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-*

groups $A_{F,p}$, $A_{L_1,p}$, $\cdots$, $A_{L_n,p}$. *Moreover, if* p *is also prime to* m, *then we have*

$$C_{K,p}/A_{k,p}=A_{F,p}/A_{k,p}\times<A_{L_1,p}, \cdots, A_{L_n,p}>/A_{k,p}.$$

Finally, in § 3, using above theorem we shall prove some interesting results concerning with the p-class group $C_{K,p}$ of K when K is an S_n-extension over k, that is, when the Galois group $G(K/k)$ is isomorphic to the symmetric group S_n of degree n.

§ 2. p-class groups of (A)-extensions.

First, we shall prove the following group-theoretic lemma, from which our main theorem follows easily.

LEMMA. *Let* G *be a finite group of order* mn *such that it satisfies the condition* (A). *Let* $\mathfrak{M}$ *be a finite* G*-module such that each element of* $\mathfrak{M}$ *has the finite order prime to* n *and assume that if* a *is an element of* $\mathfrak{M}$ *and we have* $\sigma a=a$ *for any* $\sigma\in G$, *then we have* $a=0$. *Then, if we put*

$$\mathfrak{N}=\{a\in\mathfrak{M} \mid \sigma a=a,\ \forall\sigma\in N\},$$

$$\mathfrak{H}_i=\{a\in\mathfrak{M} \mid \sigma a=a,\ \forall\sigma\in H_i\}, \qquad (i=1, 2, \cdots, n),$$

then we have

$$\mathfrak{M}=\mathfrak{N}+\mathfrak{H}_1+\cdots+\mathfrak{H}_n. \tag{1}$$

Moreover, if the order of each element of $\mathfrak{M}$ *is also prime to* m, *then we have the direct sum as following:*

$$\mathfrak{M}=\mathfrak{N}\oplus(\mathfrak{H}_1+\cdots+\mathfrak{H}_n). \tag{2}$$

Particularly, if $m=n$ *and all* H_i $(i=1, 2, \cdots, n)$ *are also normal subgroups of* G, *then* $\mathfrak{M}$ *is perfectly decomposed into the direct sum as following:*

$$\mathfrak{M}=\mathfrak{N}\oplus\mathfrak{H}_1\oplus\cdots\oplus\mathfrak{H}_n. \tag{3}$$

PROOF. Let us put

$$N=\{\varepsilon, \alpha_1, \cdots, \alpha_{n-1}\},$$

$$H_i=\{\varepsilon, \beta_{i1}, \cdots, \beta_{i\,m-1}\} \qquad (i=1, 2, \cdots, n)$$

and define $n+1$ endomorphisms $\varphi, \psi_1, \cdots, \psi_n$ of $\mathfrak{M}$ by

$$\varphi(a)=a+\alpha_1 a+\cdots+\alpha_{n-1}a,$$

$$\psi_i(a)=a+\beta_{i1}a+\cdots+\beta_{i\,m-1}a, \qquad (i=1, 2, \cdots, n)$$

for any $a\in\mathfrak{M}$ respectively. Then, we have clearly $\varphi(\mathfrak{M})\subset\mathfrak{N}$ and $\psi_i(\mathfrak{M})\subset\mathfrak{H}_i$ $(i=1, 2, \cdots, n)$. Now, we put

$$\Phi=\varphi+\psi_1+\cdots+\psi_n$$

and we shall prove that Φ is an automorphism of $\mathfrak{M}$. Since we have $H_i \cap H_j = \{\varepsilon\}$ for $i \neq j$ by our assumption and it is easily seen that $N \cap H_i = \{\varepsilon\}$ for $i=1, 2, \cdots, n$, it follows immediately that mn elements $\varepsilon, \alpha_1, \cdots, \alpha_{n-1}, \beta_{11}, \cdots, \beta_{1\,m-1}, \beta_{21}, \cdots, \beta_{n\,m-1}$ of G are distinct to each other and hence they exhaust all elements of G. Therefore, we have

$$\begin{aligned}\Phi(a)&=\varphi(a)+\psi_1(a)+\cdots+\psi_n(a)\\&=(a+\alpha_1 a+\cdots+\alpha_{n-1}a)+(a+\beta_{11}a+\cdots+\beta_{1\,m-1}a)\\&\quad+\cdots+(a+\beta_{n1}a+\cdots+\beta_{n\,m-1}a)\\&=na+\sum_{\sigma\in G}\sigma a=na\end{aligned}$$

