ON THE ABSOLUTE IDEAL CLASS GROUPS OF RELATIVELY META-CYCLIC NUMBER FIELDS OF A CERTAIN TYPE

TAIRA HONDA

Notations. The following notations will be used throughout this paper.

ι : the identity of a finite group.

Q : the rational number field.

P : an algebraic number field of finite degree, fixed as the ground field.

l : a prime number.

ζ_l : a primitive l-th root of unity.

For any algebraic number field k and for any cyclic extension k' of k,

$k^{\times}$: the multiplicative group of all the non-zero elements of k'.

h_k : the class number of k.

$\mathfrak{K}_k$: the absolute ideal class group (briefly the class group) of k.

$a_{k'/k}$: the number of ambigous classes of k'/k.

$\mathfrak{K}_{k'/k}$: the subgroup of $\mathfrak{K}_{k'}$ composed of all the ambigous classes of k'/k.

k° : the absolute class field of k.

For any finite multiplicative abelian group $\mathfrak{K}$,

$\mathfrak{K}^{(n)}$: the n-fold direct product of $\mathfrak{K}$.

$\prod_{i=1}^{n}\mathfrak{K}_i$: the direct product of $\mathfrak{K}_1, \ldots, \mathfrak{K}_n$.

$\mathfrak{K} \underset{\mu}{\cong} \mathfrak{K}'$ means that the subgroup of $\mathfrak{K}$ composed of all the elements whose orders are prime to an integer μ is isomorphic to the corresponding subgroup of $\mathfrak{K}'$ (briefly, $\mathfrak{K}$ is *μ-isomorphic to* $\mathfrak{K}'$).

Introduction

Let $\mathfrak{G}$ be a finite group which contains a subgroup $\mathfrak{H}$ with the following property: $\mathfrak{H} \cap \rho\mathfrak{H}\rho^{-1}$ is reduced to $\{\iota\}$ for any element ρ of $\mathfrak{G}$ which does not belong to $\mathfrak{H}$. Then, by a theorem of Frobenius, the elements of $\mathfrak{G}$ which do

Received June 22, 1960.

not belong to any conjugate of $\mathfrak{H}$ constitute together with the identity a normal subgroup $\mathfrak{N}$ of $\mathfrak{H}$. In the case where $\mathfrak{N}$, $\mathfrak{H}$ are both cyclic, let us call such a group $\mathfrak{G}$ *meta-cyclic of type F*, and write $\mathfrak{S}$, $\mathfrak{T}$ instead of $\mathfrak{N}$, $\mathfrak{H}$ respectively.

In the present paper we shall first investigate the structure of the (absolute ideal) class group $\mathfrak{K}_L$ of a normal extension L of P with a meta-cyclic Galois group $\mathfrak{G}$ of type F. (Such an extension L/P will be called also *meta-cyclic of type F.*) Let K, Ω be the intermediate fields of L/P corresponding to $\mathfrak{S}$, $\mathfrak{T}$ respectively, and put $s=(L:K)=$ order of $\mathfrak{S}$ and $t=(L:\Omega)=$ order of $\mathfrak{T}$. Then our result is as follows: if $a_{L/K}=1$, we have $\mathfrak{K}_L \cong \mathfrak{K}_{L/\Omega}^{(t)}$. Here $\mathfrak{K}_{L/\Omega}$ is isomorphic to a subgroup $\mathfrak{K}'_\Omega$ of $\mathfrak{K}_\Omega$ and the factor group $\mathfrak{K}_\Omega/\mathfrak{K}'_\Omega$ is a cyclic group of order $(K \cap \mathrm{P}^\circ : \mathrm{P})$. In the case where $a_{L/K} \neq 1$, the analogous assertion holds by replacing "isomorphic" by "sh_k-isomorphic". This result is a generalization of the main theorem of author's previous paper [4], and its proof is given by a slight modification of the previous one.

In §**1** we shall study some properties of a meta-cyclic group of type F and of abelian groups which have such a group as operator domain. In §**2** we shall give a proof of the fact mentioned above by the method in [4].

