TOKYO J. MATH.
VOL. 1, No. 2, 1978

Construction of Number Fields with Prescribed l-class Groups

Osamu YAHAGI

Waseda University

Let G be a finite abelian l-group, where l is a prime number, and k be an arbitrary number field. The purpose of this paper is to show that for each prime number l which does not divide the class number of k, there exist infinitely many algebraic extensions of k whose l-class groups are isomorphic to G (cf. Theorem and its Corollary). F. Gerth III [1] solved this problem under the conditions that G is any finite elementary abelian l-group and k is the field $\boldsymbol{Q}$ of rational numbers. We extend his result to the general case where the group G is any finite abelian l-group.

§1. Preliminaries.

Throughout this paper, l will denote a fixed prime number and k will denote a number field whose class number is prime to l (by a number field we shall always mean a finite extension of the field $\boldsymbol{Q}$ of rational numbers). For an arbitrary number field L, let S_L and E_L denote the l-class group of L (i.e., the Sylow l-subgroup of the ideal class group of L) and the group of units in L, respectively. For a Galois extension M/L of finite degree, $G(M/L)$ denotes its Galois group and $[\mathfrak{P}, M/L]$ denotes the Frobenius symbol for a prime ideal $\mathfrak{P}$ of M in M/L. Especially, if M/L is an abelian extension, $(\mathfrak{a}, M/L)$ denotes the Artin symbol for an ideal $\mathfrak{a}$ of L in M/L. For a finite abelian group $\bar{G}$ and a natural number n, we shall denote by $|\bar{G}|$ its order and put $\bar{G}^n=\{g^n; g\in\bar{G}\}$. Let Z/l^nZ be the cyclic group of order l^n and ζ_n a primitive n-th root of unity. Furthermore, we use the following notations:

$h=h_k$: the class number of k;

$\mathfrak{O}$: the ring of integers of k:

$(\mathfrak{O}/\mathfrak{M})^\times$: the multiplicative group of the residue class ring $\mathfrak{O}/\mathfrak{M}$, where $\mathfrak{M}$ is an integral ideal of k;

$k(n)=k(\{\zeta_{l^{n+s}}, \sqrt[l^n]{\varepsilon_i}; 1\leqq i\leqq r\})$, where l^s is the order of the group of l-

Received March 4, 1978

power-th roots of unity in k, and $\{\varepsilon_i;\ 1 \leqq i \leqq r\}$ is a system of fundamental units in k. For example, $k(n)=k(\zeta_{l^{n+\delta}})$ if $k=\boldsymbol{Q}$ or an imaginary quadratic field. Let $\bar{F}$ be a cyclic extension of k of degree l^n, and let τ be a generator of the cyclic group $G(\bar{F}/k)$. We put $S_{\bar{F}}^{1-\tau}=\{c^{1-\tau};\ c \in S_{\bar{F}}\}$, $S_{\bar{F}}^{(\tau)}=\{c \in S_{\bar{F}};\ c^{\tau}=c\}$ and $S_{\bar{F}\,s}^{(\tau)}=\{c \in S_{\bar{F}};\ c$ contains an ideal $\mathfrak{a}$ of $\bar{F}$ such that $\mathfrak{a}^{\tau}=\mathfrak{a}\}$.

LEMMA 1. *Notation being as above, let K be the maximal abelian l-extension of k contained in the genus field of $\bar{F}/k$.*

Then: (1) *The Artin map gives an isomorphism*:

$$S_{\bar{F}}/S_{\bar{F}}^{1-\tau} \xrightarrow{\ \sim\ } G(K/\bar{F})\ .$$

$$(2) \qquad |S_{\bar{F}}^{(\tau)}| = |S_{\bar{F}}/S_{\bar{F}}^{1-\tau}| = \frac{\tilde{\prod} e(\mathfrak{p})}{l^n \cdot [E_k : E_k \cap N_{\bar{F}/k}(\bar{F}^{\times})]}\ ,$$

where $\tilde{\prod} e(\mathfrak{p})$ is the product of the ramification indices of all the finite and the infinite prime divisors in k with respect to $\bar{F}/k$, and $N_{\bar{F}/k}$ is the norm map from $\bar{F}$ to k.

For the proof, see Yokoi [4], pp. 35 and 37.

