[3] K. F. Roth, *On irregularities of distribution*, Mathematika 1 (1954), pp. 73–79.
[4] — *On irregularities of distribution, II*, Communications on Pure and Applied Math. XXIX (1976), pp. 749–754.
[5] Wolfgang M. Schmidt, *Irregularities of distribution, X*, Journal of Number Theory, to appear.
[6] J. H. Halton and S. K. Zaremba, *The extreme and L^2 discrepancies of some plane sets*, Monatsh. für Math. 73 (1969), pp. 316–328.
[7] Brian E. White, *Mean-square discrepancies of the Hammersley and Zaremba sequences for arbitrary radix*, ibid. 80 (1975), pp. 219–229.
[8] I. V. Vilenkin, *Plane nets of integration* (Russian), Ž. Vyčisl. Mat. i Mat. Fiz. 7 (1967), pp. 189–196; Engl. transl. in U.S.S.R. Comp. Math. and Math. Phys. 7 (1) (1967), pp. 258–267.

IMPERIAL COLLEGE
London S. W. 7, England

Received on 11. 1. 1977 (908)

ACTA ARITHMETICA
XXXV (1979)

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

by

KIYOAKI IIMURA (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] F. 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:*

$$f = l^{u+v}\prod_i p_i \prod_j q_j,$$

where p_i and q_j are rational primes such that

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

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

$u = 1$ if $l|f$ and $l\nmid d$, $u = 0$ otherwise; and $v = 0$ or 1.

Furthermore the discriminant of L/Q is $d^{(l-1)/2}f^{l-1}$.

Our main result is:

THEOREM 1. *Let l be an odd prime number $\neq 3$. Let k be a quadratic extension of Q with discriminant d, and let K be a dihedral extension of 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 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 $q \equiv \left(\frac{d}{q}\right) = -1 \pmod{l}$. Let e be the fundamental unit of k when $d > 0$, and let $e = 1$ when $d < 0$. Let*

$$A_1 = \{q \in A \mid e \text{ is an } l\text{-th power residue } (\operatorname{mod} qO_k)\},$$

where 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 $l \mid d$ (resp. $\left(\frac{d}{l}\right) = -1$), let $B = \{l\}$ when e is an l-th power residue* (mod lO_k) *(resp.* mod l^2O_k), *and let B is empty when e is an l-th power nonresidue* (mod lO_k) *(resp. l^2O_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 $l \mid d$ and $l \in B$;*

(iv) *$f = lq$ if $l \mid d$, $l \notin B$, and q is any element of A_2;*

(v) *$f = l^2$ if $\left(\frac{d}{l}\right) = -1$ and $l \in B$;*

(vi) *$f = l^2q$ if $\left(\frac{d}{l}\right) = -1$, $l \notin B$, 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 $d \neq (-1)^{(l-1)/2}l$, and so does when $d < 0$ and $d \neq (-1)^{(l-1)/2}l$.* (Note that A is empty if $d = (-1)^{(l-1)/2}l$.)

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 or a ring on a module is expressed by exponentiation. Furthermore $(x^\sigma)^\tau = x^{\sigma\tau}$, and $\left(\frac{\ ,\ }{\ }\right)$ will denote the lth Hilbert symbol.

2. l-class groups of dihedral extensions. Let K be a dihedral extension of Q of degree $2l$, where l is an odd prime number. Let $\{\sigma, \tau\}$ be a set of generators of $\operatorname{Gal}(K/Q)$ with the relations $\sigma^l = \tau^2 = 1$, $\sigma\tau = \tau\sigma^{-1}$. Let k (resp. L) be the fixed field of $\langle\sigma\rangle$ (resp. $\langle\tau\rangle$). Then k/Q is quadratic and L/Q is non-Galois of degree l. Note that the subfields of K, except Q and K, are only k and l conjugates of L. For any finite algebraic extension F of Q, let $H(F)$ denote the l-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

$$H_i(K) = \{h \in H(K) \mid h^{(\sigma-1)^i} = 1\}$$

and

$$H_i(L) = \{h \in H_i(K) \mid h^\tau = h\}.$$

Then: $H_i(K)$ is a subgroup of $H(K)$ and is a $\boldsymbol{Z}[\operatorname{Gal}(K/Q)]$-module; $H_i(L)$ is a subgroup of $H(L)$ and $H_i(L) = H_i(K)^{1+\tau}$; $H_i(K) = H(K)$ for large i (cf. [5], 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 $H(L) = H(K)^{1+\tau}$ and $H(Q) = 1$.

