J. Math. Soc. Japan
Vol. 26, No. 4, 1974

On the l-class rank in some algebraic number fields

By Shinju KOBAYASHI

(Received May 12, 1973)

§0. Introduction.

The field in question is a non-Galois extension Ω of $\boldsymbol{Q}$ of prime degree $l>2$, with the following three conditions:

(i) The Galois closure K of Ω contains an absolutely cyclic subfield k with $[K:k]=l$.

(ii) The closure K is abelian over no proper subfield of k.

(iii) The class number h_k of k is prime to l.

Put $d=[k:\boldsymbol{Q}]=[K:\Omega]$. As is shown in [7], §1, the condition (ii) implies that $d \mid l-1$. For each divisor s of d, denote by Ω_S the intermediate field of K/Ω with $[K:\Omega_S]=s$. Furthermore, let C_K be the ideal class group of K and σ be a fixed generator of the Galois group $G(K/k)$. Define the integers $\nu_i \geqq 0$, $i=1, \cdots, l-1$, by $(C_K^{(1-\sigma)^{i-1}} C_K^l : C_K^{(1-\sigma)^i} C_K^l)=l^{\nu_i}$. The aim of this paper is to prove the following results.

THEOREM 1. *Notations and assumptions being as above, let* $\{p_i\}_{i=1}^t$ *be the set of all rational primes totally ramified in* Ω, *and* g_i, $i=1, \cdots, t$, *be the order of the decomposition group of* p_i *in* $k/\boldsymbol{Q}$. *Then, for each divisor* s *of* $g=(g_1, \cdots, g_t)$ (*the g.c.d. of* $g_1, \cdots, g_t$), *we have*

$$d^{(l)}C_{\Omega_S}=\sum_{j=1}^{(l-1)/s} \nu_{js},$$

where $d^{(l)}C_{\Omega_S}$ *denotes the l-rank of the ideal class group* C_{Ω_S} *of* Ω_S.

If g is equal to d in Theorem 1, we get $d^{(l)}C_\Omega$, and this leads to several consequences. On the one hand, we obtain $d^{(l)}C_\Omega=\nu_{l-1} \leqq \nu_1$ in the case $g=d=l-1$, and this seems to be a substantial upper bound for $d^{(l)}C_\Omega$. For, in this case, ν_1 can not exceed $t-1$, and we also know that $d^{(l)}C_\Omega \geqq t-r_\Omega$, where r_Ω denotes the number of infinite primes in Ω (cf. [8]).

On the other hand, we can show that $\nu_1=\nu_2$ when K is a dihedral extension and $g=2$. This gives, together with Theorem 1, the exact value of $d^{(3)}C_\Omega$ for certain non-Galois cubic fields Ω (Theorem 2, §4). It also enables us to get a generalization to the dihedral case of a theorem of Honda in [3], which states that $3 \mid h_\Omega$ if and only if $3 \mid h_K$ in the pure cubic case (Theorem 3, §5).

§§ 1 and 2 contain preliminary results and Theorem 1 is proved in § 3. We list below some notations used throughout this paper.

l: a fixed prime number >2.
$\boldsymbol{F}_l$: the finite field with l elements.
C_F: the ideal class group of a field F (we mean by a field exclusively a finite extension of $\boldsymbol{Q}$).
h_F: the class number of F.
$d^{(l)}C_F$: the l-rank of C_F.
E_F: the unit group of F.
$t_{F/E}$: the number of primes in E totally ramified in F (in fact, we use this only when $F/E=\Omega/\boldsymbol{Q}$ or K/k).
ζ_n: a primitive n-th root of 1.
$g=(g_1, \cdots, g_t)$: as defined in Theorem 1 ($t=t_{\Omega/\boldsymbol{Q}}$).

§ 1. A reduction step.

Let F/E be a cyclic extension of degree prime to l, and $\tilde{F}$ (resp. $\tilde{E}$) be the unramified abelian extension of F (resp. E) corresponding to C_F^l (resp. C_E^l) in the sense of class field theory. As $l \nmid [F:E]$, the following Proposition is obvious.