LEMMA 2. *Notations being as in Lemma* 1, *define the map φ: $S_{\bar{F}}^{(\tau)} \to S_{\bar{F}}/S_{\bar{F}}^{1-\tau}$ so that the following diagram is commutative.*

$$\begin{array}{ccc} S_{\bar{F}}^{(\tau)} & \xrightarrow{\ \textit{inclusion}\ } & S_{\bar{F}} \\ & \varphi \searrow \quad \circlearrowleft & \Big\downarrow \textit{canonical surjection} \\ & & S_{\bar{F}}/S_{\bar{F}}^{1-\tau} \end{array}$$

Then the following conditions are equivalent:

(1) *φ is surjective.*

(2) *φ is injective.*

(3) $S_{\bar{F}}=S_{\bar{F}}^{(\tau)}$.

In these cases, we have $S_{\bar{F}}=S_{\bar{F}}^{(\tau)} \cong S_{\bar{F}}/S_{\bar{F}}^{1-\tau} \cong G(K/\bar{F})$.

PROOF. From the exact sequence $1 \to S_{\bar{F}}^{(\tau)} \to S_{\bar{F}} \xrightarrow{f} S_{\bar{F}} \to S_{\bar{F}}S_{\bar{F}}^{1-\tau} \to 1$, where the first map is the natural inclusion, the second map f is defined by $f(c)=c^{1-\tau}$ for $c \in S_{\bar{F}}$ and the third map is the canonical surjection, we see that $S_{\bar{F}}^{(\tau)}$ and $S_{\bar{F}}/S_{\bar{F}}^{1-\tau}$ have the same order; hence the equivalence of (1) and (2) is clear. It is obvious that (3) implies (1). Now suppose that φ is surjective; then $S_{\bar{F}}=S_{\bar{F}}^{(\tau)}S_{\bar{F}}^{1-\tau}=S_{\bar{F}}^{(\tau)}S_{\bar{F}}^{(1-\tau)^2}= \cdots =S_{\bar{F}}^{(\tau)}S_{\bar{F}}^{(1-\tau)^{l^n}}$. On the other hand, l divides $(1-\tau)^{l^n}$. Hence $S_{\bar{F}}=S_{\bar{F}}^{(\tau)}S_{\bar{F}}^{l}$, i.e., $S_{\bar{F}}=S_{\bar{F}}^{(\tau)}$.

LEMMA 3. *Let m be an integer $\geqq 1$ and $\mathfrak{p}$ a prime ideal of k. Then the following three conditions are equivalent:*

(1) *There exists a unique cyclic extension of k of degree l^m in the Strahl class field modulo $\mathfrak{p}$.*

(2) $|(\mathfrak{O}/\mathfrak{p})^\times/(E_k+\mathfrak{p}/\mathfrak{p})|$ *is divisible by l^m.*

(3) *The prime ideal $\mathfrak{p}$ is prime to l and splits completely in the Galois extension $k(m)/k$.*

PROOF. Let $\overline{k(\mathfrak{p})}$ be the Strahl class field modulo $\mathfrak{p}$. Set

$I_\mathfrak{p}=\{\mathfrak{a};\ \mathfrak{a}$ is an ideal of k and $(\mathfrak{a}, \mathfrak{p})=1\}$,

$P_\mathfrak{p}=\{(a);\ (a)$ is a principal ideal generated by $a\in k$ and $((a), \mathfrak{p})=1\}$,

$S_\mathfrak{p}=\{(a);\ (a)$ is a principal ideal generated by $a\in k$ and $a\equiv 1(\mathrm{mod}^\times \mathfrak{p})\}$,

where $\mathrm{mod}^\times\ \mathfrak{p}$ means the multiplicative congruence. By class field theory, $I_\mathfrak{p}/S_\mathfrak{p}$ is isomorphic to $G(\overline{k(\mathfrak{p})}/k)$. On the other hand, it contains the subgroup $P_\mathfrak{p}/S_\mathfrak{p}$ of index h which is prime to l by our assumption. Hence the Galois group of the maximal abelian l-extension of k contained in $\overline{k(\mathfrak{p})}$ over k, is isomorphic to the Sylow l-subgroup of $P_\mathfrak{p}/S_\mathfrak{p}$. For a class $a \bmod \mathfrak{p}\in(\mathfrak{O}/\mathfrak{p})^\times$, put $f(a \bmod \mathfrak{p})=(a)\in P_\mathfrak{p}/S_\mathfrak{p}$, where (a) is the principal ideal generated by a. Then the map $f\colon(\mathfrak{O}/\mathfrak{p})^\times\to P_\mathfrak{p}/S_\mathfrak{p}$ is a well defined, surjective homomorphism and

