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

By
Teruo TAKEUCHI*

(Received November 2, 1977)

1. Introduction

Let p be a rational odd prime and let k be an algebraic number field of finite degree, whose class number h_k is prime to p. Let K/k be a cyclic extension of degree p, let $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ be the prime ideals of k, ramified in K, and assume $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ are prime to p. If $\sharp(I(\mathfrak{p}_i)/H(\mathfrak{p}_i)=p$ for $i=1, \cdots\cdots, t$, then we can study the p-class group M_K of K analogously to the case $k=\boldsymbol{Q}$, where $I(\mathfrak{p}_i)$ denotes the ideal group of k, prime to $\mathfrak{p}_i$ $P_{\mathfrak{p}_i}$, the ray mod $\mathfrak{p}_i$ and $H(\mathfrak{p}_i)=I(\mathfrak{p}_i)^p P_{\mathfrak{p}_i}$. From Lemma 1 it follows that if k does not contain the primitive p-th roots of unity, then there are infinitely many such $\mathfrak{p}_i$'s which satisfy some conditions each other.

In the present paper we treat the existence of cyclic extensions K/k's of degree p and t-tuples of prime ideals $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$, which have some properties. Unless otherwise stated the notation of [4] will be taken over. In particular $\mathfrak{o}$ denotes the maximal order of the cyclotomic field of p-th roots of unity and $\mathfrak{p}$ denotes the prime divisor of p in $\mathfrak{o}$. Let K/k be a cyclic extension of degree p, in which only $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ are ramified. Then for $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ the structue of p-class group M_K, in general, is not determined uniquely. In fact we can prove the following theorem.

THEOREM 1. *Let k be an algebaic number field of finite degree such that $p \nmid h_k$ and $k \not\ni \xi_p$, where ξ_p denotes a primitive p-th root of unity. Then for any given natural number t ($\geqq 3$), there exist infinitely many t-tuples of prime ideals $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ of k, which satisfy the following conditions:*

there are cyclic extensions K'/k and K''/k in which only $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ are ramified, such that rank $M_{K'}=t-1$ and rank $M_{K''} \geqq 2t-3-u$, where u denotes the p-rank of unit group E_k of k.

Let $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ be prime ideals of k such that $\sharp(I(\mathfrak{p}_i)/H(\mathfrak{p}_i))=p$ for $i=1, \cdots\cdots, t$, let K/k be a cyclic extension of degree p, in which only $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ are ramified and let L be the p-genus field (i.e. p-part of the genus field) with respect to K/k. In the case $k=\boldsymbol{Q}$,

* Niigata University

A. Fröhlich [1] determined conditions that $p \nmid h_L$ for $t \leqq 3$, and showed $p|h_L$ for $t \leqq 4$. Next we shall state for $t \leqq 3$, a condition that $p \nmid h_L$ as conditions on cyclic extensions K/k's contained in L. If $p \nmid h_L$, then for any cyclic extension K/k contained in L, we have $M_K \approx (\mathfrak{o}/\mathfrak{p})^{s-1}$, where s denotes the number of prime ideals of k, ramified in K. In the case $t \leqq 3$, the inverse is also true. That is, we have following theorem.

THEOREM 2. *Let k be an algebraic number field of finite degree such that $p \nmid h_k$. Let $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ prime ideals of k such that that $\#(I(\mathfrak{p}_i)/H(\mathfrak{p}_i))=p$ for $i=1, \cdots\cdots, t$. Moreover let the notation be as above. Assume $t \leqq 3$. Then a necessary and sufficient condition that $p \nmid h_L$ is that for any cyclic extension K/k contained in L, $M_k \approx (\mathfrak{o}/\mathfrak{p})^{s-1}$, where s denotes the number of prime ideals of k, ramified in K.*

From the above theorem and the proof of Lemma 1, it follows that for $t=2, 3$, there exits infinitely many t-tuples of prime ideals $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ such that $p|h_L$ and for $t=2$ there exist infinitely many couples of prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$ such that $p \nmid h_L$. And moreover if $k \not\ni \xi_p$, then we see that for $t=3$ there exist infinitely many triples of prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ such that $p \nmid h_L$.