Now, let $L_1, \ldots, L_m$ be meta-cyclic fields of type F over P with a common maximally abelian intermediate field K, and M be their composite. If $(L_i:K)=l$ for $1 \leqq i \leqq m$, we can combine our result with Nehrkorn's result on the class groups of abelian fields of prime exponent to study the structure of $\mathfrak{K}_M$. In particular this can be applied to a Kummer's field $M=\mathrm{P}(\zeta_l, \sqrt[l]{\alpha_1}, \ldots, \sqrt[l]{\alpha_m})$ where $\alpha_1, \ldots, \alpha_m$ are arbitrary elements of $\mathrm{P}^\times$, and, as will be shown in §**3**, we can reduce the study of $\mathfrak{K}_M$ to the study of the class groups of fields of type $\mathrm{P}(\sqrt[l]{\alpha})$ $(\alpha \in \mathrm{P}^\times)$ in the sense of lh_K-isomorphism, where $K=\mathrm{P}(\zeta_l)$. In particular, we shall show that, if the class number of the cyclotomic field $Q(\zeta_l)$ is equal to 1, there exist an infinite number of Kummer's fields (in Kummer's original sense) whose class groups are $(l-1)$-fold direct products of some abelian groups.

§1. Meta-cyclic groups of type F

Let $\mathfrak{G}$ be a meta-cyclic group of type F and $\mathfrak{S}$, $\mathfrak{T}$ be the subgroups with the same meaning as in the introduction. Denote by s, t their orders and by σ, τ their generators respectively. Put

$$\tau^{-1}\sigma\tau=\sigma^a, \qquad 1 \leqq a \leqq s-1.$$

Then the structure of $\mathfrak{G}$ is perfectly determined by s, t, and a. Let us call (s, t, a) an *invariant* of $\mathfrak{G}$. (Note that, for given $\mathfrak{G}$, a is not always determined uniquely. It may change by taking another generator of $\mathfrak{T}$).

As for the structure of $\mathfrak{G}$, we have

LEMMA 1. *Let $\mathfrak{G}$ be a meta-cyclic group of type F with an invariant (s, t, a) and with subgroups $\mathfrak{S}$, $\mathfrak{T}$ as above. Then $\mathfrak{T}$ is a complete system of representatives of $\mathfrak{G}/\mathfrak{S}$, the commutator group $D(\mathfrak{G})$ of $\mathfrak{G}$ coincides with $\mathfrak{S}$, and we have*

$$(a^i - 1, s) = 1 \qquad \text{for } 1 \leqq i \leqq t-1.$$

Proof. By the definition of type F, we obtain $\mathfrak{G} = \mathfrak{S}\mathfrak{T}$ and $\mathfrak{S} \cap \mathfrak{T} = \{\iota\}$. Therefore $\mathfrak{G}/\mathfrak{S}$ is isomorphic to $\mathfrak{T}$ and the first assertion is clear. Next, as

$$\sigma^j \tau^i \sigma^{-j} = \tau^i \sigma^{(a^i-1)j} \qquad \text{for } 1 \leqq i \leqq t-1,\ 1 \leqq j \leqq s-1,$$

we obtain by the definition of type F

$$\sigma^{(a^i-1)j} \neq \iota \qquad \text{for } 1 \leqq i \leqq t-1,\ 1 \leqq j \leqq s-1,$$

and so $(a^i - 1, s) = 1$ for $1 \leqq i \leqq t-1$. Finally it is clear that $D(\mathfrak{G}) \subset \mathfrak{S}$. On the other hand, because $\tau^{-1}\sigma\tau\sigma^{-1} = \sigma^{a-1}$ is a generator of $\mathfrak{S}$, $\mathfrak{S}$ is contained in $D(\mathfrak{G})$, hence coincides with $D(\mathfrak{G})$. This completes our proof.

LEMMA 2. *Let (s, t, a) be an invariant of a meta-cyclic group $\mathfrak{G}$ of type F. For any prime divisor p of s, we have*

$$p \equiv 1 \qquad (\text{mod } t).$$

In particular we have

$$(s, t) = 1.$$

Proof. Let $\mathfrak{S}_p$ be the (only) subgroup of $\mathfrak{S}$ of order p. Because $\mathfrak{S}$ is a normal subgroup of $\mathfrak{G}$, any conjugate of $\mathfrak{S}_p$ is contained in $\mathfrak{S}$ and so coincides with $\mathfrak{S}_p$. Thus $\mathfrak{S}_p$ is a normal subgroup of $\mathfrak{G}$. Now we divide $\mathfrak{S}_p$ into conjugate classes. It can easily be seen from Lemma 1 that the centralizer of any element of $\mathfrak{S}_p$ other than ι coincides with $\mathfrak{S}$. Therefore every class of $\mathfrak{S}_p$ other than the class of the identity contains just t elements, from which follows the assertion of the lemma.

