J. Math. Soc. Japan
Vol. 64, No. 4 (2012) pp. 1071–1089
doi: 10.2969/jmsj/06441071

The l-class group of the $\boldsymbol{Z}_p$-extension over the rational field

By Kuniaki Horie and Mitsuko Horie

(Received July 2, 2010)
(Revised Mar. 1, 2011)

Abstract. Let p be an odd prime, and let $\boldsymbol{B}_\infty$ denote the $\boldsymbol{Z}_p$-extension over the rational field. Let l be an odd prime different from p. The question whether the l-class group of $\boldsymbol{B}_\infty$ is trivial has been considered in our previous papers mainly for the case where l varies with p fixed. We give a criterion, for checking the triviality of the l-class group of $\boldsymbol{B}_\infty$, which enables us to discuss the triviality when p varies with l fixed. As a consequence, we find that, if l does not exceed 13 and p does not exceed 101, then the l-class group of $\boldsymbol{B}_\infty$ is trivial.

Introduction.

Let p be any odd prime number. Let $\boldsymbol{Z}_p$ denote the ring of p-adic integers, and $\boldsymbol{B}_\infty$ the $\boldsymbol{Z}_p$-extension over the rational field $\boldsymbol{Q}$, namely, the unique abelian extension over $\boldsymbol{Q}$, contained in the complex field $\boldsymbol{C}$, whose Galois group over $\boldsymbol{Q}$ is topologically isomorphic to the additive group of $\boldsymbol{Z}_p$. The p-class group of $\boldsymbol{B}_\infty$ is known to be trivial (cf. Iwasawa [**7**]). Let l be an odd prime different from p. In the present paper, we shall first give a sufficient condition for the triviality of the l-class group of $\boldsymbol{B}_\infty$ by means of the reflection theorem on l-class groups (cf. Leopoldt [**8**]) together with some results obtained through algebraic study of the analytic class number formula (cf. Hasse [**2**], [**4**], Washington [**11**]). Discussing the sufficient condition with the help of a personal computer, we shall next see that, if $l \leq 13$ and $p \leq 101$, then the l-class group of $\boldsymbol{B}_\infty$ is trivial. Although our numerical result is thus limited, our criterion for checking the triviality of the l-class group of $\boldsymbol{B}_\infty$ seems to be widely applicable. In any case, the upper bounds for l and p in the above would become larger by further calculations.

As to the 2-class group of $\boldsymbol{B}_\infty$, we have given in [**5**] a sufficient condition for its triviality on the basis of some results in [**3**], [**4**]. Such a study motivates the investigation of the present paper; while, in connection with the contents of [**3**], [**5**], Ichimura and Nakajima have recently shown in [**6**] that, if $p < 500$, then the

2010 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R20, 11R23.
Key Words and Phrases. $\boldsymbol{Z}_p$-extension, l-class group, reflection theorem, class number formula, Iwasawa theory.

2-class group of $\boldsymbol{B}_\infty$ is trivial.

Acknowledgements. The authors are thankful to the referee who suggested natural modifications to the original proof of Lemma 4 including corrections of mistakes in the proof.

1. Notations and Theorems.

For each positive integer a, we put

$$\xi_a = e^{2\pi i/p^a}.$$

Let $\boldsymbol{P}_\infty$ denote the composite, in $\boldsymbol{C}$, of the cyclotomic fields of p^bth roots of unity for all positive integers b, i.e., let

$$\boldsymbol{P}_\infty = \bigcup_{b=1}^{\infty} \boldsymbol{Q}(\xi_b) = \boldsymbol{B}_\infty(\xi_1).$$

Let F be the decomposition field of l for the abelian extension $\boldsymbol{P}_\infty/\boldsymbol{Q}$. We note that $\boldsymbol{P}_\infty/F(\xi_1)$ is a $\boldsymbol{Z}_p$-extension. There exists a unique positive integer ν for which $\boldsymbol{Q}(\xi_\nu)$ is an extension of F and the degree of $\boldsymbol{Q}(\xi_\nu)/F$ divides $p-1$:

$$F \subseteq \boldsymbol{Q}(\xi_\nu), \quad [\boldsymbol{Q}(\xi_\nu) : F] \mid p-1.$$

In other words, ν is the positive integer determined by

$$l^{p-1} \equiv 1 \pmod{p^\nu}, \qquad l^{p-1} \not\equiv 1 \pmod{p^{\nu+1}}.$$

Let $\mathfrak{O}$ denote the ring of algebraic integers in F. Let S be the minimal set of non-negative integers less than $\varphi(p^\nu) = p^{\nu-1}(p-1)$ such that the additive group in $\boldsymbol{Q}(\xi_\nu)$ generated by ξ_ν^m for all $m \in S$ contains $\mathfrak{O}$, i.e.,

$$\mathfrak{O} \subseteq \sum_{m \in S} \boldsymbol{Z}\xi_\nu^m,$$

$\boldsymbol{Z}$ being the ring of (rational) integers. Evidently, S is not empty: $0 < |S| \leq \varphi(p^\nu)$. Now, take any cyclic group Γ of order p^ν, and a generator γ of Γ;

$$\Gamma = \{\gamma^m \mid m \in \boldsymbol{Z},\ 0 \leq m < p^\nu\}.$$

Let S^* denote the minimal set of non-negative integers less than p^ν such that in $\boldsymbol{Z}[\Gamma]$, the group ring of Γ over $\boldsymbol{Z}$,

$$\left(1-\gamma^{p^{\nu-1}}\right)\sum_{m\in S} b_m\gamma^m \in \sum_{m'\in S^*}\boldsymbol{Z}\gamma^{m'}$$

for every sequence $\{b_m\}_{m\in S}$ of integers with $\sum_{m\in S} b_m\xi_\nu^m \in \mathfrak{O}$. We easily see that S^* does not depend on the choice of Γ or γ. It also follows that $0<|S^*|\le p^\nu$.

Let v be the number of distinct prime divisors of $(p-1)/2$. Take the prime powers $q_1>1,\ldots,q_v>1$ satisfying

$$\frac{p-1}{2}=q_1\ldots q_v,$$

and let V denote the subset of the cyclic group $\langle e^{2\pi i/(p-1)}\rangle$ consisting of

$$e^{\pi i m_1/q_1}\ldots e^{\pi i m_v/q_v}$$

for all v-tuples $(m_1,\ldots,m_v)$ of integers with $0\le m_1<q_1,\ldots,0\le m_v<q_v$. We understand that $V=\{1\}$ if $p=3$. Furthermore, V is a complete set of representatives of the factor group $\langle e^{2\pi i/(p-1)}\rangle/\langle -1\rangle$. Let Φ denote the family of maps from V to the set of non-negative integers at most equal to $l|S^*|$. We put

$$M=\max_{\kappa\in\Phi}\left|\mathfrak{N}\left(\sum_{\varepsilon\in V}\kappa(\varepsilon)\varepsilon-1\right)\right|,$$

where $\mathfrak{N}$ denotes the norm map from $\boldsymbol{Q}(e^{2\pi i/(p-1)})$ to $\boldsymbol{Q}$. Clearly, M is a positive integer.

