S. Shirai
Nagoya Math. J.
Vol. 75 (1979), 121-131

ON GALOIS GROUPS OF CLASS TWO EXTENSIONS OVER THE RATIONAL NUMBER FIELD

SUSUMU SHIRAI

Introduction

Let $\boldsymbol{Q}$ be the rational number field, $K/\boldsymbol{Q}$ be a maximal[1] Abelian extension whose degree is some power of a prime ℓ, and let $f(K)$ be the conductor of $K/\boldsymbol{Q}$; if $\ell=2$, let K be complex, and if in addition $f(K)\equiv 0 \pmod 2$, let $f(K)\equiv 0 \pmod{16}$. Denote by $\mathfrak{F}(K)$ the Geschlechtermodul of K over $\boldsymbol{Q}$ and by $\hat{K}$ the maximal central ℓ-extension of $K/\boldsymbol{Q}$ contained in the ray class field mod $\mathfrak{F}(K)$ of K. A. Fröhlich [1, Theorem 4] completely determined the Galois group of $\hat{K}$ over $\boldsymbol{Q}$ in purely rational terms. The proof is based on [1, Theorem 3], though he did not write the proof in the case $f(K)\equiv 0 \pmod{16}$. Moreover he gave a classification theory of all class two extensions over $\boldsymbol{Q}$ whose degree is a power of ℓ. Hence we know the set of fields of nilpotency class two over $\boldsymbol{Q}$, because a finite nilpotent group is a direct product of all its Sylow subgroups. But the theory becomes cumbersome, and it is desirable to reconstruct a more elementary one.

In the present paper we take the m-th cyclotomic field K_m as K and the central class field $\hat{K}_{mp_\infty}$[2] mod mp_∞ of $K_m/\boldsymbol{Q}$ as $\hat{K}$, where p_∞ stands for the real prime divisor of $\boldsymbol{Q}$. Then we determine the Galois group of $\hat{K}_{mp_\infty}$ over $\boldsymbol{Q}$ by refining the methods used in [1] when $(m, 16)\neq 8$ (Theorem 6). The proof is based on [5, Theorem 32] which is a generalization of [1, Theorem 3] to a cyclotomic field over $\boldsymbol{Q}$. We have already shown in [5] that if $L/\boldsymbol{Q}$ is a normal extension whose Galois group is of nilpotency class two, then there exists a positive integer m such that $L\subset\hat{K}_{mp_\infty}$. Thus as regards Galois groups, we possess the set of all nilpotency class

Received July 19, 1978.

1) This is of sense of Fröhlich [1], which implies that the union of all Abelian ℓ-extensions defined mod $f(K)$ over $\boldsymbol{Q}$ is K itself, in other words, the ℓ-genus field of $K/\boldsymbol{Q}$ contained in the ray class field mod $\mathfrak{F}(K)$ of K coincides with K.

2) See [5, §3].

two extensions over $\boldsymbol{Q}$ as well as the set of cyclotomic fields over $\boldsymbol{Q}$. It seems that in this approach to the theory of fields of class two over $\boldsymbol{Q}$ the structural relation between the fields becomes more transparent in comparison with the case of Fröhlich [1].

Notation

Throughout this paper the following notation will be used.

$\boldsymbol{Z}$ the ring of rational integers on which a finite group acts trivially.

$\boldsymbol{Q}$ the field of rational numbers as in Introduction.

$U_K^{(i)}$ the i-th unit group of K with $i \geqq 0$ when K is a local field.

$G(K/k)$ the Galois group of K over k.

$N_{K/k}$ the Norm of K to k.

(a, b) the commutator $aba^{-1}b^{-1}$ of a and b when a, b are elements in a group.

(A, B) the subgroup generated by the commutators (a, b) of all $a \in A$, $b \in B$ when A, B are subsets in a group.

$\langle A \rangle$ the subgroup generated by A when A is a subset in a group.

$\psi(n)$ the Euler's function, that is, the number of positive integers $\leqq n$ which are relatively prime to n.

Moreover we will use the results and notation of the preceding paper [5].

§ 1. The Schur multiplicator of a finite group

In this section we describe a well-known result of I. Schur for later use.

