J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

On the divisibility of the class number in an algebraic number field

Dedicated to Professor Iyanaga on his sixties birthday

By Hideo YOKOI[1)]

(Received Jan. 25, 1967)

§ 1. Introduction.

In this paper, we shall consider the divisibility of the class number of an algebraic number field K, namely, the problem to determine which number may be a factor of the ideal class number of K. The fact that the class number of K is divisible by an integer c shows that there exists a subgroup of order c in the absolute ideal class group $\boldsymbol{C}_K$ of K, and also means that there exists an unramified abelian extension field of degree c over K. Therefore, the problem to investigate which number may be a factor of the ideal class number of K is reduced to corresponding problems related to the orders of subgroups of $\boldsymbol{C}_K$, or the degrees of unramified abelian extension fields of K.

Among such subgroups and extension fields, what we know well are the ambiguous class group and the genus field. Namely, let F be an algebraic number field, and let K be a cyclic extension of finite degree n over F. Then, it is well-known that the ambiguous class number $a=a(K/F)$ with respect to K/F is of the following form[2)]:

$$a=h_F\cdot\frac{\tilde{\Pi}e(\mathfrak{p})}{n\cdot[\varepsilon:\eta]}, \tag{1}$$

where $\tilde{\Pi}e(\mathfrak{p})$ is the product of the ramification exponents of all the finite and infinite prime divisors in F with respect to K/F, h_F is the class number of F, and $[\varepsilon:\eta]$ is the index of the subgroup (η) of units, which are norms of numbers in K, in the group (ε) of units in F.

In this case where K/F is cyclic, we have on the other hand

$$g^*=a=h_F\cdot\frac{\tilde{\Pi}e(\mathfrak{p})}{n\cdot[\varepsilon:\eta]}, \tag{2}$$

since the relative genus number $g^*=g^*(K/F)$ with respect to K/F is equal to

1) Supported in part by Research Institute for Mathematical Sciences, Kyoto University.

2) Cf. H. Yokoi [11], Lemma 4.

the ambiguous class number a with respect to K/F[3].

It is easily observed in this formula that the first factor h_F of the right side is the ideal class number of F, and the second factor $\frac{\tilde{\Pi} e(\mathfrak{P})}{n \cdot [\varepsilon : \eta]}$ of the right side is composed of prime factors of n only. Therefore, from our point of view, the first question is whether the ideal class number of K is divisible by the ideal class number of F, and the second question is whether the ideal class number of K is divisible by a prime factor of degree n.

As regards the first question, we already proved the following[4]:

THEOREM 1. *Let K/F be a finite extension over an algebraic number field F of finite degree such that K and the absolute class field $\tilde{F}$ of F are disjoint over F, i.e., $\tilde{F} \cap K = F$. Then we have*

(i) *the class number of K is always divisible by the class number of F,*

(ii) *if K/F is abelian, then the relative genus number with respect to K/F is divisible by the class number of F,*

(iii) *if K/F is cyclic, then the ambiguous class number with respect to K/F is divisible by the class number of F,*

(iv) *if K/F is cyclic and has one and only one ramified prime divisor in K/F, then the ambiguous class number with respect to K/F is equal to the class number of F.*

As regards the second question, we know the following:

THEOREM. (K. Iwasawa)[5] *Let F be an algebraic number field, and let K/F be a cyclic extension of a prime power degree l^ν such that there exists a completely ramified prime divisor in K/F and any other prime divisor is never ramified in K/F. Moreover, assume that the class number of K is divisible by l. Then, the class number of F is also divisible by l.*

The main aim of this paper is to prove the following more general theorem:

THEOREM 2. *Let F be an algebraic number field, and let K be a Galois extension of degree n over F. Denote by h_K* resp. *h_F the number of absolute ideal classes in K* resp. *F, and by $a = a(K/F)$ the number of ambiguous ideal classes with respect to K/F. Then we have*

(i) *if $a = h_F$ and h_K is prime to the degree n, then h_F is also prime to n,*

(ii) *if both h_F and h_K are prime to the degree n, then $a = h_F$,*

(iii) *if the degree n is a prime power l^ν, h_F is prime to the degree n, and moreover $a = h_F$, then h_K is also prime to n, h_K is divisible by h_F, and moreover $\frac{h_K}{h_F} \equiv 1 \pmod{l}$.*

After the proof of this main theorem, we shall give some corollaries as

3) Cf. H. Yokoi [**11**], Prop. 1.