$$\mathrm{Ker}\,(f)=\{a \bmod \mathfrak{p}\in(\mathfrak{O}/\mathfrak{p})^\times;\ a\equiv\varepsilon(\mathrm{mod}\ \mathfrak{p})\ \text{for some}\ \varepsilon\in E_k\}\,.$$

Therefore we have the equivalence of (1) and (2).

(2)$\Rightarrow$(3): Let $k_\mathfrak{p}$ be the completion of k with respect to $\mathfrak{p}$. If we assume (2), we have $\zeta_{l^m}\in k_\mathfrak{p}$, since $N\mathfrak{p}\equiv 1(\mathrm{mod}\ l^m)$ (where $N\mathfrak{p}$ is the absolute norm of the prime ideal $\mathfrak{p}$). And the equation $x^{l^m}\equiv\varepsilon(\mathrm{mod}\ \mathfrak{p})$ is solvable in $\mathfrak{O}$ for all $\varepsilon\in E_k$, since the group $(\mathfrak{O}/\mathfrak{p})^\times$ is a cyclic group. Therefore the equation $x^{l^m}=\varepsilon$ is solvable in $k_\mathfrak{p}$ for all $\varepsilon\in E_k$, since $(l, \mathfrak{p})=1$; this implies (3).

(3)$\Rightarrow$(2): Conversely suppose (3). Then $N\mathfrak{p}\equiv 1(\mathrm{mod}\ l^{m+\delta})$, since $\zeta_{l^{m+\delta}}\in k_\mathfrak{p}$ and $(l, \mathfrak{p})=1$; and all $\varepsilon\in E_k$ are l^m-th power residues modulo $\mathfrak{p}$, since the equation $x^{l^m}=\varepsilon$ is solvable in the ring of $\mathfrak{p}$-adic integers in $k_\mathfrak{p}$. Therefore we have (2).

REMARK. There exist infinitely many prime ideals of k which satisfy the above condition. In fact, there exist infinitely many rational primes which split completely in $k(m)$.

COROLLARY. *For a fixed integer $n\geqq 1$, there exist infinitely many cyclic extensions of k of degree l^n whose class numbers are not divisible by l.*

PROOF. By the above remark, we have infinitely many cyclic extensions of k of degree l^n in which one and only one prime ideal ramifies. Then their class numbers are not divisible by l, since the class number of k is prime to l (see Iwasawa [3]).

§2. Construction.

Let $e_1, e_2, \cdots, e_i, \cdots, e_{t+1}$ be natural numbers such that $1 \leqq e_1 \leqq e_2 \leqq \cdots \leqq e_i \leqq \cdots \leqq e_{t+1}$; let $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_i, \cdots, \mathfrak{p}_{t+1}$ be distinct prime ideals of k such that $|(\mathfrak{O}/\mathfrak{p}_i)^\times/(E_k+\mathfrak{p}_i/\mathfrak{p}_i)|$ is divisible by l^{e_i} for each i. Note that in the case $k=\boldsymbol{Q}$, this condition is equivalent to the one that $p_i \equiv 1 \pmod{2 \cdot l^{e_i}}$, where p_i is a prime number such that $(p_i)=\mathfrak{p}_i$.

Put $e_{t+1}=n$ and let k_i, $i=1, 2, \cdots, t+1$, be the unique cyclic extension of k of degree l^{e_i} in the Strahl class field modulo $\mathfrak{p}_i$. Let $K=\prod_{i=1}^{t+1} k_i$ be the composite of the fields k_i, $i=1, 2, \cdots, t+1$. $G(K/k)$ is the direct product of the cyclic groups $G(k_i/k)$, $i=1, 2, \cdots, t+1$. In the following, we restrict ourselves to the case $t \geqq 1$. (When $t=0$, Corollary of Lemma 3 says that the l-class group of each intermediate field of K/k is trivial.)

