On Schertz’s class number formula related to elliptic units
for some non-Galois extensions

by

JIRO SUZUKI (Tokyo)

Introduction. The purpose of this paper is to give a refinement of Schertz’s
class number formula related to elliptic units. We are going to study some
non-Galois cases. Let \( K/Q \) be a finite non-Galois extension, \( k \) be an imaginary
quadratic field, and put \( L = Kk \). We denote by \( h \) the class number of \( K \) and by
\( E \) the unit group of \( K \). Suppose that \( L/k \) is an abelian extension. Then Schertz
[6] has shown a class number formula related to elliptic units as follows:

**Theorem (Schertz).** Notations being as above, one can construct a group
\( F \) of certain elliptic units of \( K \) such that

\[
ch/h_0 = (E:FE_0)
\]

with an explicit constant \( c \) depending only on the construction of \( F \). Here, \( h_0 \) and
\( E_0 \) are the class number and the unit group of the maximal absolutely abelian
subfield \( K_0 \) of \( K \), respectively.

In this formula, \( h_0 \) can be known in various ways because \( K_0 \) is absolutely
abelian. But the constant \( c \) is much more complicated and not so small in [6].
Now, to know the class number \( h \), we shall make \( c \) as small and explicit as
possible. Then we have the best possible construction of \( F \) in Schertz’s formula.
Namely,

**Theorem 1.** Notations being as above, suppose that the Galois closure \( L \) of
\( K \) is dihedral over \( Q \) and cyclic over \( k \). Let \( n = [K:Q] \). Then we can construct
a group \( F \) of certain elliptic units such that

\[
h = (E:F) \quad \text{if } n \text{ is odd,}
\]

\[
2^b h/h_0 = (E:FE_0) \quad \text{if } n = 4 \text{ or } 2l, \ (2, l) = 1.
\]

In (0.3), \( K_0 \) is a quadratic field and \( b \) is a computable positive integer.

The proof of Theorem 1 is described in Section 3. For that purpose, we
prepare some properties of \( Z \)-modules in cyclotomic fields in Section 1. Schertz’s result above is described in Section 2 precisely. Finally, in Section 4,
we discuss a few more cases where $L/Q$ is not dihedral. In particular, in the case where $[K:Q]$ is the product of two primes we prove Theorem 2 which, together with Theorem 1, completely give a formula for $n = pq$ with primes $p$, $q$. The class number formula (0.1) is previously studied in detail by H. Hayashi [1], K. Nakamura [2], [3], [4] when $n = 3, 4, 5, 6$.

1. Preliminaries on cyclotomic fields. Let $m$ be a positive integer, $> 2$. Let $\zeta = \zeta_m$ be a primitive $m$th root of unity and put $Q_m = Q(\zeta)$. Let $J$ be the complex conjugation of $Q_m$ and let $Q_m^+$ be the fixed field of $Q_m$ for $J$. Then $Q_m^+$ is the maximal real subfield of $Q_m$. Let $O$ (resp. $O^+$) be the ring of integers of $Q_m$ (resp. $Q_m^+$), and $D_m$ (resp. $D_m^+$) be the discriminant of $Q_m$ (resp. $Q_m^+$). Let $N$ be the norm on $Q_m/Q$. Let $\Phi_m(X)$ be the $m$th cyclotomic polynomial:

$$\Phi_m(X) = \prod_{(a,m)=1} (X - \zeta_a).$$

Throughout this section, $p$ always denotes a prime number.

Let $n \in Q$. We define the function $\Phi^*_n$ from $\{\pm 1\}$ to $Z$ according to the value $\Phi_n(\pm 1)$ as follows

$$\Phi^*_n(\pm 1) = \begin{cases} \Phi_n(\pm 1) & \text{if } n > 2, n \in Z, \\ 1 & \text{if } n \in Q - Z. \end{cases}$$

When $n = 1$ or 2, $\Phi^*_1(1) = \Phi^*_2(1) = 1$ and $\Phi^*_1(-1) = \Phi^*_2(1) = 2$.

