ON THE CLASS NUMBER OF A RELATIVELY CYCLIC NUMBER FIELD

HIDEO YOKOI

To Professor KIYOSHI NOSHIRO on the occasion of his 60th birthday

Introduction

Let l be a rational prime. For each $n \geqq 0$, denote by ζ_{l^n} a primitive l^n-th root of unity and by $\mathbf{Q}(\zeta_{l^n})$ the cyclotomic field obtained by adjoining ζ_{l^n} to the rational field $\mathbf{Q}$. Then a theorem which was proved by H. Weber[1] is well known:

THEOREM (H. WEBER). *The class number of* $\mathbf{Q}(\zeta_{2^\nu})$ *is odd.*

As a generalization of this theorem of Weber, Ph. Furtwängler[2] gave:

THEOREM (PH. FURTWÄNGLER). *The class number of* $\mathbf{Q}(\zeta_{l^\nu})$ *is divisible by the prime* l *if and only if the class number of* $\mathbf{Q}(\zeta_l)$ *is divisible by* l.

Moreover, Ph. Furtwängler[3] obtained

THEOREM (PH. FURTWÄNGLER). *Let* F *and* K *be two subfields of* $\mathbf{Q}(\zeta_{l^\nu})$. *If* F *is contained in* K, *then the class number of* K *is divisible by the class number of* F.

Afterwards, K. Iwasawa[4] generalized these theorems, and got

THEOREM (K. IWASAWA)[5]. *Let* F *be an algebraic number field, and let* K *be a finite Galois extension of* F. *Then we have the following facts:*

(*I*) *If there exists a prime divisor* P *of* F *which is fully ramified in the extension* K/F, *then the class number of* K *is divisible by the class number of* F.

(*II*) *If, furthermore,* K/F *is a cyclic extension of prime power degree* l^ν *and*

Received February 16, 1966.

1) Cf. H. Weber [21].

2) Cf. Ph. Furtwängler [7].

3) Cf. Ph. Furtwängler [6].

4) Cf. K. Iwasawa [12].

5) This theorem is often referred to e.g. in S.-N.Kuroda [16], K. Iwasawa [14] etc.

has no ramified prime divisor other than P, then conversely the class number of F is divisible by l provided the class number of K is divisible by l.

In the present paper, we shall give some results on the ideal class number of a relatively cyclic number field including, in particular, a generalization of the theorem of Iwasawa. We shall first give some preliminaries in § 2. Next we shall consider in § 3 the ideal class group of a relatively cyclic number field, and in § 4 ideal class numbers and unit groups. Finally in § 5 we shall give main theorems which include the theorem of Iwasawa.

§ 1. Notations

Generally, for an arbitrary abelian group B and its subgroup B', the order of B and the index of B' in B are denoted by $[B]$ and $[B : B']$, respectively.

The notations which are used throughout this paper for an arbitrary number field k are:

E_k: the group of units in k.

$\mathbf{C}_k$: the group of absolute ideal classes in k.

$\tilde{k}$: the absolute class field of k.

h_k: the number of absolute ideal classes in k.

Let K/F be a Galois extension with finite degree n over an algebraic number field F of finite degree, and $G = G(K/F)$ be the Galois group of K/F. Then, as usual, we shall denote by $H^r(G, B)$ or sometimes simply by $H^r(B)$ the r-dimensional Galois cohomology group of G acting on an abelian group B, and by $Q(B)$ the *Herbrand quotient* of B, i.e. $Q(B) = [H^0(G, B)]/[H^1(G, B)]$. Furthermore, we used the notations

$\Pi e(\mathfrak{p})$: product of the ramification exponents of all the finite prime divisors $\mathfrak{p}$ in F with respect to K/F.

$\Pi e(\mathfrak{p}_\infty)$: product of the ramification exponents of all the infinite prime divisors $\mathfrak{p}_\infty$ in F with respect to K/F.

$\tilde{\Pi} e(\mathfrak{p})$: product of the ramification exponents of all the finite and infinite prime divisors in F with respect to K/F, i.e. $\tilde{\Pi} e(\mathfrak{p}) = \Pi e(\mathfrak{p}) \times \Pi e(\mathfrak{p}_\infty)$.

(A) : the group of principal ideals in K.

(α) : *the group of principal ideals in F.*

(ε) : the group of units in F.

(η) : the group of units which are norms of numbers in K.

(A_0) : the group of ambiguous principal ideals in K/F.

$(\mathfrak{a}_F)$: the group of ideals in F.

$(\mathfrak{a}_0)$: the group of ambiguous ideals in K/F.

$\mathbf{A}$: the group of ambiguous ideal classes in K/F.

$\mathbf{A}_0$: the group of ideal classes represented by ambiguous ideals in K/F.

$\mathbf{A}_F$: the group of ideal classes of K represented by ideals of F.

$N\mathbf{C}_K$: the image by the norm homomorphism of $\mathbf{C}_K$ with respect to K/F.

${}_N\mathbf{C}_K$: the kernel by the norm homomorphism of $\mathbf{C}_K$ with respect to K/F.

a : the number of ambiguous ideal classes in K/F, i.e. $a = [\mathbf{A}]$.

a_0 : the number of ideal classes represented by ambiguous ideals in K/F, i.e. $a_0 = [\mathbf{A}_0]$.

h_0 : the number of ideal classes of F which become principal in K.

§ 2. Preliminaries

Let K/F be a Galois extension with finite degree n over an algebraic number field F of finite degree. Then we have the following two lemmas:

LEMMA 1.