For $t=4$ the condition $M_K \approx (\mathfrak{o}/\mathfrak{p})^{s-1}$ is a necessary condition that $p \nmid h_L$, but is not a sufficient condition. Finally we shall show the following theorem.

THEOREM 3. *Let k be an algebraic number field of finite degree such that $p \nmid h_k$, $\xi_p \notin k$ and p-rank $E_k \leqq 1$. Then there exist infinitely many 4-tuples of prime ideals $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_4$ with $\#(I(\mathfrak{p}_i)/H(\mathfrak{p}_i))=p$ for $i=1, \cdots\cdots, 4$, which satisfy the following conditions:*

Let L be the class field corresponding to $I(\mathfrak{p}_1 \cdots\cdots \mathfrak{p}_4)/H(\mathfrak{p}_1 \cdots\cdots \mathfrak{p}_4)$.

Then (i) for any cyclic extension K/k contained in L, $M_K \approx (\mathfrak{o}/\mathfrak{p})^{s-1}$, where s is the number of prime ideals of k, ramified in K.

(ii) $p|h_L$.

2. Preliminaries

Let p be an odd rational prime and let k be an algebraic number field of finite degree, whose class number h_k is prime to p. For an ideal $\mathfrak{o}$ of k let $I(\mathfrak{a})$ denote the ideal group of k, prime to $\mathfrak{a}$, $P_\mathfrak{a}$ the ray mod $\mathfrak{a}$ and $H(\mathfrak{a})=I(\mathfrak{a})^p P_\mathfrak{a}$. Let $\mathfrak{p}_i$ be a prime ideal of k. Then the p-Sylow subgroup of $I(\mathfrak{p}_i)/P_{\mathfrak{p}_i}$ is cyclic since $p \nmid h_k$. So $I(\mathfrak{p}_i)/H(\mathfrak{p}_i)$ is cyclic of degree p or trivial.

LEMMA 1. *Let k be as above and assume $k \not\ni \xi_p$, where ξ_p denotes a primitive p-th root of unity. Let $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ be prime ideals of k such that $\#(I(\mathfrak{p}_i)/H(\mathfrak{p}_i))=p$ for $i=1, \cdots\cdots, t$. For $i=1, \cdots\cdots, t$ let α_i be an element of $I(\mathfrak{p}_i)/H(\mathfrak{p}_i)$ and n_i be a natural number such that $1 \leqq n_i \leqq p$. Then there exist infinitely many prime ideals $\mathfrak{p}_{t+1}$'s, which satisfy the following conditions:*

$$\mathfrak{p}_{t+1} \equiv \alpha_i \quad \mathit{mod}\ H(\mathfrak{p}_i) \ \mathit{for}\ i=1, \cdots\cdots, t,$$

$$\mathfrak{p}_i \equiv \alpha^{n_i} \ \mathit{mod}\ H(\mathfrak{p}_{t+1}) \quad \mathit{for}\ i=1, \cdots\cdots, t,$$

$$\#(I(\mathfrak{p}_{t+1})/H(\mathfrak{p}_{t+1}))=p,$$

where α is a generator of $I(\mathfrak{p}_{t+1})/H(\mathfrak{p}_{t+1})$.

PROOF. Let K_i be the class field corresponding to $I(\mathfrak{p}_i)/H(\mathfrak{p}_i)$. Then K_i/k is the unique cyclic extension of degree p, in which only $\mathfrak{p}_i$ is ramified. Hence $K_1, \cdots\cdots, K_t$ are linearly disjoint over k, so $\overline{K}=K_1\cdots\cdots K_t$ is an abelian extension of degree p^t over k. Put