4) Cf. H. Yokoi [**11**], Theorem 1.

5) Cf. K. Iwasawa [**2**].

application of this main theorem, and we shall add a theorem on the divisibility of the class number by a ramified prime divisor in an absolutely normal extension field.

As an example of an algebraic number field K such that the class number of K is composed of only prime factors of the class number of subfields in K and of the degree, we can give absolutely abelian fields of (2, 2)-type [6].

Another more interesting example is an absolutely abelian fields of $(l, l, \cdots, l)$--type for any prime l.

§ 2. Proof of main theorem.

In order to prove our main theorem, we require three lemmas.

LEMMA 1. *Let K/F be a Galois extension of a prime power degree l^ν. Denote by h_K the ideal class number of K, and by $a=a(K/F)$ the ambiguous class number with respect to K/F. Then, we have $h_K \equiv a \pmod{l}$.*

PROOF. Let $G=G(K/F)$ be the Galois group of K/F. Then, for any ideal class C of K, $G_C=\{\tau \in G : C^\tau = C\}$ is a subgroup of G. Since G is of prime power order l^ν, we may put $r_C=[G: G_C]=l^{\nu_C}$. Then, the index r_C expresses the number of all distinct G-conjugate ideal classes of C, and we can easily verify

$$\nu_C=0 \rightleftarrows r_C=1 \rightleftarrows G=G_C \rightleftarrows C \in \boldsymbol{A},$$

where $\boldsymbol{A}$ is the group of ambiguous ideal classes with respect to K/F. In other words, this shows that

$$C \notin \boldsymbol{A} \rightleftarrows \nu_C \neq 0 \rightleftarrows r_C=l^{\nu_C} \neq 1 \rightleftarrows r_C \equiv 0 \pmod{l}.$$

Therefore, we get finally

$$h_K=a+\Sigma'_{C\in A} r_C \equiv a \pmod{l},$$

where the summation Σ' is extended over all representatives of distinct G-conjugate classes which do not contain any ambiguous ideal class of K/F.

LEMMA 2. *Let K/F be a Galois extension of degree n. Denote by $a=a(K/F)$ the ambiguous class number with respect to K/F, and by $a_0=a_0(K/F)$ the number of ideal classes represented by ambiguous ideals with respect to K/F. Then, $\frac{a}{a_0}$ is composed of prime factors of n only.*

PROOF. Let C be an ambiguous ideal class with respect to K/F, and let $\mathfrak{A}$ be an ideal in the class C. Then, the norm $N_{K/F}\mathfrak{A}$ of $\mathfrak{A}$ with respect to K/F is contained in the ideal class C^n of K. On the other hand, the norm $N_{K/F}\mathfrak{A}$ of $\mathfrak{A}$ is clearly an ambiguous ideal with respect to K/F. Therefore, the ideal class C^n is an ambiguous ideal class represented by an ambiguous ideal with

6) Cf. T. Kubota [3] and S. Kuroda [4].

respect to K/F. This shows that $\frac{a}{a_0}$ is composed of prime factors of n only.

LEMMA 3. *Let K/F be a Galois extension of degree n. Denote by h_F the ideal class number of F, and by $a=a(K/F)$ the ambiguous class number with respect to K/F. Suppose that $\frac{a}{h_F}$ is prime to n. Then, we have $\frac{a}{h_F}=1$; a is equal to h_F.*

PROOF. If we put $a_0'=\frac{a}{a_0}$, then it follows immediately from lemma 2 that a_0' is composed of prime factors of n only. Since $a=a_0'\cdot a_0$ and $a_0=\frac{\Pi e(\mathfrak{p})}{[H^1(G, E_K)]}\cdot h_F$ [7], we have the following equality:

$$\frac{a}{h_F}=a_0'\cdot\frac{\Pi e(\mathfrak{p})}{[H^1(G, E_K)]}. \tag{3}$$

Here, it is easily seen that the right side of this equality (3) is composed of prime factors of n only, and by the assumption the left side of the equality (3) does not contain any prime factor of n. Therefore, both sides of the equality (3) are equal to 1; this shows $a=h_F$, which proves our lemma 3.