Let G be a finite group, and let

$$1 \to R \to F \to G \to 1$$

be a free presentation of G in which F is free. Denote by F' the derived group of F. Then the sequence in which all groups are Abelian

$$0 \to R \cap F'/(R, F) \to R/(R, F) \to R/R \cap F' \to 0$$

is exact. Since $R/R \cap F'$ is isomorphic to a subgroup RF'/F' of the free Abelian group F/F', the above sequence splits, and hence there exists a complement $S/(R, F)$ to $R \cap F'/(R, F)$ in $R/(R, F)$. Of course this S is not uniquely determined.

LEMMA 1[3]. *Notation being as above, we have*

3) See for instance B. Huppert [2, §23]. This follows also from MacLane's theorem [4, §§50, 52].

$$H^{-3}(G, Z) \simeq R/S .$$

We note that if $\{z_\lambda \bmod F'\}_{\lambda\in\Lambda}(R \supset \{z_\lambda\}_{\lambda\in\Lambda})$ is a basis for the free Abelian group RF'/F', then we can take

$$S = < \{z_\lambda\}_{\lambda\in\Lambda}, (R, F) > . \tag{1}$$

§ 2. Relations of local Galois groups

Let p be a rational prime, $\boldsymbol{Q}_p$ be the p-adic number field, $T/\boldsymbol{Q}_p$ be a finite unramified extension, ζ be a primitive p^ν-th root of unity, and let $K = T(\zeta)$. We denote by $\hat{K}$ a central extension of $K/\boldsymbol{Q}_p$ such that the p-exponent $\mu(\hat{K}/\boldsymbol{Q}_p)$ of the Galois conductor[4] of $\hat{K}/\boldsymbol{Q}_p$ does not exceed ν.

We first assume $p \neq 2$. Let g be a primitive root mod p^ν, and let

$$\sigma = (p, K/\boldsymbol{Q}_p)^{-1} , \qquad \tau = (g, K/\boldsymbol{Q}_p) , \tag{2}$$

where $(, K/\boldsymbol{Q}_p)$ denotes the local norm residue symbol for $K/\boldsymbol{Q}_p$. Then σ is the Frobenius automorphism of $K/\boldsymbol{Q}_p(\zeta)$ and τ a generator of the inertia group $G(K/T)$ of $K/\boldsymbol{Q}_p$. It is obvious that $\{\sigma, \tau\}$ is a system of generators of $G(K/\boldsymbol{Q}_p)$.

LEMMA 2. *If $p \neq 2$, then there exists a system of generators $\{\tilde{\sigma}, \tilde{\tau}\}$ of $G(\hat{K}/\boldsymbol{Q}_p)$ such that*

$$\tilde{\tau}^{\psi(p^\nu)}(\tilde{\tau}^{p^{\nu-1}}, \tilde{\sigma}) = 1 ,$$

where $\tilde{\sigma}$, $\tilde{\tau}$ are extensions of σ and τ defined by (2) to $\hat{K}$, respectively.

Proof. There exists $\alpha \in U_T^{(0)}$ such that $N_{T/\boldsymbol{Q}_p}\alpha = g$, because $T/\boldsymbol{Q}_p$ is unramified. Then $\tau = (\alpha, K/T)$. Since K/T is cyclic, $\hat{K}/T$ is Abelian. We take

$$\tilde{\tau} = (\alpha, \hat{K}/T) .$$

As is generally known, the unit group $U_T^{(0)}$ is a direct product of the group of $(p^f - 1)$st roots of unity and $U_T^{(1)}$, here $f = [T: \boldsymbol{Q}_p]$, the extension degree. Thus we may write,

$$\alpha = \xi\varepsilon , \quad \xi^{p^f-1} = 1 , \quad \varepsilon \in U_T^{(1)} ,$$

and hence

$$\tilde{\tau}^{p^{\nu-1}} = (\xi^{p^{\nu-1}}, \hat{K}/T) .$$

4) See [5, §1].

