83. *Central Class Numbers in Central Class Field Towers*

By Susumu SHIRAI
Department of Liberal Arts and Sciences,
Chubu Institute of Technology, Kasugai

(Comm. by Kenjiro SHODA, M. J. A., June 3, 1975)

1. Introduction. Let $K_0=k$ be an algebraic number field of finite degree and K_n be the central class field of K_{n-1} over k, i.e. the maximal unramified abelian extension over K_{n-1} such that the Galois group of K_n over K_{n-1} is contained in the center of the Galois group of K_n over k. Then the sequence of fields

$$k=K_0\subseteq K_1\subseteq\cdots K_{n-1}\subseteq K_n\subseteq\cdots$$

is called the central class field tower of k, and the extension degree $z_n=[K_{n+1}:K_n]$ is called the central class number[1] of K_n over k. $z_0=[K_1:k]$ is the class number of k.

The existence of algebraic number fields admitting infinite central class field towers is shown by Golod and Šafarevič [5]. In connection with the result, Brumer [2], Furuta [4] and Roquette [7] estimate lower bounds on the l-rank of the ideal class group of a finite Galois extension, where l is a rational prime.

The aim of the present paper is to give an upper bound on the central class number z_n of K_n over k (Main Theorem) and also to give an upper bound on the rank of the Galois group of K_{n+1} over K_n (Theorem 5).

Main Theorem. *Let z_n be as above and d be the minimal number of generators of the ideal class group of k. Then we have*

$$z_{n-1}^d\equiv 0 \pmod{z_n} \qquad \text{for } n>1$$

and

$$z_0^{z_0(d-1)}\equiv 0 \pmod{z_1} \qquad \text{for } n=1.$$

In particular,

$$h^{h(d-1)d^{n-1}}\equiv 0 \pmod{z_n} \qquad \text{for } n\geqq 1,$$

where $h=z_0$ is the class number of k.

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

Z the ring of rational integers
Q the field of rational numbers
K^* the multiplicative group of all non-zero elements of a field K
J_K the idele group of a finite algebraic number field K

1) Cf. Furuta [3].

U_K	the unit idele group[2] of a finite algebraic number field K
E_k	the unit group of a finite algebraic number field k
$N_{K/k}$	the Norm of K to k
$G(K/k)$	the Galois group of a Galois extension K over k
I_K	the ideal group of a finite algebraic number field K
$I_{K/k}$	the subgroup of I_K consisting of ideals whose norm to k are principal in k
I_K^D	the subgroup of I_K generated by the ideals $\mathfrak{a}^{\sigma-1}$ such that $\mathfrak{a} \in I_K$ and $\sigma \in G(K/k)$
(H)	the principal ideal group induced from a number group H in k
$d(G)$	the minimal number of generators of a finite group G
$\|G\|$	the number of elements of a finite group G

3. The central class number. Let k be an algebraic number field of finite degree and K be a finite unramified Galois extension of k. Since U_K is cohomologically trivial as a $G(K/k)$-module, the exact sequence

$$1 \to U_K \to J_K \to I_K \to 1$$

gives an isomorphism

$$H^{-1}(G(K/k), I_K) \cong H^{-1}(G(K/k), J_K) = 0. \tag{1}$$

Therefore, if $N_{K/k}\mathfrak{a}=1$ for $\mathfrak{a} \in I_K$, we have $\mathfrak{a} \in I_K^D$, where 1 denotes the unit element of I_K.

Lemma 1. *Let $H=k^* \cap N_{K/k}J_K$ and K/k be a finite unramified Galois extension. Then we have*

$$I_{K/k}/I_K^D \cdot (K^*) \cong (H)/(N_{K/k}K^*)$$

and the isomorphism is induced from $N_{K/k}$.

Proof. Let $\mathfrak{p}$ be a finite prime in k and $\mathfrak{P}$ be a prime factor of $\mathfrak{p}$ in K. By the local theory we know that an element of $k_{\mathfrak{p}}^*$ is a norm from $K_{\mathfrak{P}}^*$ if and only if its normalized exponential valuation at $\mathfrak{p}$ is divisible by the degree of $\mathfrak{P}$ over $\mathfrak{p}$. Thus $N_{K/k}$ is an epimorphism of $I_{K/k}$ to (H), because K is an unramified extension over k. Suppose that $N_{K/k}\mathfrak{a} \in (N_{K/k}K^*)$ for $\mathfrak{a} \in I_{K/k}$, then there exists α in K^* such that $N_{K/k}(\alpha)\mathfrak{a}=1$. Thus by (1) we have $\mathfrak{a} \in I_K^D \cdot (K^*)$. This completes the proof.