PROPOSITION 1. *Let F_0 be a subextention of $\tilde{F}/F$ which is Galois over E and E_0 be the maximal subextension of $\tilde{E}/E$ contained in F_0. Then E_0F is the fixed field of the commutator subgroup $[G(F_0/E), G(F_0/E)]$ of $G(F_0/E)$.*

Let F_0 be as in Proposition 1 and η be a fixed generator of $G(F/E)$. Then η operates on $H=G(F_0/F)$ through the inner automorphism $\rho \mapsto \eta\rho\eta^{-1}$ and $G(F_0/E)=H.\langle\eta\rangle$ (semi-direct product). Since H is a vector space of finite dimension over $\boldsymbol{F}_l$, η is represented by a matrix X over $\boldsymbol{F}_l$ w. r. t. a suitable basis of H. If we put (by identifying H with the space of column vectors over $\boldsymbol{F}_l$)

$$\bar{H}=\left\{\begin{pmatrix} I & \boldsymbol{a} \\ 0 & 1 \end{pmatrix} \middle| \, \boldsymbol{a} \in H\right\}, \qquad \bar{X}=\begin{pmatrix} X & 0 \\ 0 & 1 \end{pmatrix},$$

we see

$$\bar{X}\begin{pmatrix} I & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}\bar{X}^{-1}=\begin{pmatrix} I & X\boldsymbol{a} \\ 0 & 1 \end{pmatrix},$$

and hence we obtain $H \simeq \bar{H}$, $G(F_0/E) \simeq \bar{H}.\langle\bar{X}\rangle$ (semi-direct product) and

$$\left[X, \begin{pmatrix} I & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}\right]=\begin{pmatrix} I & (I-X^{-1})\boldsymbol{a} \\ 0 & 1 \end{pmatrix}.$$

It is easy to see that $[G(F_0/E), G(F_0/E)]$ is equal to $(X-I)H$, so we must know the rank of the matrix $X-I$. Let X_1 be the Jordan's normal form of

X. Then, as the order of X is prime to l, we see that the elements of X_1 just below the diagonal must be 0, i.e., X_1 is a diagonal matrix. This proves the following

PROPOSITION 2. *The rank of the elementary abelian l-group $G(E_0/E)$ is equal to the multiplicity of* 1 *appearing as an eigenvalue of X.*

§ 2. The descending central series.

Let k be a field with $l \nmid h_k$ and K/k be a cyclic extension of degree l. Fix a generator σ of $G(K/k)$. We have the following sequences of subgroups of C_K and of unramified abelian extensions over K corresponding to these ideal groups:

$$C_K \supset C_K^{1-\sigma} C_K^l \supset \cdots \supset C_K^{(1-\sigma)^{l-1}} C_K^l = C_K^l ,$$

$$K \subset K_1 \subset \cdots \subset K_{l-1} = \tilde{K} .$$

The equality on the right hand side is due to Proposition 1, [4], and K_1 is what we denoted by K_0 in [4]. Put $G = G(\tilde{K}/k)$ and define $G^{(i)}$, $i = 1, \cdots, l-1$, successively by

$$G^{(1)} = [G, G] , \qquad G^{(i+1)} = [G^{(i)}, G] .$$

PROPOSITION 3. $G(\tilde{K}/K_i) = G^{(i)}$.

PROOF. C_K/C_K^l is mapped isomorphically onto $G(\tilde{K}/K)$ by the Artin's reciprocity map $\left(\frac{\tilde{K}/K}{\quad}\right)$, and each $C_K^{(1-\sigma)^i} C_K^l / C_K^l$ corresponds to $G(\tilde{K}/K_i)$ under this isomorphism. The assertion being verified for $i=1$ by Proposition 2, [4], we assume inductively that $G(\tilde{K}/K_i) = G^{(i)}$. Then for any $c \in C_K$, we have

$$\left(\frac{\tilde{K}/K}{c^{(1-\sigma)^{i+1}}}\right) = \left[\tilde{\sigma}, \left(\frac{\tilde{K}/K}{c^{(1-\sigma)^i}}\right)\right] \in G^{(i+1)} ,$$

where we denoted by $\tilde{\sigma}$ an element of $G = G(\tilde{K}/k)$ extending $\sigma \in G(K/k)$. The inclusion $G^{(i+1)} \subset G(\tilde{K}/K_{i+1})$ is equally obvious (note that $\tilde{K}/K$ is abelian and $G^{(1)} \subset G(\tilde{K}/K)$). q. e. d.

