INFINITE CLASS FIELD TOWERS

JING LONG HOELSCHER

Abstract. This paper studies infinite class field towers of number fields $K$ that are ramified over $\mathbb{Q}$ only at one finite prime. In particular, we show the existence of such towers for a general family of primes including $p = 2, 3$ and $5$.

1. Introduction

This paper is concerned with number fields ramified only at one finite prime over $\mathbb{Q}$, which allow an infinite class tower. Suppose $K = K_0$ is an algebraic number field. For $i = 0, 1, 2, \ldots$, take $K_{i+1}$ to be the maximal abelian unramified extension of $K_i$, i.e. $K_{i+1}$ is the Hilbert class field of $K_i$. If there are no integers $i \geq 0$ such that $K_i = K_{i+1}$, we say that $K$ admits an infinite class field tower. I. R. Šafarevič gave an example of an infinite class tower of a number field ramified at seven finite primes over $\mathbb{Q}$ in [Sha]. More examples can be found in [GS], and [Ha], etc. Later René Schoof showed in [Sc] that $K = \mathbb{Q}(\zeta_{877}), \mathbb{Q}(\sqrt{-3321607}), \mathbb{Q}(\sqrt{39345017})$ and $\mathbb{Q}(\sqrt{-222637549223})$ each have an infinite class field tower where the only finite primes ramified in $K/\mathbb{Q}$ are respectively 877, 3321607, 39345017, 222637549223. In this paper we prove that either the cyclotomic field $K = \mathbb{Q}(\zeta_{p^m})$ or a degree $p$ extension $L$ of an unramified abelian extension $H$ of $K$ has an infinite class field tower under certain explicit conditions on the order of the class group of $K$. This yields a number field ramified only at one finite prime that has an infinite class field tower. The main theorem of this paper is:

**Theorem 1.1.** Let $p$ be a prime, suppose there exists a cyclotomic field $K = \mathbb{Q}(\zeta_{p^m})$ for some $m \in \mathbb{N}$ and a cyclic unramified Galois extension $H/K$ of prime degree $h$, which satisfy either of the following two conditions:

(I) $p \mid |Cl_H|$, $p$ is regular and $f_{p,h}^2 - 4f_{p,h} \geq 2h \cdot \varphi(p^m)$;

(II) $p \nmid |Cl_H|$ and $h \geq 2\varphi(p^{m+1}) + 4$,

where $f_{p,h}$ is the order of $p$ in $(\mathbb{Z}/h\mathbb{Z})^*$. Then there is a number field ramified only at $p$ and $\infty$ over $\mathbb{Q}$ that admits an infinite class tower.

As an application we will show:

**Theorem 1.2.** For $p = 2, 3$ and $5$, there exist algebraic number fields ramified over $\mathbb{Q}$ only at $p$ and $\infty$ which admit an infinite class tower.

2. Infinite class field towers

Let $K = \mathbb{Q}(\zeta_{p^m})$, and let $H$ be a cyclic unramified Galois extension over $K$ of prime degree $h$. Denote by $Cl_H$ the ideal class group of $H$. The principal prime ideal $(1 - \zeta_{p^m})$
in $K$ above $p$ splits completely as $(1 - \zeta_{p^m}) = \prod_{i=1}^h \mathfrak{p}_i$ in the subfield $H$ of the Hilbert class field of $\mathbb{Q}(\zeta_{p^m})$.

**Proposition 2.1.** Under condition (I) in Theorem 1.1, the number field $H$ has an infinite class tower.

*Proof.* Since $p\mid |Cl_H|$, we can pick a degree $p$ cyclic unramified extension $M_0/H$. If $M_0/K$ is Galois, the Galois group $\text{Gal} (M_0/K) \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/h\mathbb{Z}$ since $(p,h) = 1$. Now $p$ is regular, i.e. $p \nmid |Cl_{\mathbb{Q}(\zeta_p)}|$, by Theorem 10.4(a) in [Wa] we know $p$ does not divide the class number of $\bar{K} = \mathbb{Q}(\zeta_p)$. So the semi-direct product $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/h\mathbb{Z}$ is not abelian, we have a non-trivial homomorphism $\mathbb{Z}/h\mathbb{Z} \to \mathbb{Z}/(p-1)\mathbb{Z}$. So $\mathfrak{m}|(p-1)$, since $\mathfrak{m}$ is assumed to be a prime, i.e. the order $f_{(p,h)}$ of $\mathfrak{m}$ in $(\mathbb{Z}/h\mathbb{Z})^*$ is 1, in contradiction to the condition $f_{(p,h)}^2 - 4f_{(p,h)} \geq 2h\varphi(p^m)$.

