New York Journal of Mathematics

New York J. Math. **20** (2014) 27–33.

# On infinite class field towers ramified at three primes

**Jonah Leshin**

Abstract. For a prime $l \geq 3$, we construct a class of number fields with infinite $l$-class field tower in which only $l$ and two other primes ramify. As an application, we find an $S_3$ number field with infinite 3-class field tower with smallest known (to the author) root discriminant among all $S_3$ fields with infinite 3-class field tower.

Contents



## 1. Introduction

Let $K := K_0$ be a number field, and for $i \geq 1$, let $K_i$ denote the Hilbert class field of $K_{i-1}$ — that is, $K_i$ is the maximum abelian unramified extension of $K_{i-1}$. The tower $K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$ is called the Hilbert class field tower of $K$. If the tower stabilizes, meaning $K^i = K^{i+1}$ for some $i$, then the class field tower is finite. Otherwise, $\cup_i K^i$ is an infinite unramified extension of $K$, and $K$ is said to have infinite class field tower. For a prime $p$, we define the $p$-Hilbert class field of $K$ to be the maximal abelian unramified extension of $K$ of $p$-power degree over $K$. We may then analogously define the $p$-Hilbert class field tower of $K$. In 1964, Golod and Shafarevich demonstrated the existence of a number field with infinite class field tower [5]. This finding has motivated the construction of number fields with various properties that have infinite class field tower. One of Golod and Shafarevich's examples of a number field with infinite class field tower was any quadratic extension of the rationals ramified at sufficiently many primes, which was shown to have infinite 2-class field tower. An elementary

Received December 16, 2013; revised January 6, 2014.
2010 *Mathematics Subject Classification.* 11R29, 11R37.
*Key words and phrases.* Class field tower, ramification theory, root discriminant.

ISSN 1076-9803/2014

exercise shows that if $K$ has infinite class field tower, then any finite extension of $K$ does as well. Thus a task of interest becomes finding number fields of small size with infinite class field towers. The size of a number field $K$ might be measured by the number of rational primes ramifying in $K$, the size of the rational primes ramifying in $K$, the root discriminant of $K$, or any combination of these three.

With regard to number of primes ramifying, Schmithals [6] gave an example of a quadratic number field with infinite class field tower in which a single rational prime ramified. Odlyzko's bounds [4] imply that any number field with infinite class field tower must have root discriminant at least 22.3 (44.6 if we assume GRH); Martinet showed that the number field $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1}, \sqrt{46})$, with root discriminant $\approx 92.4$, has infinite class field tower [3]. The primes ramifying in this field are also "small."

Here we use a theorem of Schoof to produce a class of $\mathbb{Z}/l\mathbb{Z} \rtimes \mathbb{Z}/(l-1)\mathbb{Z}$ extensions of $\mathbb{Q}$ with infinite class field tower. Our fields are ramified at three primes including $l$. Our main theorem is the following.

**Theorem 1.** *Let $l$, $p$ be distinct primes and suppose that the class number $h$ of $\mathbb{Q}(\zeta_l, \sqrt[l]{p})$ is at least 3 if $l \geq 5$, and that $h \geq 6$ if $l = 3$, where $\zeta_l$ is a primitive $l$th root of unity. For infinitely many primes $q$, there exists $\delta \in \{p^a q^b\}_{1 \leq a,b \leq l-1}$ such that $\mathbb{Q}(\zeta_l, \sqrt[l]{\delta})$ has infinite $l$-class field tower.*

As a direct consequence of the proof of Theorem 1, we find that $\mathbb{Q}\big(\omega, \sqrt[3]{79 \cdot 97}\big)$ has infinite 3-class field tower.

## 2. Proof of Theorem 1

Our construction is analogous to that of Schoof [7], Theorem 3.4. From hereon, for a prime $l$, define

$$A_l = l\text{th powers in } \mathbb{Z}/l^2\mathbb{Z}.$$

We begin with a lemma.