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

Proof. For a_0 we have

$$a_0 = [\mathbf{A}_0] = [(A)(\mathfrak{a}_0) : (A)] = [(\mathfrak{a}_0) : (A_0)] = \frac{[(\mathfrak{a}_0) : (\alpha)]}{[(A_0) : (\alpha)]}.$$

On the other hand, we know that $H^1(G, E_K)$ is canonically isomorphic with the factor group of the group of ambiguous principal ideals of K modulo the group of principal ideals of F[6], i.e.

$$H^1(G, E_K) \cong (A_0)/(\alpha).$$

Since $[(\mathfrak{a}_0) : (\alpha)] = [(\mathfrak{a}_0) : (\mathfrak{a}_F)][(\mathfrak{a}_F) : (\alpha)] = \Pi e(\mathfrak{p}) \times h_F$, lemma 1 is clear.

LEMMA 2. *In the following diagram:*

---

6) Cf. K. Iwasawa [13] or A. Brumer-M. Rosen [3].

$$\begin{tikzcd}
 & (\mathfrak{a}_0) \arrow[d, dash] \\
 & (A_0)(\mathfrak{a}_F) \arrow[dl, dash] \arrow[dd, dash] \\
(A_0) \arrow[dd, dash] & \\
 & (\mathfrak{a}_F) \arrow[dl, dash] \\
(A_0)\cap(\mathfrak{a}_F) \arrow[d, dash] & \\
(\alpha) &
\end{tikzcd}$$

we have

$[(A_0)\cap(\mathfrak{a}_F) : (\alpha)] = h_0,$

$[(\mathfrak{a}_F) : (A_0)\cap(\mathfrak{a}_F)] = [(A_0)(\mathfrak{a}_F) : (A_0)] = h_F/h_0,$

$[(A_0) : (A_0)\cap(\mathfrak{a}_F)] = [(A_0)(\mathfrak{a}_F) : (\mathfrak{a}_F)] = [H^1(G, E_K)]/h_0,$

$[(\mathfrak{a}_0) : (A_0)(\mathfrak{a}_F)] = \Pi e(\mathfrak{p})\cdot h_0/[H^1(G, E_K)].$

In particular, h_0 *is a common divisor of* h_F *and* $[H^1(G, E_K)]$.

Proof. $[(A_0)\cap(\mathfrak{a}_F) : (\alpha)] = h_0$ is a direct consequence of our definition of h_0. Since $[(\mathfrak{a}_F) : (\alpha)] = h_F$, we have $[(\mathfrak{a}_F) : (A_0)\cap(\mathfrak{a}_F)] = h_F/h_0$, and hence $[(A_0)(\mathfrak{a}_F) : (A_0)] = h_F/h_0$. On the other hand, since $[(A_0) : (\alpha)] = [H^1(G, E_K)]$[7], we have $[(A_0) : (A_0)\cap(\mathfrak{a}_F)] = [H^1(G, E_K)]/h_0$, and hence $[(A_0)(\mathfrak{a}_F) : (\mathfrak{a}_F)] = [H^1(G, E_K)]/h_0$.

Finally, since by lemma 1 we know $[(\mathfrak{a}_0) : (A_0)] = a_0 = \Pi e(\mathfrak{p})\cdot h_F/[H^1(G, E_K)]$, we have $[(\mathfrak{a}_0) : (A_0)(\mathfrak{a}_F)] = \Pi e(\mathfrak{p})\cdot h_0/[H^1(G, E_K)]$.

From now in this §, we suppose especially that K/F is cyclic of finite degree n, and let σ be a generator of the Galois group G.

Lemma 3.

$$Q(E_K) = \Pi e(\mathfrak{p}_\infty)/n \text{ [8] } \textit{and } Q(C_K) = 1,$$

namely $[H^r(G, C_K)]$ *is a constant which does not depend on* r.

Proof. If we let E'_K be any G-subgroup of E_K with finite index, then by the lemma of Herbrand we have $Q(E'_K) = Q(E_K)$. In particular, we may choose the unit group of Artin[9] as E'_K, and we have $Q(E'_K) = \Pi e(\mathfrak{p}_\infty)/n$. Hence we

---

[7] Cf. K. Iwasawa [13] or A. Brumer-M. Rosen [3].

[8] Cf. C. Chevalley [5] for the case where K/F is cyclic of prime degree.

[9] Cf. E. Artin [2].

get $Q(E_K) = \Pi e(\mathfrak{p}_\infty)/n$.

On the other hand, since $\mathbf{C}_K$ is a finite G-group, we have $Q(\mathbf{C}_K) = 1$, namely $[H^0(G, \mathbf{C}_K)] = [H^1(G, \mathbf{C}_K)]$, and since K/F is cyclic, we know that $[H^r(G, \mathbf{C}_K)]$ is a constant which does not depend on r[10].

LEMMA 4. *Let n_1, n_2 be invariants of K/F determined by* $\frac{h_F}{n_1} = [\mathbf{C}_K : {}_N\mathbf{C}_K]$ *and* $\frac{\tilde{\Pi} e(\mathfrak{p})}{n_2 \cdot [\varepsilon : \eta]} = [{}_N\mathbf{C}_K : \mathbf{C}_K^{1-\sigma}] = [H^r(G, \mathbf{C}_K)]$ *for any integer r. Then, for the ambiguous class number a, we have* $a = \frac{h_F}{n_1} \times \frac{\tilde{\Pi} e(\mathfrak{p})}{n_2 \cdot [\varepsilon : \eta]}$. $n_1 \times n_2 = n$.