Let R be a set of positive integers smaller than p such that

$$R\cap\{p-a\mid a\in R\}=\emptyset,\quad R\cup\{p-a\mid a\in R\}=\{1,\ldots,p-1\}.$$

Given any integer $u\ge 0$, let R_u denote the set of integers b for which $b^{p-1}\equiv 1 \pmod{p^{u+1}}$, $0<b<p^{u+1}$, and $b\equiv a \pmod p$ with some $a\in R$. It follows that $|R_u|=|R|=(p-1)/2$; because, for each $a\in R$, there exists a unique $b\in R_u$ with $b\equiv a \pmod p$. For each positive integer n and each $\lambda\in\boldsymbol{Q}$ either relatively prime to p or in $p\boldsymbol{Z}$, we denote by $z_n(\lambda)$ the integer such that

$$z_n(\lambda)\equiv\lambda \pmod{p^n},\quad 0\le z_n(\lambda)<p^n.$$

As easily seen, any $b \in R_u$, any integer c with $p \nmid c$, and any integer $u' > u$ satisfy

$$(z_{u'}(c^{-1})z_{u+1}(bc))^{p-1} \equiv 1 \pmod{p^{u+1}},$$

whence

$$(z_{u'}(c^{-1})z_{u+1}(bc))^{p^{\nu}-1} \equiv 1 \pmod{p^{u+1}}.$$

We then define $w_{u,u'}(b,c)$ to be the least non-negative residue, modulo p^{ν}, of the integer $(1-(z_{u'}(c^{-1})z_{u+1}(bc))^{p^{\nu}-1})p^{-u-1}$:

$$w_{u,u'}(b,c) = z_{\nu}\big((1-(z_{u'}(c^{-1})z_{u+1}(bc))^{p^{\nu}-1})p^{-u-1}\big).$$

Let $\boldsymbol{B}_u$ denote the subfield of $\boldsymbol{B}_{\infty}$ with degree p^u, and let h_u denote the class number of $\boldsymbol{B}_u$. Since p is totally ramified for $\boldsymbol{B}_{\infty}/\boldsymbol{Q}$, class field theory shows that $h_{n-1} \mid h_n$ for every positive integer n. One of our results is now stated as follows.

THEOREM 1. *Let n be an integer $\geq 2\nu - 1$, so that $n \geq \nu$. Assume that, for any positive integer $j \leq l-2$ relatively prime to $l-1$, there exists an integer c with $p \nmid c$ for which the algebraic integer*

$$\sum_{b \in R_{n-\nu}} \sum_{a=0}^{z_{\nu}(bc)-1} \sum_{r=0}^{l-1} \big(z_{n-\nu+1}(bc) + p^{n-\nu+1}r\big)^j \xi_{\nu}^{z_{\nu}(b^{-1}c^{-1})(la+r)+w_{n-\nu,n+1}(b,c)}$$

is relatively prime to l, i.e., does not belong to any prime ideal of $\boldsymbol{Q}(\xi_{\nu})$ dividing l. Then l does not divide the integer h_n/h_{n-1}.

On the other hand, [**4**, Lemma 3] means that l does not divide $h_{n'}/h_{n'-1}$ for any integer $n' \geq 2\nu - 1$ satisfying $p^{n'-\nu+1} > M$. Hence the above theorem leads us to the following.

THEOREM 2. *Let n_0 be an integer $\geq 2\nu - 2$. Assume that $l \nmid h_{n_0}$ and that, for any positive integer $j \leq l-2$ relatively prime to $l-1$ and for any integer $n > n_0$ satisfying $p^{n-\nu+1} \leq M$, there exists an integer c with $p \nmid c$ for which*

$$\sum_{b \in R_{n-\nu}} \sum_{a=0}^{z_{\nu}(bc)-1} \sum_{r=0}^{l-1} \big(z_{n-\nu+1}(bc) + p^{n-\nu+1}r\big)^j \xi_{\nu}^{z_{\nu}(b^{-1}c^{-1})(la+r)+w_{n-\nu,n+1}(b,c)}$$

is relatively prime to l. Then the l-class group of $\boldsymbol{B}_{\infty}$ is trivial.

For each pair (r, n) of positive integers, let $H_n(r)$ denote the set of positive integers a with $p \nmid a$ satisfying $a/p^{n+1} < r/l$, and for each integer b with $p \nmid b$, let $y_n(b)$ denote the least non-negative residue, modulo p^n, of the integer $(1-b^{p^n-1})/p$. The following result, independent of ν, is useful in checking the indivisibility $l \nmid h_n/h_{n-1}$ particularly for a positive integer $n \leq 2\nu - 2$.

THEOREM 3. *Let n be a positive integer. Assume that, for each positive integer $j \leq l-2$ relatively prime to $l-1$, the algebraic integer*

$$\sum_{r=1}^{(l-1)/2} \sum_{a \in H_n(r)} r^j \xi_n^{y_n(a)}$$

is relatively prime to l. Then l does not divide h_n/h_{n-1}.

2. Proofs of Theorems 1 and 3.

To prove Theorems 1 and 3, we shall first give some preliminaries. Let $\boldsymbol{Z}_l$, $\boldsymbol{Q}_l$, and Ω_l denote the ring of l-adic integers, the field of l-adic numbers, and an algebraic closure of $\boldsymbol{Q}_l$, respectively. All algebraic numbers in $\boldsymbol{C}$ will also be regarded as elements of Ω_l through a fixed imbedding, into Ω_l, of the algebraic closure of $\boldsymbol{Q}$ in $\boldsymbol{C}$. In the rest of the paper, we suppose every Dirichlet character to be primitive. Given any Dirichlet character χ, we denote by g_χ the order of χ, denote by f_χ the conductor of χ, put $\mu_\chi = e^{2\pi i/f_\chi}$, and define χ^* to be the homomorphism of the Galois group $\mathrm{Gal}(\boldsymbol{Q}(\mu_\chi)/\boldsymbol{Q})$ into the multiplicative group of Ω_l such that, for each integer a relatively prime to f_χ, $\chi(a)$ is the image under χ^* of the automorphism in $\mathrm{Gal}(\boldsymbol{Q}(\mu_\chi)/\boldsymbol{Q})$ sending μ_χ to μ_χ^a. Let K_χ denote the fixed field in $\boldsymbol{Q}(\mu_\chi)$ of the kernel of χ^*:

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

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

$$G_\chi = \mathrm{Gal}(K_\chi/\boldsymbol{Q})$$

and let A_χ denote the l-class group of K_χ, which becomes a module over the group ring $\boldsymbol{Z}_l[G_\chi]$ in the obvious manner. Let $\widetilde{\chi}$ denote the rational irreducible character of G_χ such that, for each $\mathfrak{s} \in \mathrm{Gal}(\boldsymbol{Q}(\mu_\chi)/\boldsymbol{Q})$, the image under $\widetilde{\chi}$ of the restriction of $\mathfrak{s}$ to K_χ is the sum of $\chi^*(\mathfrak{s})^j$ for all positive integers $j \leq g_\chi$ relatively prime to g_χ. When l does not divide $g_\chi = [K_\chi : \boldsymbol{Q}]$, we can define an idempotent $\mathfrak{e}(\chi)$ of $\boldsymbol{Z}_l[G_\chi]$ by

$$\mathfrak{e}(\chi) = \frac{1}{g_\chi} \sum_{\sigma \in G_\chi} \widetilde{\chi}(\sigma^{-1})\sigma,$$

and $A_\chi^{\mathfrak{e}(\chi)} = \{\alpha^{\mathfrak{e}(\chi)} \mid \alpha \in A_\chi\}$ is the $\boldsymbol{Z}_l[G_\chi]$-submodule of A_χ consisting of all elements β of A_χ with $\beta^{\mathfrak{e}(\chi)} = \beta$. On the other hand, when χ is odd, i.e., $\chi(-1) = -1$, we put

$$h_\chi = \delta_\chi \prod_j \Bigl(-\frac{1}{2f_\chi} \sum_{a=1}^{f_\chi} \chi^j(a)a \Bigr).$$

Here, if f_χ is a power of an odd prime and $g_\chi = \varphi(f_\chi)$, then δ_χ denotes the prime divisor of f_χ; otherwise, δ_χ denotes 1; and j ranges over the positive integers $< g_\chi$ relatively prime to g_χ. In this case, $4h_\chi$ is known to be a positive integer, so that $h_\chi \in \boldsymbol{Z}_l \setminus \{0\}$ (cf. [**2**, Sections 27–33]). Furthermore, unless f_χ is a power of a prime number, h_χ itself is a positive integer since

$$-\frac{1}{2f_\chi} \sum_{a=1}^{f_\chi} \chi(a)a$$

is an algebraic integer (cf. [**2**, Section 28]).

Lemma 1. *Let χ be a Dirichlet character as above. Assume that χ is odd and $l \nmid g_\chi$. Then the order of $A_\chi^{\mathfrak{e}(\chi)}$ is equal to the l-part of h_χ, i.e., the highest power of l dividing h_χ.*

Proof. Let A_χ^- denote the kernel of the homomorphism $A_\chi \to A_{\chi^2}$ induced by the norm map from the ideal class group of K_χ to that of K_{χ^2}. Since K_{χ^2} is the maximal real subfield of K_χ, A_χ^- is none other than the Sylow l-subgroup of the relative class group of K_χ. Naturally A_χ^-, as well as A_{χ^u} for each positive divisor u of g_χ, becomes a $\boldsymbol{Z}_l[G_\chi]$-module. Let T be the set of positive odd divisors of g_χ. By the assumption $l \nmid g_\chi$, each $u \in T$ gives in $\boldsymbol{Z}_l[G_\chi]$ an idempotent $\mathfrak{e}_u = g_\chi^{-1} \sum_{\sigma \in G_\chi} \widetilde{\chi^u}(\sigma^{-1})\sigma$, A_χ^- is the direct product of its $\boldsymbol{Z}_l[G_\chi]$-submodules $A_\chi^{\mathfrak{e}_u}$ for all $u \in T$, and the natural map $A_{\chi^u} \to A_\chi$ for each $u \in T$ induces an isomorphism $A_{\chi^u}^{\mathfrak{e}(\chi^u)} = A_{\chi^u}^{\mathfrak{e}_u} \xrightarrow{\sim} A_\chi^{\mathfrak{e}_u}$ of $\boldsymbol{Z}_l[G_\chi]$-modules. We therefore obtain

$$\bigl|A_\chi^-\bigr| = \prod_{u \in T} \Bigl| A_{\chi^u}^{\mathfrak{e}(\chi^u)} \Bigr|.$$

The analytic class number formula implies, however, that $|A_\chi^-|$ coincides with the l-part of $\prod_{u\in T} h_{\chi^u}$; in fact, the relative class number of K_χ is equal to $2^b \prod_{u\in T} h_{\chi^u}$ for some positive integer b (cf. [**2**, Satz 34]). Thus we can prove the lemma by induction on g_χ. □

We denote by ω the Teichmüller character modulo l, namely, the odd Dirichlet character of order $l-1$ with conductor l such that, in Ω_l,

$$\omega(a) \equiv a \pmod{l} \qquad \text{for every } a \in \boldsymbol{Z}.$$

LEMMA 2. *Let n be a positive integer, and ψ a Dirichlet character of order p^n with conductor p^{n+1}. If $A_{\omega\psi^u}^{\mathfrak{e}(\omega\psi^u)}$ is trivial for every positive integer $u < p^n$ relatively prime to p, then $A_\psi^{\mathfrak{e}(\psi)}$ is trivial.*

PROOF. Let

$$\mathfrak{K} = K_\omega K_\psi = K_\psi(e^{2\pi i/l}),$$

and let $G_\mathfrak{K}$ denote the Galois group of the abelian extension $\mathfrak{K}/\boldsymbol{Q}$: $G_\mathfrak{K} = \mathrm{Gal}(\mathfrak{K}/\boldsymbol{Q})$. We take any Dirichlet character χ with $K_\chi \subseteq \mathfrak{K}$. The composite of the restriction map $G_\mathfrak{K} \to G_\chi$ and $\widetilde{\chi}$ defines a rational irreducible character of $G_\mathfrak{K}$, and an idempotent $\boldsymbol{e}(\chi)$ of $\boldsymbol{Z}_l[G_\mathfrak{K}]$ is defined by

$$\boldsymbol{e}(\chi) = \frac{1}{[\mathfrak{K}:\boldsymbol{Q}]} \sum_{\boldsymbol{s}\in G_\mathfrak{K}} \widetilde{\chi}(\boldsymbol{s}_\chi^{-1})\boldsymbol{s},$$