We recall that $m > 2$, then $\Phi_m(\pm 1)$ is known as follows:

$$(1.1) \quad \Phi_m(1) = \begin{cases} p, & m = p^a, \ a \geq 1, \\ 1, & \text{otherwise}. \end{cases}$$

Since $\Phi_m(-1) = \prod (-1 - \zeta_a) = \prod (1 + \zeta_a)$,

$$\Phi_m(-1) = \begin{cases} \Phi_{m/2}(1) & \text{if } m = 2(\text{mod } 4), \\ \Phi_m(1) & \text{if } m = 0(\text{mod } 4), \\ \Phi_{2m}(1) & \text{if } m = \pm 1(\text{mod } 4). \end{cases}$$

Therefore,

$$(1.2) \quad \Phi_m(-1) = \begin{cases} p, & m = 2p^a, \ a \geq 1, \\ 1, & \text{otherwise}. \end{cases}$$

Note that $N(\zeta - 1) = \Phi_m(1)$. We shall only use $\Phi^*_n(\pm 1)$ as the absolute norm of some ideal $\neq (0)$. When we use $\Phi^*_n(\pm 1)$ as the meaning of some positive integer, we can use $\Phi_n(\pm 1)$ instead of $\Phi^*_n(\pm 1)$, without confusion.

Let $p = (\zeta - 1)O$. Then $p$ is a prime ideal of $O$ when $m$ is a prime power, otherwise $p = O$.

The following lemma is known (see Washington [7], Lemma 4.19).
**Lemma 1.** The discriminant of the maximal real subfield $Q^+_m$ is given by

$$|D^+_m| = (m^{\phi(m)}) \prod_{p \mid m} p^{\phi(m)/(p-1)} \Phi_m(1) \Phi_{m/2}(1)^{1/2},$$

where $p$ runs through all prime divisors of $m$.

Here, the factor $\Phi_m(1) \Phi_{m/2}(1)$ equals $p$ or $4$ according as $m$ or $m/2$ is $p^a$ or $2^a$, where $p$ is an odd prime. Otherwise, $\Phi_m(1) \Phi_{m/2}(1) = 1$.

Let $\zeta_0$ be an $m$th root of unity. We consider a $Z$-module given by the following formula:

$$M = \sum_{j=1}^{m-1} Z((\zeta^j - 1) + \zeta_0 (\zeta^{-j} - 1)).$$

Since $m > 2$, $M \neq 0$. Denote by $d(M)$ the absolute value of the discriminant of the $Z$-module $M$. Suppose $\zeta_0 = \pm 1$.

**Lemma 2.** Let $\zeta_0 = 1$. Then $M = p \cap O^+$, and

$$d(M) = \Phi_m(1)^2 |D^+_m|.$$

**Proof.** Since $\zeta_0 = 1$, we have $M = \sum_{j=1}^{m-1} Z(\zeta^j + \zeta^{-j} - 2)$ from (1.3). We shall prove the above in 3 steps.

1. $M$ is an ideal of $O^+$. Since $O^+ = Z[\zeta + \zeta^{-1}]$ (see [7], Proposition 2.16), the $Z$-module $M$ is an ideal of $O^+$. Indeed,

$$(\zeta + \zeta^{-1})(\zeta^j + \zeta^{-j} - 2) = (\zeta^{j+1} + \zeta^{-j+1} - 2) + (\zeta^{j-1} + \zeta^{-j-1} - 2) - 2(\zeta + \zeta^{-1} - 2).$$

2. $p^2 \cap O^+ \subseteq M \subseteq p \cap O^+$. The inclusion $M \subseteq p \cap O^+$ is clear. Since $M$ is an ideal of $O^+$ and $(\zeta + \zeta^{-1} - 2) \in M$,

$$p^2 \cap O^+ = (\zeta - 1)^2 O \cap O^+ = (\zeta + \zeta^{-1} - 2) O^+ \subseteq M.$$

3. $p^2 \cap O^+ = p \cap O^+$. If $p = O$ then the equality is trivial. Assume $p \neq O$, then $p$ is the prime ideal which totally ramifies in $Q_m/Q$. Let $p^+ = p \cap O^+$. Since $[Q_m : Q^+_m] = 2$, $p^+ O = p^2$. This implies that $p^2 \cap O^+ = p \cap O^+$. Hence $M = p \cap O^+$. In step 3, we saw that $[O^+ : p \cap O^+] = \Phi_m(1)$. Using the formula for the discriminant of an ideal of an algebraic number field, the lemma is proved.