$$\sigma_i=\left(\frac{K_i/k}{\alpha_i}\right) : \text{Artin symbol},$$

$$\sigma=\sigma_1\times\cdots\cdots\times\sigma_t\in Gal\,(\overline{K}/k),$$

$$K_0=k_0(\sqrt[p]{E_k}),$$

where E_k is the unit group of k and k_0/k is the ray class field mod $p\cdot p_\infty$. As E_k is finite rank, K_0/k is finite extension. Moreover since $k_0\ni\xi_p$, K_0/k_0 is an abelian extension and K_0/k is a Galois extension. First we consider the case $n_1\neq p$. Let m be a natural number such that $n_1\cdot m\equiv 1$ *mod* p. Put

$$M_1=k(\sqrt[p]{\mathfrak{p}_1{}^h}),$$

$$M_i=k(\sqrt[p]{(\mathfrak{p}_1{}^{mn_i}\mathfrak{p}_i{}^{-1})^h}) \qquad \text{for } i=2,\cdots\cdots, t, \text{ where } h=h_k,$$

$$L=M_1\cdots\cdots M_t K_0,$$

$$M=M_2\cdots\cdots M_t K_0.$$

Then L/M is a cyclic extension of degree p. As $k\not\ni\xi_p$, L and $\overline{K}$ are liearly disjoint over k. Hence we can chose an element ρ from $Gal\,(N/k)$ such that $\rho=\sigma\times\tau\in Gal\,(N/k)$, where τ is a generator of $Gal\,(N/M)$ and $N=\overline{K}L$. Then from Čĕbotarev Density Theorem we see that there exist infinitely many prime ideals $\mathfrak{p}_{t+1}$'s unramified in N, such that

$$\rho=\left(\frac{N/k}{\mathfrak{P}_{t+1}}\right) : \text{Frobenius symbol},$$

where $\mathfrak{P}_{t+1}$ is a prime divisor of $\mathfrak{p}_{t+1}$ in N, and $\mathfrak{p}_{t+1}$ is prime to p. Then $\mathfrak{p}_{t+1}$ is completely decomposed in M, in partcular, in k_0. Hence $\mathfrak{p}_{t+1}\in P_{p\cdot p_\infty}$. And for any $\varepsilon\in E_k$, $\mathfrak{p}_{t+1}$ is completely decomposed in $k(\sqrt[p]{\varepsilon})$. So the congruence equation $X^p\equiv\varepsilon$ mod $\mathfrak{p}_{t+1}$ has integer solution in k. Therefore we see $\sharp(E_k k_{\mathfrak{p}_{t+1}} k(\mathfrak{p}_{t+1})^p/k_{\mathfrak{p}_{t+1}} k(\mathfrak{p}_{t+1})^p)=1$, where $k(\mathfrak{p}_{t+1})$ denotes the subgroup of k^*, prime to $\mathfrak{p}_{t+1}$, and $k_{\mathfrak{p}_{t+1}}=\{\alpha\in k^* \mid \alpha\equiv 1 \textit{ mod } \mathfrak{p}_{t+1}\}$. So using the isomorphism $I(\mathfrak{p}_{t+1})/H(\mathfrak{p}_{t+1})\approx k(\mathfrak{p}_{t+1})/E_k k_{\mathfrak{p}_{t+1}} k(\mathfrak{p}_{t+1})^p$, we have $\sharp(I(\mathfrak{p}_{t+1}/H(\mathfrak{p}_{t+1}))=\sharp(k(\mathfrak{p}_{t+1})/k_{\mathfrak{p}_{t+1}} k(\mathfrak{p}_{t+1})^p)=p$. Moreover, as $\mathfrak{p}_{t+1}$ is completely decomposed in $M_2\cdots\cdots M_t$, the congruence equations

$$X^p\equiv(\mathfrak{p}_1{}^{mn_i}\mathfrak{p}_i{}^{-1})^h \qquad \textit{mod } \mathfrak{p}_{t+1}$$

have integer solutions in k. Hence for $i=2,\cdots\cdots, t$,

$$\mathfrak{p}_1{}^{mn_i}\equiv\mathfrak{p}_i \qquad \textit{mod } H(\mathfrak{p}_{t+1}).$$

