ON CLASS NUMBERS OF FINITE ALGEBRAIC NUMBER FIELDS

AKIO YOKOYAMA

(Received August 17, 1965)

In this paper, we shall investigate some relations between the class number, the absolute ideal class group of a finite algebraic number field and that of its Galois extension of finite degree.

It is well known that the class number of the cyclotomic field is divisible by the class number of its subfield. In §1 we shall show that the class number of a finite algebraic number field is a divisor of the class number of its finite extension if the class number of the finite algebraic number field is prime to the degree of the extension field. In §2 we shall give main results of this paper which contain, as a special case, theorems of H. Weber, K. Iwasawa and others. In §3 we shall give a note on prime factors of the class number of the splitting field of a binomial equation with respect to the rational number field.

Throughout this paper the following notations will be used.

l, q : fixed rational prime numbers. p : any rational prime number.
$f_{q,p}$: the smallest positive integer f such that $q \mid p^f-1$.
P : the rational number field.
$P_{(n)}$: the cyclotomic field generated by the primitive l^{n+1}-th root of unity over P.
k : the ground field which is a finite algebraic number field.
h_k : the class number of k. $h_{k,p}$: the p-part of h_k.
$V_{p,k}$: the least number of generators of the p-class group of k.
$[K:k]$: the relative degree of an extension K/k.
$\overline{k}_{(p)}$: the intermediate field of k and the absolute class field of k such that $[\overline{k}_{(p)}:k] = h_{k,p}$.
$G(K/k)$: the Galois group of a Galois extension K/k.

1. Let p be any prime number. The Sylow p-subgroup of the absolute ideal class group of k will be called *the p-class group of k*. Let K/k be a Galois extension with the Galois group $\mathfrak{G} = G(K/k)$. The Galois group $\mathfrak{G}$ acts on the ideal group of K and the p-class group of K in an obvious way. They may be considered as $\mathfrak{G}$-groups.

Let $\mathfrak{N}$ be the subgroup of all ideals $\mathfrak{a}$ in the ideal group $\mathfrak{D}$ of K such

that for an integer n prime to p, $\mathfrak{a}^n$ is a principal ideal. Then the factor group $\mathfrak{D}/\mathfrak{N}$ is $\mathfrak{g}$-isomorphic with the p-class group of K. By class field theory, the class field $\overline{K}_{(p)}$ corresponds to the ideal group $\mathfrak{N}$ and the relative degree of the extension $\overline{K}_{(p)}/K$ is $h_{K,p}$. As K is a Galois extension over k, $\overline{K}_{(p)}$ is also a Galois extension over k. Therefore the Galois group $G(\overline{K}_{(p)}/K)$ may be considered as a $\mathfrak{g}$-group. By Artin's reciprocity law, $G(\overline{K}_{(p)}/K)$ is $\mathfrak{g}$-isomorphic with the factor group $\mathfrak{D}/\mathfrak{N}$ and so the p-class group of K.

Now, the subgroup of all ideal classes in the p-class group of K which are left invariant under $\mathfrak{g}$ will be called *the ambiguous p-class group of K with respect to k* whose order will be denoted by $a_p(K/k)$.

We now prove the following

PROPOSITION 1. *Let K be a finite extension of degree m over k and p be any prime number prime to m. If the class number of k is divisible by p^a, then the class number of K is divisible by p^a. Furthermore, the p-class group of k is isomorphic with a subgroup of the p-class group of K. In particular, if h_k is prime to m, then h_K is divisible by h_k.*

PROOF. Let $\mathfrak{C}_K$ and $\mathfrak{C}_k$ be the p-class groups of K and k respectively. Let C be any ideal class in $\mathfrak{C}_k$ and let $\mathfrak{a}$ be an ideal in C different from a principal ideal. Suppose that $\mathfrak{a}$ is principal in K. Then $N_{K/k}\mathfrak{a}=\mathfrak{a}^m$ is principal in k which contradicts the fact that $\mathfrak{a}$ is contained in C. Therefore, no non-principal ideal class in $\mathfrak{C}_k$ becomes a principal ideal class in $\mathfrak{C}_K$ and hence, the mapping $\varphi: \mathfrak{C}_k \to \mathfrak{C}_K$ induced by the injection of the ideal group of k into the ideal group of K is an isomorphism. The class number of K is therefore divisible by p^a.

