Y. Furuta
Nagoya Math. J.
Vol. 48 (1972), 147–157

ON CLASS FIELD TOWERS AND THE RANK OF IDEAL CLASS GROUPS

YOSHIOMI FURUTA*

1. Introduction. The following theorem on infinite class field towers is well-known.

THEOREM A (Golod and Šafarevič [4]). *Let K be an algebraic number field and l be any rational prime. Denote by ρ_l the l-rank of the unit group of K and by d_l the l-rank of the ideal class group of K. If we have an inequality*

$$d_l \geq 3 + 2\sqrt{\rho_l + 2}\ ,$$

then K admits an infinite unramified l-extension.

This theorem can be deduced immediately from the following three theorems.[1)]

THEOREM B (Iwasawa [5]). *Let l be a rational prime and K be a finite l-extension of an algebraic number field k. Denote by $G(K/k)$ the Galois group of K/k and by E_K (resp. E_k) the unit group of K (resp. of k). Suppose that K is an unramified extension over k and the class number of K is prime to l. Then we have*

$$E_k/N_{K/k}E_K \cong H^{-3}(G(K/k), Z)\ .$$

THEOREM C. *Let l be a rational prime and G be a finite l-group. Denote by $d(G)$ the minimum number of relations of the generators. Then we have*

$$\dim H^{-3}(G, Z) = r(G) - d(G)\ .$$

THEOREM D (Golod and Šafarevič [4]). *Let l be a rational prime and G be a finite l-group. Then we have*

Received March 23, 1971.

* This work was done mainly while the author was at the University of Maryland, 1970–71.

1) Cf. Šafarevič [7] and also Serre [10].

$$r(G) > \frac{1}{4}(d(G) - 1)^2 ,$$

where $r(G)$ and $d(G)$ are the same as in Theorem C.

This theorem is made better by Roquette [11] as follows:

THEOREM D′. *Notation and assumption being as above, we have*

$$r(G) > \frac{1}{4}d(G)^2 .$$

According to Theorem D′, Theorem A is also made better (cf. Roquette [11]).

The main aim of the present note is to get a generalization of Theorem A by using results on central class fields[2] contained in [3]. In fact, Theorem B can be considered as one of the properties of the central class field (Theorem 5). We can calculate a lower bound for the l-rank of the absolute ideal class groups by combining Theorem C, Theorem D′ and a formula for the central class number (Theorems 1 and 2). This immediately implies a generalization of Theorem A and of the reformed theorem in Roquette [11] (Theorem 3). The sufficient condition in the original Theorem A for the existence of an infinite class field tower over K is given in terms of the unit group and the absolute ideal class group of K itself. But in our generalized theorem, the condition is given by means of the unit group and the ramification with respect to a *subfield* of K. Moreover we can treat not only the existence of infinite class field towers but also the rank of each step of such towers. Also the following fact, obtained as a special case, is remarkable.[3] Let l be any rational prime and m be a rational integer. Assume that the number of different prime divisors p of m such that $p \equiv 1 \pmod{l}$ is equal to or greater than 8 (this number should be replaced by 9, only when $l = 2$ and $m \not\equiv 0 \pmod{4}$). Then the class number of the m-th cyclotomic field of the rational number field is always divisible by l and moreover the m-th cyclotomic field admits an infinite unramified l-extension (Theorem 4).

The author wishes to express his hearty thanks to Drs. T. Kubota, R. Greenberg, G. Fujisaki and T. Takahashi for their valuable advice.

[2] For the definition, see §3.

[3] Cf. Brumer [1].