PROPOSITION 4. *Let ν_i, $i = 1, \cdots, l-1$, be as defined in Theorem* 1. *Then l^{ν_i} is equal to the l-part of the index $(C_K^{(1-\sigma)^{i-1}} : C_K^{(1-\sigma)^i})$.*

PROOF. By Proposition 1, [4], the Sylow l-subgroup of $C_K/C_K^{(1-\sigma)^{l-1}}$ is elementary (i.e. of type $(l, \cdots, l)$). So it suffices to show that the map: $C_K^{(1-\sigma)^{i-1}} / C_K^{l(1-\sigma)^{i-1}} C_K^{(1-\sigma)^i} \rightarrow C_K^{(1-\sigma)^{i-1}} C_K^l / C_K^{(1-\sigma)^i} C_K^l$ is an isomorphism. The surjectivity is obvious. So let $c \in C_K^{(1-\sigma)^{i-1}} \cap C_K^l$, $c = c_1^l$, $c_1 \in C_K$. Then putting $a = (C_K^l : C_K^{(1-\sigma)^{l-1}})$, we get $c^a \in C_K^{(1-\sigma)^{l-1}}$, hence by $l \nmid a$, $c \in C_K^{l(1-\sigma)^{i-1}} C_K^{(1-\sigma)^i}$. q. e. d.

§ 3. Inertia generators.

Let Ω, K, and k satisfy the conditions (i) to (iii) in § 0, and σ and τ be fixed generators of $G(K/k)$ and $G(K/\Omega)$ respectively. We have a relation $\tau\sigma\tau^{-1}=\sigma^{r}$ for some $r\in \boldsymbol{Z}$, and the condition (ii) implies that $d=[k:\boldsymbol{Q}]$ is equal to the order of $r \bmod l$ (cf. [7], § 1). In order to carry out the procedure described in § 1, we have to find suitable generators for $H=G(\tilde{K}/K)$. But as we have seen in § 2, H has the following sequence of subspaces:

$$H\supset G^{(1)}\supset\cdots\supset G^{(l-1)}=\{1\},$$

(where we put $G=G(\tilde{K}/k)$), and each $G^{(i)}$ is invariant under τ. So, in fact, it suffices to find convenient generators for each of the factor spaces $G^{(i)}/G^{(i+1)}$.

This is done exactly as in [5]. Namely, $G(K_1/k)$ is an elementary l-extension. For each prime $\mathfrak{p}$ in k, ramified in K, denote by $T_{\mathfrak{p}}$ the inertia group of $\mathfrak{p}$ in $G(K_1/k)$. They are all of order l, and by the assumption $l\nmid h_k$, their composite coincides with $G(K_1/k)$. So we can choose a basis $\{\sigma_1,\cdots,\sigma_m\}$ of $G(K_1/k)$ such that each σ_i is a generator of some $T_{\mathfrak{p}}$. Extend σ_i to an element of $G=G(\tilde{K}/k)$ and use the same symbol. Then, by the theory of p-groups, $\{\sigma_1,\cdots,\sigma_m\}$ is a minimal system of generators of G.

LEMMA 1. *$H/G^{(1)}$ is generated by $\sigma_j\sigma_{j+1}^{-1}$, $j=1,\cdots,m-1$ (with a suitable choice of σ_j's).*

PROOF. The same as we stated in [5], § 3. $H/G^{(1)}$ is an $(m-1)$-dimensional subspace of $G(K_1/k)$ and is defined by a linear equation $\sum_{j=1}^{m}c_jx_j\equiv 0 \pmod{l}$ for the exponents x_j of σ_j. Each $c_j\not\equiv 0 \pmod{l}$, so replacing σ_j by a suitable power of it, we can assume that $c_j\equiv 1 \pmod{l}$, $j=1,\cdots,m$. q. e. d.