Now $\mathfrak{p}_1{}^m$ generates $I(\mathfrak{p}_{t+1})/H(\mathfrak{p}_{t+1})$. In fact if $\mathfrak{p}_1{}^m\in H(\mathfrak{p}_{t+1})$, then the congruence equation

$X^p \equiv \mathfrak{p}_1{}^{mh}$ *mod* $\mathfrak{p}_{t+1}$ has integer solution in k. Thus $\mathfrak{p}_{t+1}$ is completely decomposed in M_1, hence in L, which is a contradiction. So, if we put $\alpha_1{}^m$, then

$$\mathfrak{p}_i \equiv \alpha^{n_i} \quad mod\ H(\mathfrak{p}_{t+1}) \text{ for } i=1, \cdots\cdots t.$$

On the other hand, as the restriction of ρ to K_i is σ_i,

$$\left(\frac{K_i/k}{\mathfrak{p}_{t+1}}\right) = \left(\frac{K_i/k}{\alpha_i}\right),$$

so we have $\mathfrak{p}_{t+1} \equiv \alpha_i$ *mod* $H(\mathfrak{p}_i)$ for $i=1, \cdots\cdots, t$.

In the case $n_1 = \cdots\cdots = n_t = p$ the proof is analogous to the above. Q.E.D.

Let K/k be a cyclic extension of degree p, let $\mathfrak{p}_1, \cdots\cdots \mathfrak{p}_t$ be the prime ideals of k, ramified in K, and assume $\mathfrak{p}_1, \cdots\cdots \mathfrak{p}_t$ are prime to p. Then $N\mathfrak{p}_i \equiv 1$ *mod* p for $i=1, \cdots\cdots, t$. From the proof of Lemma 1, we see that the natural homorphism:

$$(1) \qquad I(\mathfrak{p}_1 \cdots\cdots \mathfrak{p}_t)/H(\mathfrak{p}_1 \cdots\cdots \mathfrak{p}_t) \to (I(\mathfrak{p}_1)/H(\mathfrak{p}_1)) \times \cdots \times (I(\mathfrak{p}_t)/H(\mathfrak{p}_t))$$

is surjective. On the other hand $\sharp(I(\mathfrak{p}_1 \cdots\cdots {}_t)/H(\mathfrak{p}_1 \cdots\cdots \mathfrak{p}_t)) \leq p^t$. Assume $\sharp(I(\mathfrak{p}_i)/H(\mathfrak{p}_i)) = p$ for $i=1, \cdots\cdots, t$, then the natural homorphism (1) is an isomorphism. Hence in this case we have $[E_k : E_k \cap N_{K/k}K^*] = 1$ since the p-genus field with respect to K/k corresponds to $I(\mathfrak{p}_1 \cdots\cdots {}_t)/H(\mathfrak{p}_1 \cdots\cdots \mathfrak{p}_t)$. Thus with the notation of [4 §2] we have $r = t-1$ and $\widehat{X} = G^t$. Let H be the congruence ideal group corresponding to K/k and let H' be the subgroup of $(I(\mathfrak{p}_1)/H(\mathfrak{p}_1)) \times \cdots\cdots \times (I(\mathfrak{p}_t)/H(\mathfrak{p}_t))$, corresponding to H by the isomorphism (1). Then for $i \neq j$,

$$(2) \qquad \left(\frac{\alpha_i : K/k}{\mathfrak{p}_j}\right) = 1 \qquad \text{if and only if } \mathfrak{p}_i \in H(\mathfrak{p}_j)$$

and

$$(3) \qquad \left(\frac{\alpha_i : K/k}{\mathfrak{p}_i}\right) = 1 \qquad \text{if and only if } (\mathfrak{p}_i, \cdots\cdots, \mathfrak{p}_i, \overset{\overset{i}{\vee}}{1}, \mathfrak{p}_i, \cdots\cdots, \mathfrak{p}_i) \in H',$$

where $(\alpha_i) = \mathfrak{p}_i{}^h$. Let $p^w = [E_k \cap N_{K/k}K^* : N_{K/k}E_K]$, then $w \leq p$-*rank* E_k and $cl_p(\mathfrak{p}_1), \cdots\cdots$, $cl_p(\mathfrak{p}_t)$ generate the subgroup of $M_{K(\sigma-1)}$, of rank $t-1-w$, where $\mathfrak{p}_i$ is the prime divisor of $\mathfrak{p}_i$, in K and σ is a generator of $Gal(K/k)$. Put

