J. Math. Soc. Japan
Vol. 24, No. 4, 1972

On the relative class number of a relative Galois number field

By Kiichiro OHTA

(Received Aug. 27, 1971)
(Revised May 17, 1972)

§ 1. Introduction.

Let k be an algebraic number field of finite degree. Let p be any rational prime number. The p-Sylow subgroup of the absolute ideal class group of k will be called the p-class group of k whose order will be denoted by $h_{k,p}$.

Let K be a Galois extension of degree m over k. Then there are many known results as to the p-class groups of K and k in case K/k is abelian or when m is a prime power (in which case K/k is a soluble extension); in particular, many relations are known to hold between $h_{K,p}$ and $h_{k,p}$ (K. Iwasawa [2], H. Yokoi [3], [4], A. Yokoyama [5], [6], [7]).

But, at the present time, it seems that there are no convenient literatures as to the p-class groups of K and k in such case where the Galois group $G(K/k)$ is non-abelian and simple. (For instance, it is such case where the group $G(K/k)$ is isomorphic to the alternative group A_n of degree $n(>4)$.) So, in this paper we shall deal with the p-class groups of K and k in such special case. The main purpose of this paper is to prove the following theorem:

THEOREM 1. *Let k be an algebraic number field of finite degree. Let K be a Galois extension of degree m over k such that the Galois group $G(K/k)$ is non-abelian and simple. Let Ω_K and Ω_k be the absolute class fields of K and k respectively. Let p be any rational prime number prime to m. Let $\bar{H}$ be the p-Sylow subgroup of the Galois group $G(\Omega_K/K\Omega_k)$, whose rank is denoted by r. If $\bar{H}$ is non-trivial, then we have $r>1$ and*

$$(p^r-1)(p^{r-1}-1)\cdots(p-1)\equiv 0 \pmod{m}.$$

After the proof of our main theorem, we shall refer to some results which are easily verified from above theorem.

§ 2. Preliminaries.

In this section we shall prove three lemmas which are required in order to prove our main theorem.

LEMMA 1. *Let k, F and K be three algebraic number fields of finite degree such as $k\subset F\subset K$. Let p be any rational prime number prime to $m=[F:k]$. Assume that F and K are both Galois over k. Moreover, assume that the Galois group $G(F/k)$ of order m is non-abelian and simple, and the Galois group $G(K/F)$ is an abelian p-group whose rank is denoted by r. If we have either $r=1$ or*

$$(p^r-1)(p^{r-1}-1)\cdots(p-1)\not\equiv 0 \pmod{m},$$

then there exists the subfield L of K which satisfies the following (1) *and* (2):

(1) *we have $FL=K$ and $F\cap L=k$,*

(2) *L is Galois over k.*

PROOF. For brevity we put $\bar{G}=G(K/k)$, $\bar{N}=G(K/F)$ and $\bar{H}=G(F/k)$ and we denote the order of $\bar{N}$ by p^n. Let

$$\bar{G}=\bar{N}\sigma_1+\bar{N}\sigma_2+\cdots+\bar{N}\sigma_m$$

be the disjoint union of cosets of $\bar{N}$. Let $\bar{\sigma}_i$ $(i=1, 2, \cdots, m)$ be the automorphisms of $\bar{N}$ given by $x\to\sigma_i^{-1}x\sigma_i$ for all $x\in\bar{N}$. Then it is clear that the mapping ϕ given by $\bar{N}\sigma_i\to\bar{\sigma}_i$, for $i=1, 2, \cdots, m$, is a homomorphism from $\bar{H}$ into the automorphism group $A(\bar{N})$ of $\bar{N}$. Moreover, it is easily verified by the assumption for $\bar{H}$ that the kernel of ϕ must be either the identity group $\bar{E}$ of $\bar{H}$ or $\bar{H}$ itself.

Now, we assume that the kernel is $\bar{E}$. Then we know at once that ϕ is an injection and the image $\phi(\bar{H})$ is a subgroup of $A(\bar{N})$ which is isomorphic to $\bar{H}$. Since $A(\bar{N})$ must be non-abelian in our case, so we have $r>1$, and it is well known that the order of $A(\bar{N})$ is a divisor of $p^{r(n-r)}(p^r-1)(p^r-p)\cdots(p^r-p^{r-1})$. Hence, the order m of $\phi(\bar{H})$ must be so. But this is a contradiction. Therefore, it follows immediately that the kernel of ϕ must be $\bar{H}$ itself, and hence all $\bar{\sigma}_i$ must be the identity of $A(\bar{N})$. As we have $(p, m)=1$ by our assumption, this means that $\bar{N}$ is the p-Sylow subgroup of $\bar{G}$ such as contained in the center of $\bar{G}$, and hence it follows immediately by Burnside's theorem that $\bar{N}$ has the normal p-Sylow complement $\bar{Z}$ in $\bar{G}$.