where $\boldsymbol{s}_\chi$ denotes the restriction of each $\boldsymbol{s} \in G_\mathfrak{K}$ to K_χ. Let $A_\mathfrak{K}$ denote the l-class group of $\mathfrak{K}$. We consider A_χ, as well as $A_\mathfrak{K}$, to be a $\boldsymbol{Z}_l[G_\mathfrak{K}]$-module in the obvious manner. Since $l \nmid [\mathfrak{K} : K_\chi]$, the natural map $A_\chi \to A_\mathfrak{K}$ induces an isomorphism $A_\chi^{\mathfrak{e}(\chi)} \xrightarrow{\sim} A_\mathfrak{K}^{\boldsymbol{e}(\chi)}$ of $\boldsymbol{Z}_l[G_\mathfrak{K}]$-modules. Noting that $l \nmid g_\chi$, let $\dot{\chi}$ denote the l-adic irreducible character of G_χ such that, for each $\mathfrak{s} \in \mathrm{Gal}(\boldsymbol{Q}(\mu_\chi)/\boldsymbol{Q})$, the image under $\dot{\chi}$ of the restriction of $\mathfrak{s}$ to K_χ is the sum of $\chi^*(\mathfrak{s})^{l^a}$ for all non-negative integers a smaller than the order of l modulo g_χ. We then define an idempotent $\boldsymbol{i}(\chi)$ of $\boldsymbol{Z}_l[G_\mathfrak{K}]$ by

$$\boldsymbol{i}(\chi) = \frac{1}{[\mathfrak{K}:\boldsymbol{Q}]} \sum_{\boldsymbol{s}\in G_\mathfrak{K}} \dot{\chi}(\boldsymbol{s}_\chi^{-1})\boldsymbol{s}.$$

It follows that $\boldsymbol{e}(\chi)\boldsymbol{i}(\chi) = \boldsymbol{i}(\chi)$ in $\boldsymbol{Z}_l[G_\mathfrak{K}]$.

Now, let H denote the set of positive integers $< p^n$ relatively prime to p. Assume that $A_{\omega\psi^u}^{\mathfrak{e}(\omega\psi^u)} = \{1\}$, i.e., $A_{\mathfrak{K}}^{\boldsymbol{e}(\omega\psi^u)} = \{1\}$ with any $u \in H$. Then $A_{\mathfrak{K}}^{\boldsymbol{i}(\omega\psi^u)} = A_{\mathfrak{K}}^{\boldsymbol{e}(\omega\psi^u)\boldsymbol{i}(\omega\psi^u)} = \{1\}$, while the reflection theorem (cf. [**8**, Section 3 Der Spigelungssatz]) implies that the rank of (the finite abelian l-group) $A_{\mathfrak{K}}^{\boldsymbol{i}(\psi^{-u})}$ does not exceed the rank of $A_{\mathfrak{K}}^{\boldsymbol{i}(\omega\psi^u)}$. We thus obtain $A_{\mathfrak{K}}^{\boldsymbol{i}(\psi^{-u})} = \{1\}$ for every $u \in H$. Furthermore, in $\boldsymbol{Z}_l[G_{\mathfrak{K}}]$, $\boldsymbol{e}(\psi) = \boldsymbol{e}(\psi^{-1})$ is the sum of all elements of $\{\boldsymbol{i}(\psi^{-u}) \mid u \in H\}$. Hence $A_{\mathfrak{K}}^{\boldsymbol{e}(\psi)} = \{1\}$, and consequently $A_{\psi}^{\mathfrak{e}(\psi)} = \{1\}$. □

By means of the lemmas proved above, let us give

Proof of Theorem 1. Take any Dirichlet character ψ of order p^n with conductor p^{n+1}. Then $K_\psi = \boldsymbol{B}_n$, $K_{\psi^p} = \boldsymbol{B}_{n-1}$, and the order of $A_{\psi}^{\mathfrak{e}(\psi)}$is the l-part of the integer h_n/h_{n-1}. The present proof therefore concludes if the triviality of $A_{\psi}^{\mathfrak{e}(\psi)}$ can be shown. On the other hand, Lemmas 1 and 2 show that $A_{\psi}^{\mathfrak{e}(\psi)} = \{1\}$ if l does not divide the integer $h_{\omega\psi'}$ for any Dirichlet character ψ' of order p^n with conductor p^{n+1}. Hence it suffices to prove that l does not divide

$$h_{\omega\psi} = \prod_{j} \biggl(-\frac{1}{2lp^{n+1}} \sum_{a=1}^{lp^{n+1}} \omega^j(a)\psi^j(a)a \biggr),$$

where j ranges over all positive integers $< (l-1)p^n/\gcd(l-1, p^n)$ relatively prime to $(l-1)p$. We put

$$\Theta = -\frac{1}{2lp^{n+1}} \sum_{a=1}^{lp^{n+1}} \omega^j(a)\psi^j(a)a, \quad \eta = \psi^j(1 + p^{n-\nu+1}),$$

with any positive integer j relatively prime to $(l-1)p$. Note that Θ is an algebraic integer in $\boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_n)$, and η is a primitive p^νth root of unity. We denote by $\mathfrak{T}$ the trace map from $\boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_n)$ to $\boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_\nu)$. Since $F \subseteq \boldsymbol{Q}(\xi_\nu)$, we have

$$\boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_\nu) \neq \boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_{\nu+1}),$$
$$\text{i.e.,} \ \bigl[\boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_n) : \boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_\nu)\bigr] = p^{n-\nu}.$$

Recalling that $n \geq 2\nu - 1$, let c range over the integers not divisible by p. Arguments in the first part of [**11**, Section **IV**] then teach us that

$$\mathfrak{T}(-\psi^{-j}(c)\Theta) = p^{n-\nu} \sum_{b\in R_{n-\nu}} \psi^{-j}(c)\psi^{j}(z_{n-\nu+1}(bc)) \times \sum_{r=0}^{l-1} \omega^{j}(z_{n-\nu+1}(bc) + p^{n-\nu+1}r) \frac{\eta^{z_\nu(b^{-1}c^{-1})r}}{\eta^{z_\nu(b^{-1}c^{-1})l} - 1}$$

(cf., in particular, [**11**, (**)]). Each $\psi^{-j}(c)\psi^{j}(z_{n-\nu+1}(bc))$ above is a p^νth root of unity, and an integer u with $\eta^u = \psi^{-j}(c)\psi^{j}(z_{n-\nu+1}(bc))$ satisfies

$$(z_{n+1}(c^{-1})z_{n-\nu+1}(bc))^{p-1} \equiv (1 + p^{n-\nu+1})^{(p-1)u} \pmod{p^{n+1}},$$

so that

$$(z_{n+1}(c^{-1})z_{n-\nu+1}(bc))^{p^\nu-1} \equiv (1 + p^{n-\nu+1})^{(p^\nu-1)u} \equiv 1 - p^{n-\nu+1}u \pmod{p^{n+1}},$$

and consequently

$$u \equiv w_{n-\nu,n+1}(b,c) \pmod{p^\nu}.$$

We thus obtain

$$\mathfrak{T}((1-\eta^l)\psi^{-j}(c)\Theta) = p^{n-\nu} \sum_{b\in R_{n-\nu}} \sum_{r=0}^{l-1} \omega^{j}(z_{n-\nu+1}(bc) + p^{n-\nu+1}r) \times \eta^{w_{n-\nu,n+1}(b,c)+z_\nu(b^{-1}c^{-1})r} \frac{\eta^l - 1}{\eta^{z_\nu(b^{-1}c^{-1})l} - 1}.$$