Our first step in this section is to give information about the l-class group of K which contains L such that $H(L) = 1$. The following result is known (cf. [1], Proposition 3.9):

LEMMA 2. *If $H(L) = 1$, then there is no rational prime which decomposes in k and ramifies fully in L.*

Since $N(H(L)) = 1$, Proposition 4.1 of [4] applies to yield

$$H_{l-1}(L) = \{h \in H(L) \mid h^l = 1\},$$

from which it is clear that $H(L) = 1$ if and only if $H_{l-1}(L) = 1$. So we are now interested only in the group $H_{l-1}(L)$. Now we let, for $i = 1, 2, \ldots$

$$V_i = \langle H_i(L), H_{i-1}(K)\rangle$$

and

$$\tilde{V}_i = \{h \in H(K) \mid h^{(\sigma-1)} \in V_i\}.$$

Then it is easily checked that V_i and $\tilde{V}_i$ are both subgroups of $H(K)$ and $\boldsymbol{Z}[\operatorname{Gal}(K/Q)]$-modules for each $i \geqslant 1$. Also $H_{i-1}(K) \subset V_i \subset H_i(K)$ and $V_i \subset \tilde{V}_i \subset H_{i+1}(K)$.

LEMMA 3. *For all $i \geqslant 1$, there is an exact sequence*

$$1 \to \tilde{V}_i^{1-\tau} \to H_{i+1}(K) \xrightarrow{1+\tau} H_{i+1}(L) \to 1.$$

Proof. Since $H_{i+1}(K)$ is of course a $\boldsymbol{Z}_l[\tau]$-module, then

$$H_{i+1}(K) = H_{i+1}(L) \times H_{i+1}(K)^{1-\tau}$$

(cf. [2], proof of Lemma 2.1). So to show the exactness of the above sequence, it suffices to show that $\tilde{V}_i^{1-\tau} = H_{i+1}(K)^{1-\tau}$ for all $i \geqslant 1$. By definition $\tilde{V}_i \subset H_{i+1}(K)$, and so $\tilde{V}_i^{1-\tau} \subset H_{i+1}(K)^{1-\tau}$. Now let $h \in H_{i+1}(K)^{1-\tau}$. Then $h^{(\sigma-1)^{i+1}} = 1$ and $h^{\tau} = h^{-1}$. Now

$$h^{(\sigma-1)(\tau-1)} = h^{2-\sigma-\sigma^{-1}} = h^{-(\sigma^{(l-1)/2}-\sigma^{-(l-1)/2})^2} \in H_{i-1}(K) \cap H(K)^{1-\tau} = H_{i-1}(K)^{1-\tau}$$

since

$$(\sigma^{(l-1)/2} - \sigma^{-(l-1)/2})^2 \in (\sigma-1)^2 \boldsymbol{Z}[\sigma] \quad \text{and} \quad h^{(\sigma-1)^2} \in H_{i-1}(K).$$

On the other hand, since $h^{\sigma-1} \in H_i(K)$, there are $h_1 \in H_i(L)$, $h_2 \in H_i(K)^{1-\tau}$ such that $h^{\sigma-1} = h_1 h_2$. Then $h^{(\sigma-1)(\tau-1)} = h_2^{-2} \in H_{i-1}(K)^{1-\tau}$, which implies that $h_2 \in H_{i-1}(K)^{1-\tau}$. So $h^{\sigma-1} = h_1 h_2 \in H_i(L) H_{i-1}(K)^{1-\tau} \subset V_i$, which implies that $h \in \tilde{V}_i \cap H_{i+1}(K)^{1-\tau} = \tilde{V}_i^{1-\tau}$. So $\tilde{V}_i^{1-\tau} = H_{i+1}(K)^{1-\tau}$.

