(\zeta_n)$ contains the decomposition field of l for $\boldsymbol{Q}(\zeta_{g_\chi})/\boldsymbol{Q}$. Assume that l divides h_χ, hence $f_\chi \neq 9$, and that f_χ is not a prime number. Then*

$$l < \sqrt{D_n}\left(\frac{2^{\lambda(\chi)-2}\varphi(f_\chi)\varphi(n)^2\Xi(n)}{(\log 2)g_\chi\sqrt{D_n}}\log\left(\frac{f_\chi}{\pi}+1\right)\right)^{\varphi(n)}.$$

Proof. Let σ be a generator of $\mathrm{Gal}(K_\chi/\boldsymbol{Q})$. By Proposition 1, there exists a prime ideal $\mathfrak{l}$ of $\boldsymbol{Q}(\zeta_n)$ dividing l such that, for each γ in $l\mathfrak{l}^{-1}$, $|\eta_\chi^{\gamma_\sigma}|$ is an l-th power in E_χ. Let $\mathfrak{K}$ be the decomposition field of l for $\boldsymbol{Q}(\zeta_g)/\boldsymbol{Q}$. Since the norm of $l\mathfrak{l}^{-1}$ for $\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}$ is $l^{([\mathfrak{K}:\boldsymbol{Q}]-1)[\boldsymbol{Q}(\zeta_n):\mathfrak{K}]}$, Minkowski's lattice theorem shows that

$$\|\alpha\| \leq \left(\sqrt{D_n}\,l^{([\mathfrak{K}:\boldsymbol{Q}]-1)[\boldsymbol{Q}(\zeta_n):\mathfrak{K}]}\right)^{1/\varphi(n)}$$

with some element α of $l\mathfrak{l}^{-1}\setminus\{0\}$. It follows that

$$0 < \|\alpha\| \leq \left(\sqrt{D_n}\,l^{\varphi(n)-1}\right)^{1/\varphi(n)}; \tag{4}$$

in particular, $\alpha = \pm 1$ if $n \leq 2$. Let us write α in the form

$$\alpha = \sum_{j=1}^{\varphi(n)} a_j \zeta_n^{j-1} \qquad \text{with } a_1, \cdots, a_{\varphi(n)} \in \boldsymbol{Z}.$$

Then, in $\boldsymbol{Z}[\mathrm{Gal}(K_\chi/\boldsymbol{Q})]$,

$$\alpha_\sigma = \sum_{j=1}^{\varphi(n)} a_j (\sigma^{g/n})^{j-1},$$

so that

$$\left\|\eta_\chi^{\alpha_\sigma}\right\| \leq \max\left(\|\eta_\chi\|, \left\|\eta_\chi^{-1}\right\|\right)^{\sum_{j=1}^{\varphi(n)} |a_j|}.$$

Hence we obtain, from Lemma 2,

$$\log\left\|\eta_\chi^{\alpha_\sigma}\right\| \leq \frac{2^{\lambda(\chi)-2}\varphi(f)}{g} \log\left(\frac{f}{\pi}+1\right) \sum_{j=1}^{\varphi(n)} |a_j|. \tag{5}$$

We next define a square matrix X of degree $\varphi(n)$ by

$$X = \left(\zeta_n^{r_u(j-1)}\right)_{u,j=1,\cdots,\varphi(n)}.$$

Here r_u denotes, for each positive integer $u \leq \varphi(n)$, the u-th positive integer relatively prime to n. Note that, by definition,

$$D_n = |\det(X)|^2. \tag{6}$$

Now, take any positive integer $j \leq \varphi(n)$. For each positive integer $u \leq \varphi(n)$, let d_u denote the (j,u)-cofactor of X. Then

$$a_j = \frac{1}{\det(X)} \sum_{u=1}^{\varphi(n)} d_u \alpha^{(u)},$$

with $\alpha^{(u)}$ for each u the image of α under the automorphism of $\boldsymbol{Q}(\zeta_n)$ mapping ζ_n to $\zeta_n^{r_u}$. Hence (4), (6), and Hadamard's inequality yield

$$|a_j| \leq \frac{\varphi(n)\Xi(n)}{\sqrt{D_n}}\left(\sqrt{D_n}\, l^{\varphi(n)-1}\right)^{1/\varphi(n)}.$$

We therefore see from (5) that

$$\log\left\|\eta_\chi^{\alpha_\sigma}\right\| \leq \frac{2^{\lambda(\chi)-2}\varphi(f)\varphi(n)^2\Xi(n)}{g\sqrt{D_n}}\left(\sqrt{D_n}\, l^{\varphi(n)-1}\right)^{1/\varphi(n)} \log\left(\frac{f}{\pi}+1\right). \tag{7}$$

On the other hand, the l-th power $|\eta_\chi^{\alpha_\sigma}|$ in E_χ is not equal to 1; because η_χ^2 generates over $\boldsymbol{Z}[\zeta_g]$ the cyclic free $\boldsymbol{Z}[\zeta_g]$-module H_χ^2. Hence, by Lemma 1, we have

$$l \log 2 < \log \left\| \eta_\chi^{\alpha_\sigma} \right\|.$$

This and (7) then give us the inequality to be proved. $\square$

3.

We devote this section to giving some elementary lemmas, which will be needed in the next section.

LEMMA 3. *Let p be a prime number, m a positive integer not divisible by p, U a finite set of integers, and $\mathfrak{w}$ a map $U \to \boldsymbol{Z}[\zeta_m]$. Taking an integer $a > 1$, a positive integer $a' < a$, and any integer b, put*

$$\omega = \sum_{u \in U} \mathfrak{w}(u) \zeta_{p^a}^u, \quad \omega' = \sum_{u \in U'} \mathfrak{w}(u) \zeta_{p^a}^u,$$

where U' denotes the set of all $u \in U$ with $u \equiv b \pmod{p^{a'}}$.

(i) *If $\omega = 0$, then $\omega' = 0$.*
(ii) *If c is an integer and if $\omega \equiv 0 \pmod{c}$, namely $\omega \in c\boldsymbol{Z}[\zeta_{mp^a}]$, then $\omega' \equiv 0 \pmod{c}$.*

PROOF. The assertion (i) follows from the fact that the p^a-th cyclotomic polynomial in an indeterminate y belongs to $\boldsymbol{Z}[y^{p^{a-1}}]$ and is irreducible over $\boldsymbol{Q}(\zeta_m)$. The assertion (ii) is an immediate consequence of (i). $\square$

As in the introduction, we let

$$\tilde{q} = \gcd(2, q) q \qquad \text{for each } q \in \boldsymbol{P}.$$

LEMMA 4. *Let p be a prime number, m a positive integer not divisible by p, a a positive integer which exceeds 2 in the case $p = 2$, V a complete set of representatives of the factor ring $\boldsymbol{Z}/\tilde{p}\boldsymbol{Z}$, and r an integer such that $\tilde{p}$ is the p-part of $r - 1$. Then $\zeta_{p^a}^{jr^u}$, for all $j \in V \setminus p\boldsymbol{Z}$ and all non-negative integers $u < \varphi(p^a/\tilde{p})$, are linearly independent over $\boldsymbol{Q}(\zeta_m)$.*

PROOF. When the integer $p^a/\tilde{p}$ is 1 or 2, the lemma certainly holds. Let us consider the case where $p^a/\tilde{p} > 2$, i.e, $\tilde{p}^2 \mid p^a$. Let $s = p^a/\tilde{p}^2$, let w be any non-negative integer less than s, and let $t = (r^s - 1)\tilde{p}/p^a$ so that t is an integer relatively prime to p. We assume that

$$\sum_{u=0}^{\varphi(p^a/\tilde{p})-1} \sum_{j \in V \setminus p\boldsymbol{Z}} b_j(u) \zeta_{p^a}^{jr^u} = 0$$

with each $b_j(u)$ in $\boldsymbol{Q}(\zeta_m)$. Clearly, for each u, $r^u \equiv r^w \pmod{p^a/\tilde{p}}$ if and only if $u \equiv w \pmod{s}$. Therefore, by Lemma 3, we have

$$\sum_{c=0}^{\varphi(\tilde{p})-1} b_j(w+cs)\left(\zeta_{p^a}^{jr^w}\right)^{r^{cs}} = 0$$

for each j. Because every c satisfies $r^{cs} \equiv 1 + ctp^a/\tilde{p} \pmod{p^a}$ in the above equation, it follows that

$$\zeta_{p^a}^{jr^w} \sum_{c=0}^{\varphi(\tilde{p})-1} b_j(w+cs)\left(\zeta_{\tilde{p}}^{jr^w t}\right)^c = 0,$$

which yields $b_j(w+cs) = 0$ for each c. □

Lemma 5. *Let α be a nonzero algebraic integer, k a number field with finite degree, $\mathfrak{o}$ the ring of algebraic integers in k, β an algebraic integer in $\mathfrak{o}[\alpha]$, and d the degree of α over k; $d = [k(\alpha) : k]$. Let $\mathfrak{b}$ be an ideal of $\mathfrak{o}$ relatively prime to the principal ideal of $\mathfrak{o}$ generated by the product of $N_{k(\alpha)/k}(\alpha)$ and the discriminant of α over k. Viewing $\mathfrak{o}[\alpha]$ as an $\mathfrak{o}$-module in the usual manner, assume that*

$$\beta\alpha^j \in \mathfrak{b} \oplus \mathfrak{o}\alpha \oplus \cdots \oplus \mathfrak{o}\alpha^{d-1}$$

for every non-negative integer $j < d$. Then

$$\beta \in (\mathfrak{o}[\alpha])\mathfrak{b} = \mathfrak{b} \oplus \mathfrak{b}\alpha \oplus \cdots \oplus \mathfrak{b}\alpha^{d-1}.$$