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

then

$$(4) \qquad t-1 \geq rank(a_{ij}) + w \geq v \geq rank\ (a_{ij}),$$

where $\sharp\,\widehat{(\chi_{K/k}}(M_{K(\sigma-1)})) = p^v$. Hence, if *rank* $(a_{ij}) = t-1$, then $w=0$ and $v=t-1$. So M_K is an elementary abelian group of rank $t-1$ by [4 Theorem 2].

3. Proof of Theorem 1

Proof of theorem 1. From Lemma 1 we see that there exist infinitely many t-tuples of prime ideals $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ which satisfy the following conditions:

$$\sharp(I(\mathfrak{p}_i)/H(\mathfrak{p}_i))=p \qquad \text{for } i=1, \cdots\cdots, t,$$

$$\mathfrak{p}_1 \in H(\mathfrak{p}_2 \cdots\cdots \mathfrak{p}_t),$$

$$\mathfrak{p}_2 \notin H(\mathfrak{p}_1),\ \mathfrak{p}_2 \in H(\mathfrak{p}_3 \cdots\cdots \mathfrak{p}_t),$$

$$\mathfrak{p}_3 \notin H(\mathfrak{p}_1),\ \mathfrak{p}_3 \notin H(\mathfrak{p}_2),\ \mathfrak{p}_3 \in H(\mathfrak{p}_3 \cdots\cdots \mathfrak{p}_t),$$

$$\mathfrak{p}_i \mathfrak{p}_3^{-1} \in H(\mathfrak{p}_1 \mathfrak{p}_2),\ \mathfrak{p}_i \in H(\mathfrak{p}_3 \cdots\cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots\cdots \mathfrak{p}_t) \qquad \text{for } i=4, \cdots\cdots, t.$$

Let K/k be a cyclic extension of degree p, in which only $\mathfrak{p}_1, \cdots\cdots, \mathfrak{p}_t$ are ramified. Then by (2) and (3) we have

$$\left(\left(\frac{\alpha_i : K/k}{\mathfrak{p}_j}\right)\right)_{i,j=1,\cdots\cdots t} = \begin{pmatrix} 1, & 1, & 1, & 1, & 1, & \cdots\cdots 1 \\ *, & *, & 1, & 1, & 1, & \cdots\cdots 1 \\ *, & *, & ?, & 1, & 1, & \cdots\cdots 1 \\ *, & *, & 1, & ?, & 1, & \cdots\cdots 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \cdots\cdots \\ *, & *, & 1, & 1, & 1, & \cdots\cdots ? \end{pmatrix},$$

where $(\alpha_i)=\mathfrak{p}_i^h$ and * denotes non-identity. First let $K=K'$ be such that $(\mathfrak{p}_3, \mathfrak{p}_3\ 1, \mathfrak{p}_3, \cdots\cdots, \mathfrak{p}_3) \notin H'$ (such an extension certainly exists). Then, as $(\mathfrak{p}_3, \mathfrak{p}_3, 1, \mathfrak{p}_3, \cdots\cdots \mathfrak{p}_3) \equiv (\mathfrak{p}_i, \cdots\cdots \mathfrak{p}_i, \overset{i}{\check{1}}, \mathfrak{p}_i, \cdots\cdots, \mathfrak{p}_i)$ *mod* $H(\mathfrak{p}) \times \cdots\cdots \times H(\mathfrak{p}_t)$ for $i=4, \cdots\cdots, t$, we have $\mathit{rank}\left(\left(\frac{\alpha_i : K'/k}{\mathfrak{p}_j}\right)\right)=t-1$ by (3). Thus we obtain $M_{K'} \approx (\mathfrak{o}/\mathfrak{p})^{t-1}$ from [4 Theorem 2]. Next let $K=K''$ be such that $(\mathfrak{p}_3, \mathfrak{p}_3, 1, \mathfrak{p}_3, \cdots\cdots, \mathfrak{p}_3) \in H'$ (such an extension also exist). Then we have similarly rank $\left(\left(\frac{\alpha_i : K''/k}{\mathfrak{p}_j}\right)\right)=1$. So from [4 Theorem 2] and (4), we see rank $M_{K''} \geqq 2t-3-u$.