2. Notation. Throughout this note the following notation will be used.

Z	the ring of rational integers
l	a rational prime number
$K^\times$	the multiplicative group of all non-zero elements of an algebraic number field K which is identified with the principal idele group of K.
J_K	the idele group of an algebraic number field K.
U_K	the unit idele group[4] of an algebraic number field K.
E_K	the unit group of an algebraic number field K.
$G(K/k)$	the Galois group of a Galois extension K over k.
$N_{K/k}$	the Norm of K to k.
$[A:B]$	the index of a subgroup B in a group A or the extension degree of an algebraic extension A over a field B.
$d(G)$	The minimum number of generators of a finite group G.
$r(G)$	the minimum number of relations of a minimal generating system for a finite group G.
$d_l(G)$	the l-rank of a finite abelian group G.
$G_\mathfrak{p}(K/k)$	a decomposition group of any one of the prime divisors in K of a prime $\mathfrak{p}$ in k.
$T_\mathfrak{p}(K/k)$	an inertia group of any one of the prime divisors in K of a prime $\mathfrak{p}$ in k.
$F(K/k)$	the subgroup of the Tate cohomology group $H^{-3}(G(K/k), Z)$ generated by the canonical injections of $H^{-3}(G_\mathfrak{p}(K/k), Z)$ to $H^{-3}(G(K/k), Z)$, where the Galois groups operate trivially on Z and $\mathfrak{p}$ runs over all finite and infinite primes of k.

3. The genus number and central class number. Let k be an algebraic number field of finite degree and K be a finite Galois extension of k. Denote by $\overline{K}$ the absolute class field of K, i.e., the maximal unramified[5] abelian extension of K. Denote by K^* the maximal subfield of $\overline{K}$ which is a composite of K and an abelian extension over k. Denote by $\hat{K}$ the maximal subfield of $\overline{K}$ such that the Galois group $G(\hat{K}/K)$ is contained in the center of the Galois group $G(\hat{K}/k)$. We call K^* and $\hat{K}$ the *genus*

[4] The infinite components of U_K are the same as those of J_K.

[5] All finite and also all infinite primes are unramified.

https://doi.org/10.1017/S0027763000015130 Published online by Cambridge University Press

field and the *central class field of K with respect to k* respectively. Furthermore we call the extension degrees $[K^*:K]$ and $[\hat{K}:K]$ the *genus number* and the *central class number of K with respect to k* respectively and denote them by $g_{K/k}$ and $z_{K/k}$ respectively. Denote by h_K the class number (in the narrow sense) of K, which is equal to the degree $[\overline{K}:K]$.

We have the following formulas for $g_{K/k}$ and $z_{K/k}$ contained in [2] and [3]:

$$g_{K/k} = \frac{h_k \prod e'_{\mathfrak{p}}}{[K_0:k][E_k : E_k \cap N_{K/k}U_K]}, \tag{1}$$

$$z_{K/k} = g_{K/k} \cdot \frac{[k^\times \cap N_{K/k}J_K : N_{K/k}K^\times]}{[E_k \cap N_{K/k}U_K : E_k \cap N_{K/k}K^\times]}, \tag{2}$$

where K_0 is the maximal abelian extension of k contained in K, $e'_{\mathfrak{p}}$ is the ramification index of a prime $\mathfrak{p}$ of k in K_0 and in the product $\prod$, $\mathfrak{p}$ runs through all finite and infinite primes.[6]

4. The Galois group of $\hat{K}$ over K^*. We show in this section that the calculations for the formulas following (5) contained in [3] can be replaced by calculations of isomorphisms of groups and this implies an isomorphism for the Galois group of $\hat{K}$ over K^*.

Since K^* is unramified over K, the local completion of K^* is equal to a composite of the local completion of K and an abelian extension of the local completion of k. The similar statement holds for $\hat{K}$. Hence both K^* and $\hat{K}$ are EL-abelian extensions of K over k as defined by Masuda [6]. Since moreover K^* is a central extension of K over k and $\hat{K}$ is a maximal central extension of K over k contained in $\overline{K}$, we have the following canonical isomorphisms by Theorem 3 of Masuda [6].

$$G(K^*/K) \cong N_{K/k}J_K/(N_{K/k}K^\times \cdot N_{K^*/k}J_{K^*}), \tag{3}$$

$$G(\hat{K}/K) \cong N_{K/k}J_K/(N_{K/k}K^\times \cdot N_{\overline{K}/k}J_{\overline{K}}). \tag{4}$$