for any $a\in\mathfrak{M}$ because we have $\sum_{\sigma\in G}\sigma a=0$ by our assumption. Since the order of any $a\in\mathfrak{M}$ is prime to n, this implies clearly that Φ is an automorphism of $\mathfrak{M}$. Hence we have

$$\begin{aligned}\mathfrak{M}=\Phi(\mathfrak{M})&=\varphi(\mathfrak{M})+\psi_1(\mathfrak{M})+\cdots+\psi_n(\mathfrak{M})\\&\subset\mathfrak{N}+\mathfrak{H}_1+\cdots+\mathfrak{H}_n\subset\mathfrak{M}\end{aligned}$$

and we have $\mathfrak{M}=\mathfrak{N}+\mathfrak{H}_1+\cdots+\mathfrak{H}_n$ evidently.

Since we have $\varphi(a)=na=\Phi(a)$ for any $a\in\mathfrak{N}$ it follows easily that Φ coincides to φ on $\mathfrak{N}$, and hence the restriction of $\varphi: \mathfrak{M}\to\mathfrak{N}$ to $\mathfrak{N}$ is an automorphism of $\mathfrak{N}$. Hence, if we put $\operatorname{Ker}\varphi=\mathfrak{K}$, then it is easily verified that $\mathfrak{M}=\mathfrak{N}\oplus\mathfrak{K}$. Since we have

$$\psi_i(a)=a+\beta_{i1}a+\cdots+\beta_{i\,m-1}a=ma$$

for any $a\in\mathfrak{H}_i$ and the decomposition of G by N is

$$G=N+N\beta_{i1}+\cdots+N\beta_{i\,m-1}, \qquad (i=1, 2, \cdots, n)$$

by our assumption, if $a\in\mathfrak{H}_i$ then we have

$$\begin{aligned}\varphi(ma)&=ma+\alpha_1(ma)+\cdots+\alpha_{n-1}(ma)\\&=(a+\beta_{i1}a+\cdots+\beta_{i\,m-1}a)+\alpha_1(a+\beta_{i1}a+\cdots+\beta_{i\,m-1}a)\\&\quad+\cdots+\alpha_{n-1}(a+\beta_{i1}a+\cdots+\beta_{i\,m-1}a)\\&=\sum_{\sigma\in G}\sigma a=0.\end{aligned}$$

This implies $ma\in\mathfrak{K}$ clearly. Now, if we assume that the order of each element of $\mathfrak{M}$ is also prime to m, then we have $\mathfrak{H}_i\subset\mathfrak{K}$ for $i=1, 2, \cdots, n$ and hence

$$\mathfrak{N}\cap(\mathfrak{H}_1+\cdots+\mathfrak{H}_n)\subset\mathfrak{N}\cap\mathfrak{K}=\{0\}.$$

This implies $\mathfrak{M}=\mathfrak{N}\oplus(\mathfrak{H}_1+\cdots+\mathfrak{H}_n)$ immediately.

Finally if we assume $m=n$ and all H_i $(i=1, 2, \cdots, n)$ are also normal subgroups of G, then it is easily verified that $G=H_iH_j$ for $i\neq j$ because we have

$$H_iH_j/H_j\cong H_i/H_i\cap H_j\cong H_i.$$

As we have $N\cap H_i=\{\varepsilon\}$ $(i=1, 2, \cdots, n)$, if we replace H_i with N in our lemma, then it follows

$$\mathfrak{H}_i\cap(\mathfrak{N}+\mathfrak{H}_1+\cdots+\mathfrak{H}_{i-1}+\mathfrak{H}_{i+1}+\cdots+\mathfrak{H}_n)=\{0\}$$

for $i=1, 2, \cdots, n$. This implies the holding of (3) clearly. Thus, our lemma is proved completely.

PROOF OF THEOREM 1. Our theorem is the immediate consequence of Lemma applying to the abelian group $C_{K,p}/A_{k,p}$ with $G=G(K/k)$ as the operator domain.

COROLLARY. *Notations being same as Theorem* 1, *and moreover if we assume* $(p, m)=1$ *and* $h_{k,p}<h_{K,p}$, *then there exists a subfield of* K *such that the order of its* p*-class group is greater than* $h_{k,p}$.

