Dihedral extensions of $Q$ of degree $2l$ which contain non-Galois extensions with class number not divisible by $l$

by

Kiyokazu Iwasaki (Tokyo)

1. Main results. In this paper we specify all dihedral extensions $K$ of degree $2l$ over the rational numbers $Q$ which contain non-Galois extensions of odd prime degree $l \neq 3$ over $Q$ with class number not divisible by $l$ in terms of the conductor of the cyclic extension $K/k$ of degree $l$, where $k$ is a unique quadratic subfield of $K$. In [3] E. Gerth III completely gave the discriminants of all (non-Galois) cubic extensions of $Q$ whose class numbers are not divisible by 3. Our paper extends in essence his work to all non-Galois extensions of $Q$ of odd prime degree $l \neq 3$ whose normal closures have degree $2l$ over $Q$.

Now to state our results we need the following fact proved by J. Martinet [7].

**Lemma 1.** Let $K$ be a dihedral extension of $Q$ of degree $2l$, where $l$ is an odd prime number $\neq 3$, let $k$ be the quadratic subfield of $K$ with discriminant $d$, and let $L$ be a non-Galois extension of $Q$ of degree $l$ contained in $K$. Then the conductor $f$ of the cyclic extension $K/k$ of degree $l$ has the following form:

$$f = \prod_{i=1}^{l} p_i \prod_{j=1}^{l} q_i,$$

where $p_i$ and $q_i$ are rational primes such that

$$p_i = \left( \frac{d}{p_i} \right) = 1 \pmod{l},$$

$$q_i = \left( \frac{d}{q_i} \right) = -1 \pmod{l};$$

$u = 1$ if $l \mid f$ and $l \nmid d$, $u = 0$ otherwise; and $v = 0$ or 1. Furthermore the discriminant of $L/Q$ is $d^{l-1}v^{l-1}$.

Our main result is:
Theorem 1. Let \( p \) be an odd prime number \( \neq 3 \). Let \( k \) be a quadratic extension of \( \mathbb{Q} \) with discriminant \( d \), and let \( K \) be a dihedral extension of \( \mathbb{Q} \) of degree \( 2l \) containing \( k \). Let \( H(k) \) denote the \( l \)-class group of \( k \); i.e., the Sylow \( l \)-subgroup of the ideal class group of \( k \). In each part below, we give the conductor \( f \) of the cyclic extension \( K \) of \( k \) (of degree \( l \)) which contains non-Galois extensions of \( \mathbb{Q} \) of degree \( l \) with class number not divisible by \( l \).

There exists a unique \( K \) with the specified conductor \( f \).

(a) \( H(K) \) is not cyclic. Then no such \( K \) exists.
(b) \( H(K) \neq 1 \) but is cyclic. Then \( f = 1 \); i.e., \( K/k \) is unramified.
(c) \( H(K) = 1 \). Let \( A \) be the set of rational primes \( q \) such that \( q = \left( \frac{d}{q} \right) = -1 \) (mod \( l \)). Let \( e \) be the fundamental unit of \( k \) when \( d > 0 \), and let \( e = 1 \) when \( d < 0 \). Let

\[
A_1 = \{ q \in A \mid \text{e is a } l\text{-th power residue (mod } q\mathcal{O}_k) \},
\]

where \( \mathcal{O}_k \) is the ring of integers of \( k \), and let \( A_2 = A \setminus A_1 \). (Note that \( A_1 = A \) when \( d < 0 \).) If \( l \mid f \) (resp. \( \left( \frac{d}{l} \right) = -1 \)), let \( B = \{ \} \) when \( e \) is an \( l\)-th power residue (mod \( l\mathcal{O}_k \)), resp. \( \mathcal{O}_k \), and let \( B = \{ \} \) when \( e \) is an \( l\)-th power nonresidue (mod \( l\mathcal{O}_k \)), resp. \( \mathcal{O}_k \). Then the conductors \( f \) are given as follows:

(i) \( f = q \) where \( q \) is any element of \( A_1 \);
(ii) \( f = q_1q_2 \) where \( q_1 \) and \( q_2 \) are any distinct elements of \( A_2 \);
(iii) \( f = l \) if \( l \nmid f \) and \( g \in B \);
(iv) \( f = -l \) if \( l \mid f \) and \( g \) is an element of \( A_2 \);
(v) \( f = l^2 \) if \( \left( \frac{d}{l} \right) = -1 \) and \( g \in B \);
(vi) \( f = P \) if \( \left( \frac{d}{l} \right) = -1 \), \( l \nmid f \), and \( q \) is any element of \( A_2 \).