Proof. Let Z be the square matrix of degree d with coefficients in $\mathfrak{o}$ such that

$$Z \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{d-1} \end{pmatrix} = \beta \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{d-1} \end{pmatrix}.$$

Taking the conjugates $\alpha_1, \ldots, \alpha_d$ of α over k, with $\alpha_1 = \alpha$, let T be the adjugate matrix of the matrix $(\alpha_m^{j-1})_{j,m=1,\ldots,d}$. Then T is invertible and TZT^{-1} is a diagonal matrix whose $(1,1)$-component is β. Hence the $(1,1)$-component of TZ is equal to $\beta\gamma$, where γ denotes the $(1,1)$-component of T. On the other hand, by the assumption of the lemma, the components of the first column of Z belong to $\mathfrak{b}$ and, by the definition of $(1,1)$-cofactor, γ is a divisor of

$$N_{k(\alpha)/k}(\alpha)\det\left((\alpha_m^{j-1})_{j,m=1,\ldots,d}\right)$$

in the ring $\mathfrak{o}[\alpha_1, \ldots, \alpha_d]$. Thus the lemma is proved. □

For each integer $m > 1$, we let $Q(m)$ denote the set of prime-powers $u > 1$ dividing m and satisfying $\gcd(u, m/u) = 1$. Furthermore, we denote by $\mathscr{B}_m$ the set of roots of unity in the form

$$\prod_{u \in Q(m)} \zeta_u^{j_u}$$

where j_u for each u in $Q(m)$ ranges over the non-negative integers smaller than $\varphi(u)$. It is obvious that $\mathscr{B}_m$ contains 1 and forms a free basis of the $\boldsymbol{Z}$-module $\boldsymbol{Z}[\zeta_m]$.

LEMMA 6. *Let n be an integer greater than 1. For any algebraic integer α in $\boldsymbol{Z}[\zeta_n]$, let $c(\alpha)$ denote the coefficient of 1 in the expression of α as a linear combination of elements of $\mathscr{B}_n$ with coefficients in $\boldsymbol{Z}$. Let b be an integer relatively prime to n, and β an algebraic integer in $\boldsymbol{Z}[\zeta_n]$. If $c(\beta\zeta_n^j) \equiv 0 \pmod b$ for all non-negative integers $j < \varphi(n)$, then $\beta \equiv 0 \pmod b$.*

PROOF. Assume that $c(\beta\zeta_n^j) \equiv 0 \pmod b$ for all non-negative integers $j < \varphi(n)$. Then we find that $c(\beta\zeta_n^j) \equiv 0 \pmod b$ for all integers j. Let P' be any subset of $Q(n)$, let u be any element of $Q(n) \setminus P'$, and let

$$n' = \prod_{u' \in P'} u', \quad n'' = n'u.$$

Note that $\mathscr{B}_n \cap \langle\zeta_{n/n'}\rangle$ is a free basis of the $\boldsymbol{Z}[\zeta_{n'}]$-module $\boldsymbol{Z}[\zeta_n]$ and that $\mathscr{B}_n \cap \langle\zeta_{n/n''}\rangle$ is a free basis of the $\boldsymbol{Z}[\zeta_{n''}]$-module $\boldsymbol{Z}[\zeta_n]$. For any α in $\boldsymbol{Z}[\zeta_n]$, we let $c'(\alpha)$ denote the coefficient of 1 in the expression of α as a linear combination of elements of $\mathscr{B}_n \cap \langle\zeta_{n/n'}\rangle$ with coefficients in $\boldsymbol{Z}[\zeta_{n'}]$; similarly, we let $c''(\alpha)$ denote the coefficient of 1 in the expression of α as a linear combination of elements of $\mathscr{B}_n \cap \langle\zeta_{n/n''}\rangle$ with coefficients in $\boldsymbol{Z}[\zeta_{n''}]$. Obviously, for every γ in $\boldsymbol{Z}[\zeta_n]$,

$$c'(c''(\gamma)) = c'(\gamma), \quad c''(\gamma\zeta_u) = c''(\gamma)\zeta_u.$$

Now we take any n/n''-th root ξ of unity: $\xi \in \langle\zeta_{n/n''}\rangle$. Since b is relatively prime to u, it follows from Lemma 5 that, if $c'(\beta\xi\zeta_u^j) \equiv 0 \pmod b$ for all non-negative integers $j < \varphi(u)$, then $c''(\beta\xi) \equiv 0 \pmod b$. Hence we can complete the proof by induction on $|Q(n)|$. □

4.

This section is a sequel to §2. With χ, f, and g the same as in §2, we shall prove other preliminary results for the proof of Theorem 1.

Let p be any prime number. We let $f(p)$ and $g(p)$ denote respectively the p-part of f_χ and that of g_χ. In the case $p \geq 5$, let W_p denote the set of roots of unity in the form

$$\prod_{u \in Q((p-1)/2)} \zeta_{2u}^{s_u}$$

where, for each u in $Q((p-1)/2)$, s_u ranges over the non-negative integers smaller than u. Let $W_p = \{1\}$ in the case $p \leq 3$. Then W_p, a subset of $\boldsymbol{Q}(\zeta_{\varphi(\tilde{p})}) = \boldsymbol{Q}(\zeta_{p-1})$, is a complete set of representatives of the quotient group $\langle \zeta_{\varphi(\tilde{p})} \rangle / \langle -1 \rangle$. Next, let a be any positive integer. Let $\varPhi_p(a)$ denote the set of all maps from W_p into the set of the non-negative integers not more than a. We then put

$$M_p(a) = \max_{\mathfrak{m} \in \varPhi_p(a)} \left| N_{\boldsymbol{Q}(\zeta_{p-1})/\boldsymbol{Q}} \left(\sum_{\delta \in W_p} \mathfrak{m}(\delta)\delta - 1 \right) \right|.$$

Proposition 3. *Let p be a prime number as above, l a prime number distinct from p, and n a positive divisor of g_χ such that $\boldsymbol{Q}(\zeta_n)$ contains the decomposition field of l for $\boldsymbol{Q}(\zeta_{g_\chi})/\boldsymbol{Q}$. Assume that*

$$\tilde{p} \mid n, \quad f(p) = \tilde{p} g(p), \quad l \nmid f_\chi g_\chi, \quad l \mid h_\chi.$$

Then

$$M_p \left(\frac{2(p-1)\varphi(f_\chi) n l}{p g_\chi} \right) \geq \frac{f(p)}{\nu_p},$$

where ν_p denotes the p-part of n.

