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 $\boldsymbol{Z}/l^n\boldsymbol{Z}$ 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