Cutting towers of number fields

Farshid Hajir · Christian Maire · Ravi Ramakrishna

Received: 19 June 2020 / Accepted: 21 January 2021 / Published online: 22 February 2021
© Fondation Carl-Herz and Springer Nature Switzerland AG 2021

Abstract
Given a prime $p$, a number field $K$ and a finite set of places $S$ of $K$, let $K_S$ be the maximal pro-$p$ extension of $K$ unramified outside $S$. Using the Golod–Shafarevich criterion one can often show that $K_S/K$ is infinite. In both the tame and wild cases we construct infinite subextensions with bounded ramification using the refined Golod–Shafarevich criterion. In the tame setting we are able to produce infinite asymptotically good extensions in which infinitely many primes split completely, and in which every prime has Frobenius of finite order, a phenomenon that had been expected by Ihara. We also achieve new records on Martinet constants (root discriminant bounds) in the totally real and totally complex cases.

Keywords
Root-discriminant · Asymptotically good extensions · Golod–Shafarevich theorem

Mathematics Subject Classification
11R29 · 11R37 · 11R21

Résumé
Etant donnés un nombre premier $p$, un corps de nombres $K$ et un ensemble fini $S$ de places de $K$, soit $K_S$ la pro-$p$ extension maximale de $K$ non-ramifiée en dehors de $S$. À l’aide du critère de Golod–Shafarevich, on parvient souvent à montrer que l’extension $K_S/K$ est infinie. Dans les cas modéré et sauvage, nous construisons des sous-extensions infinies où la ramification est bornée, et ce à l’aide d’un raffinement du critère de Golod–Shafarevich. Dans le cas modéré, nous exhibons des extensions infinies et asymptotiquement bonnes pour lesquelles l’ensemble des premiers totalement décomposés est infini et où l’élément de Frobenius de chaque premier est fini, une possibilité qui avait été suggérée par Ihara. Nous établissons également de nouveaux records pour les constantes de Martinet (bornes sur le discriminant normalisé) dans les extensions totalement réelles ainsi que dans les extensions totalement complexes.

This work has been done during a visiting scholar position for the second author at Cornell University for the academic year 2017–2018, and funded by the program “Mobilité sortante” of the Région Bourgogne Franche-Comté; CM thanks the Department of Mathematics at Cornell University for providing a beautiful research atmosphere. Christian Maire was also partially supported by the ANR project FLAIR (ANR-17-CE40-0012) and by the EIPHI Graduate School (ANR-17-EURE-0002). Ravi Ramakrishna was supported by Simons Collaboration Grant 524863.

Extended author information available on the last page of the article
1 Introduction

Given a minimal presentation $(\mathcal{P})$ of a finitely generated pro-$p$ group $G$ with $d$ generators and $r$ relations, the well-known criterion of Golod–Shafarevich states that if $1 - dt + r t^2$ vanishes on $[0,1]$, then $G$ is infinite. In fact one may replace this polynomial with $P(\mathcal{P})(t) := 1 - dt + \sum_{k\geq 2} r_k t^k$, where $r_k$ is the number of relations in the presentation $(\mathcal{P})$ of depth $k$ in the Zassenhaus filtration. We may then employ the same vanishing test for infiniteness. See Sect. 2.

While all relations in a minimal presentation have depth at least 2, it is sometimes possible to find a presentation of a group with deep relations. Proving the group is infinite can be more tractable under these circumstances. Alternatively, one can take quotients (cutting) of an infinite group by deep elements and guarantee the quotient will be infinite. In the context of pure pro-$p$ group theory, Wilson in fact used the idea of cutting in [37].

The best uses of this refinement in number theory are probably the work on deep relations of Galois groups of Koch [20, Chapter 12], Koch and Venkov [21], Kisilevski and Labute [19] and Schoof [32].

Let $p$ be a prime number, $K$ a number field and $S$ a finite set of finite places of $K$. Denote by $K_S$ and $G_S$ the maximal pro-$p$ extension of $K$ unramified outside $S$ and $\text{Gal}(K_S/K)$ respectively. We make no assumption that $S$ contains any primes. Indeed, $S$ may be empty. When $G_S$ is infinite, we will exhibit some special infinite quotients of $G_S$. More precisely, by starting with an infinite tower $K_S/K$, we cut (quotient) $G_S$ in order to produce three kinds of results:

(i) Here we take $S$ coprime to $p$. We cut by Frobenii; this allows us to produce asymptotically good extensions where the set of places that split completely is infinite. It is necessary that these Frobenii have depth in $G_S$ going to infinity. We also cut by large $p$-powers of Frobenii to produce asymptotically good extensions in which every prime outside $S$ has Frobenius of finite order. These orders are not bounded. That the first type of example might exist is clear from the title of Ihara’s paper paper [17]. That the second type might exist is implicit in [17].

(ii) We cut by powers of the generators of tame inertia groups; this allows us to improve upon the results of Hajir-Maire [14] in the totally complex case and Martin [25] in the totally real case concerning Martinet constants (root discriminants) in infinite towers of number fields (also see [26]). We obtain bounds of $78,427$ and $857,567$ in the totally real and totally complex cases respectively. Our improvements towards the GRH lower bounds in these cases are, by one metric, about $7.55\%$ and $4.36\%$. In contrast, the improvements made in [14] over [26] were, respectively, $16.27\%$ and $6.54\%$;

(iii) In the wild ramification context, we cut by local commutators and powers of generators of the inertia group. This forces decomposition groups above $p$ to be abelian and have finite inertia subgroup. The root discriminants in the corresponding tower are then bounded. As an application, let $K$ be a totally imaginary number field of degree at least 12 and let $K_{Sp}$ be its maximal pro-$p$ extension ramified only at primes above $p$. Then, for infinitely many primes $p$ (assuming a recent conjecture of Gras concerning $p$-rational fields [8])

(a) the extension $K_{Sp}/K$ contains an infinite unramified tower of number fields,

(b) there exists a constant $\beta > 0$ and a sequence of $p$-rational number fields $(L_n)$ in $K_{Sp}/K$ such that $\log d_p Cl_{L_n} \gg (\log[\mathbb{L} : \mathbb{Q}])^\beta$, where $Cl_{L_n}$ is the class group of $L_n$. 

\textcopyright Springer
When the class group of a number field $L$ is not trivial, $p$-rationality of $L$ implies that the Hilbert $p$-class field $H$ of $L$ must be contained in the compositum of the $\mathbb{Z}_p$-extensions of $L$, a rare phenomenon. See [9, Chapter IV, Sect. 3] for a good explanation.

We also study the question of the depth of the generator $\tau_p$ of tame inertia in $G_S$. Let $T$ be a finite set of finite places of $K$, disjoint from $S$. Let $G_T^S$ be the quotient of $G_S$ by all the Frobenius elements of places of $T$. Then we prove that given $k > 0$ there exists a Chebotarev set of primes $\mathcal{D}$ with the following property: for every $q \in \mathcal{D}$ there are infinitely many primes $p$, coprime to $pq$ such that the depth of $\tau_p$ in $G_{\mathcal{D},q}$ is at least $k$ (see Theorem 12).

This work contains six sections, beginning with the Introduction. In Sect. 2 we recall the refined Golod–Shafarevich Theorem, and we indicate how we use it. We then develop asymptotically good extensions; in Sect. 4 to obtain the new root discriminant records in the question of the depth of tame inertia in $G_S$. Good references are [22, Appendice] and [20].

2 Depth of relations and the theorem of Golod–Shafarevich

Good references are [22, Appendice] and [20].
2.1 The Zassenhaus filtration

Consider a finitely generated pro-$p$ group $G$. Denote by $I := I_G$ the augmentation ideal of the completed algebra $\mathbb{F}_p[[G]]$, i.e., $I_G := \ker(\mathbb{F}_p[[G]] \to \mathbb{F}_p)$. The powers $I^n$ of $I$ are closed ideals and topologically finitely generated over $\mathbb{F}_p$.

**Definition 1** Given $x \in G$, $x \neq 1$, denote by $\omega(x) := \max \{n, x - 1 \in I^n\}$. We call the integer $\omega(x)$ the depth or level/weight of $x$. Put $\omega(1) = \infty$.

Recall the Zassenhaus filtration of $G$:

$$G_n = \{ g \in G, \omega(g) \geq n \}, \quad n \geq 1,$$

and that $I/I^2 \cong G/[G, G]G^p$, hence, $G_2 = [G, G]G^p$.

The sequence $G_n$ is a filtration of open normal subgroups of $G$.

**Proposition 1** One has the following properties:

(i) For $x \in G$, $\omega(x^p) \geq p \omega(x)$. Hence, if $x \in G_n$, then $x^p \in G_{np}$;

(ii) For $x \in G_n$ and $y \in G_m$, one has $[x, y] \in G_{n+m}$;

(iii) For $x, y \in G$, $\omega(xy) \geq \min(\omega(x), \omega(y))$.