LEMMA 2. *For $i\geqq 2$, $G^{(i-1)}/G^{(i)}$ is generated by the elements of the form*

$$[\sigma_{j_1},\cdots,\sigma_{j_i}].$$

PROOF. As G is generated by $\sigma_1,\cdots,\sigma_m$ and $G(\tilde{K}/K)$ is abelian, we have only to show that the i-variable function $[x_1,\cdots,x_i] \bmod G^{(i)}$ is "multilinear". The assertion being verified easily by a direct computation for $i=2$, we assume it to be valid for $i-1$. Then

$$\begin{aligned}[x_1,\cdot,x_ix_i'] &= [[x_1,\cdot,x_{i-1}],x_i'][[x_1,\cdot,x_{i-1}],x_i][[x_1,\cdot,x_{i-1}],x_i,x_i'] \\ &\equiv [x_1,\cdot,x_i][x_1,\cdot,x_i'] \mod G^{(i)}.\end{aligned}$$

For $a<i$, by the induction hypothesis,

$$\begin{aligned}&[x_1,\cdot,x_ax_a',\cdot,x_i] \\ &\quad=[[x_1,\cdot,x_ax_a',\cdot,x_{i-1}],x_i] \\ &\quad=[[x_1,\cdot,x_a,\cdot,x_{i-1}][x_1,\cdot,x_a',\cdot,x_{i-1}]y,x_i]\end{aligned}$$

$$=[[\cdot, x_a, \cdot][\cdot, x'_a, \cdot], x_i][[\cdot, x_a, \cdot][\cdot, x'_a, \cdot], x_i, y][y, x_i]$$
$$\equiv[[\cdot, x_a, \cdot], x_i][[\cdot, x_a, \cdot], x_i, [\cdot, x'_a, \cdot]][[\cdot, x'_a, \cdot], x_i]$$
$$\equiv[\cdot, x_a, \cdot, x_i][\cdot, x'_a, \cdot, x_i] \mod G^{(i)},$$

where $y\in G^{(i-1)}$. q. e d.

PROOF OF THEOREM 1. Put $d=sn$. Then $G(K/\Omega_S)=\langle\tau^n\rangle$ and we can apply the procedure given in § 1 to $F/E=K/\Omega_S$, $F_0=\tilde{K}$. By the assumption that $s\,|\,g$, $g=(g_1, \cdots, g_t)$, $\tau^n\langle\sigma_j\rangle\tau^{-n}=\langle\sigma_j\rangle$ in $G(K_1/k)$, hence we can put $\tau^n\sigma_j\tau^{-n}=\sigma_j^{a_j}x_j$, $x_j\in G^{(1)}$. Apply this on K. Since σ_j is non-trivial on K, the relation $\tau^n\sigma\tau^{-n}=\sigma^{r^n}$ implies the same for σ_j and we get $a_j=r^n$. Now on $H/G^{(1)}$,

$$\tau^n(\sigma_j\sigma_{j+1}^{-1})\tau^{-n}\equiv(\sigma_j\sigma_{j+1}^{-1})^{r^n} \mod G^{(1)}.$$

On $G^{(i-1)}/G^{(i)}$, $i\geqq 2$,

$$\tau^n[\sigma_{j1}, \cdots, \sigma_{ji}]\tau^{-n}\equiv[\sigma_{j1}, \cdots, \sigma_{ji}]^{rin} \mod G^{(i)}.$$

For this we note that the function $[\cdot, \cdots, \cdot]$ is "multilinear" and $[x_1, \cdot, [y, y'], \cdot, x_i]\equiv[[x_1, \cdot, y, \cdot, x_i], [x_1, \cdot, y', \cdot, x_i]]\equiv 1 \mod G^{(i)}$. On each $G^{(i-1)}/G^{(i)}$, therefore, τ^n is represented by a scalar matrix and its eigen-value is r^{in}, which is $\equiv 1 \pmod l$ if and only if $i\equiv 0 \pmod s$. q. e. d.