LEMMA 4. *For all $i \geqslant 1$, there is an exact sequence*

$$1 \to \tilde{V}_i^{1-\tau} \to \tilde{V}_i \xrightarrow{1+\tau} H_i(L) \to 1.$$

Proof. Since $\tilde{V}_i = \tilde{V}_i^{1+\tau} \times \tilde{V}_i^{1-\tau}$, it suffices to show that $\tilde{V}_i^{1+\tau} = H_i(L)$. Clearly $V_i^{1+\tau} = H_i(L)$, and so $\tilde{V}_i^{1+\tau} \supset H_i(L)$. Now let $h \in \tilde{V}_i$. Then $h^{\sigma-1} \in V_i$. Write $h^{\sigma-1} = h_1 h_2$ with $h_1 \in H_i(L)$, $h_2 \in H_{i-1}(K)$; then

$$\begin{aligned} h^{(1+\tau)(\sigma-1)^i} &= (h^{(1+\tau)(\sigma-1)})^{(\sigma-1)^{i-1}} = (h^{(\sigma-1)+(\sigma^{l-1}-1)\tau})^{(\sigma-1)^{i-1}} \\ &= (h_1 h_2)^{[1+(1+\sigma+\ldots+\sigma^{l-2})\tau](\sigma-1)^{i-1}} \\ &= h_1^{[1-\tau\sigma+(1+\sigma+\ldots+\sigma^{l-1})\tau](\sigma-1)^{i-1}} = h_1^{-(\sigma-1)^i} = 1 \end{aligned}$$

since $h_2 \in H_{i-1}(K)$ and $h_1^{1+\sigma+\ldots+\sigma^{l-1}} = N(h_1) \in N(H(L)) = 1$. So

$$h^{1+\tau} \in H_i(K) \cap H(L) = H_i(L),$$

which implies that $\tilde{V}_i^{1+\tau} \subset H_i(L)$.

LEMMA 5. *For all $i \geqslant 1$, $V_i/H_i(L) \cong H_{i-1}(K)/H_{i-1}(L)$.*

Proof. Since $H_{i-1}(K) \cap H_i(L) = H_{i-1}(L)$, then

$$\begin{aligned} V_i/H_i(L) &= \langle H_i(L), H_{i-1}(K)\rangle / H_i(L) \cong H_{i-1}(K)/(H_{i-1}(K) \cap H_i(L)) \\ &= H_{i-1}(K)/H_{i-1}(L). \end{aligned}$$

LEMMA 6. *For all integers $i \geqslant 1$, we have*

$$|H_{i+1}(K)/H_{i+1}(L)| = |\tilde{V}_i/V_i| \cdot |H_{i-1}(K)/H_{i-1}(L)|. \tag{2.1}$$

Proof. We have

$$\begin{aligned} |\tilde{V}_i^{1-\tau}| &= |H_{i+1}(K)/H_{i+1}(L)| \quad \text{(by Lemma 3)} \\ &= |\tilde{V}_i/H_i(L)| \quad \text{(by Lemma 4)} = |\tilde{V}_i/V_i|\,|V_i/H_i(L)| \\ &= |\tilde{V}_i/V_i|\,|H_{i-1}(K)/H_{i-1}(L)| \quad \text{(by Lemma 5)}. \end{aligned}$$

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

$$|H_i(K)/H_{i-1}(K)| = l^{t-1-r_i}|H(k)/N(H_{i-1}(K))|, \tag{2.2}$$

$$|\tilde{V}_i/V_i| = l^{t-1-r'_i}|H(k)/N(V_i)|, \tag{2.3}$$

where t denotes the number of primes of k which ramify in K, and r_i and r'_i for each $i \geqslant 1$, are both nonnegative rational integers whose precise definitions will be given after equation (2.6). Now in view of the definition of V_i, $N(H_i(L)) = 1$ implies that $N(V_i) = N(H_{i-1}(K))$ for all $i \geqslant 1$. Hence from equations (2.2) and (2.3),

$$|\tilde{V}_i/V_i| = l^{r_i-r'_i}|H_i(K)/H_{i-1}(K)|. \tag{2.4}$$

Equations (2.1) with $i = 1, 3, \ldots, l-2$ put together to give

$$|H_{l-1}(K)/H_{l-1}(L)| = \prod_{j=1}^{(l-1)/2} |\tilde{V}_{2j-1}/V_{2j-1}|. \tag{2.5}$$