In particular, $h_F \times \tilde{\Pi} e(\mathfrak{p}) \equiv 0$ mod. n[11].

Proof. Since $[\mathbf{C}_K : {}_N\mathbf{C}_K] = [N\mathbf{C}_K]$ is a divisor of h_F and $[{}_N\mathbf{C}_K : \mathbf{C}_K^{1-\sigma}]$ is a divisor of $[(\alpha) : (\nu)] = \tilde{\Pi} e(\mathfrak{p})/[\varepsilon : \eta]$[12], we may obtain integers n_1, n_2 such that

$$h_F = [\mathbf{C}_K : {}_N\mathbf{C}_K] \times n_1, \quad \frac{\tilde{\Pi} e(\mathfrak{p})}{[\varepsilon : \eta]} = [{}_N\mathbf{C}_K : \mathbf{C}_K^{1-\sigma}] \times n_2.$$

Since $a = [\mathbf{A}] = [\mathbf{C}_K : \mathbf{C}_K^{1-\sigma}] = [\mathbf{C}_K : {}_N\mathbf{C}_K][{}_N\mathbf{C}_K : \mathbf{C}_K^{1-\sigma}]$, we have

$$a = \frac{h_F}{n_1} \times \frac{\tilde{\Pi} e(\mathfrak{p})}{n_2 \cdot [\varepsilon : \eta]}. \tag{1}$$

Furthermore, from lemma 3 we have for any integer r

$$\frac{\tilde{\Pi} e(\mathfrak{p})}{n_2 \cdot [\varepsilon : \eta]} = [{}_N\mathbf{C}_K : \mathbf{C}_K^{1-\sigma}] = [H^{-1}(G, \mathbf{C}_K)] = [H^r(G, \mathbf{C}_K)].$$

On the other hand, since for $a = [\mathbf{A}] = [\mathbf{A} : (A)(\mathfrak{a}_0)] \times [(A)(\mathfrak{a}_0) : (A)] = [\mathbf{A} : (A)(\mathfrak{a}_0)] \times a_0$ we have $[\mathbf{A} : (A)(\mathfrak{a}_0)] = [\eta : NE_K]$[13], we see at once from lemma 1

$$a = h_F \times \frac{\Pi e(\mathfrak{p})}{[H^1(E_K)]} \times [\eta : NE_K].$$

Since $\frac{[H^0(G, E_K)]}{[H^1(G, E_K)]} = Q(E_K) = \frac{\Pi e(\mathfrak{p}_\infty)}{n}$ by lemma 3, and $[H^0(G, E_K)] = [\varepsilon : NE_K] = [\varepsilon : \eta][\eta : NE_K]$, we have

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

10) Cf. lemma 4.

11) For the absolutely cyclic extension, this relation is already found in S. Iyanaga-T. Tamagawa [15]. Cf. H. W. Leopoldt [17], too.

12) Cf. lemma 5.

13) Cf. lemma 6.

Consequently, we obtain $n = n_1 \times n_2$ from (1) and (2), and it is clear from (2) that $h_F \times \tilde{\Pi} e(\mathfrak{p}) \equiv 0 \bmod n$ holds. Thus we have proved all the assertions of our lemma 4.

LEMMA 5. *$\tilde{\Pi} e(\mathfrak{p})$ is divisible by $[\varepsilon : \eta]$ and the conditions:*

$$\text{(I)} \quad a = h_F, \qquad \text{(II)} \quad \frac{\tilde{\Pi} e(\mathfrak{p})}{[\varepsilon : \eta]} = n$$

are equivalent to each other.

Proof. Let (ν) be the group of principal ideals (ν) in F such that ν is a norm residue of mod an ideal $\mathfrak{m}$ with respect to K/F. If we choose the ideal $\mathfrak{m}$ suitably, then the index of (ν) in (α) is equal to $\tilde{\Pi} e(\mathfrak{p})/[\varepsilon : \eta]$. Hence $\tilde{\Pi} e(\mathfrak{p})$ is divisible by $[\varepsilon : \eta]$.

On the other hand, it is evident from lemma 4 that $a = h_F$ and $\tilde{\Pi} e(\mathfrak{p}) = n \cdot [\varepsilon : \eta]$ are equivalent to each other.

LEMMA 6. *In the decomposition*

$$a = [\mathbf{A}] = [\mathbf{A} : (A)(\mathfrak{a}_0)][(A)(\mathfrak{a}_0) : (A)(\mathfrak{a}_F)][(A)(\mathfrak{a}_F) : (A)]$$

of a, we have $[\mathbf{A} : (A)(\mathfrak{a}_0)] = [\eta : NE_K]$, $[(A)(\mathfrak{a}_0) : (A)(\mathfrak{a}_F)] = \dfrac{\Pi e(\mathfrak{p}) \cdot h_0}{[H^1(G, E_K)]}$ and $[(A)(\mathfrak{a}_F) : (A)] = \dfrac{h_F}{h_0}$. Hence

$$a = [\eta : NE_K] \times \frac{\Pi e(\mathfrak{p}) \cdot h_0}{[H^1(G, E_K)]} \times \frac{h_F}{h_0}.$$

Proof. To any ideal $\mathfrak{a}$ belonging to an ambiguous class in K/F, there corresponds an unit η in (η) in the following way:
since $\mathfrak{a}^{1-\sigma}$ is a principal ideal, there exists a number θ in K such that $\mathfrak{a}^{1-\sigma} = (\theta)$, and $N\theta$ is clearly an unit η in F. In this correspondence, an ideal which belongs to an ideal class represented by an ambiguous ideal in K/F corresponds to an element in NE_K. Hence we have

$$[\mathbf{A} : (A)(\mathfrak{a}_0)] = [\eta : NE_K].$$

$[(\mathbf{A})(\mathfrak{a}_F) : (\mathbf{A})] = h_F/h_0$ is evident from the definition of h_0.

