Tohoku Math. J.
57 (2005), 375–394

THE IDEAL CLASS GROUP OF THE BASIC Z_p-EXTENSION OVER AN IMAGINARY QUADRATIC FIELD

KUNIAKI HORIE

(Received October 14, 2003, revised Novemer 15, 2004)

Abstract. We shall discuss the local triviality in the ideal class group of the basic $\boldsymbol{Z}_p$-extension over an imaginary quadratic field and prove, in particular, a result which implies that such triviality distributes with natural density 1.

Introduction. Let p be a prime number, which will be fixed throughout this paper. We shall suppose that all algebraic extensions over the rational field $\boldsymbol{Q}$ are contained in the complex field $\boldsymbol{C}$. Let $\boldsymbol{Z}_p$ denote the ring of p-adic integers, and $\boldsymbol{B}_\infty$ the $\boldsymbol{Z}_p$-extension over $\boldsymbol{Q}$, namely, the unique abelian extension over $\boldsymbol{Q}$ such that the Galois group $\mathrm{Gal}(\boldsymbol{B}_\infty/\boldsymbol{Q})$ is topologically isomorphic to the additive group of $\boldsymbol{Z}_p$. Let P be the set of all prime numbers. For any algebraic extension F over $\boldsymbol{Q}$, let C_F denote the ideal class group of F and, for each $l \in P$, let $C_F(l)$ denote the l-class group of F, i.e., the l-primary component of C_F. As is well-known, the p-class group of $\boldsymbol{B}_\infty$ is trivial: $C_{\boldsymbol{B}_\infty}(p) = 1$ (cf. Fröhlich [5], Iwasawa [8]). On the other hand, the theorem of Washington [11] implies that, for every $l \in P \setminus \{p\}$, the l-class group of $\boldsymbol{B}_\infty$ is finite: $|C_{\boldsymbol{B}_\infty}(l)| < \infty$.

Now, let

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

according as $p > 2$ or $p = 2$. Let ν be a fixed positive integer such that $q \mid p^\nu$, namely,

$$\nu \geq 2 \quad \text{if} \quad p = 2\,.$$

Put

$$M = \frac{(p^{\nu-1}\log(p/2) + (6\nu+4)\log p)\varphi((p-1)q)f^3(f-1)^{(f-1)/2}}{(2\log 2)p^{(\nu-1/(p-1))(f-1)/2}}\,,$$

where φ denotes the Euler function and

$$f = \varphi(p^\nu) = (p-1)p^{\nu-1}\,.$$

In this paper, developing our arguments of [7, §2], we shall prove the following result among others.

THEOREM 1. *Let H be the class number of the subfield of $\boldsymbol{B}_\infty$ with degree $p^{2\nu-1}/q$. Then $C_{\boldsymbol{B}_\infty}(l)$ is trivial for every $l \in P$ which satisfies*

$$l^{\varphi(q)} \not\equiv 1 \pmod{qp^\nu}\,, \quad l \nmid H\,, \quad l \geq M^f\,.$$

2000 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R11, 11R20, 11R23.

Next, take any imaginary quadratic field k, and denote by Δ the maximal divisor of the discriminant of k relatively prime to p. Let K be the basic $\boldsymbol{Z}_p$-extension over k:

$$K = k\boldsymbol{B}_\infty .$$

By means of Theorem 1 and results in Washington [10, §IV], we shall eventually prove the following result.

THEOREM 2. *Let H be the same as in Theorem* 1, *and let h^* denote the relative class number of the intermediate field of K/k with degree $p^{2\nu-2}$ over k. Then $C_K(l)$ is trivial for every $l \in P$ which satisfies*

$$l^{\varphi(q)} \not\equiv 1 \pmod{qp^\nu}, \quad l \nmid Hh^*, \quad l \geq \max\left(M^f,\ p\left(\frac{q\Delta(\nu\log p+1)}{2\pi}\right)^f\right).$$

In particular, Theorem 2 implies that there exist only a finite number of $l \in P$, with $l^{\varphi(q)} \not\equiv 1 \pmod{qp^\nu}$, for which $C_K(l)$ is nontrivial. Once such a result is obtained, we shall see as a consequence that the natural density in P of the set of all $l \in P$ with $C_K(l) = 1$ is equal to 1 (cf. Theorem 3).

REMARK. For infinitely many $l \in P$, $C_K(l)$ is nontrivial while, for all $l \in P \setminus \{p\}$, $C_K(l)$ is finite (cf. [10], [11]).

The author thanks the referee who made several valuable comments on the paper.

1. We shall devote this section to proving several preliminary lemmas for the proof of Theorem 1 in the next section. As usual, let $\boldsymbol{Z}$ be the ring of (rational) integers, and $\boldsymbol{N}$ the set of positive elements of $\boldsymbol{Z}$. We put, in $\boldsymbol{C}$,

$$\xi_u = e^{2\pi i/p^u} \quad \text{for each } u \in \boldsymbol{N}.$$

Let m be any non-negative integer. In the case $p > 2$, we put

$$\eta_{m,u} = \prod_b \frac{\xi_{m+1}^b - \xi_{m+1}^{-b}}{\xi_{m+1}^{bu} - \xi_{m+1}^{-bu}} = \prod_b \frac{\sin(2\pi b/p^{m+1})}{\sin(2\pi bu/p^{m+1})}$$

for each $u \in \boldsymbol{Z}$ with $p \nmid u$. Here b ranges over the positive integers $< p^{m+1}/2$ such that $b^{p-1} \equiv 1 \pmod{p^{m+1}}$. We then let

$$\eta_m = \eta_{m,1+p^m} = \prod_b \frac{\xi_{m+1}^b - \xi_{m+1}^{-b}}{\xi_1^b\xi_{m+1}^b - \xi_1^{-b}\xi_{m+1}^{-b}}.$$

In the case $p = 2$, we put

$$\eta_{m,u} = \frac{\xi_{m+3} - \xi_{m+3}^{-1}}{\xi_{m+3}^u - \xi_{m+3}^{-u}} = \frac{\sin(\pi/2^{m+2})}{\sin(\pi u/2^{m+2})}$$

for each odd integer u, and put

$$\eta_m = \eta_{m,1+2^{m+1}} = \tan\frac{\pi}{2^{m+2}}.$$

Next, let $\boldsymbol{B}_m$ denote the intermediate field of $\boldsymbol{B}_\infty/\boldsymbol{Q}$ with degree p^m, E_m the group of all units of $\boldsymbol{B}_m$, and h_m the class number of $\boldsymbol{B}_m$. As is easily seen, each $\eta_{m,u}$ defined above belongs to E_m. Let U_m denote the group of circular units in $\boldsymbol{B}_m$, namely, the subgroup of E_m generated by -1 and by $\eta_{m,u}$ for all $u \in \boldsymbol{Z}$ with $p \nmid u$. Then the index of U_m in E_m equals h_m (cf. Hasse [6, §9]):

$$h_m = (E_m : U_m)\,. \tag{1}$$

On the other hand, h_m is divisible by the class number of any subfield of $\boldsymbol{B}_m$, since p is fully ramified for the abelian extension $\boldsymbol{B}_m/\boldsymbol{Q}$. Now, let R_m denote the group ring of $\mathrm{Gal}(\boldsymbol{B}_m/\boldsymbol{Q})$ over $\boldsymbol{Z}$. Naturally, E_m becomes an R_m-module, and U_m an R_m-submodule of E_m. Let us take an algebraic integer α in $\boldsymbol{Q}(\xi_m)$: $\alpha \in \boldsymbol{Z}[\xi_m]$. Then α is uniquely expressed in the form

$$\alpha = \sum_{j=1}^{\varphi(p^m)} a_j \xi_m^{j-1}\,, \quad a_1, \ldots, a_{\varphi(p^m)} \in \boldsymbol{Z}\,.$$

For each such α and each $\rho \in \mathrm{Gal}(\boldsymbol{B}_m/\boldsymbol{Q})$, we define an element α_ρ of R_m by

$$\alpha_\rho = \sum_{j=1}^{\varphi(p^m)} a_j \rho^{j-1}\,.$$

Next, let n be any positive integer, which we shall fix henceforth. For later convenience, we put $\zeta = e^{2\pi i/qp^n}$, that is, we put

$$\zeta = \xi_{n+1} \quad \text{or} \quad \xi_{n+2}$$

according as $p > 2$ or $p = 2$. Take any generator σ of the cyclic group $\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q})$ and any $\tau \in \mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q})$ of order p:

$$\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q}) = \langle\sigma\rangle\,, \quad \mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{B}_{n-1}) = \langle\tau\rangle\,.$$