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

$$|H_{l-1}(K)| = \prod_{i=1}^{(l-1)/2} |H_i(K)/H_{i-1}(K)|$$

then yield

$$|H_{l-1}(L)| = l^{\sum_{i=1}^{(l-1)/2}(r_{2i-1}-r'_{2i-1})} \prod_{j=1}^{(l-1)/2} |H_{2j}(K)/H_{2j-1}(K)|. \tag{2.6}$$

We now give the definitions of the numbers r_i and r'_i that appear in equations (2.2) and (2.3), following the results in [4], pp. 36–42.

Let $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_u$ (resp. $\mathfrak{A}'_1, \mathfrak{A}'_2, \ldots, \mathfrak{A}'_v$) be ideals of K (resp. L) which satisfy the following two conditions:

(C1) $H_{i-1}(K)$ (resp. $H_i(L)$) is generated by the ideal classes of the $\mathfrak{A}_j$'s (resp. the $\mathfrak{A}'_j$'s).

(C2) If we define $\mathfrak{F}$ (resp. $\mathfrak{F}'$) to be the ideal group generated by the $\mathfrak{A}_j$'s and their σ-conjugates (resp. the $\mathfrak{A}_j$'s, the $\mathfrak{A}'_j$'s, and their σ-conjugates), then $\mathfrak{F} \cap \mathfrak{F}(K)^{\sigma-1} = \mathfrak{F}^{\sigma-1}$ (resp. $\mathfrak{F}' \cap \mathfrak{F}(K)^{\sigma-1} = \mathfrak{F}'^{\sigma-1}$), where $\mathfrak{F}(K)$ denotes the group of fractional ideals of K whose ideal classes belong to $H(K)$.

Note that the ideal classes of the $\mathfrak{A}_j$'s and the $\mathfrak{A}'_j$'s generate V_i, and that $\mathfrak{F}$ and $\mathfrak{F}'$ are both $\boldsymbol{Z}[\sigma]$-modules. Let $\psi\colon k^* \to \mathfrak{F}_0(k)$ be the map defined by $\psi(\gamma) = (\gamma)$ for $\gamma \in k^* = k \setminus \{0\}$, where $\mathfrak{F}_0(k)$ denotes the group of principal fractional ideals of k; let $\Lambda = \psi^{-1}(N(\mathfrak{F}) \cap \mathfrak{F}_0(k))$ and $\Lambda' = \psi^{-1}(N(\mathfrak{F}') \cap \mathfrak{F}_0(k))$, where N is the norm map from ideals of K to ideals of k. Then Λ/Λ^l and Λ/Λ'^l, which may be viewed as vector spaces over $\boldsymbol{F}_l$, the finite field of l elements, are both of finite dimension, since $\mathfrak{F}$ and $\mathfrak{F}'$

are both finitely generated. So let $\{\alpha_j\}_{1\leqslant j\leqslant m}$ (resp. $\{\alpha'_j\}_{1\leqslant j\leqslant n}$) be a set of generators of the vector space Λ/Λ^l (resp. Λ/Λ'^l). Furthermore, let a be an element of the field $k(\zeta)$ such that $K(\zeta) = k(\zeta, \sqrt[l]{a})$, where ζ is a primitive lth root of unity; let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ be the primes of k which ramify in K; and let $\overline{\mathfrak{P}}$ be any prime of $k(\zeta)$ above $\mathfrak{p}_j$, $1\leqslant j\leqslant t$. Then we can define r_i and r'_i respectively to be the ranks of the matrices (over the finite field F_l)