**Lemma 3.** Let $\zeta_0 = -1$ and let $m$ be even. Then $M = (\zeta - \zeta^{-1}) O^+$ and

$$d(M) = \Phi_{m/2}(1) \Phi_{m/2}(-1) |D^+_m|.$$
where \( e = 1 \) or \( 0 \). Therefore \( M = (\zeta - \zeta^{-1})\mathcal{O}^+ \). The discriminant of \( M \) is given by

\[
d(M) = |N(\zeta - \zeta^{-1})| |D_m^+|,
\]

and

\[
|N(\zeta - \zeta^{-1})| = |N(\zeta^2 - 1)| = |N(\zeta - 1)N(\zeta + 1)| = \Phi_m(1)\Phi_m(-1).
\]

The lemma is proved.

**Remark 1.** The rank of \( p \cap \mathcal{O}^+ \) as \( \mathbb{Z} \)-module is \( \varphi(m)/2 \). The set \( \{\zeta^j + \zeta^{-j} - 2\mid 1 \leq j \leq \varphi(m)/2\} \) is an independent system over \( \mathbb{Z} \). Furthermore the fact that the set is a basis of \( p \cap \mathcal{O}^+ \) is proved in a way similar to the proof of the fact that \( \{\zeta^j + \zeta^{-j}\mid 0 < j < \varphi(m)/2\} \) is a basis of \( \mathbb{Z}[\zeta^{1/2}, \zeta^{-1}] \). Similarly, \( \{\zeta^j - \zeta^{-j}\mid 1 \leq j \leq \varphi(m)/2\} \) is a basis of \( (\zeta - \zeta^{-1})\mathcal{O} \).

Suppose \( \zeta_0 \neq \pm 1 \).

**Lemma 4.** Let \( \zeta_0 \) be a primitive \( d \)-th root of unity, where \( d \) is a divisor of \( m \) and \( d \neq 1, 2 \). Then there is a \( \mathbb{Z} \)-submodule \( M_0 \) of \( M \) such that the discriminant of \( M_0 \) on \( Q_m^+ \) is given by

\[
d(M_0) = \Phi_d(-1)^{\varphi(m)/\varphi(d)}\Phi_m(1)^2 |D_m^+|.
\]

**Proof.** Let \( M_0 = (1 + \zeta_0)(p \cap \mathcal{O}^+) \). Then \( M_0 \) is a \( \mathbb{Z} \)-submodule of \( M \) because \( p \cap \mathcal{O}^+ = \sum_{i=1}^{\varphi(m)/2} \mathbb{Z}(\zeta^i + \zeta^{-i} - 2) \) by Lemma 2 and

\[
(1 + \zeta_0)(\zeta^i + \zeta^{-i} - 2) = (\zeta^i - 1 + \zeta_0(\zeta^{-i} - 1)) + (\zeta^{-i} - 1 + \zeta_0(\zeta^{-i} - 1)) \in M.
\]

The discriminant of \( M_0 \) is given by \( d(M_0) = |N(1 + \zeta_0)| |d(p \cap \mathcal{O}^+)\). Since \( \zeta_0 \) is a primitive \( d \)-th root of unity, \( |N(1 + \zeta_0)| = \Phi_d(-1)^{\varphi(m)/\varphi(d)} \). The lemma is proved.

**2. Schertz's results.** In this section, we shall describe Schertz's result and give the notations. Using the class field theory, there is a positive integer \( f \) such that the ray class field \( \mathcal{H}(f) \) modulo \( f \) includes \( L \). Let \( \mathcal{C}(f) \) be the ray class group modulo \( f \) of \( k \). The Artin symbol \( (c, \mathcal{H}(f)/k) \) gives an isomorphism from \( \mathcal{C}(f) \) to the Galois group \( G(\mathcal{H}(f)/k) \). Since \( f = \tilde{f} \), the complex conjugation \( c \rightarrow \bar{c} \) is an automorphism of \( \mathcal{C}(f) \). Using this fact, we can prove the next properties. (But the proof is omitted here, see [6].)