**Lemma 1.** *Let $l$ be a prime and $n$ an integer prime to $l$. Let $\zeta_l$ be a primitive $l$th root of unity. The prime $(\zeta_l - 1)$ above $l$ of $\mathbb{Q}(\zeta_l)$ is unramified (and splits completely) in $\mathbb{Q}(\sqrt[l]{n}, \zeta_l)$ if and only if $n \in A_l$.*

**Proof.** This can also be deduced from [1, Theorem 119]. We provide our own proof for completeness.

Let $F = \mathbb{Q}(\zeta_l), M = F(\sqrt[l]{n})$. Let $\mathfrak{l} = (\zeta_l - 1)$ be the unique prime of $F$ above $l$. Suppose that $\mathfrak{l}$ were inert in $M$. Then there would only be a single prime of $M$, and therefore a single prime of $\mathbb{Q}(\sqrt[l]{n})$, lying over $l$. The extension $\mathbb{Q}(\sqrt[l]{n})/\mathbb{Q}$ cannot be unramified at $l$ since its compositum with its conjugates contains $\zeta_l$. But the extension cannot be totally ramified either since that would imply that $M/\mathbb{Q}$ has ramification degree $l(l-1)$ above $l$.

Therefore, either $M/\mathbb{Q}$ is totally ramified above $l$, or the ramification degree is $l-1$, in which case $l$ splits into $l$ primes in $M$. Suppose that we

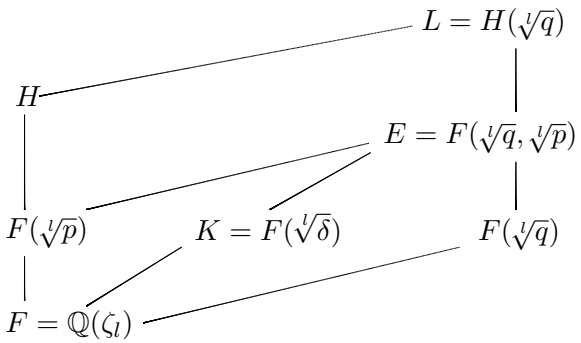


FIGURE 1. Field Diagram for Theorem 3.

are in the case of the latter, so each corresponding local extension of $M/\mathbb{Q}$ above $l$ is totally ramified of degree $l-1$. It follows that any prime $\mathfrak{l}'$ of $\mathbb{Q}(\sqrt[l]{n})$ above $l$ either splits completely in $M$ (the case $\mathbb{Q}(\sqrt[l]{n})_{\mathfrak{l}'} = M_{\tilde{\mathfrak{l}}}$, where $\tilde{\mathfrak{l}}|\mathfrak{l}$) or is totally ramified in $M$ (the case $\mathbb{Q}(\sqrt[l]{n})_{\mathfrak{l}'} = \mathbb{Q}_l$). Thus, there must be two primes above $l$ in $\mathbb{Q}(\sqrt[l]{n})$, one of which splits completely in $M$ and has ramification degree $l-1$ over $l$, and one of which ramifies completely in $M$ and is unramified over $l$ with residue degree 1. We have established:

$$\begin{aligned}\mathfrak{l} \text{ totally ramified in } M &\Leftrightarrow l \text{ totally ramified in } M\\ &\Leftrightarrow l \text{ totally ramified in } \mathbb{Q}(\sqrt[l]{n})\\ &\Leftrightarrow \text{no } l\text{th root of } n \text{ is contained in } \mathbb{Q}_l.\end{aligned}$$

Define $f(x) = x^l - n$, and let $\bar{f}$ denote its reduction modulo $l^3$. A root $\alpha$ of $\bar{f}$ satisfies $|f(\alpha)|_{\mathfrak{l}} < |f'(\alpha)|_{\mathfrak{l}}^2$, so by Hensel's lemma, $f(x)$ has a solution in $\mathbb{Q}_l$ if and only if $n$ is an $l$th power in $\mathbb{Z}/l^3\mathbb{Z}$, which is equivalent to $n$ being an $l$th power in $\mathbb{Z}/l^2\mathbb{Z}$. □

Let $p$ be any prime different from $l$, and let $h$ be the class number of $\mathbb{Q}(\zeta_l, \sqrt[l]{p})$ with $H$ its Hilbert class field. Let $q$ be a rational prime that splits completely in $H$, so by class field theory, $q$ is a prime that splits completely into principal prime ideals in $\mathbb{Q}(\zeta_l, \sqrt[l]{p})$. In particular, $q \equiv 1 \pmod{l}$, and thus by Lemma 1, $(1-\zeta_l)$ is totally ramified in $\mathbb{Q}(\zeta_l, \sqrt[l]{q})$ unless $q \equiv 1 \pmod{l^2}$. Set $F = \mathbb{Q}(\zeta_l), E = F(\sqrt[l]{p}, \sqrt[l]{q})$. In what follows, we find $\delta = \delta_{p,q} \in \{p^a q^b\}_{1 \le a,b \le l-1}$ so that $E$ is unramified over $K = K_\delta := F(\sqrt[l]{\delta})$ (see Figure 1).

