On the structure of p-class groups of certain number fields

By

Teruo TAKEUCHI*

(Received November 8, 1976)

1. Introduction

Let K/k be a cyclic extension of prime degree p over an algebraic number field k of finite degree, let M_K be the p-class group of K. The structure of M_K has been studied by many people especially by E. Inaba [5] and G. Gras [3]. In their works M_K is considered as a module over $Gal(K/k)$, where $Gal(K/k)$ is the Galois group of K/k.

In the present paper we shall show first (in **2**) that the results on M_K is, when the class number h_k of k is relatively prime to odd prime p, obtained simply by considering M_K as a module over $\mathfrak{O}$, where $\mathfrak{O}$ is the algebraic integer ring of the cyclotomic field of p-th roots of unity.

The second purpose of this paper is to study the relation between M_L and M_K using the results of **2** (in **3**), where $K/\mathbf{Q}$ is a cyclic extension of degree p such that only two primes are ramified in it, and where $L/\mathbf{Q}$ is the genus field of $K/\mathbf{Q}$. Finally we shall show (in **4**) by a similar method to that used in **3** that there exist infinitely many cyclic extensions $K/\mathbf{Q}$ of degree p such that p-ranks of M_K are 2 and p-class field towers of K are finite.

Throughout this paper we use the following notation.

$\mathbf{Z}$: the ring of rational integers

$\mathbf{Q}$: the rational number field

p: a rational odd prime

$\xi_p=\xi$: a primitive p-th root of unity

$\mathfrak{O}$: the algebraic integer ring of $\mathbf{Q}(\xi)$

$\mathfrak{p}$: the prime divisor of p in $\mathfrak{O}$

For an algebraic number field K of finite degree,

C_K: the ideal class group of K

h_K: the class number of K

M_K: the p-Sylow group of C_K

For an ideal $\mathfrak{a}$ of K

$cl(\mathfrak{a})$: the ideal class of $\mathfrak{a}$

---

* Niigata University.

$cl_p(\mathfrak{a})$: the p-part of $cl(\mathfrak{a})$ (then for a natural number a prime to p we may write $cl_p(\mathfrak{a})=cl(\mathfrak{a})^a$.)

For a module M and a homomorphism f of M,

M^f: the image of f

$M_{(f)}$: the kernel of f.

2. General results in case $p\not| h_k$

LEMMA 1. *Let M be a finite module over $\mathfrak{O}$ whose order is a power of p. Then M is $\mathfrak{O}$-isomorphic to $\sum_{i=1}^{r}\mathfrak{O}/\mathfrak{p}^{e_i}$, where $p^r=\#(M/M^{\xi-1})$.*

PROOF. Let $\mathfrak{O}_\mathfrak{p}$ be the localization of $\mathfrak{O}$ at $\mathfrak{p}$. Since the order of M is a power of p, M is a module over $\mathfrak{O}_\mathfrak{p}$. As $\mathfrak{O}_\mathfrak{p}$ is a principal ideal domain, by the general theory of a module over a principal domain we have a $\mathfrak{O}$-isomorphism; $M\approx\sum_{i=1}^{r}\mathfrak{O}/\mathfrak{p}^{e_i}$. And from

$$M/M^{\xi-1}\approx\sum_{i=1}^{r}(\mathfrak{O}/\mathfrak{p}^{e_i})/(\mathfrak{p}/\mathfrak{p}^{e_i})\approx(\mathfrak{O}/\mathfrak{p})^r,$$

we see $p^r=\#(M/M^{\xi-1})$. Q. E. D.

THEOREM 1. *Let k be an algebraic number field of finite degree. and let K/k be a cyclic extension of degree p. Assume that $p\not| h_k$. Then M_k is a module over $\mathfrak{O}$ and $\mathfrak{O}$-isomorphic to $\sum_{i=1}^{r}\mathfrak{O}/\mathfrak{p}^{e_i}$, where*

$$p^r=\frac{p^{t-1}}{(E_k\colon E_k\cap N_{K/k}K^*)}$$

t = the number of prime ideals of k ramified in K

E_k = the unit group of k.