**Proof** See Sect. 7.4 of [20].

Hence $\omega$ is a restricted filtration following the terminology of Lazard (see [22, Appendice A2, Définition 2.2 page 201]). In fact, one even has:

**Proposition 2** The Zassenhaus filtration of a pro-$p$ group $G$ is the minimal filtration on $G$ satisfying:

(i) $\omega(G) \geq 1$;

(ii) $\omega(x^p) \geq p \omega(x)$;

(iii) for all $v > 0$, $G_v := \{ x \in G, \omega(x) \geq v \}$ are closed.

**Proof** See Lazard [22, Appendice A2, Théorème 3.5, page 205].

2.2 The inequality

Let $G$ be a finitely generated pro-$p$ group of $p$-rank $d$. Let

$$1 \longrightarrow R \longrightarrow F \overset{\varphi}{\longrightarrow} G \longrightarrow 1$$

be a minimal presentation (物价) of $G$: here $F$ is a free pro-$p$ group on $d$ generators with its Zassenhaus filtration $\omega$.

Suppose that $R$ can be generated by $\{\rho_i, i = 1, \cdots\}$ as a normal subgroup of $F$. We denote $R = \langle \rho_i, i = 1, \cdots \rangle^N$. For $k \geq 1$, put

$$r_k = \#\{\rho_i, \omega(\rho_i) = k\}$$

and assume each $r_k$ is finite. Usually one assumes that $r_k = 0$ for large $k$, but this is not necessary and we will not do so in Theorem 4. We denote by

$$P_{\varphi}(t) := 1 - dt + \sum_{k \geq 2} r_k t^k \in \mathbb{R}[t]$$

a Golod–Shafarevich polynomial (in fact series) associated to this presentation (observe that $P_{\varphi}$ depends on the $\rho_i$). If we have no information about the depth of the relations of $R$, then we take $P_{\varphi}(t) = 1 - dt + r t^2$, where $r = d_p H^2(G)$ (when it is finite).
Theorem 1 (Vinberg [36]) If $G$ is finite, then

$$P_{\mathcal{F}}(t) > 0, \forall t \in ]0, 1[.$$ 

Proof Adapt the proof of [20], or see [1]. See also Anick [2].

Remark 1 One may have partial information on the depth of the relations. For example, assume that one has only $\omega(\rho_k) \geq a_k$ for all $k$. Then as $1 - dt + \sum \rho_k t^{a_k} \geq P_{\mathcal{F}}(t)$ (coefficient by coefficient), if $1 - dt + \sum \rho_k t^{a_k}$ has a root on $]0, 1[$, then $G$ is infinite. When one has to assume all relations are depth two, we obtain the Golod–Shafarevich inequality ‘$r \leq d^2/4$’ that guarantees $G$ is infinite. We say that $G$ passes the Golod–Shafarevich test if there exists $t_0 \in ]0, 1[$ such that $P_{\mathcal{F}}(t_0) < 0$. Observe that if $P_{\mathcal{F}}(t_0) = 0$ then $G$ is infinite, but for many of our applications we need some $t_0$ such that $P_{\mathcal{F}}(t_0) < 0$. Finally, it is known that if $G$ passes the Golod–Shafarevich test and $d > 2$, then $G$ is not analytic (see the exercise in annexe 3 of [34]).

2.3 Detecting the depth of an element

We start with a minimal presentation ($\mathcal{F}$) of $G$:

$$1 \rightarrow R \rightarrow F \xrightarrow{\varphi} G \rightarrow 1.$$ 

One has the following result that gives a relation between the Zassenhaus filtrations $\omega_F$ of $F$ and $\omega_G$ of $G$.

Proposition 3 The Zassenhaus filtration $\omega_G$ of $G$ coincides with the filtration quotient of the Zassenhaus filtration $\omega_F$ of $F$: for all $g \in G$, $\omega_G(g) = \max\{\omega_F(x), \varphi(x) = g\}$. Hence, for $n \geq 1,$

$$G_n \simeq F_n R / R \simeq F_n / F_n \cap R.$$ 

Proof See Lazard [22, Appendice 3, Théorème 3.5, page 205].

Definition 2 The Frattini series of a pro-$p$ group $G$ is defined by $\Phi_1(G) = G$ and $\Phi_{n+1}(G) = G^p [G_n, G_n].$

Given $g \in G$ and $x \in F$ such that $\varphi(x) = g$. Often, one wants to detect the depth of $x \in F$.

Proposition 4 Put $\varphi(x) = g \in G$ such that $\omega_G(g) = \omega_F(x).$ One has $\omega_F(x) \geq k$ if and only if $g \in G_k.$ In particular,

(i) $g \in G^p[G, G] \implies \omega_F(x) \geq 2$;
(ii) $g \in G^p_2[G, G_2] \implies \omega_F(x) \geq 3$;
(iii) $g \in \Phi_n(G) \implies \omega_F(x) \geq 2^{n-1}.$

Proof (i) Recall that $G_2 = G^p[G, G].$
(ii) Consider the $p$-central descending series $G_{(n)}.$ Then $G_{(n)} \subset G_n$ for all $n \geq 1$ (see for example Sect. 7 of [20]). Hence, if $g \in G_{(3)} = G^p_2[G, G_2],$ then $g \in G_3$ which is equivalent to $\omega_G(g) \geq 3$, and then $\omega_F(x) \geq 3$.
(iii) Clearly $\Phi_2(G) = G_2$ and as $\Phi_{n+1}(G) = (\Phi_n(G))^p[\Phi_n(G), \Phi_n(G)] \subset G_{2^n},$ the result follows.
2.4 On some special quotients of a pro-$p$ group $G$

We study some infinite quotients of $G$.

**Proposition 5** Take $(x_i)_{i \in I} \in G$ a family of elements of $G$ with $\omega_G(x_i) \geq 2$ for all $x_i$. Put $\Gamma := G/(x_i, i \in I)^N$. Suppose that $G$ is given by a minimal presentation $(\mathcal{P})$ with a Golod–Shafarevich polynomial $P_{\mathcal{P}}(t)$. Then for the natural minimal presentation

$$1 \longrightarrow \langle R, (y_i, i \in I) \rangle^N \longrightarrow F \longrightarrow \Gamma \longrightarrow 1$$

of $\Gamma$, where $y_i$ are chosen such that $\varphi(y_i) = x_i$ and $\omega_F(y_i) = \omega_G(x_i)$, a Golod–Shafarevich polynomial of $\Gamma$ for this presentation is $P_{\mathcal{P}}(t) + \sum_{i \in I} t^{\omega_G(x_i)}$.

**Proof** Obvious. \hfill $\square$

Much of what we need follows from this easy proposition:

**Proposition 6** Let $G$ be a finitely presented pro-$p$ group with a minimal presentation $(\mathcal{P})$ and a Golod–Shafarevich polynomial $P_{\mathcal{P}}(t)$ of $G$ (following $(\mathcal{P})$). Suppose that $P_{\mathcal{P}}(t_0) < 0$ for some $t_0 \in ]0, 1]$. Then for suitable $k \geq 2$ and $k' \geq 2$ we have $P_{\mathcal{P}}(t_0) + t_0^k < 0$ and $P_{\mathcal{P}}(t_0) + \frac{t_0^k}{1 - t_0} < 0$.

(i) Let $f \in F$ be such that $\omega_F(f) \geq k$. Then the group quotient $F/(R, f)^N \simeq G/\varphi(\langle f \rangle^N)$ is also infinite.

(ii) Take a sequence $(f_i)_{i \in F}$, $i \geq 0$, such that $\omega_F(f_i) \geq k' + i$. Then the group quotient $F/(R, f_i, i)^N \simeq G/\varphi(\langle f_i, i \rangle^N)$ is also infinite.

**Proof** Let us start with a minimal presentation $1 \longrightarrow R \longrightarrow F \longrightarrow \varphi \longrightarrow G \longrightarrow 1$ of $G$.

(i) When one adds a relation of depth at least $k \geq 2$, the $p$-rank does not change. Take now the following minimal presentation $(\mathcal{P}')$ of $\Gamma$:

$$1 \longrightarrow R' \longrightarrow F \longrightarrow \Gamma \longrightarrow 1,$$

where $R' = \langle f, \rho_1, i \rangle^N$, the $\rho_1$ being some generators of $R$ as normal subgroup of $F$. Now, a polynomial of Golod–Shafarevich for $\Gamma$ and $(\mathcal{P}')$ can be written as (thanks to Proposition 5) $P_{\mathcal{P}'}(t) = P_{\mathcal{P}}(t) + i^k$. But $k$ is chosen so that $P_{\mathcal{P}'}(t_0) < 0$, and hence Theorem 1 gives that $\Gamma$ is infinite.