We have, by Proposition 1 in [2] and class field theory, $N_{K/k}K^\times \cdot N_{K^*/k}J_{K^*} \subset k^\times \cdot N_{K^*/k}J_{K^*} = k^\times \cdot N_{K_0^*/k}J_{K_0^*} = k^\times \cdot N_{K/k}U_K$, where K_0^* stands for the maximal abelian subfield of K^* over k. Hence $N_{K/k}K^\times \cdot N_{K^*/k}J_{K^*} \subset N_{K/k}J_K \cap k^\times N_{K/k}U_K$. On the other hand, by (1) in [3] we have

$$G(K^*/K) \cong N_{K/k}J_K/(N_{K/k}J_K \cap k^\times N_{K/k}U_K). \tag{3'}$$

[6] $e'_{\mathfrak{p}} = 1$ for almost all primes $\mathfrak{p}$.

https://doi.org/10.1017/S0027763000015130 Published online by Cambridge University Press

Hence comparing (3) and (3′) we see $N_{K/k}K^{\times}\cdot N_{K^*/k}J_{K^*}=N_{K/k}J_K\cap k^{\times}N_{K/k}U_K$ and that (3′) is the canonical isomorphism of Theorem 3 of Masuda [6].

Since $\overline{K}$ is the class field over K corresponding to $K^{\times}\cdot U_K$ by class field theory, we have $K^{\times}\cdot N_{\overline{K}/K}J_{\overline{K}}=K^{\times}\cdot U_K$ and moreover $N_{K/k}K^{\times}\cdot N_{\overline{K}/k}J_{\overline{K}}=N_{K/k}K^{\times}\cdot N_{K/k}U_K$. Hence (4) implies the canonical isomorphism

$$G(\hat{K}/K)\cong N_{K/k}J_K/(N_{K/k}K^{\times}\cdot N_{K/k}U_K)\ . \tag{4′}$$

Now by the canonical isomorphisms (3′) and (4′) we have

$$G(\hat{K}/K^*)\cong (N_{K/k}J_K\cap k^{\times}N_{K/k}U_K)/(N_{K/k}K^{\times}\cdot N_{K/k}U_K)\ .$$

Furthermore by using the same method as that in the calcultaions following (5) contained in [3], we see

$$N_{K/k}J_K\cap k^{\times}\cdot N_{K/k}U_K=(k^{\times}\cap N_{K/k}J_K)\cdot N_{K/k}U_K \text{ and}$$

$$\begin{aligned} G(\hat{K}/K^*)&\cong\frac{(k^{\times}\cap N_{K/k}J_K)\cdot N_{K/k}U_K}{N_{K/k}K^{\times}\cdot N_{K/k}U_K}\\ &\cong\frac{k^{\times}\cap N_{K/k}J_K}{k^{\times}\cap(N_{K/k}K^{\times}\cdot N_{K/k}U_K)}\\ &\cong\frac{(k^{\times}\cap N_{K/k}J_K)/N_{K/k}K^{\times}}{(k^{\times}\cap(N_{K/k}K^{\times}\cdot N_{K/k}U_K))/\cdot N_{K/k}K^{\times}}\ . \end{aligned}\tag{5}$$

For the numerator of the last term the following formula is well-known:

$$(k^{\times}\cap N_{K/k}J_K)/N_{K/k}K^{\times}\cong H^{-3}(G(K/k),Z)/F(K/k)\ , \tag{6}$$

where $F(K/k)$ is, as in the list of notation in §2, the subgroup of $H^{-3}(G(K/k),Z)$ generated by the canonical injections of $H^{-3}(G_{\mathfrak{p}}(K/k),Z)$ to $H^{-3}(G(K/k),Z)$, $\mathfrak{p}$ running over all finite and infinite primes of k and $G_{\mathfrak{p}}(K/k)$ standing for a decomposition group of any one of the prime divisors of $\mathfrak{p}$ in K.