Furthermore we can take a prime ideal $\mathfrak{l}$ of $\boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_n)$ which divides l and $\omega(a) - a$ for all $a \in \boldsymbol{Z}$. Hence $\mathfrak{T}((1-\eta^l)\psi^{-j}(c)\Theta)$ is congruent to

$$p^{n-\nu} \sum_{b\in R_{n-\nu}} \sum_{a=0}^{z_\nu(bc)-1} \sum_{r=0}^{l-1} (z_{n-\nu+1}(bc) + p^{n-\nu+1}r)^{j_0} \eta^{z_\nu(b^{-1}c^{-1})(la+r)+w_{n-\nu,n+1}(b,c)}$$

modulo $\mathfrak{l}$ in $\boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_n)$, where j_0 denotes the least positive residue of j modulo $l-1$. It follows from the definition of ν, however, that every prime ideal of $\boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_\nu)$ dividing l remains prime in $\boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_n)$. Therefore, in view of the assumption of the theorem, $(1-\eta^l)\psi^{-j}(c)\Theta$ is not divisible by $\mathfrak{l}$ for some c, and hence Θ is not divisible by $\mathfrak{l}$. This fact implies that $\mathfrak{l}$ does not divide $h_{\omega\psi}$, namely, l does not divide $h_{\omega\psi}$. □

We successively proceed to

Proof of Theorem 3. Let ψ be any Dirichlet character of order p^n with conductor p^{n+1}. As in the proof of Theorem 1, put

$$\Theta = -\frac{1}{2lp^{n+1}} \sum_{a=1}^{lp^{n+1}} \omega^j(a)\psi^j(a)a, \quad \eta = \psi^j(1+p),$$

with any positive integer j relatively prime to $(l-1)p$. Then, for each $b \in \boldsymbol{Z}$ with $p \nmid b$, $\psi^j(b) = \eta^{y_n(b)}$ holds, because η is a primitive p^nth root of unity and an integer u with $\psi^j(b) = \eta^u$ satisfies $b^{p^n-1} \equiv (1+p)^{u(p^n-1)} \pmod{p^{n+1}}$. Let $\mathfrak{l}$ be a prime ideal of $\boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_n)$ dividing l and $\omega(a) - a$ for all $a \in \boldsymbol{Z}$. It follows from [**2**, Section 28, (3)] that

$$\Theta = \omega^j(p^{n+1})\psi^j(l) \sum_{r=1}^{(l-1)/2} \sum_{b \in H_n(r)} \omega^j(r)\psi^j(b).$$

Thus, in $\boldsymbol{Q}(e^{2\pi i/(l-1)}, \xi_n)$,

$$\Theta \equiv \omega^j(p^{n+1})\psi^j(l) \sum_{r=1}^{(l-1)/2} \sum_{b \in H_n(r)} r^j \eta^{y_n(b)} \pmod{\mathfrak{l}}.$$

Hence, by the hypothesis of the theorem, Θ is relatively prime to $\mathfrak{l}$ and, consequently, l does not divide $h_{\omega\psi}$. Lemmas 1 and 2 therefore show that $A_{\psi}^{\mathfrak{e}(\psi)}$ is trivial, namely, l does not divide h_n/h_{n-1}. □

3. Supplementary results.

We add a simple result supplementary to Theorem 2.

Lemma 3.

$$M < \left(\frac{(p-1)l|S^*|}{2}\right)^{\varphi(p-1)}.$$

Proof. Take any $\kappa \in \Phi$. Then

$$\left|\mathfrak{N}\left(\sum_{\varepsilon \in V} \kappa(\varepsilon)\varepsilon - 1\right)\right| = \prod_{\rho} \left|\sum_{\varepsilon \in V} \kappa(\varepsilon)\varepsilon^{\rho} - 1\right|,$$

with ρ ranging over all automorphisms of $\boldsymbol{Q}(e^{2\pi i/(p-1)})$, and

$$\left|\sum_{\varepsilon\in V}\kappa(\varepsilon)\varepsilon^{\rho}-1\right|\le|\kappa(1)-1|+\sum_{\varepsilon\in V\setminus\{1\}}\kappa(\varepsilon)<\frac{p-1}{2}\cdot l|S^*|.$$

Therefore

$$\left|\mathfrak{N}\left(\sum_{\varepsilon\in V}\kappa(\varepsilon)\varepsilon-1\right)\right|<\left(\frac{(p-1)l|S^*|}{2}\right)^{\varphi(p-1)}. \qquad \square$$

Now, let us consider the case $\nu=1$. We put $d=[F:\boldsymbol{Q}]$ for simplicity. It follows that $(p-1)/d$ is the order of l modulo p. Let χ be any Dirichlet character of order d with conductor dividing p : $g_\chi=d$, $f_\chi\mid p$. Let $\zeta=e^{2\pi i/d}$ and, for each non-negative integer $j<d$, let θ_j denote the sum of ξ_1^m for all positive integers $m<p$ with $\chi(m)=\zeta^j$, so that $\theta_j\in\mathfrak{O}$. Further, let I denote the set of non-negative integers less than d and other than $d/2$. By the fact that $\xi_1,\xi_1^2,\dots,\xi_1^{p-1}$ form a normal integral basis of $\boldsymbol{Q}(\xi_1)/\boldsymbol{Q}$, we see that $\theta_0,\dots,\theta_{d-1}$ form a normal integral basis of $F/\boldsymbol{Q}$. As $\theta_0+\cdots+\theta_{d-1}=-1$, (the additive group of) $\mathfrak{O}$ is a free $\boldsymbol{Z}$-module over $\{1,\theta_1,\dots,\theta_{d-1}\}$ and, when $\chi(-1)=-1$, d is even and $\mathfrak{O}$ is a free $\boldsymbol{Z}$-module over $\{1\}\cup\{\theta_j\mid j\in I\}$. In particular, we have