Finally, from the above two assertions and lemma 4 we see easily $[(\mathbf{A})(\mathfrak{a}_0) : (\mathbf{A})(\mathfrak{a}_F)] = \Pi e(\mathfrak{p}) \cdot h_0/[H^1(G, E_K)]$.

§ 3. Ideal class group

We shall, here, consider the relative genus field (Geschlechterkörper). Let K/F be an abelian extension of a number field F of finite degree, and let K^* be the maximal extension field which is abelian over F and unramified over K. After Hasse-Leopoldt[14] we shall call such a extension field K^* *the relative genus field with respect to* K/F, and call the relative degree $g^* = [K^* : K]$ *the relative genus number with respect to* K/F. Moreover, we shall call the ideal group H^*, to which the relative genus field K^* corresponds by class field theory, *the relative principal genus with respect to* K/F.

PROPOSITION 1. *If K/F is a cyclic extension of F, then the relative principal genus H^* with respect to K/F is the $(1-\sigma)$-th power of the ideal class group $\mathbf{C}_K$ of K, i.e. $H^* = \mathbf{C}_K^{1-\sigma}$, where σ is a generator of the Galois group $G = G(K/F)$. (Relative principal genus theorem)*

Moreover, the relative genus number g^* with respect to K/F is equal to the ambiguous class number a with respect to K/F, i.e. $g^* = a$.

Proof. Since K^* is an unramified abelian extension over K, K^* is contained in the absolute class field of K. Hence the relative principal genus H^* with respect to K/F contains the group of principal ideals in K and is composed of ideal classes in K. By the criterion of Hasse[15], the relative principal genus H^* must contain the $(1-\sigma)$-th power $\mathbf{C}_K^{1-\sigma}$ of the ideal class group $\mathbf{C}_K$. Moreover, H^* must be equal to $\mathbf{C}_K^{1-\sigma}$ because of the maximal property of the relative genus field K^*.

Next, in the homomorphism of $\mathbf{C}_K$ onto $\mathbf{C}_K^{1-\sigma}$ the kernel is evidently the group of ambiguous ideal classes $\mathbf{A}$ with respect to K/F. Hence from the theorem of homomorphism and the above relation $H^* = \mathbf{C}_K^{1-\sigma}$, it follows at once that

$$g^* = [K^* : K] = [\mathbf{C}_K : H^*] = [\mathbf{C}_K : \mathbf{C}_K^{1-\sigma}] = [\mathbf{A}] = a.$$

PROPOSITION 2. *Let K/F be a cyclic extension of degree n, and denote by a_1 the order of $\mathbf{A} \cap \mathbf{C}_K^{1-\sigma}$, i.e. $a_1 = [\mathbf{A} \cap \mathbf{C}_K^{1-\sigma}]$. Then we have*

(i) *$\mathbf{C}_K = \mathbf{A} + \mathbf{C}_K^{1-\sigma}$ is direct if and only if $a_1 = 1$,*

(ii) *a is not prime to the degree n if $a_1 \neq 1$,*

---

[14] Cf. H. Hasse [9] and H. W. Leopoldt [17].

[15] Cf. H. Hasse [10], II, § 5.

where we denote by σ a generator of the Galois group $G=G(K/F)$.

Proof. It is evident from the fact $h_K=a\times b_1$ that $\mathbf{C}_K=\mathbf{A}+\mathbf{C}_K^{1-\sigma}$ is direct if and only if $a_1=[\mathbf{A}\cap\mathbf{C}_K^{1-\sigma}]=1$, where $b_1=[\mathbf{C}_K^{1-\sigma}]$.

Next, we consider the factor group $\mathbf{B}=\mathbf{C}_K/\mathbf{A}$ of the ideal class group $\mathbf{C}_K$ modulo the group of ambiguous classes $\mathbf{A}$ with respect to K/F. Since the group of ambiguous classes $\mathbf{A}$ is a G-invariant subgroup of $\mathbf{C}_K$, the factor group $\mathbf{B}$ is also a G-module and $\mathbf{B}$ is isomorphic with the group $\mathbf{C}_K^{1-\sigma}$ as G-module. Therefore, if $a_1\neq 1$, then there exists an element $B\notin\mathbf{A}$ of $\mathbf{B}$ such that $B^\sigma=B$ holds. Namely, there exists an ideal class C of $\mathbf{C}_K$ such that $C^\sigma=CA$ holds for some ambiguous class A which is not the principal ideal class of $\mathbf{C}_K$. Since $C=C^{\sigma^n}=CA^n$, A^n is the principal ideal class of $\mathbf{C}_K$. Hence the order a of the group $\mathbf{A}$ is not prime to n.

