On $S_3$-extensions with infinite class field tower

Jonah Leshin

May 11, 2014

Abstract

We construct a class of $S_3$-extensions of $\mathbb{Q}$ with infinite 3-class field tower in which only three primes ramify. As an application, we obtain an $S_3$-extension of $\mathbb{Q}$ with infinite 3-class field tower with smallest known (to the author) root discriminant among all fields with infinite 3-class field tower.

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 $K_0 \subseteq K_1 \subseteq K_2 \ldots$ 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, $\bigcup_i K^i$ 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 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. As for small primes ramifying, Hoelscher has given examples of number fields with infinite class field tower ramified only at $p$ for $p = 2, 3,$ and 5 [11]. 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].
In this note, we use a Theorem of Schoof to produce an infinite class of $S_3$ extensions of $\mathbb{Q}$ with infinite class field tower. Our fields are ramified at three primes, one of which is the prime 3. Our main theorem is

**Theorem 1.** Let $p \neq 3$ be prime and suppose the class number $h$ of $\mathbb{Q}(\omega, \sqrt[3]{p})$ is at least 6, where $\omega$ is a primitive third root of unity. For infinitely many primes $q$, there exists $\delta \in \{p^aq^b\}_{1 \leq a, b \leq 2}$ such that $\mathbb{Q}(\omega, \sqrt[3]{\delta})$ has infinite 3-class field tower.

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

## 2 Proof of Theorem 1

Our construction is analogous to that of Schoof [7], Theorem 3.4. We begin with a lemma.

**Lemma 1.** Let $p$ be a rational prime different from 3. The prime 3 ramifies totally in $\mathbb{Q}(\sqrt[3]{p})$ if and only if $p \not\equiv \pm 1 \pmod{9}$.

**Proof.** Since $[\mathbb{Q}(\sqrt[3]{p}) : \mathbb{Q}]$ is the sum of the local degrees $[\mathbb{Q}(\sqrt[3]{p})_{q_i} : \mathbb{Q}_3]$, where $q_i$ is a prime of $\mathbb{Q}(\sqrt[3]{p})$ above 3, we see that 3 is totally ramified in $\mathbb{Q}(\sqrt[3]{p})$ if and only if no third root of $p$ is contained in $\mathbb{Q}_3$. Consider the equation $x^3 - p \equiv 0 \pmod{27}$. This equation has a solution if and only if $p \equiv \pm 1, \pm 8, \pm 10 \pmod{27}$. For such $p$, $3p^2$ is divisible by exactly one power of 3. Thus, by Hensel’s lemma, we conclude that $\mathbb{Q}_3$ contains a cube root of $p$ exactly when $p \equiv \pm 1, \pm 8, \pm 10 \pmod{27}$. But these congruences are equivalent to the congruence $p \equiv \pm 1 \pmod{9}$. □

**Remark 1.** The same proof shows that Lemma 1 holds if $p$ is replaced by any integer that is prime to 3 and not a perfect cube.

Let $p$ be any prime different from 3, and let $h$ be the class number of $\mathbb{Q}(\omega, \sqrt[3]{p})$ 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 $\mathbb{Q}(\omega, \sqrt[3]{p})$. In what follows, we find $\delta = \delta_{p,q} \in \{p^aq^b\}_{1 \leq a, b \leq 2}$ so that $E$ is unramified over $K := F(\sqrt[3]{\delta})$ (see Figure 1).

Suppose that $p \not\equiv \pm 1 \pmod{9}$, so that 3 ramifies completely in $\mathbb{Q}(\sqrt[3]{p})$ by Lemma 1. Then either $pq \not\equiv \pm 1 \pmod{9}$ or $pq^2 \not\equiv \pm 1 \pmod{9}$ (or both). Pick $\delta = pq$ or $\delta = pq^2$ so that $\delta \not\equiv \pm 1 \pmod{9}$. Let $F = \mathbb{Q}(\omega)$ and $E = F(\sqrt[3]{p}, \sqrt[3]{q})$. The ramification degree $e(F(\sqrt[3]{p}), 3)$ of 3 in $F(\sqrt[3]{p})$ is 6.