**Case I.** $p \notin A_l$.

In this case, $(\zeta_l - 1)$ ramifies totally in $F(\sqrt[l]{p})$ by Lemma 1. By viewing $(\mathbb{Z}/l^2\mathbb{Z})^*$ as $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/(l-1)\mathbb{Z}$, we see there exists $a, b$ with $1 \leq a, b \leq l-1$ such that $p^a q^b \notin A_l$. Set

$$\delta = p^a q^b.$$

We claim that the ramification degree $e(E, l)$ of $l$ in $E$ is $l(l-1)$. Suppose for contradiction that this is not so, in which case we must have $e(E, l) = l^2(l-1)$. It follows from Lemma 1 that this is impossible if $q \in A_l$, so assume $q \notin A_l$. This means that the field $E$ has a single prime $\tilde{l}$ lying above $l$, and that $E_{\tilde{l}}/\mathbb{Q}_l$ is totally ramified. Since $q \equiv 1 \pmod{l}$ but $q \not\equiv 1 \pmod{l^2}$, there exists $c$ such that $pq^c \in A_l$. Set $\gamma = pq^c$, and let $E' = \mathbb{Q}(\zeta_l, \sqrt[l]{\gamma})$. The extension $E'/\mathbb{Q}(\zeta_l)$ is unramified above above $(\zeta_l - 1)$ by Lemma 1, a contradiction.

We claim that $E/K$ is unramified. Since $E$ is generated over $K$ by either $x^l - p$ or $x^l - q$, the relative discriminant of $E/K$ must be a power of $l$. Therefore, the only possible primes of $K$ that can ramify in $E$ are those lying above $l$. It is necessary and sufficient to show that $e(K, l) = l(l-1)$. By the definition of $\delta$ and Lemma 1, we know $(\zeta_l - 1)$ is totally ramified in $K_\delta$, from which it follows that $e(K, l) = l(l-1)$.

**Case II.** $p \in A_l$.

If $q \notin A_l$, Case I with the roles of $p$ and $q$ now reversed allows us to pick $\delta$ so that $E/K_\delta$ is unramified. If $q \in A_l$, then $E/F$ is unramified above $l$, so for any choice of $\delta \in \{p^a q^b\}_{1 \leq a,b, \leq l-1}$, $E/K_\delta$ is unramified.

We are now ready to invoke a theorem of Schoof [7]. First we set notation. Given any number field $H$, let $O_H$ denote the ring of integers of $H$. Let $U_H$ be the units in the idèle group of $H$– that is, the idèles with valuation zero at all finite places. Given a finite extension $L$ of $H$, we have the norm map $N_{U_L/U_H} : U_L \to U_H$, which is just the restriction of the norm map from the idèles of $L$ to the idèles of $H$. We may view $O_H^*$ as a subgroup of $U_H$ by embedding it along the diagonal. Given a finitely generated abelian group $A$, let $d_l(A)$ denote the dimension of the $\mathbb{F}_l$-vector space $A/lA$.

**Theorem 2** (Schoof, [7])**.** *Let $H$ be a number field. Let $L/H$ be a cyclic extension of prime degree $l$, and let $\rho$ denote the number of primes (both finite and infinite) of $H$ that ramify in $L$. Then $L$ has infinite $l$-class field tower if*

$$\rho \geq 3 + d_l\big(O_H^*/(O_H^* \cap N_{U_L/U_H} U_L)\big) + 2\sqrt{d_l(O_L^*) + 1}\,.$$