Otherwise $M_0/K$ is non-Galois. Take the Galois closure $\bar{M}_0$ of $M_0/K$, which is the composite of all conjugates of $M_0$ over $K$. The Galois group $\text{Gal} (\bar{M}_0/H)$ is of the form $(\mathbb{Z}/p\mathbb{Z})^l$ for some $l \in \mathbb{N}$, and $\text{Gal} (\bar{M}_0/K) \cong (\mathbb{Z}/p\mathbb{Z})^l \rtimes \mathbb{Z}/h\mathbb{Z}$. The semi-direct product gives a non-trivial homomorphism $\mathbb{Z}/h\mathbb{Z} \to \text{GL}_l(\mathbb{F}_p) \cong \text{Aut}((\mathbb{Z}/p\mathbb{Z})^l)$, so $h \mid |\text{GL}_l(\mathbb{F}_p)| = (p^l-1)(p^l-p)\cdots (p^l-p^{l-1})$. Then $h \mid (p^{l-1})$, for some $i \leq l$, i.e. $p^i = 1$ mod $h$, and the order $f_{(p,h)}$ of $\mathfrak{m}$ in $(\mathbb{Z}/h\mathbb{Z})^*$ divides $i$. Thus $l \geq i \geq f_{(p,h)}$. So by the assumption we know $l^2 - 4l \geq 2h \cdot \varphi(p^m)$. On the other hand, there are $l$ linearly disjoint cyclic degree $p$ unramified extensions of $H$, i.e. $h_1 = \dim H^1(G, \mathbb{Z}/p\mathbb{Z}) \geq l$, where $G = \text{Gal} (\Omega_H/H)$ is the Galois group of the maximal unramified $p$-extension $\Omega_H$ of $H$. If $\Omega_H$ were finite, we would have $l^2 - l \leq h_1^2 - h_2 - h_1 \leq r_1 + r_2 = h\varphi(p^m)/2$, where the first inequality comes from the fact $M_0/K$ is non-Galois thus $h_1 \geq l \geq 2$. So $l^2 - 4l < 2h\varphi(p^m)$, contradiction. \(\square\)

From now on we will focus on the case under condition (II) in Theorem 1.1.

**Proposition 2.2.** Assume $p \nmid |Cl_H|$, then there exist a prime $\mathfrak{p}$ in $H$ above $p$ and an integer $k$ such that $p$ divides $|Cl_H^k|/|Cl_H|$, where $Cl_H^k$ is the ray class group of $H$ for the modulus $\mathfrak{p}^k$.

*Proof.* Suppose the conclusion were false. Then for any integer $k$ and any prime ideal $\mathfrak{p}_i$ in $H$ above $p$, we have $p \nmid |Cl_H^k|/|Cl_H|$. Taking the modulus $\mathfrak{m} = \mathfrak{p}_1^k \cdots \mathfrak{p}_h^k$ for $k \in \mathbb{N}$, we have the following exact sequence from class field theory

$$1 \rightarrow \mathcal{O}^* / \mathcal{O}^m \rightarrow (\mathcal{O}_H/\mathfrak{m})^* \rightarrow Cl_H^m \rightarrow Cl_H \rightarrow 1,$$

where $\mathcal{O}^*$, resp. $\mathcal{O}^m$, is the group of units in $\mathcal{O}_H$, resp. of units $\equiv 1$ mod $\mathfrak{m}$ in $\mathcal{O}_H$. Combining with Chinese Remainder Theorem, we have

$$|Cl_H^m|/|Cl_H| = |(\mathcal{O}_H/\mathfrak{m})^*| = \prod_{i=1}^h |(\mathcal{O}_H/\mathfrak{p}_i^k)^*| = \prod_{i=1}^h |\mathcal{O}^*/\mathcal{O}^p_i^k|.$$

So $p \mid |Cl_H^m|$. Taking $k = \varphi(p^m)k_0$ with $k_0 \in \mathbb{N}$, the modulus $\mathfrak{m} = \mathfrak{p}_1^k \cdots \mathfrak{p}_h^k = (1 - \zeta_{p^m})^k = (p)^{k_0}$ is a power of $p$. With the assumption $p \nmid |Cl_H|$, Equation (2.3) says that there are no totally ramified abelian $p$-extensions of $H$ that are ramified over $\mathbb{Q}$ only at $p$. 


