Tôhoku Math. Journ.
31 (1979), 301-307.

NOTES ON THE CLASS FIELD TOWERS OF CYCLIC FIELDS OF DEGREE l

TERUO TAKEUCHI

(Received July 31, 1978, revised October 5, 1978)

1. Introduction. Let l be a rational odd prime. Let k be an algebraic number field of finite degree, K/k be a cyclic extension of degree l, and $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ denote the prime ideals in k ramified in K. Then, as is well-known, the genus number of K with respect to k is given by $h(k)l^{t-1}/(E_k\colon E_k \cap N_{K/k}K^{\times})$, where $h(k)$ denotes the class number of k and E_k denotes the group of units in k. (See, for instance, [1].) Though the genus number of K/k is determined uniquely by $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$, this expression does not give explicitly the relations between the genus number of K/k and the prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$.

Let p_i denote the rational prime contained in $\mathfrak{p}_i$ and assume $p_i \equiv 1 \bmod l$ for $i = 1, \cdots, t$. In this note, we shall first show that the genus number of K/k is calculated by the subgroup of $\mathrm{Gal}\,(k(\zeta, E_k^{1/l})/k)$ which is generated by the decomposition groups of prime divisors of $\mathfrak{p}_i$ in $k(\zeta, E_k^{1/l})$, where ζ is a primitive l-th root of unity.

Next, we shall apply the above result together with the Čebotarev density theorem to the class field tower problem to show the existence of fields which satisfy some properties.

Let $k/\boldsymbol{Q}$ be a cyclic extension of degree l and $p_1, \cdots, p_t$ denote the primes in $\boldsymbol{Q}$ ramified in k. It is well-known that the l-class field tower of k is infinite if t is sufficiently large. (Cf. [5].) Moreover, we know by a result of Y. Furuta [2] that if $p_1, \cdots, p_t$ are prime to l and $8 \leqq t$, then the l-class field tower of k is infinite. On the other hand, if $t = 1$, then $l \nmid h(k)$ so the l-class field tower of k is finite. In this note, we consider the case when $t = 2$ and obtain the following theorems.

THEOREM 1. *Let l and p_1 be odd primes with $13 \leqq l$ and $p_1 \equiv 1 \bmod l$. Then there exist infinitely many primes p_2 which satisfy the following conditions*:

(i) $p_2 \equiv 1 \bmod l$,

(ii) *the l-class field tower of k is infinite for every cyclic extension $k/\boldsymbol{Q}$ of degree l in which only p_1 and p_2 are ramified.*

THEOREM 2. *Let l be an odd prime and p_1 be an odd prime with*

$p_1 \equiv 1 \bmod \boldsymbol{l}$. Let $k_1/\boldsymbol{Q}$ be the cyclic extension of degree $\boldsymbol{l}$ in which only p_1 is ramified. Assume that $4(2+\boldsymbol{l}) \leqq h(k_1)$, where $h(k_1)$ is the class number of k_1. Then there exist infinitely many primes p_2 which satisfy the following conditions:

(i) $p_2 \equiv 1 \bmod \boldsymbol{l}$,

(ii) *the $\boldsymbol{l}$-class field tower of k is finite but the class field tower of k is infinite for every cyclic extension $k/\boldsymbol{Q}$ of degree $\boldsymbol{l}$ in which only p_1 and p_2 are ramified.*

2. The genus numbers of cyclic extensions. Let l be a rational odd prime. Let k be an algebraic number field of finite degree and let K be a cyclic extension of degree l over k. For an ideal $\mathfrak{a}$ in k, let $I(\mathfrak{a})$ denote the group of ideals in k prime to $\mathfrak{a}$, $P(\mathfrak{a})$ the group of principal ideals in $I(\mathfrak{a})$, and $P_{\mathfrak{a}}$ the ray mod $\mathfrak{a}$. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ be the prime ideals in k ramified in K, and put $\mathfrak{c} = \mathfrak{p}_1 \cdots \mathfrak{p}_t$. Let $K^{(1)}$ be the Hilbert class field of K. Then, by definition, the genus field of K/k is the maximal abelian extension of k included in $K^{(1)}$. If $\mathfrak{c}$ is prime to $\boldsymbol{l}$, then the conductor of K/k is $\mathfrak{c}$. So the following lemma is easily proved.