$$S=\{m\in\boldsymbol{Z}\mid 0\le m\le p-2,\ \chi(m)\ne\chi(-1)\}.$$

This implies that

$$|S|=1+(d-1)\frac{p-1}{d}=p-\frac{p-1}{d}.$$

LEMMA 4. *If $\nu=1$, then*

$$|S^*|=p+1-\frac{p-1}{[F:\boldsymbol{Q}]}=|S|+1.$$

PROOF. Assuming that $\nu=1$, we let $d=[F:\boldsymbol{Q}]$ and $\zeta=e^{2\pi i/d}$ as before. Obviously, $S^*=\{0,1\}$ if $F=\boldsymbol{Q}$; so we also assume $d>1$. Let χ be any Dirichlet character of order d with conductor p. For any non-negative integer $j<d$, define N_j to be the number of positive integers $m\le p-2$ which satisfy

$$\chi(m)=\chi(m+1)=\zeta^j.$$

Then

$$N_j = \sum_{m=1}^{p-2} \left(\frac{1}{d} \sum_{a=0}^{d-1} \chi^a(m)\zeta^{-ja} \right) \left(\frac{1}{d} \sum_{b=0}^{d-1} \chi^b(m+1)\zeta^{-jb} \right)$$
$$= \frac{1}{d^2} \Biggl(p - 2 + \sum_{a=1}^{d-1} \zeta^{-ja} \sum_{m=1}^{p-2} \chi^a(m) + \sum_{b=1}^{d-1} \zeta^{-jb} \sum_{m=1}^{p-2} \chi^b(m+1)$$
$$+ \sum_{b=1}^{d-1} \zeta^{-j(d-b)-jb} \sum_{m=1}^{p-2} \chi^{d-b}(m)\chi^b(m+1) + \sum_{(a,b)\in W} \zeta^{-ja-jb} J_{a,b} \Biggr),$$

where W denotes the set of pairs (a, b) of positive integers less than d with $a+b \neq d$, and

$$J_{a,b} = \sum_{m=1}^{p-2} \chi^a(m)\chi^b(m+1) \qquad \text{for each } (a,b) \in W.$$

Since

$$\sum_{m=1}^{p-2} \chi^a(m) = -\chi^a(-1), \quad \sum_{m=1}^{p-2} \chi^b(m+1) = -1,$$
$$\sum_{m=1}^{p-2} \chi^{d-b}(m)\chi^b(m+1) = \sum_{m=1}^{p-2} \chi^b(z_1(m^{-1})+1) = -1$$

in the above, it follows that

$$N_j = \frac{1}{d^2} \left(p - d - 1 - \sum_{a=1}^{d-1} \chi^a(-1)\zeta^{-ja} - \sum_{b=1}^{d-1} \zeta^{-jb} + \sum_{(a,b)\in W} \zeta^{-j(a+b)} J_{a,b} \right).$$

Therefore we eventually obtain

$$\sum_{j=0}^{d-1} N_j = \frac{p-d-1}{d}. \tag{1}$$

Let us recall that Γ is a cyclic group of order p generated by γ. For each non-negative integer $j < d$, we denote by γ_j the sum of γ^m, in $\boldsymbol{Z}[\Gamma]$, for all positive integers $m \leq p-2$ with $\chi(m) = \zeta^j$. Meanwhile, for each positive integer $m < p$, we denote by $\iota(m)$ the non-negative integer less than d such that $\chi(m) = \zeta^{\iota(m)}$.

Suppose now that $\chi(-1) = 1$. As already seen,

$$\mathfrak{O} = \boldsymbol{Z} \oplus \boldsymbol{Z}\theta_1 \oplus \cdots \oplus \boldsymbol{Z}\theta_{d-1}.$$

Given arbitrary integers s, $t_1, \dots, t_{d-1}$, take the integers $c_0, \dots, c_{p-1}$ satisfying

$$c_0 + c_1\gamma + \cdots + c_{p-1}\gamma^{p-1} = (1-\gamma)\left(s + \sum_{j=1}^{d-1} t_j \gamma_j\right).$$

Then $c_0 = s$, $c_1 = -s$, and for any positive integer $m \leq p-2$,

$$c_{m+1} = \begin{cases} t_{\iota(m+1)} - t_{\iota(m)} & \text{if } \chi(m) \neq 1,\ \chi(m+1) \neq 1; \\ t_{\iota(m+1)} & \text{if } \chi(m) = 1,\ \chi(m+1) \neq 1; \\ -t_{\iota(m)} & \text{if } \chi(m) \neq 1,\ \chi(m+1) = 1; \\ 0 & \text{if } \chi(m) = \chi(m+1) = 1. \end{cases}$$

We therefore find that

$$|S^*| = p - \sum_{j=0}^{d-1} N_j.$$

Hence (1) yields

$$|S^*| = p - \frac{p-d-1}{d} = p + 1 - \frac{p-1}{d}.$$

We next suppose that $\chi(-1) = -1$. In this case, $2 \mid d$ and

$$\mathfrak{O} = \boldsymbol{Z} \oplus \left(\bigoplus_{j \in I} \boldsymbol{Z}\theta_j\right)$$

as already seen. Similarly to the case $\chi(-1) = 1$, let s be any integer and let t_j be any integer for each $j \in I$. Take the integers $c'_0, \dots, c'_{p-1}$ satisfying

$$c'_0 + c'_1\gamma + \cdots + c'_{p-1}\gamma^{p-1} = (1-\gamma)\left(s + \sum_{j \in I} t_j \gamma_j\right).$$

Then $c_0' = s$, $c_1' = t_0 - s$, and for any positive integer $m \le p-2$,

$$c'_{m+1} = \begin{cases} t_{\iota(m+1)} - t_{\iota(m)} & \text{if } \chi(m) \neq -1,\ \chi(m+1) \neq -1; \\ t_{\iota(m+1)} & \text{if } \chi(m) = -1,\ \chi(m+1) \neq -1; \\ -t_{\iota(m)} & \text{if } \chi(m) \neq -1,\ \chi(m+1) = -1; \\ 0 & \text{if } \chi(m) = \chi(m+1) = -1. \end{cases}$$

Hence

$$|S^*| = p - \sum_{j=0}^{d-1} N_j$$

again so that, by (1),

$$|S^*| = p + 1 - \frac{p-1}{d}. \qquad \square$$

4. Computational results.

Let s_0 be the least positive primitive root modulo p^2. Let us take as R $(= R_0)$ the set of $z_1(s_0^u)$ for all non-negative integers $u \le (p-3)/2$. Given any integer $n \ge 2\nu - 1$, any positive integer $j \le l-2$ relatively prime to $l-1$, and any integer c with $p \nmid c$, we define

$$P_{n,j,c}(X) = \sum_{b \in R_{n-\nu}} \sum_{a=0}^{z_\nu(bc)-1} \sum_{r=0}^{l-1} (z_{n-\nu+1}(bc) + p^{n-\nu+1} r)^j X^{z_\nu(b^{-1}c^{-1})(la+r) + w_{n-\nu,n+1}(b,c)}$$

