On the l-dimension of the ideal class groups of Kummer extensions of a certain type

By Shinju KOBAYASHI

(Communicated by Y. Kawada)

§ 1. Introduction

Let k be an algebraic number field of finite degree and C_k its ideal class group. For each prime number l, we define the l-dimension of C_k by,

$$d^{(l)}C_k = \dim_{F_l}(C_k/C_k^l) ,$$

where F_l denotes the finite field of l elements. In other words, $d^{(l)}C_k$ is the number of invariants of C_k (as a finite abelian group) which are divisible by l. Several authors have given estimates of $d^{(l)}C_k$ from below. (See, e.g., [1].) The purpose of this paper is to improve them for Kummer extensions. Namely, we prove the following

THEOREM 1. *Let l be a regular odd prime number and put $k=\boldsymbol{Q}(\zeta_l)$, where ζ_l denotes a primitive l-th root of unity. For each l-th power free rational integer m (>1), put $K=k(\sqrt[l]{m})$, $\Omega=\boldsymbol{Q}(\sqrt[l]{m})$, and define an integer $\nu(K/k)$ by $(C_K^G:1)=h_k l^{\nu(K/k)}$, where G is the Galois group $G(K/k)$, h_k is the class number of k and C_K^G is the subgroup of G-invariant elements of C_K. Then we have,*

$$d^{(l)}C_K \geqq \nu(K/k)+d^{(l)}C_\Omega-s .$$

Here s denotes the number of prime factors p of m such that $p\equiv 1 \pmod{l}$.

COROLLARY. *Put $l=3$ in Theorem 1. Suppose every prime factor p of m other than 3 is such that $p\equiv -1 \pmod 3$, and that at least one of them satisfies $p^2\not\equiv 1 \pmod{3^2}$. Then if t is the number of primes totally ramified in $\Omega=\boldsymbol{Q}(\sqrt[l]{m})$, we have,*

$$d^{(3)}C_\Omega = t-2 .$$

Before proving these results, we restate the Theorem of [1] and compare with our Theorem 1. The result obtained in [1] is as follows.

THEOREM. *Let F be a finite algebraic number field and K a finite extension of F. Put*

$$w_{K/F} = \dim_{F_l}(F^* \cap K^{*l})/F^{*l}$$

and denote by $t_{K/F}$ the number of prime ideals $\mathfrak{p}$ of F which satisfy the fol-

lowing two conditions:

(i) *the order of the class containing* $\mathfrak{p}$ *in* C_F *is prime to* l,

(ii) *the ramification indices of the prime factors of* $\mathfrak{p}$ *in* K *are all divisible by* l.

Then we have,

$$(1) \qquad d^{(l)}C_K \geqq d^{(l)}C_F + t_{K/F} - (w_{K/F} + d^{(l)}E_K - d^{(l)}E_F) .$$

Here E_K *denotes the unit group of* K *and* $d^{(l)}E_K$ *is defined as in the case of* C_K. *If* K/F *is a Galois extension,* $d^{(l)}E_K - d^{(l)}E_F$ *can be replaced by* $(\rho_K - \rho_F)/(l-1)$, *where* ρ_K *is the number of fundamental units of* K.

The outline of the proof is as follows: suppose $h_F = 1$ for brevity. Then the condition (i) is always satisfied, and if a prime number π of F satisfies (ii), it can be written in the form,

$$(\pi) = \mathfrak{A}(\pi)^l$$

where $\mathfrak{A}(\pi)$ is an ideal of K. Hence the class $c(\pi)$ containing $\mathfrak{A}(\pi)$ in K has the order l if $\mathfrak{A}(\pi)$ is not principal. Now (1) is obtained by calculating the number of independent classes among those of the form $c(\pi)$.

On the other hand, in the situation of Theorem 1 where K/k is a cyclic extension of degree l, the classes in K of the form $c(\pi)$ belong to C_K^G and hence the right hand side of (1) is essentially equivalent to $\nu(K/k)$. Theorem 1 asserts that $d^{(l)}C_K$ is bigger than that by $d^{(l)}C_\Omega - s$ (which may be positive according to (1)).

In §2, we prove $d^{(l)}C_K \geqq \nu(K/k)$ for a cyclic extension K/k of degree l with $l \nmid h_k$, and prove Theorem 1 in §3. Throughout this paper, l denotes a fixed odd prime number. If K/k is an abelian extension, $\mathfrak{f}(K/k)$ denotes its conductor. For a positive integer n, ζ_n denotes a primitive n-th root of unity.

