INFINITE CLASS FIELD TOWERS OF NUMBER FIELDS OF PRIME POWER DISCRIMINANT

by

Farshid Hajir, Christian Maire, Ravi Ramakrishna

Abstract. — For every prime number p, we show the existence of a solvable number field L ramified only at $\{p, \infty\}$ whose p-Hilbert Class field tower is infinite.

For a number field L of degree n over $\mathbb{Q}$, the root discriminant is defined to be $D_{\mathrm{L}}^{1/n}$ where D_{L} is the absolute value of the discriminant of L. Given a finite set S of places of $\mathbb{Q}$, it is an old question as to whether there is an infinite sequence of number fields unramified outside S with bounded root discriminant. This question is related to the constants of Martinet [**8**] and Odlyzko's bounds [**10**]. Since the root discriminant is constant in unramified extensions, an approach to answering the previous question in the positive is to find a number field L (of finite degree) unramified outside S having an infinite class field tower. In the case of $\mathrm{K}/\mathbb{Q}$ quadratic, it is a classical result of Golod and Shafarevich that if $\mathrm{K}/\mathbb{Q}$ is ramified at at least 8 places, then K has an infinite class field tower. On the other hand, if p is a prime, and $S = \{p, \infty\}$, the question becomes whether there exist number fields with p-power discriminant having an infinite unramified extension. Schmitals [**11**] and Schoof [**12**] produced a few isolated examples of this type. See also [**3**], [**7**], etc. For $p \in \{2, 3, 5\}$, Hoelscher [**4**] announced the existence of number fields unramified outside $\{p, \infty\}$ and having an infinite Hilbert class field tower. Here we prove:

Theorem. — *For every prime number p, there exists a solvable extension* $\mathrm{L}/\mathbb{Q}$*, ramified only at $\{p, \infty\}$, having an infinite Hilbert p-class field tower. Consequently, there exists an infinite nested sequence of number fields of p-power discriminant with bounded root discriminant.*

Our proof is based on the idea of cutting of wild towers introduced in [**2**]; in particular it does not involve the usual technique of genus theory. For the more refined question where S consists of a single prime number p (i.e. if we focus our attention on totally real fields only), we do not know whether for every prime p, there is a totally real number field of p-power discriminant having an infinite Hilbert class field tower. In [**12**, Corollary 4.4] it is shown that $\mathbb{Q}(\sqrt{39345017})$ (which is ramified only at the prime 39345017) has infinite Hilbert class field tower. In [**13**], Shanks studied primes of the form $p = a^2 + 3a + 9$

We all thank Mathematisches Forschungsinstitut Oberwolfach for sponsoring a "Research in Pairs" stay during which this work was done. The second author was partially supported by the ANR project FLAIR (ANR-17-CE40-0012) and by the EIPHI Graduate School (ANR-17-EURE-0002). The third author was supported by Simons collaboration grant 524863.

and the corresponding totally real cubic subfields $\mathrm{K} \subset \mathbb{Q}(\mu_p)$ and showed the minimal polynomials of K are $x^3 - ax^2 - (a+3)x - 1$. Taking $a = 17279$ so $p = 298615687$, one can compute that the 2-part of the class group of K has rank 6. It is not hard to see, using the Golod-Shafarevich criterion, that K has infinite 2-Hilbert class field tower. Thus some examples exist in the totally real case.

1. The results we need

Let p be a prime number. Let $\mathrm{K}/\mathbb{Q}$ be a finite Galois extension. Assume $\mu_p \subset \mathrm{K}$ and moreover that K is totally imaginary when $p = 2$. For a prime $\mathfrak{p}$ of K dividing p denote by e (resp. f) the ramification index (resp. the residue degree) of $\mathfrak{p}$ in $\mathrm{K}/\mathbb{Q}$.