in $(\boldsymbol{Z}/l\boldsymbol{Z})[X]$, the polynomial ring in an indeterminate X over the residue field $\boldsymbol{Z}/l\boldsymbol{Z}$. Here, for each pair (m,u) of integers with $u \ge 0$, we understand that mX^u denotes the monomial in X of degree u with coefficient the class of m in $\boldsymbol{Z}/l\boldsymbol{Z}$ or denotes the zero element of $(\boldsymbol{Z}/l\boldsymbol{Z})[X]$ according to whether $l \nmid m$ or $l \mid m$. Note also that $R_{n-\nu}$ is the set of $z_{n-\nu+1}(s_0^{p^{n-\nu}u})$ for all non-negative integers $u \le (p-3)/2$. We denote by $Q_{n,j,c}(X)$ the greatest common divisor of $P_{n,j,c}(X)$ and the p^νth cyclotomic polynomial in $(\boldsymbol{Z}/l\boldsymbol{Z})[X]$, with the leading coefficient of $Q_{n,j,c}(X)$ assumed to be the unity element of $\boldsymbol{Z}/l\boldsymbol{Z}$:

$$Q_{n,j,c}(X) = \gcd\left(P_{n,j,c}(X),\ \sum_{u=0}^{p-1} X^{p^{\nu-1}u}\right).$$

Since $\boldsymbol{Z}[\xi_\nu]$ is the ring of algebraic integers of $\boldsymbol{Q}(\xi_\nu)$, it then follows that

$$\sum_{b\in R_{n-\nu}} \sum_{a=0}^{z_\nu(bc)-1} \sum_{r=0}^{l-1} (z_{n-\nu+1}(bc) + p^{n-\nu+1}r)^j \xi_\nu^{z_\nu(b^{-1}c^{-1})(la+r)+w_{n-\nu,n+1}(b,c)}$$

is relatively prime to l if and only if

$$Q_{n,j,c}(X) = 1.$$

We keep this fact in mind from now on. To do most of calculations stated below, such as the calculation of each $Q_{n,j,c}(X)$ in question, we have used *Mathematica* on a personal computer.

First of all, let us deal with the case where $(l,p) \in \{(3,11),(7,5),(11,71)\}$ so that $\nu = 2$. Let j be any positive integer $\le l-2$ relatively prime to $l-1$, and let n be an integer not smaller than $2\nu - 1 = 3$. As $|S^*| \le p^2$, the condition $p^{n-\nu+1} \le M$ implies by Lemma 3 that

$$p^{n-1} < \left(\frac{l(p-1)p^2}{2}\right)^{\varphi(p-1)}, \quad \text{i.e.,} \quad n < \frac{\varphi(p-1)\log(l(p-1)/2)}{\log p} + 2\varphi(p-1) + 1.$$

Furthermore, we have checked that

$$Q_{n,j,1}(X) = 1, \quad \text{when } 3 \le n < \frac{\varphi(p-1)\log(l(p-1)/2)}{\log p} + 2\varphi(p-1) + 1. \tag{2}$$

Now, let m be 1 or 2. Then, in $(\boldsymbol{Z}/l\boldsymbol{Z})[X]$, we have

$$\gcd\left(\sum_{r=1}^{(l-1)/2} \sum_{a\in H_m(r)} r^j X^{y_m(a)},\ \sum_{u=0}^{p-1} X^{p^{m-1}u}\right) = 1,$$

namely, $\sum_{r=1}^{(l-1)/2} \sum_{a\in H_m(r)} r^j \xi_m^{y_m(a)}$ is relatively prime to l. Hence, by Theorem 3, l does not divide h_m/h_{m-1}. This implies $l \nmid h_2$, since $h_0 = 1$. Theorem 2 for $n_0 = 2$, together with (2), thus proves the following

LEMMA 5. *The l-class group of $\boldsymbol{B}_\infty$ is trivial if (l,p) is either $(3,11)$, $(7,5)$*

or $(11, 71)$.

In the rest of this section, we let n range over all positive integers less than

$$\frac{\varphi(p-1)}{\log p}\log\left(\frac{l(p-1)}{2}\left(p+1-\frac{p-1}{[F:\boldsymbol{Q}]}\right)\right),$$

i.e., all positive integers such that

$$p^n < \left(\frac{l(p-1)}{2}\left(p+1-\frac{p-1}{[F:\boldsymbol{Q}]}\right)\right)^{\varphi(p-1)}.$$

Suppose now that $l=3$, $p \le 173$, $p \ne 11$ and so $\nu = 1$. Then we can check not only that $Q_{n,1,1}(X) = 1$ if $(p,n) \notin \{(13,3),(13,4),(13,5)\}$ but that, in the case $p=13$,

$$Q_{3,1,2}(X) = Q_{4,1,4}(X) = Q_{5,1,2}(X) = 1.$$

Hence Theorem 2 for $n_0 = 0$ combined with Lemmas 3 and 4 shows the triviality of the 3-class group of $\boldsymbol{B}_\infty$. Therefore, by Lemma 5, we have

Proposition 1. *If $p \le 173$, then the 3-class group of $\boldsymbol{B}_\infty$ is trivial.*

Remark 1. In the case $(l,p) = (3,13)$,

$$Q_{3,1,1}(X) = X^3 + X^2 + X + 2, \qquad Q_{4,1,1}(X) = X^3 + 2X + 2,$$
$$Q_{4,1,2}(X) = X^6 + 2X^4 + 2X^3 + 2X^2 + 1, \qquad Q_{4,1,3}(X) = X^3 + 2X^2 + 2X + 2,$$
$$Q_{5,1,1}(X) = X^3 + 2X^2 + 2X + 2.$$

Suppose next that $l=5$, $p \le 137$, and hence $\nu = 1$. We then have $Q_{n,1,1}(X) = 1$ unless $(p,n) = (71,35)$; we also have $Q_{n,3,1}(X) = 1$ unless $(p,n) = (31,4)$ or $(p,n) = (31,5)$. Furthermore,

$$Q_{35,1,2}(X) = 1 \qquad \text{when } p = 71;$$
$$Q_{4,3,2}(X) = Q_{5,3,2}(X) = 1 \qquad \text{when } p = 31.$$

Therefore Theorem 2 for $n_0 = 0$, together with Lemmas 3 and 4, gives the following result.