The extension \( \mathcal{H}(f)/\mathbb{Q} \) is Galois, the Galois group \( G(\mathcal{H}(f)/\mathbb{Q}) \) is the semi-direct product \( G(\mathcal{H}(f)/k) \cdot \langle J \rangle \), and \( G(\mathcal{H}(f)/k) \) is a normal subgroup of \( G(\mathcal{H}(f)/\mathbb{Q}) \). Since \( J^{-1}(c, \mathcal{H}(f)/k) = (\bar{c}, \mathcal{H}(f)/k) \), we define \( c^J \) by \( \bar{c} \). Let \( U \) be the subgroup of \( \mathcal{C}(f) \) corresponding to the field \( L \). Since \( [L : K] = 2 \), \( U^J = U \) can be proved. (See [6, II], pp. 67–68.) Therefore \( L/\mathbb{Q} \) is Galois. There is an element \( c_0 \) of \( \mathcal{C}(f) \mod U \) such that \( G(L/K) = \langle c_0, L/\mathbb{Q} \rangle J \), the Galois group \( G(L/\mathbb{Q}) \) is the semi-direct product \( G(L/k) \cdot \langle c_0, L/\mathbb{Q} \rangle J \), and \( G(L/k) \) is a normal subgroup of \( G(L/\mathbb{Q}) \). For the maximal abelian subfield \( K_0 \) of \( K \), the composite \( L_0 = K_0k \) is the maximal abelian subfield of \( L \). Let \( U_0 \) be the subgroup of \( \mathcal{C}(f) \) corresponding to \( L_0 \). Then \( U_0 = \{ c^J \mid c \in \mathcal{C}(f) \} \). Let \( A = \mathcal{C}(f)/U \) and \( X \).
be the character group of $A$. Since $U' = U$, we define the action of the automorphism $J$ on $X$ by $\chi'(c) = \chi(c)$ for any $\chi \in X$. Let $X_0 = \{ \chi \in X | \chi' = \chi \}$. Then $X_0$ is the character group of $U_0$. The classes of characters $W = (X - X_0)/\sim$ are defined by the equivalence relation:

$$\chi \sim \chi' \quad \text{if and only if} \quad \langle \chi \rangle = \langle \chi' \rangle \quad \text{or} \quad \langle \chi' \rangle = \langle \chi' \rangle.$$

If $L/Q$ is dihedral, then $\langle \chi \rangle = \langle \chi' \rangle$ is equivalent to $\langle \chi' \rangle = \langle \chi' \rangle$. Therefore, we assume that $\chi \sim \chi'$ satisfies $\langle \chi \rangle = \langle \chi' \rangle$ in this section. Later, we shall treat the case $\langle \chi' \rangle \neq \langle \chi \rangle$ in Section 4. For any class $\omega$ of $W$, let $m_\omega$ be the order of an element of $\omega$. We take the subset $\omega'$ of $\omega$ defined by

$$\omega' = \{ \chi' | 1 \leq j \leq m_\omega/2, (j, m_\omega) = 1 \}.$$

Then $\omega' \cap \omega' = \omega$ and $\omega' \cap \omega' = \emptyset$. Put $r_\omega = \# \omega' = \varphi(m_\omega)/2$. The rank $r$ of $F$ is found in [6], namely,

$$(2.1) \quad r = \sum_{\omega \in W} r_\omega + r_0, \quad r_0 = \# \{ \chi \in X_0 | \chi(c_0) = 1, \chi \neq 1 \}.$$

For any class $\omega$, let $U_\omega$, $A_\omega$, and $k_\omega$ be the following:

$$U_\omega = \{ c \in \text{Cl}(f) | \chi(c) = 1 \text{ for any } \chi \in \omega \},$$

$$A_\omega = \text{Cl}(f)/U_\omega,$$

$$k_\omega \text{ is the field corresponding to } U_\omega.$$

Now, $F$ is constructed by canonical elliptic units $\theta_\omega(a)$ of $L (a \in A_\omega, \omega \in W)$. (For elliptic units in the case where $H_{(f)}$ is the ring class field, see [5].) For each class $\omega$ of $W$, we take integers $\lambda_i (a) (i = 1, \ldots, r_\omega, a \in A_\omega)$ such that $d_\omega = |\det(v_{ij})| \neq 0$ where

$$v_{ij} = \sum_{a \in A_\omega} \lambda_i ((\chi'(a) - 1) + \chi'(c_0)(\chi^{-j}(a) - 1)) \quad \text{for } i, j = 1, \ldots, r_\omega.$$