PROPOSITION 3. *Let K/F be a cyclic extension of a prime power degree l^ν, and put $a_i=[\mathbf{A}\cap\mathbf{C}_K^{(1-\sigma)^i}]$, $b_j=[\mathbf{C}_K^{(1-\sigma)^j}]$ $(i,j=0,1,2,\dots)$. Then there exists an integer s $(\geqq 0)$ such that*

(i) $h_K=a_0\times a_1\times\cdots\times a_{s-1}\times a_s\times b_{s+1}$,

(ii) *a_i is divisible by a_{i+1} $(i=0,1,\dots,s-1)$,*

(iii) $\left\{\begin{array}{l} a_0\equiv a_1\equiv\cdots\equiv a_{s-2}\equiv 0 \\ a_{s-1}>a_s=1,\ b_{s+1}\equiv 1\end{array}\right. \quad (mod\ l).$

Proof. Since the group $\mathbf{C}_K$ is an abelian group with finite order h_K, there exists an integer $s\geqq 0$ such that $\mathbf{C}_K\supsetneqq\mathbf{C}_K^{1-\sigma}\supsetneqq\mathbf{C}_K^{(1-\sigma)^2}\supsetneqq\cdots\supsetneqq\mathbf{C}_K^{(1-\sigma)^{s-1}}\supsetneqq\mathbf{C}_K^{(1-\sigma)^s}=\mathbf{C}_K^{(1-\sigma)^{s+1}}=\cdots$, where σ is a generator of the Galois group $G=G(K/F)$.

Put here $\mathbf{A}_i=\mathbf{A}\cap\mathbf{C}_K^{(1-\sigma)^i}$ for convenience. Then, since $b_i=a_i\times b_{i+1}$ $(i=0,1,2,\dots)$ and

$$\mathbf{A}_0=\mathbf{A}\geqq\mathbf{A}_1\geqq\mathbf{A}_2\geqq\cdots\geqq\mathbf{A}_{s-1}\supsetneqq\mathbf{A}_s=\mathbf{A}_{s+1}=\cdots=\{1\},$$

we have first

$$h_K=b_0=a_0\times b_1=a_0\times(a_1\times b_2)=\cdots=(\Pi_{i=0}^s a_i)\times b_{s+1}$$

and $a_{s-1}\neq a_s=1$.

Next, since each $\mathbf{A}_{i+1}$ is a subgroup of $\mathbf{A}_i$, a_i is divisible by a_{i+1} for every integer $i=0,1,2,\dots,s-1$.

Finally, since $[\mathbf{A}\cap\mathbf{C}_K^{(1-\sigma)^{s-1}}]=a_{s-1}\neq 1$ holds, we know easily by the same way as in the proof of proposition 2 that the order a_{s-2} of $\mathbf{A}\cap\mathbf{C}_K^{(1-\sigma)^{s-2}}$ is not prime to the degree l^ν of K/F, namely a_{s-2} is divisible by l. Therefore we get $a_0 \equiv a_1 \equiv \cdots \equiv a_{s-2} \equiv 0$ mod. l. Since the order of the Galois group $G = G(K/F)$ is a prime power l^ν, each element of $\mathbf{C}_K^{(1-\sigma)^i}$ which is not in $\mathbf{A} \cap \mathbf{C}_K^{(1-\sigma)^i}$ has at least two, and so a multiple of the prime l different G-conjugates for every $i = 0, 1, \ldots$. Therefore we have at once $b_i \equiv a_i$ mod. l in the decomposition of b_i, i.e. $b_i = a_i \times b_{i+1}$. In particular, since $a_s = 1$ we have $b_{s+1} = a_s \times b_{s+1} = b_s \equiv a_s = 1$ mod. l.

§ 4. Ideal class number and unit group

Proposition 4. *Let K/F be any Galois extension of finite degree n. If h_F is prime to the degree n, i.e. $(h_F, n) = 1$, then*

(i) $\mathbf{A}_F = (A)(\mathfrak{a}_F) \cong \mathbf{C}_F$ i.e. $h_F = [\mathbf{A}_F : (A)]$

and $h_0 = n_1 = 1$,

(ii) $\mathbf{C}_K = \mathbf{A}_F + {}_N\mathbf{C}_K$ *is direct,*

(iii) $\Pi e(\mathfrak{p}) = [H^1(G, E_K)][(A)(\mathfrak{a}_0) : (A)(\mathfrak{a}_F)]$.

Proof. (i) By the assumption $(h_F, n) = 1$ and lemma 2, 4, we have $h_0 = 1$, $n_1 = 1$ at once. Hence we obtain $h_F = [\mathbf{A}_F : (A)]$ and a natural isomorphism $\mathbf{A}_F \cong \mathbf{C}_F$.

(ii) Let C be any ideal class in $\mathbf{A}_F \cap {}_N\mathbf{C}_K$. Then, since C belongs to ${}_N\mathbf{C}_K$, $N_{K/F}C$ is the principal ideal class I_F in $\mathbf{C}_F$. Moreover, since C also belongs to $\mathbf{A}_F$, we have $N_{K/F}C = \mathfrak{a}_F^n \cdot I_F$ for an ideal $\mathfrak{a}_F$ in F. Hence $\mathfrak{a}_F^n$ is a principal ideal of F. On the other hand, from the assumption $(h_F, n) = 1$, $\mathfrak{a}_F$ itself must be a principal ideal of F. Hence C is the principal ideal class of $\mathbf{C}_K$, namely $\mathbf{A}_F + {}_N\mathbf{C}_K$ is direct in $\mathbf{C}_K$.