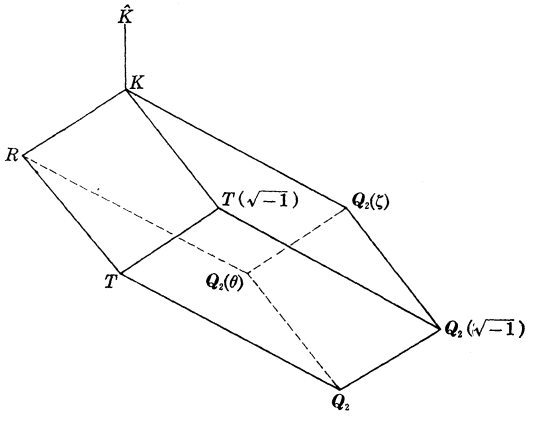
Because it follows from $\mu(\hat{K}/T) = \mu(\hat{K}/\boldsymbol{Q}_p) \leqq \nu$ that

$$N_{\hat{K}/T}\hat{K}^* \supset U_T^{(\nu)} \overset{5)}{\supset} U_T^{(1)p^{\nu-1}} \ni \varepsilon^{p^{\nu-1}},$$

where $\hat{K}^*$ is the multiplicative group of all non-zero elements of $\hat{K}$. Then for any extension $\tilde{\sigma}$ of σ to $\hat{K}$, we have

$$\tilde{\sigma}\tilde{\tau}^{p^{\nu-1}}\tilde{\sigma}^{-1} = ((\xi^{\sigma})^{p^{\nu-1}}, \hat{K}/T) = (\xi^{p^{\nu}}, \hat{K}/T) = \tilde{\tau}^{p^{\nu}}. \qquad \text{Q.E.D.}$$

Next we assume $p = 2$. In this case K/T is not cyclic when $\nu \geqq 3$. Therefore the situation becomes more complicated in comparison with the case of $p \neq 2$, because $\hat{K}/T$ is not necessarily Abelian. The relation between fields to be considered below can be described by the following diagram, in which we put $R = T(\theta)$, $\theta = \zeta + \zeta^{-1}$. Note that extensions $\hat{K}/R$, $\hat{K}/T(\sqrt{-1})$, $\hat{K}/\boldsymbol{Q}_2(\zeta)$ are Abelian, because K/R, $K/T(\sqrt{-1})$, $K/\boldsymbol{Q}_2(\zeta)$ are cyclic and $G(\hat{K}/K)$ is contained in the center of $G(K/\boldsymbol{Q}_2)$.



Now set

$$(3) \qquad \sigma = (2, K/\boldsymbol{Q}_2)^{-1}, \quad \tau^* = (-1, K/\boldsymbol{Q}_2), \quad \tau = (5, K/\boldsymbol{Q}_2).$$

Then σ is the Frobenius automorphism of $K/\boldsymbol{Q}_2(\zeta)$. By direct computation of norm residue symbols, we have

$$\zeta^{\tau^*} = \zeta^{-1}, \qquad \zeta^{\tau} = \zeta^5.$$

Thus τ^*, τ are generators of $G(K/R)$ and $G(K/T(\sqrt{-1}))$, respectively. We first investigate a relation to be satisfied by a suitable extension $\tilde{\tau}$ of τ

5) Furthermore we have $U_T^{(\nu)} = U_T^{(1)p^{\nu-1}}$ when $p \neq 2$.

to $\hat{K}$. Since $T(\sqrt{-1})/\boldsymbol{Q}_2(\sqrt{-1})$ is unramified, there exists $\alpha \in U^{(0)}_{T(\sqrt{-1})}$ such that $N_{T(\sqrt{-1})/\boldsymbol{Q}_2(\sqrt{-1})}\alpha = 1 + 2\sqrt{-1}$. Then

$$\tau = (1 + 2\sqrt{-1}, K/\boldsymbol{Q}_2(\sqrt{-1})) = (\alpha, K/T(\sqrt{-1}))\,,$$

because of $N_{\boldsymbol{Q}_2(\sqrt{-1})/\boldsymbol{Q}_2}(1 + 2\sqrt{-1}) = 5$. We take

$$\tilde{\tau} = (\alpha, \hat{K}/T(\sqrt{-1}))\,. \tag{4}$$

LEMMA 3. $$\tilde{\tau}^{2^{\nu-2}} = 1\,.$$

Proof. The Hasse's function for $\boldsymbol{Q}_2(\zeta)/\boldsymbol{Q}_2$ is given by

$$\varphi_{\boldsymbol{Q}_2(\zeta)/\boldsymbol{Q}_2}(i-1) = 2^{\nu-1}(i - \nu + 1) - 1 \qquad \text{for } i \geqq \nu\,.$$