Let σ_i be a fixed generator of $G(k_i/k)$ and let H be the subgroup of $G(K/k)$ generated by $\{\sigma_i \cdot \sigma_{t+1}^{l^{n-e_i}}; 1 \leqq i \leqq t\}$. Then the factor group $G(K/k)/H$ is a cyclic group of order l^n, and $\{\sigma_{t+1}^j; 0 \leqq j \leqq l^n-1\}$ is a full set of representatives for the cosets modulo H in $G(K/k)$. Hence the subfield F of K corresponding to H is a cyclic extension of k of degree l^n. On the other hand, the inertia group of $\mathfrak{p}_i$ for K/k is $\langle \sigma_i \rangle$ and $\sigma_i \equiv \sigma_{t+1}^{-l^{n-e_i}} \pmod{H}$. Therefore ramification theory shows that the ramified primes of F/k are $\mathfrak{p}_i$, $i=1, 2, \cdots, t+1$, with ramification index l^{e_i}. Moreover K is an unramified abelian extension of F, since $H \cap \langle \sigma_i \rangle = \{1\}$ holds for all $i=1, 2, \cdots, t+1$. Therefore it follows from Lemma 1 that K coincides with the maximal abelian l-extension of k contained in the genus field of F/k, since the degree of K over F is $\prod_{i=1}^{t} l^{e_i}$.

In the following, F always denotes the subfield of K which corresponds to H. We call this field F *the field associated with* the set of primes $\{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{t+1}\}$. For the field F, we give a condition for S_F to be equal to $S_{F,s}^{(r)}$. Let $K_i=k_i \cdot F$, $1 \leqq i \leqq t$, be the composite of the field k_i and the field F. Then we have $K=\prod_{i=1}^{t} K_i$ (the composite of K_i, $i=1, 2, \cdots, t$), and $G(K/F)$ is the direct product of the cyclic groups $G(K_i/F)$, $i=1, 2, \cdots, t$.

LEMMA 4. *For each prime ideal $\mathfrak{p}_i$ such that $e_i<n$, the following conditions are equivalent:*

(1) *There exists only one prime ideal of F above $\mathfrak{p}_i$.*

(2) $((\prod_{\mathfrak{P}|\mathfrak{p}_i}\mathfrak{P})^h, K_i/F)$ *generates* $G(K_i/F)$, *where* $(\ , K_i/F)$ *is the Artin symbol in* K_i/F *and the product is taken over all the prime ideals* $\mathfrak{P}$ *of* F *above* $\mathfrak{p}_i$.

PROOF. Let Z (resp. T) be the decomposition group (resp. the inertia group) of $\mathfrak{p}_i$ for the abelian extension K_i/k. $G(K_i/k)$ is the direct product of $G(K_i/F)$ and $G(K_i/k_i)$, since $e_i<n$. Let σ (resp. ρ) be a generator of $G(K_i/F)$ (resp. $G(K_i/k_i)$). Then T is a cyclic group, since $(l, \mathfrak{p}_i)=1$. The ramification index of $\mathfrak{p}_i$ in F/k (resp. k_i/k) is l^{e_i} (resp. l^{e_i}). So, after replacing σ and ρ if necessary, we may assume that T is generated by $\sigma\cdot\rho^{l^{n-e_i}}$. Now suppose (1); then $Z\cdot G(K_i/F)=G(K_i/k)$, so we have $\rho=\sigma^c\cdot z$ for some integer c and some $z\in Z$. From the fact that $T=\langle\sigma\cdot\rho^{l^{n-e_i}}\rangle\subset Z$ it follows that

$$\sigma^{1+cl^{n-e_i}}=\sigma\cdot\rho^{l^{n-e_i}}\cdot z^{-l^{n-e_i}}\in Z\ ,$$

which implies that $\sigma\in Z$, since $n>e_i$. Hence we have $Z=G(K_i/k)$, i.e., there exists only one prime ideal of K_i above $\mathfrak{p}_i$. This implies that $(\mathfrak{P}^h, K_i/F)$ generates $G(K_i/F)$, since K_i/F is an unramified abelian l-extension.

