The ideal class group of the $\boldsymbol{Z}_{23}$-extension over the rational field

By Kuniaki HORIE[*] and Mitsuko HORIE[**),†]

(Communicated by Masaki KASHIWARA, M.J.A., Nov. 12, 2009)

Abstract: Given any prime number l which is a primitive root modulo 529 $(= 23^2)$, we shall prove that the l-class group of the $\boldsymbol{Z}_{23}$-extension over the rational field is trivial.

Key words: $\boldsymbol{Z}_{23}$-extension; ideal class group; Iwasawa theory.

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 $\boldsymbol{Q}$ (contained in the complex field). The p-class group of $\boldsymbol{B}_\infty$ is known to be trivial (cf. Iwasawa [5]). Let l be a prime number different from p. We have shown in [1–4], through arithmetic study of the analytic class number formula, that the l-class group of $\boldsymbol{B}_\infty$ is trivial if l is a primitive root modulo p^2 and if

$$p \le 19 \quad \text{or} \quad l > \frac{3}{2}(p-1)\varphi(p-1)\log_2(p\log p);$$

here φ denotes the Euler function and, for each real number $r > 0$, $\log_2 r = (\log r)/\log 2$ as usual. In this paper, we shall prove the following result by means of some results in [1–3] with the help of a personal computer.

Theorem. *If $p = 23$ and l is a primitive root modulo 23^2, then the l-class group of $\boldsymbol{B}_\infty$ is trivial.*

Remark. The condition that l is a primitive root modulo 23^2 means that l is congruent modulo 23 to some integer in $\{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}$ and is not congruent modulo 529 to any integer in $\{28, 42, 63, 130, 195, 263, 274, 352, 359, 411\}$.

We have used *Mathematica* for our calculations by computer.

1. To begin with, we give lemmas helpful for the computations in the proof of our theorem. Let the notations p and l be as before, except that we assume $l > 2$. For each integer $m \ge 0$, let $\boldsymbol{B}_m$ denote the subfield of $\boldsymbol{B}_\infty$ with degree p^m, and h_m the class number of $\boldsymbol{B}_m$. Let n be any positive integer. Since the prime ideal of $\boldsymbol{B}_{n-1}$ dividing p is totally ramified in $\boldsymbol{B}_n$, class field theory shows that h_{n-1} divides h_n, i.e., h_n/h_{n-1} is an integer. The notation n, as well as p and l, will be used henceforth.

Now, let ν be the number of distinct prime divisors of $(p-1)/2$, and let $g_1, \ldots, g_\nu$ be the prime-powers > 1 pairwise relatively prime such that

$$\frac{p-1}{2} = g_1 \cdots g_\nu.$$

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

$$e^{\pi i m_1/g_1} \cdots e^{\pi i m_\nu/g_\nu}$$

for all ν-tuples $(m_1, \ldots, m_\nu)$ of integers with $0 \le m_1 < g_1, \ldots, 0 \le m_\nu < g_\nu$. It is naturally understood that $V = \{1\}$ if $p = 3$. Let Φ denote the set of maps

$$z : V \to \{0, \ldots, 2l\}$$

such that $l \nmid z(\xi)$ for some $\xi \in V$ and $l \mid z(\xi')$ for all $\xi' \in V \setminus \{\xi\}$. We put

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

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

Next, 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 $a < p^{n+1}$ for which $a \equiv \xi \pmod{\mathfrak{p}^{n+1}}$ with some $\xi \in V$. Since $\mathfrak{p}$ is of degree 1 over $\boldsymbol{Q}$ and since no pair (ξ_1, ξ_2) of distinct elements of V satisfies $\xi_1 - \xi_2 \in \mathfrak{p}$, each $\xi \in V$ gives a unique $a \in I$ congruent to ξ modulo $\mathfrak{p}^{n+1}$ and the map $\xi \mapsto a$ defines a bijection from V to I. We note that I contains 1. Let $\hat{I}$ denote the set of all maps from I to the ring $\boldsymbol{Z}$ of (rational) integers, so that $\hat{I}$ is regarded as a module in the usual manner. Let $\mathfrak{F}$ denote the set of maps j in $\hat{I}$ with $j(I) \subseteq \{0, l\}$ and, for each $a \in I$, let $\mathfrak{G}_a$ denote the set of maps j in $\hat{I}$ such that

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

*) Department of Mathematics, Tokai University, 1117, Kitakaname, Hiratsuka, Kanagawa 259-1292, Japan.