Proof. As the proof is not short, we divide it into seven steps.

i) For each positive integer j, we denote by $P(j)$ the set of prime divisors of j and, when j is a divisor of f, we let

$$G_j = \mathrm{Gal}(\boldsymbol{Q}(\zeta_f)/\boldsymbol{Q}(\zeta_j)).$$

It follows that $G_1 = \mathrm{Gal}(\boldsymbol{Q}(\zeta_f)/\boldsymbol{Q})$ is the direct product of $G_{f/f(q)}$ for all primes q in $P(f)$:

$$G_1 = \prod_{q \in P(f)} G_{f/f(q)} = G_{f/f(p)} \times G_{f(p)}.$$

Given any prime v in $P(g)$, we can fix a prime v_* in $P(f)$ satisfying

$$\chi^*(G_{f/f(v_*)}) \ni \zeta_{g(v)}$$

since g is the least common multiple of the orders of $\chi^*|G_{f/f(q)}$ for all q in $P(f)$. We may therefore suppose that

$$\boldsymbol{s}_\chi = \prod_{v \in P(g)} \boldsymbol{s}(v),$$

where each $\boldsymbol{s}(v)$ is an element of $G_{f/f(v_*)}$ such that $\chi^*(\boldsymbol{s}(v))$ is a primitive $g(v)$-th root of unity. Hence, for each v in $P(g)$,

$$\zeta_{f/f(v_*)}^{\boldsymbol{s}(v)} = \zeta_{f/f(v_*)}, \quad \boldsymbol{s}_\chi^{g/g(v)}\boldsymbol{s}(v)^{-g/g(v)} \in \mathrm{Ker}(\chi^*) = \mathrm{Gal}(\boldsymbol{Q}(\zeta_f)/K_\chi),$$

and we may also suppose that

$$\boldsymbol{s}(v)^{g(v)} = 1 \qquad \text{if } v_* = v.$$

In particular, the assumption $f(p) = \tilde{p}g(p)$ enables us to let

$$p_* = p, \quad \boldsymbol{s}(p)^{g(p)} = 1.$$

ii) Now, put

$$\sigma = \boldsymbol{s}_\chi|K_\chi = \boldsymbol{\sigma}(\chi)|K_\chi.$$

By the assumptions on n, l and by Proposition 1, there exists a prime ideal $\mathfrak{l}$ of $\boldsymbol{Q}(\zeta_n)$ dividing l such that $|\eta_\chi^{\gamma_\sigma}|$ is an l-th power in E_χ for every element γ of $l\mathfrak{l}^{-1}$. We denote by $\mathfrak{Z}$ the set of elements of G_1 in the form

$$\prod_{v\in P(g/g(p))} \boldsymbol{s}(v)^{j_v g/\nu_v}$$

where, for each v in $P(g/g(p)) = P(g) \setminus \{p\}$, ν_v denotes the v-part of n and j_v ranges over the non-negative integers less than $\varphi(\nu_v)$. It should be added that

$$\chi^*\left(\boldsymbol{s}(v)^{j_v g/\nu_v}\right) = \zeta_{\nu_v}^{j_v}.$$

Let α be an algebraic integer in $l\mathfrak{l}^{-1} \setminus l\boldsymbol{Z}[\zeta_n]$. Writing α as

$$\alpha = \sum_{j=1}^{\varphi(\nu_p)} \sum_{\boldsymbol{z}\in\mathfrak{Z}} a_{\boldsymbol{z},j}\chi^*(\boldsymbol{z})\zeta_{\nu_p}^{j-1} \qquad \text{with each } a_{\boldsymbol{z},j} \text{ in } \boldsymbol{Z},$$

we then have, in $\boldsymbol{Z}[\mathrm{Gal}(K_\chi/\boldsymbol{Q})]$,

$$\alpha_\sigma = \sum_{j=1}^{\varphi(\nu_p)} \sum_{\boldsymbol{z}\in\mathfrak{Z}} a_{\boldsymbol{z},j}(\boldsymbol{z}|K_\chi)\sigma^{(j-1)g/\nu_p}. \tag{8}$$

Next let $\mathfrak{p}$ be a prime ideal of $\boldsymbol{Q}(\zeta_{p-1})$ dividing p. Let $f(\mathfrak{p})$ denote the highest power of $\mathfrak{p}$ dividing $f(p)$, and I the set of positive integers less than $f(p)$ and congruent to suitable elements of W_p modulo $f(\mathfrak{p})$. For each u in I, let $[u]$ denote the automorphism in $G_{f/f(p)}$

mapping $\zeta_{f(p)}$ to $\zeta_{f(p)}^u$. As the degree of $\mathfrak{p}$ for $\boldsymbol{Q}(\zeta_{p-1})/\boldsymbol{Q}$ equals 1, $\{[u] \mid u \in I\}$ is a complete set of representatives of the quotient group

$$G_{f/f(p)}/\mathrm{Gal}\big(\boldsymbol{Q}(\zeta_f)/\boldsymbol{Q}\big(\zeta_{f/f(p)}, \zeta_{\tilde{p}} + \zeta_{\tilde{p}}^{-1}\big)\big).$$

We put, in $\boldsymbol{Z}[G_1]$,

$$\varUpsilon = \sum_{\boldsymbol{x} \in \mathrm{Ker}(\chi^*)} \boldsymbol{x}, \quad \varDelta' = \prod_{v \in P(g/g(p))} (1 - \boldsymbol{s}(v)^{g/v}).$$

Note that $\varUpsilon \boldsymbol{s}(v)^{g/g(v)} = \varUpsilon \boldsymbol{s}_\chi^{g/g(v)}$ for each v in $P(g)$. Let $\boldsymbol{i}$ be the complex conjugation in G_1, namely, the automorphism of $\boldsymbol{Q}(\zeta_f)$ mapping ζ_f to ζ_f^{-1}. Let P_1 be the set of primes v in $P(g)$ with $v_* \neq p$, i.e, $\boldsymbol{s}(v) \in G_{f(p)}$, and let G' be the subgroup of $G_{f(p)}$ generated by $\boldsymbol{s}(v)^{g(v)/\nu_v}$ for all v in P_1 and by the image of $\mathrm{Ker}(\chi^*)$ under the canonical surjection $G_1 \to G_{f(p)}$. Let $\mathscr{T}$ denote the direct product, as a set, of G', I, and the set of positive integers not exceeding $\varphi(\nu_p)$:

$$\mathscr{T} = \{(\boldsymbol{x}, u, j) \mid \boldsymbol{x} \in G',\ u \in I,\ j \in \boldsymbol{Z},\ 1 \leq j \leq \varphi(\nu_p)\}.$$

In view of

$$\boldsymbol{i} \in \mathrm{Ker}(\chi^*) \setminus \{\boldsymbol{x}[u]\boldsymbol{s}(p)^m \mid \boldsymbol{x} \in G', u \in I, m \in \boldsymbol{Z}, 1 \leq m \leq g(p)\},$$

we can define integers $b_{\boldsymbol{x},u,j}$, for all $(\boldsymbol{x}, u, j)$ in $\mathscr{T}$, by

$$\varUpsilon(1 - \boldsymbol{s}(p)^{g/p})\varDelta' \sum_{j=1}^{\varphi(\nu_p)} \sum_{\boldsymbol{z} \in \mathfrak{Z}} a_{\boldsymbol{z},j} \boldsymbol{z} \boldsymbol{e}^{j-1} = (1 + \boldsymbol{i})(1 - \boldsymbol{s}(p)^{g/p}) \sum_{(\boldsymbol{x},u,j) \in \mathscr{T}} b_{\boldsymbol{x},u,j} \boldsymbol{x}[u] \boldsymbol{e}^{j-1}, \tag{9}$$

where we put $\boldsymbol{e} = \boldsymbol{s}(p)^{g/\nu_p}$. Further let a' be an integer such that

$$\zeta_f^{\boldsymbol{s}(p)^{g/p}} = \zeta_f^{2a'+1}, \quad \text{i.e.,} \quad \zeta_f^{a'} (\zeta_f - 1)^{1 - \boldsymbol{s}(p)^{g/p}} \in \boldsymbol{R}.$$

Since

$$\big(\zeta_{2f} - \zeta_{2f}^{-1}\big)^{1 - \boldsymbol{\sigma}(\chi)^{g/p}} = \zeta_{2f}^{\boldsymbol{\sigma}(\chi)^{g/p} - 1} (\zeta_f - 1)^{1 - \boldsymbol{s}_\chi^{g/p}}, \quad \zeta_{2f}^{\boldsymbol{\sigma}(\chi)^{g/p} - 1} \in \langle \zeta_f \rangle,$$

we then obtain, by the definition of η_χ,

$$\eta_\chi^2 = (\zeta_f - 1)^{(1 - \boldsymbol{s}_\chi^{g/p})\varUpsilon\varDelta'} = \Big(\zeta_f^{a'} (\zeta_f - 1)^{1 - \boldsymbol{s}(p)^{g/p}}\Big)^{\varUpsilon\varDelta'}.$$

Therefore, it follows from (8) and (9) that

$$\eta_\chi^{2\alpha_\sigma} = \prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\zeta_f^{a'}(\zeta_f - 1)^{1-\boldsymbol{s}(p)^{g/p}}\right)^{2b_{\boldsymbol{x},u,j}\boldsymbol{x}[u]\boldsymbol{e}^{j-1}}.$$