Applying this to $k=P_{(0)}$, we have

COROLLARY. *Let K be any finite algebraic number field of degree m over $P_{(0)}$, where m is prime to l. If the class number of K is not divisible by l, then l is a regular prime, that is, the class number of $P_{(0)}$ is prime to l.*

We now quote the following known lemma which shall be used later. (cf. [1])

LEMMA. *Let K/k be a finite extension. If there exists no abelian unramified extension of k in K, then h_K is divisible by h_k.*

Let K be a Galois extension of degree m over k and p be any prime number prime to m. Then the Galois group $G(\overline{K}_{(p)}/k)$ splits over the Galois

group $G(\overline{K}_{(p)}/K)$. (cf. [2]) Hence we can find an intermediate field F of k and $\overline{K}_{(p)}$ such that $[F:k]=h_{K,p}$, $\overline{K}_{(p)}=KF$ and $K\cap F=k$. Now suppose that the p-class group of K coincides with the ambiguous p-class group of K with respect to k. Then, from Artin's reciprocity law, it can easily be seen that the Galois group $G(\overline{K}_{(p)}/K)$ is contained in the center of $G(\overline{K}_{(p)}/k)$. Therefore, it follows that the extension F/k is a Galois extension and so an abelian extension. As the ramification exponent of any prime divisor of $\overline{K}_{(p)}$ is a divisor of m and so prime to p, F is an unramified extension over k and hence, is contained in $\overline{k}_{(p)}$. We see further that $F=\overline{k}_{(p)}$ holds by Proposition 1; the p-class group of K is isomorphic with that of k. If, in particular, h_K is prime to m, it is easy to show that the absolute ideal class group of K is isomorphic with a subgroup of that of k. Assume further that there exists no abelian unramified extension of k in K. Then from Lemma, it follows that the absolute ideal class group of K is isomorphic with that of k.

Conversely, assume that the p-class group of K is isomorphic with that of k. It is then easily verified that the centralizer of $G(\overline{K}_{(p)}/K)$ in $G(\overline{K}_{(p)}/k)$ is equal to $G(\overline{K}_{(p)}/k)$. Therefore, the p-class group of K coincides with the ambiguous p-class group of K with respect to k.

Thus the following proposition is proved:

PROPOSITION 2. *Let K be a Galois extension of degree m over k and p be a prime number prime to m. Then the p-class group of K is isomorphic with that of k if and only if the Galois group $G(K/k)$ leaves the p-class group of K fixed elementwise.*

In particular, if, further, there exists no abelian unramified extension of k in K and the class number of K is prime to m, then the absolute ideal class group of K is isomorphic with that of k if and only if the absolute ideal class group of K is left invariant elementwise under the Galois group $G(K/k)$.

In the case K/k is cyclic, the result of Proposition 2 can be obtained more simply in the following manner: the number a of ambiguous classes of K/k is given by the well-known formula:

$$(*) \qquad a=\frac{h_k\cdot\prod_{\mathfrak{P}} e_{\mathfrak{P}}}{[K:k](\varepsilon:N(\theta))}$$

where ε stands for units in k, θ for elments in K whose norms $N(\theta)=N_{K/k}\theta$ are units in k and $e_{\mathfrak{P}}$ is the ramification exponent of any prime divisor $\mathfrak{P}$ of k and the product $\prod_{\mathfrak{P}} e_{\mathfrak{P}}$ is taken over all prime divisors of k including infinite

prime divisors.

As p is prime to m, we can see that the p-part of a coincides with the p-part of h_k and that the p-class group of K is isomorphic with that of k if and only if the p-part of h_K is equal to the p-part of h_k. Furthermore, the ambiguous p-class group of K with respect to k is the Sylow p-subgroup of the ambiguous class group of K with respect to k, i.e. the subgroup of all ideal classes in the absolute ideal class group of K which are left invariant under the Galois group of K/k. The result of Proposition 2 then follows immediately from these facts.

2. As a partial converse to Proposition 1 we have the following

THEOREM 1. *Let K be a Galois extension of degree m over k and p be any prime number prime to m; let $q_1, \cdots, q_r$ be all the different prime factors of m and let f be the minimal number of all $f_{q_i,p}$. If $V_{p,K} < f$, then the p-class group of K is isomorphic with that of k.*