Q.E.D.

4. Proof of Theorem 2

Lemma 2. *Let A be an abelian group of type $(p, p, p,)$ and let N be a cyclic group of order p. Let $1 \rightarrow N \rightarrow G \rightarrow A \rightarrow 1$ be a non abel central extension of N by A. Then the order of the center of G is p^2.*

Proof. Easy.

Proof of theorem 2. We prove only the sufficiency in the case $t=3$. Assume that for any cyclic extension K/k contained in L, $M_K \approx (\mathfrak{o}/\mathfrak{p})^{s-1}$. Furthermore suppose that $p \mid h_L$. Then $p \mid z_{L/K}$ since by [2 Satz 2] we have $h_L \equiv z_{L/K}$ *mod* p, where $z_{L/K}$ denotes the central class number with respect to L/K. So there exists an unramified cyclic extension L_1/L of degree p such that L_1/k is a Galois extension and *Gal* (L_1/L) is contained in the center of $Gal\,(L_1/L)$. Put $A=Gal\,(L/K)$, $N=Gal\,(L_1/L)$ and $G=Gal\,(L_1/k)$. Let Z be the center of G and let E be the intermediate field corresponding to Z. Then $E\subset L$ and E/k is of degree p^2 by Lemma 2. And at least two prime ideals are ramified. We first consider the case that only $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are ramified in E. Then $E=K_1K_2$ and the inertia group of a prime divisor of $\mathfrak{p}_3$ in L_1 is cyclic of oder p and contained in Z, where K_i denotes the class field corresponding to $I(\mathfrak{p}_i)/H(\mathfrak{p}_i)$. So the inertia groups of all prime divisors of $\mathfrak{p}_3$ in L_1 coincide. Let F be the inertia field of the prime divisors of $\mathfrak{p}_3$ in L_1. Then F/E is an unramified cyclic extension of degree p. Hence $p\,|\,h_E$, so for any cyclic extension K/k contained in E, $\#(M_K)\geqq p^2>p^{s-1}$, which cotradicts the assumption. Next we consider the case that $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are ramified in E. Let K be a cyclic extension contained in E, in which $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are ramified. Since E/k is an abelian extension of type (p, p) and $p+1>3$, such an extension certainly exists. Then L_1/K is an unramified Galois extension of degree p^3. Moreover, since E/K is cyclic of degree p and z is the center of G, we see that L_1/K is abelian. Hence we have $\#(M_K)\geqq p^3$, which contradicts the assumption that $M_K\approx(\mathfrak{p}/\mathfrak{p})^{s-1}=(\mathfrak{o}/\mathfrak{p})^2$. Thus we have $p\nmid h_L$. Q.E.D.