PROOF. Let σ be a generator of $Gal(K/k)$. Since $p\not| h_k$, the restriction of the norm map $N_{K/k}$: $C_K\to C_k\to C_K$ to M_K is trivial. Hence we can view M_K as a module over $Z[\sigma]/N$, where $N=Z[\sigma](1+\sigma+\dots\dots+\sigma^{p-1})$. Since $Z[\sigma]/N\approx\mathfrak{O}$ by $\sigma N\to\xi_p$, we can also view M_K as a module over $\mathfrak{O}$. On the other hand we note that:

$$M_K/M_K^{\sigma-1}\approx M_{K(\sigma-1)}=C_{K(\sigma-1)}\cap M_K,$$

$$\#(C_{K(\sigma-1)})=h_k\frac{p^{t-1}}{(E_K\colon E_k\cap N_{K/k}K^*)}.$$

Therefore using that $p\not| h_k$ and $(E_k\colon E_k\cap N_{K/k}K^*)$ is a power of p, we have

$$\#(M_K/M_K^{\sigma-1})=\frac{p^{t-1}}{(E_k\colon E_k\cap N_{K/k}K^*)}.$$

Hence by Lemma 1 we have our theorem. Q. E. D.

Let K/k be as in Theorem 1. Then as $p\not| h_k$, K/k is ramified. If $t=1$, then $r=0$ so

$M_K=\{1\}$. And we assume $t\geqq 2$. Let $\mathfrak{p}_1, \ldots\ldots \mathfrak{p}_t$ be the prime ideals ramified in K/k, and let for $\alpha\in k^*$,

$\chi_i(\alpha)=\left(\frac{\alpha:K/k}{\mathfrak{p}_i}\right)$; norm residue symbol locally at $\mathfrak{p}_i$. Let $\chi: k^*\to G^t$ by $\chi(\alpha)=(\chi_1(\alpha), \ldots\ldots, \chi_t(\alpha))$, where $G=Gal(K/k)$. And let $\hat{X}=G^t/\chi(E_k)$. For an element a of M_K, let $\mathfrak{a}$ be an ideal of K such that $a=cl(\mathfrak{a})$. Then as $p\nmid h_k$, $N_{K/k}(\mathfrak{a})$ is principal in k. Say $N_{K/k}(\mathfrak{a})=(\alpha)$, $\alpha\in k^*$. Then we define $\hat{\chi}$: $M_K\to\hat{X}$ by $\hat{\chi}(a)=\chi(\alpha) \bmod \chi(E_k)\in\hat{X}$. By the property of norm residue symbol, it is easily verified that this is well-defined. Furthermore since $\hat{\chi}(M_K{}^{\sigma-1})=1\in\hat{X}$, $\hat{\chi}$ induces the homomorphism $\hat{\chi}_{K/k}$: $M_K/M_K{}^{\sigma-1}\longrightarrow\hat{X}$. Then, the next lemma is essentially a special case of [2, Theorem] and follows from **Hasse Norm Theorem** and **Hilbert's Theorem 90.**

LEMMA 2. $\hat{\chi}_{K/k}$: $M_K/M_K{}^{\sigma-1}\longrightarrow\hat{X}$ is a monomorphism.

REMARK. Let χ': $k^*\longrightarrow G^{t-1}$ by $\chi(\alpha)=(\chi_1(\alpha),\ldots\ldots, \chi_{t-1}(\alpha))$ and $\hat{X}'=G^{t-1}/\chi'(E_K)$. If we define a homomorphism

$$\hat{\chi}'_{K/k}: M_K/M_K{}^{\sigma-1}\longrightarrow\hat{X}'$$

by means of $\hat{\chi}'$ and $\hat{X}'$, then $\hat{\chi}_{K/k}$ is an isomorphism. (cf. [4, Satz 1])

By $\hat{\chi}_{K/k}$ we can form an estimate of *rank* M_K.

THEOREM 2. *Let the notation and assumption be as in Theorem 1. Let rank* $M_K=d$ (i. e. $\#(M_K/M_K{}^p)=p^d$), $\#(\chi_{K/k}(M_{K(\sigma-1)}))=p^s$.
Then

(i) $2r-s\leqq d\leqq(p-2)(r-s)+r$,

(ii) *especially, if* $r=s$, *then* $d=r$ *and* M_K *is elementary.*

PROOF. Let $M_K\approx\sum_{i=1}^{r}\mathfrak{O}/\mathfrak{p}^{e_i}$, where $e_1\ldots\ldots e_r$, and $rank(\mathfrak{O}/\mathfrak{p}^{e_i})=d_i$. Then $d=d_1+\ldots\ldots+d_r$ and $1\leqq d_i\leqq p-1$. On the other hand $d_i=1$ if and only if $e_i=1$, and $(\mathfrak{O}/\mathfrak{p}^{e_i})_{(\xi-1)}=\mathfrak{p}^{e_i-1}/\mathfrak{p}^{e_i}$. Therefore it follows from Lemma 2 that $e_1=\ldots\ldots=e_s=d_1=\ldots\ldots=d_s=1$, and $2\leqq d_i\leqq p-1$ for $i=s+1, \ldots\ldots, r$. This proves (i). If $r=s$, then $e_1=\ldots\ldots=e_r=1$ and $M_K\approx(\mathfrak{O}/\mathfrak{p})^r$. This proves (ii). Q. E. D.