PROOF. Since all degrees $[K:k]$, $[K:F]$ and $[K:L_i]$ $(i=1, 2, \cdots, n)$ are prime to p by our assumption, it follows easily that $A_{k,p}$, $A_{F,p}$ and $A_{L_i,p}$ are isomorphic to $C_{k,p}$, $C_{F,p}$ and $C_{L_i,p}$ respectively. [3] Moreover, it is clear by our assumption that at least one of the p-groups $A_{F,p}/A_{k,p}$ and $A_{L_i,p}/A_{k,p}$ $(i=1, 2, \cdots, n)$ is not the unit group. From above our assertion follows immediately.

THEOREM 2. *Let* k *be an algebraic number field of finite degree, and let* K *be a Galois extension over* k *such that the Galois group* $G(K/k)$ *is an abelian group of type* (l, l), *where* l *is a rational prime number. Let* $F_1, F_2, \cdots, F_{l+1}$ *be the proper intermediate fields between* k *and* K. *If the class number* h_K *of* K *is divisible by a rational prime number* p $(\neq l)$, *then* $C_{K,p}/A_{k,p}$ *is decomposed into the direct product as following:*

$$C_{K,p}/A_{k,p}=A_{F_1,p}/A_{k,p}\times\cdots\times A_{F_{l+1},p}/A_{k,p}.$$

PROOF. This theorem follows immediately by applying the last assertion of Lemma to the p-group $C_{K,p}/A_{k,p}$.

§ 3. p-class groups of S_n-extensions.

In this section, we shall be mainly concerned with the applying of Theorem 1 and 2 to the p-class groups of S_n-extensions.

THEOREM 3. *Let* k *be an algebraic number field of finite degree, and let* K *be an* S_n*-extension over* k *where we assume* $n\geqq 4$. *If we have* $h_{K,p}>a_{k,p}$ *for any rational prime number* p, *then there exist proper intermediate fields* F *and* $L_1, L_2, \cdots, L_r$ *between* k *and* K *such that* $L_1, L_2, \cdots, L_r$ *are conjugate to each* *other over k and we have*

$$C_{K,p}=\langle A_{F,p},\ A_{L_1,p},\ \cdots,\ A_{L_r,p}\rangle\ .$$

Moreover, if $p>2$, then there exists a proper subfield of K such that the order of its p-class group is greater than $a_{k,p}$. If $n\geqq 6$, then this is also true for $p=2$.

PROOF. We may regard the Galois group $G=G(K/k)$ as the symmetric group S_n of n letters $a_1, a_2, \cdots, a_n$.

(1) the case when $p>2$.

Let T_1 be the subfield of K corresponding to the subgroup $\{I, (a_1a_2), (a_3a_4), (a_1a_2)(a_3a_4)\}$ of G by the Galois theory. Then, it is obvious that K is an (A)-extension over T_1. Hence, if we denote by F, L_1 and L_2 the proper intermediate fields between T_1 and K, where we assume L_1 and L_2 are conjugate to each other over k, then using Theorem 1 we have

$$C_{K,p}=\langle A_{F,p},\ A_{L_1,p},\ A_{L_2,p}\rangle$$

clearly. Moreover, since $C_{K,p}/A_{k,p}$ is non-trivial by our assumption, it follows immediately that among the p-groups $A_{F,p}/A_{k,p}$, $A_{L_1,p}/A_{k,p}$ and $A_{L_2,p}/A_{k,p}$ there exists at least one which is non-trivial. Now, since $A_{F,p}$, $A_{L_1,p}$ and $A_{L_2,p}$ are isomorphic to $C_{F,p}$, $C_{L_1,p}$ and $C_{L_2,p}$ respectively in our case, it follows immediately that among $h_{F,p}$, $h_{L_1,p}$ and $h_{L_2,p}$ there exists at least one which is greater than $a_{k,p}$.

(2) the case when $p=2$.

Let T_2 be an intermediate field between k and K such that K is an S_3-extension over T_2. Moreover, let F, L_1, L_2 and L_3 be proper intermediate fields between T_2 and K, where we assume L_1, L_2 and L_3 are conjugate to each other over k. Then, since K is an (A)-extension over T_2, using Theorem 1 we have

$$C_{K,2}=\langle A_{F,2},\ A_{L_1,2},\ A_{L_2,2},\ A_{L_3,2}\rangle$$

immediately. Finally, if we assume $n\geqq 6$, then there exists a subfield of K corresponding to the subgroup $\langle(a_1a_2a_3), (a_4a_5a_6)\rangle$ of G which is of type (3,3). Now, our assertion concerning with the order of 2-class group follows similarly as the case when $p>2$. Q.E.D.