Now, if we denote by L the subfield of K corresponding to $\bar{Z}$ by the Galois theory, then it is easy to verify that L satisfies our conditions (1) and (2).

LEMMA 2. *Let k, F, L and K be four algebraic number fields of finite degree such as $k\subset F\subset L\subset K$. Denote the degrees $[L:F]$ and $[K:L]$ by m and n respectively. Assume that F and K are both Galois over k, and L is Galois over F. If we have $(m, n)=1$, then L is Galois over k.*

PROOF. We put $L=k(\theta)$ and $r=[F:k]$, and we denote the minimal polynomial of θ over k by $f(X)$. Then $f(X)$ whose degree is mr, has a factorization

$$f(X)=\phi_1(X)\phi_2(X)\cdots\phi_r(X)$$

in $F[X]$, where each $\phi_i(X)$ $(i=1, 2, \cdots, r)$ is an irreducible polynomial of degree m. If we have $\phi_1(\theta)=0$, then L is the minimal splitting field of $\phi_1(X)$ over F. If we denote the minimal splitting fields of $\phi_i(X)$ $(i=2, 3, \cdots, r)$ by L_i respectively, then each L_i is a Galois extension of degree m over F, and it is the conjugate of L over k.

Now, let M be the minimal splitting field of $f(X)$ over k, then M is Galois over k, and we have $L\subset M\subset K$. Hence, it is clear that $u=[M:L]$ is a divisor of n. But, on the other hand, we have $M=LL_2\cdots L_r$, and if $m=q_1^{e_1}q_2^{e_2}\cdots q_s^{e_s}$ is the prime factorization of m, then u must have the prime factorization as $u=q_1^{t_1}q_2^{t_2}\cdots q_s^{t_s}$ $(t_j\geqq 0)$. Hence, in our case we have $(u, n)=1$, and consequently $u=1$. Now it is obvious that we have $L=M$.

LEMMA 3. *Let k, F and K be three algebraic number fields of finite degree such as $k\subset F\subset K$. Assume that F and K are both Galois over k. Let $\bar{H}$ and $\bar{Z}$ be two subgroups of the Galois group $G(K/F)$ such that we have $G(K/F)=\bar{H}\times\bar{Z}$ (direct product). If the orders of $\bar{H}$ and $\bar{Z}$ are relatively prime to each other, then the subfield L of K corresponding to $\bar{H}$ is Galois over k.*

PROOF. For any $\sigma\in G(K/k)$ and for any $\tau\in\bar{H}$ we have $\sigma^{-1}\tau\sigma\in\bar{H}$ because τ and $\sigma^{-1}\tau\sigma$ have the same orders. Hence, $\bar{H}$ is a normal subgroup of $G(K/k)$, and this means immediately the holding of our assertion.

§ 3. The proof of main theorem.

PROOF OF THEOREM 1. Since K is Galois over k and Ω_K is the absolute class field of K, it is obvious that Ω_K is a Galois extension of k. If we denote the class numbers of K and k by h_K and h_k respectively, then h_K is divisible by h_k because we have clearly $K\cap\Omega_k=k$ by our assumption for the Galois group $G(K/k)$.

Now, it is evident that the order p^n of $\bar{H}$ is equal to $h_{K,p}/h_{k,p}$. If we put $N=K\Omega_k$, and if we denote the p-Sylow complement of $G(\Omega_K/N)$ by $\bar{Z}$, then it is easily verified that $\bar{H}$ and $\bar{Z}$ satisfy the assumption of Lemma 3 when we apply it to three fields k, N and Ω_K. Hence, the subfield F of Ω_K which corresponds to $\bar{Z}$ is Galois over k, and we have $[F:N]=p^n$. Furthermore, it is evident that the Galois group $G(F/N)$ is isomorphic to $\bar{H}$.