To prove (2)$\Rightarrow$(1), let $\mathfrak{P}_j$, $1\leqq j\leqq l^s$, be the prime ideals of F above $\mathfrak{p}_i$; then $\mathfrak{P}_j=\mathfrak{P}^{\sigma_j}$ holds for some $\sigma_j\in G(K_i/k)$, $1\leqq j\leqq l^s$. Hence $(\mathfrak{P}_j, K_i/F)=(\mathfrak{P}_1, K_i/F)$, $1\leqq j\leqq l^s$, and therefore we have $((\prod_{\mathfrak{P}|\mathfrak{p}_i}\mathfrak{P})^h, K_i/F)=(\mathfrak{P}_1^h, K_i/F)^{l^s}$, from which it is clear that (2) implies that $l^s=1$.

REMARK. The condition (1) is equivalent to the one that there exists only one prime ideal of F_0 above $\mathfrak{p}_i$, where F_0 is the subfield of F of degree l over k.

Through the isomorphism $S_F/S_F^{1-\tau}\cong G(K/F)\cong\prod_{i=1}^t G(K_i/F)$, we may assume that the image of φ is contained in $\prod_{i=1}^t G(K_i/F)$ (see Lemma 2). It is well known that $S_{F,s}^{(\tau)}$ is generated by $\prod_{\mathfrak{P}|\mathfrak{p}_i}\mathrm{cl}\,(\mathfrak{P})^h$, $1\leqq i\leqq t+1$, where the product is taken over all the prime ideals $\mathfrak{P}$ of F above $\mathfrak{p}_i$ and $\mathrm{cl}\,(\mathfrak{P})$ denotes the ideal class of the prime ideal $\mathfrak{P}$. The factor group $\prod_{i=1}^t G(K_i/F)/(\prod_{i=1}^t G(K_i/F))^l$ can be regarded as a vector space over the finite field with l elements; hence the classes of $\varphi(\prod_{\mathfrak{P}|\mathfrak{p}_i}\mathrm{cl}\,(\mathfrak{P})^h)$, $1\leqq i\leqq t+1$, determine a matrix M whose (i, j)-th element is $((\prod_{\mathfrak{P}|\mathfrak{p}_i}\mathfrak{P})^h, K_j/F)$ $\mathrm{mod}\, G(K_j/F)^l$, $1\leqq i\leqq t+1$, $1\leqq j\leqq t$ (cf. Gerth [1]).
Therefore: $\mathrm{rank}\, M=t\Leftrightarrow\varphi(S_{F,s}^{(\tau)})=S_F/S_F^{1-\tau}\Leftrightarrow S_F=S_F^{(\tau)}=S_{F,s}^{(\tau)}(\cong\prod_{i=1}^t G(K_i/F)$ (see Lemma 2)).

We are now ready to prove the following

Theorem. *Let G be a finite abelian l-group with exponent l^m, $m \geqq 0$. Then, for all n, $n \geqq m$, $n \geqq 1$, there exist infinitely many cyclic extensions of k of degree l^n whose l-class groups are isomorphic to the group G.*

Proof. If $m=0$, the statement is equivalent to Corollary of Lemma 3; hence we may assume that $m \geqq 1$. By the structure theorem for finite abelian groups, we may assume that G is the direct sum of the cyclic groups $\boldsymbol{Z}/l^{e_i}\boldsymbol{Z}$, $i=1, 2, \cdots, t$; $1 \leqq e_1 \leqq e_2 \leqq \cdots \leqq e_t = m$. To prove the theorem, it is sufficient, by the above arguments, to find infinitely many sets of $t+1$ prime ideals $\{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{t+1}\}$ of k such that rank $M=t$. In fact, in this case, $S_F \cong \prod_{i=1}^t G(K_i/F) \cong G$, where F is, as before, a cyclic extension of k *associated with* $\{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{t+1}\}$. We will consider two cases separately. In the following conditions on $\mathfrak{p}_i$, π_i denotes an integer of $\mathfrak{O}$ such that $\mathfrak{p}_i^h = (\pi_i)$ and C_i denotes the cyclic group $(\mathfrak{O}/\mathfrak{p}_i)^\times/(E_k + \mathfrak{p}_i/\mathfrak{p}_i)$.

i) Case $n>m$. The conditions on $\{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{t+1}\}$ are

(1) $|C_{t+1}|$ is divisible by l^n,

(2) $|C_i|$ is divisible by l^{e_i} $(1 \leqq i \leqq t)$ and

(3) The class of each π_i, $1 \leqq i \leqq t$, in the cyclic group C_{t+1} is not contained in C_{t+1}^l.