It follows from [5, Lemma 4] that

$$\mu(\hat{K}/\boldsymbol{Q}_2(\zeta)) \leqq \varphi_{\boldsymbol{Q}_2(\zeta)/\boldsymbol{Q}_2}(\nu - 1) + 1 = 2^{\nu-1}\,,$$

and hence

$$N_{\hat{K}/\boldsymbol{Q}_2(\zeta)}\hat{K}^* \supset U^{(2^{\nu-1})}_{\boldsymbol{Q}_2(\zeta)}\,.$$

Thus we have

$$\begin{aligned}\tilde{\tau}^{2^{\nu-2}} &= (\alpha^{2^{\nu-2}}, \hat{K}/T(\sqrt{-1})) = (N_{K/T(\sqrt{-1})}\alpha, \hat{K}/T(\sqrt{-1}))\\ &= (\alpha, \hat{K}/K) = (N_{K/\boldsymbol{Q}_2(\zeta)}\alpha, \hat{K}/\boldsymbol{Q}_2(\zeta))\\ &= (1 + 2\sqrt{-1}, \hat{K}/\boldsymbol{Q}_2(\zeta)) = 1\,,\end{aligned}$$

because of $1 + 2\sqrt{-1} \in U^{(2^{\nu-1})}_{\boldsymbol{Q}_2(\zeta)}$. Q.E.D.

We next study a relation to be satisfied by suitable extensions $\tilde{\sigma}$, $\tilde{\tau}^*$, $\tilde{\tau}$ of σ, τ^*, τ to $\hat{K}$, here $\tilde{\tau}$ is the extension defined by (4) to $\hat{K}$. There exists $\beta \in U^{(0)}_R$ such that $N_{R/\boldsymbol{Q}_2(\theta)}\beta = \theta^2 + \theta - 1$. It can be easily checked that

$$N_{\boldsymbol{Q}_2(\theta)/\boldsymbol{Q}_2}(\theta^2 + \theta - 1) = -1 \qquad \text{for } \nu \geqq 2\,.$$

Hence

$$\tau^* = (\theta^2 + \theta - 1, K/\boldsymbol{Q}_2(\theta)) = (\beta, K/R)\,.$$

We take

$$\tilde{\tau}^* = (\beta, \hat{K}/R)\,.$$

Then

$$\begin{aligned}\tilde{\tau}^{*2} &= (\beta^2, \hat{K}/R) = (N_{K/R}\beta, \hat{K}/R) = (\beta, \hat{K}/K)\\ &= (N_{K/\boldsymbol{Q}_2(\zeta)}\beta, \hat{K}/\boldsymbol{Q}_2(\zeta)) = (\theta^2 + \theta - 1, \hat{K}/\boldsymbol{Q}_2(\zeta))\,.\end{aligned}$$

Since $N_{Q_2(\zeta)/Q_2}(1-\zeta)=2$, we have

$$\sigma=(1-\zeta, K/Q_2(\zeta))^{-1}\ .$$

We take

$$\tilde{\sigma}=(1-\zeta, \hat{K}/Q_2(\zeta))^{-1}\ .$$

Then

$$\begin{aligned}(\tilde{\tau}^*, \tilde{\sigma}) &= \tilde{\tau}^*\tilde{\sigma}\tilde{\tau}^{*-1}\tilde{\sigma}^{-1}=(1-\zeta/1-\zeta^{\tau^*}, \hat{K}/Q_2(\zeta))\\ &=(1-\zeta/1-\zeta^{-1}, \hat{K}/Q_2(\zeta))=(-\zeta, \hat{K}/Q_2(\zeta))\ ,\end{aligned}$$