PROOF. If $V_{p,K}=0$, that is, $h_{K,p}=1$, then $h_{k,p}=1$ by Proposition 1. Hence this theorem is true in this case. Now, suppose $V_{p,K} \geqq 1$. Since m and p are relatively prime, the Galois group $G(\overline{K}_{(p)}/k)$ splits over the Galois group $G(\overline{K}_{(p)}/K)$. Hence we can find an intermediate field F of k and $\overline{K}_{(p)}$ such that $[F: k] = h_{K,p}$, $\overline{K}_{(p)} = KF$ and $K \cap F = k$. Then each element of the Galois group $G(\overline{K}_{(p)}/F)$ induces an automorphism of $G(\overline{K}_{(p)}/K)$. It is known that the order of the group of automorphisms of $G(\overline{K}_{(p)}/K)$ divides

$$\eta(p) = p^{v(n-v)}(p^v-1)(p^v-p)\cdots(p^v-p^{v-1})$$

where $V_{p,K}=v$ and n denotes the exponent of p in $h_{K,p}$. (cf. [2]) m is relatively prime to $\eta(p)$ under the assumption $V_{p,K} < f$. Therefore, these m automorphisms of $G(\overline{K}_{(p)}/K)$ coincide with identity. We see then that the extension F/k is a Galois extension and so an abelian extension of degree $h_{K,p}$. As the ramification exponent of any prime divisor of $\overline{K}_{(p)}$ is a divisor of m and so prime to p, F is an unramified extension over k. We see further $F = \overline{k}_{(p)}$ from Proposition 1. This completes our proof.

REMARK. This theorem is also valid under the assumption $h_{K,p} < p^f$ instead of the assumption $V_{p,K} < f$.

Particularly, as to an abelian extension we have the following

COROLLARY. i) *Let K be an abelian extension of degree m over k, $m = q_1^{a_1} \cdots q_r^{a_r}$ be the decomposition of m as a product of primes and L_i be*

a subfield of K such that $[L_i : k] = q_i^{a_i}$. If $V_{\mathfrak{p},K} < f_{q_i,\mathfrak{p}}$, then the p-class group of L_i is isomorphic with that of k.

ii) *Assume further that p is any prime number such that $p \not\equiv 0, 1 \bmod q_i$ for all i and that the extension $\overline{K}_{(p)}/K$ is cyclic. Then the p-class group of any subfield of K is isomorphic with that of k.*

This follows immediately from Proposition 1 and Theorem 1.

Let K/k be again a Galois extension of finite degree. When a subgroup of an ideal class group of K is left invariant under any element of $G(K/k)$, the subgroup will be called a *$G(K/k)$-invariant subgroup (of the ideal class group of K)*.

We shall now prove a complementary theorem of Theorem 1 as follows:

THEOREM 2. *Let K be a Galois extension of degree m over k, q_i, $i=1,\cdots,r$ be all the different prime factors of m and p be any prime number such that $p \not\equiv 0, 1 \bmod q_i$ for all i and let f be the minimal number of all $f_{q_i,\mathfrak{p}}$. If $h_{K,\mathfrak{p}} \neq 1$ and the p-class group of K has a $G(K/k)$-invariant subgroup of index p^a $(1 \leqq a < f)$ in it, then the class number of k is divisible by p^a.*

PROOF. In the case m is even, there exists no prime number p which satisfies the condition $p \not\equiv 0, 1 \bmod 2$. Therefore we assume that m is odd. Let E be the intermediate field of K and $\overline{K}_{(p)}$ corresponding to the $G(K/k)$-invariant subgroup above. E/k is then a Galois extension of degree mp^a over k. Putting E in the place of the field $\overline{K}_{(p)}$ in the proof of Theorem 1, the remaining part can then be proved in the same way as in the proof of Theorem 1.

REMARK. When the Galois group $G(\overline{K}_{(p)}/k)$ is supersolvable, the p-class group of K has always a $G(K/k)$-invariant subgroup of index p^a in it. (cf. [2])

We now prove the following

THEOREM 3. *Let K be a Galois extension over k of degree p^a. If $a_p(K/k) = 1$, then h_K is prime to p. If, further, there exists no abelian unramified extension of k in K, then h_K and h_k are both prime to p.*

PROOF. Suppose that h_K is divisible by p. Then the Galois group $G(\overline{K}_{(p)}/K)$ is not trivial and the Galois group $G(\overline{K}_{(p)}/k)$ is a p-group. Put $\mathfrak{G} = G(\overline{K}_{(p)}/k)$ and $\mathfrak{H} = G(\overline{K}_{(p)}/K)$ respectively. Since the group $\mathfrak{G}$ is supersolvable and $\mathfrak{H}$ is a normal subgroup of $\mathfrak{G}$, we can find a principal chain

through $\mathfrak{H}$ such that

$$\mathfrak{G} = \mathfrak{G}_0 \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_k \supset \mathfrak{H} \supset \mathfrak{G}_{k+1} \supset \cdots \supset \mathfrak{G}_{s-1} \supset \mathfrak{G}_s = e,$$