That is contrary to the fact that $H(\zeta_p^m)/H$, with $a \in \mathbb{N}$ big enough, is a totally ramified $p$-extension ramified only at primes above $p$. 

By Proposition 2.2 above, we know there exists an integer $k$ and a prime, say $p_1$ above $p$ in $H$, such that $p | [O_{H_p}^k]/[O_H]$. Since $p$ does not divide the class number $[Cl_H]$, there exists a degree $p$ extension $H_1$ of $H$ ramified only at $p_1$. Since $H_1/H$ is a Kummer extension, $H_1$ is of the form $H(\sqrt[p]{x_i})$ for some $x_i \in O_H$. The conjugates of $H_i$ of $H_1$ over $\mathbb{Q}(\zeta_p)$ are degree $p$ extensions of $H$ ramified only at $p_1$, and they are of the form $H_i = H(\sqrt[p]{x_i})$ for some $x_i \in O_H$. If $x_1 \in p_1$, then $x_i \in p_1$ for $1 \leq i \leq h$ since $x_i$ are the conjugates of $x_1$; similarly if $x_1 \in O_H$, we will have $x_i \in O_H$ for any $1 \leq i \leq h$. We denote by $\delta_{H_i}(\sqrt[p]{x_i})/H_{p_i}$ and $\delta_{H_i}(\sqrt[p]{x_i})/H_{p_i}$ respectively the discriminants of the $p$-adic extension $H_{p_i}(\sqrt[p]{x_i})/H_{p_i}$ and $H_{p_i}(\sqrt[p]{x_i} \cdots \sqrt[p]{x_h})/H_{p_i}$. Let $L$ be the field $H(\sqrt[p]{x_1} \cdots \sqrt[p]{x_h})$.

PROPOSITION 2.4. $\delta_{L/H} = \prod_{i=1}^{h} \delta_{H(\sqrt[p]{x_i})/H_{p_i}}$.

Proof. The extension $H_i/H$ is ramified only at $p_i$, so the discriminant $\delta_{H_i/H}$ satisfies $\delta_{H_i/H} = \delta_{H_{p_i}(\sqrt[p]{x_i})/H_{p_i}}$. And for the discriminant of the extension $L/H$, we have $\delta_{L/H} = \prod_{i=1}^{h} \delta_{H_{p_i}(\sqrt[p]{x_i} \cdots x_i)/H_{p_i}}$. If suffices to show $\delta_{H_{p_i}(\sqrt[p]{x_i} \cdots x_i)/H_{p_i}} = \delta_{H_{p_i}(\sqrt[p]{x_i})/H_{p_i}}$.

We may assume the valuation $v_i = v_{p_i}O_{H_{p_i}}(x_i) \in \{0, 1\}$ by Lemma 2.1 of [Da]. The extension $H_{p_i}(\sqrt[p]{x_j})/H_{p_i}$ is unramified at $p_i$ when $j \neq i$, by Theorem 2.4 of [Da] $x_j$ is a $p$ power of a unit mod $(p_iO_{H_{p_i}})_{p_i}^m$.

Case (a). For all $1 \leq i \leq h$, $x_i \in p_i$. We have $x_1 \cdots x_h \in p_i$ and $v_{p_i}O_{H_{p_i}}(x_i) = v_{p_i}O_{H_{p_i}}(x_1 \cdots x_h)$, since $x_j$ is a unit in $O_{H_{p_i}}$ for $j \neq i$. By Theorem 2.4 of [Da] we know $\delta_{H_{p_i}(\sqrt[p]{x_1} \cdots x_i)/H_{p_i}} = \delta_{H_{p_i}(\sqrt[p]{x_i})/H_{p_i}}$.