We shall now study the structure of a finite multiplicative abelian group $\mathfrak{R}$ which has a meta-cyclic group of type F as operator domain.

The identity of $\mathfrak{R}$ will be denoted by 1. Assume that the identity of $\mathfrak{G}$

operates on $\mathfrak{K}$ as the identity mapping and that for any $\rho_1, \rho_2 \in \mathfrak{G}$ and for $C \in \mathfrak{K}$

$$C^{\rho_1\rho_2} = (C^{\rho_1})^{\rho_2}.$$

For any element C of $\mathfrak{K}$ and for any element ρ of $\mathfrak{G}$ of order m, we denote $C^{1+\rho+\cdots+\rho^{m-1}}$ by $N_\rho C$.

As in [4], we put ${}_\rho\mathfrak{K} = \{C \in \mathfrak{K} \mid N_\rho C = 1\}$ and $\mathfrak{K}_\rho = \{C \in \mathfrak{K} \mid C^{\rho-1} = 1\}$ for any element ρ of $\mathfrak{G}$. Let μ be the product of s and of the order of $\mathfrak{K}_\sigma$, and denote by $\mathfrak{K}_\mu$ the subgroup of $\mathfrak{K}$ of all the elements whose orders contain only prime divisors of μ.

LEMMA 3. *If $C \in \mathfrak{K}$ and $C^{1-\sigma} \in \mathfrak{K}_\mu$, we must have*

$$C \in \mathfrak{K}_\mu.$$

Proof. As

$$N_\sigma C = C^{1+\sigma+\cdots+\sigma^{s-1}} \in \mathfrak{K}_\sigma \subset \mathfrak{K}_\mu$$

we obtain by the assumption

$$C^s \in \mathfrak{K}_\mu$$

and therefore

$$C \in \mathfrak{K}_\mu,$$

which was to be proved.

The following two theorems are generalizations of Theorem 3 and Theorem 4 in [4] respectively.

THEOREM 1. *For any finite abelian group $\mathfrak{K}$ with a meta-cyclic group $\mathfrak{G}$ of type F as operator domain we have*

$$\bigcap_{i=0}^{t-1} {}_{\sigma^{-i}\tau\sigma^i}\mathfrak{K} \underset{\mu}{\cong} \{1\}.$$

Here μ is defined as above. In particular, if $\mathfrak{K}_\sigma = \{1\}$, we have

$$\bigcap_{i=0}^{t-1} {}_{\sigma^{-i}\tau\sigma^i}\mathfrak{K} = \{1\}.$$

In this case $\mathfrak{K}$ need not be finite.

THEOREM 2. *Dually to theorem 1, the product of subgroups $\mathfrak{K}_\tau, \mathfrak{K}_{\sigma^{-1}\tau\sigma}, \ldots, \mathfrak{K}_{\sigma^{-(t-1)}\tau\sigma^{t-1}}$ is μ-isomorphic to their direct product. If $\mathfrak{K}_\sigma = \{1\}$, "$\mu$-isomorphic" can be replaced by "isomorphic" and in this case $\mathfrak{K}$ need not be finite.*

Proof of Theorem 1 and Theorem 2. If $\mathfrak{K}_\sigma = \{1\}$, the proof of Theorem 3 and Theorem 4 in [4] can be word for word applied here by using Lemma 1 in the present paper instead of Lemma 2 in [4]. In the case where $\mathfrak{K}_\sigma \neq \{1\}$, replace $\mathfrak{K}$ by its subgroup $\bar{\mathfrak{K}}$ of all the elements whose orders are prime to μ, then we can apply the above results to this $\bar{\mathfrak{K}}$, because $(\bar{\mathfrak{K}})_\sigma = \{1\}$ by Lemma 3. Thus we obtain the assertions to be proved.