We apply Schoof's theorem to the extension $L := H(\sqrt[l]{q})$ over $H$, where $H$, as above, is the Hilbert class field of $F(\sqrt[l]{p})$. All $hl(l-1)$ primes in $H$ above $q$ ramify completely in the field $H(\sqrt[l]{q})$. Thus $\rho \geq hl(l-1)$, with strict inequality if and only if the primes above $l$ in $H$ ramify in $L$. By Dirichlet's unit theorem, $d_l(O_L^*) = \frac{1}{2}hl^2(l-1)$ and $d_l(O_H^*) = \frac{1}{2}hl(l-1)$. Thus, after some rearranging, we see that if $h$ and $l$ satisfy

$$\frac{1}{2}h(l-1) \geq \frac{3}{l} + 2\sqrt{\frac{1}{2}h(l-1) + \frac{1}{l^2}},$$

then $L$ will have infinite $l$-class field tower. If $l = 3$, the minimal such $h$ is given by $h = 6$. If $l \geq 5$, the minimal such $h$ is given by $h = 3$. Since $L/K$ is an unramified (as both $L/E$ and $E/K$ are unramified) solvable extension, it follows that $K$ has infinite class field tower as well.

This proves the following version of our main theorem.

**Theorem 3.** *Let $p$ and $l$ be distinct primes and suppose the class number $h$ of $\mathbb{Q}(\zeta_l, \sqrt[l]{p})$ satisfies $h \geq 3$ if $l \geq 5$, and satisfies $h \geq 6$ if $l = 3$. Let $q$ be a prime that splits completely into principal ideals in $\mathbb{Q}(\zeta_l, \sqrt[l]{p})$. Then there exists $\delta \in \{p^a q^b\}_{1 \leq a,b \leq l-1}$ such that $\mathbb{Q}(\zeta_l, \sqrt[l]{\delta})$ has infinite class field tower.*

**Remark 1.** By the Chebotarev density theorem, the density of such $q$ is $\frac{1}{l(l-1)h}$.

**Remark 2.** If $\delta \in A_l$ then $\delta^c \in A_l$ as well for all powers $c$. Thus, the proof of Theorem 3 goes through with $\delta$ replaced by $\delta^c$, and we always generate $l-1$ extensions of $\mathbb{Q}$ with Galois group $\mathbb{Z}/l\mathbb{Z} \rtimes \mathbb{Z}/(l-1)\mathbb{Z}$ unramified outside $\{l, p, q\}$ with infinite class field tower.

In the proof of Theorem 3, we were assuming that

$$d_l(O_H^*) = d_l(O_H^* \cap N_{U_L/U_H} U_L).$$

Let $x$ be an arbitrary element of $O_H^*$. We attempt to construct $y = (y_w) \in U_L$ such that $Ny = x$. Consider first the primes of $H$ that are unramified in $L$. Let $v$ be such a prime and suppose $\{w_1, \ldots, w_a\}$ ($a = 1$ or $l$) are the primes above $v$ in $L$. Because $v$ is unramified, the local norm map $N : O_{L_{w_i}}^* \to O_{H_v}^*$ is surjective, so we can pick $y_v \in L_{w_1}$ such that $Ny_v = x$. Put 1 in the $w_i$ components of $y$ for $i \geq 2$ if $a = l$.

Now let $v$ be a prime of $H$ that ramifies (totally) in $L$. If $v$ splits completely in $H(\sqrt[l]{O_H^*})$, then $\sqrt[l]{O_H^*} \in H_v$. Letting $w$ be the prime above $v$ in $L$, we set $y_w = \sqrt[l]{x}$. Putting the ramified and unramified components of $y$ together gives the desired element. The inequality needed for an infinite class field tower is then

$$h(l-1) \geq \frac{3}{l} + 2\sqrt{\frac{1}{2}h(l-1) + \frac{1}{l^2}},$$

which is satisfied by $h \geq 2$ if $l = 3$, and is satisfied with no restriction on $h$ if $l \geq 5$.

Suppose now that the primes of $H$ that ramify in $L$ split completely in $H(\sqrt[l]{O_H^*})$. If $p \in A_l$ and $q \notin A_l$, then ramification considerations show that the primes above $l$ in $H$ ramify in $L$; otherwise, the only primes in $H$ ramifying in $L$ are those above $q$. This gives us the following result.