1.1. On the group G_S. — Denote by S the set of places of K above p, and consider K_S the maximal pro-p extension of K unramified outside S; put $\mathrm{G}_S = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$. Let $g = |S|$ be the number of places of K above p.
Let h'_{K} be the S-class number of K. By class field theory, h'_{K} is equal to $[\mathrm{K}' : \mathrm{K}]$ where K'/K is the maximal abelian of K unramified everywhere in which all places of S split completely. The Kummer radical of the p-elementary subextension $\mathrm{K}'(p)/\mathrm{K}$ of K'/K is

$$\mathrm{V}_S := \{x \in \mathrm{K}^\times \mid x\mathscr{O}_{\mathrm{K}} = \mathfrak{A}^p,\ x \in \mathrm{K}_v^{\times p}, \forall v \in S\}.$$

In particular $p \nmid h'_{\mathrm{K}}$ if and only if $\mathrm{V}_S/\mathrm{K}^{\times p}$ is trivial.

By work of Koch and Shafarevich the pro-p group G_S is finitely presented. More precisely, in our situation one has:

Theorem. — *Let $\mathrm{K}/\mathbb{Q}$ be a totally imaginary Galois extension containing μ_p. Let $S = \{p, \infty\}$. Then*

$$\dim H^1(\mathrm{G}_S, \mathbb{F}_p) = \frac{efg}{2} + 1 + \dim H^2(\mathrm{G}_S, \mathbb{F}_p)$$

and

$$\dim H^2(\mathrm{G}_S, \mathbb{F}_p) = g - 1 + \dim \mathrm{V}_S/\mathrm{K}^{\times p}.$$

Proof. — This is well-known, see for example [**9**, Corollary 8.7.5 and Theorem 10.7.3]. □

We immediately have:

Corollary 1.1. — *If $p \nmid h_{\mathrm{K}}$ then $\dim H^1(\mathrm{G}_S, \mathbb{F}_p) = g(\frac{ef}{2} + 1)$ and $\dim H^2(\mathrm{G}_S, \mathbb{F}_p) = g - 1$.*

1.2. The cutting towers strategy. —

1.2.1. The Golod-Shafarevich Theorem. — Let G be a finitely generated pro-p group. Consider a minimal presentation $1 \to \mathrm{R} \to \mathrm{F} \stackrel{\varphi}{\to} \mathrm{G}$ of G, where F is a free pro-p group. Set $d = d(\mathrm{G}) = d(\mathrm{F})$, the number of generators of G and F. Suppose that $\mathrm{R} = \langle \rho_1, \cdots, \rho_r \rangle^{Norm}$ is generated as normal subgroup of F by a finite set of relations ρ_i. We recall the depth function ω on F. See [**6**, Appendice] or [**5**] for more details. The augmentation ideal I of $\mathbb{F}_p[[\mathrm{G}]]$ is, by definition, generated by the set of elements $\{g - e\}_{g \in \mathrm{G}}$. Then for $e \neq g \in \mathrm{F}$, define $\omega(g) = \max_k \{g - e \in I^k\}$; put $\omega(e) = \infty$. It is not difficult to see that $\omega([g, g']) \geqslant 2$ and that $\omega(g^{p^k}) \geqslant p^k$ for every $g, g' \in \mathrm{G}$ and $k \in \mathbb{Z}_{>0}$. Observe also that as the presentation φ is minimal, $\omega(\rho_i) \geqslant 2$ for all the relations ρ_i.

The Golod-Shafarevich polynomial associated to the presentation φ of G is the polynomial $P_{\mathrm{G}}(t) = 1 - dt + \sum_i t^{\omega(\rho_i)}$.

***Theorem* (Golod-Shafarevich, Vinberg [14]).** — *If* G *is finite then* $P_{\mathrm{G}}(t) > 0$ *for all* $t \in]0,1[$.

Of course if we have no information about the ρ_i's we may take $1 - dt + rt^2$ (where $r = \dim H^2(G, \mathbb{F}_p)$) as Golod-Shafarevich polynomial for G: if $1 - dt + rt^2$ is negative at $t_0 \in]0,1[$, then $P_{\mathrm{G}}(t_0) < 0$ and G is infinite.