Case (b). For all $1 \leq i \leq h$, $x_i \in O_{H_i}^*$. We know $x_j$ is a $p$th power mod $(p_iO_{H_{p_i}})_{p_i}^m$ for $j \neq i$. If we define

$$\kappa(x) = \max_{0 \leq t \leq p^m} \{l | \exists \gamma \in O_{H_{p_i}}^{*} : \gamma^p = x \ mod (p_iO_{H_{p_i}})^l\}$$

as a function of $x$, we have $\kappa(x_i) = \kappa(x_1 \cdots x_h)$. By Theorem 2.4 of [Da], again we get $\delta_{H_{p_i}(\sqrt[p]{x_1} \cdots x_i)/H_{p_i}} = \delta_{H_{p_i}(\sqrt[p]{x_i})/H_{p_i}}$.

We will show next that $L = H(\sqrt[p]{x_1} \cdots x_h)$ has many linearly disjoint unramified abelian extensions.

LEMMA 2.5. The extension $L(\sqrt[p]{x_i})/L$ is unramified for $1 \leq i \leq h$.

Proof. Let $M = H(\sqrt[p]{x_1}, \cdots, \sqrt[p]{x_h})$. We will show $M/L$ is unramified. Consider the discriminant of $M/H$. On the one hand, for each $1 \leq i \leq h$, $H_i/H$ is ramified only at $p_i$, so these extensions are linearly disjoint. The extension $M/H$, being the compositum of these extensions, has discriminant $\delta_{M/H} = \prod_{i=1}^{h} \delta_{H_i/H}^{p-1}$. On the other hand, considering
the tower of extensions $M/L/H$, we have by Proposition 2.3

$$\delta_{M/H} = \delta_{L/H}^{p_{M/H}^{-1}} N_{L/H}(\delta_{M/L}) = \left(\prod_{i=1}^h \delta_{H_i/H}ight)^{p_{M/H}^{-1}} N_{L/H}(\delta_{M/L}).$$

Comparing these two equations, we get $\delta_{M/L} = 1$, i.e. $M/L$ is unramified. □

**Proposition 2.6.** With the assumption of condition (II) in Theorem 1.1, the number field $L$ admits an infinite class tower.

*Proof.* Let $\Omega$ be the maximal unramified pro-$p$ extension of $L$, with Galois group $G = \text{Gal}(\Omega/L)$. We claim $\Omega/L$ is infinite. Suppose $\Omega/L$ were a finite extension. Then $G$ is a finite $p$-group and $\Omega$ admits no cyclic unramified extensions of degree $p$. By Proposition 29 in [Sh] we know that

$$h_2 - h_1 \leq r_1 + r_2 = r_2 = \frac{p\varphi(p^m)h}{2} = \frac{\varphi(p^{m+1})h}{2},$$

where $h_i = \text{dim} H^i(G, \mathbb{Z}/p\mathbb{Z})$, and $r_1, r_2$ denote the number of real places and pairs of complex places of $L$. By Lemma 2.5 we have $h$ linearly disjoint unramified $p$-extensions $L(\sqrt[p^m]{x_i})$ over $L$, so

$$h_1(G) \geq h.$$  

By the Šafarevič-Golod theorem (page 82 of [Sh]), we have

$$h_2 > \frac{h_2^2}{4}.$$  

Condition (II) says $h$ is a prime with $h(\geq 2\varphi(p^{m+1})+4) > 4$. Combining all the inequalities and the fact that the function $x^2 - 4x$ monotonically increases with $x$ if $x \geq 2$, we have $\frac{h_2^2}{4} - h \leq \frac{h_2^2}{4} - h_1 < h_2 - h_1 \leq \frac{\varphi(p^{m+1})h}{2}$, which implies $h < 2\varphi(p^{m+1}) + 4$, contradiction. □

Combining Proposition 2.6 and Proposition 2.1, we can conclude Theorem 1.1 in the introduction.

## 3. Examples for small primes

As a consequence of Theorem 1.1 we will verify in the cases $p = 2, 3, 5$ that there are number fields ramified only at $p$ and $\infty$ which have an infinite class tower. The following examples rely on Table 3 of [Wa] for the relative class number of the cyclotomic number field $K$, i.e. the ratio of the class number $|Cl_K|$ of $K$ and the class number $|Cl_{K^+}|$ of the maximal real subfield $K^+$. Also the computation of the order of the $f_{(p,h)}$ of $p$ in $(\mathbb{Z}/h\mathbb{Z})^*$ is done by [PARI2].