Remark. When \( l = 3 \) and \( H(k) = 1 \), there are nine cases to appear in [3], Theorem 2 (c), including our six cases (i)-(vi) in Theorem 1 (c).

Theorem 2. In Theorem 1, the sets \( A_1 \) and \( A_2 \) both have infinite cardinalities whenever \( d > 0 \) and \( d \neq (-1)^{(l-1)/2} \), and so does \( d < 0 \).

In Section 2 we shall prove Theorem 1, and Theorem 2 will be proved in Section 3 using the Tchebotarev density theorem.

Throughout this paper we use multiplicative notation for groups and modules, and the action of a group on a ring on a module is expressed by exponentiation. Furthermore, \( (x^r)^f = x^{fr} \), and \( (\frac{d}{l}) \) will denote the \( l \)-th Hilbert symbol.
sequence, it suffices to show that \( \tilde{V}_i^{0\rightarrow t} = H_{i+1}(K)^{0\rightarrow t} \) for all \( t \geq 1 \). By definition \( \tilde{V}_i \subset H_{i+1}(K) \), and so \( \tilde{V}_i^{0\rightarrow t} \subset H_{i+1}(K)^{0\rightarrow t} \). Now let \( h \in H_{i+1}(K)^{0\rightarrow t} \).

Then \( h^{(s-1)i} = 1 \) and \( h^{s-1} = h^{-1} \). Now

\[
U^{(s-1)i} = U^{(s-1)i} \in H_{i+1}(K)^{0\rightarrow t} = H_{i+1}(K)^{0\rightarrow t} = H_{i+1}(K)^{0\rightarrow t}
\]

since

\[
(s-1)i \in (s-1)i \in \mathbb{Z}[\sigma] \quad \text{and} \quad h^{(s-1)i} \in H_{i+1}(K).
\]

On the other hand, since \( h^{s-1} \in H_{i+1}(K) \), there are \( h_1 \in H_{i+1}(K) \), \( h_2 \in H_{i+1}(K)^{0\rightarrow t} \) such that \( h^{s-1} = h_1 h_2 \). Then \( h^{(s-1)i} = h_1 h_2 \in H_{i+1}(K)^{0\rightarrow t} \), which implies that \( h_1 \in H_{i+1}(K)^{0\rightarrow t} \). So \( h^{(s-1)i} = h_1 h_2 \in H_{i+1}(K)^{0\rightarrow t} \), which implies that \( h_1 \in \tilde{V}_i \cap H_{i+1}(K)^{0\rightarrow t} = \tilde{V}_i^{0\rightarrow t} \). So \( \tilde{V}_i^{0\rightarrow t} = H_{i+1}(K)^{0\rightarrow t} \).

**Lemma 4.** For all \( i \geq 1 \), there is an exact sequence

\[
1 \rightarrow \tilde{V}_i^{0\rightarrow t} \rightarrow \tilde{V}_{i+1}^{0\rightarrow t} \rightarrow H_{i+1}(K)^{0\rightarrow t} \rightarrow 1.
\]

**Proof.** Since \( \tilde{V}_i = \tilde{V}_i^{0\rightarrow t} \times \tilde{V}_i^{0\rightarrow t} \), it suffices to show that \( \tilde{V}_i^{0\rightarrow t} = H_{i+1}(K) \).

Clearly \( \tilde{V}_i^{0\rightarrow t} = H_{i+1}(K) \), and so \( \tilde{V}_i^{0\rightarrow t} = H_{i+1}(K) \). Now let \( h \in \tilde{V}_i \). Then \( h^{s-1} \in \tilde{V}_i \).