Moreover, if $E_k=\{\pm 1\}$ i. e. $k=\mathbf{Q}$ or k is a imaginary quadratic field such that $k\neq\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{-1})$, then s in Theorem 2 is expressed more explicitly as follows. In this case, $r=t-1$ and $\hat{X}=G^t$ since $E_k=N_{K/k}E_K=\{\pm 1\}$. Furthermore, as $(E_k\cap N_{K/k}K^*: N_{K/k}E_K)=1$, every ambiguous ideal class in K/k is represented by an ambiguous ideal in K/k. Hence $M_{K(\sigma-1)}$ is generated by $cl(\mathfrak{P}_1{}^{h_k}), \ldots\ldots, cl(\mathfrak{P}_t{}^{h_k})$, where $\mathfrak{P}_i$ is the prime divisor of $\mathfrak{p}_i$ in K. Therefore $\hat{\chi}_{K/k}(M_{K(\sigma-1)})$ is generated by

$$\left(\left(\frac{\alpha_i:K/k}{\mathfrak{p}_1}\right), \ldots\ldots, \left(\frac{\alpha_i:K/k}{\mathfrak{p}_t}\right)\right), \text{ where } (\alpha_i)=\mathfrak{p}_i{}^{h_k},$$

for $i=1, \ldots\ldots, r$. And for a generator σ of $Gal(K/k)$, let

$$\left(\left(\frac{\alpha_i: K/k}{\mathfrak{p}_j}\right)\right)_{i,j=1,\cdots\cdots,t} = (\sigma^{a_{ij}})_{i,j=1,\cdots\cdots,t}$$

where $a_{ij} \in \mathbf{Z}/p\mathbf{Z}$, then $s = rank(a_{ij})$.

In case $k=\mathbf{Q}(\sqrt{-3})$ $(p \neq 3)$, $k=\mathbf{Q}(\sqrt{-1})$, similar results hold.

REMARK. Let $\mathfrak{q}$ be a prime ideal of k with $\mathrm{N}\mathfrak{q} \equiv 1 \bmod p$. If $p \nmid h_k$, then the p-Sylow group of $I(\mathfrak{q})/P\mathfrak{q}$ is cyclic, where $I(\mathfrak{q})$ is the ideal group of k prime to $\mathfrak{q}$ and $P\mathfrak{q}$ is the ray mod $\mathfrak{q}$. Let $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_m$ be prime ideals of k with $\mathrm{N}\mathfrak{p}_i \equiv 1 \bmod p$, and let $\mathfrak{c} = p \cdot \mathfrak{p}_1 \cdots\cdots \mathfrak{p}_m$. Assume $p \nmid h_k$ and $E_k = \{\pm 1\}$. Then the p-Sylow group of $I(\mathfrak{c})/P\mathfrak{c}$ is isomorphic to the p-Sylow group of $(I(p)/P_p) \times (I(\mathfrak{p}_1)/P_{\mathfrak{p}_1}) \times \cdots\cdots \times (I(\mathfrak{p}_m)/P_{\mathfrak{p}_m})$ by the natural homomorphism;

$$I(\mathfrak{c})/P\mathfrak{c} \longrightarrow (I(p)/P_p) \times (I(\mathfrak{p}_1)/P_{\mathfrak{p}_1}) \times \cdots\cdots \times (I(\mathfrak{p}_m)/P_{\mathfrak{p}_m}).$$

Hence it follows from **Dirichlet Density Theorem** that for each integer $t \geqq 2$, there exist infinitely many t-tuples of prime ideals $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$, such that

$\mathrm{N}\mathfrak{p}_i \equiv 1 \bmod p$, $i=1, \cdots\cdots, t$,

$\mathfrak{p}_2$: p-th power nonresidue mod $P_{\mathfrak{p}_1}$

$\mathfrak{p}_i$: p-th power residue mod $P_{\mathfrak{p}_1 \cdots\cdots \mathfrak{p}_{i-2}}$

but p-th power nonresidue mod $P_{\mathfrak{p}_{i-1}}$ for $i=3, \cdots\cdots, t$.