PROOF OF THEOREM 2. (i) This is obvious from the assumption $a=h_F$ and from the fact that the ambiguous class number a with respect to K/F is a divisor of the class number h_K of K.

(ii) First, we see from the assumption $(h_K, n)=1$ that the divisor a of h_K is prime to n. Therefore, it follows at once from the assumption $(h_F, n)=1$ that $\frac{a}{h_F}$ does not contain any prime factor of n. Thus, we obtain finally $a=h_F$ from lemma 3.

(iii) There exists an integer b such that $h_K=a\cdot b$, because the class number h_K of K is divisible by the ambiguous class number a with respect to K/F. Since $a\equiv h_K \pmod{l}$ by lemma 1, we obtain $a\equiv a\cdot b \pmod{l}$. Hence $a(b-1)\equiv 0 \pmod{l}$. On the other hand, it follows immediately from assumptions $a=h_F$ and $(h_F, l^\nu)=1$ that a is prime to l. Therefore, we have $b\equiv 1 \pmod{l}$. Thus, we see finally that $h_K=a\cdot b$ is prime to l and $\frac{h_K}{h_F}=\frac{h_K}{a}\equiv 1 \pmod{l}$.

§ 3. Applications.

By using these theorems and lemmas, many known results on divisibility of the ideal class number can be shortly proved, and can also be easily generalized.

For instance, the above mentioned theorem of K. Iwasawa is generalized by using theorems 1 and 2 as follows:

COROLLARY 1. *Let K/F be a Galois extension of a prime power degree l^ν,*

7) Cf. H. Yokoi [**11**], Lemma 1.

and assume that the ambiguous class number a with respect to K/F is equal to the class number h_F of F. Then, we have $(h_K, l)=1$ if and only if $(h_F, l)=1$.

Moreover, a result of M. Moriya[8], namely, "*Let K/F be a cyclic extension of a prime degree l, and assume that the ambiguous class number a with respect to K/F is prime to l. Then, h_K is also prime to l.*" is generalized by using lemma 1 as follows:

COROLLARY 2. *Let K/F be a Galois extension of a prime power degree l^ν, and assume that the ambiguous class number a with respect to K/F is prime to l. Then, the ideal class number h_K of K is also prime to l.*

If, moreover, we assume that a is equal to 1, *then h_K is congruent to* 1 mod *l.*

Furthermore, in the special case of absolutely Galois extension, we can prove following two corollaries by using theorem 2 and lemma 1.

COROLLARY 3. *Let $K/\boldsymbol{Q}$ be an absolutely Galois extension of a prime power degree l^ν. Then, the class number h_K of K is congruent to* 0 *or* 1 mod *l, and the following three conditions are all equivalent to each other:*

(i) *h_K is prime to l,*

(ii) *the ambiguous class number a with respect to $K/\boldsymbol{Q}$ is equal to* 1,

(iii) *h_K is congruent to* 1 mod *l.*

PROOF. It follows first from theorem 2 that $a=1$ is equivalent to $(h_K, l)=1$, because the class number $h_{\boldsymbol{Q}}$ of the rational number field $\boldsymbol{Q}$ is equal to 1. Next, if $a=1$, then by lemma 1 we have $h_K \equiv a=1 \pmod{l}$. Conversely, if $h_K \equiv 1 \pmod{l}$, then $(h_K, l)=1$ is obvious. Hence, we obtain finally $a=1$ from the above assertion.

COROLLARY 4[9]. *Let $K/\boldsymbol{Q}$ be an absolutely cyclic extension of an odd prime power degree l^ν. Then, the following four conditions are all equivalent to each other:*

(i) *the class number h_K of K is prime to l,*

(ii) *the ambiguous class number a with respect to $K/\boldsymbol{Q}$ is equal to* 1,

(iii) *the class number h_K is congruent to* 1 mod *l,*

(iv) *the extension $K/\boldsymbol{Q}$ has a prime power conductor.*

PROOF. For the proof of this corollary, it is sufficient to show that $a=1$ is equivalent to the assertion of (iv), because the first three conditions of this corollary are all equivalent to each other by corollary 3.