Next, since h_F is prime to n, $\mathbf{A}_F$ is isomorphic to $\mathbf{C}_F$ and $N_{K/F}\mathbf{A}_F = \mathbf{C}_F$ holds. Hence we obtain $N_{K/F}\mathbf{C}_K = N_{K/F}\mathbf{A}_F = \mathbf{C}_F$. Thus we know that $\mathbf{C}_K$ is contained in $\mathbf{A}_F + {}_N\mathbf{C}_K$, namely we know that $\mathbf{C}_K = \mathbf{A}_F + {}_N\mathbf{C}_K$ is direct.

(iii) By proposition 4, (i) we have $a_0 = h_F \cdot [(A)(\mathfrak{a}_0) : (A)(\mathfrak{a}_F)]$. Hence we have $\Pi e(\mathfrak{p}) = [H^1(G, E_K)][(A)(\mathfrak{a}_0) : (A)(\mathfrak{a}_F)]$ by lemma 1.

Proposition 5. *If K/F is a cyclic extension of finite degree n and a is prime to the degree n, i.e. $(a, n) = 1$, then we have*

(i) $\mathbf{C}_K = \mathbf{A} + \mathbf{C}_K^{1-\sigma}$ *is direct,*

(ii) $a = h_F/h_0$, $h_0 = n_1$ *and* $a_1 = 1$,

(iii) $[H^1(G, E_K)] = \Pi e(\mathfrak{p}) \cdot h_0$, $[H^0(G, E_K)] = [\varepsilon : \eta] = h_0 \cdot \tilde{\Pi} e(\mathfrak{p})/n$, $H^r(G, \mathbf{C}_K)$

$=\{1\}$ *for any integer* r.

Moreover, if we assume that K/F *is cyclic with a prime power degree* l^{ν}, *then we have* $b_1=b_2\equiv 1$ *mod.* l, *where* $b_i=[\mathbf{C}_K^{(1-\sigma)^i}]$ $(i=1, 2)$.

Remark. The natural homomorphism $\mathbf{C}_F\to\mathbf{C}_K$ gives an isomorphism of $N\mathbf{C}_K\subset\mathbf{C}_F$ into $\mathbf{C}_K$. For, since $[N\mathbf{C}_K:(\alpha)]=h_F/n_1$, $[(A)(\mathfrak{a}_F):(A)]=h_F/h_0=[\mathbf{A}]$ and $h_0=n_1$ by proposition 5, (ii), we have $[N\mathbf{C}_K:(\alpha)]=[(A)(\mathfrak{a}_F):(A)]$.

Proof. By the assumption $(a, n)=1$ and proposition 2, we know that $a_1=1$ and $\mathbf{C}_K=\mathbf{A}+\mathbf{C}_K^{1-\sigma}$ is direct. In particular, we have $b_1=b_2\equiv 1$ mod. l by proposition 3 provided that K/F is cyclic with a prime power degree l^{ν}.

On the other hand, the numbers

$$\frac{h_F}{n_1},\ \frac{\tilde{\Pi}e(\mathfrak{p})}{n_2\cdot[\varepsilon:\eta]},\ [\eta:NE_K],\ \frac{\Pi e(\mathfrak{p})}{[H^1(G, E_K)]}\cdot h_0 \text{ and } \frac{h_F}{h_0}$$

appearing in the representations

$$a=\frac{h_F}{n_1}\times\frac{\tilde{\Pi}e(\mathfrak{p})}{n_2\cdot[\varepsilon:\eta]}=[\eta:NE_K]\cdot\frac{\Pi e(\mathfrak{p})}{[H^1(G, E_K)]}\cdot h_0\times\frac{h_F}{h_0} \text{ of a,}$$

are all integers. Moreover $\frac{\tilde{\Pi}e(\mathfrak{p})}{n_2\cdot[\varepsilon:\eta]}$, $[\eta:NE_K]$, $\frac{\Pi e(\mathfrak{p})}{[H^1(G, E_K)]}\cdot h_0$ are composed of the prime factors of n. Hence we have $\frac{\tilde{\Pi}e(\mathfrak{p})}{n_2\cdot[\varepsilon:\eta]}=[\eta:NE_K]=\frac{\Pi e(\mathfrak{p})}{[H^1(G, E_K)]}\cdot h_0=1$ and $[H^1(G, E_K)]=\Pi e(\mathfrak{p})\cdot h_0$, $[H^0(G, E_K)]=[\varepsilon:\eta]=\tilde{\Pi}e(\mathfrak{p})/n_2$. Furthermore we have $a=h_F/h_0=h_F/n_1$. Therefore we obtain $h_0=n_1$ and hence $[H^0(G, E_K)]=\tilde{\Pi}e(\mathfrak{p})/n_2=\tilde{\Pi}e(\mathfrak{p})\cdot h_0/n$.

§ 5. Main theorems

THEOREM 1. *Let* K/F *be a finite extension over a 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) *if* K/F *is Galois, then* h_K *is divisible by* h_F, *i.e.* h_F/h_K,

(ii) *if* K/F *is abelian, then the relative genus number* g^* *with respect to* K/F *is divisible by* h_F, *i.e.* h_F/g^*,

(iii) *if* K/F *is cyclic, then* a *is divisible by* h_F, *i.e.* h_F/a,

(iv) *if* K/F *is cyclic and has one and only one ramified prime divisor, then* h_F *is equal to* a *and* $[\varepsilon:\eta]=1$.