**) Department of Mathematics, Ochanomiz University, 2-1-1, Otsuka, Bunkyo-ku, Tokyo 112-8610, Japan.

†) Corresponding author.

doi: 10.3792/pjaa.85.155

$0 < j(a) < l$ and that $j(b) = 0$ or $j(b) = l$ for every $b \in I \setminus \{a\}$. Given any $m \in \boldsymbol{Z}$, we then define $\mathcal{P}_a(m)$ to be the set of $(j, y) \in \mathfrak{G}_a \times \mathfrak{F}$ satisfying

$$\sum_{b \in I}((p^n + 1)j(b) + y(b))b \equiv m \pmod{p^{n+1}};$$

further, we define $\mathcal{Q}_a(m)$ to be the set of $(j, y) \in \mathfrak{F} \times \mathfrak{G}_a$ satisfying

$$\sum_{b \in I}((p^n + 1)j(b) + y(b))b \equiv m \pmod{p^{n+1}}.$$

We also put

$$s(m) = \sum_{a \in I}\left(\sum_{(j,y) \in \mathcal{Q}_a(m)} (-1)^{y(a)+\sum_{b \in I}(j(b)+y(b))}\widetilde{y(a)} - \sum_{(j,y) \in \mathcal{P}_a(m)} (-1)^{j(a)+\sum_{b \in I}(j(b)+y(b))}\widetilde{j(a)}\right);$$

here, for each integer c relatively prime to l, $\tilde{c}$ denotes the positive integer smaller than l such that $c\tilde{c} \equiv 1 \pmod{l}$. For each $a \in I$, let $\mathfrak{H}_a$ denote the set of maps f in $\hat{I}$ satisfying

$$f(a) \in \{1, \ldots, 2l - 1\} \setminus \{l\}, \quad f(I \setminus \{a\}) \subseteq \{0, l, 2l\}.$$

Every pair (j, y) in $(\mathfrak{G}_a \times \mathfrak{F}) \cup (\mathfrak{F} \times \mathfrak{G}_a)$ then gives a map $j + y$ in $\mathfrak{H}_a$. We put

$$\mathcal{R}(m) = \bigcup_{a \in I}(\mathcal{P}_a(m) \cup \mathcal{Q}_a(m)),$$

$$\mathfrak{H}(m) = \left\{ f \in \bigcup_{a \in I}\mathfrak{H}_a \,\middle|\, \sum_{b \in I} f(b)b \equiv m \pmod{p^n} \right\},$$

so that every (j, y) in $\mathcal{R}(m)$ satisfies $j + y \in \mathfrak{H}(m)$. We denote by ψ_m the map in $\hat{I}$ such that $\psi_m(1) = m$ and that $\psi_m(a) = 0$ for all a in $I \setminus \{1\}$. Obviously, $\psi_m \in \mathfrak{H}(m)$ when $m \in \{1, \ldots, 2l - 1\} \setminus \{l\}$. On the other hand, $\psi_m = 0$ in $\hat{I}$ when $m = 0$.

Lemma 1. *Let n_0 be any positive integer, and u an integer in $\{1, \ldots, 2l - 1\} \setminus \{l\}$. Then the following statements are equivalent.*
(i) $\mathfrak{H}(u) = \{\psi_u\}$ *in the case* $n = n_0$;
(ii) $\mathfrak{H}(u) = \{\psi_u\}$ *whenever* $n \geq n_0$.