Let $\theta_{i\omega} = \prod_{a \in A_\omega} (\theta_\omega(a))^{1+(c_0L/k)^j} \lambda_i a$. The group $F$ is generated by $\{ \theta_{i\omega} | i = 1, \ldots, r_\omega, \omega \in W \}$. We give the constant $c$ in (0.1) as follows. Let

$$c_1 = n^{(r-1)/2}, \quad c_2 = n_0^{(1-r_0)/2} \quad \text{and} \quad c_3 = \prod_{\omega \in W} d_\omega m_\omega$$

where $n_0 = [K_0 : Q]$. Let $c_4 = c_1 c_2 c_3$ and $c_5 = \prod_{\omega \in W} 24 t_\omega$, where $t_\omega = \min \{ t | t(U_\omega : 1) = 0 (\text{mod } h_k) \}$, $h_k$ is the class number of $k$. The constant $c$ is given by

$$c = c_4 c_5.$$

Remark 2. Let $b$ be the number of classes in $W$ which have even order. Using II, Satz 3.2 in [6], we can take $c_5 = 2^b$ by the choice of $\theta_\omega(a)$. For the number $d_\omega$, Schertz [6] showed that we can take $d_\omega$ such that $d_\omega \neq 0$ and $d_\omega$ divides $(4m_\omega)^{\varphi(m_\omega)/2} \Phi_m(1)|D_m^+|$. But this is not enough for our purpose.
3. Proof of Theorem 1. First, by Remark 2, we can take $c_5 = 2^b$ for some integer $b$. Therefore, if we prove $c_4 = 1$ then $c = 2^b$. Since $L/k$ is cyclic, we assume that $X = \langle \chi \rangle$. Since $L/Q$ is dihedral, $\chi' = \chi^{-1}$. Hence, the relation $(\chi')^2 = \chi$ implies that the order of $\chi'$ is 1 or 2. Therefore,
\[ X_0 = \begin{cases} \{1, \chi^{n/2}\} & \text{if } n \text{ is even}, \\ \{1\} & \text{if } n \text{ is odd}. \end{cases} \]

Therefore, $n_0 = [K_0:Q] = 1$ or 2. Let
\[ e = \begin{cases} 1 & \text{if } n \text{ is even}, \\ 0 & \text{if } n \text{ is odd}. \end{cases} \]

Then we have $n_0 = 2^e$. For the value of $\chi(c_0)$, the next lemma holds.

**Lemma 5.** Let notations be as above. Let $n = [L:k]$. Assume that $n = 2^a u$, $(2, u) = 1$. Then there is an element $b$ of $\text{Cl}(f)$ such that $G(L/K') = \langle c_0 b^2, L/k \rangle$ and $\chi(c_0 b^2)$ is a $2^a$-th root of unity. Here, $K'$ is a conjugate of $K$.

**Proof.** Let $(b, L/k) \in G(L/k)$. Then the conjugate of $(c_0, L/k)$ by $(b, L/k)$ is $(b^{-2} c_0, L/k)$. Since $(u, 2) = 1$, we can choose an element $b$ of $\text{Cl}(f)$ such that $\chi(b^{-2} c_0)$ is a $2^a$-th root of unity.

By the above lemma, we assume that $\chi(c_0)$ is a $2^a$-th root of unity. We shall prove the theorem by considering three cases.

**Case 1.** $\chi(c_0) = 1$. Fix a class $\omega$ of $W$. Since $\chi(c_0) = 1$, $\chi'(c_0) = 1$ for any $j$. Therefore $v_{ij} = \sum_{\omega \in \Lambda_\omega} \lambda_{ij} (\psi^{j}(a) + \psi^{-j}(a) - 2)$. Put $m = m_\omega$ and $r = r_\omega$. Since $v_{ij} \in \mathcal{O}^+$ and $\{v_{ij} \mid \psi_j \in \omega\}$ are all conjugates of $v_{i1}$ over $Q^-_{m}/Q$, $d_\omega = |\det(v_{ij})| = d((v_{i1}, \ldots, v_{r1}))^{1/2}$, where $r = \varphi(m)/2$. Let $\zeta_0 = \psi(c_0)$. Then $M = \sum_{j=1}^{m-1} Z(\zeta_j + \zeta_j - 2)$. Using Lemmas 1 and 2, we have
\[ (3.1) \quad d(M) = \Phi_m(1)^2 (m^{\varphi(m)} / \prod_{p|m} p^{\varphi(m)/(p-1)} \Phi_m(1) \Phi_{m/2}(1))^{1/2}. \]