Proof. (i) This assertion is already known[16], but for the sake of completeness, we add a simple proof.

Since $\tilde{F}K/K$ is unramified and its Galois group $G(\tilde{F}K/K)$ is isomorphic to the Galois group $G(\tilde{F}/F)$, $\tilde{F}K$ is contained in the absolute class field $\tilde{K}$ of K and the relative degree $[\tilde{F}K : K]$ is equal to the relative degree $[\tilde{F} : F] = h_F$. Hence h_K is divisible by h_F.

(ii) Since $\tilde{F}K/K$ is unramified and $\tilde{F}K/F$ is abelian, $\tilde{F}K$ is contained in the relative genus field K^* with respect to K/F. Therefore the relative genus number g^* with respect to K/F is divisible by $[\tilde{F}K : K] = [\tilde{F} : F] = h_F$.

(iii) Since by proposition 1 the number a of ambiguous ideal classes with respect to K/F is equal to the relative genus number g^* with respect to K/F, our assertion (iii) is obvious by (ii).

(iv) By the above proved (ii) and lemma 4, $a/h_F = \tilde{\Pi}e(\mathfrak{p})/[K : F][\varepsilon : \eta]$ is a rational integer. On the other hand, from the assumption that K/F has one and only one ramified prime divisor and $\tilde{F} \cap K = F$, we have at once $\tilde{\Pi}e(\mathfrak{p}) = [K : F]$. Hence we obtain $[\varepsilon : \eta] = 1$ and $a/h_F = 1$.

Theorem 2. *Let K/F be a cyclic extension of a finite degree n. If we assume $a = h_F$, then we have*

(i) $\tilde{\Pi}e(\mathfrak{p}) = n \cdot [\varepsilon : \eta]$,

(ii) $[H^1(G, E_K)] = \Pi e(\mathfrak{p}) \cdot [\eta : NE_K]$,

(iii) *h_K is divisible by h_F, h_F is divisible by h_0 and h_0 is divisible by $[\eta : NE_K]$, i.e. $[\eta : NE_K]/h_0/h_F/h_K$.*

Furthermore, if we assume that K/F is cyclic with a prime power degree l^ν, then h_F is not prime to l provided that h_K is not prime to l.

Proof. (i) This assertion follows trivially from lemma 5 and assumption $a = h_F$.

(ii) By lemma 3 and (i) we have easily

$$[H^1(G, E_K)] = \frac{n \cdot [H^0(G, E_K)]}{\Pi e(\mathfrak{p}_\infty)} = \frac{n \cdot [\varepsilon : \eta][\eta : NE_K]}{\Pi e(\mathfrak{p}_\infty)} = \frac{\tilde{\Pi}e(\mathfrak{p})[\eta : NE_K]}{\Pi e(\mathfrak{p}_\infty)}$$
$$= \Pi e(\mathfrak{p})[\eta : NE_K].$$

(iii) Since $h_K = a \times b_1$ is divisible by $a = h_F$, we know first h_F/h_K. Next, h_0/h_F is evident from lemma 2. Finally, from lemma 6 and theorem 2, (ii),

16) Cf. e.g. C. Chevalley [4], K. Iwasawa [12] or N. C. Ankeny-S. Chowla-H. Hasse [1].

it follows that $[(A)(\mathfrak{a}_0) : (A)(\mathfrak{a}_F)] = \Pi e(\mathfrak{p}) \cdot h_0/[H^1(G, E_K)] = h_0/[\eta : NE_K]$ is integer, and so $[\eta : NE_K]/h_0$.

Moreover, we assume that K/F is cyclic with a prime power degree l^ν. If h_F is prime to l, then by the assumption $a = h_F$, a is prime to l. Hence we have $b_1 \equiv 1$ mod. l by proposition 5.

Since $h_K = a \times b_1$, we know that h_K is prime to l provided h_F is prime to l.

It is evident that those theorems 1, 2 are a generalization of the theorem of K. Iwasawa.

Next, we give a corollary of this theorem 2 which is a generalization of the result of S.-N. Kuroda[17] for a cyclic extension of prime degree.

Corollary. *Let K/F be a cyclic extension of finite degree n and denote by σ a generator of the Galois group $G = G(K/F)$. If we assume that $a = h_F$ and h_F is prime to n, then we have*

(i) $a = a_0 = h_F$, $a_1 = h_0 = n_1 = 1$,

(ii) $\mathbf{C}_K = \mathbf{A} + \mathbf{C}_K^{1-\sigma} = \mathbf{A}_F + {}_N\mathbf{C}_K$ *(direct)*,

(iii) $[\eta : NE_K] = 1$, $[H^0(G, E_K)] = [\varepsilon : \eta] = \tilde{\Pi} e(\mathfrak{p})/n$, $[H^1(G, E_K)] = \Pi e(\mathfrak{p})$, $H^r(G, \mathbf{C}_K) = \{1\}$ *for every integer r.*

Moreover, if we assume that K/F is cyclic with a prime power degree l^ν, then we have

(iv) h_K *is prime to l,*

(v) $b_1 = h_K/h_F \equiv 1$ *mod. l.*

Proof. This corollary is evident by theorem 2 and proposition 4, 5.

Appendix. Unramified cyclic extension.

