J. Math. Soc. Japan
Vol. 38, No. 4, 1986

On infinite unramified Galois extensions of algebraic number fields with many primes decomposing almost completely

By Ken YAMAMURA

(Received Feb. 26, 1985)

§ 1. Introduction.

Recently, Ihara [5] proved a natural inequality for an infinite unramified Galois extension M/K of a global field, which gives an upper bound for some 'weighted cardinality' of the set T of those primes of K that decompose almost completely in M/K:

$$(*) \qquad \sum_{P\in T}\alpha_P \leqq \begin{cases} \frac{1}{2}\log D_K & \text{(in the number field case, assuming GRH),} \\ (g-1)\log q & \text{(in the function field case).} \end{cases}$$

Here, α_P is some positive 'weight' of a prime P of K and GRH means the Generalized Riemann Hypothesis for all K' with $K\subset K'\subset M$, $[K':K]<\infty$ (for details see § 2). In the function field case there are cases such that the equality in (*) holds ([2], cf. also [1], [3]). However, in the number field case such cases are still unknown. Therefore, Ihara considered $\rho(M/K)$, the ratio of two sides of (*), i. e.

$$\rho(M/K)=\sum_{P}\alpha_P\Big/\Big(\frac{1}{2}\log D_K\Big),$$

and gave an example such that $\rho(M/K)\geqq 0.7517\cdots$. The lower bound of this $\rho(M/K)$ is fairly smaller than 1. In this paper, we shall give a way to construct examples of M/K with large $\rho(M/K)$, considering some class field tower with many finite primes decomposing completely. Our maximum lower bound obtained in this way is $0.9115\cdots$, i. e. we obtain M/K such that

$$\rho(M/K)\geqq 0.9115\cdots.$$

This value is much nearer to 1 than that given by Ihara's example. Therefore, this value seems to be helpful for further study. This value is achieved by the following K and M:

K: the composite field of the absolute class field of $\boldsymbol{Q}(\sqrt{15377})$ and $\boldsymbol{Q}(\sqrt{-5\cdot 7\cdot 15377})$;

M: the maximum unramified pro-2-extension of K in which all primes in $\mathfrak{S}$ decompose completely, where $\mathfrak{S}$ is the set of primes of K consisting of all prime divisors of 3, 11, 13, 37 and one prime divisor of 43 ($|\mathfrak{S}|=105$).

This paper is part of the author's Master's thesis [8]. The author wishes to express his sincere gratitude to his teacher Y. Ihara who suggested him to consider this problem.

§ 2. Ihara's inequality.

In this section, we shall review Ihara's inequality.

NOTATION.

K: a global field, i.e. either an algebraic number field of finite degree (NF), or an algebraic function field of one variable over a finite field (FF);

M/K: an infinite unramified Galois extension (the unramifiedness refers also to the archimedean primes of K);

S_0: the set of all non-archimedean primes of K;

$f(P)$: the residue extension degree of $P\in S_0$ in M/K $(1\leqq f(P)\leqq\infty)$;

$N(P)$: the absolute norm of $P\in S_0$;

$S=\{P\in S_0 : f(P)<\infty\}$;

S_∞: the set of all archimedean primes of K;

For each prime $P\in S\cup S_\infty$, the constant α_P is defined as follows:

$$\begin{aligned}\alpha_P &= \frac{\log N(P)}{N(P)^{f(P)/2}-1} && (P\in S)\\ &= \frac{1}{2}\left(\log 8\pi+\frac{\pi}{2}+\gamma\right) && (P\in S_\infty;\ \text{real})\\ &= \log 8\pi+\gamma && (P\in S_\infty;\ \text{imaginary})\end{aligned}$$

where γ is Euler's constant;

$$\gamma=\lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log n\right)=0.577\cdots.$$

In the following theorem of Ihara, when K is a number field, we assume that the Riemann Hypothesis is valid for the Dedekind zeta function $\zeta_{K'}(s)$ for all K' with $K\subset K'\subset M$, $[K':K]<\infty$ (GRH) and when K is a function field, we assume that the genus g of K is positive.