Write \( h^{(s-1)i} = (h^{(s-1)i} h^{(s-1)i})^{(s-1)i} = (h^{(s-1)i} h^{(s-1)i})^{(s-1)i} = h^{(s-1)i} h^{(s-1)i} = h^{(s-1)i} h^{(s-1)i} = 1 \),

since \( h \in H_{i+1}(K) \) and \( h^{(s-1)i} h^{(s-1)i} = N(h_1) \in N(H_{i+1}(K)) = 1 \). So \( h^{s-1} \in H_{i+1}(K)^{0\rightarrow t} \) and \( h^{s-1} \in H_{i+1}(K)^{0\rightarrow t} \).

**Lemma 5.** For all \( i \geq 1 \), \( V_i / H_i(L) \cong H_{i+1}(K) / H_{i+1}(L) \).

**Proof.** Since \( H_{i+1}(K) / H_{i+1}(L) = H_{i+1}(K) / H_{i+1}(L) \), then

\[
V_i / H_i(L) = H_{i+1}(K) / H_{i+1}(L).
\]

**Lemma 6.** For all integers \( i \geq 1 \), we have

\[
|H_{i+1}(K) / H_{i+1}(L)| = \left| \tilde{V}_{i+1} / \tilde{V}_{i} \right| \left| H_{i+1}(K) / H_{i+1}(L) \right|.
\]

**Proof.** We have

\[
|\tilde{V}_{i+1} / \tilde{V}_{i}| = \left| H_{i+1}(K) / H_{i+1}(L) \right| \quad \text{by Lemma 3},
\]

\[
= \left| \tilde{V}_{i+1} / H_i(L) \right| \quad \text{(by Lemma 4)} = \left| \tilde{V}_{i} / \tilde{V}_{i} / H_i(L) \right|
\]

\[
= \left| \tilde{V}_{i+1} / H_i(L) \right| \left| H_{i+1}(K) / H_{i+1}(L) \right| \quad \text{(by Lemma 5)}.
\]

Now if we apply [4], Theorem 4.3 to both \( \mathbb{Z}[\sigma] \)-modules \( H_{i+1}(K) \) and \( V_i \), we have, for every \( i \geq 1 \):

\[
|H_{i+1}(K) / H_{i+1}(L)| = \left| \tilde{V}_{i+1} / \tilde{V}_{i} \right| \left| H_{i+1}(K) / H_{i+1}(L) \right|
\]

(2.2)

\[
|\tilde{V}_{i+1} / \tilde{V}_{i} / H_i(L)| = \left| H_{i+1}(K) / H_{i+1}(L) \right|
\]

(2.3)

where \( t \) denotes the number of primes of \( k \) which ramify in \( K \), and \( r_i \) and \( r_i^i \) for each \( i \geq 1 \), are both nonnegative rational integers whose precise definitions will be given after equation (2.2). Now in view of the definition of \( V_i / H_i(L) \), \( N(H_i(L)) = 1 \) implies that \( N(V_i) = N(H_{i+1}(K)) \) for all \( i \geq 1 \). Hence from equations (2.2) and (2.3),

\[
|\tilde{V}_{i+1} / \tilde{V}_{i} / H_i(L)| = \left| H_{i+1}(K) / H_{i+1}(L) \right|
\]

(2.4)

Equations (2.1) with \( i = 1, \ldots, l - 1 \) put together to give

\[
|H_{l-1}(K) / H_{l-1}(L)| = \prod_{i=1}^{l-1} \left| \tilde{V}_{i+1} / \tilde{V}_{i} / H_i(L) \right|
\]

(2.5)

Equations (2.4) and (2.5) together with the equation

\[
|H_{l-1}(K)| = \prod_{i=1}^{l-1} \left| H_i(K) / H_{i+1}(L) \right|
\]

then yield

\[
|H_{l-1}(K)| = \prod_{i=1}^{l-1} \left| H_i(L) / H_{i+1}(L) \right|
\]

(2.6)

We now give the definitions of the numbers \( r_i \) and \( r_i^i \) that appear in equations (2.2) and (2.3), following the results in [4, pp. 36-42].