Let K/k be a cvclic extension of degree p in which only $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ are ramified. Then it holds that for $i \neq j$

$\left(\frac{\alpha_i: K/k}{\mathfrak{p}_j}\right) = 1$ if and only if $\mathfrak{p}_i$: p-th power residue mod $P_{\mathfrak{p}_j}$, where $(\alpha_i) = \mathfrak{p}_i$. Hence M_K satisfies the condition of Theorem 2, (ii) and so $M_K \approx (\mathfrak{O}/\mathfrak{p})^{t-1}$.

[1, Theorem 1] is a special case ($k=\mathbf{Q}$) of this remark.

3.

Let $K/\mathbf{Q}$ be a cyclic extension of degree p in which only p_1, p_2 are ramified. Then from Theorem 1 we know

$$M_K \approx \mathfrak{O}/\mathfrak{p}^e : \quad e \geqq 1.$$

And let L be the genus field of $K/\mathbf{Q}$, then L/K is an unramified extension of degree p. Moreover let $K_i/\mathbf{Q}$ be the cyclic extension of degree p in which only p_i is ramified. Then noting L/K_i is cyclic with degree p and $p \nmid h_{K_i}$, we have

$$M_L \approx \sum_{i=1}^{r} \mathfrak{O}/\mathfrak{p}^{e_i}.$$

And from the results of **1**, it follows that $e > 1$ if and only if

$$\begin{pmatrix} \left(\frac{p_1 : K/\mathbf{Q}}{p_1}\right) & \left(\frac{p_1 : K/\mathbf{Q}}{p_2}\right) \\ \left(\frac{p_2 : K/\mathbf{Q}}{p_1}\right) & \left(\frac{p_2 : K/\mathbf{Q}}{p_2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

If $e=1$, then it is easily seen from **Burnside Basis Theorem** that $M_L=\{1\}$. And so we suppose $e\geqq 2$. Let $\mathfrak{p}_i$ be the prime divisor of p_i in K. Then at least one of $\mathfrak{p}_1$, $\mathfrak{p}_2$ is not principal. Say $\mathfrak{p}_2$ be not principal. Let $\mathfrak{p}_{i1}$ be a prime divisor of $\mathfrak{p}_i$ in K_1, and let τ be a generator of $Gal(K_1/\mathbf{Q})$. As p_1 is ramified in K_1 and p_2 is completely decomposed in K_1, it holds that

$$(p_1)=\mathfrak{p}_{11}{}^{p}$$

$$(p_2)=\mathfrak{p}_{21}\mathfrak{p}_{21}{}^{\tau}\cdots\cdots\mathfrak{p}_{21}{}^{\tau^{(p-1)}}.$$

Then only $\mathfrak{p}_{21}, \mathfrak{p}_{21}{}^{\tau}, \cdots\cdots, \mathfrak{p}_{21}{}^{\tau^{(p-1)}}$ are ramified in L/K_1.

THEOREM 3. *Let $K/\mathbf{Q}$ be a cyclic extension of degree p in which only p_1, p_2 are ramified, and let L be the genus field of $K/\mathbf{Q}$. Let $\mathfrak{p}_i$ be the prime divisor of p_i in K, and let $\mathfrak{P}_i$ be a prime divisor of $\mathfrak{p}_i$ in L. Assume $\mathfrak{p}_2$ is not principal. Let $K_1/\mathbf{Q}$ be the cyclic extension of degree p in which only p_1 is ramified. Let $M_K\approx\mathfrak{O}/\mathfrak{p}^e$, and assume $e\geqq 2$. Then the following conditions are equivalent;*

(i) $e=2$,

(ii) $(E_{K_1}\cap N_{L/K_1}L^*: N_{L/K_1}E_L)=1$ *and* $M_L\approx(\mathfrak{O}/\mathfrak{p})^r$,

(iii) $\chi_{L/K_1}(cl_p(\mathfrak{P}_2{}^{(\tau-1)^{r-1}}))\neq 1$,

where

$$p^r=\frac{p^{p-1}}{(E_{K_1}: E_{K_1}\cap N_{L/K_1}L^*)}$$

$\tau =$ *a generator of* $Gal(L/K)$.