THEOREM (Ihara [5]). *When K is a number field, let D_K denote the absolute value of the discriminant of K. When K is a function field, let F_q denote the exact constant field of K. Then*

$$(*)\qquad \sum_{P\in S\cup S_\infty} \alpha_P \leqq \begin{cases} \dfrac{1}{2}\log D_K & (NF,\ \textit{under GRH}) \\ (g-1)\log q & (FF), \end{cases}$$

the series on the left being convergent.

We shall also review the examples given by Ihara.

EXAMPLE 1 (FF-case). When M/K corresponds to a torsion-free co-compact irreducible discrete subgroup Γ of $PSL_2(\boldsymbol{R})\times PSL_2(F_\mathfrak{p})$ ($F_\mathfrak{p}$: a $\mathfrak{p}$-adic field), the equality in (*) holds. (See [1]~[5]. A survey is given in [4].)

EXAMPLE 2 (NF-case). Let K be an imaginary quadratic number field $\boldsymbol{Q}(\sqrt{d})$

$$d = -3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 23\cdot 31 \quad (\equiv 1 \pmod 8)$$

and $\mathfrak{S}$ be the set of two distinct prime divisors of (2) in K. Then by the Gaschütz-Wienberg refinement of Golod-Šafarevič theory for class field tower (cf. [7] and § 14 of [5]), M/K is infinite, where M is the maximum unramified pro-2-extension of K in which two primes in $\mathfrak{S}$ decompose completely. Easy computation shows that

$$\rho(M/K) \geqq 0.7517\cdots .$$

The lower bound of this $\rho(M/K)$ is the largest among the examples that Ihara considered in [5].

§ 3. Class field tower with finite primes decomposing completely.

In preparation for construction of infinite unramified Galois extensions of algebraic number fields M/K with large $\rho(M/K)$, we extend a result of Martinet ([6]) for class field tower.

DEFINITION. Let K be an algebraic number field of finite degree, and p be a prime number. Let $\mathfrak{S}$ be a given set of finite primes of K and $K_\infty^{(p)}(\mathfrak{S})$ be the maximum unramified pro-p-extension in which all primes in $\mathfrak{S}$ decompose completely. When $K_\infty^{(p)}(\mathfrak{S})/K$ is infinite (resp. finite), we say that K has an infinite (resp. finite) $\mathfrak{S}$-decomposing p-class field tower.

NOTATION. For an algebraic number field of finite degree F, we denote by $r_1(F)$ (resp. $r_2(F)$) the number of real (resp. imaginary) primes of F. For a prime number p, $\delta_F^{(p)}$ denotes 1 or 0, according as F contains a primitive p-th root of unity or not.

Combining Ihara's remark ([5], § 14) to Golod-Šafarevič theory (cf. [7]) and Martinet's result ([6]), we easily obtain the following

THEOREM. *Let K/k be a cyclic extension of degree p (p: a prime number) of an algebraic number field of finite degree. Let $\mathfrak{S}$ be a given set of finite primes of K. Let r' be the number of those finite primes of k which are ramified in K and none of its extension to K belongs to $\mathfrak{S}$. If*

$$r' \geqq r_1+r_2+\delta_k^{(p)}+2-\rho+2\sqrt{H+p(r_1+r_2-\rho/2)+\delta_k^{(p)}},$$

then K has an infinite $\mathfrak{S}$-decomposing p-class field tower. Here ρ denotes the number of real primes of k which are ramified in K, $r_1=r_1(k)$, $r_2=r_2(k)$, and $H=|\mathfrak{S}|$.

§ 4. Construction of infinite unramified Galois extensions with large ratio of Ihara's inequality.

In this section, we shall give a way to construct infinite unramified Galois extensions M/K with large $\rho=\rho(M/K)$. We use the following

PROPOSITION. *Let $F=\boldsymbol{Q}(\sqrt{D})$ be a real quadratic number field with discriminant D. Let q_i ($1\leqq i\leqq t$) be prime numbers with the following properties:*

(1) $(D/q_i)=-1$ ($1\leqq i\leqq t$); *i.e., each q_i remains prime in F.*

(2) $-q_1q_2\cdots q_t\equiv 1 \pmod 4$.