Since

$$(1-\tau)\left(\sum_{u=0}^{p-1} \sigma^{up^{n-1}}\right) = 0 \quad \text{in } R_n, \tag{2}$$

we have

$$\varepsilon^{(1-\tau)(\alpha+\beta)_\sigma} = \varepsilon^{(1-\tau)(\alpha_\sigma+\beta_\sigma)}\,, \quad \varepsilon^{(1-\tau)(\alpha\beta)_\sigma} = \varepsilon^{(1-\tau)\alpha_\sigma\beta_\sigma}$$

for all $\varepsilon \in E_n$ and all $(\alpha, \beta) \in \boldsymbol{Z}[\xi_n] \times \boldsymbol{Z}[\xi_n]$. The map $(\alpha, \varepsilon') \mapsto \varepsilon'^{\alpha_\sigma}$ of $\boldsymbol{Z}[\xi_n] \times E_n^{1-\tau}$ into $E_n^{1-\tau}$ thus makes $E_n^{1-\tau}$ a module over the Dedekind domain $\boldsymbol{Z}[\xi_n]$. Then $U_n^{1-\tau}$ becomes a $\boldsymbol{Z}[\xi_n]$-submodule of E_n. Furthermore, we obtain the following

LEMMA 1. *The $\boldsymbol{Z}[\xi_n]$-module $E_n^{1-\tau}$ is isomorpic to a nonzero ideal of $\boldsymbol{Z}[\xi_n]$, and $U_n^{1-\tau}$ is a free $\boldsymbol{Z}[\xi_n]$-module generated by $\eta_{n,s}^{1-\tau}$, where s is an integer such that an extension of σ in* $\mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$ *maps ζ to ζ^s.*

PROOF. Assume that

$$\varepsilon^{(1-\tau)\alpha_\sigma} = 1\,, \quad \text{with } \varepsilon \in E_n, \alpha \in \boldsymbol{Z}[\xi_n]\,.$$

Let N be the norm of α for $\boldsymbol{Q}(\xi_n)/\boldsymbol{Q}$. Then $N = \alpha\beta$ for some $\beta \in \boldsymbol{Z}[\xi_n]$, and hence

$$\varepsilon^{(1-\tau)N} = \varepsilon^{(1-\tau)N_\sigma} = (\varepsilon^{(1-\tau)\alpha_\sigma})^{\beta_\sigma} = 1\,.$$

Thus $\varepsilon^{1-\tau}$ is equal to 1 or -1.

We next assume that $\varepsilon^{1-\tau} = -1$, namely, that

$$\varepsilon \in E_n \setminus E_{n-1}\,, \quad \varepsilon^2 \in E_{n-1}\,.$$

As $[\boldsymbol{B}_{n-1}(\varepsilon) : \boldsymbol{B}_{n-1}] = 2$ follows, we have

$$p = 2, \quad \boldsymbol{Q}(\xi_{n+2}) = \boldsymbol{Q}(\xi_{n+1}, \varepsilon)\,, \quad \varepsilon^2 \in \boldsymbol{Q}(\xi_{n+1})\,,$$

so that $\xi_{n+2}\varepsilon^{-1}$ belongs to $\boldsymbol{Q}(\xi_{n+1})$ whose unit index equals 1. Therefore, $\xi_{n+2}\varepsilon^{-1} = \xi_{n+1}^{\,u}\varepsilon'$ for some $u \in \boldsymbol{Z}$ and some $\varepsilon' \in E_{n-1}$. In particular, $\xi_{n+2}\xi_{n+1}^{-u}$ must be real. This contradiction shows that $E_n^{1-\tau}$ is a torsion-free $\boldsymbol{Z}[\xi_n]$-module.

Since the map $\gamma \mapsto \gamma^{1-\tau}$, $\gamma \in E_n$, induces a group isomorphism $E_n/E_{n-1} \to E_n^{1-\tau}$, it follows from the above that $E_n^{1-\tau}$ is a free abelian group of rank $\varphi(p^n)$. On the other hand, the group U_n is generated by -1 and by $\eta_{n,s}^{\sigma^u}$ for all nonnegative integers $u \le p^n - 2$. We also note that the quotient group $E_n^{1-\tau}/U_n^{1-\tau}$ is finite in virtue of (1). Hence we see from (2) that $U_n^{1-\tau}$ is a free abelian group freely generated by $\eta_{n,s}^{(1-\tau)\sigma^u}$ for all non-negative integers $u < \varphi(p^n)$. It is now easy to complete the proof of the lemma. □

REMARK. Neither $E_n^{1-\tau}$ nor $U_n^{1-\tau}$ depends upon the choice of τ.

LEMMA 2. *Let l be a prime number different from p, σ a generator of* Gal$(\boldsymbol{B}_n/\boldsymbol{Q})$, *and F an extension in $\boldsymbol{Q}(\xi_n)$ of the decomposition field of l for $\boldsymbol{Q}(\xi_n)/\boldsymbol{Q}$. Then l divides the integer h_n/h_{n-1} if and only if there exists a prime ideal $\mathfrak{l}$ of F dividing l such that $\eta_n^{\alpha_\sigma}$ is an l-th power in E_n for any element α of the integral ideal $l\mathfrak{l}^{-1}$ of F.*

PROOF. Let τ be the restriction to $\boldsymbol{B}_n$ of the automorphism of $\boldsymbol{Q}(\zeta)$ mapping ζ to $\xi_1\zeta = e^{2\pi i/p}\zeta$. Obviously, τ is an element of Gal$(\boldsymbol{B}_n/\boldsymbol{Q})$ of order p. Take an integer s for which σ is the restriction to $\boldsymbol{B}_n$ of the automorphism of $\boldsymbol{Q}(\zeta)$ mapping ζ to ζ^s. It then follows that

$$\eta_n^{1-\sigma} = \eta_{n,s}^{1-\tau}\,. \tag{3}$$

The map $\varepsilon \mapsto \varepsilon^{1-\tau}$ of E_n into $E_n^{1-\tau}$, together with its restriction to U_n, gives rise to an exact sequence

$$1 \to U_nE_{n-1}/U_n \to E_n/U_n \to E_n^{1-\tau}/U_n^{1-\tau} \to 1$$

of finite groups, so that

$$(E_n : U_n) = (E_{n-1} : U_n \cap E_{n-1})(E_n^{1-\tau} : U_n^{1-\tau})\,.$$

Putting, in R_n,

$$T = \sum_{u=0}^{p-1} \sigma^{up^{n-1}} = 1 + \tau + \cdots + \tau^{p-1},$$

we also have

$$(U_n \cap E_{n-1})^p = (U_n \cap E_{n-1})^T \subseteq U_n^T \subseteq U_{n-1} \subseteq U_n \cap E_{n-1},$$

while h_n is known to be relatively prime to p (cf. [5], [8]). Hence, by (1),

$$(E_n^{1-\tau} : U_n^{1-\tau}) = \frac{h_n}{h_{n-1}}. \tag{4}$$

Let $\mathfrak{o}$ denote the ring of algebraic intgers in F. Write d for the degree of $\boldsymbol{Q}(\xi_n)$ over F: $d = [\boldsymbol{Q}(\xi_n) : F]$. Then $\boldsymbol{Z}[\xi_n]$ is a free module over its subring $\mathfrak{o}$, and $1, \xi_n, \ldots, \xi_n^{d-1}$ form a basis of the $\mathfrak{o}$-module $\boldsymbol{Z}[\xi_n]$. We consider the quotient $E_n^{1-\tau}/U_n^{1-\tau}$ of $\boldsymbol{Z}[\xi_n]$-modules to be an $\mathfrak{o}$-module in the obvious manner. Hence there exists a finite set $\mathcal{S}$ of integral ideals of F which yields an isomorphism

$$E_n^{1-\tau}/U_n^{1-\tau} \cong \bigoplus_{\mathfrak{a}\in\mathcal{S}} (\mathfrak{o}/\mathfrak{a})$$

of $\mathfrak{o}$-modules.