(ii) Put $\Gamma := G/\varphi(\langle f_i, i \rangle^N)$. First, as the elements $f_i$ are in $F_{k' + i}$, with $k' + i \geq 2$, then $d_p R' = d_p G = d$. As in (i), take now the following minimal presentation $(\mathcal{P}')$ of $\Gamma$:

$$1 \longrightarrow R' \longrightarrow F \longrightarrow \Gamma \longrightarrow 1,$$

where $R' = \langle \rho_j, f_i, i, f \rangle^N$, the $\rho_j$ being some generators of $R$ as normal subgroup of $F$. Now, a polynomial of Golod–Shafarevich for $\Gamma$ and $(\mathcal{P}')$ can be written as (thanks to Proposition 5):

$$P_{\mathcal{P}'}(t) \leq P_{\mathcal{P}}(t) + i^k \sum_{i \geq 0} i^i = P_{\mathcal{P}}(t) + i^k \frac{1}{1 - t},$$

which is negative at $t = t_0$ by assumption. Apply Theorem 1 as in (i). \hfill $\square$
Sometimes one can say a little bit more. As usual, let \( d \) and \( r \) be the number of generators and relations of \( G \). Set \( a = 2r/d \). Suppose \( a > 1 \) and put

\[
\lambda = \begin{cases} 
\lfloor a \rfloor & a \notin \mathbb{Z} \\
 a - 1 & a \in \mathbb{Z}_{>0}
\end{cases}.
\]

Choose now \( m \in \mathbb{Z}_{\geq 2} \) such that

\[
1 - \frac{d^2}{4r} \left( \frac{\lambda}{a} \right)^m + \frac{\left( \frac{\lambda}{a} \right)^m}{1 - \frac{\lambda}{a}} < 0.
\]

**Lemma 1** Let \( G \) be a finitely presented pro-\( p \) group such that \( r < d^2/4 \) and \( 2r/d > 1 \). Take \( \lambda \) and \( m \) as above. For \( k \geq 0 \), take distinct elements \( f_{j,k} \in F \) with \( j = 1, \ldots, \lambda^{k+m} \), such that \( \omega_f(f_{j,k}) \geq m+k \). Then the group quotient \( G/\phi(\langle f_{j,k}, j, k \rangle) \) is also infinite.

**Proof** Put \( \Gamma := G/\phi(\langle f_{j,k}, j, k \rangle) \). As before the new relations all have depth at least two so \( d_p \Gamma = d_p G = d \). Take for \( G \) the polynomial \( P_\phi(t) = 1 - dt + rt^2 \). Here, a Golod–Shafarevich polynomial \( P_\phi' \) of \( \Gamma \) can be taken as

\[
P_\phi'(t) = P_\phi(t) + \sum_{k \geq 0} \lambda^{m+k} t^{m+k}.
\]

As \( \lambda < 2r/d \), the series converges in the neighborhood of \( t_0 = d/2r \). Hence, one has:

\[
P_\phi'(d/2r) \leq 1 - \frac{d^2}{4r} + \frac{\left( \frac{\lambda}{a} \right)^m}{1 - \frac{\lambda}{a}} < 0,
\]

and Theorem 1 applies. \( \square \)

In Galois contexts the quotients of Propositions 5 and 6 correspond to subextensions, so we will use the term ‘cut’ to apply both to Galois groups and the corresponding towers of fields.

### 3 Splitting in infinite subextensions of \( K_S/K \)

In this section we address the question in the title of Ihara’s paper [17], namely we give examples of an infinite unramified algebraic extension of a number field in which infinitely many primes split completely. We also give examples where all primes have Frobenius with finite order, though these orders are not uniformly bounded.

#### 3.1 Wilson’s result

Our main result, Theorem 4, builds on a group-theoretic result of Wilson [37], the number-theoretic interpretation of which we give below.

**Theorem 2** Let \( K \) be a number field, and \( S \) be a finite set of places of \( K \) coprime to \( p \). Suppose that \( G_S \) passes the test of Golod–Shafarevich (which is the case if \( d_p G_S > \alpha_{K,S} \)). Then there exists an infinite pro-\( p \) extension \( \tilde{K}/K \) in \( K_S/K \) where all Frobenius elements of primes outside of \( S \) are torsion.
Proof Let $P_{\gamma}(t)$ be a Golod–Shafarevich polynomial of $G_S$ for which $G_S$ passes the test. Let $x_1, x_2, \ldots$ be an enumeration of all Frobenii of primes not in $S$. By hypothesis $P_{\gamma}(t_0) = -\delta < 0$ for some $t_0 \in ]0, 1[$. Using Proposition 1 (i) and Proposition 6 we can add in a relation corresponding to a suitable $p$-power of $x_1$ so that the new Golod–Shafarevich polynomial with this relation imposed is $P_{\gamma}(t) + t^{k_1}$ and $P_{\gamma}(t_0) + t_0^{k_1} < -\delta/2$. Now add in a suitable relation corresponding to a power of $x_2$ and the new Golod–Shafarevich polynomial with this relation imposed is $P_{\gamma}(t) + t^{k_1} + t^{k_2}$ and $P_{\gamma}(t_0) + t_0^{k_1} + t_0^{k_2} < -\delta/2$. Continuing on with powers of $x_3, x_4$ etc. the resulting series, $\tilde{P}_{\gamma}(t)$ satisfies $\tilde{P}_{\gamma}(t_0) \leq -\delta/2 < 0$ so the corresponding quotient of $G_S$, fixing $K$, is infinite. By construction, the Frobenius of any unramified prime in this quotient is torsion. □

Remark 2 For extensions for which Frobenius elements have uniformly bounded orders see Checcoli [4].

Remark 3 Note that every $p$-adic analytic quotient of the infinite quotient that appears in Theorem 2 is finite: this is more or less obvious, due to the fact that an infinite $p$-adic analytic group has an open subgroup of finite cohomological dimension and is then torsion free (note here, we can do the same operation with $G_{S_p}$).

3.2 Main result

Definition 3 Let $K$ be a number field and let $L/K$ be a (possibly infinite) algebraic extension. The root discriminant of $K$ is $rd_K := |Disc(K)|^{1/[K:Q]}$. The root discriminant of $L/K$ is $\lim sup_J |Disc(J)|^{1/[J:K]}$ where $L \supset J \supset K$ and $[J : K] < \infty$.

Definition 4 An infinite Galois extension $L/K$ is called asymptotically good if its root discriminant is finite.

Given a (possibly infinite) Galois extension $L/K$, and a prime $p$ of $K$, let $f(p)$ be the residue degree extension of $p$ in $L/K$.

Put $\mathcal{P}_{L/K} = \{ p \subseteq \mathcal{O}_K \mid p \text{ a prime ideal}, f(p) < \infty \}$.

We introduce the estimate given by Ihara in [17]. See also Tsfasman and Vladut [35]. Let $\gamma$ be Euler’s constant and for an infinite place $v$ of $K$ set

$$\alpha_v = \begin{cases} \frac{1}{2} (\log(8\pi) + \gamma + \frac{3}{2}) & \text{if } v \text{ is real,} \\ \log(8\pi) + \gamma & \text{if } v \text{ is imaginary.} \end{cases}$$

Theorem 3 Let $L/K$ be an infinite asymptotically good extension. Then (assuming the GRH),

$$\lim_{X \to \infty} \sum_{p \in \mathcal{P}_{L/K}(X)} \frac{\log N(p)}{N(p)^{f(p)/2} - 1} \sum_{v|\infty} \alpha_v \leq \frac{\log |Disc(K)|}{2}.$$ 

(For an unconditional estimate, remove the square root in the denominator.)

Theorem 2 produces asymptotically good extensions $L/K$ where $\mathcal{P}_{L/K}$ is maximal, namely it consists of all primes of $\mathcal{O}_K$ except the finite set of ramified primes in $L/K$ ($L/K$ asymptotically good implies only finitely many primes ramify). This had been suspected by Ihara in [17]. In fact we can do more.

Let

$$\mathcal{P}_{L/K} = \{ p \subseteq \mathcal{O}_K \mid p \text{ a prime ideal}, f(p) = 1 \},$$
be the set of prime ideals \( p \) of \( K \) that split completely in \( L/K \). Using Proposition 6, we will exhibit an asymptotically good extension \( L/K \) for which \( \mathcal{S}_{L/K} \) is infinite.

**Theorem 4** Let \( K \) be a number field, and \( S \) be a finite set of places of \( K \) coprime to \( p \). Suppose that \( d_p G_S > \alpha K . S \). Then there exist infinite pro-\( p \) extensions \( L/K \) in \( K_S/K \) and \( L'/K \) in \( L/K \) such that:

(i) the set \( \mathcal{S}_{L/K} \) is infinite;

(ii) the set \( \mathcal{S}_{L'/K} \) contains all primes not in \( S \); in particular \( \mathcal{S}_{L'/K} \) contains all primes when \( S = \emptyset \).