Proof. This follows immediately from the definitions of I and $\mathfrak{H}(u)$. □

Lemma 2. *Let u be an integer in $\{1, \ldots, 2l - 1\} \setminus \{l\}$ such that $p \nmid u$ or $p \nmid 2l - u$ according to whether $u < l$ or $u > l$. Assume that $\mathfrak{H}(u) = \{\psi_u\}$. Then l does not divide $h_{n'}/h_{n'-1}$ for any integer $n' \geq n$.*

Proof. By Lemma 1, it suffices to prove that l does not divide h_n/h_{n-1}. Let us first consider the case $u < l$. We take any (j, y) in $\mathcal{R}(u)$ and any (j', y') in $\mathcal{R}(u + up^n)$. It follows that not only $j + y$ but also $j' + y'$ belongs to $\mathfrak{H}(u)$. Hence, by the assumption $\mathfrak{H}(u) = \{\psi_u\}$,

$$j(1) + y(1) = u, \quad j'(1) + y'(1) = u,$$

and, for each $b \in I \setminus \{1\}$,

$$j(b) = y(b) = j'(b) = y'(b) = 0.$$

Furthermore, neither of the equalities

$$(j(1), y(1)) = (u, 0), \quad (j'(1), y'(1)) = (0, u)$$

holds, because u is not divisible by p. We thus obtain

$$(j, y) = (0, \psi_u), \quad (j', y') = (\psi_u, 0).$$

These mean that

$$\mathcal{R}(u) = \mathcal{Q}_1(u) = \{(0, \psi_u)\},$$

$$\mathcal{R}(u + up^n) = \mathcal{P}_1(u + up^n) = \{(\psi_u, 0)\}.$$

In particular,

$$s(u) = \tilde{u}, \quad s(u + up^n) = -\tilde{u}.$$

Since l does not divide $2\tilde{u} = s(u) - s(u + up^n)$, we then see from [3, Lemma 2] (or [2, Lemma 3]) that l does not divide h_n/h_{n-1}.

In the case $u > l$, taking any (j, y) in $\mathcal{R}(u + lp^n)$ and any (j', y') in $\mathcal{R}(u + (u - l)p^n)$, we have by the hypothesis

$$(j, y) = (\psi_l, \psi_{u-l}), \quad (j', y') = (\psi_{u-l}, \psi_l),$$

similarly to the above, and hence we have successively

$$\mathcal{R}(u + lp^n) = \mathcal{Q}_1(u + lp^n) = \{(\psi_l, \psi_{u-l})\},$$

$$\mathcal{R}(u + (u - l)p^n) = \mathcal{P}_1(u + (u - l)p^n) = \{(\psi_{u-l}, \psi_l)\},$$

$$s(u + lp^n) = -\tilde{u}, \quad s(u + (u - l)p^n) = \tilde{u}.$$

It therefore follows again from [3, Lemma 2] that l does not divide h_n/h_{n-1}. □

2. Assume now that p is 23 and l a primitive root modulo 529. In the rest of the paper, we are devoted to the proof of the theorem already stated.

Let $\rho = e^{\pi i/11}$, so that

$$V = \{\rho^0 = 1, \ldots, \rho^{10}\}, \quad \rho^{11} = -1.$$

We take any $z \in \Phi$ and put

$$\alpha = \sum_{\xi \in V} z(\xi)\xi - 1 = \sum_{m=0}^{10} \rho^m w_m,$$

where $w_0 = z(1) - 1$, $w_1 = z(\rho), \ldots, w_{10} = z(\rho^{10})$. We further put

$$W_c = \sum_{m=c}^{10} w_m w_{m-c} - \sum_{m=0}^{c-1} w_{m+11-c} w_m$$

for each $c \in \{1, \ldots, 5\}$. Let σ be any automorphism of $\boldsymbol{Q}(\rho)$. It follows that

$$\begin{aligned}
|\sigma(\alpha)|^2 &= \left(\sum_{m=0}^{10} \sigma(\rho)^m w_m\right)\left(\sum_{m=0}^{10} \sigma(\rho)^{-m} w_m\right) \\
&= \sum_{c=1}^{10} (\sigma(\rho)^c + \sigma(\rho)^{-c}) \sum_{m=c}^{10} w_m w_{m-c} + \sum_{m=0}^{10} w_m^2 \\
&= \sum_{c=1}^{5} (\sigma(\rho)^c + \sigma(\rho)^{-c}) W_c + \sum_{m=0}^{10} w_m^2.
\end{aligned}$$