$$(\beta_{j\nu}) \quad (1\leqslant j\leqslant m,\ 1\leqslant \nu\leqslant t)$$

and

$$(\beta'_{j\nu}) \quad (1\leqslant j\leqslant n,\ 1\leqslant \nu\leqslant t),$$

where

$$\zeta^{\beta_{j\nu}} = \left(\frac{\alpha_j,\ a}{\overline{\mathfrak{P}}_\nu}\right) \quad (1\leqslant j\leqslant m,\ 1\leqslant \nu\leqslant t),$$

$$\text{(2.7)} \qquad \zeta^{\beta'_{j\nu}} = \left(\frac{\alpha'_j,\ a}{\overline{\mathfrak{P}}_\nu}\right) \quad (1\leqslant j\leqslant n,\ 1\leqslant \nu\leqslant t).$$

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

Now if we choose a set of generators of Λ'/Λ'^l such that Λ/Λ^l is generated by one of its subsets (such a set does exist), we see at once from the definitions of r_i and r'_i that $r_i\leqslant r'_i$ for all $i\geqslant 1$. But in some special cases, for example, when $t\leqslant 1$ or when the condition of the next lemma is fulfilled, it occurs that $r_i = r'_i$ for all $i\geqslant 1$.

LEMMA 7. *Assume that there is no rational prime which decomposes in k and ramifies fully in L. Then $r_i = r'_i$ for all integers $i\geqslant 1$, and hence equation* (2.6) *becomes*

$$\text{(2.8)} \qquad |H_{l-1}(L)| = \prod_{j=1}^{(l-1)/2} |H_{2j}(K)/H_{2j-1}(K)|.$$

Furthermore, $H(L) = 1$ if and only if $|H_2(K)/H_1(K)| = 1$.

Proof. Note that a set $\{\alpha'_j\}_{1\leqslant j\leqslant n}$ of generators of Λ'/Λ' may be choosen so that, a subset $\{\alpha'_j\}_{1\leqslant j\leqslant m}$ generates Λ/Λ^l and α'_j is a rational number for $m+1\leqslant j\leqslant n$. Then the same argument as in the proof of [6], Lemma 3, shows that $\left(\frac{\alpha'_j,\ a}{\overline{\mathfrak{P}}_\nu}\right) = 1$ for $m+1\leqslant j\leqslant n$, $1\leqslant \nu\leqslant t$. Clearly this implies that $r_i = \bar{r}_i$ for each integer $i\geqslant 1$. The last result follows at once from equation (2.8) and the fact that $(\sigma-1)$ maps $H_{i+1}(K)/H_i(K)$ injectively into $H_i(K)/H_{i-1}(K)$ for all $i\geqslant 1$.

Our next step is to compute the order of $H_2(K)/H_1(K)$ under the assumption of Lemma 7. From equation (2.2),

$$|H_2(K)/H_1(K)| = l^{t-1-r_2}\big|H(k)/N\big(H_1(K)\big)\big|.$$

So we must consider the group $N\big(H_1(K)\big)$ and the number r_2. First we want to show that $N\big(H_1(K)\big) = H(k)^l$. Let $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_t$ be the primes of K which are ramified over k, and let $H'_1(K)$ be the subgroup of $H_1(K)$ generated by the image of $H(k)$ and the ideal classes of the $\mathfrak{P}_j^2$'s. Then $N\big(H'_1(K)\big) = H(k)^l$, since $N(\mathfrak{P}_j^2) = \mathfrak{P}_j^{2l}$ $(1\leqslant j\leqslant t)$ is principal in k. Also $H_1(K)/H'_1(K)$ is either trivial or cyclic of order l, and in the latter case there is an ideal of L the image in $H_1(K)/H'_1(K)$ of whose ideal class generates $H_1(K)/H'_1(K)$ (cf. [5], proof of Proposition 2 or [6], proof of Proposition 6). So in both cases $N\big(H_1(K)\big) = N\big(H'_1(K)\big) = H(k)^l$. Hence