We can also define a depth function ω_{G} on G associated to its augmentation ideal. Then:

Proposition 1.2. — *For every* $g \in \mathrm{G}$, *one has*

$$\omega_{\mathrm{G}}(g) = \max\{\omega(y), \varphi(y) = g\}.$$

Proof. — See [**6**, Appendice 3, Theorem 3.5]. □

We now study quotients Γ of G such that $d(\mathrm{G}) = d(\Gamma)$. In this case, the initial minimal presentation of G induces a minimal presentation of Γ

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{R} & \longrightarrow & \mathrm{F} & \stackrel{\varphi}{\longrightarrow} & \mathrm{G} & \longrightarrow & 1 \\ & & & & & \searrow & \downarrow & & \\ & & & & & & \Gamma & & \end{array}$$

Suppose that $\Gamma = \mathrm{G}/\langle x_1, \cdots, x_m\rangle^{Norm}$. Here $\langle x_1, \cdots, x_m\rangle^{Norm}$ is the normal subgroup of G generated by the x_i's. Lift the x_i's to $y_i \in \mathrm{F}$ such that $\omega_{\mathrm{G}}(x_i) = \omega(y_i)$ for each i. Hence, $\Gamma = \mathrm{F}/\mathrm{R}'$, where $\mathrm{R}' = \mathrm{R}\langle y_1, \cdots, y_m\rangle^{Norm}$. In particular, if $\mathrm{R} = \langle \rho_1, \cdots, \rho_r\rangle^{Norm}$, then $\mathrm{R}' = \langle \rho_1, \cdots, \rho_r, y_1, \cdots, y_m\rangle^{Norm}$.
If we have no information about the ρ_i's, we can take $P_\Gamma(t) = 1 - dt + rt^2 + \sum_i t^{\omega(y_i)}$ as Golod-Shafarevich polynomial for Γ.

1.2.2. Cutting of G_S. — We want to consider some special quotients Γ of G_S, this is what we call "cutting wild towers".

Each place $v \in S$ corresponds to some extension $\mathrm{K}_v/\mathbb{Q}_p$ (in fact these fields are isomorphic as $\mathrm{K}/\mathbb{Q}$ is Galois) of degree ef. Then, as $\mu_p \subset \mathrm{K}_v$, the $\mathbb{F}_p$-vector space $\mathrm{K}_v^\times/\mathrm{K}_v^{\times p}$ has dimension $ef+2$, and local class field theory implies the Galois group of the maximal pro-p extension of K_v is generated by $ef+2$ elements. Thus the decomposition subgroup G_v of v in K_S/K is generated by at most $ef+2$ elements $z_{i,v}$. Consider now the commutators $[z_{i,v}, z_{k,v}]$ of all these elements; there are at most $\binom{ef+2}{2}$ such elements. Now we cut G_S by $\langle [z_{i,v}, z_{k,v}], i,k; v \in S\rangle^{Norm}$, and denote by Γ the corresponding quotient. As $\omega_{\mathrm{G}_S}([z_{i,v}, z_{k,v}]) \geqslant 2$, one can take $P_\Gamma = 1 - dt + rt^2 + g\binom{ef+2}{2}t^2$ as Golod-Shafarevich polynomial for Γ; here $d = \dim H^1(\mathrm{G}_S, \mathbb{F}_p)$ and $r = \dim H^2(\mathrm{G}_S, \mathbb{F}_p)$. This quotient Γ of G_S corresponds to the maximal subextension $\mathrm{K}_S^{loc-ab}/\mathrm{K}$ of K_S/K locally abelian everywhere. Observe that $\mathrm{K}_S^{loc-ab}/\mathrm{K}$ contains the compositum of all $\mathbb{Z}_p$-extensions.

Suppose that there exists some $t_0 \in]0,1[$ such that $P_\Gamma(t_0) < 0$. We will then cut the infinite pro-p group Γ by all the $z_{v,i}^{p^k}$ for some large k. There are $g(ef+2)$ such elements. Denote by Γ_k the new quotient and by $\mathrm{K}_S^{[k]}$ the new extension of K corresponding to Γ_k. Since $\omega_\Gamma(z_{v,i}^{p^k}) \geqslant p^k$, we may take $P_{\Gamma_k}(t) = P_\Gamma(t) + g(ef+2)t^{p^k}$ as the Golod-Shafarevich

polynomial for Γ_k. When k is sufficiently large, clearly $P_\Gamma(t_0) < 0 \implies P_{\Gamma_k}(t_0) < 0$, so $\mathrm{K}_S^{[k]}/\mathrm{K}$ is infinite.
The main interest of $\mathrm{K}_S^{[k]}/\mathrm{K}$ is:

Proposition 1.3. — *Suppose* $\mathrm{K}_S^{[k]}/\mathrm{K}$ *infinite. Then there exists a finite subextension* L/K *of* $\mathrm{K}_S^{[k]}/\mathrm{K}$ *having an infinite Hilbert p-class field tower.*

Proof. — In $\mathrm{K}_S^{[k]}/\mathrm{K}$ the (wild) ramification is finite: indeed for each $v \in S$, the decomposition groups in $\mathrm{K}_S^{[k]}/\mathrm{K}$ are abelian, finitely generated and of finite exponent. There exists a finite extension L/K inside $\mathrm{K}_S^{[k]}/\mathrm{K}$ absorbing all the ramification, so $\mathrm{K}_S^{[k]}/\mathrm{L}$ is unramified everywhere and infinite. □

2. Proof

Proposition 2.1. — *Let* $\mathrm{K}/\mathbb{Q}$ *be finite Galois with* $\mu_p \subset \mathrm{K}$. *Assume that* $g \geqslant 8$. *Then there exists a finite subextension* L/K *of* K_S/K *such that the Hilbert p-class field tower of* L *is infinite.*

Proof. — Let H be the "top" of the Hilbert Class Field Tower of K. If H/K is infinite, we are done, so suppose $[\mathrm{H}:\mathrm{K}] < \infty$. Note that H has class number 1 so by Corollary 1.1, working over H, $\dim H^1(\mathrm{G}_S, \mathbb{F}_p) = g\left(\frac{ef}{2}+1\right)$ and $\dim H^1(\mathrm{G}_S, \mathbb{F}_p) = g-1$. As in Section 1.2.2, consider the quotient Γ of G_S by the normal subgroup generated by the local commutators at each $v \in S$; one has $\binom{ef+2}{2}$ such commutators. The group Γ can be described by $d := g\left(\frac{ef}{2}+1\right)$ generators and by $r := g-1+g\frac{(ef+2)(ef+1)}{2}$ relations.
The Golod-Shafarevich polynomial of Γ may be written as $P_\Gamma(t) = 1 - dt + rt^2$, when assuming the worst case that all the relations are of depth 2. Clearly $d/2r < 1$, and $P_\Gamma(d/2r) = 1 - \frac{d^2}{4r}$. In particular, if $P_\Gamma(d/2r) < 0$, then one has room to cut by some large p-power of the local generators, in order to obtain at the end some finite local groups. For the result to follow, we thus need $4r < d^2$, or equivalently

$$4\left(g-1+g\frac{(ef+2)(ef+1)}{2}\right) \overset{?}{<} \frac{g^2}{4}(ef+2)^2$$

which is equivalent to

$$16(g-1)+8g(ef+2)(ef+1) \overset{?}{<} g^2(ef+2)^2.$$

Replacing the $16(g-1)$ term on the left by $16g$ and dividing by g, and setting $x = ef$, we need to verify

$$16+8(x+2)(x+1) \overset{?}{<} g(x+2)^2.$$

This holds for $g \geqslant 8$ and $x = ef \geqslant 1$. Proposition 1.3 allows us to conclude $\mathrm{K}_S^{[k]}/\mathrm{K}$ is infinite when k is sufficiently large. □

Proof Theorem : Recall that the principal prime $\mathfrak{p} = (1-\zeta_{p^s})$ of $\mathbb{Q}(\zeta_{p^s})$ is the unique prime dividing p and by class field theory $\mathfrak{p}$ splits completely in the Hilbert class field H of $\mathbb{Q}(\zeta_{p^s})$. Thus if the class group has order at least 8, Proposition 2.1 applied to the solvable number field H gives the result.

In the proof of [**15**, Corollary 11.17], the class number of $\mathbb{Q}(\zeta_{p^r})$ is shown to be at least 10^9 for $\phi(p^r) = p^{r-1}(p-1) > 220$. Choosing $r \geqslant 9$ for *any* p completes the proof of the Theorem.