On the other hand, since $\left|\eta_\chi^{\alpha_\sigma}\right|$ is an l-th power in E_χ and l does not divide f, Lemma 5 of [**3**] shows that the image of $\left|\eta_\chi^{\alpha_\sigma}\right|$ under the Frobenius automorphism of l for $\boldsymbol{Q}(\zeta_f)/\boldsymbol{Q}$ is congruent to $\left|\eta_\chi^{\alpha_\sigma}\right|^l$ modulo l^2. Hence, in the case $l > 2$,

$$\begin{aligned}\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} &\left(\zeta_f^{la'}\left(\zeta_f^l - 1\right)^{1-\boldsymbol{s}(p)^{g/p}}\right)^{b_{\boldsymbol{x},u,j}\boldsymbol{x}[u]\boldsymbol{e}^{j-1}} \\ &\equiv \prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\zeta_f^{a'}(\zeta_f - 1)^{1-\boldsymbol{s}(p)^{g/p}}\right)^{lb_{\boldsymbol{x},u,j}\boldsymbol{x}[u]\boldsymbol{e}^{j-1}} \pmod{l^2} \end{aligned} \tag{10}$$

while, in the case $l = 2$,

$$\begin{aligned}\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} &\left(\zeta_f^{2a'}\left(\zeta_f^2 - 1\right)^{1-\boldsymbol{s}(p)^{g/p}}\right)^{b_{\boldsymbol{x},u,j}\boldsymbol{x}[u]\boldsymbol{e}^{j-1}} \\ &\equiv \kappa \prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\zeta_f^{a'}(\zeta_f - 1)^{1-\boldsymbol{s}(p)^{g/p}}\right)^{2b_{\boldsymbol{x},u,j}\boldsymbol{x}[u]\boldsymbol{e}^{j-1}} \pmod{4} \end{aligned} \tag{11}$$

with $\kappa = \pm 1$.

iii) We now assume that

$$M_p\left(\frac{2(p-1)\varphi(f)nl}{pg}\right) < \frac{f(p)}{\nu_p} \tag{12}$$

contrary to the conclusion of the propostion. Define a polynomial $J(y)$ in an indeterminate y over $\boldsymbol{Z}$ by

$$J(y) = \sum_{c=1}^{l-1} \frac{(-1)^{c-1}}{l}\binom{l}{c} y^c \quad \text{or} \quad J(y) = -y + 1$$

according as $l > 2$ or $l = 2$:

$$(y-1)^l = y^l - 1 + lJ(y).$$

Take an integer r satisfying

$$\zeta_{f(p)}^{\;r} = \zeta_{f(p)}^{\boldsymbol{s}(p)^{g/g(p)}},$$

so that the p-part of $r-1$ is $\tilde{p}$. In the rest of this proof, we let

$$\zeta = \zeta_{f/f(p)}, \quad d = r^{g(p)/\nu_p}, \quad t = r^{g(p)/p} = d^{\nu_p/p},$$

and let, for each positive integer j,

$$\xi_j = \zeta_{f(p)}^{\boldsymbol{e}^{j-1}} = \zeta_{f(p)}^{d^{j-1}}.$$

iv) For the present, let us consider the case where $l > 2$ or $(l, \kappa) = (2, 1)$. We easily see from (10) or (11) that

$$\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\frac{\zeta^{l\boldsymbol{x}}\xi_j^{lu} - 1}{\zeta^{l\boldsymbol{x}}\xi_j^{ltu} - 1}\right)^{b_{\boldsymbol{x},u,j}} \equiv \prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\frac{\zeta^{\boldsymbol{x}}\xi_j^{u} - 1}{\zeta^{\boldsymbol{x}}\xi_j^{tu} - 1}\right)^{lb_{\boldsymbol{x},u,j}} \pmod{l^2}.$$

Furthermore, in the above,

$$\left(\zeta^{\boldsymbol{x}}\xi_j^{u'} - 1\right)^{lb_{\boldsymbol{x},u,j}} \equiv \left(\zeta^{l\boldsymbol{x}}\xi_j^{lu'} - 1\right)^{b_{\boldsymbol{x},u,j}-1}\left(\zeta^{l\boldsymbol{x}}\xi_j^{lu'} - 1 + lb_{\boldsymbol{x},u,j}J\left(\zeta^{\boldsymbol{x}}\xi_j^{u'}\right)\right) \pmod{l^2}$$

with $u' = u$ or tu. Therefore,

$$\begin{aligned}
&\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\left(\zeta^{l\boldsymbol{x}}\xi_j^{lu} - 1\right)\left(\zeta^{l\boldsymbol{x}}\xi_j^{ltu} - 1 + lb_{\boldsymbol{x},u,j}J\left(\zeta^{\boldsymbol{x}}\xi_j^{tu}\right)\right)\right) \\
&\quad\equiv \prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\left(\zeta^{l\boldsymbol{x}}\xi_j^{lu} - 1 + lb_{\boldsymbol{x},u,j}J\left(\zeta^{\boldsymbol{x}}\xi_j^{u}\right)\right)\left(\zeta^{l\boldsymbol{x}}\xi_j^{ltu} - 1\right)\right) \pmod{l^2},
\end{aligned}$$

that is,

$$\begin{aligned}
&\left(\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\zeta^{l\boldsymbol{x}}\xi_j^{lu} - 1\right)\right) \sum_{(\boldsymbol{y},w,m)\in\mathscr{T}} b_{\boldsymbol{y},w,m}J\left(\zeta^{\boldsymbol{y}}\xi_m^{tw}\right)\mathit{\Pi}_{\boldsymbol{y},w,m} \\
&\quad\equiv \left(\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\zeta^{l\boldsymbol{x}}\xi_j^{ltu} - 1\right)\right) \sum_{(\boldsymbol{y},w,m)\in\mathscr{T}} b_{\boldsymbol{y},w,m}J\left(\zeta^{\boldsymbol{y}}\xi_m^{w}\right)\mathit{\Pi}'_{\boldsymbol{y},w,m} \pmod{l} \qquad (13)
\end{aligned}$$

where, for each $(\boldsymbol{y}, w, m)$ in $\mathscr{T}$,

$$\begin{aligned}
\mathit{\Pi}_{\boldsymbol{y},w,m} &= \left(\zeta^{l\boldsymbol{y}}\xi_m^{ltw} - 1\right)^{-1} \prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\zeta^{l\boldsymbol{x}}\xi_j^{ltu} - 1\right), \\
\mathit{\Pi}'_{\boldsymbol{y},w,m} &= \left(\zeta^{l\boldsymbol{y}}\xi_m^{lw} - 1\right)^{-1} \prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\zeta^{l\boldsymbol{x}}\xi_j^{lu} - 1\right).
\end{aligned}$$

Let $\mathit{\Psi}$ be the set of maps from $\mathscr{T}$ to $\{0, 1\}$. For each $\mathfrak{n}$ in $\mathit{\Psi}$, we put

$$A(\mathfrak{n}) = \sum_{(\boldsymbol{x},u,j)\in\mathscr{T}} l\mathfrak{n}(\boldsymbol{x},u,j)ud^{j-1}, \quad B(\mathfrak{n}) = \sum_{(\boldsymbol{x},u,j)\in\mathscr{T}} \mathfrak{n}(\boldsymbol{x},u,j),$$

$$\Sigma(\mathfrak{n}) = \sum_{(\boldsymbol{x},u,j)\in\mathscr{T}} l\mathfrak{n}(\boldsymbol{x},u,j)\boldsymbol{x}$$

and, for each $(\boldsymbol{y},w,m)$ in $\mathscr{T}$, we put

$$\Psi_{\boldsymbol{y},w,m} = \{\mathfrak{v}\in\Psi \mid \mathfrak{v}(\boldsymbol{y},w,m)=0\}.$$