LEMMA 1. *Let the notations be as above. Assume $\mathfrak{c}$ is prime to $\boldsymbol{l}$. Then the genus field of K over k is the class field corresponding to the ideal class group $I(\mathfrak{c})/P(\mathfrak{c})^l P_{\mathfrak{c}}$.*

Next, we shall study the order of $P(\mathfrak{c})/P(\mathfrak{c})^l P_{\mathfrak{c}}$. Let $P^*(k)$ be the set of prime ideals $\mathfrak{p}$ in k which are prime divisors of rational primes p with $p \equiv 1 \bmod \boldsymbol{l}$. Let ζ be a primitive $\boldsymbol{l}$-th root of unity and put $k_0 = k(\zeta)$. Let $\bar{k}_0 = k_0(E_k^{1/l})$, where E_k is the group of units in k. Then $\bar{k}_0$ is a Galois extension of k. Put $G = \mathrm{Gal}\,(\bar{k}_0/k_0)$ and $\bar{E} = E_k/E_k^l$. Then we see that

$$k_0^l E_k/k_0^l \approx \bar{E} = E_k/E_k^l \,.$$

Indeed, for ε in E_k if ε is in k_0^l, then ε is in k^l, therefore ε is in E_{k^l}. Hence we can develop the Kummer theory for $\bar{E}$, as follows. Let Z_l denote the group of $\boldsymbol{l}$-th roots of unity. We define $\langle\ ,\ \rangle : G \times \bar{E} \to Z_l$ by $\langle \sigma, \bar{\varepsilon} \rangle = \sigma(\varepsilon^{1/l})/\varepsilon^{1/l}$. Then $\langle\ ,\ \rangle$ is a non-degenerate bilinear form. Let $\mathfrak{c} = \mathfrak{p}_1 \cdots \mathfrak{p}_t$ be a product of distinct primes in $P^*(k)$ and let $\bar{E}(\mathfrak{c}) = (E_k \cap k(\mathfrak{c})^l k_{\mathfrak{c}})/E_{k^l}$, where $k(\mathfrak{c}) = \{\alpha \in k \mid (\alpha) \in P(\mathfrak{c})\}$ and $k_{\mathfrak{c}} = \{\alpha \in k \mid (\alpha) \in P_{\mathfrak{c}}\}$. Let $\bar{G}(\mathfrak{c})$ be the group of elements orthogonal to $\bar{E}(\mathfrak{c})$ with respect to $\langle\ ,\ \rangle$.

Let $\mathfrak{P}_i$ be a prime divisor of $\mathfrak{p}_i$ in $\bar{k}_0$ and let $G(\mathfrak{P}_i)$ be the decomposition group of $\mathfrak{P}_i$. Then $G(\mathfrak{P}_i) \subset G$, since $\mathfrak{p}_i$ is completely decomposed in k_0. Therefore, by the Kummer theory, $G(\mathfrak{P}_i)$ is a normal subgroup of

$\mathrm{Gal}(\bar{k}_0/k)$. Hence $G(\mathfrak{P}_i)$ depends only on $\mathfrak{p}_i$. Thus we may write $G(\mathfrak{p}_i)$ instead of $G(\mathfrak{P}_i)$.

Under the above notations, we have the following propositions.

PROPOSITION 1.

(i) *If $\mathfrak{p}$ is in $P^*(k)$, then $\bar{G}(\mathfrak{p}) = G(\mathfrak{p})$.*

(ii) *If $\mathfrak{c}_1$ and $\mathfrak{c}_2$ are relatively prime, then $\bar{G}(\mathfrak{c}_1\mathfrak{c}_2) = \bar{G}(\mathfrak{c}_1)\bar{G}(\mathfrak{c}_2)$.*

(iii) *If σ is an automorphism of $\bar{k}_0$ which induces an automorphism on k, then $\bar{G}(\sigma\mathfrak{c}) = \sigma\bar{G}(\mathfrak{c})\sigma^{-1}$.*