In view of the above expansion and the simple fact that, for real constants r_1 and r_2, the function $x^2 + r_1 x + r_2$ of a real variable x defined on a closed interval takes its maximum at an endpoint of the interval, we find that if the real function

$$\left(\sum_{m=0}^{10} \sigma(\rho)^m x_m - 1\right)\left(\sum_{m=0}^{10} \sigma(\rho)^{-m} x_m - 1\right)$$

of eleven variables $x_0, \ldots, x_{10}$ in the closed interval $[0, 2l]$ takes its maximum, then each value of $x_0, \ldots, x_{10}$ is 0 or $2l$ and so

$$-4l^2 < \sum_{m=1}^{10} x'_m x'_{m-1} - x'_{10} x'_0 \leq 36 l^2,$$

$$-8l^2 < \sum_{m=2}^{10} x'_m x'_{m-2} - \sum_{m=0}^{1} x'_{m+9} x'_m \leq 28 l^2,$$

$$-12l^2 < \sum_{m=3}^{10} x'_m x'_{m-3} - \sum_{m=0}^{2} x'_{m+8} x'_m \leq 20 l^2,$$

$$-12l^2 \leq \sum_{m=4}^{10} x'_m x'_{m-4} - \sum_{m=0}^{3} x'_{m+7} x'_m < 16 l^2,$$

$$-12l^2 < \sum_{m=5}^{10} x'_m x'_{m-5} - \sum_{m=0}^{4} x'_{m+6} x'_m \leq 12 l^2,$$

where $x'_0 = x_0 - 1$, $x'_1 = x_1, \ldots, x'_{10} = x_{10}$. Hence

$$\begin{aligned}
\mathfrak{N}(\alpha) &= \prod_{d=0}^{4} \left| \sum_{c=1}^{5} 2W_c \cos\frac{\pi c 3^d}{11} + \sum_{m=0}^{10} w_m^2 \right| \\
&< \Bigg(\bigg(18\cos\frac{\pi}{11} + 14\cos\frac{2\pi}{11} + 10\cos\frac{3\pi}{11} \\
&\qquad + 8\cos\frac{4\pi}{11} + 6\cos\frac{5\pi}{11} + 11\bigg) \\
&\quad \times \bigg(18\cos\frac{3\pi}{11} + 4\cos\frac{5\pi}{11} + 6\cos\frac{2\pi}{11} \\
&\qquad + 6\cos\frac{\pi}{11} + 6\cos\frac{4\pi}{11} + 11\bigg) \\
&\quad \times \bigg(2\cos\frac{2\pi}{11} + 14\cos\frac{4\pi}{11} + 10\cos\frac{5\pi}{11} \\
&\qquad + 6\cos\frac{3\pi}{11} + 6\cos\frac{\pi}{11} + 11\bigg) \\
&\quad \times \bigg(18\cos\frac{5\pi}{11} + 4\cos\frac{\pi}{11} + 6\cos\frac{4\pi}{11} \\
&\qquad + 8\cos\frac{2\pi}{11} + 6\cos\frac{3\pi}{11} + 11\bigg) \\
&\quad \times \bigg(2\cos\frac{4\pi}{11} + 4\cos\frac{3\pi}{11} + 10\cos\frac{\pi}{11} \\
&\qquad + 6\cos\frac{5\pi}{11} + 6\cos\frac{2\pi}{11} + 11\bigg)\Bigg)(4l^2)^5.
\end{aligned}$$

We thus obtain

$$M < 50412966(2l)^{10}.$$

Let P be the set of prime numbers which are primitive roots modulo 529. Let S be the set of pairs (n', l') such that n' is a positive integer, l' is a prime number in P, and

$$23^{n'} < 50412966(2l')^{10}, \quad l' < 11 \log_2\left(\frac{23^{n'+1}}{\pi} \sin\frac{\pi}{23}\right).$$

Each (n', l') in S then satisfies

$$n' \leq 31, \quad l' \leq 1523.$$

By [3, Lemma 1], (n, l) belongs to S if l divides h_n/h_{n-1}.