We now assume that l divides h_n/h_{n-1}. By (4) and the above isomorphism, there are a prime ideal $\mathfrak{l}$ of F dividing l and an injective $\mathfrak{o}$-module homomorphism $\mathfrak{o}/\mathfrak{l} \to E_n^{1-\tau}/U_n^{1-\tau}$. Hence there further exists a unit ε_0 in $E_n^{1-\tau} \setminus U_n^{1-\tau}$ such that $\varepsilon_0^{\beta_\sigma}$ belongs to $U_n^{1-\tau}$ for every $\beta \in \mathfrak{l}$. Lemma 1 thus implies that

$$\varepsilon_0^l = \eta_{n,s}^{(1-\tau)\omega_\sigma} \quad \text{with a unique } \omega \in \boldsymbol{Z}[\xi_n], \tag{5}$$

where, since $\boldsymbol{Z}[\xi_n] = \mathfrak{o} \oplus \mathfrak{o}\xi_n \oplus \cdots \oplus \mathfrak{o}\xi_n^{d-1}$, ω is uniquely expressed in the form

$$\omega = \sum_{j=1}^{d} \upsilon_j \xi_n^{j-1} \quad \text{with } \upsilon_1, \ldots, \upsilon_d \in \mathfrak{o}.$$

To see that ω is not an element of $\mathfrak{l}\boldsymbol{Z}[\xi_n]$, the ideal of $\boldsymbol{Z}[\xi_n]$ generated by $\mathfrak{l}$, suppose contrarily that ω is an element of $\mathfrak{l}\boldsymbol{Z}[\xi_n]$. Then all υ_j, $j \in \{1, \ldots, d\}$, belong to $\mathfrak{l}$. As $\mathfrak{l}$ is unramified for $F/\boldsymbol{Q}$, we can take an element β' of $l\mathfrak{l}^{-1}$ satisfying $1 - \beta' \in \mathfrak{l}$. Note that $\beta'\upsilon_j l^{-1}$ belongs to $\mathfrak{o}$ for every $j \in \{1, \ldots, d\}$. On the other hand, we have, by (5),

$$\varepsilon_0^{l\beta'_\sigma} = \eta_{n,s}^{(1-\tau)(\sum_{j=1}^{d} \beta'\upsilon_j \xi_n^{j-1})_\sigma}.$$

Consequently,

$$\varepsilon_0 = \varepsilon_0^{(1-\beta'+\beta')_\sigma} = \varepsilon_0^{(1-\beta')_\sigma} \eta_{n,s}^{(1-\tau)(\sum_{j=1}^{d} \beta'\upsilon_j l^{-1} \xi_n^{j-1})_\sigma} \in U_n^{1-\tau};$$

but this contradicts the choice of ε_0. Thus ω is not an element of $\mathfrak{l}\boldsymbol{Z}[\xi_n]$. Let $\mathfrak{G} = \mathrm{Gal}(\boldsymbol{Q}(\xi_n)/F)$. We then have

$$\omega^\rho \notin \mathfrak{l}\boldsymbol{Z}[\xi_n] \quad \text{for any } \rho \text{ in } \mathfrak{G}, \tag{6}$$

since $\mathfrak{l}\boldsymbol{Z}[\xi_n]$ is the only prime ideal of $\boldsymbol{Q}(\xi_n)$ dividing $\mathfrak{l}$. Next, define a square matrix Y of degree d with coefficients in $\mathfrak{o}$ by

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

Clearly,

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

so that

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

Hence it follows from (6) that

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

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

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

Furthermore, (5) gives $\eta_{n,s}^{(1-\tau)(\omega\xi_n^{j-1})_\sigma}=\varepsilon_0^{l(\xi_n^{j-1})_\sigma}$ as j ranges over the positive integers not greater than d, and hence, from the definition of Y, we obtain

$$\eta_{n,s}^{(1-\tau)(\det(Y))_\sigma}=\varepsilon_0^{l(\sum_{j=1}^{d}\chi_j\xi_n^{j-1})_\sigma},$$

with χ_j denoting the $(j,1)$-cofactor of Y. Since l divides $\alpha(1-\beta''\det(Y))$, it follows that $\eta_{n,s}^{(1-\tau)\alpha_\sigma}$ is an l-th power in $E_n^{1-\tau}$. Therefore, by (3),

$$\eta_n^{(1-\sigma)\alpha_\sigma}=\varepsilon_1^{l}\qquad \text{for some } \varepsilon_1\in E_n^{1-\tau}.$$

We can also take an element θ of R_n satisfying $\eta_n^{p^2}=\eta_n^{(1-\sigma)\theta}$; because

$$(\eta_n^{T})^{p}=1,\quad \text{i.e.,}\quad \eta_n^{p^2}=\eta_n^{p(p-T)}=\eta_n^{p\sum_{u=1}^{p-1}(1-\tau^u)}.$$

Hence we have $\eta_n^{p^2\alpha_\sigma}=\varepsilon_1^{\theta l}$ and, consequently, $\eta_n^{\alpha_\sigma}$ is an l-th power in $E_n^{1-\tau}$.

Taking any algebraic integer α' in $l\mathfrak{l}^{-1}$ for which $\alpha' l^{-1}\mathfrak{l}+l\mathfrak{o}=\mathfrak{o}$, we assume from now on that $\eta_n^{\alpha'_\sigma}$ is an l-th power in E_n. This assumption implies by (3) that

$$\eta_{n,s}^{(1-\tau)\alpha'_\sigma}=\varepsilon_2^{l}\quad \text{with some } \varepsilon_2\in E_n.$$

Therefore

$$\varepsilon_2^{l}\in E_n^{1-\tau},\quad (\varepsilon_2^{T})^{l}=1.$$

Since ε_2 can be replaced by $-\varepsilon_2$ in the case $l = 2$, we may obtain $\varepsilon_2^T = 1$, which yields

$$\varepsilon_2^p = \varepsilon_2^{p-T} \in E_n^{1-\tau} .$$

Hence ε_2 itself belongs to $E_n^{1-\tau}$. Lemma 1 therefore shows that

$$U_n^{(1-\tau)\alpha'_\sigma} \subseteq E_n^{(1-\tau)l} .$$

Again by Lemma 1,

$$(E_n^{1-\tau} : E_n^{(1-\tau)l}) = l^{\varphi(p^n)} , \quad (U_n^{1-\tau} : U_n^{(1-\tau)\alpha'_\sigma}) = |N'| ,$$

where N' denotes the norm of α' for $\boldsymbol{Q}(\xi_n)/\boldsymbol{Q}$. The choice of α' guarantees, however, that the highest power of l dividing N' is $l^{\varphi(p^n)-d'}$, with d' the degree of $\boldsymbol{Q}(\xi_n)$ over the decomposition field of l for $\boldsymbol{Q}(\xi_n)/\boldsymbol{Q}$. Hence, in virtue of (4), h_n/h_{n-1} must be divisible by $l^{d'}$. Thus our lemma is completely proved.

For each algebraic number α, we put

$$\|\alpha\| = \max_\rho |\alpha^\rho| ,$$

where ρ runs through all isomorphisms of $\boldsymbol{Q}(\alpha)$ into $\boldsymbol{C}$. As is easily verified,

$$\|\beta\beta'\| \leq \|\beta\|\|\beta'\| , \quad \|\beta^m\| = \|\beta\|^m$$

for every algebraic number β, every algebraic number β', and every $m \in \boldsymbol{N}$.

LEMMA 3. *Let u be a positive integer, let ε be a unit in $E_n \setminus \{-1, 1\}$ whose norm for $\boldsymbol{B}_n/\boldsymbol{B}_{n-1}$ equals 1 or -1, and assume that $n > 1$ in the case $p = 3$. If ε is a u-th power in E_n, then*

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

PROOF. Contrary to the assertion, suppose that $2^u \geq \|\varepsilon\|$, with $\varepsilon = \varepsilon_0^u$ for some $\varepsilon_0 \in E_n$. Then we have $\|\varepsilon_0\| \leq 2$. Since ε_0 is totally real, it follows from §II of Kronecker [9] that $\varepsilon_0 = \delta + \delta^{-1}$ for some root δ of unity. On the other hand, unless $\boldsymbol{Q}(\varepsilon_0)$ coincides with $\boldsymbol{B}_n$, we have $\varepsilon = \varepsilon_0^u \in \boldsymbol{B}_{n-1}$ and so ε^p, the norm of ε for $\boldsymbol{B}_n/\boldsymbol{B}_{n-1}$, equals 1 or -1; but, by the hypothesis $\varepsilon^2 \neq 1$, ε is not a root of unity. Thus

$$\boldsymbol{Q}(\delta + \delta^{-1}) = \boldsymbol{Q}(\varepsilon_0) = \boldsymbol{B}_n .$$

In particlar, $\boldsymbol{Q}(\delta)$ is a quadratic extension over $\boldsymbol{B}_n$ and the conductor of $\boldsymbol{Q}(\delta)$ equals that of $\boldsymbol{B}_n$. Here, by the equality $1 + \delta^2 = \varepsilon_0\delta$, it is impossible that $p = 2$, namely, that δ is a primitive 2^{n+2}-th root of unity. Hence p must be 3 and δ^2 is a primitive 3^{n+1}-th root of unity. We then deduce that the norm of $\delta + \delta^{-1}$ for $\boldsymbol{B}_n/\boldsymbol{B}_{n-1}$ equals $\delta^3 + \delta^{-3}$, which is not a root of unity by the assumption $n > 1$. However, the norm of $(\delta + \delta^{-1})^u = \varepsilon$ for $\boldsymbol{B}_n/\boldsymbol{B}_{n-1}$ was 1 or -1. We are therefore led to a contradiction and, hence, the lemma is proved.