LEMMA 3. *Let L/K be an unramified cyclic extension of degree p, and let τ be a generator of $Gal(L/K)$. Then $(E_K: E_K\cap N_{L/K}L^*)=1$ and $M_L/M_L{}^{\tau-1}$ is isomorphic to $N_{L/K}M_L$ ($\subset M_K$) under the norm map $N_{L/K}$.*

PROOF. Since $(M_K: N_{L/K}M_L)=p$, we have $\#(N_{L/K}M_L)=\#(M_K)/p$. Let $\mathbf{N}_{L/K}: M_L/M_L{}^{\tau-1}\rightarrow M_K$ be the homomorphism induced from the norm map $N_{L/K}$. Then, as

$$\#(M_L/M_L{}^{\tau-1})=\#(M_{L(\tau-1)})=\frac{\#(M_K)}{p(E_K: E_K\cap N_{L/K}L^*)},$$

we have

$$\#(Ker\ \mathbf{N}_{L/K})=\frac{\#(M_L/M_L{}^{\tau-1})}{\#(N_{L/K}M_L)}=\frac{1}{(E_K: E_K\cap N_{L/K}L^*)}. \qquad \text{Q. E. D.}$$

PROOF of Theorem 3. Let σ be a generator of $Gal(L/K_1)$, then we can consider σ as a generator of $Gal(K/\mathbf{Q})$. Since $(M_K: N_{L/K}M_L)=p$ and $N_{L/K}M_L$ is σ–admissible,

$N_{L/K}M_L = M_K^{\sigma-1}$. Hence by Lemma 3 we have

$$N_{L/K}\colon M_L/M_L^{\tau-1} \approx M_K^{\sigma-1} \approx \mathfrak{p}/\mathfrak{p}^e.$$

Assume (i). Then $\#(M_L/M_L^{\tau-1}) = p$. As $\mathfrak{p}_2$ is not principal, we have $N_{L/K}\, cl_p(\mathfrak{P}_2) = cl(\mathfrak{p}_2)^a \neq 1 \in M_K$. Hence by Lemma 3 $cl_p(\mathfrak{P}_2) \notin M_L^{\tau-1}$. Thus M_L is generated by $cl_p(\mathfrak{P}_2)$, $cl_p(\mathfrak{P}_2)^{\tau-1}$, $cl_p(\mathfrak{P}_2)^{(\tau-1)^2}, \ldots\ldots$ As $\mathfrak{P}_2$ is an ambiguous ideal in L/K_1, $M_{L(\sigma-1)} = M_L$ and every class in M_L is represented by ambiguous idal in L/K_1. On the other hand, let $C_{L(\sigma-1)}{}^0$ be the group of ideal classes represented by ambiguous ideals in L/K_1. Then $(M_{L(\sigma-1)}\colon M_{L(\sigma-1)}{}^0) = 1$ implies $(C_{L(\sigma-1)}\colon C_{L(\sigma-1)}{}^0) = 1$ since $(C_{L(\sigma-1)}\colon C_{L(\sigma-1)}) = (E_{K_1} \cap N_{L/K_1}L^*\colon N_{L/K_1}E_L) =$ a power of p, where $M_{L(\sigma-1)}{}^0 = C_{L(\sigma-1)}{}^0 \cap M_L$. Hence $(E_{K_1} \cap N_{L/K_1} L^*\colon N_{L/K_1}E_L) = 1$. This proves that (i) implies (ii). Conversely, assume (ii). Then $M_L = M_{L(\sigma-1)}$ and every ambiguous class in L/K_1 is represented by an ambiguous ideal in L/K_1. Therefore M_L is generated by $cl_p(\mathfrak{P}_2)$, $cl(\mathfrak{P}_2)^\tau, \ldots\ldots, cl_p(\mathfrak{P}_2)^{\tau^{p-1}}$. And since $cl_p(\mathfrak{P}_2)^\tau \equiv cl_p(\mathfrak{P}_2) \bmod M_L^{\tau-1}$, $M_L/M_L^{\tau-1}$ is generated by $cl_p(\mathfrak{P}_2)M_L^{\tau-1}$. Since $cl_p(\mathfrak{P}_2) \notin M_L^{\tau-1}$ and the order of $cl_p(\mathfrak{P}_2)$ is p, we have $\#(M_L/M_L^{\tau-1}) = p$. Hence $e = 2$, which proves that (ii) implies (i).