PROPOSITION 2. *If $p \leq 137$, then the 5-class group of $\boldsymbol{B}_\infty$ is trivial.*

REMARK 2. When $(l, p) = (5, 71)$,

$$Q_{35,1,1}(X) = X^5 + 3X^4 + 3X^3 + 2X^2 + 4X + 4;$$

when $(l, p) = (5, 31)$,

$$Q_{4,3,1}(X) = X^3 + 2X^2 + 4X + 4, \quad Q_{5,3,1}(X) = X^3 + X^2 + X + 4.$$

Assume that $l = 7$ and $p \leq 131$. To see the triviality of the 7-class group of $\boldsymbol{B}_\infty$, we may also assume by Lemma 5 that $p \neq 5$ so that $\nu = 1$. We then have $Q_{n,1,1}(X) = 1$; further, unless $(p, n) = (3, 1)$, we have $Q_{n,5,1}(X) = 1$. In the case $p = 3$, it is well known that $h_1 = 1$. Therefore, letting $n_0 = 0$ or $n_0 = 1$ in Theorem 2 according to whether $p > 3$ or $p = 3$, we obtain the following result from the theorem, Lemma 3, and Lemma 4.

PROPOSITION 3. *If $p \leq 131$, then the 7-class group of $\boldsymbol{B}_\infty$ is trivial.*

REMARK 3. In the case $(l, p) = (7, 3)$, one has $\{h_{\omega\psi}, h_{\omega\psi^2}\} = \{1, 7\}$ for a Dirichlet character ψ of order 3 with conductor 9 (cf. [**2**, Tafel II, p. 168]), whence the proofs of Theorems 1 and 3 tell us that neither of the hypotheses of the theorems is satisfied for $n = 1$.

Assume that $l = 11$ and $p \leq 109$. Let us prove the triviality of the 11-class group of $\boldsymbol{B}_\infty$. By Lemma 5, we may further assume that $p \neq 71$ so that $\nu = 1$. We let j range over the integers in $\{1, 3, 7, 9\}$. Unless $(p, n, j) = (5, 1, 9)$, our computations show that $Q_{n,j,c}(X) = 1$ for some $c \in \boldsymbol{Z}$ with $p \nmid c$. Precise results are as follows: $Q_{n,j,1}(X) = 1$ unless

$$(p, n, j) \in \{(5, 4, 1), (5, 2, 3), (5, 3, 3), (5, 2, 7), (5, 5, 7), (5, 1, 9), (5, 4, 9)\};$$

and, when $p = 5$,

$$Q_{4,1,1}(X) = X^2 + 9X + 3, \quad Q_{4,1,2}(X) = 1, \quad Q_{2,3,1}(X) = X + 7,$$
$$Q_{2,3,2}(X) = 1, \quad Q_{3,3,1}(X) = Q_{3,3,2}(X) = Q_{3,3,3}(X) = X + 2, \quad Q_{3,3,4}(X) = 1,$$
$$Q_{2,7,1}(X) = X + 6, \quad Q_{2,7,2}(X) = 1, \quad Q_{5,7,1}(X) = X + 6, \quad Q_{5,7,2}(X) = 1,$$
$$Q_{4,9,1}(X) = X + 8, \quad Q_{4,9,2}(X) = X + 6, \quad Q_{4,9,3}(X) = X^2 + 4X + 1,$$
$$Q_{4,9,4}(X) = X^2 + 8X + 1, \quad Q_{4,9,6}(X) = 1.$$

It is also known that $h_1 = 1$ when $p = 5$ (cf. Bauer [**1**], Masley [**9**]). Therefore, once we set $n_0 = 0$ or $n_0 = 1$ in Theorem 2 according as $p \neq 5$ or $p = 5$, the following result is deduced from the theorem, Lemma 3, and Lemma 4.

Proposition 4. *If $p \leq 109$, then the 11-class group of $\boldsymbol{B}_\infty$ is trivial.*

Remark 4. In the case $(l, p) = (11, 5)$, the relative class numbers of just two fields in $\{K_{\omega\psi}, K_{\omega\psi^2}, K_{\omega\psi^3}, K_{\omega\psi^4}\}$ are equal to 55 for a Dirichlet character ψ of order 11 with conductor 121 (cf. Schrutka von Rechtenstamm [**10**, p. 45]) so that neither of the hypotheses of Theorems 1 and 3 is satisfied for $n = 1$.

Assume finally that $l = 13$, $p \leq 101$, and hence $\nu = 1$. Let j vary through $\{1, 5, 7, 11\}$. Then $Q_{n,j,1}(X) = 1$ except that $Q_{3,5,1}(X) = X^2 + X + 1$ in the case $p = 3$. Furthermore, when $p = 3$, we have $Q_{3,5,2}(X) = 1$. Therefore Theorem 2, together with Lemmas 3 and 4, gives

Proposition 5. *If $p \leq 101$, then the 13-class group of $\boldsymbol{B}_\infty$ is trivial.*

Still for several cases of (l, p) not treated in this section, the triviality of the l-class group of $\boldsymbol{B}_\infty$ can be verified along the same lines as we have discussed it so far, but we omit the details here.

References

[1] H. Bauer, Numerische Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper, J. Number Theory, **1** (1969), 161–162.

[2] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952; Springer-Verlag, Berlin, 1985.

[3] K. Horie and M. Horie, The narrow class groups of some $\boldsymbol{Z}_p$-extensions over the rationals, Acta Arith., **135** (2008), 159–180.

[4] K. Horie and M. Horie, The ideal class group of the $\boldsymbol{Z}_p$-extension over the rationals, Tohoku Math. J., **61** (2009), 551–570.

[5] K. Horie and M. Horie, On the narrow class groups of the $\boldsymbol{Z}_p$-extensions over $\boldsymbol{Q}$ for several primes p, In: Proceedings of the workshop on Number Theory 2010 (eds. K. Hashimoto and K. Komatsu), Institute of Pure and Applied Mathematics, Waseda University, 2010, pp. 17–26.

[6] H. Ichimura and S. Nakajima, On the 2-part of the ideal class group of the cyclotomic $\boldsymbol{Z}_p$-extension over the rationals, Abh. Math. Sem. Univ. Hamburg, **80** (2010), 175–182.

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

[8] H. W. Leopoldt, Zur Struktur der l-Klassengruppe galoisscher Zahlkörper, J. reine angew. Math., **199** (1958), 165–174.

[9] J. Masley, Class numbers of real cyclic number fields with small conductor, Comp. Math., **37** (1978), 297–319.

[10] G. Schrutka von Rechtenstamm, Tabelle der (Relativ)-Klassenzahlen der Kreiskörper, deren ϕ-Funktion des Wurzelexponenten (Grad) nicht grösser als 256 ist, Abh. Deutschen

Akad. Wiss. Berlin, Kl. Math. Phys., no. 2 (1964), 1–64.
[11] L. C. Washington, Class numbers and $\boldsymbol{Z}_p$-extensions, Math. Ann., **214** (1975), 177–193.

Kuniaki Horie
3-9-2-302 Sengoku, Bunkyo-ku
Tokyo 112-0011, Japan

Mitsuko Horie
Department of Mathematics
Ochanomizu University
2-1-1 Otsuka, Bunkyo-ku
Tokyo 112-8610, Japan
E-mail: horie.mitsuko@ocha.ac.jp