$$\big|H(k)/N\big(H_1(K)\big)\big| = |H(k)/H(k)^l| = l^{r(k)},$$

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 $H_1(K)$ by taking appropriate ideals as the $\mathfrak{A}_j$'s with properties (C1) and (C2). Let $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_{r(k)}$ be ideals of k whose ideal classes generate $H(k)$, and let $\mathfrak{q}_i^{e_i} = (\pi_i)$ $(1\leqslant i\leqslant r(k))$, where $\pi_i\in k$ and e_i is the order of the ideal class of $\mathfrak{q}_i$ in $H(k)$. Let $p_1, p_2, \ldots, p_t$ be the rational primes which ramify fully in L; let $\mathfrak{A}$ be an ideal of L whose ideal class is contained in $H_1(K)\setminus H'_1(K)$ when $H_1(K)\neq H'_1(K)$; let $\mathfrak{A} = (1)$ when $H_1(K) = H'_1(K)$; and let a be a rational number such that $N(\mathfrak{A}) = (a)$. If we put $\mathfrak{A}_j = \mathfrak{q}_j$ for $1\leqslant j\leqslant r(k)$, $\mathfrak{A}_{r(k)+j} = \mathfrak{P}_j$ for $1\leqslant j\leqslant t$, and $\mathfrak{A}_{r(k)+t+1} = \mathfrak{A}$, then it is easy to see that these $\mathfrak{A}_j$'s satisfy conditions (C1) and (C2). Also the vector space Λ/Λ^l (over the finite field F_l) corresponding to these $\mathfrak{A}_j$'s, is generated by $\{e, p_1, p_2, \ldots, p_t, \pi_1, \pi_2, \ldots, \pi_{r(k)}, a\} = S$, where e 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 $\left(\frac{b, a}{\overline{\mathfrak{P}}_\nu}\right) = 1$ for $b = p_1, p_2, \ldots, p_t$, a and $1\leqslant \nu\leqslant t$, where $\overline{\mathfrak{P}}_\nu$ is any prime of $k(\zeta)$ above p_ν $(1\leqslant \nu\leqslant t)$, ζ is a primitive lth root of unity, and a is an element of $k(\zeta)$ such that $K(\zeta) = k(\zeta, \sqrt[l]{a})$ (cf. [6], proof of Lemma 3). Furthermore the product formula for the lth Hilbert symbol says that $\prod_{\nu=1}^{t}\left(\frac{\gamma,\ a}{\overline{\mathfrak{P}}_\nu}\right) = 1$ for all elements γ of S. Hence from these and equation (2.7), we get

$$r_2 = \operatorname{rank}(\beta_{j\nu}) \quad (1\leqslant j\leqslant r(k)+1,\ 1\leqslant \nu\leqslant t-1),$$

where

$$\zeta^{\beta_{j\nu}} = \left(\frac{\pi_j,\ a}{\overline{\mathfrak{P}}_\nu}\right) \quad \text{for} \quad 1\leqslant j\leqslant r(k),\ 1\leqslant \nu\leqslant t-1,$$

$$\text{(2.9)} \qquad \zeta^{\beta_{j\nu}} = \left(\frac{e,\ a}{\overline{\mathfrak{P}}_\nu}\right) \quad \text{for} \quad j = r(k)+1,\ 1\leqslant \nu\leqslant t-1.$$

We summarize these results in the following

Lemma 8. *With the assumptions of Lemma 7 and the above notations,*

$$|H_2(K)/H_1(K)| = l^{r(k)+t-1-r_2},$$

where r_2 *is the rank of the* $\big((r(k)+1)\times(t-1)\big)$*-matrix over the finite field* F_l *defined by equation* (2.9). (Note that $r_2 = 0$ when $t \leqslant 1$.)