In this appendix we shall consider an unramified cyclic extension K/F over an algebraic number field F of finite degree. Namely, we prove the following proposition:

Proposition. *Let K/F be an unramified cyclic extension, then we have*

(i) $[\varepsilon : \eta] = 1$, *i.e.* $[H^0(G, E_K)] = [\eta : NE_K]$,

(ii) $a = h_F/[K : F]$,[18] *i.e.* $\tilde{F} = K^*$,

(iii) $h_0 = [H^1(G, E_K)] = [K : F][\eta : NE_K]$,

---

[17] Cf. S.-N. Kuroda [16].

[18] For the cyclic extension of prime degree, this relation is already found in M. Moriya [18], T. Honda [11] etc.

where $G=G(K/F)$ is the Galois group of K/F, and K^* is the relative genus field with respect to K/F.

Remark. Assertion (iii) says that the number h_0 of ideal classes of F which become principal in K is a multiple of the degree $[K:F]$, and that the principal ideal theorem of Terada-Tannaka[19] claiming that all the ambiguous ideal classes with respect to K/F become principal in the absolute class field $\tilde{F}$ of F is truely a generalization of the original principal ideal theorem of Hilbert-Furtwängler[20] when $[H^0(G, E_K)]=[\eta : NE_K]\neq 1$. For, by assertion (iii), $[\eta : NE_K]=1$ holds if and only if $h_0=[K:F]$, and moreover by the assertion (ii) the condition $h_0=[K:F]$ is equivalent to $a=h_F/h_0$. On the other hand, the relation $a=h_F/h_0$ is equivalent to $[\mathbf{A} : (A)(\mathfrak{a}_F)]=1$ by lemma 6, namely the group of ambiguous ideal classes $\mathbf{A}$ with respect to K/F is exactly the group of ideal classes of K represented by ideals of F.

Proof. (i) Since K/F is an unramified cyclic extension, $[\varepsilon : \eta]=1$ is evident from lemma 5.

(ii) From (i) and lemma 4 we obtain at once $a=h_F/[K:F]$. Hence we have easily $\tilde{F}=K^*$ by proposition 1.

(iii) Since K/F is unramified, we have $a_0=h_F/[H^1(G, E_K)]$ by lemma 1 and $a_0=[(A)(\mathfrak{a}_F) : (A)]$ from the definition of a_0, respectively. On the other hand, we have $[(A)(\mathfrak{a}_F) : (A)]=h_F/h_0$ by lemma 6. Hence we obtain $h_0=[H^1(G, E_K)]$ for any unramified extension K/F. In particular, if K/F is cyclic and unramified, then we obtain moreover $[H^1(G, E_K)]=[K:F][\eta : NE_K]$ by lemma 3 and assertion (i).

References

[1] N. C. Ankeny-S. Chowla-H. Hasse, On the class-number of the maximal real subfield of a cyclotomic field, J. reine angew. Math., **217** (1965), 217-220.

[2] E. Artin, Über Einheiten relativ Galoischer Zahlkörper, J. reine angew. Math., **167** (1931), 153-156.

[3] A. Brumer-M. Rosen, Class number and ramification in number fields, Nagoya Math. J., **23** (1963), 97-101.

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

---

[19] Cf. F. Terada [20] and T. Tannaka [19].

[20] Cf. Ph. Furtwängler [8] etc.

[5] C. Chevalley, Class field theory, (Th. 10. 3), Notes at Nagoya University 1954.
[6] Ph. Furtwängler, Über die Klassenzahlen abelscher Zahlkörper, J. reine angew. Math., **134** (1908), 91-94.
[7] Ph. Furtwängler, Über die Klassenzahlen der Kreisteilungskörper, J. reine angew. Math., **140** (1911), 29-32.
[8] Ph. Furtwängler, Beweis des Hauptidealsatzes für die Klassenkörper algebraischer Zahlkörper, Abh. Math. Sem. Hamburg, **7** (1930), 14-36.
[9] H. Hasse, Zur Geschlechtertheorie in quadratischen Zahlkörper, J. Math. Soc. Japan., **3** (1951), 45-51.
[10] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper II, (1930), Jahresberichte der D.M.V.
[11] T. Honda, On absolute class fields of certain algebraic number field, J. reine angew. Math., **203** (1960), 80-89.
[12] K. Iwasawa, A note on class numbers of algebraic number fields, Abh. Math. Sem. Hamburg, **20** (1956), 257-258.
[13] K. Iwasawa, A note on the group of units of algebraic number field, J. math. pure appl., **35** (1956), 189-192.
[14] K. Iwasawa, A class number formula for cyclotomic fields, Ann. of Math., **76** (1962), 171-179.
[15] S. Iyanaga-T. Tamagawa, Sur la théorie du corps de classes sur le corps de nombres rationelles, J. Math. Soc. Japan, **3** (1951), 220-227.
[16] S.-N. Kuroda, Über die Klassenzahl eines relativzyklischen Zahlkörpers von Primzahlgrade, Proc. Japan Acad., **40** (1964), 623-626.
[17] H. W. Leopoldt, Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr., **9** (1953), 351-362.
[18] M. Moriya, Über die Klassenzahl eines relativzyklischen Zahlkörpern von Primzahlgrad, Japanese J. Math., **10** (1933), 1-18.
[19] T. Tannaka, Some remarks concerning principal ideal theorem, Tōhoku Math. J., **1** (1949), 270-278.
[20] F. Terada, On a generalization of the principal ideal theorem, Tōhoku Math. J., **1** (1949), 229-269.
[21] H. Weber, Theorie der algebraischen Zahlkörper, Acta Math., **8** (1886), 193-263.

Mathematical Institute
Nagoya University