LEMMA 4. *In the case $p > 2$,*

$$\max(\|\eta_n\|, \|\eta_n^{-1}\|) < \left(\frac{p^{n+1}}{\pi} \sin\frac{\pi}{p} + \cos\frac{\pi}{p}\right)^{(p-1)/2} ;$$

in the case $p = 2$,

$$\|\eta_n\| = \|\eta_n^{-1}\| = \cot \frac{\pi}{2^{n+2}} .$$

PROOF. We first assume that p is odd. As Lemma 4 of [7] states that

$$\|\eta_n\| < \left(\frac{p^{n+1}}{\pi} \sin \frac{\pi}{p} \right)^{(p-1)/2} ,$$

we shall prove that

$$\|\eta_n^{-1}\| < \left(\frac{p^{n+1}}{\pi} \sin \frac{\pi}{p} + \cos \frac{\pi}{p} \right)^{(p-1)/2} .$$

By the definition of η_n,

$$\|\eta_n^{-1}\| \le \left\| \frac{\sin(2\pi(p^n+1)/p^{n+1})}{\sin(2\pi/p^{n+1})} \right\|^{(p-1)/2} .$$

Let m range over the positive integers less than $p^{n+1}/2$ and relatively prime to p, and let

$$\gamma_m = \frac{\sin(m\pi(p^n+1)/p^{n+1})}{\sin(m\pi/p^{n+1})} = \frac{\sin(m\pi/p)}{\tan(m\pi/p^{n+1})} + \cos \frac{m\pi}{p} .$$

We then easily see that

$$\left\| \frac{\sin(2\pi(p^n+1)/p^{n+1})}{\sin(2\pi/p^{n+1})} \right\| = \max_m |\gamma_m| .$$

Therefore it suffices to show that

$$|\gamma_m| < \frac{p^{n+1}}{\pi} \sin \frac{\pi}{p} + \cos \frac{\pi}{p} . \tag{7}$$

If $m < p/2$, then

$$\gamma_m > 0 , \quad \tan \frac{m\pi}{p^{n+1}} > \frac{m\pi}{p^{n+1}} , \quad \cos \frac{m\pi}{p} \le \cos \frac{\pi}{p} , \quad \frac{p}{m\pi} \sin \frac{m\pi}{p} \le \frac{p}{\pi} \sin \frac{\pi}{p} ,$$

and hence

$$|\gamma_m| = \gamma_m < \frac{p^{n+1}}{m\pi} \sin \frac{m\pi}{p} + \cos \frac{m\pi}{p} \le \frac{p^{n+1}}{\pi} \sin \frac{\pi}{p} + \cos \frac{\pi}{p} .$$

If $p/2 < m < p^{n+1}/2$, we obtain

$$|\gamma_m| < \frac{p^{n+1}}{\pi} \sin \frac{\pi}{p}$$

by an argument quite similar to that in the proof of [7, Lemma 4]. Thus (7) is proved.

We next assume $p = 2$. In this case, $-\eta_n^{-1}$ is the image of η_n under the automorphism of $\boldsymbol{Q}(\xi_{n+2})$ mapping ξ_{n+2} to $-\xi_{n+2}$. Hence the second assertion of the lemma follows from the fact that

$$\|\eta_n^{-1}\| = \max_m \left| \frac{\cos(\pi m/2^{n+2})}{\sin(\pi m/2^{n+2})} \right| ,$$

where m ranges over the odd positive integers smaller than 2^{n+1}. □

LEMMA 5. *Let S be a finite set of integers, ψ a map from S to $\boldsymbol{Z}$, a any integer, b an integer exceeding* 1, *and b' a positive integer smaller than b. Let*

$$S' = \{w \in S \mid w \equiv a \pmod{p^{b'}}\}.$$

(i) *If $\sum_{w\in S} \psi(w)\xi_b^w = 0$, then $\sum_{w\in S'} \psi(w)\xi_b^w = 0$.*

(ii) *If $\sum_{w\in S} \psi(w)\xi_b^w \equiv 0 \pmod{c}$ with an integer c, then $\sum_{w\in S'} \psi(w)\xi_b^w \equiv 0 \pmod{c}$.*

PROOF. We may assume $S \subseteq \{0\} \cup \boldsymbol{N}$. Under this assumption, it is easy to prove the assertion (i), since the p^b-th cyclotomic polynomial in an indeterminate y belongs to $\boldsymbol{Z}[y^{p^{b-1}}]$. The assertion (ii) readily follows from (i). □

LEMMA 6. *Let l be a prime number different from p, F an extension in $\boldsymbol{Q}(\xi_n)$ of the decomposition field of l for $\boldsymbol{Q}(\xi_n)/\boldsymbol{Q}$, and D the absolute value of the discriminant of F. Assume that l divides h_n/h_{n-1} and that $F \subseteq \boldsymbol{Q}(\xi_\nu) \subseteq \boldsymbol{Q}(\xi_n)$. Then*

$$l < \sqrt{D}\left(\frac{f^2(f-1)^{(f-1)/2}}{(\log 2)\,p^{(\nu-1/(p-1))f/2}}\log(\max(\|\eta_n\|, \|\eta_n^{-1}\|))\right)^{[F:\boldsymbol{Q}]}.$$

PROOF. Let σ be a generator of $\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q})$. By Lemma 2, there exists a prime ideal $\mathfrak{l}$ of F dividing l such that, for any $\beta \in l\mathfrak{l}^{-1}$, $\eta_n^{\beta_\sigma}$ is an l-th power in E_n. Let $\mathfrak{K}$ denote the decomposition field of l for $\boldsymbol{Q}(\xi_n)/\boldsymbol{Q}$. Then the norm of $l\mathfrak{l}^{-1}$ for $F/\boldsymbol{Q}$ is $(l^{[\mathfrak{K}:\boldsymbol{Q}]-1})^{[F:\mathfrak{K}]}$. Therefore, Minkowski's lattice theorem shows that

$$\|\alpha\| \le (\sqrt{D}(l^{[\mathfrak{K}:\boldsymbol{Q}]-1})^{[F:\mathfrak{K}]})^{1/[F:\boldsymbol{Q}]} \quad \text{with some } \alpha \in l\mathfrak{l}^{-1}\setminus\{0\}. \tag{8}$$

As $\boldsymbol{Q}(\xi_\nu)$ contains F, α is written in the form

$$\alpha = \sum_{j=1}^{f} a_j \xi_\nu^{j-1}, \quad a_1, \dots, a_f \in \boldsymbol{Z}.$$

It follows that

$$\alpha_\sigma = \sum_{j=1}^{f} a_j \sigma^{p^{n-\nu}(j-1)} \quad \text{in } R_n,$$

so that

$$\|\eta_n^{\alpha_\sigma}\| \le \max(\|\eta_n\|, \|\eta_n^{-1}\|)^{\sum_{j=1}^{f}|a_j|}. \tag{9}$$

We define a square matrix X of degree f by

$$X = \left(\xi_\nu^{r_u(j-1)}\right)_{u,j=1,\dots,f}.$$

Here, for each $u \in \{1, \dots, f\}$, r_u denotes the u-th positive integer relatively prime to p. We note that $\det(X)^2$ equals the discriminant of $\boldsymbol{Q}(\xi_\nu)$:

$$\det(X)^2 = (-1)^{f/2} p^{(\nu-1/(p-1))f}. \tag{10}$$

Now take any $j \in \{1, \dots, f\}$. Let z_u denote, for each $u \in \{1, \dots, f\}$, the (j, u)-cofactor of X. Then

$$a_j = \det(X)^{-1} \sum_{u=1}^{f} z_u \alpha^{(u)} ,$$

where for each $u \in \{1, \dots, f\}$, $\alpha^{(u)}$ is the image of α under the automorphism of $\boldsymbol{Q}(\xi_\nu)$ mapping ξ_ν to $\xi_\nu^{r_u}$. Hence (8) and (10), together with Hadamard's inequality, yield

$$|a_j| \le \frac{f(f-1)^{(f-1)/2}}{p^{(\nu-1/(p-1))f/2}} (\sqrt{D} l^{[F:\boldsymbol{Q}]-[F:\mathfrak{K}]})^{1/[F:\boldsymbol{Q}]} .$$