*Case $(p = 2)$.* Pick $K = \mathbb{Q}(\zeta_{128})$. The relative class number of $K$ is 359057 = 17 · 21121. Let $H$ be a subfield of the Hilbert class field of $K$ with $\text{Gal}(H/K) \cong \mathbb{Z}/21121\mathbb{Z}$. When $2 \mid |Cl_H|$, condition (I) in Theorem 1.1 is satisfied since 2 is regular and $f_{2,21121} = 10560$ thus $f_{2,21121}^2 - 4f_{2,21121} \geq 2 \cdot h \cdot \varphi(128)$; when $2 \nmid |Cl_H|$, condition (II) in Theorem 1.1 is satisfied since $h = 21121$ and thus $h \geq 2\varphi(2^8) + 4 = 260$. 


INFINITE CLASS FIELD TOWERS

|      | $K$          | $h$  | $f_{p,h}$ |
|------|--------------|------|-----------|
| $p = 2$ | $\mathbb{Q}(\zeta_{128})$ | 21121 | 10560 |
| $p = 3$ | $\mathbb{Q}(\zeta_{81})$ | 2593  | 648      |
| $p = 5$ | $\mathbb{Q}(\zeta_{125})$ | 20602801 | 10301400 |

Case $(p = 3)$. Pick $K = \mathbb{Q}(\zeta_{81})$. The relative class number of $K$ is 2593. Let $H$ an abelian unramified extension over $K$ with Galois group $\mathbb{Z}/2593\mathbb{Z}$. When $3 \mid |Cl_H|$, condition (I) in Theorem 1.1 is satisfied since 3 is regular and $f_{3,2593} = 648$ thus $f_{3,2593}^2 - 4f_{3,2593} \geq 2 \cdot h \cdot \varphi(81)$; when $3 \nmid |Cl_H|$, condition (II) in Theorem 1.1 is satisfied since $h = 2593$ thus $h \geq 2\varphi(3^4) + 4 = 112$.

Case $(p = 5)$. Pick $K = \mathbb{Q}(\zeta_{125})$. The relative class number of $K$ is $2801 \cdot 20602801$. Let $H$ be the subfield of the Hilbert class field of $K$ with $\text{Gal}(H/K) \cong \mathbb{Z}/20602801\mathbb{Z}$. When $5 \mid |Cl_H|$, condition (I) in Theorem 1.1 is satisfied since 5 is regular and $f_{5,20602801} = 103011400$ thus $f_{5,20602801}^2 - 4f_{5,20602801} \geq 2 \cdot h \cdot \varphi(125)$; when $5 \nmid |Cl_H|$, condition (II) in Theorem 1.1 is satisfied since $h = 20602801$ thus $h \geq 2\varphi(5^4) + 4 = 1004$.

All the cases above complete the proof of Theorem 1.2.

References

[Da] Mario Daberkow, On computations in Kummer Extensions, J. Symbolic Computation, 31 (2001), 113-131.
[GS] E. Golod and I. Šafarevič, On class field towers, Izv. Akad. Nauk SSSR, 28 (1964), 261-272 (Russian); English translation: Amer. Math. Soc. Transl. 48 (1965), 91-102.
[Ha] Hajir, Farshid, On a theorem of Koch, Pacific J. Math., 176 (1996), no. 1, 15-18.
[PARI2] The PARI-Group, PARI/GP, Version 2.3.1, Bordeaux, 2006, available from http://pari.math.u-bordeaux.fr/
[Sc] René Schoof, Infinite class field towers of quadratic fields, Journal fur die reine und angewandte Mathematik, (1986) 372, 209-220.
[Sh] Stephen S. Shatz, Profinite groups, arithmetic, and geometry, Annals of Mathematics Studies (67), Princeton University Press, (1972).
[Sha] I. R. Šafarevič, Algebraic number fields, Proc. Int. Congr. Math. Stockholm, (1962), 163-176 (Russian); English translation: Amer. Math. Soc. Transl., 31(2), 25-39.
[Wa] Lawrence C. Washington, Introduction to Cyclotomic Fields, Graduate Texts in Mathematics, Springer-Verlag, (1996).

UNIVERSITY OF ARIZONA, TUCSON, AZ 85721
E-mail address: jlong@math.arizona.edu