Now, for the subfields of S_n-extensions we shall consider a condition concerning with the divisibility of their class numbers by a rational prime number p.

THEOREM 4. *Let k be an algebraic number field of finite degree, and let K be an S_n-extension over k where we assume $n\geqq 5$. Let M be the subfield of K such that we have $[M:k]=2$. Moreover, we assume $h_{K,p}>a_{M,p}$ for a rational prime number p. If F and $L_1, L_2, \cdots, L_r$ are proper intermediate fields between k and K such that they satisfy the assertion of Theorem 3 and $[K:L_i]$ $(i=1, 2, \cdots, r)$ is prime to p, then we have $h_{L_i,p}>a_{k,p}$ for $i=1, 2, \cdots, r$.*

PROOF. Since it follows easily from our assumption that $C_{L_i,p}$ is isomorphic to $A_{L_i,p}$ for $i=1, 2, \cdots, r$, we have $a_{k,p}\leqq a_{L_i,p}=h_{L_i,p}$ clearly. Now, we assume $h_{L_i,p}=a_{k,p}$, from which it follows $A_{L_i,p}=A_{k,p}$ evidently. Then, since we have $C_{K,p}=\langle A_{F,p}, A_{L_1,p}, \cdots, A_{L_r,p}\rangle$ we obtain $C_{K,p}=A_{F,p}$ clearly. If $F_1=F, F_2, \cdots, F_s$ are all of the conjugates of F over k, then we have also $C_{K,p}=A_{F_i,p}$ ($i=1, 2, \cdots, s$) because $A_{F_i,p}$ ($i=1, 2, \cdots, s$) is isomorphic to $A_{F,p}$ clearly. Hence, if we put $T=\bigcap_{i=1}^{s} F_i$, then it is easily verified that we have $C_{K,p}=A_{T,p}$. Now, since the Galois group $G(K/T)$ is a normal subgroup of $G(K/k)$ and it is well known that the alternative group A_n of degree n is the unique proper normal subgroup of S_n when $n\geqq 5$, we must have $G(K/T)\supset G(K/M)$ and this implies $T\subset M$ immediately. Hence we have $C_{K,p}=A_{T,p}\subset A_{M,p}$ and this is a contradiction clearly. Thus, we have $h_{L_i,p}>a_{k,p}$ for $i=1, 2, \cdots, r$, and our theorem is proved completely.

COROLLARY 1. *The fields k, K and M being same as Theorem* 4, *and similarly we assume $h_{K,p}>a_{M,p}$ for an odd prime number p. Moreover, let π be an element of S_n and let L be a subfield of K corresponding to the subgroup of S_n generated by π. Then, if we have one of the following cases:*

(1) *π is a transposition,*

(2) *π is a cycle of length $q-1$, where q ($\leqq n$) is an odd prime number such that $(p, q(q-1))=1$,*

(3) *π is a product of $(q-1)/2$ disjoint transpositions, where q ($\leqq n$) is an odd prime number different from p, then we have always $h_{L,p}>a_{k,p}$.*

PROOF. It is easily shown for each of above cases that there exists a subfield T of K such that $[K: T]$ is prime to p and K/T is an (A)-extension in which L plays a part of L_i. Now, our assertion follows immediately from Theorem 4. Q. E. D.

If the fields K and M are same as Theorem 4, then it is easily verified that we have $h_{M,p}\leqq a_{M,p}$. Now, in following corollary, we shall deal with the case where we may assume $h_{K,p}>h_{M,p}$ instead of $h_{K,p}>a_{M,p}$.

COROLLARY 2. *The fields k, K and M being same as Theorem* 4, *and we assume $h_{K,p}>h_{M,p}$ for an odd prime number p (>3). Moreover, if $p\leqq n$, then we assume that there exists no prime ideal of M whose ramification index in K is divisible by p. Then, if F and $L_1, L_2, \cdots, L_r$ are proper intermediate fields between k and K such that they satisfy the assertion of Theorem* 3 *and $[K: L_i]$ ($i=1, 2, \cdots, r$) is prime to p, then we have $h_{L_i,p}>a_{k,p}$ for $i=1, 2, \cdots, r$.*

To prove this corollary we must use the following lemma, which has been proved in [2].