Let K be the composite field of the imaginary quadratic number field $L=\boldsymbol{Q}(\sqrt{-q_1\cdots q_tD})$ and the absolute class field k of F. Let $\mathfrak{S}$ be a set of finite primes of K with $|\mathfrak{S}|=H$, satisfying the following conditions:

(3) *All primes in $\mathfrak{S}$ are prime to each q_i ($1\leqq i\leqq t$).*

(4) $th\geqq 3+2\sqrt{H+2h+1}$, *where h is the class number of F.*

Then K has an infinite $\mathfrak{S}$-decomposing 2-class field tower.

PROOF. We apply the theorem in § 3 to K/k. In this case,

$$r_1=\rho=[k:\boldsymbol{Q}]=2h,\quad r_2=0,\quad \delta_k^{(2)}=1;$$

hence it is sufficient to show that

$$r'\geqq 3+2\sqrt{H+2h+1}.$$

Therefore, by (4) we require only $r'\geqq th$. By (2), the finite primes of k which are ramified in K are the prime divisors of q_i ($1\leqq i\leqq t$). By (1) and class field theory, each q_i decomposes completely into h prime divisors in k. Hence $r'=th$.

Before constructing examples we give some remarks. The constant

$$\alpha_P=\log N(P)/(N(P)^{f(P)/2}-1)$$

decreases as $N(P)$ grows larger when $f(P)$ is fixed. Dividing two sides of Ihara's inequality by $n=[K:\boldsymbol{Q}]$, we obtain

$$\frac{1}{n}\sum_{P\in S}\alpha_P+\frac{r_1}{n}\alpha_r+\frac{r_2}{n}\alpha_i \leqq \frac{1}{2}\log D_K^{1/n},$$

where $r_1=r_1(K)$, $r_2=r_2(K)$, and

$$\alpha_r=\frac{1}{2}\left(\log 8\pi+\frac{\pi}{2}+\gamma\right)$$

$$\alpha_i=\log 8\pi+\gamma.$$

Therefore, in order to obtain examples of M/K with large $\rho(M/K)$ using Proposition, we should note the following two points:

(a) Take K with small root-discriminant $D_K^{1/n}$. It is easy to see that $D_K^{1/n}=(Dq_1\cdots q_t)^{1/2}$. Hence we need to take all q_i as small as possible.

(b) Take $\mathfrak{S}$ consisting of primes with small norm. Primes of K with small norm are prime divisors of primes of F decomposing completely in k. Therefore, we need to take D such that many small primes q satisfy $(D/q)=-1$.

With the above in mind, the author calculated some examples. From his observation, it seems that for our purpose we may restrict ourselves only to the case where

$$D=p\,(\text{prime})\equiv 1\,(\text{mod } 4),\qquad t=2,\qquad H>0$$

in the above proposition. In this case, (4) is equivalent to

(4)′ $$H-1\leqq h(h-5).$$

Now we give a way to construct required examples:

1° We first take a prime number $p\equiv 1$ (mod 4) such that $F=\boldsymbol{Q}(\sqrt{p})$ has a class number larger than four and among those prime numbers q with

(i) $$(p/q)=-1$$

there are small ones as 3, 5, 7, ⋯.

2° Let $h'=(h-5)/2$ (integer). Then (4) is equivalent to $H\leqq 2hh'+1$. Take the first $h'+3$ prime numbers satisfying (i), and denote by $\mathfrak{S}_0$ the set of these primes. From $\mathfrak{S}_0$ we select q_1 and q_2 such that $q_1q_2\equiv 3$ (mod 4), and put the others $q^{(1)}, q^{(2)}, \cdots, q^{(h'+1)}$, where $q^{(h'+1)}$ is the largest one.