A slightly more detailed analysis using Table §3 of [**15**] shows the fields below suffice:

p	K	$g = h$
$p > 23$	$\mathrm{K} = \mathbb{Q}(\zeta_p)$	$\geqslant 8$
$7 \leqslant p \leqslant 23$	$\mathrm{K} = \mathbb{Q}(\zeta_{p^2})$	$\geqslant 43$
$p = 5$	$\mathrm{K} = \mathbb{Q}(\zeta_{125})$	57708445601
$p = 3$	$\mathrm{K} = \mathbb{Q}(\zeta_{81})$	2593
$p = 2$	$\mathrm{K} = \mathbb{Q}(\zeta_{64})$	17

□

Remark 2.2. — In [**4**] a proof of the Theorem for $p = 2, 3$ and 5 was given. Our proof is partially modeled on the ideas there, namely considering the Hilbert class field of a cyclotomic field. There are two cases in [**4**]: Case I, where the Hilbert class field tower is infinite; and Case II, where ramification is allowed at one prime above p in the Hilbert class field H and a $\mathbb{Z}/p$-extension of H ramified at exactly this prime is used. Gras has given a criterion for such an extension to exist: see [**1**, Chapter V, Corollary 2.4.4]. Gras' criterion is not verified in [**4**]. Given the size of the number fields H, it seems very difficult to do so. We therefore we regard the results of [**4**] as incomplete.

References

[1] G. Gras, Class Field Theory, From Theory to practice, corr. 2nd ed., Springer Monographs in Mathematics, Springer (2005), xiii+507 pages.

[2] F. Hajir, C. Maire, R. Ramakrishna, *Cutting towers of number fields*, arXiv:1901.04354, 2019.

[3] F. Hajir and C. Maire, *Unramified subextensions of ray class field towers*, J. Algebra **249** (2002), no. 2, 528–543.

[4] J. L. Hoelscher, *Infinite class field towers*, Mathematische Annalen **344** (2009), 923-928.

[5] H. Koch, *Galois Theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag, Berlin 2002.

[6] M. Lazard, *Groupes analytiques p-adiques*, IHES, Publ. Math. **26** (1965), 389-603.

[7] J. Leshin, *On infinite class field towers ramified at three primes*, New York Journal of Math **20** (2014), 27-33.

[8] J. Martinet, *Tours de corps de classes et estimations de discriminants*, Inventiones math. **44** (1978), 65-73.

[9] J. Neukirck, A. Schmidt and K. Wingberg, Cohomology of Number Fields, GMW 323, Second Edition, Corrected 2nd printing, Springer-Verlag Berlin Heidelberg, 2013.

[10] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, J. Théor. Nombres Bordeaux **2** (1990), no. 2, 119-141.

[11] B. Schmithals, *Konstruktion imaginärquadratischer Körper mit unendlichem Klassenkörperturm*, (German) Arch. Math. (Basel) **34** (1980), no. 4, 307-312.

[12] R. Schoof, *Infinite class field towers of quadratic fields*, J. Reine Angew. Math. **372** (1986), 209-220.

[13] D. Shanks *The simplest cubic fields*, Mathematics of Computation, v.28, no. 128, 1137-1152 (1974).

[14] E. B. Vinberg, *On a theorem concerning on infinite dimensionality of an associative algebra*, Izv. Akad. Nauk SSSR Ser. Mat. **29** (1965), 208-214; english transl., Amer. Mat. Soc. Transl. (2) **82** (1969), 237-242.

[15] L. C. Washington, Introduction to Cyclotomic Fields, GTM 80, Second Edition, Springer, 1997.

April 14, 2019

Farshid Hajir, Christian Maire, Ravi Ramakrishna, Department of Mathematics, University of Massachussetts, Amherst, MA 01003, USA • FEMTO-ST Institute, Université Bourgogne Franche-Comté, CNRS, 15B avenue des Montboucons, 25000 Besançon, FRANCE • Department of Mathematics, Cornell University, Ithaca, USA • *E-mail :* `hajir@math.umass.edu`, `christian.maire@univ-fcomte.fr`, `ravi@math.cornell.edu`