§ 4. Calculation of ν_1 and ν_2 in the dihedral case.

In this section, we assume $d=2$ in the conditions (i) to (iii), so $G(K/\boldsymbol{Q})$ is a dihedral group of order $2l$ and k is a quadratic field. Define the integer δ by $(E_k : E_k\cap N_{K/k}(K^\times))=l^\delta$. Then we have two cases:

Case (A): $\delta=0$, i. e., k is real and the fundamental unit ε_0 of k belongs to $N_{K/k}(K^\times)$, or $l=3$, $k=\boldsymbol{Q}(\sqrt{-3})$ and $\zeta_3\in N_{K/k}(K^\times)$, or k is imaginary and either $l\neq 3$ or $k\neq\boldsymbol{Q}(\sqrt{-3})$.

Case (B): $\delta=1$.

Then by Satz 13, [2], we get

PROPOSITION 5. $\nu_1=t_{K/k}-1-\delta$.

As for ν_2, by Proposition 4, § 2, it is equal to the exponent of the l-part of the index $(C_K^{1-\sigma} : C_K^{(1-\sigma)^2})=|C_K^{1-\sigma}\cap C_K^G|$, where C_K^G is the subgroup of $G=G(K/k)$-invariant classes in K. So we must find the Sylow l-subgroup of $C_K^{1-\sigma}\cap C_K^G$. As we have seen in [5], an ideal $\mathfrak{a}$ in K belongs to $C_K^{1-\sigma}$ if and only if $N_{K/k}(\mathfrak{a})$ is a principal ideal generated by an element of $N_{K/k}(K^\times)$.

From now on, we assume $g=(g_1, \cdots, g_t)=2$. We first study the subgroup D_K of C_K^G generated by G-invariant ideals in K. Let $p_1, \cdots, p_t$, $t=t_{\Omega/\boldsymbol{Q}}=t_{K/k}$, be the rational primes totally ramified in Ω. If l is among them, we put $p_t=l$. For each p_i, let $\mathfrak{P}_i$ be the prime factor of p_i in K. If $p_t=l$, denote the prime factors of l in k and K by $\mathfrak{l}$ and $\mathfrak{L}$ respectively, and put $\mathfrak{P}_t=\mathfrak{L}^e$, where e is the ramification index of l in $k/\boldsymbol{Q}$. Then the Sylow l-subgroup of D_K is generated by $\mathfrak{P}_1,\cdots,\mathfrak{P}_t$ (cf. [7], Satz V, VI).

LEMMA 3. *If* $g=2$, $\mathfrak{P}_i$, $i=1,\cdots,t$, *belong to* $C_K^{1-\sigma}$.

PROOF. We take p_i as a generator of $N_{K/k}(\mathfrak{P}_i)$. Put $\boldsymbol{Q}'=\boldsymbol{Q}(\zeta_l)$, $k'=k(\zeta_l)$, $K'=K(\zeta_l)$, and $K'=k'(\sqrt[l]{\alpha})$, $\alpha\in k'^{\times}$. By virtue of the results in [1], Chapter III, $p_i\in N_{K/k}(K^{\times})$ if and only if $p_i\in N_{K'/k'}(K'^{\times})$, and furthermore, the Hilbert's norm residue symbol $\left(\frac{p_i,\alpha}{\mathfrak{P}'}\right)$ defined in k' depends only on the prime in k under $\mathfrak{P}'$. In particular, we have only to check the symbol for those $\mathfrak{P}'$'s in k' not dividing l (the number of prime factors of l in k' is either 1 or 2). Since (p_i) is a norm from K, the symbol equals to 1 except for the $\mathfrak{P}'$'s ramified in K'/k', i.e., $\mathfrak{P}'\mid p_j$ for some j. Note that $p_i\equiv -1 \pmod{l}$ if $p_i\neq l$ (Satz V, VI, [7]). Now we have three cases:

a) k is not contained in $\boldsymbol{Q}'$.

b) $l\equiv 3 \pmod 4$ and $k=\boldsymbol{Q}(\sqrt{-l})\subset\boldsymbol{Q}'$.

c) $l\equiv 1 \pmod 4$ and $k=\boldsymbol{Q}(\sqrt{l})\subset\boldsymbol{Q}'$.