**Proof** Let \( 1 \rightarrow R \rightarrow F \xrightarrow{\varphi} G_S \rightarrow 1 \) be a minimal presentation of \( G_S \). By hypothesis \( r < d^2/4 \). Take \( P_\varphi(t) = 1 - dt + rt^2 \) as a Golod–Shafarevich polynomial, and note that \( P_\varphi(d/2r) = 1 - d^2/4r < 0 \). We will apply Proposition 6 \((ii)\) with \( t_0 = d/2r \in ]0, 1[ \) and \( k' \) as given there. We will take the quotient by infinitely many Frobenii \( x_i \) of unramified primes whose depth is at least \( k' + i \) in \( G_S \). For \( i \geq 2 \), denote by \( G_i \) the image \( \varphi(F_i) \); Proposition 3 gives that \( G_i \) is also the Zassenhaus filtration of \( G_S \). Now, for \( i \geq 0 \), choose a prime ideal \( p_i \) of \( G_K \) such that its Frobenius \( x_i \) is in \( G_k+i \) (in fact a conjugacy class there), and such that \( p_i \notin \{ p_0, \ldots , p_{i-1} \} \). Choose \( y_i \in F_{k'+i} \) such that \( \varphi(y_i) = x_i \) so \( \omega_y(y_i) \geq k' + i \). The quotient \( \Gamma \) of \( G_S \) by the normal subgroup generated by the Frobenius \( x_i \) of the primes \( p_i \), \( i \geq 0 \) is

\[ \Gamma \simeq G_S/(x_i, i)^N \simeq F/(R, y_i, i)^N. \]

Denote by \( L \subset K_S \) the fixed field by \( \langle x_i, \ i \geq 0 \rangle^N \); \( \text{Gal}(L/K) \simeq \Gamma \). By Proposition 6 \((ii)\), the pro-\( p \) extension \( L/K \) is infinite, and each prime \( p_i \) has trivial Frobenius in \( L \) and thus splits completely; in other words \( \mathcal{S}_{L/K} \) is infinite. Observe now that we can take

\[ P(t) = 1 - dt + rt^2 + \sum_{m \geq k} t^m = 1 - dt + rt^2 + \frac{t^k}{1 - t} \]

as a Golod–Shafarevich series for \( L/K \); here \( k \) has been taken such that \( P(t_0) < 0 \), where \( t_0 = d/2r \in ]0, 1/2[ \). This settles \((i)\).

For \((ii)\) one need only apply Theorem 2 to \( L/K \) to obtain a subextension \( L'/K \) of \( L/K \) for which \( \mathcal{S}_{L'/K} \) contains all primes not in \( S \).

**Remark 4** The difference between the left and right hand sides of Theorem 3 is called the **deficiency** of the tower \( L/K \). Theorem 4 is particularly interesting in the context of Tsfasman and Vladut [35] where the deficiency of towers of global fields is extensively studied. See also Lebacque [23].

In Theorem 4 one can say a little bit more about \( \mathcal{S}_{L/K} \). For a (possibly infinite) Galois extension \( L/K \) of a number field \( K \), and for \( X \geq 0 \), put

\[ \mathcal{S}_{L/K}(X) := \{ p \in \mathcal{S}_{L/K}, \ N(p) \leq X \}, \text{ and } \pi_{L/K}(X) = |\mathcal{S}_{L/K}(X)|. \]

The effective version of Chebotarev’s Theorem allows us to give an upper bound for \( \pi_{L/K}(X) \) when the extension \( L/K \) is asymptotically good. Indeed:

**Proposition 7** If \( L/K \) is Galois and asymptotically good, there exists a constant \( B \geq 0 \) such that for \( X \geq 2 \) (assuming the GRH),

\[ \pi_{L/K}(X) \leq CX^{1/2} \left( |K:\mathbb{Q}| \log X + \log |\text{Disc}(K)| + B \right), \]

where \( C \) is an absolute constant. When \( L/K \) is unramified, one can take \( B = 0 \).
3.3 Norm of ideals in \( K_S/K \)

For this subsection we suppose \( G_S \) is tame and infinite and set \( G := G_S \) and \( G_n \) to be the \( n \)th group in its Zassenhaus filtration. Suppose also that \( r < d^2/4 \) so the pro-\( p \) group \( G \) is not analytic and \( G_n \neq G_{n+1} \) for all \( n \) (see [5, Chapter 11, Theorem 11.4]).

**Remark 5** When \( G := G_S \) is tame and infinite, the tame Fontaine–Mazur conjecture [7, Conjecture (5a)] implies it is not analytic and then \( G_n \neq G_{n+1} \) for all \( n \).

**Definition 5** For a prime \( p \notin S \), denote by \( x_p \) the Frobenius at \( p \) in \( G \). Define for \( n \geq 1 \),

\[
N_n := \min\{N(p), x_p \in G_n \setminus G_{n+1}\}.
\]

Recall local different in tamely ramified extensions of inertial degree \( e \) have exponent \( e - 1 \). Using this fact, it is an easy exercise to show that pro-\( p \) extensions of a number field that are tamely ramified at a finite set of places are always asymptotically good. One can produce asymptotically good extensions where the set of primes that splits completely is infinite, and in particular, by our construction, the series \( \sum_{n \geq 2} \frac{\log N_n}{\sqrt{N_n}} \) converges. This immediately gives us:

**Theorem 5** Assume the GRH. Let \( K_S/K \) be a pro-\( p \) and tame extension for which \( d_p G_S > \alpha_{K,S} \). Then one has along the tower \( K_S/K \) the estimate: for infinitely many \( n \),

\[
N_n \gg n^2.
\]

One can say more when \( d < r \) and \( r < d^2/4 \), that is when \( 2\sqrt{r} < d < r \).

**Definition 6** Set \( G := G_S \) be tame and infinite, and for a prime \( p \) denote by \( x_p \) the Frobenius at \( p \) in \( G \). Define for \( n \geq 1 \), and \( k \in \mathbb{Z} \geq 1 \),

\[
N_n^{(k)} := \text{the } k \text{th smallest norm of a prime } p \text{ with } x_p \in G_n \setminus G_{n+1}.
\]

Of course, \( N_n^{(1)} = N_n \).

**Theorem 6** Assume the GRH. Let \( G_S \) be the Galois group of a tame \( p \)-tower for which \( r < d^2/4 \). Choose \( \lambda \) and \( m \) as for Lemma 1. Put \( \beta_{k,m} := \lambda^{k+m} \). Then for infinitely many \( k \),

\[
N_k^{(\beta_{k,m})} \gg \lambda^{2k}.
\]

**Proof** Set \( G := G_S \). Observe that here \( r - d \geq 0 \). For \( k \geq 0 \), let us choose \( \lambda^{k+m} \) different prime ideals \( p_{i,k} \subset \mathcal{O}_K \) (of minimal norm) such that \( x_{p_{i,k}} \in G_{m+k} \setminus G_{m+k+1} \). The element \( x_{p_{i,k}} \) is of depth \( m + k \). Denote by \( \tilde{K} := K_S^{(\psi(v_{i,k}), i,k)^N} \). Then Lemma 1 implies that \( \tilde{K}/K \) is infinite: it is an asymptotically good extension where each prime \( p_{i,k} \) splits completely. Put \( \beta_{k,m} := \lambda^{k+m} \). Then by the estimation of Ihara (Theorem 3) for \( \tilde{K}/K \), one has:

\[
\sum_{k \geq 0} \lambda^{k+m} \frac{\log N_k^{(\beta_{k,m})}}{\sqrt{N_k^{(\beta_{k,m})}}} < \infty,
\]

which implies that \( N_k^{(\beta_{k,m})} \gg \lambda^{2k+2m} \) for infinitely many \( k \).  

\[\square\]
3.4 The case of the center

Using Proposition 6, one can also cut $G_S$ by some special commutators. As we will see, this shows the limits of our method.

Let $G_S$ be as usual and let $\{a_1, \cdots, a_d\}$ be a minimal system of generators of $G_S$ with Zassenhaus filtration $\omega_G$. Let $x$ be a non-trivial Frobenius element in $G_S$. Then $\omega_G([x, a_i]) \geq 1 + \omega_G(x)$. Hence, assuming that $G_S$ passes the Golod–Shafarevich test ($r < d^2/4$), we are guaranteed that when $\omega_G(x)$ is large then $\zappa := G_S/\langle [x, a_i], i = 1, \cdots d \rangle^N$ is also infinite.

**Proposition 8** The class of the Frobenius element $x$ in $\zappa$ is non-trivial and is in the center $Z(\zappa)$ of $\zappa$.

**Proof** In $\zappa$, the class of $x$ commutes with the class of $a_i$, for $i = 1, \cdots, d$, and thus with every element as the $a_i$’s topologically generate $\zappa$. That $\omega_G([x, a_i]) > \omega_G(x)$ implies $x$ is not trivial in $\zappa$. $\square$

Now let us remark that $\langle [x, a_i], i = 1, \cdots, d \rangle \subset \langle x \rangle^N$, hence $\zappa := G_S/\langle [x, a_i], i = 1, \cdots, d \rangle^N \to \zappa' := G_S/\langle x \rangle^N$.