The fact that (ii) implies (iii) is obvious. Conversely assume (iii). Then since $p^r = \#(M_{L(\sigma-1)})$, $M_{L(\sigma-1)}$ is generated by $cl_p(\mathfrak{P}_2)$, $cl_p(\mathfrak{P}_2)^{\tau-1}, \ldots\ldots, cl_p(\mathfrak{P}_2)^{(\tau-1)^{r-1}}$. Hence every ambiguous class in L/K_1 is represented by an ambiguous ideal in L/K_1. Thus we have $(E_{K_1} \cap N_{L/K_1}L^*\colon N_{L/K_1}E_L) = 1$. Next suppose there exist $a \in M_{L(\sigma-1)}$ and $b \in M_L$ such that $a = b^{\sigma-1} \neq 1$. Put $a_i = cl_p(\mathfrak{P}_2)^{(\tau-1)^i}$ for $i = 0, 1, \ldots\ldots, r-1$. Then we can write $a = a_j^{f_j} \cdot a_{j+1}^{f_{j+1}} \ldots\ldots a_{r-1}^{f_{r-1}}$, where $f_j \not\equiv 0 \bmod p$. Then $a^{(\tau-1)^{r-1-j}} = a_{r-1}^{f_j} = b^{(\tau-1)^{r-1-j}(\sigma-1)}$. Hence $cl_p(\mathfrak{P}_2)^{(\tau-1)^{r-1}f_j} = b^{(\tau-1)^{r-1-j}(\sigma-1)}$. Thus $\widehat{\chi}_{L/K_1}(cl_p(\mathfrak{P}_2{}^{(\tau-1)^{r-1}})) = 1$ which is a contradiction. Therefore $M_L = M_{L(\sigma-1)} \approx (\mathfrak{O}/\mathfrak{p})^r$. This proves that (iii) implies (ii). Q. E. D.

Let p_1, p_2 be odd primes such that $p_i \equiv 1 \bmod p$ or $p_i = p$. Then there exist $p-1$ cyclic extensions $K/\mathbf{Q}$ of degree p in which only p_1, p_2 are ramified, and the genus fields L of such $K/\mathbf{Q}$ coincide. In general, however, every M_K is not necessarily isomorphic to others. But if $M_K \approx \mathfrak{O}/\mathfrak{p}$ for some K, then $p \nmid h_L$. So $M_K \approx \mathfrak{O}/\mathfrak{p}$ for all K. Moreover,

Corollary 1. ([3 Proposition VI 6]) *If $M_K \approx \mathfrak{O}/\mathfrak{p}^2$ for some K, then $M_K \approx \mathfrak{O}/\mathfrak{p}^2$ for all K.*

Proof. Let $K/\mathbf{Q}$, $\widehat{K}/\mathbf{Q}$ be cyclic extensions of degree p in which only p_1, p_2 are ramified, and let $M_K \approx \mathfrak{O}/\mathfrak{p}^2$, $M_{\widehat{K}} \approx \mathfrak{O}/\mathfrak{p}^e$. Let notation be as in Theorem 3. Then we can take a generator $\widehat{\tau}$ of $Gal(L/\widehat{K})$ such that $\widehat{\tau} = \tau \cdot \sigma^j$ for some j. Since it follows from Theorem 3 (ii) that σ operates trivially on M_L, the operations of τ and $\widehat{\tau}$ on M_L coincide. Hence $M_L/M_L^{\widehat{\tau}-1} = M_L/M_L^{\tau-1}$, so $\#(M_L/M_L^{\widehat{\tau}-1}) = p$. Thus we have $M_{\widehat{K}} \approx \mathfrak{O}/\mathfrak{p}^2$. Q. E. D.

Corollary 2. *If for each p_i, $i = 1, 2$ there exists a K in which the prime divisor of p_i is not principal and $M_K \approx \mathfrak{O}/\mathfrak{p}^2$, then $M_L \approx \mathfrak{O}/\mathfrak{p}$.*

Proof. Let the prime divisor $\mathfrak{p}_2$ of p_2 in K be not principal, and let the prime divisor

$\hat{\mathfrak{p}}_1$ of p_1 in $\hat{K}$ be not principal. Then by Theorem 3 $M_L \approx (\mathfrak{O}/\mathfrak{p})^r$, and $Gal(L/K_1)$, $Gal(L/K_2)$ operate trivially on M_L. Let τ be a generator of $Gal(L/K)$. Then τ operates trivially on M_L, so $M_L^{\tau-1} = \{1\}$. Thus we have $M_L \approx M_L/M_L^{\tau-1} \approx \mathfrak{O}/\mathfrak{p}$. Q. E. D.