We therefore see from (9) that

$$\text{(11)} \qquad \log \|\eta_n^{\alpha_\sigma}\| \le \frac{f^2(f-1)^{(f-1)/2}}{p^{(\nu-1/(p-1))f/2}} (\sqrt{D} l^{[F:\boldsymbol{Q}]-1})^{1/[F:\boldsymbol{Q}]} \log(\max(\|\eta_n\|, \|\eta_n^{-1}\|)) .$$

On the other hand, $\eta_n^{\alpha_\sigma}$ is neither 1 nor -1; indeed, if $(\eta_n^{\alpha_\sigma})^2 = 1$, then $\eta_n^{2N} = 1$, N being the norm of α for $F/\boldsymbol{Q}$. It is also known that $h_1 = 1$ if $p = 3$. Hence, by Lemma 3, we have

$$l \log 2 < \log \|\eta_n^{\alpha_\sigma}\| .$$

This and (11) lead us to the inequality which is to be proved. □

Now, in the case $p > 2$, let v be the number of distinct prime numbers dividing $(p-1)/2$, let

$$\frac{p-1}{2} = m_1 \cdots m_v ,$$

where $m_1, \dots, m_v$ are prime-powers greater than 1 and pairwise relatively prime, and let V denote the set of roots of unity

$$e^{\pi i c_1/m_1} \cdots e^{\pi i c_v/m_v}$$

for all v-tuples $(c_1, \dots, c_v)$ of integers with $0 \le c_1 < m_1, \dots, 0 \le c_v < m_v$. Then V is a complete set of representatives of the quotient group

$$\langle e^{2\pi i/(p-1)} \rangle / \{-1, 1\} .$$

We let $V = \{1\}$ in the case $p = 2$.

Let l be any prime number other than p. Let Φ_l denote the set of maps from V into $\{u \in \mathbf{Z} \mid 0 \le u \le 2fl\}$. Denoting by $\mathfrak{N}$ the norm map from $\boldsymbol{Q}(e^{2\pi i/(p-1)})$ to $\boldsymbol{Q}$, we put

$$\mu(l) = \max_{g \in \Phi_l} \left| \mathfrak{N}\left(\sum_{\delta \in V} g(\delta)\delta - 1 \right) \right| .$$

LEMMA 7. *Let l be as above. Assume that l divides h_n/h_{n-1}, $p^{2\nu}$ divides qp^n, and $\boldsymbol{Q}(\xi_\nu)$ contains the decomposition field of l for $\boldsymbol{Q}(\xi_n)/\boldsymbol{Q}$. Then*

$$\mu(l) \ge qp^{n-\nu} .$$

PROOF. Note first that the hypothesis $p^{2\nu} \mid qp^n$ yields

$$n \geq \nu\,, \quad qp^n \mid (qp^{n-\nu})^2\,.$$

Let $r = 1 + qp^{n-\nu}$. Then, from the above divisibility, we obtain

$$r^b \equiv 1 + bqp^{n-\nu} \pmod{qp^n} \quad \text{for every } b \in \boldsymbol{Z}\,. \tag{12}$$

Let s be an integer such that

$$s^{p^{n-\nu}} \equiv r \pmod{qp^n}\,,$$

and let σ be the restriction to $\boldsymbol{B}_n$ of the automorphism of $\boldsymbol{Q}(\zeta)$ mapping ζ to ζ^s. It follows that $\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q}) = \langle\sigma\rangle$. As Lemma 2 shows under our assumptions, there exists a prime ideal $\mathfrak{l}$ of $\boldsymbol{Q}(\xi_\nu)$ dividing l such that $\eta_n^{\beta_\sigma}$ is an l-th power in E_n for every $\beta \in l\mathfrak{l}^{-1}$. Let α be an algebraic integer which is contained in $l\mathfrak{l}^{-1}$ but not divisible by l: $\alpha \in l\mathfrak{l}^{-1} \setminus l\boldsymbol{Z}[\xi_\nu]$. Let us write α as

$$\alpha = \sum_{j=1}^{f} a_j \xi_\nu^{j-1}\,, \quad a_1, \ldots, a_f \in \boldsymbol{Z}\,.$$

Then, in R_n,

$$\alpha_\sigma = \sum_{j=1}^{f} a_j \sigma^{p^{n-\nu}(j-1)}\,.$$

Now, let $\mathfrak{p}$ be a prime ideal of $\boldsymbol{Q}(e^{2\pi i/(p-1)})$ dividing p. Let I denote the set of positive integers $< qp^n$ congruent to elements of V modulo $\mathfrak{q}\mathfrak{p}^n$, where $\mathfrak{q}$ denotes the highest power of $\mathfrak{p}$ dividing q. Note that $I = \{1\}$ when $p = 2$. Put $t = 1 + qp^{n-1}$. As the degree of $\mathfrak{p}$ is equal to 1, we obtain, in the case $p > 2$,

$$\eta_n = \prod_{u \in I} \frac{\zeta^u - \zeta^{-u}}{\zeta^{tu} - \zeta^{-tu}} = \prod_{u \in I} \xi_1^u \frac{\zeta^{2u} - 1}{\zeta^{2tu} - 1}\,,$$

so that, by the definition of σ,

$$\eta_n^{\alpha_\sigma} = \prod_{j=1}^{f} \prod_{u \in I} \left(\xi_1^{ur^{j-1}} \frac{\zeta^{2ur^{j-1}} - 1}{\zeta^{2tur^{j-1}} - 1} \right)^{a_j}.$$

In the case $p = 2$,

$$\eta_n = i\,\frac{\zeta - 1}{\zeta^t - 1}\,, \quad \text{and hence} \quad \eta_n^{\alpha_\sigma} = \prod_{j=1}^{f} \left(i^{r^{j-1}} \frac{\zeta^{r^{j-1}} - 1}{\zeta^{tr^{j-1}} - 1} \right)^{a_j}.$$

Consequently, it always follows that

$$\prod_{j=1}^{f} \prod_{u \in I} \left(\frac{\zeta^{ur^{j-1}} - 1}{\zeta^{tur^{j-1}} - 1} \right)^{a_j} = \varepsilon^l \quad \text{for some } \varepsilon \in \boldsymbol{Z}[\zeta]\,.$$

Hence, by Lemma 5 of [7] (cf. Ennola [4]),

$$\prod_{j=1}^{f}\prod_{u\in I}\left(\frac{\zeta^{lur^{j-1}}-1}{\zeta^{ltur^{j-1}}-1}\right)^{a_j} \equiv \prod_{j=1}^{f}\prod_{u\in I}\left(\frac{\zeta^{ur^{j-1}}-1}{\zeta^{tur^{j-1}}-1}\right)^{a_j l} \pmod{l^2}. \tag{13}$$

Next, let y be an indeterminate. Define an element $J(y)$ of $\mathbf{Z}[y]$ 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 $l=2$. Then

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

and, for each $b\in\mathbf{Z}$ and each $u'\in\mathbf{Z}$ with $p\nmid u'$,

$$(\zeta^{u'}-1)^{bl}\equiv(\zeta^{lu'}-1)^{b-1}(\zeta^{lu'}-1+blJ(\zeta^{u'})) \pmod{l^2}.$$

We therefore see from (13) that

$$\begin{aligned}&\prod_{j=1}^{f}\prod_{u\in I}((\zeta^{lur^{j-1}}-1)(\zeta^{ltur^{j-1}}-1+a_jlJ(\zeta^{tur^{j-1}})))\\ &\qquad\equiv\prod_{j=1}^{f}\prod_{u\in I}((\zeta^{lur^{j-1}}-1+a_jlJ(\zeta^{ur^{j-1}}))(\zeta^{ltur^{j-1}}-1)) \pmod{l^2}.\end{aligned}$$