Here for the infiniteness of $\zappa$ one has to check if $1 - dt + rt^2 + dt^{1+k}$ has a root in $[0, 1]$. For the quotient $\zappa'$, one has to check if $1 - dt + rt^2 + t^k$ has a root in $[0, 1]$. Some easy algebra shows that (2) is stronger than (1): in other words, to prove that $\zappa$ is infinite it is better to use the criteria for $\zappa'$. Indeed, when $(d, r) = (9, 21)$ and $k = 3$, the polynomial $1 - 9t + 20t^2 + t^3$ has a root in $[0, 1]$ but $1 - 9t + 20t^2 + 9t^4$ does not, so the Golod–Shafarevich test gives $\zappa'$ is infinite and we can only conclude that $\zappa$ is infinite as it has $\zappa'$ as a quotient. Note:

**Proposition 9** Suppose that all primes in $S$ are coprime to $p$. The pro-$p$ group $\zappa$ is infinite if and only if $\zappa'$ is infinite.

**Proof** Clearly $\#\zappa' = \infty \implies \#\zappa = \infty$.

Let $N$ and $N'$ be the kernels of the maps $G_S \to \zappa$ and $G_S \to \zappa'$. If $\zappa'$ is finite then $K_S^{N'}$ is a number field and $K_S^{N}/K_S^{N'}$ is a finitely generated tamely ramified abelian $p$-extension. By class field theory such extensions are always finite so $K_S^N/K$ is finite and thus $\zappa$ is finite. $\square$

This situation shows that some cuts may be not optimal.

4 The constants of Martinet

In this section we set new records for root discriminants in asymptotically good totally complex and totally real towers.

Recall that for a number field $K$ with $[K : \mathbb{Q}] = n$, the root discriminant of $K$, denoted $rd_K$, is $|Disc(K)|^{1/n}$. There are absolute lower bounds, improved over the years, that include
terms that go to 0 as \( n \to \infty \). These lower bounds depend on the signature of \( K \) and have been achieved by analytic methods. The best lower bounds depend on the GRH.

The term that goes to 0 with increasing degree makes it natural to consider towers of number fields and take the lim sup of the root discriminants. For the \( p \)-power cyclotomic tower it is an exercise to see that this lim sup is \( \infty \). It is also an exercise to see that root discriminants are constant in unramified extensions. Thus the work of Golod and Shafarevich establishing the existence of infinite Hilbert Class Field towers also immediately gave a rich supply infinite towers with bounded root discriminants. Recall Euler’s constant \( \gamma := \lim_{n \to \infty} \left( \sum_{k=1}^{n} \frac{1}{k} - \log n \right) \). The current GRH lower bounds for infinite towers are \( 8\pi e^{\gamma} \approx 44.763 \) for totally complex fields and \( 8\pi e^{\gamma} + \pi^2 \approx 215.33 \) for totally real fields. See [29] for a nice history of this work up until 1990.

It is also natural to seek explicit examples of infinite towers with small lim sup of the root discriminants. Martinet and then Hajir–Maire gave totally real and totally complex infinite towers with small root discriminant.

Hajir–Maire introduced the idea of allowing tame ramification. One can show the relevant Galois groups are infinite using the Golod–Shafarevich criterion, and the root discriminants can be bounded by tame ramification theory. Here we improve their results by using our technique of cutting towers.

### 4.1 Tame towers with finite ramification-exponent

We will again use Proposition 6. The set \( S \) will consist of \( p \) with \( N(p) \equiv 1 \mod p \). Recall that \( d = d_p H^1(G_S) = d_p G_S \) is the \( p \)-rank of \( G_S \) and \( r = d_p H^2(G_S) \) is the minimal number of relations of \( G_S \).

**Definition 7** Fix \( k \geq 1 \). Denote by \( K_S^{[k]} / K \) the maximal pro-\( p \) extension of \( K \) unramified outside \( S \) and where the exponent of ramification at \( p \in S \) is at most \( p^k \) so \( K^{[\infty]}_S = K_S \). Put \( G^{[k]}_S := \text{Gal}(K^{[k]}_S / K) \).

**Remark 6** The extension \( K^{[k]}_S / K \) is well-defined because inertia groups are cyclic in the tame case.

**Proposition 10** Assume that \( r < d^2 / 4 \). Put \( k_0 = \lceil \log \left( \frac{d^2}{4r} - 1 \right) / \log(d/2r) \rceil \). Then, for \( k \geq \log_p(k_0) \), the extension \( K_S^{[k]} / K \) is infinite.

**Proof** We follow the notation of Proposition 6. We have chosen \( k_0 \) so that \( P(t) = 1 - dt + rt^2 + t^{k_0} \) is negative at \( t = d/2r \). Take as \( x \) a generator of the inertia group at \( p \) in \( K_S / K \), cut by \( x^{p^k} \) and apply Proposition 6 (i). \( \square \)

In [13] it is shown, by taking the limit in the above Proposition, that the root discriminant of \( K_S / K = K^{[\infty]}_S / K \) is bounded by \( rd_K \cdot (N(p) \left( \frac{1}{\sqrt[p^k-1]} \right) ) \). We also have the slightly stronger result:

**Proposition 11** In the tower \( K_S^{[k]} / K \) the root discriminant is bounded by

\[
rd_K \cdot (N(p) \left( \frac{1}{\sqrt[p^k-1]} \right) )^{1 - \frac{1}{p^k}}.
\]

**Proof** The result follows from the basic theory of tame ramification. \( \square \)

We can now give an answer to a central question of [12]:

\( \square \) Springer
Theorem 7 Suppose $S \neq \emptyset$ such that $d_p G_S > \alpha_{K,S}$. Then there exists a finite extension $L/K$ in $K_S/K$ such that $L_0/L$ is infinite.

Proof Observe that wlog we can assume that $S = \{p\}$ contains only one prime. By hypothesis, $r < d^2/4$, so for large $k$, the extension $K_S^{(k)}/K$ is infinite. The inertia group at $p$ is a quotient of $\mathbb{Z}/p^k\mathbb{Z}$. By changing the base field, there exists a finite extension $L/K$ such that $K_S^{(k)}/L$ is unramified and infinite. □

4.2 Some set up

Let $K$ be a number field and $S$ a finite set of finite places of $K$.

Let $V_S = \{x \in K^\times \mid x \in (K_v^\times)^p \text{ for } v \in S, \text{ and } v(x) \equiv 0 \mod p, \forall v\}$

and let $\Gamma_S$ to be the character group of $V_S/(K^\times)^p$. Recall the exact sequence

$$0 \to \Pi_2^S \to H^2(G_S) \to \bigoplus_{v \in S} H^2(G_{K_v})$$

where each term on the right is just $\mathbb{Z}/p\mathbb{Z}$ or 0 depending on $\delta_{K_v,p} = 1$ or 0; observe also that when $\delta_{K_v,p} \neq 0$, global reciprocity implies the image of the right map lies in the hyperplane of terms that sum to zero.

From Chapter 11 of [20] we know

$$d_p G_S = \left(\sum_{v \in S_p} [K_v : \mathbb{Q}_v]\right) - \delta_{K,p} + \left(\sum_{v \in S} \delta_{K_v,p}\right) - (r_1 + r_2) + 1 + d_p(\Gamma_S) \quad (3)$$

and there is a natural injection $\Pi_2^S \hookrightarrow \Gamma_S$ which is an isomorphism if $S$ contains all primes of $K$ dividing $p$ (and infinity for $p = 2$).

Remark 7 Numerically showing the injection above is not an isomorphism in explicit tame cases would likely lead to strong improvements in root discriminant bounds in asymptotically good towers.

When $S$ is tame software will allow us to explicitly compute $d_p G_S$ in many cases, thus giving $d_p \Gamma_S$ exactly and the upper bound

$$r(G_S) \leq \begin{cases} 
  d_p \Gamma_{\emptyset} & S = \emptyset \\
  d_p \Gamma_S + |S| - \delta_{K,p} & S \neq \emptyset
\end{cases} \quad (4)$$

4.3 Examples and records

In our experience, setting records for root discriminants in towers is (unfortunately) to some extent an ad hoc process. Our strategy is to find fields whose unramified $p$-towers are not provably infinite via the Golod–Shafarevich criterion, but whose corresponding polynomials attain values close to zero on the unit interval. We then allow a small amount of additional ramification so that the new polynomial has a root and the corresponding pro-$p$ group is infinite.

For various computations of $H^1$s and ray class groups we have used the software packages PARI/GP [31] and MAGMA [3]. We take always $p = 2$ in this subsection.
4.3.1 An example of J. Martin

In his Ph.D. thesis, [25], Martin found a degree 8 totally real number field $K$ whose 2-class group has rank 8. Equation (3) gives that $\dim \Gamma_\emptyset = 16$ so $\dim H^2(G_\emptyset) = \dim \mathbb{H}_\emptyset^2 \leq \dim \Gamma_\emptyset = 16$. The Golod–Shafarevich polynomial is (at worst) $P(t) = 1 - 8t + 16t^2$. Note $P(1/4) = 0$ so $G_\emptyset$ is infinite. As Martin’s thesis is unpublished, we record his polynomial here: $x^8 - 3297x^6 + 14709x^5 + 3555341x^4 - 24457440x^3 - 1347361755x^2 + 7744222350x + 149856133975$. Its discriminant is $(3^2 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 29^2 \cdot 53 \cdot 109)^2$ and the root discriminant is less than 913.4927.