We claim that $e(E, 3) = 6$. Suppose for contradiction that this is not so, in which case we must have $e(E, 3) = 18$. This means that the field $E$ has a single prime $I$ lying above 3, and that $[E_I : \mathbb{Q}_3] = [E : \mathbb{Q}]$, and likewise for every intermediate field between $\mathbb{Q}$ and $E$. One checks that at least one element of the set $\{q, pq, pq^2 \ (\text{mod 9})\}$ is congruent to $\pm 1 \ (\text{mod 9})$. Pick $\gamma \in \{q, pq, pq^2\}$ so that $\gamma \equiv \pm 1 \pmod{9}$. Let $E' = \mathbb{Q}(\sqrt[3]{\gamma})$. The extension $E'/\mathbb{Q}$ is
degree 3, but the corresponding extension of local fields is either degree one or two (depending on which prime above three in $E'$ one chooses). This gives the desired contradiction.

We claim that $E/K$ is unramified. Since $E$ is generated over $K$ by either $x^3 - p$ or $x^3 - q$, the relative discriminant of $E/K$ must divide the ideal $(3^3)$ of $K$. Therefore, the only possible primes of $K$ that can ramify in $E$ are those lying above 3. It is necessary and sufficient to show that $e(K, 3) = 6$. Since $\delta \not\equiv \pm 1 \pmod{9}$, Remark 1 shows that 3 is totally ramified in $\mathbb{Q}(\sqrt[3]{\delta})$, from which it follows that $e(K, 3) = 6$.

Suppose now that $p \equiv \pm 1 \pmod{9}$. If $q \not\equiv \pm 1 \pmod{9}$, take $\delta = pq$. The previous argument, with the roles of $p$ and $q$ now reversed, shows that $e(E, 3) = 6$ and that $E/K$ is unramified. If $q \equiv \pm 1 \pmod{9}$, then there is a prime of $\mathbb{Q}(\sqrt[3]{\delta})$ lying above 3 and unramified over 3, and likewise for $\mathbb{Q}(\sqrt[3]{p})$. It follows that $\mathbb{Q}(\sqrt[3]{p}, \sqrt[3]{q})$ also has a prime lying above 3 and unramified over 3, and from here that $e(E, \mathbb{Q}) = 2$. So in the case $p, q \equiv \pm 1 \pmod{9}$, we may take $\delta$ to be any element of $\{p^a q^b\}_{1 \le a, b \le 2}$, and $E/K$ will be unramified.

We are now ready to invoke the 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 $N_{U_L/U_H} : U_L \rightarrow U_H$, 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

$$\rho \ge 3 + d_l(O_H^*/(O_H^* \cap N_{U_L/U_H}U_L)) + 2 \sqrt{d_l(O_L^*)} + 1.$$
We apply Schoof’s theorem to the extension \( L := H(\sqrt[3]{79}) \) over \( H \), where \( H \), as above, is the Hilbert class field of \( F(\sqrt[3]{79}) \). All \( 6h \) primes in \( H \) above \( q \) ramify completely in the field \( H(\sqrt[3]{q}) \). Thus \( \rho \geq 6h \), with strict inequality if and only if the primes above 3 in \( H \) ramify. By Dirichlet’s unit theorem, \( d_3(O_L^*) = 9h \) and \( d_3(O_K^*) = 3h \). Thus if \( h \) satisfies \( 6h \geq 3 + 3h + 2\sqrt{9h+1} \), then \( L \) will have infinite 3-class field tower. 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. The minimal such \( h \) is given by \( h = 6 \).

This proves the following version of our main theorem:

**Theorem 3.** Let \( p \neq 3 \) be prime and suppose the class number \( h \) of \( \mathbb{Q}(\omega, \sqrt[3]{p}) \) is at least 6. Let \( q \) be a prime that splits completely into principal ideals in \( \mathbb{Q}(\omega, \sqrt[3]{p}) \). Then there exists \( \delta \in \{ p^a q^b \}_{1 \leq a, b \leq 2} \) such that \( \mathbb{Q}(\omega, \sqrt[3]{\delta}) \) has infinite class field tower.