in which every $\mathfrak{G}_{i-1}/\mathfrak{G}_i$, $\mathfrak{G}_k/\mathfrak{H}$ and $\mathfrak{H}/\mathfrak{G}_{k+1}$ are of order p. As the group $\mathfrak{G}_{s-1}$ is a normal subgroup of order p in $\mathfrak{G}$, $\mathfrak{G}_{s-1}$ is contained in the center of $\mathfrak{G}$. (cf. [2]) From Artin's reciprocity law, we see that the group $\mathfrak{G}_{s-1}$ corresponds to a subgroup $\mathfrak{C}$ of the p-class group of K and, further, the subgroup $\mathfrak{C}$ is contained in the ambiguous p-class group of K with respect to k; this implies $a_p(K/k) \neq 1$ which contradicts the assumption. Hence h_K is prime to p. Furthermore, it follows from Lemma that the latter part of this theorem is also true.

Concerning subfields of cyclotomic fields $P_{(n)}$ we have

COROLLARY. *Let l be any prime number and K be any subfield of $P_{(n)}$ such that $[K:P]$ is a power of 2. Then the class number of K is odd. If l is of the form $2^r p^s+1$, then the class number of $P_{(0)}$ is prime to p if and only if the class number of K is prime to p.*

PROOF. Applying (*) in the remark of Proposition 2 to the extension K/P, we have $a=1$ and hence, it follows from Theorem 3 that the first part of this corollary is true.

On the other hand, applying (*) to the extension $P_{(0)}/K$, we have $a=h_K$. If h_K is prime to p, then we have $a_p(P_{(0)}/K)=1$. Therefore the class number of $P_{(0)}$ is prime to p, as we see from Theorem 3. The 'only if' part follows immediately from Lemma.

REMARK. The following results are known:

The class number of a quadratic field $P(\sqrt{p^*})$ is odd, where $p^*=(-1)^{\frac{p-1}{2}} \cdot p$. In the case where $l = 2$, the class number of $P_{(0)}$ is odd. In the case where $l=2^r+1$, the class number of the maximal real subfield of $P_{(0)}$ is odd. (cf. [4], [5], [6])

When $a_p(K/k) \neq 1$ we have the following theorem which is a generalization of a theorem of K. Iwasawa. (cf. [5])

THEOREM 4. *Let K be a Galois extension of degree p^a over k. Assume that there exists exactly one prime divisor of k which is ramified for the extension K/k. If the class number of K is divisible by p, then the class number of k is divisible by p.*

PROOF. Let $\mathfrak{p}$ be a prime divisor of $\overline{K}_{(p)}$ dividing the ramified prime divisor of k and $T_{\mathfrak{p}}$ be the inertia group of $\mathfrak{p}$ in $\overline{K}_{(p)}$. Then there exists a maximal normal subgroup $\mathfrak{H}$ of $G(\overline{K}_{(p)}/k)$ containing $T_{\mathfrak{p}}$, as the Galois group $G(\overline{K}_{(p)}/k)$ is a p-group. It is easy to see that all the inertia groups of the other prime divisors of $\overline{K}_{(p)}$ are also contained in the subgroup $\mathfrak{H}$. Now, let F be the intermediate field of k and $\overline{K}_{(p)}$ corresponding to the subgroup $\mathfrak{H}$. F is then an abelian unramified extension of degree p over k and hence, is contained in $\overline{k}_{(p)}$. Therefore the class number of k is divisible by p.

REMARK. When K/k is cyclic and there exists exactly one ramified prime divisor of k which is, further, fully ramified for K/k, this theorem is proved by K. Iwasawa [5].

PROPOSITION 3. *Let K be a Galois extension of degree m over k and p be a prime factor of m. Assume that there exists a prime divisor $\mathfrak{p}$ of k which is fully ramified by the extension K/k and no ramified prime divisor other than $\mathfrak{p}$. Then the p-class group of K is isomorphic with that of k if and only if the Galois group $G(K/k)$ leaves the p-class group of K fixed elementwise.*