§2. The case of a cyclic extension of degree l

In this section, we assume that K/k is a cyclic extension of degree l, and fix a generator σ of $G = G(K/k)$. As in Theorem 1, we define $\nu(K/k)$ by,

$$(C_K^G : 1) = (C_K : C_K^{1-\sigma}) = h_k l^{\nu(K/k)} .$$

According to [4, I$_a$] Satz 13,

$$\nu(K/k) = t + q^* - (r_k + o) ,$$

where

t is the number of primes of k which are ramified in K,

r_k is the number of infinite primes of k,

q^* is given by $(N_{K/k}(K^*)\cap E_k : E_k^l)=l^{q^*}$,

and

o means 1 or 0 according to whether k contains ζ_l or not.

The next proposition shows the relation between $d^{(l)}C_K$ and $\nu(K/k)$.

PROPOSITION 1. *If $l\nmid h_k$, we have*

(i) $C_K^l \supset C_K^{(1-\sigma)^{l-1}}$,

(ii) $(C_K^l : C_K^{(1-\sigma)^{l-1}})$ *is prime to* l,

and hence

(iii) $\nu(K/k)\leqq d^{(l)}C_K \leqq (l-1)\nu(K/k)$.

For the proof, we need a lemma.

LEMMA 1 ([7], Hilfssatz 1). *There exist polynomials $f, \varphi, \psi \in \boldsymbol{Z}[X]$ such that,*

(a) $(1-X)^{l-1}=(1+X+\cdots+X^{l-1})+lf(X)$,

(b) $l=(1-X)^{l-1}\varphi(X)+(1+X+\cdots+X^{l-1})\psi(X)$.

PROOF OF PROPOSITION 1. Let $c\in C_K$. If we use (a),

$$c^{(1-\sigma)^{l-1}}=N_{K/k}(c)\cdot c^{lf(\sigma)}.$$

Since $l\nmid h_k$, this proves (i). Similarly by (b),

$$c^l=c^{(1-\sigma)^{l-1}\varphi(\sigma)}\cdot N_{K/k}(c^{\psi(\sigma)}).$$

Hence $(c^l)^{h_k}\in C_K^{(1-\sigma)^{l-1}}$, which implies (ii).

Now if $l\nmid h_k$, there exist subgroups H and H' of C_K containing $C_K^{1-\sigma}$ such that,

$$(2)\qquad \begin{cases} C_K/C_K^{1-\sigma}=H/C_K^{1-\sigma}\times H'/C_K^{1-\sigma}, \\ (C_K : H)=l^{\nu(K/k)}, \quad (C_K : H')=h_k. \end{cases}$$

Let K_0 be the class field over K corresponding to the ideal group H. Then by Proposition 1, $G(K_0/K)$ is an elementary abelian group of exponent l and of rank $\nu(K/k)$. In fact, the following proposition holds.

PROPOSITION 2. (i) *K_0 is unramified over K and abelian over k and its degree over K is a power of l. Moreover K_0 is maximal among the extensions of K with these properties.*

(ii) *$G(K_0/k)$ is an elementary abelian group of exponent l.*

REMARK. Proposition 2 is essentially contained in [5], but we reproduce the proof for the sake of completeness.

PROOF OF PROPOSITION 2. (i) Let K_1 be an unramified abelian extension of K and H_1 the corresponding ideal group in K in the sense of class field theory. Then by the argument in [4, II] §5, K_1 is abelian over k if and only if H_1 contains $C_K^{1-\sigma}$. By the definition of H (see (2)), this proves (i).

(ii) We know that $G(K_0/k)$ is an abelian group of exponent at most l^2. So assume that there exists an element τ of order l^2, and let $\mathfrak{p}$ be a prime ideal in k such that $\left(\frac{K_0/k}{\mathfrak{p}}\right)=\tau$. Then $\mathfrak{p}$ must have degree l in K/k and therefore,

$$\left(\frac{K_0/K}{\mathfrak{p}}\right)=\left(\frac{K_0/k}{N_{K/k}(\mathfrak{p})}\right)=\tau^l .$$

But since $\mathfrak{p}^{h_k}\sim 1$ in k and $l\nmid h_k$, we have $\mathfrak{p}\sim 1 \bmod H$ in K, and this contradicts the assumption.

§3. The proof of Theorem 1

We use the same notations as in Theorem 1 in §1, and put $\mathfrak{l}=(1-\zeta_l)$ in k. By hypothesis, $l\nmid h_k$ and Propositions 1 and 2 hold.