Remark. The condition (3) is equivalent to saying that each $\mathfrak{p}_i$, $1 \leqq i \leqq t$, is not decomposed in the unique cyclic extension $(k_{t+1})_0$ of k of degree l, contained in the Strahl class field modulo $\mathfrak{p}_{t+1}$: in fact (cf. the proof of Lemma 3),

the condition (3)$\Leftrightarrow((\pi_i), (k_{t+1})_0/k) \neq 1 \Leftrightarrow (\mathfrak{p}_i, (k_{t+1})_0/k) \neq 1$.

By putting $e_{t+1}=n$, let F be a cyclic extension of k of degree l^n *associated with* the above set of prime ideals, and let F_0 be, as before, subfield of F of degree l over k. Then we easily see that $F_0 = (k_{t+1})_0$, since F_0 is contained in $\prod_{i=1}^{t+1} k_i$, and since only $\mathfrak{p}_{t+1}$ ramifies in F_0/k. On the other hand, if we identify $G(K_j/F)$ with $G(k_j/k)$, $j=1, 2, \cdots, t$, we have, by the translation theorem, $((\prod_{\mathfrak{P}|\mathfrak{p}_i} \mathfrak{P})^h, K_j/F) = (\mathfrak{p}_i, k_j/k)^{hl^{n-e_i}}$ for every $i \neq j$. Therefore, for each prime ideal $\mathfrak{p}_i$ such that $e_i < n$, an (i, j)-th element of the matrix M is trivial (cf. [1]) whenever $j \neq i$. Also Lemma 4 shows that for such a prime ideal $\mathfrak{p}_i$, an (i, i)-th element is trivial if and only if $\mathfrak{p}_i$ is decomposed in F_0. Therefore, by the above remark, we see that rank $M=t$. Existence of such a set of prime ideals can be seen as follows. Let $\mathfrak{p}$ be a prime ideal of k which satisfies the condition (1) and put $\mathfrak{p}_{t+1} = \mathfrak{p}$. Then we have $k(e_t) \cap k_{t+1} = k$, since $\mathfrak{p}_{t+1}$ is unramified in $k(e_t)$ by the definition of $k(e_t)$. Hence the Galois group $G(k_{t+1}k(e_t)/k)$ is the direct product of the subgroups $G(k_{t+1}k(e_t)/k(e_t))$ and $G(k_{t+1}k(e_t)/k_{t+1})$; the former subgroup is a cyclic one of order l^n. Therefore the

Tschebotarev density theorem shows that there exist infinitely many prime ideals $\mathfrak{P}_i$ of $k_{t+1}k(e_i)$ for which

$$\langle[\mathfrak{P}_i, k_{t+1}k(e_i)/k]\rangle = G(k_{t+1}k(e_i)/k(e_i)) .$$

It is easy to see that $\mathfrak{p}_i = \mathfrak{P} \cap k$ satisfies both conditions (2) and (3), since $\mathfrak{p}_i$ splits completely in $k(e_i)$ and since $[\mathfrak{P}_i, k_{t+1}k(e_i)/k]_{|k_{t+1}} = (\mathfrak{p}_i, k_{t+1}/k)$ generates the Galois group $G(k_{t+1}/k)$. Hence we can obtain distinct prime ideals $\mathfrak{p}_i$, $1 \leqq i \leqq t+1$, of k which satisfy the above conditions (1)-(3). Infiniteness is also deduced from the density theorem.

ii) Case $n=m$. Put $e_{t+1}=n$, and let d be the largest integer i such that $e_i<n$ (if $e_1=e_2=\cdots=e_t=n$, put $d=1$). Take any prime ideal $\mathfrak{p}_d$ of k such that $|C_d|$ is divisible by l^{e_d}; and then take distinct prime ideals $\mathfrak{p}_{d+1}, \mathfrak{p}_{d+2}, \cdots, \mathfrak{p}_{t+1}$ of k which satisfy the following conditions. The conditions on $\mathfrak{p}_{d+1}$ are

(1) $|C_{d+1}|$ is divisible by l^n,

(2) The class of π_{d+1} in C_d is not contained in C_d^l.