3° Let K be the composite field of the absolute class field k of F and the imaginary quadratic number field $L=\boldsymbol{Q}(\sqrt{-q_1q_2p})$. It is easy to see from the choice of $q^{(s)}$ that each $q^{(s)}$ $(1\leqq s\leqq h'+1)$ decomposes in K as follows:

$$q^{(s)}=q_1^{(s)}q_2^{(s)}\cdots q_{2h}^{(s)},\quad N_{K/\boldsymbol{Q}}q_j^{(s)}=q^{(s)2}\qquad (1\leqq s\leqq h'+1,\ 1\leqq j\leqq 2h).$$

Let

$$\mathfrak{S}=\{q_j^{(s)}\ (1\leqq s\leqq h',\ 1\leqq j\leqq 2h),\ q_1^{(h'+1)}\}.$$

Then K has an infinite $\mathfrak{S}$-decomposing 2-class field tower.

4° Let $M=K_\infty^{(2)}(\mathfrak{S})$. Since $S\supset\mathfrak{S}$ (for definition of S, see § 2), we can calculate the lower bound of $\rho(M/K)$. Thus we have a required example M/K with large ρ, In fact, if $p<20000$, $h\geqq 13$, and $\mathfrak{S}_0\ni 3, 5, 7, 13, 17, 31$, then we have $\rho>0.87$.

We give three examples:

1. Let $p=15377$. Then $h=13$ (cf. [**9**]), $h'=4$, and

$$\mathfrak{S}_0=\{3, 5, 7, 11, 13, 37, 43\}.$$

Let $q_1=5$ and $q_2=7$. Then we obtain

$$\rho(M/K)\geqq 0.9115\cdots.$$

2. Let $p=65537$. Then $h=21$ (cf. [**9**]), $h'=8$, and

$$\mathfrak{S}_0=\{3, 5, 7, 11, 23, 29, 31, 41, 43, 47, 59\}.$$

Let $q_1=5$ and $q_2=7$. Then we obtain

$$\rho(M/K)\geqq 0.91079\cdots.$$

3. Let $p=13457$. Then $h=13$ (cf. [**9**]), $h'=4$, and

$$\mathfrak{S}_0=\{3, 5, 7, 13, 17, 31, 47\}.$$

Let $q_1=5$ and $q_2=7$. Then we obtain

$$\rho(M/K)\geqq 0.9059\cdots.$$

The value $0.9115\cdots$ in example 1 is much nearer to 1 than that given by Ihara's example. Therefore, this value seems to be helpful for further study.

References

[1] Y. Ihara, The congruence monodromy problems, J. Math. Soc. Japan, **20** (1968), 107-121.

[2] ———, Non-abelian classfields over function fields in special cases, Actes du Congrès Internat. Math. Nice 1970, Tome 1, Gauthier-Villars, Paris, pp. 381-389.

[3] ———, Congruence relations and Shimura curves, Proc. Sympos. Pure Math., **33**, Vol. 2, Amer. Math. Soc., 1979, pp. 291-311; II, J. Fac. Sci. Univ. Tokyo Sect. IA, **25** (1979), 301-361.

[4] ———, On unramified extensions of function field over finite fields, Advanced Studies in Pure Math., **2**, (the Proc. of Nagoya Symposium on Galois group and their applications 1981), Kinokuniya, Tokyo, 1983, pp. 89-97.

[5] ———, How many primes decompose completely in an infinite unramified Galois extension of a global field?, J. Math. Soc. Japan, **35** (1983), 683-709.

[6] J. Martinet, Tour de corps de classes et estimations de discriminants, Invent. Math.,

44 (1978), 65-73.

[7] P. Roquette, On class field towers, Algebraic Number Theory (Proc. of Instr. Conf. 1967), ed. Cassels and Fröhlich, Academic Press, pp. 231-249.

[8] K. Yamamura, On unramified extensions of algebraic number fields, Master's thesis, Univ. of Tokyo, 1984.

[9] H. Wada, A Table of Ideal Class Numbers of Real Quadratic Fields, Lecture Notes in Math., **10**, Sophia Univ., 1981.

Ken YAMAMURA
Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo 113
Japan