Let $\tilde{\Omega}$ be the class field over Ω corresponding to the ideal group $C_{\mathfrak{l}}^{l}$. It suffices to show that $[\tilde{\Omega}K\cap K_0 : K]=l^s$. First we prove a lemma.

LEMMA 2.[1] *Let G be a finite non-abelian group of order $l^2(l-1)$, having three subgroups H, H_1 and S such that,*

(i) *H is normal in G and isomorphic to $\boldsymbol{F}_l\oplus\boldsymbol{F}_l$,*

(ii) *H_1 is a subgroup of H of order l and contained in the center of G,*

(iii) *S is a cyclic group of order $l-1$.*

Then G is the direct product of H_1 and a normal subgroup of index l.

PROOF. It is easily verified that $G=H\cdot S$ (semi-direct product), where S acts on H through inner automorphisms in G. So by the hypothesis (i), S has a representation φ into $GL(2, \boldsymbol{F}_l)$ by choosing a suitable basis $\{e_1, e_2\}$ of H. In particular, if we take e_1 in H_1 and if τ is a generator of S, $\varphi(\tau)=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ fixes $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and hence $(a, c)=(1, 0)$. Moreover, we can show that $d\neq 1$. In fact, if $d=1$, we get $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^l=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so that $\varphi(\tau)$ must be either of order l or the identity element. But as we assumed S to be of order $l-1$ and G non-abelian, neither is the case. Then an arbitrary non-zero $\beta\in\boldsymbol{F}_l$ and $\alpha=b\beta/(d-1)$ satisfy $\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}=d\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, i.e., $e_2'=\alpha e_1+\beta e_2$ is an eigen-vector of $\varphi(\tau)$ which is not contained in H_1, so that $H_2=\boldsymbol{F}_l\cdot e_2'$ is an S-invariant subgroup of H and $H=H_1\oplus H_2$. Hence the semi-direct product $H_2\cdot S$ is defined and

$$G=H\cdot S=H_1\times H_2\cdot S . \qquad \text{q.e.d.}$$

Now we return to the proof of Theorem 1.

Let L be an arbitrary extension of K of degree l contained in $\tilde{\Omega}K\cap K_0$. L is

[1] The author owes Mr. E. Bannai for his kind advices in proving this lemma.

clearly a Galois extension of $\boldsymbol{Q}$. Denote by Ω_1 the extension of Ω corresponding to the cyclic subgroup of order $l-1$ of $G(L/\Omega)$. Put $G=G(L/\boldsymbol{Q})$, $H=G(L/k)$, $H_1=G(L/K)$, $S=G(L/\Omega_1)$. Then by Proposition 2, G, H, H_1 and S satisfy the assumptions in Lemma 2, and hence L contains a cyclic extension M of degree l over $\boldsymbol{Q}$ such that $L=KM$.

We assert that M is contained in the composite field $\prod \boldsymbol{Q}(\zeta_p)$, where the product is taken over all the prime factors p of m such that $p\equiv 1 \pmod{l}$.[2] In fact, by [4, $\mathrm{I_a}$] Satz 3, $\mathfrak{f}(M/\boldsymbol{Q})$ is one of the following two forms:

$$\mathfrak{f}(M/\boldsymbol{Q})=\prod \mathfrak{p}\,, \qquad \forall p\equiv 1 \pmod{l}\,,$$

or, if l is ramified in M,

$$\mathfrak{f}(M/\boldsymbol{Q})=\mathfrak{l}^2 \prod \mathfrak{p}\,, \qquad \forall p\equiv 1 \pmod{l}.$$

Since the primes which do not divide lm are unramified in L, we have only to show that l is unramified in M. So assume the converse and let k' be the cyclic extension of degree l over $\boldsymbol{Q}$ contained in $\boldsymbol{Q}(\zeta_{l^2})$. Then Mk' is contained in $\boldsymbol{Q}(\zeta_{l^2})\cdot \prod_{p\mid m,\, p\equiv 1 \pmod{l}} \boldsymbol{Q}(\zeta_p)$ and hence l must be unramified in Mk'/M. So l is unramified in $L\boldsymbol{Q}(\zeta_{l^2})/L$ and hence unramified in $K\boldsymbol{Q}(\zeta_{l^2})/K$. So the inertia field T of $\mathfrak{l}$ in $K\boldsymbol{Q}(\zeta_{l^2})/k$ is cyclic of degree l over k and T is of the form $k(\sqrt[l]{\zeta_l m^x})$. Since $\mathfrak{l}$ is unramified in T, we have, by [4, $\mathrm{I_a}$], Satz 9,