For the denominator, by using the same method as that preceding (6) in [3], we see $k^{\times}\cap(N_{K/k}K^{\times}\cdot N_{K/k}U_K)=N_{K/k}K^{\times}\cdot(k^{\times}\cap N_{K/k}U_K)=N_{K/k}K^{\times}\cdot(E_k\cap N_{K/k}U_K)$ and further

$$\begin{aligned} &(k^{\times}\cap(N_{K/k}K^{\times}\cdot N_{K/k}U_K))/N_{K/k}K^{\times}\\ &\quad\cong(N_{K/k}K^{\times}\cdot(E_k\cap N_{K/k}U_K))/N_{K/k}K^{\times}\\ &\quad\cong(E_k\cap N_{K/k}U_K)/((E_k\cap N_{K/k}U_K)\cap N_{K/k}K^{\times})\\ &\quad\cong(E_k\cap N_{K/k}U_K)/(E_k\cap N_{K/k}K^{\times})\ . \end{aligned}\tag{7}$$

https://doi.org/10.1017/S0027763000015130 Published online by Cambridge University Press

5. Upper bound on $d(F(L/k))$ for l-extensions L/k.

LEMMA 1. *Let L be a finite l-extension of an algebraic number field k and L_0 be the maximal abelian extension of k contained in L. Then we have*

$$d(H^{-3}(G(L/k), Z)) > \frac{1}{4}(d(G(L_0/k)) - 2)^2 - 1 .$$

Proof. We have $r(G(L/k)) > \frac{1}{4}(d(G(L/k)))^2$ by Theorem D′ and this is equivalent to the fact that $r(G(L/k)) - d(G(L/k)) > \frac{1}{4}(d(G(L/k)) - 2)^2 - 1$ by a simple calculation. Since $d(G(L/k)) = d(G(L_0/k))$ by Burnside's basis theorem, the lemma follows immediately from Theorem C and the above inequality.

LEMMA 2. *Let H be a finite group and G be an extension of H by a cyclic group. Then we have*

$$r(G) - d(G) \leq r(H) .$$

Proof. Let α_i $(i = 1, 2, \cdots, d(H))$ be a minimal system of generators of H, σ be a generator of G/H and U_σ be a representative of σ in G. Let m be the order of σ. Clearly $d(G) = d(H) + 1$ or $= d(H)$. First consider the case where $d(G) = d(H) + 1$. Then G can be generated by U_σ and α_i $(i = 1, 2, \cdots, d(H))$. A system of relations for the generators of G can be chosen from the system of $r(H)$ relations of α_i for H and the $(d(H) + 1)$ relations $U_\sigma^m \alpha$, $U_\sigma \alpha_i U_\sigma^{-1} \beta_i$ $(i = 1, \cdots, d(H))$ for some $\alpha, \beta_i \in H$. Thus we have $r(G) \leq r(H) + d(H) + 1$ and hence $r(G) - d(G) \leq r(H)$.

In the case where $d(G) = d(H)$, we can assume that G is generated by U_σ and α_i $(i = 2, 3, \cdots, d(H))$. Then $\alpha_1 = U_\sigma^n \cdot \prod_{i=2}^{d(G)} \alpha_i^{n_i}$ for some integers n and n_i. A system of relations for the generators of G can be chosen from the system of $r(H)$ relations of α_i for H where α_1 is replaced by the right hand side of the above equality, and the $d(H)$ relations $U_\sigma^m \cdot \alpha$, $U_\sigma \alpha_i U_\sigma^{-1} \beta_i$ $(i = 2, 3, \cdots, d(H))$ for some $\alpha, \beta_i \in H$. Thus we have $r(G) \leq r(H) + d(H)$ and hence $r(G) - d(G) \leq r(H)$.

LEMMA 3. *Let L be a finite l-extension of an algebraic number field k and τ_l be the number of finite primes of k which are prime to l and ramified in L. Let $\mathfrak{l}_i$ $(i = 1, 2, \cdots, v)$ be the different prime divisors of l in k and put $\Lambda_l = \sum_{i=1}^{v} r(T_{\mathfrak{l}_i}(L/k))$, where $T_{\mathfrak{l}_i}(L/k)$ is as in the notation in §2. Then we have*

$$d(F(L/k)) \leq \tau_l + \Lambda_l .$$

Proof. Since $F(L/k)$ is generated by homomorphic images of $H^{-3}(G_\mathfrak{p}(L/k), Z)$, we have

$$d(F(L/k)) \leq \sum_{\mathfrak{p}} d(H^{-3}(G_\mathfrak{p}(L/k), Z)) . \tag{8}$$