Now, as to the rank r of $\bar{H}$ we assume that we have either $r=1$ or

$$(p^r-1)(p^{r-1}-1)\cdots(p-1)\not\equiv 0 \pmod{m}.$$

Then, from Lemma 1 there exists the subfield L of F such that we have $NL=F$, $N\cap L=\Omega_k$ and L is Galois over Ω_k. Next, as we have $[F:L]=[N:\Omega_k]$

$=m$ and $[L:\Omega_k]=[F:N]=p^n$, applying Lemma 2 to four fields k, Ω_k, L and F, it is easily verified that L is Galois over k. Moreover, as the Galois group $G(F/L)$ is isomorphic to $G(K/k)$, it follows at once that we have $K\cap L=k$ and $KL=F$. Hence, the Galois group $G(L/k)$ is abelian as well as $G(F/K)$ because they are isomorphic to each other.

On the other hand, since F is unramified over N and we have $(m, p^n)=1$ by our assumptions, it follows easily that the ramification index of any ramified prime divisor in F/Ω_k is prime to p^n. This means immediately that L is unramified over Ω_k. Hence, L must be an unramified abelian extension of k. Now, since Ω_k is the maximal unramified abelian extension of k, we must have $L\subset\Omega_k$. But this is a contradiction to $[L:\Omega_k]=p^n$ (>1).

Thus, our theorem is proved completely. Q. E. D.

Now, for the relative class numbers, we have immediately the following theorem. Namely:

THEOREM 2. *Let k be an algebraic number field of finite degree. Let K be a Galois extension of degree m over k such that the Galois group $G(K/k)$ is non-abelian and simple. Let p be any rational prime number prime to m, and let r be the minimal natural number such as $r>1$ and*

$$(p^r-1)(p^{r-1}-1)\cdots(p-1)\equiv 0 \pmod{m}.$$

Denote the class numbers of K and k by h_K and h_k respectively. If $d=h_K/h_k$ is divisible by p, then d is divisible by p^r.

Moreover, the following theorem will be easily verified by making use of Theorem 1.

THEOREM 3. *Let k be an algebraic number field of finite degree. Let K be a Galois extension of degree m over k such that the Galois group $G(K/k)$ is non-abelian and simple. Let p be any rational prime number prime to m. Denote the ranks of p-class groups of K and k by $r_{K,p}$ and $r_{k,p}$ respectively. Let $q_1, q_2, \cdots, q_s$ be all the different prime factors of m, and for $i=1, 2, \cdots, s$, let f_i be the order of the residue class p mod q_i. If $h_{K,p}/h_{k,p}$ is divisible by p, then we have*

$$\max(2, f_1, f_2, \cdots, f_s)\leqq r_{K,p}-r_{k,p}.$$

PROOF. Let Ω_K and Ω_k be the absolute class fields of K and k respectively. Let $\bar{H}$ be the p-Sylow subgroup of $G(\Omega_K/K\Omega_k)$, and we denote the rank of $\bar{H}$ by r. Then, as p is prime to m, it is easily verified from Theorem 1 that we have

$$\max(2, f_1, f_2, \cdots, f_s)\leqq r.$$

Now, let $C_{K,p}$ and $C_{k,p}$ be the p-class groups of K and k respectively. Let A_K be the ambiguous ideal class group with respect to K/k, and we put $A_{K,p}=A_K\cap C_{K,p}$. Then it is known that we have

$$C_{K,p}=A_{K,p}\times B_{K,p}\qquad \text{(direct product)}$$

and $A_{K,p}$ is isomorphic to $C_{k,p}$. (Cf. A. Yokoyama [6]). Hence, it follows from the class field theory that $B_{K,p}$ is isomorphic to $\bar{H}$ and thus we obtain

$$r_{K,p}=r+r_{k,p}\,. \qquad \text{Q.E.D.}$$

Finally, as to the relative class numbers of the intermediate fields, we have the following theorem. Namely:

THEOREM 4. *Let k be an algebraic number field of finite degree. Let K be a Galois extension of degree m over k such that the Galois group $G(K/k)$ is non-abelian and simple. Let F be a proper intermediate field between k and K. Let p be any rational prime number prime to m. If $h_{K,p}/h_{k,p}$ is divisible by p, then $h_{K,p}/h_{F,p}$ is divisible by p too.*