PROOF. (i) Let ε be a unit of k. If ε is in $k_\mathfrak{p}k(\mathfrak{p})^l$, then the equation $X^l \equiv \varepsilon \bmod \mathfrak{p}$ has an integral solution in k. Therefore $\mathfrak{p}$ is completely decomposed in $k(\varepsilon^{1/l})$, hence ε is in the decomposition field $\bar{k}_0^{G(\mathfrak{p})}$ of $\mathfrak{p}$. Conversely, if ε is in $\bar{k}_0^{G(\mathfrak{p})}$, then ε is in $k_\mathfrak{p}k(\mathfrak{p})^l$. For (ii) it suffices to note that $\bar{E}(\mathfrak{c}_1\mathfrak{c}_2) = \bar{E}(\mathfrak{c}_1)\bar{E}(\mathfrak{c}_2)$. (iii) It is easy to see that $\varepsilon \in \bar{E}(\sigma\mathfrak{c})$ if and only if $\sigma^{-1}\varepsilon \in \bar{E}(\mathfrak{c})$, and $\langle \tau, \varepsilon \rangle = 1$ if and only if $\langle \sigma^{-1}\tau\sigma, \sigma^{-1}\varepsilon \rangle = 1$. Thus the assertion follows immediately.

PROPOSITION 2. *Let $\mathfrak{c} = \mathfrak{p}_1 \cdots \mathfrak{p}_t$ be a product of distinct primes in $P^*(k)$. Then $\#(P(\mathfrak{c})/P(\mathfrak{c})^l P_\mathfrak{c}) = l^t/\#(\bar{G}(\mathfrak{c}))$.*

PROOF. We first note that

$$P(\mathfrak{c})/P(\mathfrak{c})^l P_\mathfrak{c} \approx k(\mathfrak{c})/E_k k(\mathfrak{c})^l k_\mathfrak{c} \,.$$

Since $k(\mathfrak{c})/k(\mathfrak{c})^l k_\mathfrak{c}$ is an elementary abelian group of rank t, we see that

$$\begin{aligned} \#(P(\mathfrak{c})/P(\mathfrak{c})^l P_\mathfrak{c}) &= \#(k(\mathfrak{c})/E_k k(\mathfrak{c})^l k_\mathfrak{c}) \\ &= \#(k(\mathfrak{c})/k(\mathfrak{c})^l k_\mathfrak{c})/\#(E_k k(\mathfrak{c})^l k_\mathfrak{c}/k(\mathfrak{c})^l k_\mathfrak{c}) \\ &= l^t/\#(E_k k(\mathfrak{c})^l k_\mathfrak{c}/k(\mathfrak{c})^l k_\mathfrak{c}) \,. \end{aligned}$$

On the other hand,

$$E_k k(\mathfrak{c})^l k_\mathfrak{c}/k(\mathfrak{c})^l k_\mathfrak{c} \approx E_k/(E_k \cap k(\mathfrak{c})^l k_\mathfrak{c})$$

and $\#(E_k/(E_k \cap k(\mathfrak{c})^l k_\mathfrak{c})) = l^r/\bar{E}(\mathfrak{c}) = \#(\bar{G}(\mathfrak{c}))$, where r is the l-rank of E_k. Hence we have $\#(P(\mathfrak{c})/P(\mathfrak{c})^l P_\mathfrak{c}) = l^t/\#(\bar{G}(\mathfrak{c}))$.

3. Proof of Theorem 1. Let l be an odd prime. Let p_1 be an odd prime with $p_1 \equiv 1 \bmod l$, and let $k_1/\boldsymbol{Q}$ be a cyclic extension of degree l in which only p_1 is ramified, where $\boldsymbol{Q}$ is the field of rationals. Let σ be a generator of $\mathrm{Gal}(k_1/\boldsymbol{Q})$ and let $\mathcal{O}$ be the maximal order of $\boldsymbol{Q}(\zeta)$, where ζ denotes a primitive l-th root of unity. Let E_1 be the group of units in k_1. Then E_1/E_1^l is a module over $\boldsymbol{Z}[\sigma]$. Moreover, since $N(E_1) = \{\pm 1\} \subset E_1$, E_1/E_1^l is also a module over $\boldsymbol{Z}[\sigma]/(1 + \sigma + \cdots + \sigma^{l-1})\boldsymbol{Z}[\sigma]$, where N denotes the norm map of k_1 to $\boldsymbol{Q}$. Therefore we can consider E_1/E_1^l as a module over $\mathcal{O}$ by $\sigma \mapsto \zeta$.