Assume that we can choose prime ideals $\mathfrak{p}_d, \mathfrak{p}_{d+1}, \cdots, \mathfrak{p}_{d+j}$ ($j \geqq 1$). The conditions on $\mathfrak{p}_{d+j+1}$ are

(3) $|C_{d+j+1}|$ is divisible by l^n,

(4) The class of π_{d+j+1} in C_{d+j} is not contained in C_{d+j}^l,

(5) The class of π_{d+j+1} in C_{d+i} is contained in $C_{d+i}^{l^n}$ for all $i=0, 1, \cdots, j-1$.

If $d \geqq 2$, we choose $d-1$ distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{d-1}$ of k which satisfy the following conditions:

(6) $|C_i|$ is divisible by $l^{e_i}(1 \leqq i \leqq d-1)$.

(7) The class of each π_i, $1 \leqq i \leqq d-1$, in C_{d+1} is not contained in C_{d+1}^l.

(8) The class of each π_i, $1 \leqq i \leqq d-1$, in C_{d+j} is contained in $C_{d+j}^{l^n}$ for all $j=2, 3, \cdots, t-d+1$.

Existence of such a set of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{t+1}$ can be seen as follows. By the same arguments as in the case $n>m$, existence of $\mathfrak{p}_{d+1}$ is easily verified. We note here that the condition (2) is equivalent to

(2)′ The Artin symbol $(\mathfrak{p}_{d+1}, k_d/k)$ generates $G(k_d/k)$.

Assume now that we can choose prime ideals $\mathfrak{p}_d, \mathfrak{p}_{d+1}, \cdots, \mathfrak{p}_{d+j}$ ($j \geqq 1$). By the density theorem, there exist infinitely many prime ideals $\mathfrak{P}_{d+j+1}$ of $k(n) \cdot (\prod_{i=0}^{j} k_{d+i})$ (the composite of the field $k(n)$ and the fields k_{d+i}, $i=0, 1, \cdots, j$) for which

$$\left\langle\left[\mathfrak{P}_{d+j+1}, k(n) \cdot \left(\prod_{i=0}^{j} k_{d+i}\right)\Big/k\right]\right\rangle = G\left(k(n) \cdot \left(\prod_{i=0}^{j} k_{d+i}\right)\Big/k(n)\left(\prod_{i=0}^{j-1} k_{d+i}\right)\right) .$$

Then $\mathfrak{p}_{d+j+1} = \mathfrak{P}_{d+j+1} \cap k$ satisfies the conditions (3)-(5), since the conditions

(4) and (5) are equivalent respectively to

(4)′ The Artin symbol $(\mathfrak{p}_{d+j+1}, k_{d+j}/k)$ generates $G(k_{d+j}/k)$, and

(5)′ The Artin symbol $(\mathfrak{p}_{d+j+1}, k_{d+i}/k)$ is equal to 1 for all $i=0, 1, \cdots, j-1$.

Therefore existence of $\mathfrak{p}_d, \mathfrak{p}_{d+1}, \cdots, \mathfrak{p}_{t+1}$ is proved. Now suppose that $d\geqq 2$. Again the density theorem shows that there exist infinitely many prime ideals $\mathfrak{P}_i$ of $k(e_i)\cdot(\prod_{j=d+1}^{t+1} k_j)$ (the composite for the field $k(e_i)$ and the fields k_j, $d+1\leqq j\leqq t+1$) for which

$$\left\langle\left[\mathfrak{P}_i, k(e_i)\left(\prod_{j=d+1}^{t+1} k_j\right)\Big/k\right]\right\rangle=G\left(k(e_i)\left(\prod_{j=d+1}^{t+1} k_j\right)\Big/k(e_i)\left(\prod_{j=d+2}^{t+1} k_j\right)\right).$$

We also see that $\mathfrak{p}_i=\mathfrak{P}_i\cap k$ satisfies the conditions (6)-(8). Hence we can obtain $t+1$ distinct prime ideals $\mathfrak{p}_i$, $1\leqq i\leqq t+1$, of k.