4

Let $K/\mathbf{Q}$ be a cyclic extension of degree p, and let $r(M_K)$ be the rank of M_K. Then from the results of [6] it follows that if $r(M_K) \geqq 2+2\sqrt{p}$, the p-class field tower of K is infinite.

Using **Čebotarev Density Theorem,** we can show by a similar method to that used in Corollary of Theorem 3 that there exist infinitely many cyclic extensions $K/\mathbf{Q}$ of degree p such that $r(M_K)=2$ and p-class field towers of K are finite.

THEOREM 4. *There exist infinitely many triples of odd primes p_1, p_2, p_3 such that $p \nmid h_{\bar{L}}$, where $\bar{L}$ is the genus field of $K/\mathbf{Q}$ and $K/\mathbf{Q}$ is a cyclic extension of degree p in which only p_1, p_2, p_3 are ramified.*

LEMMA 4. *Let p be an odd prime. For an odd prime p_1 such that $p_1 \equiv 1$ mod p, there exist infinitely many odd primes p_2 which satisfy the following conditions* (i), (ii), (iii);

(i) $p_2 \equiv 1$ *mod* p,

(ii) p_2 *is p-th power nonresidue modulo* p_1,

(iii) p_1 *is p-th power nonresidue modulo* p_2.

PROOF. Put $k=\mathbf{Q}(\xi_p)$, $K_1=\mathbf{Q}\left(\sqrt[p]{p_1}\right)$, $\bar{K}_1=k\cdot K_1$ and let $K/\mathbf{Q}$ be the cyclic extension of degree p in which only p_1 is ramified. Then from **Čebotarev Density Theorem** it follows that the Dirichlet density of the rational primes whose decomposition fields in $\bar{K}_1/\mathbf{Q}$ are k is $1/p$, and that of the rational primes whose decomposition fields in $K\cdot\bar{K}_1/\mathbf{Q}$ are $k\cdot K$ is $1/p^2$. Hence there exist infinitely many odd primes p_2 such that p_2 are not decomposed in $K/\mathbf{Q}$ and their decomposition fields in $\bar{K}_1/\mathbf{Q}$ are k. Then it is obvious that p_2 satisfy (i), (ii). In order to prove (iii), we suppose that p_1 is p-th power residue modulo p_2 Then the equation $X^p-p_1\equiv 0$ mod p_2 has a rational integer solution. Now we may assume $p_2 \nmid \left(\mathfrak{O}_{K_1}: \mathbf{Z}\left[\sqrt[p]{p_1}\right]\right)$, where $\mathfrak{O}_{K_1}$ denotes the integer ring of K_1. So there exists a prime divisor $\mathfrak{p}_2$ of p_2 in K_1 such that $N_{K_1/\mathbf{Q}}\mathfrak{p}_2=p_2$. Let $\mathfrak{P}_2$ be a prime divisor of $\mathfrak{p}_2$ in $\bar{K}_1$, then we have $N_{\bar{K}_1/\mathbf{Q}}\mathfrak{p}_2=p_2{}^p$ since the decomposition field of $\mathfrak{P}_2$ is k. On the other hand, we have $N_{\bar{K}_1/K_1}\mathfrak{P}_2=\mathfrak{p}_2{}^i$ for $1\leqq i\leqq p-1$, which is a contradiction. This proves (iii).

Q. E. D.

COROLLARY *There exist infinitely many triples of odd primes satisfying the following conditions* (i)$\sim$(vi);

(i) $p_i \equiv 1$ *mod* p, $i=1, 2, 3$,

(ii) p_1 *is p-th power nonresidue modulo* p_2,

(iii) p_1 *is p-th power nonresidue modulo* p_3,

(iv) *p_2 is p-th power nonresidue modulo p_1,*

(v) *p_3 is p-th power residue modulo p_1,*

(vi) *p_3 is p-th power nonresidue modulo p_2.*

The proof is analogous to Lemma 4.