This implies that

$$\begin{aligned}&\left(\prod_{j=1}^{f}\prod_{u\in I}(\zeta^{lur^{j-1}}-1)\right)\sum_{m=1}^{f}\sum_{w\in I}a_mJ(\zeta^{twr^{m-1}})\Pi_{m,w}\\ &\qquad\equiv\left(\prod_{j=1}^{f}\prod_{u\in I}(\zeta^{ltur^{j-1}}-1)\right)\sum_{m=1}^{f}\sum_{w\in I}a_mJ(\zeta^{wr^{m-1}})\Pi'_{m,w} \pmod{l}.\end{aligned}\tag{14}$$

Here

$$\Pi_{m,w}=\prod_{(j,u)\neq(m,w)}(\zeta^{ltur^{j-1}}-1), \quad \Pi'_{m,w}=\prod_{(j,u)\neq(m,w)}(\zeta^{lur^{j-1}}-1),$$

with (j,u) running through $\{1,\dots,f\}\times I\setminus\{(m,w)\}$. Let Ψ be the set of maps from $\{1,\dots,f\}\times I$ to $\{0,1\}$. Put

$$A(\kappa)=\sum_{j=1}^{f}\sum_{u\in I}lur^{j-1}\kappa(j,u) \quad \text{for each } \kappa\in\Psi.$$

For any $(m, w) \in \{1, \dots, f\} \times I$, let $\Psi_{m,w}$ denote the set of the restrictions of maps in Ψ to $\{1, \dots, f\} \times I \setminus \{(m, w)\}$. We then put, for each $\kappa' \in \Psi_{m,w}$ and each $\kappa \in \Psi$,

$$B(\kappa') = \sum_{(j,u)\neq(m,w)} lur^{j-1}\kappa'(j,u)\,,$$
$$G(\kappa,\kappa') = \kappa(m,w) + \sum_{(j,u)\neq(m,w)} (\kappa(j,u)+\kappa'(j,u))\,,$$

where (j, u) runs through $\{1, \dots, f\} \times I \setminus \{(m, w)\}$. It follows that

$$\left(\prod_{j=1}^{f}\prod_{u\in I}(\zeta^{lur^{j-1}}-1)\right)\sum_{m=1}^{f}\sum_{w\in I} a_m J(\zeta^{twr^{m-1}})\Pi_{m,w}$$
$$= -\sum_{m=1}^{f}\sum_{w\in I}\sum_{\kappa\in\Psi}\sum_{\kappa'\in\Psi_{m,w}}(-1)^{G(\kappa,\kappa')}a_m J(\zeta^{twr^{m-1}})\zeta^{A(\kappa)+tB(\kappa')}\,, \tag{15}$$

$$\left(\prod_{j=1}^{f}\prod_{u\in I}(\zeta^{ltur^{j-1}}-1)\right)\sum_{m=1}^{f}\sum_{w\in I} a_m J(\zeta^{wr^{m-1}})\Pi'_{m,w}$$
$$= -\sum_{m=1}^{f}\sum_{w\in I}\sum_{\kappa\in\Psi}\sum_{\kappa'\in\Psi_{m,w}}(-1)^{G(\kappa,\kappa')}a_m J(\zeta^{wr^{m-1}})\zeta^{tA(\kappa)+B(\kappa')}\,. \tag{16}$$

To apply Lemma 5 to (14) later, we now consider the two congruences

$$twr^{m-1}c + A(\kappa) + tB(\kappa') \equiv \sum_{j=1}^{f}\sum_{u\in I} l(1+t)ur^{j-1} - 1 \pmod{qp^{n-\nu}}\,, \tag{17}$$

$$wr^{m-1}c + tA(\kappa) + B(\kappa') \equiv \sum_{j=1}^{f}\sum_{u\in I} l(1+t)ur^{j-1} - 1 \pmod{qp^{n-\nu}}\,. \tag{18}$$

Here $(m, w) \in \{1, \dots, f\} \times I$, $\kappa \in \Psi$, $\kappa' \in \Psi_{m,w}$, and

$$c \in \{1, \dots, l-1\} \quad \text{or} \quad c \in \{0, 1\}$$

according as $l > 2$ or $l = 2$. We easily find that either of the above congruences is equivalent to the following:

$$\sum_{u\in I\setminus\{w\}}\left(2fl - \sum_{j=1}^{f} l(\kappa(j,u)+\kappa'(j,u))\right)u - 1$$
$$+\left(2fl - \sum_{j=1}^{f} l\kappa(j,w) - \sum_{j\in\{1,\dots,f\}\setminus\{m\}} l\kappa'(j,w) - c\right)w \equiv 0 \pmod{qp^{n-\nu}}\,. \tag{19}$$

By the definition of Φ_l, there exists a unique $g \in \Phi_l$ such that

$$g(\delta) = 2fl - \sum_{j=1}^{f} l(\kappa(j,u) + \kappa'(j,u))$$

if $\delta \in V$, $u \in I \setminus \{w\}$, and $\delta \equiv u \pmod{\mathfrak{q}\mathfrak{p}^n}$, and such that

$$g(\delta) = 2fl - \sum_{j=1}^{f} l\kappa(j,w) - \sum_{j\in\{1,\dots,f\}\setminus\{m\}} l\kappa'(j,w) - c$$

if $\delta \in V$ and $\delta \equiv w \pmod{\mathfrak{q}\mathfrak{p}^n}$. Therefore, (19) is written in the form

$$\sum_{\delta\in V} g(\delta)\delta - 1 \equiv 0 \pmod{\mathfrak{q}\mathfrak{p}^{n-\nu}}\,.$$

Now, contrary to the conclusion of the lemma, assume that $\mu(l) < qp^{n-\nu}$. Since the above congruence induces

$$\mathfrak{N}\left(\sum_{\delta\in V} g(\delta)\delta - 1\right) \equiv 0 \pmod{qp^{n-\nu}}\,,$$

the definition of $\mu(l)$ enables us to deduce

$$\sum_{\delta\in V} g(\delta)\delta - 1 = 0$$

from (17) or, equivalently, from (18). Lemma 7 of [7] then implies that $g(1) = 1$ and that $g(\delta) = 0$ for every $\delta \in V\setminus\{1\}$. Consequently, both of (17), (18) are equivalent to the condition that

$$w = 1, \quad c = l-1\,, \quad \kappa(j,u) = 1 \text{ for every } (j,u) \text{ in } \{1,\dots,f\}\times I\,,$$
$$\kappa'(j,u) = 1 \text{ for every } (j,u) \text{ in } \{1,\dots,f\}\times I \setminus \{(m,1)\}\,,$$

where

$$m \in \{1,\dots,f\}\,, \quad \kappa \in \Psi\,, \quad \kappa' \in \Psi_{m,1}\,.$$

It follows under this condition that, for each m,

$$B(\kappa') + lr^{m-1} = A(\kappa) = \sum_{j=1}^{f}\sum_{u\in I} lur^{j-1}\,, \quad G(\kappa,\kappa') = \varphi(q)f - 1\,.$$

Hence, in view of (14), (15), (16), and Lemma 5, we obtain

$$\sum_{m=1}^{f} a_m \zeta^{(l-1)tr^{m-1} + (1+t)\sum_{j=1}^{f}\sum_{u\in I} lur^{j-1} - tlr^{m-1}}$$
$$\equiv \sum_{m=1}^{f} a_m \zeta^{(l-1)r^{m-1} + (t+1)\sum_{j=1}^{f}\sum_{u\in I} lur^{j-1} - lr^{m-1}} \pmod{l}\,,$$

namely,

$$\sum_{m=1}^{f} a_m \zeta^{-tr^{m-1}} \equiv \sum_{m=1}^{f} a_m \zeta^{-r^{m-1}} \pmod{l}\,. \tag{20}$$

Furthermore, by (12),

$$\zeta^{r^{m-1}} = \zeta \xi_\nu^{m-1} \quad \text{for each } \ m\,.$$

Complex conjugation then transforms (20) into

$$\zeta^t \sum_{m=1}^{f} a_m \xi_\nu^{(m-1)t} \equiv \zeta\alpha \pmod{l}\,.$$

However, $\zeta^t = \xi_1\zeta$ holds, and $\xi_\nu^t = \xi_\nu$ follows from $\nu \le n$. Thus

$$(\xi_1 - 1)\zeta\alpha \equiv 0 \pmod{l}\,, \quad \text{i.e.}\,, \quad \alpha \in l\boldsymbol{Z}[\xi_\nu]\,.$$

This contradiction completes the proof of the lemma.