Let F be a cyclic extension of k of degree l^n as in the case $n>m$ *associated with* the set of prime ideals $\{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{t+1}\}$. For this field F, we shall show that rank $M=t$. As before, if we identify $G(K_j/F)$ with $G(k_j/k)$, $1\leqq j\leqq t$, then we have $((\prod_{\mathfrak{P}|\mathfrak{p}_i}\mathfrak{P})^h, K_j/F)=(\mathfrak{p}_i, k_j/k)^{hl^{n-e_i}}$ for every $i\neq j$. Therefore, by the conditions (2)′, (4)′, and (5)′, theorem is easily verified for the case of $d=1$. For the case $d\geqq 2$, we shall show that each $\mathfrak{p}_i$, $1\leqq i\leqq d-1$, is not decomposed in F_0. As the ramified primes in F_0/k are $\mathfrak{p}_{d+1}, \mathfrak{p}_{d+2}, \cdots, \mathfrak{p}_{t+1}$, F_0 is contained in $\prod_{j=d+1}^{t+1} k_j$. Therefore, if $\mathfrak{p}_i$ splits in F_0/k for some $i=1, 2, \cdots, d-1$, then F_0 is contained in the decomposition field for $\mathfrak{p}_i$ in $\prod_{j=d+1}^{t+1} k_j$. On the other hand, by the conditions (7) and (8), the decomposition field for $\mathfrak{p}_i$ is $\prod_{j=d+2}^{t+1} k_j$; but this implies that $\mathfrak{p}_{d+1}$ is unramified in F_0/k. Hence we have a contradiction. Now it is easy to see, as in the case $d=1$, that the rank of the matrix M is equal to t. As there exist infinitely many fields such as F, the proof of the theorem is completed.

REMARK. If we restrict ourselves to the case $k=\boldsymbol{Q}$, our theorem is also deduced by using the results of A. Fröhlich [5]. However it is still necessary to specify the prime numbers as in our paper, which is kindly pointed out by Mr. K. Iimura while I was preparing this paper.

COROLLARY. *Let G be the same as in Theorem. Then there exist infinitely many non-Galois extensions of the field $\boldsymbol{Q}$ of rational numbers whose l-class groups are isomorphic to the group G.*

PROOF. As before, let k be a number field, other than $\boldsymbol{Q}$, whose class number is prime to l; e.g., $k=\boldsymbol{Q}(\sqrt{2})$. From the proof of Theorem, it is easy to see that the primes $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{t+1}$ can be choosen so that the following additional conditions are satisfied; there exists some $1 \leqq i \leqq t+1$ such that the prime number p_i lying below $\mathfrak{p}_i$, splits completely in k, and that each $\mathfrak{p}_j$, $j \neq i$, $1 \leqq j \leqq t+1$, is not lying above p_i. Now let F be the field *associated with* such primes $\mathfrak{p}_i$, $1 \leqq i \leqq t+1$. Then it is clear that $F/\boldsymbol{Q}$ is a non-Galois extension; and by Theorem we have $S_F \cong G$. Since there exist infinitely many sets of $t+1$ prime ideals $\{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{t+1}\}$ with the property above, we get immediately the assertion of Corollary.

SUPPLEMENTARY NOTE. While preparing this paper, K. Iimura informed me that for each odd prime number l, there exist infinitely many dihedral extensions K of $\boldsymbol{Q}$ of degree $2 \cdot l^m$, with the following property: For all subfields L of K of degree l^m, S_L are isomorphic to the group G; here $l^m (m \geqq 1)$ denotes the exponent of G.

References

[1] F. GERTH III, Number fields with prescribed l-class group, Proc. Amer. Math. Soc., **49** (1975), 284–288.

[2] H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Ia, Physica-Verlag, 1970.

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

[4] H. YOKOI, On the class number of a relatively cyclic number field, Nagoya Math. J., **29** (1967), 31–44.

[5] A. FRÖHLICH, The generalization of a therem of L. Redei's, Quart. J. Math., **5** (1954), 130–140.

Present Address:
DEPARTMENT OF MATHEMATICS
SCHOOL OF SCIENCE AND ENGINEERING
WASEDA UNIVERSITY
NISHIOKUBO, SHINJUKU-KU, TOKYO 160