It follows that

$$\begin{aligned}&\Bigg(\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \big(\zeta^{l\boldsymbol{x}}\xi_j^{lu}-1\big)\Bigg) \sum_{(\boldsymbol{y},w,m)\in\mathscr{T}} b_{\boldsymbol{y},w,m} J\big(\zeta^{\boldsymbol{y}}\xi_m^{tw}\big)\Pi_{\boldsymbol{y},w,m} \\ &\quad = -\sum_{(\boldsymbol{y},w,m)\in\mathscr{T}}\ \sum_{\mathfrak{n}\in\Psi}\ \sum_{\mathfrak{v}\in\Psi_{\boldsymbol{y},w,m}} (-1)^{B(\mathfrak{n})+B(\mathfrak{v})} b_{\boldsymbol{y},w,m} J\big(\zeta^{\boldsymbol{y}}\xi_m^{tw}\big)\zeta^{\Sigma(\mathfrak{n})+\Sigma(\mathfrak{v})}\zeta_{f(p)}^{A(\mathfrak{n})+tA(\mathfrak{v})}, \quad (14)\end{aligned}$$

$$\begin{aligned}&\Bigg(\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \big(\zeta^{l\boldsymbol{x}}\xi_j^{ltu}-1\big)\Bigg) \sum_{(\boldsymbol{y},w,m)\in\mathscr{T}} b_{\boldsymbol{y},w,m} J\big(\zeta^{\boldsymbol{y}}\xi_m^{w}\big)\Pi'_{\boldsymbol{y},w,m} \\ &\quad = -\sum_{(\boldsymbol{y},w,m)\in\mathscr{T}}\ \sum_{\mathfrak{n}\in\Psi}\ \sum_{\mathfrak{v}\in\Psi_{\boldsymbol{y},w,m}} (-1)^{B(\mathfrak{n})+B(\mathfrak{v})} b_{\boldsymbol{y},w,m} J\big(\zeta^{\boldsymbol{y}}\xi_m^{w}\big)\zeta^{\Sigma(\mathfrak{n})+\Sigma(\mathfrak{v})}\zeta_{f(p)}^{tA(\mathfrak{n})+A(\mathfrak{v})}. \quad (15)\end{aligned}$$

v) We shall next see when a triplet $(\boldsymbol{y},w,m)$ in $\mathscr{T}$, a pair $(\mathfrak{n},\mathfrak{v})$ in $\Psi\times\Psi_{\boldsymbol{y},w,m}$, and an integer c, with $\min(1,l-2)\le c<l$, satisfy the two congruences

$$ctwd^{m-1}+A(\mathfrak{n})+tA(\mathfrak{v}) \equiv \sum_{(\boldsymbol{x},u,j)\in\mathscr{T}} l(1+t)ud^{j-1}-1 \pmod{f(p)/\nu_p}, \quad (16)$$

$$cwd^{m-1}+tA(\mathfrak{n})+A(\mathfrak{v}) \equiv \sum_{(\boldsymbol{x},u,j)\in\mathscr{T}} l(1+t)ud^{j-1}-1 \pmod{f(p)/\nu_p}. \quad (17)$$

Since $t\equiv d\equiv 1 \pmod{f(p)/\nu_p}$, either congruence above means that

$$\begin{aligned}&\sum_{u\in I\setminus\{w\}} \Bigg(\sum_{\boldsymbol{x}\in G'}\sum_{j=1}^{\varphi(\nu_p)} l(2-\mathfrak{n}(\boldsymbol{x},u,j)-\mathfrak{v}(\boldsymbol{x},u,j))\Bigg)u-1 \\ &\quad + \Bigg(\sum_{\boldsymbol{x}\in G'}\sum_{j=1}^{\varphi(\nu_p)} l(2-\mathfrak{n}(\boldsymbol{x},w,j)-\mathfrak{v}(\boldsymbol{x},w,j))-c\Bigg)w \equiv 0 \pmod{f(p)/\nu_p}. \quad (18)\end{aligned}$$

However, by the definition of G',

$$\varphi(\nu_p)|G'| \le \frac{(p-1)\nu_p}{p}[\boldsymbol{Q}(\zeta_f):K_\chi]\prod_{q\in P_1}\nu_q \le \frac{(p-1)\varphi(f)n}{pg}.$$

Hence there exists a map $\mathfrak{h}$ in $\Phi_p(2(p-1)\varphi(f)nl/(pg))$ such that

$$\mathfrak{h}(\delta) = \sum_{\boldsymbol{x}\in G'} \sum_{j=1}^{\varphi(\nu_p)} l(2 - \mathfrak{n}(\boldsymbol{x}, u, j) - \mathfrak{v}(\boldsymbol{x}, u, j))$$

if $\delta \in W_p$, $u \in I \setminus \{w\}$, and $\delta \equiv u \pmod{f(\mathfrak{p})}$, and such that

$$\mathfrak{h}(\delta) = \sum_{\boldsymbol{x}\in G'} \sum_{j=1}^{\varphi(\nu_p)} l(2 - \mathfrak{n}(\boldsymbol{x}, w, j) - \mathfrak{v}(\boldsymbol{x}, w, j)) - c$$

if $\delta \in W_p$ and $\delta \equiv w \pmod{f(\mathfrak{p})}$. We can therefore transform (18) into

$$\sum_{\delta\in W_p} \mathfrak{h}(\delta)\delta - 1 \equiv 0 \pmod{f(\mathfrak{p})\nu(\mathfrak{p})^{-1}},$$

where $\nu(\mathfrak{p})$ denotes the highest power of $\mathfrak{p}$ dividing ν_p. Thus (18) induces

$$N_{\boldsymbol{Q}(\zeta_{p-1})/\boldsymbol{Q}}\Bigl(\sum_{\delta\in W_p} \mathfrak{h}(\delta)\delta - 1\Bigr) \equiv 0 \pmod{f(p)/\nu_p}.$$

As this and (12) yield

$$\sum_{\delta\in W_p} \mathfrak{h}(\delta)\delta - 1 = 0,$$

Lemma 7 of [**3**] then implies that $\mathfrak{h}(1) = 1$ and that $\mathfrak{h}(\delta) = 0$ for all δ in $W_p \setminus \{1\}$. Consequently, both of (16), (17) are equivalent to the condition that

$$\begin{aligned}
&w = 1, \quad (\boldsymbol{y}, 1, m) \in \mathscr{T}, \quad \mathfrak{v} \in \Psi_{\boldsymbol{y},1,m}, \quad c = l - 1;\\
&\mathfrak{n}(\boldsymbol{x}, u, j) = 1 \qquad \text{for every } (\boldsymbol{x}, u, j) \text{ in } \mathscr{T};\\
&\mathfrak{v}(\boldsymbol{x}, u, j) = 1 \qquad \text{for every } (\boldsymbol{x}, u, j) \text{ in } \mathscr{T} \setminus \{(\boldsymbol{y}, 1, m)\}.
\end{aligned}$$

It follows, under the above condition, that

$$\begin{gathered}
(l-1)td^{m-1} + A(\mathfrak{n}) + tA(\mathfrak{v}) = \sum_{(\boldsymbol{x},u,j)\in\mathscr{T}} l(1+t)ud^{j-1} - td^{m-1},\\
(l-1)d^{m-1} + tA(\mathfrak{n}) + A(\mathfrak{v}) = \sum_{(\boldsymbol{x},u,j)\in\mathscr{T}} l(1+t)ud^{j-1} - d^{m-1},\\
B(\mathfrak{n}) + B(\mathfrak{v}) = (p-1)\varphi(\nu_p)|G'| - 1,\\
(l-1)\boldsymbol{y} + \Sigma(\mathfrak{n}) + \Sigma(\mathfrak{v}) = l(p-1)\varphi(\nu_p) \sum_{\boldsymbol{x}\in G'} \boldsymbol{x} - \boldsymbol{y}.
\end{gathered}$$

Hence, by (13), (14) and (15), Lemma 3 shows that

$$\sum_{m=1}^{\varphi(\nu_p)}\sum_{\boldsymbol{y}\in G'} b_{\boldsymbol{y},1,m}\zeta^{-\boldsymbol{y}}\xi_m^{-t} \equiv \sum_{m=1}^{\varphi(\nu_p)}\sum_{\boldsymbol{y}\in G'} b_{\boldsymbol{y},1,m}\zeta^{-\boldsymbol{y}}\xi_m^{-1} \pmod{l}.$$

Furthermore, $(t-1)p/f(p)$ is an integer relatively prime to p, and

$$\zeta_{f(p)}^{t} = \zeta_p^{(t-1)p/f(p)}\zeta_{f(p)}, \quad \zeta_p^r = \zeta_p.$$

We therefore obtain

$$\left(\zeta_p^{(1-t)p/f(p)} - 1\right)\sum_{m=1}^{\varphi(\nu_p)}\sum_{\boldsymbol{y}\in G'} b_{\boldsymbol{y},1,m}\zeta^{-\boldsymbol{y}}\xi_m^{-1} \equiv 0 \pmod{l},$$

which gives

$$\sum_{m=1}^{\varphi(\nu_p)}\sum_{\boldsymbol{y}\in G'} b_{\boldsymbol{y},1,m}\zeta^{\boldsymbol{y}}\xi_m \equiv 0 \pmod{l}.$$