PROOF. We first prove the 'only if' part. From the assumptions it follows that $K\cap\overline{k}_{(p)}=k$ and $K\overline{k}_{(p)}=\overline{K}_{(p)}$. Therefore the Galois group $G(\overline{K}_{(p)}/k)$ is the direct product of $G(\overline{K}_{(p)}/K)$ and $G(\overline{K}_{(p)}/\overline{k}_{(p)})$. This proves what we wanted. We prove the converse. Let $\mathfrak{P}$ be a prime divisor of $\mathfrak{p}$ in $\overline{K}_{(p)}$ and $T_{\mathfrak{P}}$ be the inertia field of $\mathfrak{P}$ in $\overline{K}_{(p)}$. It can then be readily verified that $[\overline{K}_{(p)}:T_{\mathfrak{P}}]=m$, $\overline{K}_{(p)}=KT_{\mathfrak{P}}$ and $K\cap T_{\mathfrak{P}}=k$. As we have seen, it is clear that $T_{\mathfrak{P}}/k$ is normal and hence, abelian. Furthermore, we have $T_{\mathfrak{P}}=\overline{k}_{(p)}$ by Lemma. This proposition is thus completely proved.

Combining Proposition 2 and Proposition 3 we obtain

PROPOSITION 4. *Let K be a Galois extension over k and assume that there exists exactly one ramified prime divisor of k which is further fully ramified by the extension K/k. Then the absolute ideal class group of K is isomorphic with that of k if and only if the Galois group $G(K/k)$ leaves the absolute ideal class group of K fixed elementwise.*

3. We consider the case where the ground field is the rational number field P.

We shall consider the splitting field $L_{n,a}$ of a binomial equation

$$x^n-a=0\,,\quad a\neq 0\in P$$

with respect to P, where l is an odd prime number.

Let $q_1, \cdots, q_r$ be all the different odd prime factors of $l-1$. In the case $L_{n,a}=P_{(0)}$, we let p be any prime number such that $p \not\equiv 0, 1 \bmod q_i$ for all i. In the other cases, $L_{n,a} \neq P_{(0)}$, we let p be any prime number such that $p \not\equiv 0$, $1 \bmod l$ and $\bmod q_i$ for all i. Furthermore, let f be the minimal number of all $f_{q_i,p}$ and let K be a subfield of $P_{(0)}$ such that $[K:P]$ is the highest power of 2 dividing $l-1$. K is also a subfield of $L_{n,a}$. Suppose that h_K is prime to p. Applying Theorem 1 to the extension $L_{n,a}/K$, we then see that the class number of $L_{n,a}$ is prime to p or divisible by p^f.

Let $P^+_{(n)}$ be the maximal real subfield of $P_{(n)}$. If l is of the form $8m+5$, then the real quadratic field $P(\sqrt{l})$ is a subfield of $P^+_{(n)}$ and the relative degree of the extension $P^+_{(n)}/P(\sqrt{l})$ is odd. If the class number of $P(\sqrt{l})$ is prime to p, it follows from Theorem 1 that the class number of $P^+_{(n)}$ is prime to p or divisible by p^f. With these notations, we summarize our results in the following

THEOREM 5. i) *If the class number of K is prime to p, then the class number of $L_{n,a}$ is prime to p or divisible by p^f.*

ii) *The case l is of the form $4m+3$. Then the class number of $P^+_{(n)}$ is prime to p or divisible by p^f.*

iii) *The case l is of the form $8m+5$. If the class number of the quadratic field $P(\sqrt{l})$ is prime to p, then that of $P^+_{(n)}$ is prime to p or divisible by p^f.*

REMARK. This result is a generalization of Theorem 3 in my previous paper [7].

From Proposition 1 and Theorem 1 we obtain immediately the following

PROPOSITION 5. *Let E be an abelian extension of degree m over P, L_i be a subfield of E such that $[L_i:P]$ is the q_i-part of m and f be the maximal number of all $f_{q_i,p}$. If the class number of E is divisible by p, then that of E is at least divisible by p^f.*

REFERENCES

[1] C. CHEVALLEY, Relation entre le nombre de classes d'un sous-corps et celui d'un sur-corps, C. R., Paris, 192(1931), 257-258.

[2] M. HALL, The theory of groups, New York, 1959.

[3] H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, I, Ia, II, Jahresber. der Deutsch. Math. Ver., 35(1926).

[4] H. HASSE, Über die Klassenzahl abelscher Zahlkörper, Berlin, 1952.

[5] K. IWASAWA, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg, 20(1957), 257-258.

[6] M. MORIYA, Über die Klassenzahl eines relativ-zyklischen Zahlkörpers vom Primzahlgrad, Proc. Japan Acad., 6(1930), 245-247.

[7] A. YOKOYAMA, On prime factors of the class numbers of cyclotomic fields, Bulletin of the Education Faculty, Shizuoka Univ., 15(1964), 1-5.

SHIZUOKA UNIVERSITY.