LEMMA 2. *E_1/E_1^l is $\mathcal{O}$-isomorphic to $\mathcal{O}/\mathfrak{l}^{l-1}$, where $\mathfrak{l}$ is the prime divisor of l in $\mathcal{O}$.*

PROOF. Since $l \nmid h(k_1)$, the cyclotomic units in k_1 generate E_1/E_1^l. On the other hand, the cyclotomic units in k_1 are conjugate to each other. Therefore E_1/E_1^l is a principal $\mathcal{O}$-module. Since the rank of E_1/E_1^l is $l-1$, we see that E_1/E_1^l is isomorphic to $\mathcal{O}/\mathfrak{l}^{l-1}$.

PROPOSITION 3. *Let p_1 be an odd prime with $p_1 \equiv 1 \bmod l$, and let r be a natural number with $1 \leqq r \leqq l-1$. Then there exist infinitely many odd primes p_2 which satisfy the following conditions*:

(i) $p_2 \equiv 1 \bmod l$,

(ii) *the genus number of k_1k_2 with respect to k_1 is $h(k_1)l^r$, where $k_2/\boldsymbol{Q}$ is the cyclic extension of degree l in which only p_2 is ramified.*

PROOF. Let $M = (\mathcal{O}\pi^s + \boldsymbol{Z}\pi^{s-2} + \boldsymbol{Z}\pi^{s-3} + \cdots + \boldsymbol{Z}\pi + \boldsymbol{Z})/\mathfrak{l}^{l-l}$ be a subgroup of $\mathcal{O}/\mathfrak{l}^{l-l}$, where $\pi = \zeta - 1$ and $s = l - 1 - r$. Then the maximal $\mathcal{O}$-submodule included in M is $\mathcal{O}\pi^s/\mathfrak{l}^{l-1}$, that is, $\bigcap_{i=0,1\cdots,l-1} \zeta^i M = \mathcal{O}\pi^s/\mathfrak{l}^{l-1}$. Indeed, let $\alpha = a_{s-2}\pi^{s-2} + \cdots + a_0$ be in $\bigcap \zeta^i M$, where $a_i \in \boldsymbol{Z}/l\boldsymbol{Z}$. Then $\zeta\alpha$ is in M. Hence we see that $a_{s-2} = 0$, since $\zeta\alpha = a_{s-2}\pi^{s-1} + (a_{s-2} + a_{s-3})\pi^{s-2} + \cdots + (a_1 + a_0)\pi + a_0$. Similarly, $\alpha = 0$ since $\zeta^j\alpha \in M$ for $j = 2, \cdots, l-1$.

Now, let E_M be the subgroup of E_1/E_1^l corresponding to M by the isomorphism in Lemma 2. Let $k_0 = k_1(\zeta)$, $\bar{k}_0 = k_0(E_1^{1/l})$, and $k_0(M) = k_0(E_M^{1|l})$. Then $\bar{k}_0/k_0(M)$ is a cyclic extension. Let τ be a generator of Gal$(\bar{k}_0/k_0(M))$. Then we see by the Čebotarev density theorem that there exist infinitely many prime ideals $\mathfrak{P}_2$ in $\bar{k}_0$, unramified over $\boldsymbol{Q}$, such that the Frobenius symbol $[\mathfrak{P}_2, \bar{k}_0/\boldsymbol{Q}] = \tau$. Let $p_2 = \mathfrak{P}_2 \cap \boldsymbol{Q}$ and $\mathfrak{p}_2 = \mathfrak{P}_2 \cap k_1$. Then $p_2 \equiv 1 \bmod l$, hence $\mathfrak{p}_2 \in P^*(k_1)$. Since k_1 is Galois over $\boldsymbol{Q}$, p_2 is completely decomposed in k_1. Let σ be a generator of Gal$(k_1/\boldsymbol{Q})$. Then $p_2 = \mathfrak{p}_2(\sigma\mathfrak{p}_2) \cdots (\sigma^{l-1}\mathfrak{p}_2)$ in k_1. Since the prime ideals in k_1 ramified in k_1k_2 are $\mathfrak{p}_2, (\sigma\mathfrak{p}_2), \cdots, (\sigma^{l-1}\mathfrak{p}_2)$, the genus field of k_1k_2/k_1 is the class field over k_1 corresponding to the ideal class group $I(p_2)/P(p_2)^l P_{p_2}$ of k_1. Hence the genus number is $\sharp(I(p_2)/P(p_2)^l P_{p_2})/l$. On the other hand, $G(\mathfrak{p}_2) = \text{Gal}(\bar{k}_0/k_0(M))$ and $G(\sigma^i\mathfrak{p}_2) = \text{Gal}(\bar{k}_0/k_0(\zeta^i M))$ for $i = 1, \cdots, l-1$. Therefore by Proposition 1 $\bar{G}(p_2) = G(\mathfrak{p}_2) \cdots G(\sigma^{l-1}\mathfrak{p}_2) = \text{Gal}(\bar{k}_0/k_0(\cap \zeta^i M))$. Hence $\sharp(\bar{G}(p_2)) = l^{l-1}/\sharp(\cap \zeta^i M) = l^{l-1-(l-1-s)} = l^{l-1-r}$. Thus by Proposition 2 we see that

