J. Math. Soc. Japan
Vol. 19, No. 2, 1967

On the relative class number of finite algebraic number fields

By Akio YOKOYAMA

(Received May 10, 1966)
(Revised Nov. 2, 1966)

Let l be an odd prime number. The relative class number, the so-called first factor h_n^- of the class number of the cyclotomic field generated by a primitive l^{n+1}-th root of unity over the rational number field is given by the well-known formula ($n \geqq 0$):

$$h_n^- = 2l^{n+1} \prod_{\chi} \Big(-\frac{1}{2l^{n+1}} \sum_m m\chi^{-1}(m) \Big),$$

where m ranges over all integers satisfying $0 \leqq m < l^{n+1}$, $(m, l)=1$, and χ over all characters of the multiplicative group of integers mod l^{n+1} with $\chi(-1)=-1$[1]. According to this formula, it can be observed that h_n^- is divisible by h_0^-. Let L and M be totally imaginary quadratic fields over a totally real algebraic number field L_0 and M_0, respectively. Let further L and L_0 be subfields of M and M_0 respectively. Can it be proved further that the relative class number of M/M_0, i.e. the ratio of the class number of M to that of M_0 is divisible by the relative class number of L/L_0 in such a case? (Both relative class numbers of M/M_0 and L/L_0 are rational integers (cf. Chevalley [**2**]).) The main purpose of this paper is to consider this problem in more general cases. The main results are as follows. Let E and F be finite extensions of a finite algebraic number field k such that E is a Galois extension of k and $E \cap F = k$. We shall show that if there exists no non-trivial unramified abelian extension of F contained in the composite field EF, then for any prime number p prime to the relative degree of F/k, the p-part of the relative class number of F/k is less than or equal to the p-part of the relative class number of EF/E (Theorem 1). (In this paper, "an unramified abelian extension of F" means a subfield of the Hilbert's class field over F.) As an interesting consequence of this, we shall show that for any totally real algebraic number field L_0 of finite degree and any rational integer n prime to the degree of L_0, there are infinitely many totally imaginary quadratic extensions L of L_0 so that the relative class

1) See Iwasawa [**5**], in which the class number formula is used in this formula: the formula in Hasse [**3**] is slightly different from this formula.

number of each L/L_0 is divisible by n (Theorem 2). Finally we obtain a necessary and sufficient condition for the relative class number of F/k to coincide with the relative class number of EF/E (Theorem 4).

Let p be any prime number. The Sylow p-subgroup of the absolute ideal class group (in wide sense) of a finite algebraic number field 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 k. Then the Galois group of K/k acts on the p-class group of K in an obvious way. Now, the subgroup of all ideal classes in the p-class group of K which are left invariant under the Galois group of K/k will be called the *ambiguous p-class group of K with respect to k.*

Let K be a finite extension of degree m over k and p be any prime number prime to m. 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. We shall again denote the image of $\mathfrak{C}_k$ under the isomorphism φ by the same notation $\mathfrak{C}_k$. Furthermore, the kernel of the norm map $N_{K/k}:\mathfrak{C}_K\to\mathfrak{C}_k$ will be denoted by $\mathfrak{K}_{K/k}$. Since m and p are relatively prime, the norm map $N_{K/k}$ is surjective. Let ψ be the product of the norm map $N_{K/k}$ and the isomorphism φ. Then we have Ker $\psi=\mathfrak{K}_{K/k}$. We see further that $\mathfrak{K}_{K/k}$ does not contain non-principal ideal classes in $\mathfrak{C}_k$. Therefore, $\mathfrak{C}_K$ is the direct product of $\mathfrak{C}_k$ and $\mathfrak{K}_{K/k}$. Let K be a Galois extension of k. Then we see that $\mathfrak{C}_k$ coincides with the ambiguous p-class group of K with respect to k.