and hence

$$(\zeta, \hat{K}/Q_2(\zeta))^2=(\tilde{\tau}^*, \tilde{\sigma})^2=(\tilde{\tau}^{*2}, \tilde{\sigma})=1\ ,$$

because $G(\hat{K}/Q_2)$ is a finite nilpotent group of class two and $\tilde{\tau}^{*2}\in G(\hat{K}/K)\subset Z(G(\hat{K}/Q_2))$, the center of $G(\hat{K}/Q_2)$. Since $1+\zeta+\zeta^2+\zeta^3+\zeta^4=\zeta^2(\theta^2+\theta-1)$, we have

$$\begin{aligned}(\tilde{\tau}, \tilde{\sigma})^{-1}&=(\tilde{\tau}, \tilde{\sigma}^{-1})=\tilde{\tau}\tilde{\sigma}^{-1}\tilde{\tau}^{-1}\tilde{\sigma}\\ &=(1-\zeta^{\tau}/1-\zeta, \hat{K}/Q_2(\zeta))=(1-\zeta^5/1-\zeta, \hat{K}/Q_2(\zeta))\\ &=(\zeta, \hat{K}/Q_2(\zeta))^2(\theta^2+\theta-1, \hat{K}/Q_2(\zeta))\\ &=\tilde{\tau}^{*2}\ .\end{aligned}$$

Thus we have proved the following

LEMMA 4. *If $p=2$, then there exists a system of generators $\{\tilde{\sigma}, \tilde{\tau}^*, \tilde{\tau}\}$ of $G(\hat{K}/Q_2)$ such that*

$$\tilde{\tau}^{2^{\nu-2}}=1, \qquad \tilde{\tau}^{*2}(\tilde{\tau}, \tilde{\sigma})=1\ ,$$

where $\tilde{\sigma}$, $\tilde{\tau}^*$, $\tilde{\tau}$ are extensions of σ, τ^*, and τ defined by (3) *to $\hat{K}$.*

§ 3. Galois groups of class two extensions over Q

Let m be a positive integer, K_m be the m-th cyclotomic field over Q, and let $\hat{K}_{mp_\infty}$ be the central class field mod mp_∞ of K_m/Q in the sense of [5, § 3], p_∞ being the real prime divisor of Q. Then $\hat{K}_{mp_\infty}$ is a nilpotency class two extension over Q. We have proved the following theorem[6] in [5].

6) Denote by $m>0$ the finite part of the Galois conductor $\mathfrak{f}(L/Q)$ of L/Q in the sense of [5, §2]. Then it follows from the same procedure as the proof of [5, Lemma 37] that $L\subset\hat{K}_{mp_\infty}$.

THEOREM A. *If $L/\boldsymbol{Q}$ is a normal extension whose Galois group is of nilpotency class two, then there exists a positive integer m such that $L \subset \hat{K}_{mp_\infty}$.*

Hence it is enough to determine the Galois group $G(\hat{K}_{mp_\infty}/\boldsymbol{Q})$ in order to classify all nilpotency class two extensions over $\boldsymbol{Q}$. The discussion of our theory is based on the following

THEOREM B ([5, Theorem 32]). *Notation being as above, we have*

$$G(\hat{K}_{mp_\infty}/K) \simeq H^{-3}(G(K_m/\boldsymbol{Q}), \boldsymbol{Z}) \qquad \textit{when } (m, 16) \neq 8 .$$

Now put $m = 2^\nu p_1^{\nu_1} \cdots p_r^{\nu_r}$, $p_1, \cdots, p_r$ distinct odd primes. For use of Theorem B we distinguish three cases:

$$\text{(a)} \quad \nu = 0 , \qquad \text{(b)} \quad \nu = 2 , \qquad \text{(c)} \quad \nu \geqq 4 .$$

In this paper we will prove our main theorem for (c) and state the corresponding results for (a) and (b), because they follow from the result in the case (c) by only notational changes.