$$\begin{aligned}\sharp(I(p_2)/P(p_2)^l P_{p_2}) &= h(k_1)\,\sharp(P(p_2)/P(p_2)^l P_{p_2}) \\ &= h(k_1)l^l/l^{l-1-r} = h(k_1)l^{r+1}\,.\end{aligned}$$

This proves the proposition.

PROOF OF THEOREM 1. Let p_2 be a prime satisfying the conditions in Proposition 3 for $r = \boldsymbol{l} - 1$. Let $k/\boldsymbol{Q}$ be a cyclic extension of degree $\boldsymbol{l}$ in which only p_1 and p_2 are ramified. Then k_1k_2/k is an unramified cyclic extension of degree $\boldsymbol{l}$. Let L be the maximal $\boldsymbol{l}$-extension of k_1 included in the genus field of k_1k_2/k_1. Then L is the class field over k_1 corresponding to $I(p_2)/I(p_2)^{\boldsymbol{l}}P_{p_2}$. Now, we apply [2, Theorem 3] to this field L. Since the $\boldsymbol{l}$-rank of $\mathrm{Gal}\,(L/k_1)$ is $\boldsymbol{l}$ and $13 \leqq \boldsymbol{l}$, we see that

$$2 + 2(\boldsymbol{l} - 1 + \boldsymbol{l} + 1)^{1/2} \leqq \boldsymbol{l}\text{-rank}\,(\mathrm{Gal}\,(L/k_1))\ .$$

Thus the $\boldsymbol{l}$-class field tower of L is infinite and the $\boldsymbol{l}$-class field tower of k is also infinite.

REMARK. Let p_2 be a prime satisfying the conditions in Proposition 3 for $r = 1$. Let σ be a generator of $\mathrm{Gal}\,(K/k_1)$, where $K = k_1k_2$. Then we can consider the $\boldsymbol{l}$-Sylow subgroup M_K of the ideal class group of K as a module over $\mathcal{O}$ by $\sigma \mapsto \zeta$. Since the $\boldsymbol{l}$-part of the genus number of K/k_1 is $\boldsymbol{l}$, M_K is, as is seen by [4 I, Theorem 1], $\mathcal{O}$-isomorphic to $\mathcal{O}/\mathfrak{l}^e$, where e is a natural number. Let τ be a generator of $\mathrm{Gal}\,(K/k_2)$. Then τ operates on M_K and hence on $\mathcal{O}/\mathfrak{l}^e$ as an automorphism. Since σ and τ commute, τ is an $\mathcal{O}$-automorphism. Moreover, $\mathcal{O}/\mathfrak{l}^e$ is a principal $\mathcal{O}$-module. Therefore τ is represented by a unit α in $\mathcal{O}/\mathfrak{l}^e$. Since $\tau^{\boldsymbol{l}} = 1$, α is of the following form; $\alpha = 1 + a_1\pi + \beta \bmod \mathfrak{l}^e$, where β is in $\mathfrak{l}^2$, a_1 is an integer with $0 \leqq a_1 \leqq \boldsymbol{l} - 1$, and $\pi = \zeta - 1$. Let j be a natural number such that $j \not\equiv 0 \bmod \boldsymbol{l}$ and $j + a_1 \not\equiv 0 \bmod \boldsymbol{l}$. Let $\pi' = \alpha\zeta^j - 1$. Since $\alpha\zeta^j = \alpha(1 + \pi)^j = 1 + (j + a_1)\pi + \gamma\pi^2 \bmod \mathfrak{l}^e$, π' is in $\mathfrak{l}$ but not in $\mathfrak{l}^2$. Therefore $(\mathcal{O}/\mathfrak{l}^e)/\pi'(\mathcal{O}/\mathfrak{l}^e) \approx \mathcal{O}/\mathfrak{l}$. Thus we see that $M_K/M_K^{\rho-1} \approx \mathcal{O}/\mathfrak{l}$ for $\rho = \tau\sigma^j$ in $\mathrm{Gal}\,(K/\boldsymbol{Q})$. Let k be the fixed field of ρ. Then $k/\boldsymbol{Q}$ is a cyclic extension of degree $\boldsymbol{l}$ in which only p_1 and p_2 are ramified. Therefore the $\boldsymbol{l}$-Sylow subgroup M_k of the ideal class group of k is a module over $\mathcal{O}$ by $\sigma' \mapsto \zeta$, where σ' is a generator of $\mathrm{Gal}\,(k/\boldsymbol{Q})$, and it is $\mathcal{O}$-isomorphic to $\mathcal{O}/\mathfrak{l}^r$ for a natural number r. Since K/k is an unramified cyclic extension of degree $\boldsymbol{l}$, we see that $\#\,(M_K/N_{K/k}M_K) = \boldsymbol{l}$ and $M_K/M_K^{\rho-1} \approx N_{K/k}M_K \subset M_k$. Hence we have that $M_k \approx \mathcal{O}/\mathfrak{l}^2$. On the other hand, we know by [3, Proposition VI. 6] (see also [4 I, Corollary to Theorem 3]) that if $M_k \approx \mathcal{O}/\mathfrak{l}^2$ for some cyclic extension $k/\boldsymbol{Q}$ of degree $\boldsymbol{l}$ in which only p_1 and p_2 are ramified, then $M_{k'} \approx \mathcal{O}/\mathfrak{l}^2$ for every cyclic extension $k'/\boldsymbol{Q}$ of degree $\boldsymbol{l}$ in which only p_1 and p_2 are ramified.