Let \( \mathbb{F}_1, \mathbb{F}_2, \ldots, \mathbb{F}_n \) (resp. \( \mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_n \)) be ideals of \( K \) (resp. \( L \)) which satisfy the following two conditions:

(1) \( H_{i+1}(K) \) (resp. \( H_{i+1}(L) \)) is generated by the ideal classes of the \( \mathbb{F}_j \)'s (resp. \( \mathbb{G}_j \)'s).

(2) If we define \( \mathbb{G} \) (resp. \( \mathbb{G}^\prime \)) to be the ideal group generated by the \( \mathbb{F}_j \)'s and their \( \sigma \)-conjugates (resp. the \( \mathbb{H}_j \)'s, and their \( \sigma \)-conjugates), then \( \mathbb{G} \cap \mathbb{G}^\prime \) is the group of principal fractional ideals of \( k \); let \( \mathbb{A} = \mathbb{G} \cap \mathbb{G}^\prime \) and \( \mathbb{A}^\prime = \mathbb{G} \cap \mathbb{G}^\prime \), where \( \mathbb{A} \) denotes the group of fractional ideals of \( K \) whose ideal classes belong to \( H(K) \).

Note that the ideal classes of the \( \mathbb{H}_j \)'s and the \( \mathbb{K}_j \)'s generate \( V_i \), and that \( \mathbb{G} \) and \( \mathbb{G}^\prime \) are both \( \mathbb{Z}[\sigma] \)-modules. Let \( \psi : k^* \rightarrow \mathbb{G} \) be the map defined by \( \psi(\gamma) = (\gamma) \) for \( \gamma \in k^* = k \setminus \{0\} \), where \( \mathbb{G}(k) \) denotes the group of principal fractional ideals of \( k \); let \( A = \psi^{-1}(N(k)\mathbb{G}(k)) \) and \( A^\prime = \psi^{-1}(N(k)\mathbb{G}(k)) \), where \( N(k) \) is the norm map from ideals of \( K \) to ideals of \( k \). Then \( A/A^\prime \) and \( A/A^\prime \), which may be viewed as vector spaces over \( \mathbb{F}_1 \), the finite field of \( l \) elements, are both of finite dimension, since \( \mathbb{G} \) and \( \mathbb{G}^\prime \)
are both finitely generated. So, let \( \{a_j\}_{1 \leq j \leq m} \) (resp. \( \{a_j\}_{1 \leq j \leq n} \)) be a set of generators of the vector space \( A/A' \) (resp. \( A/A'' \)). Furthermore, let \( \alpha \) be an element of the field \( k(\zeta) \) such that \( K(\zeta) = k(\zeta, \sqrt[n]{a}) \), where \( \zeta \) is a primitive \( n \)-th root of unity; let \( p_1, p_2, \ldots, p_t \) be the primes of \( K \) which ramify in \( K \); and let \( \mathfrak{p} \) be any prime of \( k(\zeta) \) above \( p_j \), \( 1 \leq j \leq t \). Then we can define \( r_\alpha \) and \( r_\alpha' \) to be the ranks of the matrices (over the finite field \( F \))

\[
(\beta_j) \quad (1 \leq j \leq m, 1 \leq \nu \leq t)
\]
and

\[
(\beta'_j) \quad (1 \leq j \leq n, 1 \leq \nu \leq t)
\]

where

\[
\zeta^j \alpha = \left( \begin{array}{c} a_j \alpha \\ \mathfrak{p} \end{array} \right) \quad (1 \leq j \leq m, 1 \leq \nu \leq t);
\]

\[
(2.7)
\]

\[
\zeta^j \alpha' = \left( \begin{array}{c} a_j \alpha \\ \mathfrak{p} \end{array} \right) \quad (1 \leq j \leq n, 1 \leq \nu \leq t).
\]

(2.7)

(It should be noted that these definitions of \( r_\alpha \) and \( r_\alpha' \) are well-defined (cf. [4], Proposition 3.4 and Theorem 4.3.).)

Now if we choose a set of generators of \( A'/A'' \) such that \( A/A'' \) is generated by one of its subsets (such a set does exist), we see at once from the definitions of \( r_\alpha \) and \( r_\alpha' \) that \( r_\alpha = r_\alpha' \) for all \( \nu \geq 1 \). But in some special cases, for example, when \( \nu = 1 \) or when the condition of the next lemma is fulfilled, it occurs that \( r_\alpha = r_\alpha' \) for all \( \nu \geq 1 \).