However, by Lemma 4, $\xi_1, \ldots, \xi_{\varphi(\nu_p)}$ are linearly independent over $\boldsymbol{Q}(\zeta)$. Hence

$$\sum_{\boldsymbol{y}\in G'} b_{\boldsymbol{y},1,m}\zeta^{\boldsymbol{y}} \equiv 0 \pmod{l} \tag{19}$$

if m is any positive integer $\leq \varphi(\nu_p)$.

vi) Since $\{\boldsymbol{x}[u] \mid \boldsymbol{x} \in G', u \in I\} \cup \{\boldsymbol{i}\boldsymbol{x}[u] \mid \boldsymbol{x} \in G', u \in I\}$ is a subgroup of G_1 containing $\mathrm{Ker}(\chi^*) \cup \{\boldsymbol{s}(v) \mid v \in P(g/g(p))\}$, we can deduce from (9) that

$$\varUpsilon\varDelta' \sum_{\boldsymbol{z}\in\mathfrak{Z}} a_{\boldsymbol{z},j}\boldsymbol{z} = (1+\boldsymbol{i})\sum_{u\in I}\sum_{\boldsymbol{x}\in G'} b_{\boldsymbol{x},u,j}\boldsymbol{x}[u] \tag{20}$$

for every positive integer $j \leq \varphi(\nu_p)$. Let us put

$$P_2 = \{v \in P_1 \mid v_* = v,\ f(v) \neq 4\}.$$

For any prime v in P_2, we have $f(v) = \tilde{v}g(v)$ and $\zeta^{\boldsymbol{s}(v)^{g/v}-1}$ is a primitive v-th root of unity. Let G'' be the subgroup of G' generated by $\boldsymbol{s}(v)^{g/\nu_v}$ for all v in $P_1 \setminus P_2$ and by the image of $\mathrm{Ker}(\chi^*)$ under the canonical surjection $G_1 \to G_{f(p)}$. Let

$$\mathfrak{B} = \left\{\boldsymbol{z}_1\boldsymbol{z}_2 \,\middle|\, \boldsymbol{z}_1 \in G'',\ \boldsymbol{z}_2 \in \mathfrak{Z} \cap \prod_{v\in P_2} G_{f/f(v)}\right\}.$$

Then there exist integers $b_{\boldsymbol{w},u}$, for all $(\boldsymbol{w}, u)$ in $\mathfrak{B} \times I$, such that

$$\Upsilon\Big(\prod_{v}(1-\boldsymbol{s}(v)^{g/v})\Big)\sum_{\boldsymbol{z}\in\mathfrak{Z}} a_{\boldsymbol{z},1}\boldsymbol{z} = (1+\boldsymbol{i})\sum_{u\in I}\sum_{\boldsymbol{w}\in\mathfrak{B}} b_{\boldsymbol{w},u}\boldsymbol{w}[u], \tag{21}$$

with v running through $P(g/g(p)) \setminus P_2$. Hence, by (20),

$$(1+\boldsymbol{i})\sum_{u\in I}\sum_{\boldsymbol{x}\in G'} b_{\boldsymbol{x},u,1}\boldsymbol{x}[u] = \Big(\prod_{v\in P_2}(1-\boldsymbol{s}(v)^{g/v})\Big)(1+\boldsymbol{i})\sum_{u\in I}\sum_{\boldsymbol{w}\in\mathfrak{B}} b_{\boldsymbol{w},u}\boldsymbol{w}[u]$$

and consequently

$$\sum_{\boldsymbol{x}\in G'} b_{\boldsymbol{x},1,1}\boldsymbol{x} = \sum_{\boldsymbol{w}\in\mathfrak{B}} b_{\boldsymbol{w},1}\Big(\prod_{v\in P_2}(1-\boldsymbol{s}(v)^{g/v})\Big)\boldsymbol{w}.$$

It follows that

$$\sum_{\boldsymbol{x}\in G'} b_{\boldsymbol{x},1,1}\zeta^{\boldsymbol{x}} = \sum_{\boldsymbol{w}\in\mathfrak{B}} b_{\boldsymbol{w},1}\Big(\prod_{v\in P_2}\big(1-\zeta^{(\boldsymbol{s}(v)^{g/v}-1)\boldsymbol{w}}\big)\Big)\zeta^{\boldsymbol{w}},$$

since we have

$$\zeta^{\prod_v \boldsymbol{s}(v)^{g/v}-1} = \prod_{v}\zeta^{\boldsymbol{s}(v)^{g/v}-1}$$

whenever v runs through any subset of P_2. Therefore, in virtue of (19),

$$\sum_{\boldsymbol{w}\in\mathfrak{B}} b_{\boldsymbol{w},1}\Big(\prod_{v\in P_2}\big(1-\zeta^{(\boldsymbol{s}(v)^{g/v}-1)\boldsymbol{w}}\big)\Big)\zeta^{\boldsymbol{w}} \equiv 0 \pmod{l}.$$

Next, let $\mathfrak{B}_0$ be the set of elements $\boldsymbol{w}$ of $\mathfrak{B}$ such that $\zeta_v^{\boldsymbol{w}} = \zeta_v$ for all v in P_2. Evidently, for any v in P_2 and any $\boldsymbol{w}$ in $\mathfrak{B}$, $\zeta_v^{\boldsymbol{w}} = \zeta_v$ if and only if $\zeta_{f(v)}^{\boldsymbol{w}-1} \in \langle\zeta_{f(v)}^{\,v}\rangle$. Hence Lemma 3, together with the above congruence, yields

$$\Big(\prod_{v\in P_2}\big(1-\zeta^{\boldsymbol{s}(v)^{g/v}-1}\big)\Big)\sum_{\boldsymbol{w}\in\mathfrak{B}_0} b_{\boldsymbol{w},1}\zeta^{\boldsymbol{w}} \equiv 0 \pmod{l}.$$

It then follows that

$$\sum_{\boldsymbol{w}\in\mathfrak{B}_0} b_{\boldsymbol{w},1}\zeta^{\boldsymbol{w}} \equiv 0 \pmod{l}.$$

Furthermore, Lemma 4 implies that $\zeta^{\boldsymbol{w}}$ for all $\boldsymbol{w}$ in $\mathfrak{B}$ are linearly independent over $\boldsymbol{Q}$.

Thus

$$b_{\boldsymbol{w},1} \equiv 0 \pmod{l} \qquad \text{for all } \boldsymbol{w} \in \mathfrak{B}_0.$$

Since $a_{1,1} = b_{1,1}$ by (21), we particularly obtain

$$a_{1,1} \equiv 0 \pmod{l}.$$

On the other hand, we know that, in what we have discussed so far, α can be replaced by $\alpha\zeta_n^j$ for any non-negative integer $j < \varphi(n)$. Lemma 6 therefore shows that

$$\alpha \equiv 0 \pmod{l}.$$

This conclusion, however, contradicts the choice of α.

vii) We finally consider the case $(l,\kappa) = (2,-1)$, in which we still use the notations introduced in the step iv) for the case $(l,\kappa) = (2,1)$. It follows from (11) that

$$\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\frac{\zeta^{2\boldsymbol{x}}\xi_j^{2u}-1}{\zeta^{2\boldsymbol{x}}\xi_j^{2tu}-1}\right)^{b_{\boldsymbol{x},u,j}} \equiv -\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \left(\frac{\zeta^{\boldsymbol{x}}\xi_j^{u}-1}{\zeta^{\boldsymbol{x}}\xi_j^{tu}-1}\right)^{2b_{\boldsymbol{x},u,j}} \pmod{4},$$

so that

$$\begin{aligned}
&\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \big((\zeta^{2\boldsymbol{x}}\xi_j^{2u}-1)\big(\zeta^{2\boldsymbol{x}}\xi_j^{2tu}-1+2b_{\boldsymbol{x},u,j}J\big(\zeta^{\boldsymbol{x}}\xi_j^{tu}\big)\big)\big) \\
&\quad\equiv -\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \big(\big(\zeta^{2\boldsymbol{x}}\xi_j^{2u}-1+2b_{\boldsymbol{x},u,j}J\big(\zeta^{\boldsymbol{x}}\xi_j^{u}\big)\big)\big(\zeta^{2\boldsymbol{x}}\xi_j^{2tu}-1\big)\big) \pmod{4}.
\end{aligned}$$