Thus the following lemma is proved:

LEMMA. *Let K be a finite extension of k and p be any prime number prime to the relative degree of K/k. Then the p-class group $\mathfrak{C}_K$ of K is the direct product of the p-class group $\mathfrak{C}_k$ of k and the kernel $\mathfrak{K}_{K/k}$ of the norm map $N_{K/k}:\mathfrak{C}_K\to\mathfrak{C}_k$. If K is a Galois extension of k, then the p-class group of k coincides with the ambiguous p-class group of K with respect to k.*

THEOREM 1. *Let E and F be finite extensions of k such that E is a Galois extension of k and $E\cap F=k$; let p be any prime number prime to the relative degree of F/k. Let further K denote the composite field EF. If there exists no non-trivial unramified abelian extension of F contained in K, then*

$$\frac{h_{F,p}}{h_{k,p}}\leqq\frac{h_{K,p}}{h_{E,p}}\,.$$

PROOF. Let $\mathfrak{C}_K$, $\mathfrak{C}_E$, $\mathfrak{C}_F$ and $\mathfrak{C}_k$ be the p-class groups of K, E, F and k respectively. Let $\mathfrak{K}_{K/E}$ and $\mathfrak{K}_{F/k}$ denote the kernels of the norm map $N_{K/E}:\mathfrak{C}_K$

$\rightarrow \mathfrak{C}_E$ and the norm map $N_{F/k}: \mathfrak{C}_F \rightarrow \mathfrak{C}_k$ respectively. Then it follows from Lemma

$$(1) \qquad \mathfrak{C}_K = \mathfrak{C}_E \times \mathfrak{R}_{K/E} \text{ (direct)}, \qquad \mathfrak{C}_F = \mathfrak{C}_k \times \mathfrak{R}_{F/k} \text{ (direct)}.$$

Since the norm is transitive, we see that the image of $\mathfrak{R}_{K/E}$ under the norm map $N_{K/F}$ is contained in $\mathfrak{R}_{F/k}$. Furthermore, we have $N_{K/F}(\mathfrak{C}_E) \subset \mathfrak{C}_k$, as each ideal class in $\mathfrak{C}_E$ contains an ideal of E. Let $C(K)$ and $C(F)$ denote the absolute ideal class groups (in the wide sense) of K and F respectively. By class field theory, the index of $N_{K/F}(C(K))$ in $C(F)$ is equal to the degree of the maximal unramified abelian extension of F contained in K. Therefore, we have $N_{K/F}(C(K)) = C(F)$. From this it follows that the norm map $N_{K/F}: \mathfrak{C}_K \rightarrow \mathfrak{C}_F$ is surjective. Using (1), we see further that the restriction of the norm map $N_{K/F}$ to $\mathfrak{R}_{K/E}$ is also surjective. As the norm map $N_{K/F}$ is homomorphism, we have

$$(\mathfrak{R}_{F/k}:1) \leqq (\mathfrak{R}_{K/E}:1)$$

and our assertion follows.

In the case p is any prime number prime to the relative degree of K/k, we see at once that the norm map $N_{K/F}: \mathfrak{C}_K \rightarrow \mathfrak{C}_F$ is surjective, so that there is no need for assuming that there exists no non-trivial unramified abelian extension of F contained in K.

Let L_0 be a totally real algebraic number field and let n be any rational integer prime to the degree of L_0. It is well known that there exists infinitely many imaginary quadratic number fields, each with class number divisible by a given rational integer (cf. Ankeny and Chowla [**1**] or Nagell [**6**]). Therefore, we know that there are infinitely many imaginary quadratic number fields M so that the class number of each M is divisible by n and M, L_0 are independent over the rational number field P, i.e. $M \cap L_0 = P$. Let L denote the composite field L_0M. Then there exists no non-trivial unramified abelian extension of L_0 contained in L. Applying Theorem 1 to the extension L/P, namely putting $L=K$, $L_0=F$ and $M=E$, we have for any prime factor p of n

$$h_{L_0,p} \leqq \frac{h_{L,p}}{h_{M,p}} \qquad \text{and so} \qquad h_{M,p} \leqq \frac{h_{L,p}}{h_{L_0,p}}.$$

Hence the relative class number of L/L_0[2] is divisible by n, because the class number of M is divisible by n.