$$\zeta_l \cdot m^x \underset{(l)}{\equiv} 1 \pmod{\mathfrak{l}^l}\,.$$

Taking the complex conjugate,

$$\zeta_l^{-1} \cdot m^x \underset{(l)}{\equiv} 1 \pmod{\mathfrak{l}^l}\,,$$

hence

$$\zeta_l \underset{(l)}{\equiv} 1 \pmod{\mathfrak{l}^l}\,.$$

But this contradicts the fact that l is totally ramified in $\boldsymbol{Q}(\zeta_{l^2})=k(\sqrt[l]{\zeta_l})$.

Conversely, for each p satisfying $p\mid m$, $p\equiv 1 \pmod{l}$, let M_p be the unique cyclic extension of degree l over $\boldsymbol{Q}$ contained in $\boldsymbol{Q}(\zeta_p)$. Then $M_p\Omega/\Omega$ is unramified outside the prime factor of p in Ω. On the other hand, $M_p\Omega=M_p(\sqrt[l]{m})$ and if $\mathfrak{p}_1$ is the prime factor of p in M_p, $v_{\mathfrak{p}_1}(m)\equiv 0 \pmod{l}$. We can easily see from this, by lifting $M_p\Omega/M_p$ to a Kummer extension $M_p(\zeta_l, \sqrt[l]{m})/M_p(\zeta_l)$, that $\mathfrak{p}_1$ is unramified in $M_p\Omega/M_p$. Hence $M_p\Omega/\Omega$ is unramified and $M_p\Omega$ is contained in $\tilde{\Omega}$. $M_p\Omega K$ is therefore contained in $\tilde{\Omega}K\cap K_0$.

As the composite of all cyclic extensions of degree l over $\boldsymbol{Q}$ contained in

[2] This fact is contained in a more general theorem of [3].

$\prod_{p|m, p\equiv 1 \pmod{l}} \boldsymbol{Q}(\zeta_p)$ is equal to $\prod_{p|m, p\equiv 1 \pmod{l}} M_p$, we have proved

$$\tilde{\Omega}K \cap K_0 = K \cdot \prod_{p|m, p\equiv 1 \pmod{l}} M_p \,. \qquad \text{q.e.d.}$$

PROOF OF COROLLARY. As shown in [6], $3^{q'} = (N_{K/k}(K^*) \cap E_k : E_k^3)$ is easily calculated by means of Hilbert's norm residue symbol and it is equal to 0 in our case, hence $\nu(K/k) = t-2$. (The number of primes of k ramified in K is equal to t.) On the other hand, it is easy to see that $w_{\Omega/Q} = 1$ in the notation of (1), §1, hence

$$d^{(3)}C_\Omega \geqq t-2 \,.$$

The corollary is now an immediate consequence of Proposition 1, (iii) and Theorem 1.

REMARK. Put in general $m = 3^{x_0} \prod_{i=1}^{n} p_i^{x_i}$, $0 \leqq x_0 \leqq 2$, $1 \leqq x_i \leqq 2$, $(i = 1, \cdots, n)$. Then by [2],

$$t = \begin{cases} n & \text{if} \quad m^2 \equiv 1 \pmod{3^2} \\ n+1 & \text{if} \quad m^2 \not\equiv 1 \pmod{3^2} \,. \end{cases}$$

References

[1] Connell, I. and D. Sussman, The p-dim of class groups of number fields, J. London Math. Soc. (2) **2** (1970), 525-529.

[2] Dedekind, R., Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern, J. reine angew. Math. **121** (1900), 40-123.

[3] Fröhlich, A., The genus field and genus group in finite number fields, Mathematika **6** (1959), 40-46.

[4] Hasse, H., Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Ia, Jber. der Deutsch. Math.-Verein. **36** (1927), 231-311, II, ibid. **39** (1930), 1-204.

[5] Hasse, H., Zur Geschlechtertheorie in quadratischen Zahlkörpern, J. Math. Soc. Japan **3** (1951), 45-51.

[6] Honda, T., Pure cubic fields whose class numbers are multiples of 3, J. Number Theory **3** (1971), 7-12.

[7] Inaba, E., Über die Struktur der l-klassengruppe zyklischer Zahlkörper von Primzahlgrad l, J. Fac. Sci. Univ. Tokyo Sect. I **4** (1940), 61-115.

(Received February 24, 1971)

Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Fukazawa, Setagaya-ku, Tokyo
158 Japan