4.3.2 The totally complex case

- Take $K = \mathbb{Q}(\sqrt{13}, \sqrt{-3 \cdot 5 \cdot 17})$. Software gives $d_2 G_\emptyset = 4$ so Equation (3) gives $d_2 \Gamma_\emptyset = 6$. The Golod–Shafarevich polynomial $1 - 4t + 6t^2$ has no root so we cannot conclude $G_\emptyset$ is infinite. There are two primes above 43 in $K$, both having norm 43$^2$. Take $S$ to be either of these. We write $S = \{p_{43^2}\}$. Software gives that $d_2 G_S = 5$ so $d_2 \Gamma_S = 6$ and $r(G_S) \leq 6 + 1 - 1 = 6$. In this case the Golod–Shafarevich polynomial $1 - 5t + 6t^2$ has a root in $\mathcal{O}_S$. As $d_2 G_\emptyset = 4 < 5 = d_2 G_S$, the generator of inertia $\tau_{p_{43^2}} \in G_S$ has depth 1 by Proposition 4 (iii). We cut $G_S$ by the relation $\tau_{p_{43^2}}^4$ which has depth at least 4 by Proposition 1. As $1 - 5t^2 + 6t^2 + t^4$ has a root in $\mathcal{O}_S$, the group $G_S^{[2]}$ is infinite, and in this tower one has:

$$rd_{K_S^{[2]}} = rd_K \cdot (43^2)^{\frac{1}{2}}(1-\frac{1}{2}) < 235.9351.$$  

This is not close to the record of 82.1004 in [14].

- Take the number field $K$ with polynomial

$$x^{12} + 138x^{10} - x^9 + 6579x^8 - 1191x^7 + 142088x^6 - 78327x^5 + 1495530x^4 - 1492094x^3 + 8549064x^2 - 6548187x + 27239851.$$  

The field is totally complex and software gives

$$rd_K < 75.7332, \ d_2 G_\emptyset = 7 \text{ and } d_2 \Gamma_\emptyset = 13.$$  

The Golod–Shafarevich polynomial $1 - 7t + 13t^2$ has no root so we set $S$ to be the one prime $p_9$ above 3. It has norm 9 and software gives $d_2 G_S = d_2 G_\emptyset = 7$ so $\tau_{p_9}$ is of depth at least 2 by Proposition 4 (iii) and $\tau_{p_9}^2$ has depth at least 4. One sees that $d_2 \Gamma_S = 12$ and $r(G_S) \leq 12$. As $1 - 7t + 12t^2$ has a root in $\mathcal{O}_S$, $G_S$ is infinite. After cutting by $\tau_{p_9}^2$, our Golod–Shafarevich polynomial $1 - 7t + 12t^2 + t^4$ has a root in $\mathcal{O}_S$, so $G_S^{[1]}$ is infinite and

$$rd_{K_S^{[1]}} = rd_K \cdot (9)^{\frac{1}{2}}(1-\frac{1}{2}) < 82.9940.$$  

This is quite close to the record of 82.1004 of [14].

- In this example we establish a new record by cutting the old one. Consider the totally complex number field $K$ of degree 12 in [14] with polynomial $x^{12} + 339x^{10} - 19752x^8 - 2188735x^6 + 284236829x^4 + 4401349506x^2 + 15622982921$. Let $H$ be the Hilbert Class Field of $K$. Software yields that $Gal(H/K) \simeq (\mathbb{Z}/2)^6$ so

$$d_2 G_\emptyset = 6, \ d_2 \Gamma_\emptyset = 6 + r_2 = 6 + 6 = 12 \text{ and } r(G_\emptyset) \leq 12.$$  

The polynomial $1 - 6t + 12t^2$ is always positive so we cannot conclude that the maximal pro-2 quotient of $G_\emptyset$ is infinite. Here $rd_K < 68.3636$. Now take $S = \{p_9\}$, the unique
prime above 3 of norm 9. Software gives $d_2 G_S = 7$ so $d_2 \Gamma_S = 12$ and we have the bound $r(G_S) \leq 12 + 1 - 1 = 12$. The polynomial $1 - 7t + 12t^2$ has a root in $\mathbb{Q}, [-1, 1]$ so $G_S$ is infinite. As $d_2 G_\emptyset = 6 < 7 = d_2 G_S$, $\tau_{p_9}$ has depth 1. We cut by $\tau_{p_9}^4$ to get Golod–Shafarevich polynomial $1 - 7t + 12t^2 + t^4$ which has a root in $[0, 1]$ so $G_S^{[4]}$ is infinite, and in this tower

$$rd_{K_S^{[4]}} = rd_K \cdot (9)^{\frac{1}{12}} < 78.4269.$$ 

This is a new record with savings a factor of $3^{1/24} \approx 1.04683 \ldots$

### 4.3.3 The totally real case

We establish a new record here as well. Let $K$ be the totally real field of $[14]$ of degree 12 over $\mathbb{Q}$. Its polynomial is

$$x^{12} - 56966x^{10} + 959048181x^8 - 5946482981439x^6 + 14419821937918124x^4 - 12705425979835529941x^2 + 3527053069602078368989$$

and $rd_K < 770.6432$. All primes above 13 in $K$ have norm 13. Take $S$ to be any one of them. Software gives

$$d_2 G_\emptyset = d_2 G_S = 9, \quad d_2 \Gamma_\emptyset = 21 \quad \text{and} \quad d_2 \Gamma_S = 20.$$ 

The Golod–Shafarevich polynomial for $G_\emptyset$ is $1 - 9t + 21t^2$ and has no root in $[0, 1]$ so we cannot conclude $G_\emptyset$ is infinite, though we suspect it is. The Golod–Shafarevich polynomial for $G_S$ is $1 - 9t + 20t^2$ which has a root in $[0, 1]$. As $d_2 G_\emptyset = d_2 G_S = 9$ we see $\tau_{p_{13}}$ has depth at least 2 by Proposition 4 (iii). We cut by $\tau_{p_{13}}^2$ which has depth at least 4. As $1 - 9t + 20t^2 + t^4$ has a root in $[0, 1]$ $K_S^{[4]} / K$ is infinite and

$$rd_{K_S^{[4]}} = rd_K \cdot (13)^{\frac{1}{24}} \cdot (1 - \frac{1}{2}) < 857.5662.$$ 

This is a new record with savings a factor of $13^{1/24} \approx 1.11279 \ldots$

### 4.3.4 Comments

In the example above, a hope would be that $\tau_{p_{13}}$ has depth greater than two in $G_S$. In that case we could cut by the relation $\tau_{p_{13}}^4$ and the corresponding Golod–Shafarevich polynomial would be at most $1 - 9t + 20t^2 + t^4$ which has a root in $[0, 1]$. One would then have that $K$ has infinite 2-Hilbert Class Field Tower and the totally real root discriminant record would be $< 770.644$. We do not see how to check the depth of $\tau_{p_{13}}$ in $G_S$. See also the beginning of Sect. 6.

The totally complex record was 82.1004 with a GRH lower bound of $8\pi e^\gamma \approx 44.763$. For the totally real case, the record was 913.4927 and the GRH lower bound is $8\pi e^{\gamma + \frac{\pi}{2}} \approx 215.33$. One should probably take the ratio and then logs to measure distance to the GRH bounds. Then for a number field $K$, let us define $\partial(K) = \log(Rd_K / \alpha)$ where $\alpha = 8\pi e^\gamma$ or $8\pi e^{\gamma + \frac{\pi}{2}}$ as $K$ is totally imaginary or $K$ is totally real. Let us recall the different improvements. The ordered pairs in the table below are $(rd_K, \partial)$.

The recent improvement of $\partial$ in the totally imaginary case is 7.55%, and 4.36% for the totally real case.
5 Cutting of wild towers

5.1 Local abelian extensions

For this section, our results follow from this main observation: we can cut wildly ramified towers to be asymptotically good if we first cut by local commutators. We assume throughout this section that we are in the worst case for cutting: the assertion of Kuz’mín’s Theorem holds, that is the pro-\(p\) local Galois groups above \(p\) are maximal. In the first totally complex example of Sect. 5.2 the hypotheses of Kuz’mín’s Theorem are satisfied, but we do not include the infinite places in the totally real example. It is possible that less cutting is needed in the latter example.

**Definition 8** Let \(S = S_p\) be the set of places of \(K\) above \(p\). Denote by \(K^{[1]}_{S_p},p-\text{ab}/K\) the maximal pro-\(p\) extension unramified outside \(S\), locally abelian at all places dividing \(p\), and for which the inertia groups at \(v\mid p\) are of exponent dividing \(p^k\). Put \(G^{[1]}_{S_p}/p-\text{ab} = Gal(K^{[1]}_{S_p},p-\text{ab}/K)\).