**Lemma 7.** Assume that there is no rational prime which decomposes in \( k \) and ramifies fully in \( L \). Then \( r_\alpha = r_\alpha' \) for all integers \( \nu \geq 1 \), and hence equation (2.6) becomes

\[
(2.8) \quad |H_{\nu-1}(L)| = \prod_{j=1}^{m} |H_{\nu}(K)/H_{\nu-1}(K)|.
\]

Furthermore, \( H(L) = 1 \) if and only if \( |H_{\nu}(K)/H_{\nu-1}(K)| = 1 \).

**Proof.** Note that a set \( \{a_j\}_{1 \leq j \leq m} \) of generators of \( A'/A'' \) may be chosen so that, a subset \( \{a_j\}_{1 \leq j \leq n} \) generates \( A/A' \) and \( a_j \) is a rational number for \( m+1 \leq j \leq n \). Then the same argument as in the proof of [6], Lemma 3, shows that \( \left( \begin{array}{c} a_j \\ \mathfrak{p} \end{array} \right) = 1 \) for \( m+1 \leq j \leq n, 1 \leq \nu \leq 1 \). Clearly this implies that \( r_\alpha = r_\alpha' \) for each integer \( \nu \geq 1 \). The last result follows at once from equation (2.6) and the fact that \( (\sigma-1) \) maps \( H_{\nu+1}(K)/H_{\nu}(K) \) injectively into \( H_{\nu}(K)/H_{\nu-1}(K) \) for all \( \nu \geq 1 \).

Our next step is to compute the order of \( H_{\nu}(K)/H_{\nu-1}(K) \) under the assumption of Lemma 7. From equation (2.2),

\[
|H_{\nu}(K)/H_{\nu}(K)| = \prod_{j=1}^{m} |H_{\nu}(K)/H_{\nu-1}(K)|.
\]

So we must consider the group \( N(H_{\nu}(K)) \) and the number \( r_\nu \). First, we want to show that \( N(H_{\nu}(K)) = H_{\nu}(K) \). Let \( \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t \) be the primes of \( K \) which are ramified over \( k \), and let \( H_{\nu}(K) \) be the subgroup of \( H_{\nu}(K) \) generated by the image of \( H_{\nu}(K) \) and the ideal classes of the \( \mathfrak{p}_j \)'s. Then \( N(H_{\nu}(K)) \) is a group, since \( N(H_{\nu}(K)) = \mathfrak{p}_j \) is a principal ideal in \( k \). Also \( H_{\nu}(K)/H_{\nu}(K) \) is either trivial or cyclic of order \( s \), and in the latter case there is an ideal of \( L \) in \( H_{\nu}(K)/H_{\nu}(K) \) of whose ideal class generates \( H_{\nu}(K)/H_{\nu}(K) \) (cf. [5], proof of Proposition 2 or [6], proof of Proposition 6). So in both cases \( N(H_{\nu}(K)) = N(H_{\nu}(K)) = H_{\nu}(K) \). Hence

\[
|H_{\nu}(K)/N(H_{\nu}(K))| = |H_{\nu}(K)/H_{\nu}(K)| = r_{\nu}^t,
\]