Therefore, instead of (13), we have

$$\begin{aligned}
&\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \big((\zeta^{2\boldsymbol{x}}\xi_j^{2u}-1)(\zeta^{2\boldsymbol{x}}\xi_j^{2tu}-1)\big) \\
&\qquad + \Bigg(\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} (\zeta^{2\boldsymbol{x}}\xi_j^{2u}-1)\Bigg) \sum_{(\boldsymbol{y},w,m)\in\mathscr{T}} b_{\boldsymbol{y},w,m}J\big(\zeta^{\boldsymbol{y}}\xi_m^{tw}\big)\Pi_{\boldsymbol{y},w,m} \\
&\quad\equiv \Bigg(\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} (\zeta^{2\boldsymbol{x}}\xi_j^{2tu}-1)\Bigg) \sum_{(\boldsymbol{y},w,m)\in\mathscr{T}} b_{\boldsymbol{y},w,m}J\big(\zeta^{\boldsymbol{y}}\xi_m^{w}\big)\Pi'_{\boldsymbol{y},w,m} \pmod{2}.
\end{aligned}$$

Nevertheless,

$$\prod_{(\boldsymbol{x},u,j)\in\mathscr{T}} \big((\zeta^{2\boldsymbol{x}}\xi_j^{2u}-1)(\zeta^{2\boldsymbol{x}}\xi_j^{2tu}-1)\big) = \sum_{(\mathfrak{n},\mathfrak{n}')\in\Psi\times\Psi} (-1)^{B(\mathfrak{n})+B(\mathfrak{n}')}\zeta^{\Sigma(\mathfrak{n})+\Sigma(\mathfrak{n}')}\zeta_{f(p)}^{A(\mathfrak{n})+tA(\mathfrak{n}')}$$

and, for each $(\mathfrak{n}, \mathfrak{n}')$ in $\Psi \times \Psi$, the congruence

$$A(\mathfrak{n}) + tA(\mathfrak{n}') \equiv \sum_{(\boldsymbol{x},j,u)\in\mathscr{T}} 2(1+t)ud^{j-1} - 1 \pmod{f(p)/\nu_p}$$

can be rewritten in the form

$$\sum_{u\in I\setminus\{1\}} \Bigg(\sum_{\boldsymbol{x}\in G'} \sum_{j=1}^{\varphi(\nu_p)} 2(2-\mathfrak{n}(\boldsymbol{x},u,j) - \mathfrak{n}'(\boldsymbol{x},u,j)) \Bigg) u$$
$$+ \sum_{\boldsymbol{x}\in G'} \sum_{j=1}^{\varphi(\nu_p)} 2(2-\mathfrak{n}(\boldsymbol{x},1,j) - \mathfrak{n}'(\boldsymbol{x},1,j)) - 1 \equiv 0 \pmod{f(p)/\nu_p}.$$

Hence, checking the arguments in the steps iii), iv), v), vi), we see that the above congruence modulo 2, together with (12), leads us to the contradiction $\alpha \equiv 0 \pmod 2$ in the same way as the congruence (13) for the case $(l, \kappa) = (2, 1)$.

Consequently, the assumption (12) turns out to be false and the proposition is completely proved. $\square$

By means of Proposition 3, we now prove the following

Proposition 4. *Let l be a prime number, n a positive divisor 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 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

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

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

Proof. Put

$$\Theta_p = \frac{(p-1)\varphi(f)nl}{pg}$$

for any p in R, and take any $\mathfrak{m}$ in $\Phi_p(2\Theta_p)$. Then

$$\Bigg| N_{\boldsymbol{Q}(\zeta_{p-1})/\boldsymbol{Q}} \Bigg(\sum_{\delta\in W_p} \mathfrak{m}(\delta)\delta - 1 \Bigg) \Bigg| = \prod_{\tau} \Bigg| \sum_{\delta\in W_p} \mathfrak{m}(\delta)\delta^{\tau} - 1 \Bigg|,$$

with τ ranging over the automorphisms of the field $\boldsymbol{Q}(\zeta_{p-1})$, and

$$\left|\sum_{\delta\in W_p}\mathfrak{m}(\delta)\delta^{\tau}-1\right|\le|\mathfrak{m}(1)-1|+\sum_{\delta\in W_p\setminus\{1\}}\mathfrak{m}(\delta)<\varphi(\tilde{p})\Theta_p.$$

Therefore

$$M_p(2\Theta_p)<(\varphi(\tilde{p})\Theta_p)^{\varphi(p-1)}.$$

Hence we see from Proposition 3 that

$$\prod_{p\in R}(\varphi(\tilde{p})\Theta_p)^{\varphi(p-1)}>\prod_{p\in R}\frac{f(p)}{\nu_p},$$

namely that

$$\left(\frac{\varphi(f)nl}{g}\right)^{\sum_{p\in R}\varphi(p-1)}\prod_{p\in R}\frac{((p-1)\varphi(\tilde{p}))^{\varphi(p-1)}}{p^{\varphi(p-1)}}>\prod_{p\in R}\frac{f(p)}{\nu_p}.$$

□

5.

We shall prove Theorem 1 in the present section. The notation in the preceeding sections will be retained except that, for each Dirichlet character ψ and each $p\in\boldsymbol{P}$, we let $f_\psi(p)$ and $g_\psi(p)$ denote the p-parts of f_ψ and g_ψ, respectively.

As to F, there exists a unique abelian number field k_0 with finite degree such that $F=k_0\boldsymbol{Q}^S$ and that, for each $p\in S$, the p-part of the conductor of k_0 divides $\tilde{p}$. Let $\mathfrak{X}$ be a set of nonprincipal Dirichlet characters with the following two properties:

(i) K_ψ for each ψ in $\mathfrak{X}$ is a subfield of F,
(ii) for any nonprincipal Dirichlet character ψ' with $K_{\psi'}\subset F$, there is just one Dirichlet character ψ in $\mathfrak{X}$ satisfying $K_\psi=K_{\psi'}$.

Let f_0 denote the conductor of k_0. Then, for each $\psi\in\mathfrak{X}$ and each $l\in\boldsymbol{P}\setminus S$, we easily obtain

$$f_\psi(l)\mid f_0,\quad g_\psi(l)\mid[k_0:\boldsymbol{Q}]. \tag{22}$$

When p is any prime in S with $f_\psi(p)\ne\tilde{p}g_\psi(p)$, we also have

$$f_\psi(p)<\tilde{p}g_\psi(p),\quad g_\psi(p)\mid[k_0:\boldsymbol{Q}]. \tag{23}$$

Now, as in the introduction, let μ_p denote for each $p\in S$ the p-part of the positive integer m_0 in the hypothesis of Theorem 1. Assume first that F is real: $F\subset\boldsymbol{R}$. Taking any subset R of S, let $\mathfrak{X}^R$ denote the set of Dirichlet characters ψ in $\mathfrak{X}$ for which

$$\{p \in S \mid f_\psi(p) = \tilde{p} g_\psi(p),\ g_\psi(p) \geq \mu_p\} = R.$$

It then follows from (23) that, for each $\psi \in \mathfrak{X}^R$ and each $p \in S \setminus R$,

$$p f_\psi(p) \mid \tilde{p}\mu_p[k_0 : \boldsymbol{Q}], \quad g_\psi(p) \mid \mu_p[k_0 : \boldsymbol{Q}]. \tag{24}$$

Lemma 7. *The set $\mathfrak{X}^R$ is finite or infinite according as R is empty or non-empty.*

Proof. In the case $R \neq \varnothing$, let Γ denote the subfield of $\boldsymbol{Q}^S$ whose Galois group over $\boldsymbol{Q}$ is topologically isomorphic to $\prod_{p \in R} \boldsymbol{Z}_p$. Then an element ψ of $\mathfrak{X}$ with $K_\psi \subset \Gamma$ belongs to $\mathfrak{X}^R$ if g_ψ is divisible by $\prod_{p \in R} \mu_p$. This fact implies that $\mathfrak{X}^R$ is an infinite set.

In the case $R = \varnothing$, we see from (22) and (24) that

$$f_\psi \mid 2 f_0 m_0 [k_0 : \boldsymbol{Q}] \qquad \text{for every } \psi \in \mathfrak{X}^R,$$

so that $\mathfrak{X}^R$ is a finite set. □

Remark. $\mathfrak{X}$ is the disjoint union of $\mathfrak{X}^{R'}$ for all subsets R' of S.