Assume $\nu \geqq 4$. Let g_i be a primitive root mod $p_i^{\nu_i}$, and let

$$\sigma_i = \left(\frac{p_i, K}{p_i}\right)^{-1}, \qquad \tau_i = \left(\frac{g_i, K}{p_i}\right), \qquad i = 1, \cdots, r,$$

$$\sigma_0 = \left(\frac{2, K}{2}\right)^{-1}, \qquad \tau^* = \left(\frac{-1, K}{2}\right), \qquad \tau = \left(\frac{5, K}{2}\right),$$

where $\left(\frac{\cdot, \cdot}{\cdot}\right)$ denotes the norm residue symbol for $K/\boldsymbol{Q}$, and we write briefly

$$K = K_m , \qquad \hat{K} = \hat{K}_{mp_\infty} .$$

Then τ_i is a generator of the inertia group of a prime factor of p_i in K, and, τ^*, τ are generators of the inertia group of a prime factor of 2 in K. Since $G(K/\boldsymbol{Q})$ is isomorphic to the group of prime residue classes mod m, $\{\tau^*, \tau, \tau_1, \cdots, \tau_r\}$ is a system of generators of $G(K/\boldsymbol{Q})$. Let F be the free group with $r + 2$ generators $x^*, x, x_1, \cdots, x_r$, and let

$$1 \to R(K) \to F \to G(K/\boldsymbol{Q}) \to 1$$

be the free presentation of $G(K/\boldsymbol{Q})$ under the correspondence $x^* \to \tau^*$, $x \to \tau$, $x_i \to \tau_i$, $i = 1, \cdots, r$. Then we have, from the structure of $G(K/\boldsymbol{Q})$,

$$R(K) = < x^{*2}, x^{2^{\nu-2}}, x_1^{\psi(p_1^{\nu_1})}, \cdots, x_r^{\psi(p_r^{\nu_r})}, F' > .$$

We identify each decomposition group with the corresponding local Galois group, and choose extensions $\{\tilde{\sigma}_i, \tilde{\tau}_i\}$ and $\{\tilde{\sigma}_0, \tilde{\tau}^*, \tilde{\tau}\}$ of $\{\sigma_i, \tau_i\}$ and $\{\sigma_0, \tau^*, \tau\}$ to $\hat{K}$ to satisfy the relations contained in Lemmas 2 and 4, respectively. Then $\{\tilde{\tau}^*, \tilde{\tau}, \tilde{\tau}_1, \cdots, \tilde{\tau}_r\}$ is a system of generators of $G(\hat{K}/\boldsymbol{Q})$, because $G(\hat{K}/\boldsymbol{Q})$ is a finite nilpotent group of class two. Let

$$1 \to R(\hat{K}) \to F \to G(\hat{K}/\boldsymbol{Q}) \to 1$$

be the free presentation of $G(\hat{K}/\boldsymbol{Q})$ under the correspondence $x^* \to \tilde{\tau}^*$, $x \to \tilde{\tau}$, $x_i \to \tilde{\tau}_i$, $i = 1, \cdots, r$. Then we have

$$R(K) \supset R(\hat{K}) \supset (R(K), F)$$

and

$$[R(K): R(\hat{K})] = [\hat{K}: K] = [H^{-3}(G(K/\boldsymbol{Q}), \boldsymbol{Z}): 1] ,$$

because of Theorem B.

LEMMA 5. *Notation being as above, if σ_i can be written in the form*

$$\sigma_i = f_i(\tau^*, \tau, \tau_1, \cdots, \tau_r) , \qquad i = 0, 1, \cdots, r ,$$

then we have

$$R(\hat{K}) = < x^{*2}(x, y_0), x^{2^{\nu-2}}, x_1^{\psi(p_1^{\nu_1})}(x_1^{p_1^{\nu_1-1}}, y_1), \cdots, x_r^{\psi(p_r^{\nu_r})}(x_r^{p_r^{\nu_r-1}}, y_r), (R(K), F) > ,$$

where $y_j = f_i(x^*, x, x_1, \cdots, x_r)$, $i = 0, 1, \cdots, r$.