Moreover we have $H^{-3}(G_\mathfrak{p}(L/k), Z) = r(G_\mathfrak{p}(L/k)) - d(G_\mathfrak{p}(L/k))$ by Theorem C and $r(G_\mathfrak{p}(L/k)) - d(G_\mathfrak{p}(L/k)) \leq r(T_\mathfrak{p}(L/k))$ by Lemma 2, since $G_\mathfrak{p}(L/k)$ is an extension of $T_\mathfrak{p}(L/k)$ by a cyclic group. If $\mathfrak{p}$ is an infinite prime, then $G_\mathfrak{p}(L/k)$ is trivial or cyclic. Hence $d((H^{-3}G_\mathfrak{p}(L/k), Z)) = 0$. If $\mathfrak{p}$ is finite, ramified in L and prime to l, then $T_\mathfrak{p}(L/k)$ is cyclic. Hence $r(T_\mathfrak{p}(L/k)) = 1$. Thus we have $d(F(L/k)) \leq \sum_{\text{finite } \mathfrak{p}} r(T_\mathfrak{p}(L/k)) \leq \tau_l + \Lambda_l$.

6. The *l*-rank of ideal class groups.

THEOREM 1. *Let L be a finite l-extension of an algebraic number field k and L^* (resp. $\hat{L}$) be the genus field (resp. the central class field) of L with respect to k. Then $\hat{L}$ is also an l-extension*[7] *of L^*.*

Furthermore denote by L_0 the maximal abelian extension of k contained in L, by ρ_l the l-rank of the unit group of k and by τ_l the number of primes of k which are prime to l and ramified in L. Moreover let $\mathfrak{l}_i$ $(i = 1, 2, \cdots, v)$ be the different prime divisors of l in k and put $\Lambda_l = \sum_{i=1}^{v} r(T_{\mathfrak{l}_i}(L/k))$, where $T_{\mathfrak{l}_i}(L/k)$ are as in the notation in §2. Then we have

$$d(G(\hat{L}/L^*)) > \frac{1}{4}(d(G(L_0/k)) - 2)^2 - 1 - \rho_l - \tau_l - \Lambda_l .$$

Proof. Since $G(L/k)$ is an l-group, it follows from (6) and a property of cohomology groups that $(k^\times \cap N_{L/k}J_L)/N_{L/k}L^\times$ is an l-group. Hence $G(\hat{L}/L^*)$ is also an l-group by (5). The following inequality follows from (5), (6) and (7) immediately:

$$\begin{aligned} d(G(\hat{L}/L^*)) \geq\ & d(H^{-3}(G(L/k), Z)) - d(F(L/k)) \\ & - d((E_k \cap N_{L/k}U_L)/(E_k \cap N_{L/k}L^\times)) . \end{aligned} \tag{9}$$

Clearly $d((E_k \cap N_{L/k}U_L)/(E_k \cap N_{L/k}L^\times)) \leq \rho_l$. Hence the theorem is obtained immediately from (9), Lemma 1 and Lemma 3.

[7] This contains the case $\hat{L} = L^*$.

https://doi.org/10.1017/S0027763000015130 Published online by Cambridge University Press

For an algebraic number field K, denote by $\overline{K}$ the absolute class field of K as before. We shall obtain by Theorem 1 a lower bound for the l-rank $d_l(G(\overline{K}/K))$ of $G(\overline{K}/K)$ which is isomorphic to the ideal class group of K.

THEOREM 2. *Let K be any finite Galois extension of an algebraic number field k. Let K_0 and L be the maximal abelian extension and maximal l-extension of k contained in K respectively. Denote by ρ_l the l-rank of the unit group of k and by τ_l the number of primes of k which are prime to l and ramified in L. Let further $\mathfrak{l}_i$ $(i = 1, 2, \cdots, v)$ be the different prime divisors of l in k and put $\Lambda_l = \sum_{i=1}^{v} r(T_{\mathfrak{l}_i}(L/k))$, where $T_{\mathfrak{p}_i}(L/k)$ are as in the notation in §2.*