Recall that for \(S = S_p\), the pro-\(p\) group \(G_{S}\) is of cohomological dimension 2 and \(r(G_{S}) = d(G_{S}) - r_2 - 1\). (For \(p = 2\), \(S\) must contain all the infinite places, a vacuous condition in the totally complex case).

**Theorem 8** Take \(p = 2\). In \(K^{[1]}_{S_{p2}},2-\text{ab}/K\), the root discriminant is bounded by \(rd_{K} : \sum_{v|p} f_v \left(\frac{2^{e_v + 1}}{p^{2e_v}}\right) \frac{1}{f_v} \left(\frac{1 - \pi_v f_v}{2}\right)\).

**Proof** Fix a place \(v\mid 2\) of \(K\). By Kummer’s theory, the quadratic extensions of \(K_v\) are parametrized by the classes of \(K_v \times K_v^2 \simeq (\pi_v) / (\pi_v^2) \times U_v / U_v^2\) where the latter factor has dimension \(e_v f_v + 1\) over \(\mathbb{F}_2\) so the maximal elementary abelian 2-extension of \(K_v\) has degree \(2^{e_v f_v + 2}\). We compute its discriminant over \(K_v\) by using the conductor-discriminant formula, namely we take the product of the conductors of all quadratic characters of \(K_v\). Note there is exactly one character for each quadratic extension, so the discriminant equals the conductor in this case. It is elementary to compute an upper bound on the discriminant of a quadratic field, so by taking the product over all quadratic fields we obtain an upper bound for our local discriminant. There are \(2^{e_v f_v + 2} - 1\) quadratic extensions of \(K\):

- \(2^{e_v f_v + 1} - 1\) extensions corresponding to extracting the square root of a unit. These have conductor dividing \(4 = \pi^{2e_v}\). One extension is unramified and has conductor 1.
- \(2^{e_v f_v + 1}\) extensions corresponding to extracting the square root of the uniformizer times a unit. These have conductor \(\pi^{2e_v + 1}\).

For more details see for example [9, Chapter II, Proposition 1.6.3]. Thus the discriminant of the maximal elementary abelian 2-extension of \(K\) divides

\[
(\pi^{-2e_v})^{2^{e_v f_v + 1} - 2} \cdot (\pi^{-2e_v + 1})^{2^{e_v f_v + 1}} = \pi^{e_v \cdot 2^{e_v f_v + 3} + 2^{e_v f_v + 1} - 4e_v}.
\]
Taking the $2^{e_v/f_v+2}$th root, we get the root discriminant is

$$(\pi)^{2e_v+\frac{1}{2} - \frac{e_v}{2v/f_v}} = (2)^{2 + \frac{1}{2e_v} - \frac{1}{2v/f_v}}.$$ 

This is the local contribution. The norm of $v$ is $2^{f_v}$ so in the global root discriminant we get a the factor $2^{f_v\left(2 + \frac{1}{2e_v} - \frac{1}{2v/f_v}\right)}$. Now take the product over $v|p$ and take the $[K : \mathbb{Q}]$th root.

\[\square\]

**Remark 8** One has $G_{S_p}/\langle[D_v, D_p], v|p\rangle \rightarrow G_{S_p}^{ab} := G_S/[G_S, G_S]$ and then the maximal local abelian extension $K_S^{p-\text{ab}}/K$ of $K_S/K$ is infinite (it contains the cyclotomic extension). In order to have a criteria that $K_S^{[k], p-\text{ab}}/K$ is infinite for some $k$, we need a Golod–Shafarevich polynomial of $K_S^{p-\text{ab}}/K$ to have a root in $[0, 1[$.

### 5.2 Examples

- Take $K = \mathbb{Q}(\sqrt{-8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13})$ and $p = 2$. Software gives $G_{\emptyset}^{ab} \simeq \mathbb{Z}/8 \times (\mathbb{Z}/2)^4$, and for $S = \{p_2\}$, the unique prime above 2, $G_S^{ab} \simeq \mathbb{Z}_2^2 \times (\mathbb{Z}/2\mathbb{Z})^4$. Also $p_2$ is not principal and thus its Frobenius in $G_\emptyset$ has depth 1.

In this totally complex wild case, global duality implies the natural injection $\mathbb{III}_S^2 \hookrightarrow \mathcal{B}_S$ from Sect. 3.2 is an isomorphism and $r = r(G_S) = d - 1 - r_2 = 4$.

Recall that the decomposition group at $p_2$ in $G_S$ has at most 4 generators, as a quotient of $G_p = \text{Gal}(\overline{K}_p/K_p)$ this last group being isomorphic to the Demushkin group with 4 generators (here $\overline{K}_p$ is the maximal pro-$p$ extension of the complete field $K_p$). Denote by $(x, y, z, t)$ these generators viewed in $G_S$ where $t$ corresponds to Frobenius and $x, y$ and $z$ are generators of inertia. The structures of $G_{\emptyset}^{ab} = G_S/[G_S, G_S]$ and $G_S^{ab}$ show that the elements $x, y, z, t$ can be chosen such that $t$ and $x$ have depth 1 while $y$ and $z$ have depth at least 2. Then

- $[x, t]$ has depth at least 2,
- $[x, y], [x, z], [t, y], [t, z]$ have depth at least 3,
- and $[y, z]$ has depth at least 4.

If we cut $G_S$ by the local commutators, a Golod–Shafarevich polynomial to test becomes:

$$P(t) = (1 - 6t + 4t^2) + (t^2 + 4t^3 + t^4) = 1 - 6t + 5t^2 + 4t^3 + t^4,$$

which has a root in $[0, 1[$. Now, we can apply Proposition 6 to cut the ramification at a certain depth; observe that the ramification in $\text{Gal}(K_S^{2-\text{ab}}/K)$ is generated by the classes of $x, y, z$ and its quotient $G_S^{[1], 2-\text{ab}}$ is infinite: indeed the polynomial $1 - 6t + 6t^2 + 4t^3 + 3t^4$ has a root in $[0, 1[$.

In this case the root discriminant in $K_S^{[1], 2-\text{ab}}/K$ is bounded by $rd_K 2^{9/8} < 755.90358 \ldots$, thanks to Theorem 8.

- In this example we demonstrate the effectiveness of using a mixed strategy of simultaneous tame and wild cutting. Take $K$ to be the Hilbert Class Field of the cyclic cubic extension of conductor 163. The number field $K$ is of degree 12 over $\mathbb{Q}$ with equation given by $x^{12} - 23x^{10} + 125x^8 - 231x^6 + 125x^4 - 23x^2 + 1 = 0$. Here for $v|2$, $f_v = 3$. Take $S = \{v|2, 3, 5, 7\}$. Software and some basic theory give

- there are 4 primes in $K$ above above 2, 3 and 7. There are 6 primes above 5,
- $d_2 G_S = 18$, and Eq. (3) implies $\mathcal{B}_S = 0$ so $\mathbb{III}_S^2 = 0$ as well,
– $r(G_S) \leq 17$ so the Golod–Shafarevich polynomial is $1 - 18t + 17t^2$, which is very negative on $]0, 1[$.

We are going to cut by

– the local commutators of each place above 2, i.e. by $4 \cdot 10$ elements of depth at least 2,
– the squares of the generators of the abelian local inertia at the wild places, i.e by 12 elements of depth at least 2,
– the fourth powers of the generators of inertia at three of the six places dividing 5,
– the squares of the generators of the inertia of the eight places dividing $3 \cdot 7$ and the other three places dividing 5.

Then the pro-$p$ group of the new quotient has $1 - 18t + (17 + 40 + 12 + 11)t^2 + 3t^4$ as polynomial that has a root in $]0, 1[$. Here, one has

$$rd \leq 163^{2/3} \cdot (3 \cdot 7 \cdot 5^{1/2})^{1/2} \cdot (5^{1/2})^{3/4} \cdot 2^{23/8} < 2742.95621 \cdots$$

5.3 Cutting a $p$-rational tower

5.3.1 $p$-rational field

Let us recall the notion of $p$-rational field (see for example [10,27,28]).

**Definition 9** A number field $K$ is called $p$-rational if the maximal pro-$p$ extension of $K$ unramified outside $S_p$ is free pro-$p$.

In the context of the inverse Galois problem, this notion is also very useful for producing some special pro-$p$ extensions of number fields: see Greenberg [11], Hajir and Maire [15], etc.

An easy argument from group theory gives:

**Proposition 12** Let $K$ be a $p$-rational field and let $L/K$ be a finite extension in $K_{S_p}/K$. Then $L$ is $p$-rational.

Assuming Leopoldt’s conjecture, it is well-known that $G_{S_p}$ is pro-$p$ free if and only if $G^{ab}_{S_p}$ is torsion-free. The torsion of $G^{ab}_{S_p}$ can be estimated by class field theory: in particular for $p$ sufficiently large this torsion is isomorphic to the $p$-part of $\left( \prod_{v \in S_p} U_v \right) / \sigma_K$ which is easy to compute. After many observations Gras [8, Conjecture 7.11] recently made the following conjecture:

**Conjecture 1** (Gras) Fix a number field $K$. For large $p$, $K$ is $p$-rational.

We use Gras’ Conjecture to produce $p$-rational number fields $L$ with large $p$-class group.