Proof. Since the restriction of $f_i(\tilde{\tau}^*, \tilde{\tau}, \tilde{\tau}_1, \cdots, \tilde{\tau}_r)$ on K is σ_i, we may write

$$f_i(\tilde{\tau}^*, \tilde{\tau}, \tilde{\tau}_1, \cdots, \tilde{\tau}_r) = \tilde{\sigma}_i \rho_i , \qquad \rho_i \in G(\hat{K}/K) ,$$

and hence for any $\gamma \in G(\hat{K}/\boldsymbol{Q})$ we have

$$(\gamma, f_i(\tilde{\tau}^*, \tilde{\tau}, \tilde{\tau}_1, \cdots, \tilde{\tau}_r)) = \gamma \tilde{\sigma}_i \rho_i \gamma^{-1} \rho_i^{-1} \tilde{\sigma}_i^{-1} = \gamma \tilde{\sigma}_i \gamma^{-1} \tilde{\sigma}_i^{-1} = (\gamma, \tilde{\sigma}_i) ,$$

because $G(\hat{K}/K)$ is contained in the center of $G(\hat{K}/\boldsymbol{Q})$. Thus $R(\hat{K})$ contains the right hand side under the homomorphism $x^* \to \tilde{\tau}^*$, $x \to \tilde{\tau}$, $x_i \to \tilde{\tau}_i$, $i = 1, \cdots, r$, because of Lemmas 2 and 4. On the other hand,

$$\{x^{*2}(x, y_0) \bmod F' = x^{*2} \bmod F', x^{2^{\nu-2}} \bmod F', \cdots, x_i^{\psi(p_i^{\nu_i})}(x_i^{p_i^{\nu_i-1}}, y_i) \bmod F' = x_i^{\psi(p_i^{\nu_i})} \bmod F', \quad i = 1, \cdots, r\}$$

is a basis for the free Abelian group $R(K)F'/F'$. Hence by virtue of Lemma 1 and (1) we have

$$[R(K): \text{the right hand side}] = [H^{-3}(G(K/\boldsymbol{Q}), \boldsymbol{Z}): 1] ,$$

which implies that $R(\hat{K})$ coincides with the right hand side. Q.E.D.

According to A. Fröhlich [1], to write explicitly f_i is realized by use of the product formula in class field theory as follows. We define the symbols $[j, i]$, $[0, i]^*$, $[0, i]$ by putting

$$(5) \quad \begin{cases} p_i \equiv g_j^{[j,i]} \pmod{p_j^{\nu_j}} , & i = 0, 1, \cdots, r , \quad j = 1, \cdots, r , \quad i \neq j , \\ p_i \equiv (-1)^{[0,i]^*} 5^{[0,i]} \pmod{2^\nu} , & i = 1, \cdots, r , \\ [i, i] = 0 , & i = 1, \cdots, r , \end{cases}$$

where $p_0 = 2$. In other words $[j, i]$ is the index of p_i for the modulus $p_j^{\nu_j}$ relative to the primitive root g_j and $[0, i]^*$, $[0, i]$ are the indices of p_i for the modulus 2^ν relative to the basis $\{-1, 5\}$. These symbols are called the cross coefficients for K in [1, pp. 237–238] when $K/\boldsymbol{Q}$ is a maximal Abelian extension of prime power degree. It is obvious that

$$\left(\frac{p_i, K}{p_j}\right) = \tau_j^{[j,i]} , \quad i = 0, 1, \cdots, r , \quad j = 1, \cdots, r , \quad i \neq j ,$$

$$\left(\frac{p_i, K}{p_i}\right) = \sigma_i^{-1} , \qquad i = 0, 1, \cdots, r ,$$

$$\left(\frac{p_i, K}{2}\right) = \tau^{*[0,i]^*} \tau^{[0,i]} , \qquad i = 1, \cdots, r .$$

Therefore we have

$$\sigma_i = \tau^{*[0,i]^*} \tau^{[0,i]} \prod_{j=1}^{r} \tau_j^{[j,i]} \qquad \text{for } i = 1, \cdots, r ,$$

because of $\prod_{\text{all } p} \left(\frac{p_i, K}{p}\right) = 1$, and

$$\sigma_0 = \prod_{j=1}^{r} \tau_j^{[j,0]} ,$$

because of $\prod_{\text{all } p} \left(\frac{2, K}{p}\right) = 1$. Hence each y_i in Lemma 5 is given by

$$y_0 = \prod_{j=1}^{r} x_j^{[j,0]} ,$$

$$y_i = x^{*[0,i]^*} x^{[0,i]} \prod_{j=1}^{r} x_j^{[j,i]} , \qquad i = 1, \cdots, r .$$