where \( r(k) \) denotes the rank of \( H(k) \); i.e., the minimal number of generators of \( H(k) \). Next we give an explicit matrix associated with \( H(k) \) by taking appropriate ideals as the \( \mathfrak{p}_j \)'s with properties (O1) and (O2). Let \( a_1, a_2, \ldots, a_{\nu(t)} \) be ideals of \( k \) whose ideal classes generate \( H(k) \), and let \( a_j = (a_j) \) for \( 1 \leq j \leq \nu(t) \), where \( a_j \) is the order of the ideal class of \( a_j \) in \( H(k) \). Let \( p_1, p_2, \ldots, p_t \) be the rational primes which ramify fully in \( L \); let \( \mathfrak{p} \) be an ideal of \( L \) whose ideal class is contained in \( H_{\nu}(K) \). Let \( H_{\nu}(K) \) be the (\( \nu \)-th) Hilbert symbol for \( \nu \)-th roots of unity in \( K \), and \( a \) be a rational number such that \( H_{\nu}(K) = (a) \). If we put \( \mathfrak{p} = \mathfrak{p}_j \) for \( 1 \leq j \leq \nu(t) \), \( \mathfrak{p}_{\nu(t)+1} = \mathfrak{p}_0 \), and \( \mathfrak{p}_{\nu(t)+1+s} = \mathfrak{p}_0 \), then it is easy to see that these \( \mathfrak{p} \)'s satisfy conditions (O1) and (O2). Also, the vector space \( A/A' \) (over the finite field \( F \)) corresponding to these \( \mathfrak{p}_j \)'s is generated by \( \{a, p_1, p_2, \ldots, p_t, a_1, a_2, \ldots, a_{\nu(t)}\} = S \), where \( a \) is the fundamental unit of \( k \) or \( e = 1 \) according as \( k \) is real or complex. Since \( p_1, p_2, \ldots, p_t, a \) are rational numbers, then \( \left( \begin{array}{c} b \alpha \\ \mathfrak{p} \end{array} \right) = 1 \) for \( b = p_1, p_2, \ldots, p_t, a \) and \( 1 \leq \nu \leq t \), where \( \mathfrak{p} \) is any prime of \( k(\zeta) \) above \( p \), \( 1 \leq \nu \leq t \), \( \zeta \) is a primitive \( n \)-th root of unity, and \( a \) is an element of \( k(\zeta) \) such that \( \mathfrak{p} = k(\zeta, \sqrt[n]{\alpha}) \) (cf. [6], proof of Lemma 3). Furthermore the product formula for the \( \nu \)-th Hilbert symbol says that \( \prod_{j=1}^{\nu(t)} \left( \begin{array}{c} \zeta^j \alpha \\ \mathfrak{p} \end{array} \right) = 1 \) for all elements \( \alpha \) of \( S \). Hence from these and equation (2.7), we get

\[
r_\alpha = \text{rank}(\beta_\alpha) \quad (1 \leq j \leq r(k)+1, 1 \leq \nu \leq t-1),
\]

where

\[
(2.9) \quad \zeta^j \alpha = \left( \begin{array}{c} a_j \alpha \\ \mathfrak{p} \end{array} \right)
\]

for \( 1 \leq j \leq r(k), 1 \leq \nu \leq t-1 \),

\[
\zeta^j \alpha' = \left( \begin{array}{c} a_j \alpha \\ \mathfrak{p} \end{array} \right)
\]

for \( j = r(k)+1, 1 \leq \nu \leq t-1 \).
We summarize these results in the following

Lemma 8. With the assumptions of Lemma 7 and the above notations,
$$|H_i'(k)/H_i(k)| = r^t - t - r^t - r^t - r^t,$$
where \( r = \text{rank of the } \{(r(k) + 1) \times (t - 1)\}\)-matrix over the finite field \( F \), defined by equation (2.9). (Note that \( r = 0 \) when \( t = 0 \)).

We are now in a position to prove Theorem 1. Assume that \( K \) contains \( L \) such that \( H(L) = 1 \). Then by Lemmas 2, 7, and 8, we have \( r(k) + t - r^t - r^t - r^t < 0 \). If \( r(k) \geq 2 \) (which means \( H(k) \) is not cyclic), then
$$r(k) + t - r^t - r^t < t - r^t - r^t < t - r^t < 0,$$
which is a contradiction. So \( r(k) = 0 \) or \( r = 0 \). We first assume \( r(k) = 0 \), which means \( H(k) \neq 1 \) but is cyclic. Since \( 0 \leq r \leq \max \{0, t - 1\} \) by Lemma 8, it follows that
$$r(k) + t - r^t = r^t - r^t = 0 \Rightarrow t = 0,$$
in which case class field theory says that there is a unique cyclic extension \( K/k \) of degree \( l \) with conductor \( t \). Clearly such a field \( K \) is a dihedral extension of \( Q \) of degree \( 2l \). Thus we have proved Theorem 1 (a)-(b).