Then the l-rank of the ideal class group of K is equal to or greater than s, i.e., *$d_l(G(\overline{K}/K)) \geq s$, if*

$$d_l(G(K_0/k)) \geq 2 + 2\sqrt{\rho_l + \tau_l + \Lambda_l + s}\ .$$

Proof. Denote by L_0 the maximal abelian extension of k contained in L. Then it follows from Theorem 1 that $d(\hat{L}/L^*) \geq s$ if $\frac{1}{4}(d(G(L_0/k)) - 2)^2 - 1 - \rho_l - \tau_l - \Lambda_l \geq s - 1$. The last inequality is equivalent to the fact that $d(G(L_0/k)) \geq 2 + 2\sqrt{\rho_l + \tau_l + \Lambda_l + s}$. Clearly $d_l(G(\overline{K}/K)) \geq d_l(G(\overline{L}/L)) \geq d(G(\hat{L}/L^*))$ and $d_l(G(K_0/k)) = d(G(L_0/k))$. Hence we have the assertion of the theorem.

7. Class field towers.

THEOREM 3. *An algebraic number field K admits an infinite tower $K = K^{(0)} \subsetneqq K^{(1)} \subsetneqq K^{(2)} \subsetneqq \cdots$ of unramified class fields $K^{(i+1)}$ of $K^{(i)}$ such that the l-rank of $G(K^{(i+1)}/K^{(i)})$ is equal to or greater than s for $i = 0, 1, 2, \cdots$, if K contains a subfield k, over which K is a Galois extension and such that*

$$d_l(G(K_0/k)) \geq 2 + 2\sqrt{\rho_l + \tau_l + \Lambda_l + s}\ ,$$

where K_0 is the maximal abelian extension of k contained in K, ρ_l is the l-rank of the unit group of k, τ_l is the number of primes of k which are prime to l and ramified in the maximal l-extension L of k contained in K and $\Lambda_l = \sum_{i=1}^{v} r(T_{\mathfrak{l}_i}(L/K))$, where $\mathfrak{l}_i$ $(i = 1, 2, \cdots, v)$ are the different prime divisors of l in k and $T_{\mathfrak{l}_i}(L/k)$ are as in the notation in §2.

Proof. Put $K = K^{(0)}$ and let $K^{(i)}$ be the absolute class field of $K^{(i-1)}$

for $i = 1, 2, \cdots$. Denote by $K_0^{(i)}$ the maximal abelian extension of k contained in $K^{(i)}$ and by $L^{(i)}$ the maximal l-extension of k contained in $K^{(i)}$. Then $d_l(G(K_0^{(i)}/k)) \geq d_l(G(K_0/k))$. Since $K^{(i)}$ is an unramified extension of K, the inertia group of any prime of k in $L^{(i)}$ is equal to that in L. Hence the assumption of the theorem implies the assumption of Theorem 2 in the case where $K = K^{(i)}$. Therefore $d_l(G(\overline{K^{(i)}}/K^{(i)})) \geq s$ for $i = 1, 2, \cdots$, which imply the theorem.

Remark. (i) In Theorem 3, assume moreover that K is the absolute class field of k. Then $\tau_l = 0$, $\Lambda_l = 0$, $K = K_0$ and $d_l(G(K_0/k))$ is equal to the l-rank of the ideal class group of k. Therefore Theorem 3 implies the reformed theorem, in Roquette [11], of Theorem A in which K is replaced by k.

(ii) In Theorems 1, 2, and 3, assume moreover that the inertia group $T_{\mathfrak{l}_i}(L/k)$ is abelian with rank λ_i for $i = 1, 2, \cdots, v$. Then we can see easily that $r(T_{\mathfrak{l}_i}(L/k)) \leq \lambda_i(\lambda_i + 1)/2$. Hence Λ_l in the inequalities of the theorems can be replaced by $\sum_{i=1}^{v} \lambda_i(\lambda_i + 1)/2$.

(iii) Since $K^{(1)} = \overline{K} \supset K^*$, the genus field $(K^{(i)})^*$ of $K^{(i)}$ with respect to k is equal to $K^{(i)}$ itself. Hence denoting by $\widehat{K^{(i)}}$ the central class field of $K^{(i)}$ with respect to k, we have $G(\widehat{K^{(i)}}/(K^{(i)})^*) = G(\widehat{K^{(i)}}/K^{(i)})$ for $i = 1, 2, \cdots$.