LEMMA. *Let p (>3) be an odd prime number. Let G be a finite group and let P be a p-subgroup of G which is contained in the center of G. Then, if G/P is isomorphic to the alternative group A_n of degree n, then there exists a normal* *subgroup N of G such that we have $G=N\times P$.*

PROOF OF COROLLARY 2. If we assume $h_{L_i,p}=a_{k,p}$, then it follows $C_{K,p}=A_{M,p}$ as the proof of Theorem 4. Now, let Ω be the unramified abelian extension over K such that the Galois group $G(\Omega/K)$ is isomorphic to $C_{K,p}$. Then, it is easily verified that Ω is a Galois extension over k and the Galois group $G(\Omega/K)$ is a p-group which is contained in the center of the Galois group $G(\Omega/M)$. Since the Galois group $G(K/M)$ is isomorphic to the alternative group A_n of degree n and we have $p>3$ by our assumption, using above lemma it follows easily that there exists an abelian extension U over M such that we have $KU=\Omega$ and $K\cap U=M$ and moreover the Galois group $G(U/M)$ is isomorphic to $C_{K,p}$. Since there exists no prime ideal of M whose ramification index in Ω is divisible by p in our case, U must be an unramified abelian extension over M. This implies $h_{K,p}\leqq h_{M,p}$, which is a contradiction clearly. Thus, our assertion is proved completely. Q. E. D.

Finally, we shall deal with the rank of p-class groups of S_n-extensions. Namely, in following theorem, we shall give some lower bound for it.

THEOREM 5. *Let k be an algebraic number field of finite degree, and let K be an S_n-extension over k where we assume $n\geqq 5$. Moreover, let M be the subfield of K such that we have $[M: k]=2$. If we have $h_{K,p}>a_{M,p}$ for an odd prime number p and if we denote by ρ the rank of p-group $C_{K,p}/A_{k,p}$, then we have always $\rho\geqq 3$. Hence, $h_{K,p}/a_{k,p}$ is divisible by at least p^3 in our case.*

PROOF. We may regard the Galois group $G(K/k)$ as the symmetric group S_n of n letters $a_1, a_2, \cdots, a_n$ as before. Let L_1, L_2 and L_3 be the subfields of K corresponding to the subgroups $\langle(a_1a_2)(a_3a_4)\rangle$, $\langle(a_1a_3)(a_2a_4)\rangle$ and $\langle(a_1a_4)(a_2a_3)\rangle$ of S_n respectively, and we put $F=L_1\cap L_2\cap L_3$. Since the Galois group $G(K/F)$ is an abelian group of type (2, 2), applying Theorem 2 to it we have

$$C_{K,p}/A_{F,p}=A_{L_1,p}/A_{F,p}\times A_{L_2,p}/A_{F,p}\times A_{L_3,p}/A_{F,p}$$

immediately. As L_1, L_2 and L_3 are conjugate to each other over k, $A_{L_1,p}$, $A_{L_2,p}$ and $A_{L_3,p}$ are isomorphic to each other. Hence, it follows easily that we have $A_{L_i,p}\supsetneqq A_{F,p}$ for $i=1, 2, 3$, because if we assume otherwise, then we must have $C_{K,p}=A_{F,p}$ and from this we must have a contradiction using the same method as the proof of Theorem 4. Now, from above our assertion follows immediately.

COROLLARY. *The fields k, K and M being same as above, and we assume $h_{K,p}>h_{M,p}$ for an odd prime number p (>3). Moreover, if $p\leqq n$, then we assume that there exists no prime ideal of M whose ramification index in K is divisible by p. Then, if we denote by ρ the rank of p-group $C_{K,p}/A_{k,p}$, then we have always $\rho\geqq 3$.*

PROOF. Using same method as the proof of Corollary 2 of Theorem 4 our corollary follows easily.

References

[1] K. Ohta, On the relative class number of a relative Galois number field, J. Math. Soc. Japan, **24** (1972), 552-557.
[2] K. Ohta, On the p-class groups of S_n——Resp. A_n——extensions, (in Japanese), Sūgaku, **28** (1976), 253-257.
[3] A, Yokoyama, On the relative class number of finite algebraic number fields, J. Math. Soc. Japan, **19** (1967), 179-185.

Kiichiro OHTA
Department of Mathematics
Faculty of General Education
Gifu University
Nagara, Gifu
Japan