J. Math. Soc. Japan
Vol. 30, No. 4, 1978

On the p-class groups of a Galois number field and its subfields

By Kiichiro OHTA

(Received May 14, 1977)

§ 1. Introduction.

In general, let k be an algebraic number field of finite degree, and let p be a rational prime number. Then, the p-Sylow subgroup of the absolute ideal class group of k will be called the p-class group of k and will be denoted by $C_{k,p}$, whose order will be denoted by $h_{k,p}$. Moreover, let K be a Galois extension over k. Then, the subgroup of all ideal classes of $C_{K,p}$ which are ambigous with respect to K/k will be called the ambigous p-class group of K with respect to k and will be denoted by $A_{k,p}$, whose order will be denoted by $a_{k,p}$.

First, we shall deal with the case where K is a Galois extension of degree mn over k such that the Galois group $G=G(K/k)$ satisfies the following condition:

(A) G has a normal subgroup N of order n and n subgroups $H_1, H_2, \cdots, H_n$ of same order m such that we have $G=NH_1=\cdots=NH_n$ and $H_i \cap H_j=\{\varepsilon\}$ for $i \neq j$, where we denote by ε the unit element of G.

If the Galois group $G(K/k)$ satisfies above condition (A), then K will be called the (A)-extension over k. For example, it is clear that K is an (A)-extension over k if the Galois group $G(K/k)$ is isomorphic to one of the following groups:

(a) the non-abelian group of order pq where p and q are rational prime numbers such that $q \equiv 1 \pmod p$,

(b) the abelian group of type (p, p),

(c) the dihedral group,

(d) the Galois group $G(\boldsymbol{Q}(\zeta_q, a^{1/q})/\boldsymbol{Q})$, where q is an odd prime number, ζ_q is a primitive q-th root of unity and a is a rational integer such that $a^{1/q} \notin \boldsymbol{Q}(\zeta_q)$.

Now, our main theorem is as following. Namely:

THEOREM 1. *Let k be an algebraic number field of finite degree and let K be an* (A)*-extension over k. Let $F, L_1, \cdots, L_n$ be the subfields of K corresponding respectively to the subgroups $N, H_1, \cdots, H_n$ of the Galois group $G(K/k)$ by the Galois theory. Then, if the class number h_K of K is divisible by a rational prime number p prime to n, then the p-class group $C_{K,p}$ of K is generated by its sub-*