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 $r(k)+t-1-r_2 = 0$. If $r(k) \geqslant 2$ (which means $H(k)$ is not cyclic), then

$$r(k)+t-1-r_2 \geqslant t+1-r_2 \geqslant t+1-t > 0,$$

which is a contradiction. So $r(k)$ must be 1 or 0. We first assume $r(k) = 1$, which means $H(k) \neq 1$ but is cyclic. Since $0 \leqslant r_2 \leqslant \max\{0, t-1\}$ by Lemma 8, it follows that

$$r(k)+t-1-r_2 = t-r_2 = 0 \Leftrightarrow t = 0,$$

in which case class field theory says that there is a unique cyclic extension K/k of degree l with conductor 1. Clearly such a field K is a dihedral extension of $\boldsymbol{Q}$ 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 $t \geqslant 1$. Then in Lemma 8, the number r_2 is the rank of the $\big(1\times(t-1)\big)$-matrix whose $1j$-th element β_{1j} is given by $\zeta^{\beta_{1j}} = \left(\dfrac{e,\,a}{\mathfrak{P}_j}\right)$. So $r_2 = 0$ or 1, and hence $r(k)+t-1-r_2 = 0 \Leftrightarrow t = 1$ (and $r_2 = 0$), or $t = 2$ and $r_2 = 1$. We note that if $t = 2$, the product formula for the lth Hilbert symbol implies that both of $\left(\dfrac{e,\,a}{\mathfrak{P}_1}\right)$ and $\left(\dfrac{e,\,a}{\mathfrak{P}_2}\right)$ 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 $q \equiv \left(\dfrac{d}{q}\right) = -1 \pmod{l}$, 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 $\left(\dfrac{e,\,a}{\mathfrak{Q}}\right) = 1$ (where $\mathfrak{Q}$ is any prime of $k(\zeta)$ above q) if and only if e is an lth power residue $(\bmod\ qO_k)$, or equivalently, q is contained in the set A_1 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* $l\,|\,d$;

(iv) $f = lq$ *if* $l\,|\,d$ *and* q *is any element of* A_2;

(v) $f = l^2$ *if* $\left(\dfrac{d}{l}\right) = -1$;

(vi) $f = l^2 q$ *if* $\left(\dfrac{d}{l}\right) = -1$ *and* q *is any element of* A_2.

It still remains to determine completely for which of the possible values of f listed in Lemma 9 there exists a dihedral extension $K/\boldsymbol{Q}$ 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 ζ be a primitive $2l$-th root of unity. Let $F = \boldsymbol{Q}(\zeta)$, $\tilde{F} = F\cdot k\,(= k(\zeta))$, and let F^+ be the maximal real subfield of F. We consider the case $d \neq (-1)^{(l-1)/2} l$, in which case there is only one quadratic subextension F' of $\tilde{F}/F^+$ other than F or F^+k, since the Galois group $G(\tilde{F}/F^+)$ is the four group. Now suppose $d > 0$, and let $N = \tilde{F}\sqrt[l]{e}$). Clearly $N/\boldsymbol{Q}$ is Galois. We want to show that $G(N/F')$ is cyclic of order $2l$. Let N_0 be a subfield of N which has degree l over F', and let $\tilde{\tau}$ be the generator of $G(N/N_0)$. Since the action of $\tilde{\tau}$ on k is the same as that of the generator of $G(k/\boldsymbol{Q})$, then $(\sqrt[l]{e})^{\tilde{\tau}} = \zeta^a(\sqrt[l]{e})^{-1}$ with $a \in \boldsymbol{Z}$. But $\sqrt[l]{e} = (\sqrt[l]{e})^{\tilde{\tau}^2} = \zeta^{-2a}\sqrt[l]{e}$, which implies $a \equiv 0 \pmod{l}$. So $(\sqrt[l]{e})^{\tilde{\tau}} = (\sqrt[l]{e})^{-1}$. Now let $\tilde{\sigma}$ be a generator of $G(N/\tilde{F})$, a cyclic group of order l, and let $(\sqrt[l]{e})^{\tilde{\sigma}} = \zeta^b\sqrt[l]{e}$, where $b \in \boldsymbol{Z}$. Then $(\sqrt[l]{e})^{\tilde{\sigma}\tilde{\tau}} = (\zeta^b\sqrt[l]{e})^{-1} = (\sqrt[l]{e})^{\tilde{\tau}\tilde{\sigma}}$, which implies $\tilde{\sigma}\tilde{\tau} = \tilde{\tau}\tilde{\sigma}$, and $G(N/F')$ is cyclic of order $2l$. The Tchebotarev density theorem then shows that the set of primes $\mathfrak{Q}_1$ (resp. $\mathfrak{Q}_2$) of N for which

$$G(N/N_0) = \left\langle\left[\frac{N/\boldsymbol{Q}}{\mathfrak{Q}_1}\right]\right\rangle \quad \left(\text{resp. } G(N/F') = \left\langle\left[\frac{N/\boldsymbol{Q}}{\mathfrak{Q}_2}\right]\right\rangle\right)$$