REMARK. If $t=1$, then $L=K_1$ and $p\nmid h_L$. If $t=2$, then there exist infinitely many L's with $p\,|\,h_L$ and L's with $p\nmid h_L$. In fact, noting the proof of Lemma 1, we see that there are infinitely many $\mathfrak{p}_i$'s such that $\#(I(\mathfrak{p}_i)/H(\mathfrak{p}_i))=p$. Let $\mathfrak{p}_1$ be a prime ideal of k such that $\#(I(\mathfrak{p}_1)/H(\mathfrak{p}_1))=p$ and let K_1/k be the cyclic extension of degree p, in which only $\mathfrak{p}_1$ is ramified. Let $\mathfrak{p}_2$ be a prime ideal of k such that $\#(I(\mathfrak{p}_2)/H(\mathfrak{p}_2))=p$ and $\mathfrak{p}_2$ is not decomposed in K_1. Then for L corresponding to these $\mathfrak{p}_1$ and $\mathfrak{p}_2$, we have $p\nmid h_L$. Next put $N=k_0K_1(\sqrt[p]{E_{K_1}})$, where k_0 is the ray class field of k mod $p\cdot p_\infty$, and let $\mathfrak{P}_2'$ be a prime ideal of k such that $\mathfrak{p}_2'$ is completely decomposed in N. Then $\#(I(\mathfrak{p}_2')/H(\mathfrak{p}_2'))=p$ and $\#(I(\mathfrak{P}_2'{}_i)/H(\mathfrak{P}_2'{}_i))=p$ for $i=1, \cdots\cdots, p$, where $\mathfrak{P}_2'{}_1,\cdots\cdots\mathfrak{P}_2'{}_p$ are the prime divisors of $\mathfrak{p}_2'$ in K_1. Let K_2'/k be the cyclic extension of degree p, in which only $\mathfrak{p}_2'$ is ramified. Put $L'=K_1K_2'$. Then L'/K_1 is a cyclic extension of degree p, in which $\mathfrak{P}_2'{}_1,\cdots\cdots, \mathfrak{P}_2'{}_p$ are ramified. So $rank\ M_{L'}\geqq p-1$. Thus for $t=2$ there exist infinitely many L's such that $p\,|\,h_L$. Therefore for $t=3$, there also exist infinitely many L's such that $p\,|\,h_L$. Moreover if $k\not\ni\xi_p$, then for t$=3$ there exist infinitely many L's such that $p\nmid h_L$. In fact, in this case we see from Lemma 1 that there exist infinitely many triples of prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ of k, which satisfy the following conditions:

$$\#(I(\mathfrak{p}_i)/H(\mathfrak{p}_i))=p \qquad \text{for } i=1, 2, 3,$$

$$\mathfrak{p}_1\notin H(\mathfrak{p}_2),\ \mathfrak{p}_1\notin H(\mathfrak{p}_3),$$

$$\mathfrak{p}_2\notin H(\mathfrak{p}_1),$$

$$\mathfrak{p}_3\in H(\mathfrak{p}_1),\ \mathfrak{p}_3\notin H(\mathfrak{p}_2).$$

Then for L corresponding to these $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, we have $p\nmid h_L$ byTheorem 2.

5. Proof of Theorem 3

LEMMA 3. *Let a, b, c, d be non-zero elements of $\boldsymbol{Z}/p\boldsymbol{Z}$ and let n be a natural number. If*

$$rank\begin{pmatrix} -a-b, & 0\ , & a\ , & b \\ c\ , & -nb-c, & 0\ , & nb \\ c\ , & d\ , & -c-d, & 0 \\ 0\ , & d\ , & a\ , & -d-a \end{pmatrix}=2,$$

then $1+4n$ *is quadratic residue mod* p.

PROOF. Easy.

PROOF OF THEOREM 3. Let n be a natural number such that $1+4n$ is non quadratic reisdue mod p. By Lemma 1 there exist infinitely many 4-tuples of prime ideals $\mathfrak{p}_1,\cdots\cdots\mathfrak{p}_4$ of k, which satisfy the following conditions: $\sharp(I(\mathfrak{p}_i)/H(\mathfrak{p}_i))=p$ for $i=1,\cdots\cdots, 4$,