Lemma 2. *Let K/k be a finite unramified Galois extension. Then the sequence*

$$1 \to E_k/E_k \cap N_{K/k}K^* \to H^{-3}(G(K/k), Z) \to I_{K/k}/I_K^D \cdot (K^*) \to 1$$

is exact. Moreover if K contains the Hilbert class field of k, then we have[3]

$$z_{K/k} = |H^{-3}(G(K/k), Z)| / [E_k : E_k \cap N_{K/k}K^*],$$

2) The infinite components of U_K are the same as those of J_K.

3) The last formula follows also from a general formula of the central class numbers in Furuta [3].

where $z_{K/k}$ *denotes the central class number of* K *over* k.

Proof. Let H be as in Lemma 1. By local class field theory, we see $H \supseteq E_k$. Thus,

$$(H)/(N_{K/k}K^*) \cong H/E_k \cdot N_{K/k}K^* \cong \frac{H/N_{K/k}K^*}{E_k \cdot N_{K/k}K^*/N_{K/k}K^*}.$$

It is well-known that if K/k is an unramified Galois extension, then $H^{-3}(G(K/k), Z) \cong H/N_{K/k}K^*$. So, the exact sequence holds. Moreover if K contains the Hilbert class field of k, then we have $I_{K/k} = I_K$. By global class field theory, the central class field of K over k corresponds to the ideal group $I_K^D \cdot (K^*)$. This completes the proof.

4. The Schur Multiplicator. We note that $H^{-3}(G, Z)$ is isomorphic to the Schur multiplicator $H^2(G, Q/Z)$ of G, where G acts trivially on Q/Z. Now, let G be a finite nilpotent group of class n, and let

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{n-1} \supset G_n = 1 \qquad (2)$$

and

$$G = Z_n \supset Z_{n-1} \supset Z_{n-2} \supset \cdots \supset Z_1 \supset Z_0 = 1$$

be the lower central series, the upper central series of G, respectively. Then it follows from [1, p. 212] the following

Lemma 3. *Let* G *be a finite nilpotent group of class* $n > 1$. *Then the sequence*

$$0 \longrightarrow G_{n-1} \longrightarrow H^2(G/G_{n-1}, Q/Z) \xrightarrow{\text{inf}} H^2(G, Q/Z) \longrightarrow \text{Hom}\,(G/Z_{n-1}, G_{n-1})$$

is exact.

It is clear that $|\text{Hom}\,(G/Z_{n-1}, G_{n-1})|$ divides $|G_{n-1}|^{d(G/Z_{n-1})}$. Let $\Phi(G)$ be the Frattini subgroup of G. Then we have

$$\Phi(G) \supseteq [G, G] = G_1,$$

where $[G, G]$ denotes the commutator subgroup of G. Since

$$d(G/Z_{n-1}) \leqq d(G) = d(G/\Phi(G)) \leqq d(G/G_1),$$

$|\text{Hom}\,(G/Z_{n-1}, G_{n-1})|$ divides $|G_{n-1}|^{d(G/G_1)}$. Thus by Lemma 3 we have

Lemma 4. *If* G *is a finite nilpotent group of class* $n > 1$, *then*

$$|H^2(G/G_{n-1}, Q/Z)| \cdot |G_{n-1}|^{d(G/G_1)-1} \equiv 0 \qquad (\text{mod. } |H^2(G, Q/Z)|).$$

5. Proof of the Main Theorem. Let the situation be as in Section 1, and suppose that $z_{n-1} \neq 1$. We denote by G the Galois group of K_n over k. Then G is a finite nilpotent group of class n, and the lower central series (2) of G corresponds to the sequence of fields

$$k = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{n-1} \subset K_n.$$

Thus, $|G_{n-1}| = [K_n : K_{n-1}] = z_{n-1}$. By Lemma 2 we have

$$|H^2(G/G_{n-1}, Q/Z)| = z_{n-1} \cdot [E_k : E_k \cap N_{K_{n-1}/k}K_{n-1}^*]$$

and

$$|H^2(G, Q/Z)| = z_n \cdot [E_k : E_k \cap N_{K_{n-1}/k}K_{n-1}^*] \cdot [E_k \cap N_{K_{n-1}/k}K_{n-1}^* : E_k \cap N_{K_n/k}K_n^*].$$

Therefore, if $n > 1$, we have by Lemma 4

$$z_{n-1}^{d(G/G_1)} \equiv 0 \qquad (\text{mod. } z_n),$$

where G/G_1 is isomorphic to the ideal class group of k. This completes the proof in case of $n>1$.