§2. Structure of the absolute ideal class groups of meta-cyclic fields of type *F*

First we shall give a generalization of Theorem 2 in [4].

LEMMA 4. *For any cyclic field k'/k, $a_{k'/k}$ is a multiple of $h_k/(k' \cap k^\circ : k)$.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_u$ be the prime divisors in k ramifying in k', and $e_1, \ldots, e_u$ be their ramification exponents. The number of ambigous classes of k'/k is given by

$$a_{k'/k} = \frac{h_k \prod_{i=1}^{u} e_i}{(k' : k)(\varepsilon : N(\theta))}$$

where ε stands for units in k, and θ for elements in k' whose norms $N(\theta) = N_{k'/k}(\theta)$ are units in k. Our lemma asserts that

$$\frac{\prod_{i=1}^{u} e_i}{(k' : k' \cap k^\circ)(\varepsilon : N(\theta))}$$

is an integer. Now a unit ε in k is the norm of an element in k' if and only if

$$\left(\frac{\varepsilon, k'/k}{\mathfrak{p}_j}\right) = 1 \qquad \text{for } 1 \leqq j \leqq u.$$

Because of the product formula of norm residue symbol we can replace these u equations by arbitrary $u-1$ of them. As the number of distinct values taken by $\left(\frac{\varepsilon, k'/k}{\mathfrak{p}_j}\right)$ when ε runs over all the units in k is a divisor of e_j, $\prod e_i/(\varepsilon : N(\theta))$ is a multiple of each e_j, hence is a common multiple of $e_1, \ldots, e_u$. On the other hand, the Galois group of $k'/(k' \cap k^\circ)$ is generated by the inertia groups of $\mathfrak{p}_1, \ldots, \mathfrak{p}_u$. As k'/k is cyclic, its order is the least common multiple of $e_1, \ldots, e_u$. Thus $\prod_{i=1}^{u} e_i$ is divisible by $(k' : k' \cap k^\circ)$ $(\varepsilon : N(\theta))$. This completes our proof.

Now let L/P be a meta-cyclic field of type F with the Galois group $\mathfrak{G}$, and K, Ω be the intermediate fields corresponding to $\mathfrak{S}$, $\mathfrak{T}$ respectively. Because of

Lemma 1 K is characterized as the maximally abelian intermediate field of L/P.

LEMMA 5. *The Galois group of* $L \cap \Omega^\circ/\Omega$ *is canonically isomorphic to that of* $K \cap \mathrm{P}^\circ/\mathrm{P}$. *In particular we have*

$$(L \cap \Omega^\circ : \Omega) = (K \cap \mathrm{P}^\circ : \mathrm{P}).$$

Proof. Because $(K \cap \mathrm{P}^\circ)\Omega$ is an unramified extension of Ω contained in L, it is a subfield of $L \cap \Omega^\circ$. Moreover, as $K \cap \Omega = \mathrm{P}$, the Galois group of $(K \cap \mathrm{P}^\circ)\Omega/\Omega$ is canonically isomorphic to that of $K \cap \mathrm{P}^\circ/\mathrm{P}$. Hence we have only to prove

$$(K \cap \mathrm{P}^\circ : \mathrm{P}) \geqq (L \cap \Omega^\circ : \Omega),$$

for it implies $(K \cap \mathrm{P}^\circ)\Omega = L \cap \Omega^\circ$. Let $\mathfrak{T}_0$ be the subgroup of $\mathfrak{T}$ corresponding to $L \cap \Omega^\circ$. If $\tau_1 \in \mathfrak{T} - \mathfrak{T}_0$, all the conjugates of τ_1 do not belong to the inertia group of any prime divisor in L with respect to P. Therefore the inertia group of an arbitrary prime divisor in L with respect to P is contained in $\mathfrak{S}\mathfrak{T}_0$, and the intermediate field of K/P corresponding to $\mathfrak{S}\mathfrak{T}_0$ is unramified over P. As this field is contained in $K \cap \mathrm{P}^\circ$ and the order of $\mathfrak{S}\mathfrak{T}_0$ is equal to $s(L : L \cap \Omega^\circ)$, we obtain in fact

$$(K \cap \mathrm{P}^\circ : \mathrm{P}) \geqq \frac{st}{s(L : L \cap \Omega^\circ)} = (L \cap \Omega^\circ : \Omega).$$