8. Application to cyclotomic fields. We have the following theorem as a special case of Theorem 3:

THEOREM 4. *Let m be a rational integer and denote by t_l the number of different prime divisors p of m such that $p \equiv 1 \pmod{l}$.*

Then the m-th cyclotomic field of the rational number field admits an infinite tower of unramified class fields such that the l-rank of the Galois group of each step of the class field tower is equal to or greater than s, if

$$
\begin{aligned}
&t_l \geq 4 + 2\sqrt{3 + s} \quad \textit{when } l \textit{ is odd and } m \not\equiv 0 \pmod{l^2}, \\
&t_l \geq 3 + 2\sqrt{4 + s} \quad \textit{when } l \textit{ is odd and } m \equiv 0 \pmod{l^2}, \\
&t_l \geq 4 + 2\sqrt{4 + s} \quad \textit{when } l = 2 \textit{ and } m \not\equiv 0 \pmod{4}, \\
&t_l \geq 3 + 2\sqrt{5 + s} \quad \textit{when } l = 2 \textit{ and } m \equiv 0 \pmod{4} \\
&\qquad\qquad\qquad\qquad\qquad\qquad \textit{but } m \not\equiv 0 \pmod{8}, \\
&t_l \geq 2 + 2\sqrt{7 + s} \quad \textit{when } l = 2 \textit{ and } m \equiv 0 \pmod{8}.
\end{aligned}
$$

https://doi.org/10.1017/S0027763000015130 Published online by Cambridge University Press

In particular, if $t_l \geq 8$ ($t_l \geq 9$ *only when* $l = 2$ *and* $m \not\equiv 0 \pmod 4$), *then the class number of the m-th cyclotomic field is divisible by* l *and moreover the m-th cyclotomic field admits an infinite unramified l-extension.*

Proof. Let $k = \boldsymbol{Q}$ be the rational number field and K be the m-th cyclotomic field over $\boldsymbol{Q}$. By Remark (ii) following Theorem 3, we have $\Lambda_l = \lambda(\lambda + 1)/2$ in the present case, where λ is the rank of the inertia group of l in K over $\boldsymbol{Q}$. Moreover we have the following table:

	$d_l(G(\mathrm{K}/\boldsymbol{Q}))$	ρ_l	τ_l	λ_l	Λ_l
l is odd and $m \not\equiv 0 \pmod{l^2}$	t_l	0	t_l	0	0
l is odd and $m \equiv 0 \pmod{l^2}$	$t_l + 1$	0	t_l	1	1
$l = 2$ and $m \not\equiv 0 \pmod 4$	t_l	1	t_l	0	0
$l = 2$, $m \equiv 0 \pmod 4$ and $m \not\equiv 0 \pmod 8$	$t_l + 1$	1	t_l	1	1
$l = 2$ and $m \equiv 0 \pmod 8$	$t_l + 2$	1	t_l	2	3

Now by simple calculations, it is easy to see that each of the inequalities of the theorem implies the inequality of Theorem 3, which proves the theorem.

9. Generalization of Theorem B. This section, which is connected to §4, is added to remark that the formulas (5), (6) and (7) in §4 imply a generalization of Theorem B.

THEOREM 5. *Let* K *be a finite l-extension of an algebraic number field* k. *If the class number of* K *is prime to* l, *then we have*

$$(E_k \cap N_{K/k}U_K)/N_{K/k}E_K \cong H^{-3}(G(K/k), Z)/F(K/k) \cong (k^\times \cap N_{K/k}J_K)/N_{K/k}K^\times ,$$

where $F(K/k)$ *is as in the notation of* §2.