We put, for later convenience,

$$\begin{aligned}
S' = &\{(7, l') \mid l' \in P,\, 293 < l' \leq 389\} \\
&\cup \{(8, l') \mid l' \in P,\, 389 < l' \leq 613\} \\
&\cup \{(9, l') \mid l' \in P,\, 613 < l' \leq 1523\}.
\end{aligned}$$

From now on, suppose that (n, l) belongs to $S \cup S'$. As $h_0 = 1$, it suffices for our proof to show that l does not divide h_n/h_{n-1}. We define a unit η in $\boldsymbol{B}_n$ by

$$\eta = \prod_{a \in I} \frac{\sin(2\pi a/23^{n+1})}{\sin(2\pi(23^n + 1)a/23^{n+1})}.$$

This is a typical example of a circular (or cyclotomic) unit of $\boldsymbol{B}_n$. For each positive integer $m \leq 10$, let a_m denote the integer such that

$$a_m \equiv 5^{23^n m} \pmod{23^{n+1}}, \qquad 0 < a_m < 23^{n+1}.$$

Since 5 is a primitive root modulo 23^{n+1}, we take as $\mathfrak{p}$ the prime ideal of the 11th cyclotomic field $\boldsymbol{Q}(\rho)$ generated by 23 and $a_1 - \rho$. It follows that

$$I = \{1, a_1, \dots, a_{10}\}.$$

We let $\|\eta\|$ denote the maximum of the absolute values of all conjugates of η over $\boldsymbol{Q}$. Lemma 2 of [2] implies that $h_n/h_{n-1} \not\equiv 0 \pmod{l}$ if $l \geq \log_2 \|\eta\|$ (cf. [1, Lemmas 2, 3]).

Let us first consider the case $n \leq 5$. Put

$$S_1 = (\{1,2,3,4\} \times \{5,7,11\}) \cup (\{2,3,4\} \times \{17,19\}) \cup (\{4,5\} \times \{37\}),$$

$$S_2 = \{(5,5),(5,7),(5,11),(5,17),(5,19)\} = \{5\} \times \{5,7,11,17,19\}.$$

Table I

(n,l)	$s(1)$	$s(1+23^n)$
$(5,37)$	-20	-1
$(4,37)$	-313	-153
$(4,19)$	-70	155
$(4,17)$	-75	18
$(4,11)$	-10	13
$(4,7)$	26	-6
$(4,5)$	13	-10
$(3,17)$	-294	-322
$(3,11)$	-94	-74
$(3,5)$	29	-23
$(2,19)$	6170	1482
$(2,11)$	2803	73
$(2,5)$	211	-10
$(1,11)$	15055	-11216
$(1,7)$	-3532	-3975
$(1,5)$	115	769

Table II

(n,l)	$s(2)$	$s(2+23^n)$
$(3,19)$	242	-427
$(3,7)$	-134	-41
$(2,17)$	-1297	-2032
$(2,7)$	-55	1335