From the assumption that the ground field F is the rational number field $\boldsymbol{Q}$ and $K/\boldsymbol{Q}$ is an extension of odd degree, we have $h_F=h_{\boldsymbol{Q}}=1$ and $[\varepsilon : \eta]=1$ in the formula (1) of the ambiguous class number with respect to a cyclic

8) Cf. M. Moriya [8].

9) In the special case where $K/\boldsymbol{Q}$ is an absolutely cyclic extension of an odd prime degree, this corollary is already obtained in M. Moriya [8], [9], H. W. Leopoldt [7], and S.-N. Kuroda [6].

extension. Hence, it follows first from (1) that $a=1$ is equivalent to $\Pi e(\mathfrak{p})=l^{\nu}$.

Next, we have $\Pi e(\mathfrak{p})=l^{\nu}$ if and only if there exists one and only one ramified prime divisor and it is completely ramified in $K/\boldsymbol{Q}$.

For, if there were no prime divisor which has the rational number field $\boldsymbol{Q}$ as the inertia field in $K/\boldsymbol{Q}$, then there would exist an intermediate field of $K/\boldsymbol{Q}$ which is an unramified abelian extension over $\boldsymbol{Q}$ with the degree at least l, because the extension $K/\boldsymbol{Q}$ is cyclic of prime power degree l^{ν}. However, this is a contradiction. So, there exists at least one prime divisor which has the rational number field $\boldsymbol{Q}$ as the inertia field in $K/\boldsymbol{Q}$. Since such a prime divisor is completely ramified in $K/\boldsymbol{Q}$, it follows easily from the condition $\Pi e(\mathfrak{p})=l^{\nu}$ that there exists one and only one ramified prime divisor and it is completely ramified in $K/\boldsymbol{Q}$. Conversely, if there exists one and only one ramified prime divisor and if it is completely ramified in $K/\boldsymbol{Q}$, then we have obviously $\Pi e(\mathfrak{p})=l^{\nu}$.

Finally, it is easy to verify that the conductor of $K/\boldsymbol{Q}$ is a prime power if and only if there exists one and only one ramified prime divisor and it is completely ramified in $K/\boldsymbol{Q}$.

Thus, we prove our corollary.

REMARK. In case of quadratic field, the following fact is well-known:

"The ideal class number (in narrow sense) of a quadratic field is odd if and only if the discriminant of the quadratic field is a prime power."

§ 4. Divisibility of the class number by ramified prime divisor.

Furthermore, on the divisibility of the ideal class number, there is a question whether the ideal class number is divisible by a ramified prime divisor. Here, we shall consider this question in the special case where an absolutely abelian field has only one ramified prime divisor.

THEOREM 3. (i) *Let K be a quadratic field of a prime power conductor p^{ν}. Then, the ideal class number of K is always prime to p.*

(ii) *Let K be an absolutely abelian field of a regular prime power conductor p^{ν}. Then, the ideal class number of K is prime to p*[10].

(iii) *Let K be an absolutely abelian field of an irregular prime power conductor p^{ν}, and assume that K contains a primitive p-th root of unity. Then, the ideal class number of K is divisible by p.*

PROOF. (i) This is easily seen from the following well-known result[11]:

"If K is a quadratic field $\boldsymbol{Q}(\sqrt{p})$ such that p is a prime number satisfying

10) This part (ii) is already known by Iwasawa [2]. Here, we add a simple proof of it only for the sake of completeness.

11) Cf. e.g. M. Gut [1], M. Newman [10] etc.

$p \equiv 1 \pmod 4$, *then the ideal class number of* K *is less than* p."

In order to prove the remaining part of theorem 3, we denote by ζ_{p^m} a primitive p^m-th root of unity for each $m \geqq 0$ and for a rational prime p, and denote by $\boldsymbol{Q}(\zeta_{p^m})$ the cyclotomic field obtained by adjoining ζ_{p^m} to the rational number field $\boldsymbol{Q}$.

(ii) Let p be an odd regular prime. Then, the ideal class number of cyclotomic field $\boldsymbol{Q}(\zeta_p)$ is prime to p. In the cyclic extension $\boldsymbol{Q}(\zeta_{p^\nu})/\boldsymbol{Q}(\zeta_p)$ of prime power degree $p^{\nu-1}$, p is completely ramified and any other prime divisor is not ramified. Therefore, the ambiguous class number is equal to the ideal class number of $\boldsymbol{Q}(\zeta_p)$ by theorem 1. Hence, it follows from theorem 2 that the ideal class number of $\boldsymbol{Q}(\zeta_{p^\nu})$ is also prime to p.