But in c), $p_i\neq l$ are necessarily decomposed in k and hence we can exclude this case (if no $p_i\neq l$ exists, we have $t=1$, $C_K^g=\{1\}$, and the assertion is trivial). In case a), let $k=\boldsymbol{Q}(\sqrt{m})$ and put $\tilde{k}=\boldsymbol{Q}((\zeta_l-\zeta_l^{-1})\sqrt{m})$. In case b), put $\tilde{k}=\boldsymbol{Q}(\zeta_l+\zeta_l^{-1})$. In both cases, we can find $\alpha\in\tilde{k}^{\times}$ such that $K'=k'(\sqrt[l]{\alpha})$ (cf. [6], Chapter IV). Apply the automorphism of $G(k'/\tilde{k})$ on $\left(\frac{p_i,\alpha}{\mathfrak{P}'}\right)$, $\mathfrak{P}'\mid p_j$. Then it leaves invariant p_i, α and also $\mathfrak{P}'$. In fact, by the assumption $g=2$, we can easily see that $\mathfrak{P}'$ is inert in $k'/\tilde{k}$. But the automorphism maps ζ_l to ζ_l^{-1}. Hence we must have $\left(\frac{p_i,\alpha}{\mathfrak{P}'}\right)=1$. q.e.d.

PROPOSITION 6. *If $G(K/\boldsymbol{Q})$ is a dihedral group of order $2l$ and $g=2$, we have $\nu_1=\nu_2$.*

PROOF. If $C_K^g=D_K$, the assertion is already proved by Lemma 3. By the formula (7) in the proof of Satz 13, [2], $(C_K^g:D_K)=1$ or l, and it is equal to l if and only if k is real, $\delta=0$ and $\varepsilon_0\notin N_{K/k}(E_K)$, or $l=3$, $k=\boldsymbol{Q}(\sqrt{-3})$, $\delta=0$ and $\zeta_3\notin N_{K/k}(E_K)$. The latter case has already been finished in [5], and the former is done exactly by the same argument. Namely, let c be an element of C_K^g not contained in D_K and choose an ideal $\mathfrak{a}$ in c. Since $N_{K/k}(\mathfrak{a}^{1+\tau})=N_{K/\boldsymbol{Q}}(\mathfrak{a})$ is generated by a rational number, we have only to show that $\mathfrak{b}=\mathfrak{a}^{1+\tau}$ again belongs to C_K^g but not to D_K (cf. Proof of Lemma 3). Put $\mathfrak{a}^{1-\sigma}=(\beta)$, $\beta\in K^{\times}$. Then $N_{K/k}(\beta)=\pm\varepsilon_0^x$, $x\not\equiv 0 \pmod{l}$. If we can write $\mathfrak{b}=\mathfrak{b}_1\beta_1$ with $\mathfrak{b}_1^{1-\sigma}=(1)$, $\beta_1\in K^{\times}$, we get $\beta^{1+(1+\sigma+\cdots+\sigma^{l-2})\tau}=\varepsilon\beta_1^{1-\sigma}$, $\varepsilon\in E_K$, hence $N_{K/k}(\beta)^{1+(l-1)\tau}=N_{K/k}(\varepsilon)$, which is a contradiction, since $\varepsilon_0^{\tau}=\pm\varepsilon_0^{-1}$. q.e.d.

THEOREM 2. *If $G(K/\boldsymbol{Q})$ is isomorphic to the symmetric group of degree* 3,

$3 \nmid h_k$ *and* $g=(g_1, \cdots, g_t)=2$, *we have*

$$d^{(3)}C_{\Omega}=\nu_1, \qquad d^{(3)}C_K=2\nu_1.$$

PROOF. Immediate from Theorem 1 and Proposition 6.