Using a personal computer together with *Mathematica*, we have verified that the maximal integer not exceeding $\log_2 \|\eta\|$ is either 12, 20, 27, 40 or 38 according as n is either 1, 2, 3, 4 or 5. Therefore (n,l) satisfies $l < \log_2 \|\eta\|$ if and only if $(n,l) \in S_1 \cup S_2$. By further use of the (personal) computer under the condition $(n,l) \in S_1$, we have computed $s(m)$ for suitable integers m after the determination of $\mathcal{P}_a(m)$, $\mathcal{Q}_a(m)$ for all $a \in I$. Results for such cases of (n,l) are given in Tables I and II. We therefore know from [3, Lemma 2] that l does not divide h_n/h_{n-1} when (n,l) belongs to S_1. In the case $(n,l) \in S_2$, we can find by computer an example of u satisfying the hypothesis of Lemma 2; namely, we have $\mathfrak{H}(u) = \{\psi_u\}$, with u equal to either 3, 6, 2, 7 or 36, according to whether l is either 5, 7, 11, 17 or 19. Hence, by Lemma 2, the product $5 \cdot 7 \cdot 11 \cdot 17 \cdot 19$ is relatively prime to $h_{n'}/h_{n'-1}$ for all integers $n' \geq 5$. It is thus proved that $h_n/h_{n-1} \not\equiv 0 \pmod{l}$ whenever $n \leq 5$.

Let us next proceed to the case where $n = 6$ so that $l \leq 293$. By an argument above, we may suppose that $l \notin \{5,7,11,17,19\}$, i.e., $l \geq 37$. With the help of a computer, as in the case $(n,l) \in S_2$, we can always find an example of u satisfying the hypothesis of Lemma 2. Values of $u \in \{1,\dots,l-1\}$ such that $\mathfrak{H}(u) = \{\psi_u\}$, for all values of l, are given in Table III. Consequently, Lemma 2 actually shows that $h_n/h_{n-1} \not\equiv 0 \pmod{l}$ not only when $n = 6$ but also when $n \geq 7$ and $l \leq 293$.

Let us finally deal with the case $n \geq 7$. Naturally supposing that $l > 293$, we put

$$T = \{(n'+m, l') \mid (n',l') \in S',\ 0 \leq m \in \boldsymbol{Z}\}.$$

In the case $(n,l) \in S'$, we have checked $\mathfrak{H}(1) = \{\psi_1\}$ by computer. Therefore, in virtue of Lemma 2, l does not divide $h_{n'}/h_{n'-1}$ for all integers n' with $(n',l) \in T$. Since

$$\{(n',l') \mid (n',l') \in S,\ n' \geq 7\} \subseteq T,$$

it then follows that $h_n/h_{n-1} \not\equiv 0 \pmod{l}$ whenever $n \geq 7$. Thus the theorem is completely proved.

Correction to [1]. Instead of defining $f(\chi,u)$ by line 19 on page 258, one should define $f(\chi,u)$

Table III

l	37	43	53	61	67	79	83	89	97	103	107	113	149	157	181	191	199	227	241	251	281	283	293
u	1	1	1	2	2	1	1	2	4	2	1	90	3	3	13	3	4	8	4	8	12	281	5

as the maximal divisor of $f(\chi)$ relatively prime to u, with the notation $\tilde{u}$ retained; furthermore, on page 260, "$q_0 = \gcd(q, 2t)$" in line 3, "$f' = f(\psi_2^d)$" in line 6, and "$\psi_2^d(b) = 1$" in line 11 should be "$q_0 = f(\psi_2)/t$", "$f(\psi_2^d) \mid f'$", and "$\psi_2(b)^d = 1$", respectively.

Acknowledgment. The authors express their sincere gratitude to the referee who carefully read the paper in manuscript and made helpful comments for its improvement.

References

[1] K. Horie, Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field, J. London Math. Soc. (2) **66** (2002), no. 2, 257–275.

[2] K. Horie, Primary components of the ideal class group of the $\boldsymbol{Z}_p$-extension over $\boldsymbol{Q}$ for typical inert primes, Proc. Japan Acad. Ser. A Math. Sci. **81** (2005), no. 3, 40–43.

[3] K. Horie and M. Horie, The narrow class groups of some $\boldsymbol{Z}_p$-extensions over the rationals, Acta Arith. **135** (2008), no. 2, 159–180.

[4] K. Horie and M. Horie, The narrow class groups of the $\boldsymbol{Z}_{17}$- and $\boldsymbol{Z}_{19}$-extensions over the rational field, Abh. Math. Sem. Univ. Hamburg. (to appear).

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