It remains to prove Theorem 1 (c) (i)-(vi). So we assume \( H(k) = 1 \), which means \( r(k) = 0 \). By class field theory \( r(k) = 0 \) implies \( t \geq 1 \). Then in Lemma 8, the number \( r(k) \) is the rank of the \((1 \times (t - 1))\)-matrix whose \( 1 \)-th row \( \beta(d) \) is given by \( \overline{\beta(d)} = \left( \frac{a, \alpha}{\beta} \right) \). So \( r = 0 \) or \( 1 \), and hence
$$r(k) + t - r^t = r^t - r^t = 0 \Rightarrow t = 1 \text{ or } t = 2 \text{ and } r = 1.$$
We note that if \( t = 2 \), the product formula for the \( b \)-th Hilbert symbol implies that both of \( \left( \frac{a, \alpha}{\beta} \right) \) and \( \left( \frac{a, \alpha}{\beta} \right) \) are \( 1 \), or neither of them is \( 1 \). Furthermore, from our assumption that \( H(L) = 1 \) and from Lemmas 1 and 2 it follows that the primes of \( k \) which ramify in \( K \) must be either rational primes \( q \) such that \( q = \left( \frac{d}{q} \right) = -1 \) (mod \( l \)), \( l \) (if \( l \) is inert in \( k \)), or the unique prime of \( k \) above \( l \) (if \( l \) ramifies in \( k \)). Also it is easy to see that \( \left( \frac{e, \alpha}{\Omega} \right) = 1 \) (where \( \Omega \) is any prime of \( \Omega(e) \) above \( e \)) if and only if \( e \) is an \( h \)-th power residue \( (mod \ qO) \), or equivalently, \( q \) is contained in the set \( A_h \) defined in Theorem 1. If we correlate these results for the case when \( H(k) = 1 \), we obtain the following restrictions for the conductors \( f \) of the cyclic extensions \( K/k \) which contain \( L \) such that \( H(L) = 1 \).

Lemma 9. Let notations be as in Theorem 1, and assume \( H(k) = 1 \). Then \( K \) contains \( L \) such that \( H(L) = 1 \) if and only if the conductor \( f \) of \( K/k \) has one of the following forms:

(i) \( f = q \) where \( q \) is any element of \( A_1 \);
(ii) \( f = q_1 q_2 \) where \( q_1 \) and \( q_2 \) are any distinct elements of \( A_2 \);
(iii) \( f = l \) if \( l/1 \); (iv) \( f = l \) if \( l/1 \); (v) \( f = l \) if \( l/1 \); (vi) \( f = l \) if \( l/1 \).

It still remains to determine completely for which of the possible values of \( f \) listed in Lemma 9 there exists a dihedral extension \( K/Q \) of degree \( 2l \) such that the conductor of \( K/k \) is exactly \( f \). To do this we have only to extend the arguments in [3], Section 3, to our dihedral case. However there is no difficulty in carrying it out, and so we will not present it here. Consequently, Theorem 1 (c) (i)-(vi) is proved.

3. Proof of Theorem 2. Let notations be the same as in Theorem 1. In this section we let \( \xi \) be a primitive \( 2t \)-th root of unity. Let \( E = Q(\xi) \), \( \bar{E} = \bar{E} = k(\xi) \), and let \( E^* \) be the maximal real subfield of \( E \). We consider the case \( \bar{d} \neq (1 - 1) \) in which case there is only one quadratic subextension \( E^* \) of \( E/E^* \) other than \( E \) or \( E^* \), since the Galois group \( G(E/E^*) \) is the four group. Now suppose \( d > 0 \), and let \( N = \bar{E}(\bar{E}) \). Clearly \( N/Q \) is Galois. We want to show that \( G(N/E) \) is cyclic of order \( 2l \). Let \( N_0 \) be a subfield of \( N \) which has degree \( l \) over \( E \), and let \( \bar{f} \) be the generator of \( G(N_0) \). Since the action of \( \bar{f} \) on \( l \) is the same as that of the generator of \( G(k/Q) \), then \( \bar{f}^a = a(e)^{-1} \) with \( a \in Z \). But \( \bar{f}^a = \bar{f}^{a2} = a(e)^{-2} \), which implies \( a = 0 \) (mod 4). So \( \bar{f}^2 = \bar{f}^{-1} \). Now let \( \bar{e} \) be a generator of \( G(N/E) \), a cyclic group of order \( l \), and let \( \bar{e}^a = \bar{e}^{2a} = \bar{e}^{2a} \), where \( b \in Z \). Then \( \bar{e} = \bar{e}^{2a} = \bar{e}^{2a} \), which implies \( \bar{e} = \bar{e}^a \), and \( G(N/E) \) is cyclic of order \( 2l \). The Tchebotarev density theorem then shows that the set of primes \( O \) (resp. \( O_0 \)) of \( N \) for which