Assume that $\{v_{i1}, \ldots, v_{r1}\}$ is a basis of $M$. Then, from (3.1),
\[ (3.2) \quad d_\omega = \Phi_m(1) (m^{\varphi(m)} / \prod_{p|m} p^{\varphi(m)/(p-1)} \Phi_m(1) \Phi_{m/2}(1))^{1/4}. \]

We shall compute the coefficient $c_4$. Since $L/k$ is cyclic, the correspondence between divisors of $n$ and classes of $W$ is one-to-one. So, put $d_m = d_\omega$. We have $\prod_{\omega \in \mathcal{W}} d_\omega m_\omega^{-r_\omega} = \prod_{m|n} d_m m_{-\varphi(m)/2}$, where the product is taken over all divisors of $n$ except 1 and 2. From (3.2), we have
\[ (3.3) \quad \prod_{m|n} d_m m_{-\varphi(m)/2} = \prod_{m|n} \Phi_m(1)^{3/4} \prod_{m|n} (m_\varphi(m)^{\varphi(m)} / \prod_{p|m} p^{\varphi(m)/(p-1)} \Phi_m(1))^{-1/4}. \]

For any positive integer $n$, the formulas
\[ (3.4) \quad \sum_{m|n} \varphi(m) = n, \quad \prod_{m|n} \Phi_m(1) = n \]
are known. By comparison of the index of each prime divisor of \( n \), we obtain
\[
\prod_{m | n} \left( n^{\varphi(m)} \prod_{p | m} p^{\varphi(m)/(p-1)} \right) = n^r.
\]

Under the factorization of \( n \) in Lemma 5, using (1.1),
\[
\prod_{m | n} \Phi_{m/2}(1) = \prod_{m | u} \Phi_m(1)^e \prod_{m | 2} \Phi_{m/2}(1) = (n/2)^e.
\]

Using (3.3)–(3.6),
\[
\prod_{m | n} d_m m^{-\varphi(m)/2} = n^{(3-e-n)/4}.
\]

Since \( L/Q \) is cyclic, using (2.1), the rank \( r \) of \( E \) is given by
\[
r - r_0 = \left( \sum_{m | n} \varphi(m) - \varphi(2) - \varphi(1) \right)/2.
\]

By the assumption on the degree \( n \), \( \chi(c_0) = 1 \) yields that
\[
\begin{cases}
  r_0 = 0, \ K_0 = Q & \text{if } n \text{ is odd}, \\
  r_0 = 1, \ K_0 \text{ is a real quadratic field} & \text{if } n \text{ is even}.
\end{cases}
\]

We obtain \( r_0 = e \). From (3.4) and (3.8), the rank of \( E \) is
\[
r = (n - 1 - e)/2.
\]

From the definition of the constants \( c_1, c_2, c_3 \) in Section 2, we have
\[
c_1 = n^{(r-1)/2} = n^{(n-3+e)/4}.
\]

Since \( r_0 = e = 0 \) or \( 1 \), and \( n_0 = 2^e \),
\[
c_2 = 2^{(1-e)/2} = 1.
\]

From (3.7), \( c_3 = n^{(3-e-n)/4} \). Hence \( c_4 = c_1 c_2 c_3 = 1 \). In this case, the theorem is proved.

Case 2. \( \chi(c_0) = -1 \). If \( m_\omega \) is odd then \( d_\omega \) is the same as in case 1. Therefore we shall compare cases 1 and 2 for the value of \( d_\omega \) only in the case where \( m_\omega \) is even. For that purpose, we write \( c_1', d_\omega' \) instead of \( c_1, d_\omega \) in case 1 and so on. If \( (j, n) = 1 \), then \( j \) is odd and \( \chi'(c_0) = -1 \). Therefore,
\[
v_{ij} = \sum_{\alpha \in A_\omega} \lambda_{\alpha} (\psi_j(\alpha) - \psi^{-j}(\alpha)) \quad \text{and} \quad v_{ij} \in M = \sum_{j=1}^{m-1} Z(\zeta^j - \zeta^{-j}).
\]