Now put $\Omega_i = \Omega^{\sigma^i}$ and denote by $\overline{\Omega_i^\circ}$ and $\overline{L^\circ}$ respectively the maximum intermediate fields of Ω_i°/Ω_i and of L°/L such that the degrees $(\overline{\Omega_i^\circ} : \Omega_i)$ and $(\overline{L^\circ} : L)$ are prime to sh_K. With these notations we can state our main result as follows:

THEOREM 3. 1. *The fields* $L\Omega^\circ$, $L\overline{\Omega_1^\circ}$, $\ldots$, $L\overline{\Omega_{t-1}^\circ}$ *are independent over* L, *and their composite coincides with* $\overline{L^\circ}$.

2. $$\mathfrak{K}_L \underset{sh_K}{\cong} \prod_{i=0}^{t-1} \mathfrak{K}_{L/\Omega_i} \cong \mathfrak{K}_{L/\Omega}^{(t)}.$$

Here $\mathfrak{K}_{L/\Omega_i}$ *is* sh_K*-isomorphic to a subgroup* $\mathfrak{K}'_\Omega$ *of* $\mathfrak{K}_\Omega$ *such that* $\mathfrak{K}_\Omega/\mathfrak{K}'_\Omega$ *is cyclic and of order* $(K \cap \mathrm{P}^\circ : \mathrm{P})$.

3. *The rational number* $h_L \left\{ \dfrac{h_\Omega}{(K \cap \mathrm{P}^\circ : \mathrm{P})} \right\}^{-t}$ *contains only prime divisors of* sh_K.

In the case where $a_{L/K} = 1$, *we can replace* $\overline{\Omega_i^\circ}$ *by* Ω_i° *and* $\overline{L^\circ}$ *by* L° *in* 1, *and* sh_K *by* 1 *in* 2 *and* 3.

We can perform the proof of this theorem quite in the same manner as in the proof of the main theorem in [4] by using Theorem 1 and Theorem 2 in this paper instead of Theorem 3 and Theorem 4 in [4], and Lemma 4 in this paper instead of Theorem 2 in [4]. Thereby we have only to notice that a prime divisor of $a_{L/K}$ divides sh_K, and that $(L \cap \Omega^\circ : \Omega) = (K \cap \mathrm{P}^\circ : \mathrm{P})$ by Lemma 5.

It is easy to see that absolute class fields such as were treated in [4] are meta-cyclic fields of type F. Conversely, if L/P is a meta-cyclic field of type F with the maximally abelian intermediate field K and L is the absolute class field of K, we must have $a_{K/\mathrm{P}} = 1$. For, as is seen from the proof of Lemma 1, the centralizer of τ coincides with $\mathfrak{T}$. If we regard $\mathfrak{T}$ as the Galois group of K/P, this implies because of Artin's reciprocity law that no absolute class other than the principal class in $\mathfrak{K}$ is invariant by τ.

There are another kind of meta-cyclic fields of type F obtained in a natural way, that is, fields generated by meta-cyclic equations of prime degree. The case of binomial equations of prime degree will be treated in the next section.

§ 3. Application to Kummer's fields with a prime exponent

Theorem 3 in § **2** can be applied to the splitting field L of a binomial equation

$$x^l - \alpha = 0, \qquad \alpha \in \mathrm{P}^\times$$

with respect to P. The extension L/P is in fact meta-cyclic of type F, since L is generated by arbitrary two of the roots of this binomial equation. The maximally abelian intermediate field of L/P is $K = \mathrm{P}(\zeta_l)$. Hence we can reduce the study of the class group of the field L to the study of that of the field $\mathrm{P}(\sqrt[l]{\alpha})$ in the sense of lh_K-isomorphism. (Note that lh_K depends only on l and the ground field P, and not on α.) In particular we have

THEOREM 4. *Assume that the class number of the cyclotomic field $Q(\zeta_l)$ is equal to* 1. *Then, if a prime number q has the order $l-1$ in the reduced residue class group mod l^2, the class group of the field $Q(\zeta_l, \sqrt[l]{q})$ is isomorphic to the $(l-1)$-fold direct product of that of the field $Q(\sqrt[l]{q})$.*