Proof. Since K is an l-extension, $G(\hat{K}/K^*)$ is also an l-extension by Theorem 1. Moreover since the class number of K is prime to l, we have $G(\hat{K}/K^*) = 1$. Hence by (5), (6) and (7) we have

$$H^{-3}(G(K/k), Z)/F(K/k) \cong (E_k \cap N_{K/k}U_K)/(E_k \cap N_{K/k}K^\times) . \tag{10}$$

We can show moreover that $E_k \cap N_{K/k}K^\times = N_{K/k}E_K$. In fact, let ε be any element of $E_k \cap N_{K/k}K^\times$ and let α and β be integers of K such that $\varepsilon = N_{K/k}\alpha/\beta$. Denote by h the class number of K. Then α^h (resp. β^h)

https://doi.org/10.1017/S0027763000015130 Published online by Cambridge University Press

can be expressed as a product of integers α_i (resp. β_j) of K, i.e., $\alpha^h = \alpha_1 \cdots \alpha_m$ (resp. $\beta^h = \beta_1 \cdots \beta_n$), so that each of the principal ideals (α_i) (resp. (β_j)) is equal to a positive power $\mathfrak{p}_i^{a_i}$ (resp. $\mathfrak{q}_j^{b_j}$) of a prime ideal $\mathfrak{p}_i$ (resp. $\mathfrak{q}_j$) of K. Moreover, if it is necessary, by replacing α_i or β_j by their conjugates over k, we can assume that the set of prime ideals $\mathfrak{p}_i$ coincides with the set of prime ideals $\mathfrak{q}_j$. Then it follows that there exists a unit $\eta \in E_K$ such that $\varepsilon^h = N_{K/k}\eta$. Since h is prime to l and the right hand side of (9) is an l-group, we can conclude that $\varepsilon \in N_{K/k}E_K$. Clearly $N_{K/k}E_K \subset E_k \cap N_{K/k}K^\times$. Hence $E_k \cap N_{K/k}K^\times = N_{K/k}E_K$. The last isomorphism of the theorem is well-known.

Remark. Theorem B follows from Theorem 5. Namely, assume that K is unramified over k. Then for every prime $\mathfrak{p}$ of k, the decomposition group $G_\mathfrak{p}(K/k)$ is cyclic. Hence $H^{-3}(G_\mathfrak{p}(K/k), Z)$ is trivial for all $\mathfrak{p}$ and hence $F(K/k)$ is also trivial. Moreover we have $N_{K/k}U_K = U_k$ and hence $E_k \cap N_{K/k}U_K = E_k$. Hence we have $E_k/N_{K/k}E_K \cong H^{-3}(G(K/k), Z)$, the assertion of Theorem B.

References

[1] A. Brumer, Ramification and class towers of number fields, Michigan Math. J., **12** (1965), 129–131.

[2] Y. Furuta, The genus field and genus number in algebraic number fields, Nagoya Math. J., **29** (1967), 281–285.

[3] Y. Furuta, Über die zentrale Klassenzahl eines relativ-galoisschen Zahlkörpers, J. Number Theory, **3** (1971), 318–322.

[4] E. S. Golod and I. R. Šafarevič, On class field towers (Russian), Izv. Akad. Nauk SSSR, **28** (1964), 261–272 (Amer. Math. Soc. Transl., (2) **48**, 91–102).

[5] K. Iwasawa, A note on the group of units of an algebraic number field, J. Math. pures et appl., **35** (1956), 189–192.

[6] K. Masuda, An application of the generalized norm residue symbol, Proc. Amer. Math. Soc., **10** (1959), 245–252.

[7] I. R. Šafarevič, Algebraic number fields (Russian), Proc. int. cong. Stockholm (1962), 163–176 (Amer. Math. Soc. Transl., (2) **31**, 25–39).

[8] I. R. Šafarevič, Extensions with given points of ramification (Russian), Publ. Math. I.H.E.S., **18** (1963), 71–95 (Amer. Math. Soc. Transl., (2) **59**, 128–149).

[9] J.-P. Serre, Cohomologie galoisienne, Lecture Notes in Math., **5** (1964), Springer-Verlag.

[10] J.-P. Serre, Existence de tours infinies de corps de classes d'après Golod et Šafarevič, Le tendences géométrique en algèbres et théorie de nombres, (1966), 231–238, Center national de la recherche Scientifique.

[11] P. Roquette, On class field towers, Proc. instr. conf. at Brighton (Algebraic Number Theory), (1967), 231–249.

Kanazawa University