$$\begin{array}{llll} & \mathfrak{p}_1\in H(\mathfrak{p}_2), & \mathfrak{p}_1\notin H(\mathfrak{p}_3), & \mathfrak{p}_1\notin H(\mathfrak{p}_4), \\ \mathfrak{p}_2\notin H(\mathfrak{p}_1), & & \mathfrak{p}_2\notin H(\mathfrak{p}_3), & \mathfrak{p}_1{}^n\mathfrak{p}_2{}^{-1}\in H(\mathfrak{p}_4), \\ \mathfrak{p}_2\mathfrak{p}_3{}^{-1}\in H(\mathfrak{p}_1), & \mathfrak{p}_3\notin H(\mathfrak{p}_2), & & \mathfrak{p}_3\in H(\mathfrak{p}_4) \\ \mathfrak{p}_4\in H(\mathfrak{p}_1), & \mathfrak{p}_3\mathfrak{p}_4{}^{-1}\in H(\mathfrak{p}_2), & \mathfrak{p}_1\mathfrak{p}_4{}^{-1}\in H(\mathfrak{p}_3). & \end{array}$$

Now we shall show that these $\mathfrak{p}_1,\cdots\cdots\mathfrak{p}_4$ satisfy the conditions of our theorem. (i) If $s\leqq 3$, it is easy to see that $M_K\approx(\mathfrak{o}/\mathfrak{p})^{s-1}$. Let $s=4$ and let

$$\left(\left(\frac{\alpha_i : K/k}{\mathfrak{p}_j}\right)\right)_{i,j,=1,\cdots,4}=(\sigma^{a_{ij}}),\ a_{ij}\in\boldsymbol{Z}/p\boldsymbol{Z},$$

where σ is a generator of $Gal\ (K/k)$. Then the matrix (a_{ij}) is of the type of Lemma 3 As $1+4n$ is non quadratic residue mod p, we have $rank\ (a_{ij})=3$ by Lemma 3. Thus $M_K\approx(\mathfrak{o}/\mathfrak{p})^3$. (ii) We first note that for an arbitrary Galois extension L/k,

$$Gal\ (L_1/L_0)\approx\frac{(k^*\cap N_{L/k}J_L)/N_{L/k}L^*}{(k^*\cap(N_{L/k}L^*\cdot N_{L/k}U_L))/N_{L/k}L^*}\ ,$$

$$(k^*\cap N_{L/k}J_L)/N_{L/k}L^*\approx H^{-3}(Gal\ (L/k),\ Z)/F(L/K),$$

$$(k^*\cap(N_{L/k}L^*\cdot N_{L/k}U_L))/N_{L/k}L^*\approx(E_k\cap N_{L/k}U_L)/(E_k\cap N_{L/k}L^*),$$

where L_0 : the genus field with respect to L/k, L_1: the central class field with respect to L/k, J_L: the idele group of L, U_L: the unit idele group of L, $F(L/K)$: the subgroup of $H^{-3}(Gal(L/k),\ Z)$ generated by the canonical injection of $H^{-3}(G_{\mathfrak{p}_i}(L/k),\ Z)$ to $H^{-3}(Gal(L/k),\ Z)$, where $G_{\mathfrak{p}_i}(L/k)$ is a decomposition group of any one of the prime divisors in L of a prime $\mathfrak{p}_i$ of k and $\mathfrak{p}_i$ runs over all primes of k ramified in L (cf. [3]). Now let L/k be as in our theorem. Then from

$$\#(H^{-3}(Gal(L/k), Z) = p^{4(4-1)/2} = p^6,$$

$$\#(F(L/k)) \leqq p^4,$$

$$\#((E_k \cap N_{L/k} U_L)/(E_k \cap N_{L/k} L^*)) \leqq p,$$

we see $p \mid h_{L_0}$. Thus we have $p \mid h_L$. Q.E.D.

References

[1] A. FRÖHLICH. *On the absolute class-group of abelian field.* J. London Math. Soc., 29 (1954), 211–217.
[2] Y. FURUTA. *Über das Geschlecht und die Klassenzahl eines Relativ-Galoisschen Zahlkorpers von Primzahlpotenzgrade.* Nagoya Math. J., 37 (1970), 197–200.
[3] Y. FURUTA. *On class field towers and the rank of ideal class groups.* Nagoya Math. J., 48 (1972), 147–157.
[4] T. TAKEUCHI. *On the structure of p-class groups of certain number field.* Sci. Rep. Niigata Univ. Series A, 14 (1977), 25–33.