REMARK. In the course of preparation of this paper, Mr. G. Gras has communicated to me another proof of Theorem 2. His proof is based on a more general study of l-class groups in dihedral extensions (without the assumption (iii) in § 0).

§ 5. A generalization of a Theorem of Honda.

We first assume that Ω, K, and k satisfy only the conditions (i) and (ii) in § 0.

PROPOSITION 7. *If a prime number* $p \neq l$ *totally ramified in* Ω *is completely decomposed in* k, h_{Ω} *is divisible by* l.

PROOF. By Satz V, [7], we have $p \equiv 1 \pmod{l}$. Let M_p be the unique cyclic extension of $\boldsymbol{Q}$ of degree l contained in $\boldsymbol{Q}(\zeta_p)$. Then $\Omega M_p/\Omega$ is an unramified cyclic extension of degree l. In fact, $\Omega M_p/\Omega$ is unramified outside p. So let $\mathfrak{P}$ be a prime factor of p in M_pK. Then $\mathfrak{P}$ is ramified in $\Omega M_p/\Omega \Longleftrightarrow \mathfrak{P}$ is ramified in M_pK/K. But $\mathfrak{P}$ is already ramified in K/k and it can not be totally ramified in M_pK/k. Hence $\mathfrak{P}$ is unramified in $\Omega M_p/\Omega$. q. e. d.

Now we can prove the announced result.

THEOREM 3. *If* $G(K/\boldsymbol{Q})$ *is a dihedral group of order* $2l$ *and* $l \nmid h_k$, $l \mid h_{\Omega}$ *if and only if* $l \mid h_K$.

PROOF. The "only if" part is obvious and we show that $l \mid h_{\Omega}$ if $l \mid h_K$. If either $g=(g_1, \cdots, g_t)=2$, or there exists a rational prime $p \neq l$ which is totally ramified in Ω and decomposed in k, Theorem 1 with Proposition 6 or Proposition 7 proves the assertion. So assume that $p_1, \cdots, p_{t-1}$ and l are totally ramified in Ω and only l is decomposed in k, and put $l=\mathfrak{l}_1\mathfrak{l}_2$ in k. In particular, $k \neq \boldsymbol{Q}(\sqrt{-3})$ if $l=3$. In case (A) (cf. § 4), we apply the Propositions 1 and 2 to $F/E=K/\Omega$ and $F_0=K_1$. Let σ and τ be generators of $G(K/k)$ and $G(K/\Omega)$ as before. We have $\tau\sigma\tau^{-1}=\sigma^{-1}$. Denote generators of the inertia groups of $p_1, \cdots, p_{t-1}, \mathfrak{l}_1, \mathfrak{l}_2$ in $G(K_1/k)$ by $\sigma_1, \cdots, \sigma_{t-1}, \rho_1, \rho_2=\tau\rho_1^{-1}\tau^{-1}$. They make a basis of $G(K_1/k)$ and we can assume that $G(K_1/K)$ is generated by $\sigma_1\sigma_2^{-1}, \cdots, \sigma_{t-1}\rho_1^{-1}, \rho_1\rho_2^{-1}$ (cf. Lemma 1. Note that if $G(K_1/K)$ is defined by the linear equation $\sum_{i=1}^{t-1} c_ix_i+ay+bz \equiv 0 \pmod{l}$ for the exponents x_i, y, z of σ_i, ρ_1, ρ_2, we have $a \equiv b \pmod{l}$. In fact, we can assume that $\rho_1|K=\sigma$, which gives $\rho_2|K=\sigma$. By the equation above, we see $\rho_1^b\rho_2^{-a} \in G(K_1/K)$, hence $\sigma^{b-a}=id.$). The matrix X representing τ w. r. t. this basis has the form

$$\left(\begin{array}{ccc|cc} -1 & & & & \\ & \ddots & & & 0 \\ & & -1 & & \\ \hline & & & -1 & 0 \\ & 0 & & & \\ & & & -1 & 1 \end{array}\right).$$

So by Proposition 2, we get $l \mid h_{\boldsymbol{Q}}$.