Thus we have the following

THEOREM 2. *Let L_0 be any totally real algebraic number field of finite degree and let n be any rational integer prime to the degree of L_0. Then there are infinitely many totally imaginary quadratic extensions L of L_0 so that the*

2) The class number of L is divisible by that of L_0 (cf. Chevalley [**2**]).

relative class number of each L/L_0 is divisible by n.

Let p be an odd prime number and let h_n^- denote the first factor of the class number of the cyclotomic field $P_{(n)}$ ($n \geqq 0$) generated by a primitive p^{n+1}-th root of unity over the rational number field P. Then we can show another application of Theorem 1.

THEOREM 3. *Let K be a Galois extension of degree $p^n(p-1)$ over P which contains the cyclotomic field $P_{(0)}$ and let K_0 denote the maximal real subfield of K. Assume that there exists exactly one ramified prime divisor of $P_{(0)}$ which is further fully ramified for the extension $K/P_{(0)}$. Then the class number of K is divisible by p if and only if the relative class number of K/K_0 is divisible by p.*

In particular, the class number of the cyclotomic field $P_{(n)}$ is divisible by p if and only if the first factor h_n^- is divisible by p.

PROOF. First, from the assumption, we see that K is a quadratic extension of its maximal real subfield K_0 and from a theorem of Chevalley [**2**], that the relative class number of K/K_0 is a rational integer. The "if" part is clear. We prove the converse. It can be readily verified that the assumptions of Theorem 4 in [**7**] are satisfied for the extension $K/P_{(0)}$ with degree p^n and hence, the class number of $P_{(0)}$ is divisible by p, under the assumption that the class number of K is divisible by p. Then we know by Kummer's theorem that the first factor h_0^- is divisible by p (cf. Hasse [**4**, § 37]). Hence the relative class number of K/K_0 is divisible by p, as we see from Theorem 1.

In the excluding case where $p=2$, it is well known that the class number of the cyclotomic field $P_{(n)}$ is odd and we know further that the class number of K is odd (cf. Hasse [**4**, Satz 38] and [**7**, Theorem 3]).

For example, we consider the splitting field K of a binomial equation

$$x^p - p = 0$$

with respect to P, then K is a Galois extension of degree $p(p-1)$ over P containing $P_{(0)}$. Let $\mathfrak{p}$ be a prime divisor of p in $P_{(0)}$. As the prime number p is fully ramified for the extension $P_{(0)}/P$, i.e. $(p)=\mathfrak{p}^{p-1}$, the prime divisor $\mathfrak{p}$ is also fully ramified for the extension $K/P_{(0)}$ by Satz 9 in Hasse [**3**, Ia, § 11]. Furthermore, we see that no prime divisor of $P_{(0)}$ other than $\mathfrak{p}$ is ramified for $K/P_{(0)}$. Hence the splitting field K falls under the stated conditions in Theorem 3. The class number of K is divisible by p if and only if the relative class number of K/K_0 is divisible by p, where K_0 denotes the maximal real subfield of K.

THEOREM 4. *The assumptions being the same as in Theorem 1, let $\mathfrak{K}_{K/F}$ denote the kernel of the norm map $N_{K/F}: \mathfrak{C}_K \to \mathfrak{C}_F$, where $\mathfrak{C}_K$ and $\mathfrak{C}_F$ denote the p-class groups of K and F respectively. Then $h_{K,p}/h_{E,p} = h_{F,p}/h_{k,p}$ if and only* *if each ideal class in $\mathfrak{R}_{K/F}$ contains an ideal of E.*

PROOF. Let $\mathfrak{C}_E$, $\mathfrak{C}_k$, $\mathfrak{R}_{K/E}$ and $\mathfrak{R}_{F/k}$ denote the same notations as in the proof of Theorem 1. Then, as we have seen in the proof of Theorem 1, we have

$$\mathfrak{C}_K = \mathfrak{C}_E \times \mathfrak{R}_{K/E} \quad \text{(direct)} \tag{1.1}$$

$$\mathfrak{C}_F = \mathfrak{C}_k \times \mathfrak{R}_{F/k} \quad \text{(direct)}\,. \tag{1.2}$$