2. In this section, we shall prove the three assertions stated in the introduction. The letter x will denote a real variable.

Let us first prove the following result, which essentially implies Theorem 1.

PROPOSITION. *Let*

$$M_* = \frac{(\log p)\varphi(q) f^2 (f-1)^{(f-1)/2}}{(2\log 2)\, p^{(\nu - 1/(p-1))(f-1)/2}}\,,$$

and let λ *be the minimal positive integer such that*

$$(p-1) f (\lambda M_*)^f \le p^{(\lambda - \nu + 1)/\varphi(p-1)}\,.$$

Then $C_{\boldsymbol{B}_\infty}(l)$ *is trivial for every* $l \in P$ *satisfying*

$$l^{\varphi(q)} \not\equiv 1 \pmod{qp^\nu}\,, \quad l \nmid H\,, \quad l \ge ((\lambda - 1)M_*)^f\,.$$

PROOF. Let

$$L = ((p-1)f)^{1/f} M_* = \frac{(p-1)^{1/f}(\log p)\varphi(q) f^{2+1/f}(f-1)^{(f-1)/2}}{(2\log 2)\, p^{(\nu-1/(p-1))(f-1)/2}}\,.$$

We define a smooth function $W(x)$ by

$$W(x) = p^{(x-\nu+1)/(\varphi(p-1)f)} - Lx\,.$$

Obviously, $W(x) \to \infty$ for $x \to \infty$, and the definition of λ implies $W(\lambda) \ge 0$. We put

$$x_0 = \frac{\varphi(p-1)f}{\log p} \log\left(\frac{\varphi(p-1)fL}{\log p}\right) + \nu - 1\,,$$

so that

$$W'(x_0) = 0\,; \quad W'(x) > 0 \quad \text{if } \ x > x_0\,; \quad W'(x) < 0 \quad \text{if } \ x < x_0\,.$$

On the other hand,

$$L \geq \frac{(\log p) f^2 (f-1)^{(f-1)/2}}{(\log 2) p^{(\nu-1/(p-1))(f-1)/2}}$$
$$= \frac{\log p}{\log 2} f^2 \left(1+\frac{1}{f-1}\right)^{(1-f)/2} \left(p\left(1+\frac{1}{p-1}\right)^{1-p}\right)^{(f-1)/(2p-2)} .$$

Since

$$\left(1+\frac{1}{f-1}\right)^{(f-1)/2} < \sqrt{e}\,, \quad p\left(1+\frac{1}{p-1}\right)^{1-p} \geq 1\,,$$

it follows that

$$\frac{\varphi(p-1) f L}{\log p} > \frac{f^3}{\sqrt{e}\log 2} > 4\,, \quad L > \frac{f^2}{\sqrt{e}} > p^{1/(p-1)} .$$

Furthermore,

$$\frac{\varphi(p-1) f}{\log p} \geq \frac{p-1}{\log p} \geq \frac{1}{\log 2} .$$

We therefore see that

$$x_0 > 2\,, \quad W(1) = p^{(2-\nu)/(\varphi(p-1)f)} - L \leq p^{1/(p-1)} - L < 0 .$$

Hence we have $\lambda \geq 3$ and the restriction of $W(x)$ on the interval $[\lambda, \infty)$ is a strictly increasing function.

Now, let l be a prime number different from p such that $C_{\boldsymbol{B}_\infty}(l)$ is not trivial. Assume further that

$$l^{\varphi(q)} \not\equiv 1 \pmod{qp^\nu}\,, \quad l \nmid H .$$

It suffices to prove the inequality

$$l < ((\lambda-1)M_*)^f . \tag{21}$$

As $C_{\boldsymbol{B}_\infty}(l)$ is not trivial, l divides h_u/h_{u-1} for some $u \in \boldsymbol{N}$. By the assumption $l \nmid H$,

$$p^u > p^{2\nu-1}/q\,, \quad \text{namely}\,, \quad p^{2\nu} \mid qp^u\,,$$

so that $u \geq \nu$ follows. We then know, from the assumption $l^{\varphi(q)} \not\equiv 1 \pmod{qp^\nu}$, that $\boldsymbol{Q}(\xi_\nu)$ contains the decomposition field of l for $\boldsymbol{Q}(\xi_u)/\boldsymbol{Q}$. Therefore, by Lemma 6,

$$l < \left(\frac{2M_*}{\varphi(q)\log p}\log(\max(\|\eta_u\|, \|\eta_u^{-1}\|))\right)^f . \tag{22}$$

Hence, in the case where $u = 1$ and $p > 2$, Lemma 4 gives

$$l < \left(\frac{M_*}{\log p}\log\left(\frac{p^2}{\pi}\sin\frac{\pi}{p} + \cos\frac{\pi}{p}\right)\right)^f ,$$

which, together with $\lambda \geq 3$, proves (21).

We next suppose that $u \geq 2$ or $p = 2$. It is easily seen that

$$\frac{p^{u+1}}{\pi}\sin\frac{\pi}{p} + \cos\frac{\pi}{p} < p^u \quad \text{if} \quad p > 2 .$$

Hence, by Lemma 4 and (22),

$$l < (\tilde{u} M_*)^f \,, \tag{23}$$

where $\tilde{u} = u$ or $u+1$ according as $p > 2$ or $p = 2$; $p^{\tilde{u}} = qp^{u-1}$. Also, we obtain, for any $g \in \Phi_l$,

$$\left|\mathfrak{N}\left(\sum_{\delta \in V} g(\delta)\delta - 1\right)\right| = \prod_{\rho} \left|\sum_{\delta \in V} g(\delta)\delta^{\rho} - 1\right|.$$

Here ρ ranges over the automorphisms of $\boldsymbol{Q}(\zeta_{p-1})$, and

$$\left|\sum_{\delta \in V} g(\delta)\delta^{\rho} - 1\right| \le |g(1) - 1| + \sum_{\delta \in V \setminus \{1\}} g(\delta) < \frac{p-1}{2} \cdot 2fl \,.$$

Thus

$$\mu(l) < ((p-1)fl)^{\varphi(p-1)} \,.$$

However, since $p^{2\nu}$ divides qp^u, Lemma 7 yields $qp^{u-\nu} \le \mu(l)$. Hence

$$\frac{p^{(\tilde{u}-\nu+1)/\varphi(p-1)}}{(p-1)f} < l \,.$$

This, together with (23), implies $W(\tilde{u}) < 0$, while

$$W(x) \ge 0 \quad \text{if } x \ge \lambda \,.$$

Therefore, we have $\tilde{u} \le \lambda - 1$ and, consequently, (21) is obtained from (23). □

We are now ready to give

PROOF OF THEOREM 1. Let L, $W(x)$, x_0 be the same as in the above proof, and let

$$R = \frac{\varphi(p-1)f}{\log p} \,.$$

Then

$$\begin{aligned} RL =& \frac{\varphi((p-1)q)f^3(f(p-1))^{1/f}}{2\log 2}\left(1 + \frac{1}{f-1}\right)^{(1-f)/2}\left(p\left(1 + \frac{1}{p-1}\right)^{1-p}\right)^{(f-1)/(2p-2)} \\ <& \frac{\varphi((p-1)q)f^3 \cdot 2}{2\log 2} \cdot \frac{1}{\sqrt{2}}\left(\frac{p}{2}\right)^{p^{\nu-1}/2} . \end{aligned}$$

Therefore

$$\log(RL) < 2\log p - \log(2\sqrt{2}\log 2) + 3\nu\log p + \frac{p^{\nu-1}}{2}\log\frac{p}{2} \,.$$

We also have $\lambda - 1 < 2x_0$, because

$$\begin{aligned} W(2x_0) &= p^{(\nu-1)/(\varphi(p-1)f)}R^2L^2 - 2L(R\log(RL) + \nu - 1) \\ &\ge RL(RL - 2\log(RL) - 1) + L(R - 2(\nu-1)) > 0 \,. \end{aligned}$$

Hence

$$\lambda - 1 < 2(R\log(RL) + \nu - 1) < R\left(p^{\nu-1}\log\frac{p}{2} + (6\nu+4)\log p\right).$$