Suppose that \( \{v_{11}, \ldots, v_{r_1}\} \) is a basis of \( M \). Then using Lemma 3,
\[
d_\omega = (\Phi_m(1) \Phi_m(-1))^{1/2} |D_m^+|^{1/2}.
\]

By comparison of (3.2) and (3.9),
\[
d_\omega'/d_\omega = \Phi_m(1)/\Phi_m(1) \Phi_m(-1)^{1/2}.
\]
Put \( m = 2^a u, (2, u) = 1 \), where \( a \geq 1 \). By the assumption of the degree \( n \), if \( a \geq 2 \) then \( n = 4 \) and \( \Phi_m(1) = \Phi_m(-1) = 2 \). If \( a = 1 \) then \( \Phi_m(1) = 1 \). Therefore,

\[
d'_\omega/d_\omega = \begin{cases} 1 \Phi_m(-1)^{-1/2} & \text{if } a = 1, \\
1 & \text{otherwise.}
\end{cases}
\]

Assume \( a > 1 \). Then \( d'_\omega/d_\omega = 1 \). Since \( \chi^2(c_0) = 1, r_0 = 1 \). Therefore, \( c_4 = c'_4 = 1 \).

Assume \( a = 1 \). Then \( d'_\omega/d_\omega = \Phi_m(-1)^{1/2} \). Therefore, \( \prod_{\omega \in W}(d'_\omega/d_\omega) = u^{1/2} \). Since \( r_0 = 0 \), the rank \( r = r' - 1 \). Then \( c_1 c'_2/c_1 c_2 = (n/2)^{1/2} \). Therefore \( c'_4/c_4 = 1 \). In this case, the theorem is proved.

**Case 3.** \( \chi(c_0) \neq \pm 1 \). In this case, by the assumption of \( n \), we have \( n = 4 \) and \( W = \{ \chi \} \). We compute \( d_\omega \) immediately using Lemma 4. Then \( d_\omega = 2^{3/2} \). Since \( n_0 = 2, r_0 = 0 \) and \( r = 1 \). So \( c_4 = 1 \). Now, the proof of Theorem 1 is complete.

**Corollary.** Let \( L \) be cyclic over \( k \). If the maximal real subfield \( K \) of \( L \) is non-Galois over \( Q \) then

\[ h = 2^b h_0(E:FE_0). \]

**Proof.** Since \( K \) is the maximal real subfield of \( L \), \( \chi(c_0) = 1 \). Therefore, the corollary can be proved as in the above proof of case 1.

**4. Non-dihedral cases.** In this section, we consider the case where \( n = p \) or \( n = pq \), both \( p \) and \( q \) are primes, and the case is not included in Theorem 1. We consider the automorphism \( \tau \) of order 2 instead of the complex conjugation \( J \) on \( X \). When \( \langle \chi' \rangle \neq \langle \chi \rangle \), we choose representatives of the class \( \omega \) of \( W \) and give \( v_i \)'s which are different from those of Section 2. (More details in [6].) If \( n = p \), then \( L \) has only one character class, therefore, \( L/Q \) is dihedral. Suppose \( n = pq \). Similarly, if \( p = 2 \) and \( q \neq 2 \) then \( L/Q \) is dihedral. If \( p = q = 2 \) then \( L/Q \) is dihedral because \( G(L/Q) \) is a non-abelian group of order 8. Suppose that both \( p \) and \( q \) are odd primes. Then the next theorem holds.

**Theorem 2.** Let \( K/Q \) be non-Galois and suppose the Galois closure \( L \) of \( K \) is abelian over \( k \). Suppose \( n = [K:Q] = pq \) (both \( p \) and \( q \) are odd primes), and \( L/Q \) is not dihedral. Then we can construct a group \( F \) of elliptic units such that if \( p = q \) then \( G(L/k) \) is an abelian group of type \( (p, p) \) and,

\[ p^{p^2 + 2p^2 - 3/4} h/h_0 = (E:FE_0); \]

if \( p \neq q \) and \( K_0 \neq Q \) then,

\[ 2^{(p-1)(q-1)/2} h/h_0 = (E:FE_0). \]