Next, set $n=1$. Then G is an abelian group of order $z_0=h$. The following sequence

$$0 \longrightarrow Z/(h) \longrightarrow Q/Z \overset{h}{\longrightarrow} Q/Z \longrightarrow 0$$

is exact, where h denotes the homomorphism induced by h times multiplication. Passing to cohomology, we have the exact sequence

$$0 \longrightarrow H^1(G, Q/Z) \longrightarrow H^2(G, Z/(h)) \longrightarrow H^2(G, Q/Z) \longrightarrow 0.$$

Since $H^1(G, Q/Z) \cong \text{Hom}\,(G, Q/Z)$, we have

$$|H^2(G, Q/Z)| = |H^2(G, Z/(h))|/h. \qquad (3)$$

In the sequence

$$\cdots \longrightarrow C^1(G, Z/(h)) \overset{\delta^1}{\longrightarrow} C^2(G, Z/(h)) \overset{\delta^2}{\longrightarrow} C^3(G, Z/(h)) \longrightarrow \cdots,$$

let $C^i(G, Z/(h))$ be the group of i-cochains of G in $Z/(h)$ and δ^i be the coboundary operator. By definition, we have

$$H^2(G, Z/(h)) = \ker \delta^2 / \text{im}\, \delta^1. \qquad (4)$$

First,

$$|\text{im}\, \delta^1| = |C^1(G, Z/(h))|/|\ker \delta^1| = h^h/|\text{Hom}\,(G, Z/(h))| = h^{h-1}.$$

Next, let $\sigma_1, \sigma_2, \cdots, \sigma_d$ be the minimal generators of G. Then a 2-cocycle f is trivial if its restriction on $\{\sigma_1, \sigma_2, \cdots, \sigma_d\} \times G$ $(\subset G \times G)$ is trivial. The number of mappings of $\{\sigma_1, \sigma_2, \cdots, \sigma_d\} \times G$ into $Z/(h)$ is h^{dh}. So, $|\ker \delta^2|$ divides h^{dh}. Thus[4] by (4) $|H^2(G, Z/(h))|$ divides $h^{h(d-1)+1}$. We conclude by (3) that $|H^2(G, Q/Z)|$ divides $h^{h(d-1)}$. Therefore, by Lemma 2 we have

$$h^{h(d-1)} \equiv 0 \qquad (\text{mod. } z_1).$$

This completes the proof in case of $n=1$.

6. An upper bound on the rank of $G(K_{n+1}/K_n)$. We give an upper bound on the rank of the Galois group $G(K_{n+1}/K_n)$ in the central class field tower of k.

Theorem 5. *Let the situation and notation be as in Section* 1. *Then we have*

$$d(G(K_{n+1}/K_n)) \leqq (d+1) \cdot d(G(K_n/K_{n-1})) + r_1 + r_2 \qquad \textit{for } n>1$$

and

$$d(G(K_2/K_1)) \leqq d \cdot h \qquad \textit{for } n=1,$$

where r_1 is the number of real and r_2 the number of complex prime divisors of k. In particular,

$$d(G(K_{n+1}/K_n)) \leqq \{(d+1)^{n-1} \cdot (d^2 \cdot h + r_1 + r_2) - (r_1 + r_2)\}/d \qquad \textit{for } n \geqq 1.$$

Proof. By Lemma 2 we have[5]

4) This follows also from Schreirer's theorem [6, §36] and MacLane's theorem [6, §50].

5) On a relationship between the ranks of modules in a exact sequence, see Brumer [2].

$$d(G(K_{n+1}/K_n)) \leqq d(H^2(G, Q/Z)),$$
$$d(H^2(G/G_{n-1}, Q/Z)) \leqq d(E_k/E_k \cap N_{K_{n-1}/k}K_{n-1}^*) + d(G(K_n/K_{n-1}))$$

and also by Lemma 3

$$d(H^2(G, Q/Z)) \leqq d(H^2(G/G_{n-1}, Q/Z)) + d \cdot d(G(K_n/K_{n-1})).$$

It is clear that $d(E_k/E_k \cap N_{K_{n-1}/k}K_{n-1}^*) \leqq r_1 + r_2$, which completes the proof in case of $n > 1$.

If $n=1$, then we obtain from Section 5 that

$$d(G(K_2/K_1)) \leqq d(H^2(G, Q/Z)) \leqq d(H^2(G, Z/(h))) \leqq d(\ker \delta^2).$$

It can be easily checked that $d(\ker \delta^2) \leqq d \cdot h$. This completes the proof in case of $n=1$.

References

[1] A. Babakhanian: Cohomological Methods in Group Theory. Marcel Dekker, Inc., New York (1972).

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

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

[4] ——: On class field towers and the rank of ideal class groups. Nagoya Math. J., **48**, 147–157 (1972).

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

[6] A. G. Kurosh: The Theory of Groups (2nd ed.) Gostehizdat, Moscow (1953) (in Russian). English translation published by Chelsea, New York (1955, 1956).

[7] P. Roquette: On Class Field Towers. Proc. instr. conf. at Brighton (Algebraic Number Theory), 231–249 (1967).