(where $\left[\dfrac{N/\boldsymbol{Q}}{}\right]$ is the Frobenius symbol) and which are unramified over $\boldsymbol{Q}$, has positive density. Setting $q_i = \mathfrak{Q}_i \cap \boldsymbol{Q}$ $(i = 1, 2)$, we easily see that q_i 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 $G(F/F')$ to obtain our result.

References

[1] T. Callahan, *Dihedral field extensions of order 2p whose class numbers are multiples of p*, Canad. J. Math. 28 (1976), pp. 429–439.
[2] F. Gerth, *On 3-class groups of pure cubic fields*, J. Reine Angew. Math. 278/279 (1975), pp. 52–62.
[3] — *Cubic fields whose class numbers are not divisible by* 3, Illinois J. Math. 20 (1976), pp. 486–493.
[4] G. Gras, *Sur les l-classes d'ideaux dans les extensions cycliques relatives de degré premier l*, Ann. Inst. Fourier 23, 3 (1973), pp. 1–48.
[5] — *Sur les l-classes d'idéaux des extensions non galoisiennes de Q de degré premier impair l à clôture galoisiennes diédrale de degré 2l*, J. Math. Soc. Japan 26 (1974), pp. 677–685.
[6] S. Kobayashi, *On the l-class rank in some algebraic number fields*, J. Math. Soc. Japan 26 (1974), pp. 668–676.
[7] J. Martinet, *Sur l'arithmétique des extensions Galoisiennes à groupe de Galois diédral d'ordre 2p*, Ann. Inst. Fourier 19, 1 (1969), pp. 1–80.

DEPARTMENT OF MATHEMATICS
TOKYO METROPOLITAN UNIVERSITY
2-1-1 Fukazawa, Setagaya-ku
Tokyo, Japan

Received on 18. 3. 1977 (923)

ACTA ARITHMETICA
XXXV (1979)

On 3-class groups of non-Galois cubic fields

by

KIYOAKI IIMURA (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 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 $(x^\sigma)^\tau = x^{\sigma\tau}$. The cubic Hilbert symbol $\left(\frac{a, b}{\mathfrak{p}}\right)$ used here corresponds to $(a, b)_\mathfrak{p}$ in [5].

1. A direct summand of the 3-class group. Let L be a non-Galois cubic extension field of Q, let K be the normal closure of L, and let k be the quadratic subfield of K. Let σ be a generator of the Galois group $G(K/k)$, and let τ be the generator of $G(K/L)$. Then $G(K/Q)$ is generated by $\{\sigma, \tau\}$ with the relations $\sigma^3 = \tau^2 = 1$, $\sigma\tau = \tau\sigma^2$. For any finite algebraic extension field F of 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

$$H_i(K) = \{h \in H(K) \mid h^{(\sigma-1)^i} = 1\}$$

and

$$H_i(L) = \{h \in H_i(K) \mid h^\tau = h\}.$$

Then $H_i(K)$ is a subgroup of $H(K)$ and is a $\mathbf{Z}[G(K/Q)]$-module; $H_i(L)$ is a subgroup of $H(L)$ and $H_i(L) = H_i(K)^{1+\tau}$; $H_i(K) = H(K)$ 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 $H(L) = H(K)^{1+\tau}$ and $H(Q) = \{1\}$.

Now we let H be a maximal direct summand of $H(L)$ contained in

$$H_1(L) = \{h \in H(K) \mid h^\sigma = h^\tau = h\}.$$