Let R be the same as above. For each ψ in $\mathfrak{X}^R$, define a positive integer n_ψ by

$$n_\psi = g_\psi \prod_{p \in R} \frac{\mu_p}{g_\psi(p)}.$$

We let $\mathfrak{X}_0^R$ denote the set of ψ in $\mathfrak{X}^R$ satisfying

$$\begin{aligned} &\frac{g_\psi}{\varphi(f_\psi) n_\psi} \left(\prod_{p \in R} \frac{p^{\varphi(p-1)} f_\psi(p)}{((p-1)\varphi(\tilde{p}))^{\varphi(p-1)} \mu_p} \right)^{1/\sum_{p \in R} \varphi(p-1)} \\ &\quad < \sqrt{D_{n_\psi}} \left(\frac{2^{\lambda(\psi)-2} \varphi(f_\psi) \varphi(n_\psi)^2 \varXi(n_\psi)}{(\log 2) g_\psi \sqrt{D_{n_\psi}}} \log\left(\frac{f_\psi}{\pi} + 1 \right) \right)^{\varphi(n_\psi)}. \end{aligned}$$

Lemma 8. *$\mathfrak{X}_0^R$ is a finite set.*

Proof. By Lemma 7, we may assume R to be non-empty. Let ψ be any Dirichlet character in $\mathfrak{X}^R$. In view of (22), (24) and the definition of n_ψ, we know that

$$n_\psi \leq m_0 [k_0 : \boldsymbol{Q}], \quad f_\psi \leq 2 f_0 m_0 [k_0 : \boldsymbol{Q}] \prod_{p \in R} f_\psi(p).$$

Furthermore,

$$2^{\lambda(\psi)} \leq 2^{|S|} [k_0 : \boldsymbol{Q}], \quad \frac{\varphi(f_\psi)}{g_\psi} \leq \varphi\biggl(2 \prod_v v\biggr),$$

where v ranges over the prime numbers dividing f_0 or belonging to S. Therefore the definition of $\mathfrak{X}_0^R$ implies that, if ψ belongs to $\mathfrak{X}_0^R$, then

$$f_\psi < \rho(\log f_\psi)^{m_0^2[k_0:\boldsymbol{Q}]},$$

with a positive number ρ depending only on m_0, f_0 and $[k_0 : \boldsymbol{Q}]$. We thus see that f_ψ is bounded as ψ runs through $\mathfrak{X}_0^R$. $\square$

Now, let

$$\mathfrak{X}_0 = \mathfrak{X}^{\varnothing} \cup \left(\bigcup_{R'} \mathfrak{X}_0^{R'} \right),$$

R' ranging over the non-empty subsets of S. By Lemmas 7 and 8, $\mathfrak{X}_0$ is a finite set.

PROPOSITION 5. *Still assuming F to be real, let l be a prime number such that $\boldsymbol{Q}(\zeta_{m_0})$ contains the decomposition field of l for $\boldsymbol{Q}^S(\zeta_{m_0})/\boldsymbol{Q}$ and that*

$$l \notin S, \quad f_0[k_0 : \boldsymbol{Q}] \prod_{\psi \in \mathfrak{X}_0} h_\psi \not\equiv 0 \pmod{l}.$$

Then $C_F(l)$ is trivial.

PROOF. It suffices to prove that the class number of any subfield of F with finite degree is not divisible by the prime number l. Let k' be any subfield of F with finite degree, and $\mathfrak{X}'$ the set of all ψ in $\mathfrak{X}$ with $K_\psi \subseteq k'$. For each ψ in $\mathfrak{X}'$, we denote by $h_\psi(l)$ the l-part of h_ψ. As $l \nmid [k' : \boldsymbol{Q}]$ by the hypothesis of the proposition, it follows from [**5**, Satz 21] that

$$|C_{k'}(l)| = \prod_{\psi \in \mathfrak{X}'} h_\psi(l) \tag{25}$$

(see also the formula (10) in [**5**, §9.4]).

Suppose now that some Dirichlet character χ in $\mathfrak{X}'$ satisfies $h_\chi(l) > 1$, namely, $l \mid h_\chi$. Then there exists a unique subset R of S such that $\mathfrak{X}^R$ contains χ. We note that, for each $v \in \boldsymbol{P}$, the v-part of n_χ is μ_v or $g_\chi(v)$ according as v belongs to R or $\boldsymbol{P} \setminus R$. The hypothesis on l implies that χ is not an element of $\mathfrak{X}_0$, l does not divide $f_\chi g_\chi$, and $\boldsymbol{Q}(\zeta_{n_\chi})$ contains the decomposition field of l for $\boldsymbol{Q}(\zeta_{g_\chi})/\boldsymbol{Q}$. In particular, R is not empty, so that f_χ is not a prime number since each p in R divides g_χ. Hence, by Proposition 2,

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

and further, by Proposition 4,

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

However χ must not belong to $\mathfrak{X}_0^R$, a subset of $\mathfrak{X}_0$. This contradiction means that $h_\psi(l) = 1$ for all ψ in $\mathfrak{X}'$. Hence (25) shows that $|C_{k'}(l)| = 1$, namely, the class number of k' is not divisible by l. □

Now, let us prove Theorem 1. Proposition 5 clearly implies Theorem 1 for the case $F \subset \boldsymbol{R}$. Accordingly, we assume that F is imaginary. Replacing m_0 by its multiple if necessary, we may also assume that, for each $p \in S$, the p-part of the exponent of $\mathrm{Gal}(k_0/\boldsymbol{Q})$ is a divisor of m_0. As in the introduction, let $C_F^-(l)$ denote, for each $l \in \boldsymbol{P}$, the l-primary component of the kernel C_F^- of the norm map $C_F \to C_{F^+}$, where

$$F^+ = F \cap \boldsymbol{R} = \boldsymbol{Q}^S(k_0 \cap \boldsymbol{R}).$$

Then, by Theorem 1 of [**3**], there exist only finitely many $l \in \boldsymbol{P}$ such that $C_F^-(l)$ is nontrivial and such that $\boldsymbol{Q}(\zeta_{m_0})$ contains the decomposition field of l for $\boldsymbol{Q}^S(\zeta_{m_0})/\boldsymbol{Q}$. On the other hand, since the norm map $C_F \to C_{F^+}$ is surjective by class field theory, it follows for each $l \in \boldsymbol{P}$ that $C_F(l)$ is trivial if and only if both $C_F^-(l)$ and $C_{F^+}(l)$ are trivial. Proposition 5 therefore completes the proof of Theorem 1.

6.

In this last section, we briefly make some additional remarks on C_F and $C_{\boldsymbol{Q}^S}$ with relation to Theorem 1.

If F is imaginary, then by the remark in the introduction, C_F^- is infinite whence so is C_F (cf. [**6**]). Iwasawa theory further guarantees in this case that, for any $p \in S$, $C_F^-(p)$ can be infinite quite often, for instance, when any prime ideal of $k_0 \cap \boldsymbol{R}$ dividing p splits in k_0 or when $\gcd(4, \tilde{p})p$ divides the exponent of the kernel of the norm map $C_{k_0} \to C_{k_0 \cap \boldsymbol{R}}$.

Assume now that F is real. Certainly, for any finite abelian group $\mathfrak{A}$ with order relatively prime to all $p \in S$, there exists an example of F such that $\mathfrak{A}$ is isomorphic to some subgroup of C_F. For any $p \in S$, however, $C_F(p)$ must always be trivial if Greenberg's conjecture for $\boldsymbol{Z}_p$-extensions holds in general. Hence, in view of Theorem 1, we might expect the finiteness of C_F. It would also be an important problem to know whether $C_{\boldsymbol{Q}^S}$ is trivial or not. In fact, we have not found any prime number l for which $C_{\boldsymbol{Q}^S}(l)$ is nontrivial. Moreover, if $C_{\boldsymbol{Q}^S}$ turns out to be trivial or, at least, to be finite, then it seems very likely that C_L is finite for every totally real finite extension L of $\boldsymbol{Q}^S$. We note that, in the case $|S| = 1$, $C_{\boldsymbol{Q}^S}$ is trivial if and only if $\boldsymbol{Q}^S$ coincides with the Hilbert class field of $\boldsymbol{Q}^S$, i.e., the maximal unramified abelian extension over $\boldsymbol{Q}^S$. Anyhow, whenever an integer $u \geq 2$ is given, there exist examples of S with $|S| = u$ such that the Hilbert class field of $\boldsymbol{Q}^S$ contains an extension of degree p over $\boldsymbol{Q}^S$ for some $p \in S$ (cf. [**2**]).

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, A note on the $\boldsymbol{Z}_p \times \boldsymbol{Z}_q$-extension over $\boldsymbol{Q}$, Proc. Japan Acad. Ser. A Math., **77** (2001), 84–86.
[3] K. Horie, Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field, J. London Math. Soc., **66** (2002), 257–275.
[4] L. Kronecker, Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, J. Reine Angew. Math., **53** (1857), 173–175.
[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, New York, 1996.

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