On the other hand, since K is a field of conductor p^ν, K is contained in the cyclotomic field $\boldsymbol{Q}(\zeta_{p^\nu})$, and the prime p is completely ramified in $\boldsymbol{Q}(\zeta_{p^\nu})/K$. Hence, it is easily seen from theorem 1 that the ideal class number of K is a factor of the ideal class number of $\boldsymbol{Q}(\zeta_{p^\nu})$.

Thus, we find that the ideal class number of K is prime to p.

In case of $p=2$, the ideal class number of $\boldsymbol{Q}(\zeta_{2^\nu})$ $(\nu \geqq 2)$ is odd, because both $\boldsymbol{Q}(\zeta_2)=\boldsymbol{Q}$ and $\boldsymbol{Q}(\zeta_{2^2})=\boldsymbol{Q}(\sqrt{-1})$ have the ideal class number 1. Therefore, by a similar argument used in the above proof, we can also show that the ideal class number of K is odd.

(iii) Since K is an absolutely abelian field of prime power conductor p^ν and contains a primitive p-th root of unity, K is contained in the cyclotomic field $\boldsymbol{Q}(\zeta_{p^\nu})$ and contains the cyclotomic field $\boldsymbol{Q}(\zeta_p)$, namely, $\boldsymbol{Q}(\zeta_{p^\nu}) \supset K \supset \boldsymbol{Q}(\zeta_p)$. Moreover, p is completely ramified in $\boldsymbol{Q}(\zeta_{p^\nu})/\boldsymbol{Q}(\zeta_p)$, hence also in $K/\boldsymbol{Q}(\zeta_p)$. Thus, it follows easily from theorem 1 that the ideal class number of K is divisible by the ideal class number of $\boldsymbol{Q}(\zeta_p)$.

On the other hand, because of irregularity of p, the ideal class number of $\boldsymbol{Q}(\zeta_p)$ is divisible by p. Hence, the ideal class number of K is also divisible by p.

REMARK. Let K be a quadratic field which has a ramified prime divisor as a factor of the ideal class number. Then, it follows immediately from theorem 3 that the quadratic field K must have at least two ramified prime divisors. There is only one such quadratic field with the absolute value of the discriminant less than 100, namely, the imaginary quadratic field $K=\boldsymbol{Q}(\sqrt{-3\cdot 29})$. The ideal class number of this quadratic field is 6 and the ideal class group is a cyclic group of order 6 [12].

Mathematical Institute
Nagoya University

12) Cf. S.-N. Kuroda [5].

References

[1] M. Gut, Abschätzungen für die Klassenzahlen der quadratischen Körper, Acta Arith., **8** (1963), 113-122.
[2] K. Iwasawa, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg, **20** (1956), 257-258.
[3] T. Kubota, Über den bizyklischen biquadratischen Zahlkörper, Nagoya Math. J., **10** (1956), 65-85.
[4] S. Kuroda, Über den Dirichletschen Körper, J. Fac. Sci. Imp. Univ. Tokyo, **4** (1943), 383-406.
[5] S.-N. Kuroda, On the class number of imaginary quadratic number fields, Proc. Japan Acad., **40** (1964), 365-367.
[6] S.-N. Kuroda, Über die Klassenzahl eines relativ-zyklischen Zahlkörpers vom Primzahlgrade, Proc. Japan Acad., **40** (1964), 623-626.
[7] H. W. Leopoldt, Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr., **9** (1953), 351-362.
[8] M. Moriya, Über die Klassenzahl eines relativ-zyklischen Zahlkörpers von Primzahlgrad, Proc. Imp. Acad. Japan, **6** (1930), 245-247.
[9] M. Moriya, Über die Klassenzahl eines relativ-zyklischen Zahlkörpers vom Primzahlgrad, Japan. J. Math., **10** (1933), 1-18.
[10] M. Newman, Bounds for class numbers, Proc. Symp. pure Math., VIII, 1965, 70-77.
[11] H. Yokoi, On the class number of a relatively cyclic number field, Nagoya Math. J., **29** (1967), 31-44.