**Proof.** In both cases above, the character group \( X \) is the direct product \( \langle \chi \rangle \times \langle \psi \rangle \) where \( \chi \) and \( \psi \) are the characters of order \( p \) and \( q \), respectively. Since \( \tau^2 = 1 \) and \( L/Q \) is not abelian, we assume that \( \psi^r = \psi^{-1} \). We denote by \( \langle \psi \rangle^* \) the subset of \( \langle \psi \rangle \) whose element has order \( m \) where \( m \) is the order of \( \psi \). Let \( p = q \). Then we have two cases: (1) \( \chi^r = \chi^{-1} \), (2) \( \chi^r = \chi \).
Case 1: $W$ has $p + 1$ classes $\langle \chi \rangle^*$ and $\langle \chi^i \psi \rangle^*$ ($i = 1, \ldots, p$). In this case, the construction of $F$ is the same as in Theorem 1. For any class $\omega$, $d_\omega = p^{(p+1)/4}$ and $r_\omega = \varphi(p)/2$. Therefore $c_4 = p^{(p^2 + 2p - 3)/4}$.

Case 2: $X_0 = \langle \chi \rangle \cdot \langle (\psi^i \chi)^* \rangle = \langle \psi^{-i} \chi \rangle \neq \langle \psi^i \chi \rangle$ ($i = 1, \ldots, (p-1)/2$). Then $W$ has $(p + 1)/2$ classes $\langle \psi \rangle^*$ and $\langle \psi^i \chi \rangle^* \cup \langle \psi^{-i} \chi \rangle^*$ ($i = 1, \ldots, (p-1)/2$). If $\omega = \langle \psi \rangle^*$ then $d_\omega$ is the same as in case 1. Otherwise, we take $v_{ij}$ in Section 2 as

$$v_{ij} = \sum_{a \in \mathbb{Z}_p} \lambda_{ia}(\phi^j(a) - 1)$$

for $i, j = 1, \ldots, p$ where $\phi \in \langle \psi^k \chi \rangle^*$ for some $k$. Then $m_\omega = p$ and $d_\omega$ is the discriminant of the $\mathbb{Z}$-module constructed by $v_{ij}$'s. We can take $d_\omega = \Phi_p(1)|D_p|^{1/2}$ in [6], I, Satz 1.4. Therefore, $c_4 = \prod_{\omega \in W} d_\omega m_\omega^{-r_\omega} = p^{(p^2 + 2p - 3)/4}$ where the product is taken over all classes of $W$. In the former case, the theorem is proved.

Let $p \neq q$. Then $X_0 = \langle \chi \rangle$. Since $L/k$ is cyclic, $W$ has two classes $\langle \chi \rangle^*$ and $\langle \chi \psi \rangle^*$. If $\omega = \langle \chi \rangle^*$ then $d_\omega$ is the same as in Theorem 1. Let $Q_{pq}^*$ be the fixed field of $Q_{pq}$ for $\tau$. Let $\omega = \langle \chi \psi \rangle^*$ and $M$ be the $\mathbb{Z}$-module constructed by $v_{ij}$ in Section 2. Then $M$ includes the $\mathbb{Z}$-module $2(p \cap Q^*)$ where $Q^*$ is the ring of integers of $Q_{pq}^*$. The discriminant $D^*$ of $Q^*$ is $(pq)^{(p+q)/2} q^{1-p}$ which is easily shown by examining the ramification of $Q_{pq}/Q_{pq}^*$. If we take $v_{ij}$ as a basis of $2(p \cap Q^*)$, then $d_\omega = 2^{\sigma(pq)/2} \Phi_p(1)|D^*|^{1/2}$. Therefore, $c_4 = 2^{(p-1)(q-1)/2}$. The proof is completed.

Example. Let $K_0$ be abelian of degree $p$. Let $K \supset K_0$ and $K/Q$ be non-Galois of degree $pq$. Suppose the Galois closure $L$ of $K$ to be abelian over an imaginary quadratic field $k$ and $[L:k] = pq$. Then $L/Q$ is not dihedral.

References


DEPARTMENT OF MATHEMATICS
SOPHIA UNIVERSITY
7-1 Kioicho, Chiyoda-ku Tokyo 102, Japan

Received on 10.10.1986
and in revised form on 14.11.1989

(1679)