PROOF. Let Ω_K and Ω_k be the absolute class fields of K and k respectively. Let M be the subfield of Ω_K such that the Galois group $G(\Omega_K/M)$ is the p-Sylow complement of $G(\Omega_K/K\Omega_k)$. Then, M is Galois over k from Lemma 3, and the Galois group $\bar{H}=G(M/K\Omega_k)$ is a p-group of order p^n with $n>1$ by our assumption and Theorem 1. Moreover, since we have $[K\Omega_k:\Omega_k]=m$ and $(m, p)=1$, if we apply the Schur's theorem as to the extension of group to $G(M/\Omega_k)$, $G(K\Omega_k/\Omega_k)$ and $\bar{H}$, then we have the decomposition as following:

$$G(M/\Omega_k)=\bar{H}\bar{Z}\,.$$

Here, it is obvious that $\bar{Z}$ is isomorphic to $G(K\Omega_k/\Omega_k)$. If we denote by L the intermediate field between Ω_k and M corresponding to $\bar{Z}$ by the Galois theory, then we have clearly $L\cdot K\Omega_k=M$ and $L\cap K\Omega_k=\Omega_k$. Furthermore, it follows that L is not Galois over Ω_k. Because, if we assume otherwise, then it follows from Lemma 2 that L is Galois over k and the Galois group $G(L/k)$, which is isomorphic to $G(M/K)$, is an abelian group. Since M is unramified over $K\Omega_k$ and we have $(m, p^n)=1$ by our assumptions, it is easily verified that L is unramified over Ω_k. Hence, it follows clearly that L is an unramified abelian extension of k and we must have $L\subset\Omega_k$ by the definition of Ω_k. But it is a contradiction to $[L:\Omega_k]=p^n$. Therefore, if we put $L=\Omega_k(\theta)$ and if we denote by $f(X)$ the minimal polynomial of θ over Ω_k, then M must be the minimal splitting field of $f(X)$ over Ω_k because $\bar{Z}$ is non-abelian and simple. On the other hand, it is easily verified that $f(X)$ is irreducible in $K\Omega_k[X]$ and we have $M=K\Omega_k(\theta)$.

Finally, let Ω_F be the absolute class field of F. As we have $F\cap\Omega_k=k$, it is obvious that we have $\Omega_k\subset\Omega_F$. Now, if we assume that $h_{K,p}/h_{F,p}$ is not divisible by p, then we have $h_{K,p}=h_{F,p}$ and as $([K:F], p)=1$ in our case it follows at once that the p-class groups of K and F are isomorphic to each other. Moreover, if we denote by N the field which corresponds to the p-Sylow complement of $G(\Omega_F/F\Omega_k)$, then the Galois group $G(N/F\Omega_k)$ is isomorphic to $\bar{H}$ and we have $N\cdot K\Omega_k=M$ and $N\cap K\Omega_k=F\Omega_k$ clearly. Therefore, since $f(X)$ is a polynomial in $F\Omega_k[X]$, it is easily verified that by taking a suitable root θ' of $f(X)$ we have $N=F\Omega_k(\theta')$. As N is Galois over $F\Omega_k$ and $f(X)$ is irreducible in $F\Omega_k[X]$, N must be the splitting field of $f(X)$ and hence we must have $M\subset N$. But this is impossible because we have $[M:N]=[K:F]>1$ by our assumption.

Thus, our theorem is proved completely.

Meijō University

References

[1] M. Ishida, Class numbers of algebraic number fields of Eisenstein type, J. of Number Theory, **2** (1970), 404-413.
[2] K. Iwasawa, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg, **20** (1956), 257-258.
[3] H. Yokoi, On the class number of a relatively cyclic number field, Nagoya Math. J., **29** (1967), 31-44.
[4] H. Yokoi, On the divisibility of the class number in an algebraic number field, J. Math. Soc. Japan, **20** (1968), 411-418.
[5] A. Yokoyama, On class numbers of finite algebraic number fields, Tôhoku Math. J., (2) **17** (1965), 349-357.
[6] A. Yokoyama, Über die Relativklassenzahl eines relative Galoisschen Zahlkörpers von Primzahlpotenzgrad, Tôhoku Math. J., (3) **18** (1966), 318-324.
[7] A. Yokoyama, On the relative class number of finite algebraic number fields, J. Math. Soc. Japan, **19** (1967), 179-185.
[8] H. Zassenhaus, Lehrbuch der Gruppentheorie 1, Leipzig, 1937.