In case (B), we can use the same procedure if ρ_1 and ρ_2 are linearly independent in $G(K_1/k)$. If not, we can apply the argument used in the proof of Theorem 1, and we have to show that $\nu_2>0$ if $\nu_1>0$, i.e., if $t \geqq 2$. Let $\mathfrak{P}_1, \cdots, \mathfrak{P}_{t-1}, \mathfrak{L}_1, \mathfrak{L}_2$ be the prime factors of $p_1, \cdots, p_{t-1}, \mathfrak{l}_1, \mathfrak{l}_2$ in K, and let e be the order of $\mathfrak{l}_i$ in C_k. Then the Sylow l-subgroup of $C_K^G = D_K$ is generated by $\mathfrak{P}_1, \cdots, \mathfrak{P}_{t-1}, \mathfrak{L}_1^e, \mathfrak{L}_2^e$. Just as in Lemma 3, $\mathfrak{P}_1, \cdots, \mathfrak{P}_{t-1}, \mathfrak{L}_1^e \mathfrak{L}_2^e$ belong to $C_K^{1-\sigma}$ (since l is decomposed in k, k is not contained in $\boldsymbol{Q}(\zeta_l)$ and we are in case a) of Lemma 3). So if $\mathfrak{L}_1^e \mathfrak{L}_2^e \not\sim 1$ in K, we get $\nu_2>0$. Suppose $\mathfrak{L}_1^e \mathfrak{L}_2^e \sim 1$. Then the Sylow l-subgroup of C_K^G is generated by $\mathfrak{P}_1, \cdots, \mathfrak{P}_{t-1}$ and $\mathfrak{L}_1^e$. Hence some $\mathfrak{P}_i$ must be non-principal if $t \geqq 3$. If $t=2$, put $\mathfrak{l}_1^e = (\lambda)$, $\lambda \in k^\times$. Case (B) means that k is real and $\varepsilon_0 \notin N_{K/k}(K^\times)$. Then we can choose a power of ε_0 such that $\varepsilon_0^x \lambda \in N_{K/k}(K^\times)$ $\Big($because the only norm residue symbol to be checked is $\left(\frac{\varepsilon_0^x \lambda, \alpha}{\mathfrak{P}'}\right)$, $\mathfrak{P}' \mid p_1$ in k' and we have $\left(\frac{\varepsilon_0, \alpha}{\mathfrak{P}'}\right) \neq 1$ by $\delta=1\Big)$. Hence $\mathfrak{P}_1$ and $\mathfrak{L}_1^e$ belong to $C_K^{1-\sigma}$ and $\nu_2>0$. q.e.d.

REMARK. As $\nu_1 \geqq \cdots \geqq \nu_{l-1}$, we see that $l \mid h_K$ if and only if $\nu_1>0$.

References

[1] G. Gras, Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l, to appear in Ann. Inst. Fourier.

[2] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Ia, Jber. Deutsch. Math.-Verein., **36** (1927), 231–311.

[3] T. Honda, Pure cubic fields whose class numbers are multiples of 3, J. Number Theory, **3** (1971), 7–12.

[4] S. Kobayashi, On the l-dimension of the ideal class groups of Kummer extensions of a certain type, J. Fac. Sci. Univ. Tokyo Sec. IA, **18** (1971), 399–404.

[5] S. Kobayashi, On the 3-rank of the ideal class groups of certain pure cubic fields, to appear ibid.

[6] J. Martinet, Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre 2p, Ann. Inst. Fourier, **19** (1969), 1–80.

[7] J. Porusch, Die Arithmetik in Zahlkörpern, deren zugehörige Galoissche Körper spezielle metabelsche Gruppen bezitzen, auf klassenkörpertheoretischer Grundlage, Math. Z., **37** (1933), 134–160.

[8] P. Roquette and H. Zassenhaus, A class rank estimate for algebraic number fields, J. London Math. Soc., 44 (1969), 31-38.

Shinju KOBAYASHI
Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Fukazawa, Setagaya-ku
Tokyo, Japan