**Remark 2.** By the Chebotarev density theorem, the density of such \( q \) is \( \frac{1}{6h} \).

**Remark 3.** Since \( \delta \equiv \pm 1 \pmod{9} \) if and only if \( \delta^2 \equiv \pm 1 \pmod{9} \), the proof of Theorem 3 goes through with \( \delta \) replaced by \( \delta^2 \). Thus we always generate at least two \( S_3 \) extensions of \( \mathbb{Q} \) unramified outside \( \{3, p, q\} \) with infinite class field tower.

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

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

**Remark 4.** 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. From the tables in [2], we see that the smallest known imaginary quadratic field with 3-rank at least three is \( \mathbb{Q}(\sqrt{-3321607}) \), with root discriminant \( \approx 1822.5 \). The field \( \mathbb{Q}(\omega, \sqrt[3]{79 \cdot 97}) \) has root discriminant \( \approx 1400.4 \).

We can bring down the requirement \( h \geq 6 \). The trade off is that we will have to assume

\[ \text{ The primes of } H \text{ that ramify in } L \text{ split completely in } H(\sqrt[3]{O_H^*}). \quad (1) \]

If \( p \equiv \pm 1 \pmod{9} \) and \( q \neq \pm 1 \pmod{9} \), then ramification considerations show that the primes above 3 in \( H \) ramify in \( L \); otherwise, the only primes in \( H \) ramifying in \( L \) are those above \( q \).

Suppose (1) holds. We claim that \( O_H^* \cap N_{U_L/U_H} U_L = O_H^* \). Let \( x \) be an arbitrary element of \( O_H^* \). We construct \( y = (y_v) \in U_L \) such that \( N y = x \). 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 3) are the primes above \( v \) in \( L \). Because \( v \) is unramified, the local norm map \( N : O_{L_w_v}^* \to O_{H_v}^* \) is surjective, so we can pick \( y_v \in L_{w_1} \) such that \( N y_v = x \). Put 1 in the \( w_2 \) and \( w_3 \) components of \( y \) if \( a = 3 \).

Now let \( v \) be a prime of \( H \) that ramifies in \( L \). The assumption that \( v \) splits completely in \( H(\sqrt[3]{O_H^*}) \) means that \( \sqrt[3]{O_H^*} \in H_v \). Letting \( w_1, w_2, w_3 \) be the primes above \( v \), we can put
$\sqrt{x}$ in the $w_1$ component and 1 in the $w_2$ and $w_3$ components of $y$. Putting the ramified and unramified components of $y$ together gives the desired element.

Under assumption (1), the inequality needed for $L$ to have an infinite class field tower now becomes

$$6h \geq 3 + 2\sqrt{9h} + 1,$$

which is satisfied by $h \geq 2$. This gives

**Theorem 4.** Let $p$ be a prime with $p \not\equiv \pm 1 \pmod{9}$. Either $\mathbb{Q}(\omega, \sqrt[3]{p})$ has class number one, or there exist infinitely many primes $\{q_p\}$ such that $\mathbb{Q}(\omega, \sqrt[3]{\delta_{p,q_p}})$ has infinite class field tower.

**Proof.** For such $p$, the set $\{q_p\}$ consists of all rational primes splitting completely in $H(\sqrt[3]{\mathbb{O}_H})$.

**References**

[1] Jing Long Hoelscher. Infinite class field towers. *Math. Ann.*, 344(4):923–928, 2009.

[2] Michael J. Jacobson Jr., Shantha Ramachandran, and Hugh C. Williams. 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] Jacques Martinet. Petits discriminants. *Ann. Inst. Fourier (Grenoble)*, 29(1):xv, 159–170, 1979.

[4] A. M. Odlyzko. 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(1):119–141, 1990.

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

[6] Bodo Schmithals. Konstruktion imaginärquadratischer Körper mit unendlichem Klassenkörperturn. *Arch. Math. (Basel)*, 34(4):307–312, 1980.

[7] René Schoof. Infinite class field towers of quadratic fields. *J. Reine Angew. Math.*, 372:209–220, 1986.

[8] W.A. Stein et al. *Sage Mathematics Software*. The Sage Development Team. http://www.sagemath.org.

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