Theorem 1 thus follows from our Proposition. □

We next proceed to

PROOF OF THEOREM 2. Let C_K^- denote the kernel of the norm map $C_K \to C_{\boldsymbol{B}_\infty}$, and let $C_K^-(l)$ denote for each $l \in P$ the l-primary component of C_K^-. By class field theory, the norm map $C_K \to C_{\boldsymbol{B}_\infty}$ induces an isomorphism $C_K/C_K^- \xrightarrow{\sim} C_{\boldsymbol{B}_\infty}$. Hence, for each $l \in P$, $C_K(l) = 1$ if and only if $C_K^-(l) = C_{\boldsymbol{B}_\infty}(l) = 1$. On the other hand, let Σ be the finite set of algebraic integers in $\boldsymbol{Z}[\xi_\nu]$ of the form

$$(1-\xi_\nu)\sum_{u=1}^{\varphi(q)/2}\frac{\xi_\nu^{b_u}}{1-\xi_\nu^{\Delta c_u}}\sum_{j=1}^{\Delta} a_{j,u}\xi_\nu^{c_u j}, \tag{24}$$

where each $a_{j,u}$ ranges over -1, 0 and 1, each b_u over all integers, and each c_u over the integers relatively prime to p. It is shown in [10, §IV] not only that Σ has a nonzero element but that $C_K^-(l) = 1$ for every prime number l other than p with the following properties (cf. [7, Theorem 1]; as for the first property, see also the remark below this proof):

(i) l does not divide h^*,

(ii) l is relatively prime to all non-zero elements of Σ,

(iii) $l^{\varphi(q)} \not\equiv 1 \pmod{qp^\nu}$, namely, $\boldsymbol{Q}(\xi_\nu)$ contains the decomposition field of l for the abelian extension $\boldsymbol{B}_\infty(e^{2\pi i/q})/\boldsymbol{Q}$.

Now, let Λ be the norm for $\boldsymbol{Q}(\xi_\nu)/\boldsymbol{Q}$ of an element of Σ in the form (24). Let Z_1 denote the set of positive integers $< p^\nu$ relatively prime to p, and Z_2 the set of positive integers $< p^\nu/2$. Then

$$|\Lambda| \le p\prod_{a\in Z_1}\left(\sum_{u=1}^{\varphi(q)/2}\frac{\Delta}{|1-\xi_\nu^{\Delta c_u a}|}\right) \le p\left(\frac{1}{f}\sum_{a\in Z_1}\sum_{u=1}^{\varphi(q)/2}\frac{\Delta}{|1-\xi_\nu^{\Delta c_u a}|}\right)^f$$
$$= p\left(\frac{\varphi(q)\Delta}{2f}\sum_{a\in Z_1}\frac{1}{|1-\xi_\nu^a|}\right)^f,$$

$$\sum_{a\in Z_1}\frac{1}{|1-\xi_\nu^a|} = \sum_{a\in Z_1}\frac{1}{2\sin(\pi a/p^\nu)} \le 2\left(\sum_{a\in Z_2}\frac{1}{2\sin(\pi a/p^\nu)}\right)$$
$$< 2\left(\frac{1}{2\sin(\pi/p^\nu)} + \sum_{a\in Z_2\setminus\{1\}}\frac{p^\nu}{\pi}\int_{\pi(a-1)/p^\nu}^{\pi a/p^\nu}\frac{dx}{2\sin x}\right)$$
$$< \frac{1}{\sin(\pi/p^\nu)} + \frac{p^\nu}{\pi}\int_{\pi/p^\nu}^{\pi/2}\frac{dx}{\sin x}$$

$$< \frac{p^\nu}{\pi}\left(1+\frac{\pi^2}{3p^{2\nu}}\right)+\frac{p^\nu}{\pi}\log\left(\frac{1}{\tan(\pi/2p^\nu)}\right) < \frac{p^\nu}{\pi}(\nu\log p+1)\,.$$

Hence we have

$$|\Lambda| < p\Gamma^f \quad \text{with } \Gamma = \frac{q\Delta(\nu\log p+1)}{2\pi}\,,$$

so that, as l in (ii) above, every prime number at least equal to $p\Gamma^f$ is relatively prime to all nonzero element of Σ. We further find that $\Gamma > 1$, i.e., $p\Gamma^f > p$. Therefore Theorem 1 completes the proof of Theorem 2. □

REMARK. Theorem 1 of [7] has assumed that the relative class number of k_{m^*} is not divisible by l; but, in view of the proof of the theorem, we can change this assumption into the assumption that the relative class numbers of $k_{m^*/p'}$ for all prime divisors p' of m^* are relatively prime to l.

Finally, let

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

and put $\pi(x) = |P(x)|$ as usual. It follows from Theorem 2 that

$$\liminf_{x\to\infty}\frac{|\{l \in P(x) \mid C_K(l)=1\}|}{\pi(x)} \geq \lim_{x\to\infty}\frac{|\{l \in P(x) \mid l^{\varphi(q)} \not\equiv 1 \pmod{qp^\nu}\}|}{\pi(x)} = 1-\frac{1}{p^\nu}\,.$$

Since any integer greater than 1 can be chosen as ν, we then obtain:

THEOREM 3.

$$\lim_{x\to\infty}\frac{|\{l \in P(x) \mid C_K(l)=1\}|}{\pi(x)} = 1\,.$$

In particular,

$$\lim_{x\to\infty}\frac{|\{l \in P(x) \mid C_{\boldsymbol{B}_\infty}(l)=1\}|}{\pi(x)} = 1\,.$$

3. We conclude the paper by making some additional remarks on our main results.

With x_0 and R in the proof of Theorem 1, we actually see that

$$\lambda - 1 < x_0 + \frac{x_0}{x_0/R-1}\log\frac{x_0}{R} < \frac{17}{10}x_0\,.$$

Accordingly, in Theorems 1 and 2, the constant M can be replaced by a constant somewhat smaller than M.

Whereas Theorem 1 is proved, we have not yet found a prime number l_0 for which $C_{\boldsymbol{B}_\infty}(l_0)$ is nontrivial. It thus seems interesting to know if such a prime l_0 exists or how many examples of l_0 exist (cf. [7, §3]). We would note here that Cohn [2], closely connected with Theorem 1 for $p = 2$, is a suggestive article in spite of its incompleteness (cf. also Cerri [1], Cohn and Deutsch [3], Washington [12]).

When p, ν, and the conductor of k are small enough, we obtain a few results more precise than Theorem 2, by checking the proofs of several assertions in §1, [7], and [10].

For instance, it turns out that, if p equals 2 or 3, then the class number of $\boldsymbol{Q}(\xi_m)$ for every $m \in \boldsymbol{N}$ is relatively prime to every $l \in P$ with $l^2 \not\equiv 1 \pmod{2qp}$. On the other hand, the arguments in the present paper suggest a possibility of extending our theorems for $\boldsymbol{B}_\infty$ or K to some results for a more general type of abelian extension over $\boldsymbol{Q}$. Such generalizations and the above-mentioned improvements will be discussed in our forthcoming papers.

REFERENCES

[1] J.-P. CERRI, De l'euclidianité de $\boldsymbol{Q}(\sqrt{2+\sqrt{2+\sqrt{2}}})$ et $\boldsymbol{Q}(\sqrt{2+\sqrt{2}})$ pour la norme, J. Théor. Nombres Bordeaux 12 (2000), 103–126.

[2] H. COHN, A numerical study of Weber's real class number calculation I, Numer. Math. 2 (1960), 347–362.

[3] H. COHN AND J. DEUTSCH, Use of a computer scan to prove $\boldsymbol{Q}(\sqrt{2+\sqrt{2}})$ and $\boldsymbol{Q}(\sqrt{3+\sqrt{2}})$ are euclidean, Math. Comp. 46 (1986), 295–299.

[4] V. ENNOLA, Proof of a conjecture of Morris Newman, J. Reine Angew. Math. 264 (1973), 203–206.

[5] A. FRÖHLICH, On the absolute class-group of Abelian fields, J. London Math. Soc. 29 (1954), 211–217.

[6] H. HASSE, Über die Klassenzahl abelscher Zahlkörper, Reprint of the 1952 edition, Springer-Verlag, Berlin, 1985.

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

[8] K. IWASAWA, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257–258.

[9] L. KRONECKER, Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, J. Reine Angew. Math. 53 (1857), 173–175.

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

[11] L. C. WASHINGTON, The non-p-part of the class number in a cyclotomic $\boldsymbol{Z}_p$-extension, Invent. Math. 49 (1978), 87–97.

[12] L. C. WASHINGTON, Introduction to Cyclotomic Fields, Second edition, Springer-Verlag, New York, 1997.

DEPARTMENT OF MATHEMATICS
TOKAI UNIVERSITY
1117 KITAKANAME
HIRATSUKA 259–1292
JAPAN