PROOF of Theorem 4. Let p_1, p_2, p_3 be primes satisfying the conditions of the above corollary. Let $K_{23}/\mathbf{Q}$ be the cyclic extension of degree p in which only p_2, p_3 are ramified and p_1 is completely decomposed. It follows from above conditions (i), (ii), (iii), that such an extension always exists. Let $K_1/\mathbf{Q}$ be the cyclic extension of degree p in which only p_1 is ramified. Then because of the above condition (v), p_3 is completely decomposed in K_1. Put $L=K_1\cdot K_{23}$. Then $L/\mathbf{Q}$ is an abelian extension of degree p^2 in which only p_1, p_2, p_3 are ramified. Let $K/\mathbf{Q}$ be a subfield of L with degree p over $\mathbf{Q}$ such that $K\neq K_1$, K_{23}. Then p_1, p_2, p_3 are ramified in $K/\mathbf{Q}$, and hence L/K is unramified. Moreover

$$\left(\left(\frac{p_i: K/\mathbf{Q}}{p_j}\right)\right)_{i,j=1,2,3}=\begin{pmatrix} ? & * & * \\ * & ? & ? \\ 1 & * & ? \end{pmatrix},$$

where $*$ means nonidentity.

So by the results of **2** we have $M_K\approx(\mathfrak{O}/\mathfrak{p})^2$. Let $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ be the prime divisors of p_1, p_2, p_3 in K respectively, then these are not principal in K and $\mathfrak{p}_1$, $\mathfrak{p}_3$ are completely decomposed in L/K. And let $\mathfrak{P}_3$ be a prime divisor of $\mathfrak{p}_3$ in L, then $N_{L/K}(cl_p(\mathfrak{P}_3))=cl(\mathfrak{p}_3)^a\neq 1\in M_K$. So by Lemma 3 we have $cl_p(\mathfrak{P}_3)\notin M_L{}^{\tau-1}$, where τ is a generator of $Gal(L/K)$. On the other hand from $M_K\approx(\mathfrak{O}/\mathfrak{p})^2$, we see $\#(M_L/M_L{}^{\tau-1})=p$. Hence M_L is generated by $cl_p(\mathfrak{P}_3)$, $cl_p(\mathfrak{P}_3)^{\tau-1}$, $cl_p(\mathfrak{P}_3)^{(\tau-1)^2}$,....... As $cl(\mathfrak{P}_3)$ is an ambiguous class in L/K_1, the order of $cl_p(\mathfrak{P}_3)$ is p. Let σ_1 be a generator of $Gal(L/K_1)$, then σ_1 operates trivially on M_L since $\mathfrak{P}_3{}^{\sigma_1}=\mathfrak{P}_3$. Similarly, let $\mathfrak{P}_1$ be a prime divisor of $\mathfrak{p}_1$ in L, then $cl_p(\mathfrak{P}_1)\notin M_L{}^{\tau-1}$ and M_L is also generated by $cl_p(\mathfrak{P}_1)$, $cl_p(\mathfrak{P}_1)^{\tau-1}$, $cl_p(\mathfrak{P})^{(\tau-1)^2}$,....... Let σ_{23} be a generator of $Gal(L/K_{23})$, then σ_{23} operates trivially on M_L since $cl(\mathfrak{P}_1)$ is an ambiguous class in L/K_{23}. Therefore noting $Gal(L/\mathbf{Q})$ is generated by $Gal(L/K_1)$ and $Gal(L/K_{23})$ we see that τ also operates trivially on M_L. Thus we have $M_L=M_L/M_L{}^{\tau-1}\approx\mathfrak{O}/\mathfrak{p}$. On the other hand $\bar{L}/L$ is the unramified cyclic extension of degree p. Hence by **Burnside Basis Theorem** we have $p\nmid h_{\bar{L}}$. Q. E. D.

References

[1] F. GERTH III, *Number fields with prescribed l-class groups*, Proc. Amer. Math. Soc., 49 (1975), 284–288.

[2] R. GOLD, *Genera in abelian extensions*, Proc. Amer. Math. Soc., 47 (1975), 25–28.

[3] G. GRAS, *Sur les l-classes d'ideaux dans les extensions cycliques relative de degre premier l*, Ann. Inst. Fourier, Grenoble 23, 3 (1973), 1–48, 4 (1973), 1–44.

[4] F. HALTER-KOCH, *Ein Satz über die Geschlechter relativzyklischer Zahlkörper von Primzahlgrad und seine Anwendug auf biquadratisch-bizyklische Körper*, J. Number Theory, 4 (1972), 144–156.

[5] E. INABA, *Über die Struktur der l-klassengruppe zyklischer Zahlkörper von Primzahlgrad l*, J. Fac. Sci. Univ. Tokyo Sect I, 4 (1940), 61–115.
[6] P. ROQUETTE, *On class field towers*, Proc. instr. conf. at Brighton (Algebraic Number Theory), (1967), 231–249.