Thus we have the following.

For any odd prime p_1 with $p_1 \equiv 1 \bmod \boldsymbol{l}$, there exist infinitely many primes p_2 which satisfy the following conditions:

(i) $p_2 \equiv 1 \bmod \boldsymbol{l}$,

(ii) $M_k \approx \mathcal{O}/\mathfrak{l}^2$ for every cyclic extension $k/\boldsymbol{Q}$ of degree $\boldsymbol{l}$ in which only p_1 and p_2 are ramified.

4. **Proof of Theorem 2.** Let p_1 and k_1 be as in 3. Let K be the Hilbert class field of k_1, $K_0 = K(\zeta)$, and $\bar{K}_0 = K_0(E_K^{1/l})$.

PROPOSITION 4. *Let the notations be as above. Then there exist infinitely many primes which satisfy the following conditins*:

(i) $p_2 \equiv 1 \bmod l$.

(ii) $l \| h(k)$, i.e., $l | h(k)$ *and* $l^2 \nmid h(k)$, *for every cyclic extension* k/Q *of degree* l *in which only* p_1 *and* p_2 *are ramified.*

(iii) l-rank $(\mathrm{Gal}\,(L/K)) \geqq h(k_1)$, *where* L *is the genus field of* Kk *with respect to* K.

PROOF. Since K/Q is Galois, $\bar{K}_0/Q$ is Galois. Let σ be an element in $\mathrm{Gal}\,(\bar{K}_0/Q)$ such that $\sigma^l = 1$ and that $\sigma \notin \mathrm{Gal}\,(\bar{K}_0/K_0)$. Such σ certainly exists. Indeed, the inertia group of a prime divisor of p_1 in $\bar{K}_0$ is a cyclic group of order l, and is not included in $\mathrm{Gal}\,(\bar{K}_0/K_0)$. Then, by the Čebotarev density theorem, we see that there exist infinitely many unramified primes $\mathfrak{P}_2$ in $\bar{K}_0$ such that the Frobenius symbol $[\mathfrak{P}_2, \bar{K}_0/Q] = \sigma$. Let $p_2 = Q \cap \mathfrak{P}_2$ and $\mathfrak{p}_2 = K \cap \mathfrak{P}_2$. Since p_2 is completely decomposed in $Q(\zeta)$, it follows that $p_2 \equiv 1 \bmod l$ and that $\mathfrak{p}_2$ is in $P^*(K)$. On the other hand, σ generates $\mathrm{Gal}\,(k_1/Q)$. Indeed, since $l \nmid h(k_1)$ and K_0/k_1 is Galois, $\mathrm{Gal}\,(\bar{K}_0/K_0)$ is the unique l-Sylow subgroup of $\mathrm{Gal}\,(\bar{K}_0/k_1)$. Hence p_2 is not decomposed in k_1 and p_2 is non l-th power residue mod p_1. Therefore, by the genus theory, the l-Sylow subgroup M_k of the ideal class group of k is a cyclic group of order l. Thus we have $l \| h(k)$. Since p_2 is not decomposed in k_1, it follows that p_2 is a principal prime ideal in k_1. Hence p_2 is completely decomposed in K/k_1, say $p_2 = \mathfrak{p}_{2,1} \cdots \mathfrak{p}_{2,t}$, where $\mathfrak{p}_{2,1} = \mathfrak{p}_2$ and $t = h(k_1)$. Since $\sigma \notin \mathrm{Gal}\,(\bar{K}_0/K_0)$ and $\mathrm{Gal}\,(\bar{K}_0/K_0)$ is normal, every element conjugate to σ is not contained in $\mathrm{Gal}\,(\bar{K}_0/K_0)$. Hence $\mathfrak{p}_{2,1} \cdots \mathfrak{p}_{2,t}$ are completely decomposed in $\bar{K}_0/K$. Therefore by Proposition 1