**Theorem 4.** *Let $p$ be a prime with $p \notin A_l$. If $l \geq 5$, then for infinitely many primes $q$, there exists $\delta \in \{p^a q^b\}_{1 \leq a,b \leq l-1}$ such that $\mathbb{Q}(\zeta_l, \sqrt[l]{\delta})$ has infinite class field tower. If $l = 3$, the conclusion holds if we also assume that the class number of $\mathbb{Q}(\zeta_l, \sqrt[l]{p})$ is at least 2.*

**Proof.** For such $p$, the set of desired primes $q$ consists of all rational primes splitting completely in $H(\sqrt[3]{O_H^*})$. □

**2.1. The case $l = 3$.** We apply Theorem 3 in the case $l = 3$ to explicitly produce an infinite class field tower.

The field $\mathbb{Q}(\zeta_3, \sqrt[3]{79})$ has class number 12, and 97 splits completely into a product of principal ideals in this field [8], so we obtain:

**Corollary 1.** *The field $\mathbb{Q}\big(\omega, \sqrt[3]{79 \cdot 97}\big)$ has infinite 3-class field tower.*

## 3. Some other fields with infinite 3-class field tower

It is a Theorem of Koch and Venkov [9] that a quadratic imaginary field whose class group has $p$-rank three or larger has infinite $p$-class field tower. The table [2] of class groups of imaginary quadratic fields, although not constructed with the intent of producing number fields with infinite class field tower and small root discriminant, enables us to find a multitude of imaginary quadratic fields whose class group has 3-rank at least three, and thus have infinite 3-class field tower. From [2], we may conclude that the imaginary quadratic field with infinite 3-class field tower having smallest root discriminant is $\mathbb{Q}(\sqrt{-3321607})$, with root discriminant $\approx 1822.5$.

One may creatively use Schoof's theorem (Theorem 2) to construct various examples of number fields with infinite $l$-class field tower and small root discriminant. Below we outline an example for the case $l = 3$ that was communicated to the author by the referee.

Let $H$ be the subfield of the cyclotomic field $\mathbb{Q}(\zeta_{600})$ fixed by the order four automorphism $\zeta_{600} \mapsto \zeta_{600}^7$. By construction, the rational prime 7 splits completely in $H$ into 40 primes $\mathfrak{p}_i$. Now, let $K$ be the unique cubic subfield of $\mathbb{Q}(\zeta_7)$. All the $\mathfrak{p}_i$ ramify in $HK$, so the inequality in Theorem 2 implies that the 3-class field tower of $HK$ is finite. One checks that the root discriminant of $HK$ is $\approx 391.1$.

## References


[1] Hecke, Erich. Lectures on the theory of algebraic numbers. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen. Graduate Texts in Mathematics, 77. *Springer-Verlag, New York-Berlin*, 1981. xii+239 pp. ISBN: 0-387-90595-2. MR0638719 (83m:12001), Zbl 0504.12001.

[2] Jacobson Jr., Micheal J.; Ramachandran, Shantha; Williams, Hugh C. Supplementary tables for "Numerical results on class groups of imaginary quadratic fields", 2006. http://page.math.tu-berlin.de/~kant/ants/Proceedings/ramachandran-74/ramachandran-74-tables.pdf.

[3] Martinet, Jacques. Petits discriminants. *Ann. Inst. Fourier (Grenoble)*, **29** 1979, no. 1, xv, 159–170. MR0526782 (81h:12006), Zbl 0387.12006.

[4] Odlyzko, A. M. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Sém. Théor. Nombres Bordeaux* (2), **2** 1990, no. 1, 119–141. MR1061762 (91i:11154), Zbl 0722.11054.

[5] Roquette, Peter. On class field towers. *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)* 231–249. *Thompson, Washington, D.C.*, 1967. MR0218331 (36#1418).

[6] Schmithals, Bodo. Konstruktion imaginärquadratischer Körper mit unendlichem Klassenkörperturm. *Arch. Math. (Basel)* **34** (1980), no, 4, 307–312. MR0593948 (82f:12017), Zbl 0448.12008, doi: 10.1007/BF01224968.

[7] Schoof, René. Infinite class field towers of quadratic fields. *J. Reine Angew. Math.* **372** (1986), 209–220. MR0863524 (88a:11121), Zbl 0589.12011, doi: 10.1515/crll.1986.372.209.

[8] Stein, William; et al. Sage Mathematics Software, Version 5.10. *The Sage Development Team*, 2013. http://www.sagemath.org.

[9] Venkov, B. B.; Koh, H. The $p$-tower of class fields for an imaginary quadratic field. Modules and representations. *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* **46** (1974), 5–13, 140. MR0382235 (52 #3120), Zbl 0396.12010, doi: 10.1007/BF01085047.

151 Thayer Street, Providence, RI 02906
JLeshin@math.brown.edu

This paper is available via http://nyjm.albany.edu/j/2014/20-2.html.