Proof. Put $K = Q(\zeta_l)$ and $L = Q(\zeta_l, \sqrt[l]{q})$. As $K \cap Q^\circ = Q$, it suffices to prove that one and only one prime divisor in K ramifies in L. Then we shall obtain $a_{L/K} = 1$ (cf. § 3, [4]). Since q is a primitive root mod l, the prime ideal (q) in Q remains prime in K. Moreover the prime divisor $\mathfrak{l}$ of (l) in K does not ramify in L. For q is l-primary for $\mathfrak{l}$ by the criterion XI in Hasse [1], § 9, considering that q is an l-th power residue mod l^2, hence *a fortiori* mod $\mathfrak{l}^{(l-1)+1}$. Thus the prime divisor ramifying in L/K is only (q). This completes our proof.

Now let K be anew an algebraic number field of finite degree, and $L_1, \ldots,$ L_m be independent cyclic extensions of degree l over K. Put $M = L_1 \cdots L_m$ and denote by $L_1, \ldots, L_m, L_{m+1}, \ldots, L_n$ n intermediate fields of degree l of M/K, where $n = (l^m - 1)/(l-1)$.

Then, by a theorem in Nehrkorn [2], we have

$$\mathfrak{K}_M \underset{lh_K}{\cong} \prod_{i=1}^{n} \mathfrak{K}_{L_i}.$$

(In truth we have a somewhat stronger assertion. We can regard $\mathfrak{K}_K$ as a subgroup of $\mathfrak{K}_M$ and of $\mathfrak{K}_{L_i}$ in the sense of l-isomorphism. In this sense we have

$$\mathfrak{K}_M / \mathfrak{K}_K \underset{l}{\cong} \prod_{i=1}^{n} \mathfrak{K}_{L_i} / \mathfrak{K}_K.$$

For the proof of this result, see Kuroda [3].) In the case where K is a cyclic extension of P, and each L_i is a meta-cyclic extension of P of type F with the maximally abelian intermediate field K, we can further reduce the class groups $\mathfrak{K}_{L_i}$ by Theorem 3 in the sense of lh_K-isomorphism. In particular we can apply this reduction to the class group of a Kummer's field $\mathrm{P}(\zeta_l, \sqrt[l]{\alpha_1}, \ldots, \sqrt[l]{\alpha_m})$ with the exponent l, where $\alpha_1, \ldots, \alpha_m \in \mathrm{P}^{\times}$. In this way we have

THEOREM 5. *Let $\alpha_1, \ldots, \alpha_m$ be elements of $\mathrm{P}^{\times}$ multiplicatively independent modulo $\mathrm{P}^{\times l}$, and denote by $\Omega_1, \ldots, \Omega_n$ all the distinct fields $(\neq \mathrm{P})$ of form $\mathrm{P}(\sqrt[l]{\alpha_1^{x_1} \cdots \alpha_m^{x_m}})$ where $n = (l^m - 1)/(l-1)$ and $x_1, \ldots, x_m$ be integers. Moreover, put $K = \mathrm{P}(\zeta_l)$ and $d = (K : \mathrm{P})$. Then, for the class group of the Kummer's field $M = \mathrm{P}(\zeta_l, \sqrt[l]{\alpha_1}, \ldots, \sqrt[l]{\alpha_m})$, we have*

$$\mathfrak{K}_M \underset{lh_K}{\cong} \prod_{i=1}^{n} \mathfrak{K}_{\Omega_i}^{(d)}.$$

Here lh_K depends only on l and the ground field P, *and not on $\alpha_1, \ldots, \alpha_m$.*

References

[1] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, II (1930), Jahresberichte der D.M.V.

[2] H. Nehrkorn, Über absolute Idealklassengruppe und Einheiten in algebraischen Zahlkörpern, Abh. Math. Sem. Univ. Hamburg **9** (1933), pp. 318–334.

[3] S. Kuroda, Über die Klassenzahl algebraischer Zahlkörper, Nagoya Math. J. **1** (1950), pp. 1–10.
[4] T. Honda, On absolute class fields of certain algebraic number fields, Jour. f. Math. **203** (1960), pp. 80–89.

Department of Mathematics
University of Tokyo