It is well-known that if a, b, c are elements in a group of class two, then

$$(ab, c) = (a, c)(b, c) , \qquad (a, bc) = (a, b)(a, c) .$$

Thus we have proved the following main

THEOREM 6. *Let $m = 2^{\nu}p_1^{\nu_1} \cdots p_r^{\nu_r}$ be a natural number, K_m be the m-th cyclotomic field over the rational number field $\boldsymbol{Q}$, and let $\hat{K}_{mp_\infty}$ be the central class field* mod mp_∞ *of $K_m/\boldsymbol{Q}$, p_∞ being the real prime divisor of $\boldsymbol{Q}$. Then*:

(a) $\nu = 0$. *The Galois group $G(\hat{K}_{mp_\infty}/\boldsymbol{Q})$ of $\hat{K}_{mp_\infty}$ over $\boldsymbol{Q}$ is generated by r elements $x_1, \cdots, x_r$, and completely determined by the relations*

$$(x_i, x_j)x_k = x_k(x_i, x_j) , \qquad \textit{all } i, j, k ,$$
$$x_i^{\psi(p_i^{\nu_i})} = \left(\prod_{j=1}^{r} (x_i, x_j)^{-[j,i]}\right)^{p_i^{\nu_i - 1}} , \qquad i = 1, \cdots, r .$$

(b) $\nu = 2$. *$G(\hat{K}_{mp_\infty}/\boldsymbol{Q})$ is generated by $r + 1$ elements $x_0, x_1, \cdots, x_r$, and completely determined by the relations*

$$(x_i, x_j)x_k = x_k(x_i, x_j) , \qquad \textit{all } i, j, k ,$$
$$x_0^2 = 1 ,$$
$$x_i^{\psi(p_i^{\nu_i})} = \left((x_i, x_0)^{-[0,i]^*} \prod_{j=1}^{r} (x_i, x_j)^{-[j,i]}\right)^{p_i^{\nu_i - 1}} , \qquad i = 1, \cdots, r .$$

(c) $\nu = 4$. *$G(\hat{K}_{mp_\infty}/\boldsymbol{Q})$ is generated by $r + 2$ elements $x_{-1}, x_0, x_1, \cdots, x_r$, and completely determined by the relations*

$$(x_i, x_j)x_k = x_k(x_i, x_j) , \qquad \textit{all } i, j, k ,$$
$$x_{-1}^{2^{\nu-2}} = 1 ,$$
$$x_0^2 = \prod_{j=1}^{r} (x_{-1}, x_j)^{-[j,0]} ,$$
$$x_i^{\psi(p_i^{\nu_i})} = \left((x_i, x_{-1})^{-[0,i]}(x_i, x_0)^{-[0,i]^*} \prod_{j=1}^{r} (x_i, x_j)^{-[j,i]}\right)^{p_i^{\nu_i - 1}} , \qquad i = 1, \cdots, r ,$$

where $[j, i]$, $[0, i]^*$, $[0, i]$ are the indices defined by (5).

REFERENCES

[1] A. Fröhlich, On fields of class two, Proc. London Math. Soc. (3), 4 (1954), 235–256.
[2] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin-New York, 1967.
[3] H. Koch, Fields of class two and Galois cohomology, Algebraic Number Fields, Proc. Symp. London Math. Soc., Univ. Durham 1975, (1977), 609–624.
[4] A. G. Kurosh, The Theory of Groups, 2nd ed., Gostehizdat, Moscow, 1953 (in Rus-

sian). English translation published by Chelsea, New York, 1955, 1956.
[5] S. Shirai, On the central class field mod $\mathfrak{m}$ of Galois extensions of an algebraic number field, Nagoya Math. J., **71** (1978), 61–85.
[6] J. Smith, On class 2 extensions of algebraic number fields, Amer. J. Math., **87** (1965), 537–550.

Toyama Medical and Pharmaceutical University