Let C be any ideal class in $\mathfrak{R}_{K/F}$. Using (1.1), we can write $C = C_1 \cdot C_2$ with an ideal class C_1 in $\mathfrak{C}_E$ and C_2 in $\mathfrak{R}_{K/E}$. Then we have $1 = N_{K/F}C = N_{K/F}C_1 \cdot N_{K/F}C_2$, in which $N_{K/F}C_1$ is contained in $\mathfrak{C}_k$ and $N_{K/F}C_2$ is contained in $\mathfrak{R}_{F/k}$. Thus we get $N_{K/F}C_2 = 1$ by (1.2), that is, C_2 is contained in $\mathfrak{R}_{K/F}$. Let $\mathfrak{R}$ be the kernel of the restriction of the norm map $N_{K/F}$ to $\mathfrak{R}_{K/E}$: $\mathfrak{R} = \mathfrak{R}_{K/E} \cap \mathfrak{R}_{K/F}$. Then the ideal class C_2 is contained in $\mathfrak{R}$. Now suppose that $h_{K,p}/h_{E,p} = h_{F,p}/h_{k,p}$. Then, from (1.1) and (1.2), it follows that $(\mathfrak{R}_{K/E}:1)$ is equal to $(\mathfrak{R}_{F/k}:1)$. Therefore, the restriction of the norm map $N_{K/F}$ to $\mathfrak{R}_{K/E}$ is an isomorphism so that $\mathfrak{R} = 1$ and hence, the ideal class C_2 mentioned above is necessarily the principal ideal class. Thus we have $C = C_1$. This means that $\mathfrak{R}_{K/F}$ is contained in $\mathfrak{C}_E$, as asserted in our theorem. Conversely, suppose that $\mathfrak{R}_{K/F}$ is contained in $\mathfrak{C}_E$. Then $\mathfrak{R}$ is contained in $\mathfrak{C}_E$. From (1.1), it then follows that $\mathfrak{R} = 1$, because $\mathfrak{R}$ is contained in $\mathfrak{R}_{K/E}$. Since the restriction of the norm map $N_{K/F}$ to $\mathfrak{R}_{K/E}$ is surjective, $\mathfrak{R}_{K/E}$ is isomorphic with $\mathfrak{R}_{F/k}$. Our assertion is thus completely proved.

In the case p is any prime number prime to the relative degree of K/k, there is no need for assuming that there exists no non-trivial unramified abelian extension of F contained in K, because the norm map $N_{K/F}$ is surjective.

When K is a Galois extension over E the p-class group of E coincides with the ambiguous p-class group of K with respect to E, as we see from Lemma. Therefore, Theorem 4 can be expressed in the following way:

The assumptions being the same as in Theorem 1, *assume further that K is a Galois extension over E. Then $h_{K,p}/h_{E,p} = h_{F,p}/h_{k,p}$ if and only if $\mathfrak{R}_{K/F}$ is contained in the ambiguous p-class group of K with respect to E.*

Shizuoka University

References

[1] N. C. Ankeny and S. Chowla, On the divisiblity of the class number of quadratic fields, Pacific J. Math., **5** (1955), 321–324.

[2] C. Chevalley, Relation entre le nombre de classes d'un sous-corps et celui d'un sur-corps, C. R. Acad. Sci. Paris, **192** (1931), 257–258.

[3] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, I, Ia, II, Jber. Deutsh. Math. Verein., **35** (1926).
[4] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akad. Verlag, Berlin, 1952.
[5] K. Iwasawa, A class number formula for cyclotomic fields, Ann. of Math., **76** (1962), 171-179.
[6] T. Nagell, Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg, **1** (1922), 140-150.
[7] A. Yokoyama, On class numbers of finite algebraic number fields, Tôhoku Math. J., **17** (1965), 349-357.