$$\bar{G}(p_2) = \bar{G}(\mathfrak{p}_{2,1} \cdots \mathfrak{p}_{2,t}) = G(\mathfrak{p}_{2,1}) \cdots G(\mathfrak{p}_{2,t}) = \{1\} .$$

Thus by Proposition 2 we see that $\sharp\,(P(p_2)/P(p_2)^l P_{p_2}) = l^t$. Moreover, only $\mathfrak{p}_{2,1}, \cdots, \mathfrak{p}_{2,t}$ are ramified in Kk/K, since only p_2 is ramified in k_1k/k_1. Therefore the genus field L of Kk/K is the class field over K corresponding to the ideal class group $I(p_2)/P(p_2)P_{p_2}$ of K. Hence we have that

$$\begin{aligned} l\text{-rank}\,(\mathrm{Gal}\,(L/K)) &= l\text{-rank}\,(I(p_2)/P(p_2)^l P_{p_2}) \\ &\geqq t = h(k_1) . \end{aligned}$$

This completes the proof.

PROOF OF THEOREM 2. Let p_2 be a prime satisfying the conditions in

Proposition 4. Then $l \| h(k)$, hence the l-class field tower of k is finite. Let L be the genus field of Kk with respect to K. Now, we apply [2, Theorem 3] to this L. We first note that $h(k_1) \geqq 4(2 + l)$ implies $h(k_1) \geqq 2 + 2(lh(k_1) - 1 + h(k_1) + 1)^{1/2}$. On the other hand, l-rank $(\mathrm{Gal}\,(L/K)) \geqq h(k_1)$. Hence we have that

$$\begin{aligned} l\text{-rank}\,(\mathrm{Gal}\,(L/K)) &\geqq 2 + 2(lh(k_1) - 1 + h(k_1) + 1)^{1/2} \\ &\geqq 2 + 2(l\text{-rank}\,(E_K) + t + 1)^{1/2} . \end{aligned}$$

Thus the l-class field tower of L is infinite. Since L/Kk and Kk/k are unramified abelian extensions, the class field tower of k is infinite. This proves our theorem.

REMARK. In the case $l = 2$, an argument similar to Theorem 2 holds.

REFERENCES

[1] Y. FURUTA, The genus field and genus number in algebraic number fields, Nagoya Math. J., 29 (1967), 281-285.

[2] Y. FURUTA, On class field towers and the rank of ideal class group, Nagoya Math. J., 48 (1972), 147-157.

[3] G. GRAS, Sur les ℓ-classes d'ideaux dans les extensions cyclique relative de degré premier ℓ, Ann. Inst. Fourier 23, 3 (1973), 1-48; ibid. 23, 4 (1973), 1-44.

[4] T. TAKEUCHI, On the structure of p-class groups of certain number fields I, II, Sci. Rep. Niigata Univ. Series A 14 (1977), 25-33; ibid. 15 (1978), 35-42.

[5] P. ROQUETTE, On class field towers, in Algebraic Number Theory, 231-249, Academic Press, New York, 1968.

DEPARTMENT OF MATHEMATICS
FACULTY OF GENERAL EDUCATION
NIIGATA UNIVERSITY
NIIGATA, 950-21 JAPAN