\[ G(N/E) = \left\{ \frac{N/Q}{O} \right\} \quad \text{(resp.} \% G(N/E) = \left\{ \frac{N/Q}{O_0} \right\}) \]

(where \( \left\{ \frac{N/Q}{O} \right\} \) is the Frobenius symbol) and which are unramified over \( Q \), has positive density. Setting \( q_t = O_t/Q \) \((i = 1, 2)\), we easily see that \( q_t \) is contained in \( A_i \) \((i = 1, 2)\), which completes the proof of Theorem 2 when \( d > 0 \). For the case \( d < 0 \), we can again apply the Tchebotarev density theorem to \( G(E/E^*) \) to obtain our result.
On 3-class groups of non-Galois cubic fields

by

KITOAKI IMURA (Tokyo)

**Introduction.** In this paper we give information about a certain direct summand of the 3-class group of a non-Galois cubic extension field of the rational numbers $\mathbb{Q}$, and show using it that for any finite elementary abelian 3-group $G$, there exist infinitely many pure cubic fields whose 3-class groups are isomorphic to $G$.

Throughout this paper we use multiplicative notation for groups and modules, and the action of a group or a ring on a module is expressed by exponentiation. Furthermore $(a^p)^p = a^p$. The cubic Hilbert symbol $\left(\frac{a}{p}\right)$ used here corresponds to $(a, b)_{\mathbb{Q}}$ in [5].

1. **A direct summand of the 3-class group.** Let $L$ be a non-Galois cubic extension field of $\mathbb{Q}$, let $K$ be the normal closure of $L$, and let $k$ be the quadratic subfield of $K$. Let $\sigma$ be a generator of the Galois group $G(K|k)$, and let $\tau$ be the generator of $G(K|L)$. Then $G(K|\mathbb{Q})$ is generated by $\{\sigma, \tau\}$ with the relations $\sigma^2 = \tau^2 = 1$, $\sigma \tau = \tau \sigma$. For any finite algebraic extension field $F$ of $\mathbb{Q}$, let $H(F)$ denote the 3-class group of $F$. As the canonical homomorphism $H(L) \to H(K)$ is injective, we may consider $H(L)$ as a subgroup of $H(K)$. For all nonnegative integers $i$, we define $H_i(K) = \{h \in H(K) \mid h^{3^i} = 1\}$ and $H_i(L) = \{h \in H_i(K) \mid h^3 = h\}$. Then $H_i(K)$ is a subgroup of $H(K)$ and is a $\mathbb{Z}[G(K|\mathbb{Q})]$-module; $H_i(L)$ is a subgroup of $H(L)$ and $H_i(L) = H_i(K)^{1+i}$; $H_i(K) = H_i(K)$ for large $i$ (cf. [4], Proposition 1). Furthermore let $N : H(K) \to H(k)$ be the map induced by the norm map from ideals of $K$ to ideals of $k$. Note that $N(H(L)) = \{1\}$ since $H(L) = H(K)^{1+i}$ and $H(\mathbb{Q}) = \{1\}$.

Now we let $H$ be a maximal direct summand of $H(L)$ contained in $H_1(L) = \{h \in H(K) \mid h^3 = h^2 = h\}$. 

---

DEPARTMENT OF MATHEMATICS

TOKYO METROPOLITAN UNIVERSITY

2-11-1, HIRAKAMAYAMA

TOKYO, JAPAN

Received on 18. 3. 1977 (923)