5.3.2 Results

First, we obtain:

**Theorem 9** Let $K$ be a totally imaginary field of degree at least 12 over $\mathbb{Q}$. Choose $p > 2$ such that: (i) $p$ splits completely in $K/\mathbb{Q}$ and, (ii) $K$ is $p$-rational. Then there exists a number field $L/K$ in $K_{S_p}/K$ such that $L_\emptyset/L$ is infinite. Note that as $\text{Gal}(L_{S_p}/L)$ is a subgroup of the free pro-$p$ group $\text{Gal}(K_{S_p}/K)$ then $L$ is $p$-rational.
Proof Let $p > 2$. As $p$ splits completely in $K$, $\mu_p \not\subseteq K_v$ and $G_v$ is a free pro-$p$ group on 2 generators $x_v, \tau_v$, where $x_v$ can be chosen as the Frobenius and $\tau_v$ as a generator of the inertia group.

Suppose moreover that $K$ is $p$-rational so $G_{S_p}$ is free pro-$p$. Then we cut the free pro-$p$ group $G_{S_p}$ on $r_2 + 1$ generators by all the commutators $[x_v, \tau_v]$ for all $v | p$, to obtain a pro-$p$ extension $K_{S_p}^{p-ab}/K$ corresponding to the maximal local abelian extension at every $v | p$ of $K$ unramified outside $p$; here $r_2$ is the number of complex embeddings of $K$. Put $\Gamma := Gal(K_{S_p}^{p-ab}/K)$. A naive presentation ($\mathcal{P}$) of $\Gamma$ allows us to obtain the Golod–Shafarevich polynomial

$$P_\mathcal{P}(t) = 1 - (r_2 + 1)t + 2r_2t^2.$$ 

As $r_2 \geq 6$, we easily compute that $P_\mathcal{P}$ is negative on $]0, 1[$, and so for a large given $k$, if we cut by the powers $\tau_v^{p^k}$ of $\tau_v$, $v | p$, the extension $K_{S_p}^{[k],p-ab}/K$ is infinite. As $\mathbb{Z}/p^k$ maps onto the inertia group of all $p | p$, one concludes by changing the base to an appropriate number field $L$ that ‘absorbs’ the ramification.

Recall that if a pro-$p$ group $G$ has a presentation whose Golod–Shafarevich polynomial is negative on the unit interval (we call this passing the Golod–Shafarevich test) then $G$ is not $p$-adic analytic (when $d \geq 3$) and, by Lubotzky and Mann [24], the $p$-rank of the open subgroups $U$ of $G$ tends to infinity with $[G : U]$. In fact, one has the following due to Jaikin–Zapirain (see [18] or [6, Theorem 8.3]):

**Theorem 10** (Jaikin–Zapirain) Suppose that a pro-$p$ group $G$ passes the Golod–Shafarevich test. Then there exist infinitely many $n$ such that $\log_p d_p G_n \geq (\log_p [G : G_n])^\beta$, for some $\beta \in ]0, 1[$, where $G_n$ is the $n$th group in the Zassenhaus filtration of $G$.

In our context, as a corollary, one obtains:

**Corollary 1** Let $K$ be a totally imaginary field of degree at least 12 over $\mathbb{Q}$. Choose $p > 2$ such that: (i) $p$ splits completely in $K/\mathbb{Q}$ and, (ii) $K$ is $p$-rational. Then there exists a constant $\beta > 0$ and a sequence of $p$-rational number fields $(L_n)$ in $K_{S_p}/K$ such that

$$\log d_p Cl_{L_n} \gg (\log[L_n : \mathbb{Q}])^\beta,$$

where $Cl_{L_n}$ is the class group of $L_n$.

**Proof** Choose $k$ as in proof of Theorem 9 such that $K_{S_p}^{[k],p-ab}/K$ is infinite. Put $G = Gal(K_{S_p}^{[k],p-ab}/K)$, and consider $G_n$ the Zassenhaus filtration of $G$. Let $K_n$ be the subfield of $K_{S_p}^{[k],p-ab}/K$ fixed by $G_n$; by Proposition 12 all the fields $K_n$ are $p$-rational. Take $n_0$ large enough so that the pro-$p$ extension $K_{S_p}^{[k],p-ab}/K_{n_0}$ is unramified: this is always possible because $G_n$ forms a filtration of open subgroups of $G$ and for each $v | p$ the inertia group in $G$ is finite.

By hypothesis the group $G$ passes the Golod–Shafarevich test: by Theorem 10, for infinitely many $n \geq n_0$, we get $\log_p d_p G_n \geq (\log_p [G : G_n])^\beta$, for some $\beta \in ]0, 1[$. To conclude it suffices to note that for $n \geq n_0$ the extension $K_{S_p}^{[k],p-ab}/K_n$ is unramified, and then by class field theory one has $d_p Cl_{K_n} \geq d_p G_n$.
6 Depth of ramification

6.1 Motivation

Let us start with one comment that motivates this section. Let \( P(t) = 1 - dt + rt^2 \) be a polynomial with no root on \([0, 1]\) but such that \( 1 - dt + (r - 1)t^2 \) has a root. For example, take the totally real field of Sect. 4.3.3 where \((d, r) = (9, 21)\).

Suppose that \( G_\wp \) has, for a certain presentation, Golod–Shafarevich polynomial \( 1 - dt + rt^2 \) where \( d = \dim H^1(G_\wp, \mathbb{Z}/p) \) and \( \dim H^2(G_\wp, \mathbb{Z}/p) \leq \dim \Gamma_\wp = r \). Suppose \( \mu_p \subset K \) and set \( S = \{p\} \) with \( p \) coprime to \( p \). Then by (4), \( \dim S \) is either \( r \) or \( r - 1 \). By the global reciprocity law the image of the localization map \( H^2(G_S, \mathbb{Z}/p) \to H^2(G_p, \mathbb{Z}/p) \) is trivial so \( \dim H^2(G_S, \mathbb{Z}/p) \) is also at most \( r \) or \( r - 1 \). By (3) we have \( \dim H^1(G_S, \mathbb{Z}/p) = d + 1 \) or \( d \) respectively. For \((d, r) = (9, 21)\) the group \( G_S \) has Golod–Shafarevich polynomial \( 1 - 9t + 20t^2 \) or \( 1 - 10t + 21t^2 \) and it is easy to see \( G_S \) is infinite in either case.

Suppose now that the generator of inertia at \( p \), \( \tau_p \), has depth at least \( k \) in \( G_S \). If we cut \( G_S \) by \( \langle \tau_p \rangle \), the Golod–Shafarevich polynomial becomes \( 1 - dt + (r - 1)t^2 + t^k \), and for large \( k \) it has a root. In this case we can introduce the relation \( \tau_p \) and observe \( K_\wp/K \) is infinite. For \((d, r) = (9, 21)\) we need \( k \geq 3 \).

**Question 1** Suppose \( G_S \) is infinite. To simplify, take \( S = \{p\} \) with \( p \) coprime to \( p \). How deep can the generator \( \tau_p \) of tame inertia be in \( G_S \)?

6.2 Adding a splitting condition

6.2.1 Detect the level of inertia

Let \( S \) and \( T \) be finite disjoint sets of primes of \( K \). We denote by \( K^T_S/K \) the maximal pro-

\( p \)-subextension of \( K_S/K \) where all places of \( T \) split completely. Put \( G^T_S = Gal(K^T_S/K) \).

Consider the Frattini series \( \Phi_n(G^T_\wp) \) and \( \Phi_n(G^T_S) \). Set \( K_n := \langle (\Phi_n)^T \rangle \Phi_n(G^T_\wp) \). We abuse notation and set \( \omega := \omega_{G^T_S} \).

If \( L/K \) is a finite subextension of \( K^T_S/K \), we denote by \( G^T_{L,S} \) the Galois group \( Gal(L^T_S/L) \).

To simplify, assume that \( S = \{p\} \) where \( p \subset \mathcal{O}_K \) is coprime to \( p \). Let \( \tau_p \in G^T_S \) be a generator of the inertia group at \( p \) in \( K^T_S/K \).

**Lemma 2** If \( d_p G^T_{K_n,\wp} = d_p G^T_{K_n,s} \) for some \( n \), then \( \omega(\tau_p) \geq 2^n \).

**Proof** For \( m \geq 1 \), write \( K'_m = (K^T_S)^{\Phi_m(G^T_\wp)} \). If, for \( i \leq n + 1 \), we had a \( p \)-extension of \( K_i \) unramified outside \( S \) but actually ramified at \( p \), we could take its composite with the unramified extension \( K_n/K_i \) to contradict the equality of our hypothesis. Thus \( d_p G^T_{K_n,\wp} = d_p G^T_{K_n,s} \) for all \( i \leq n + 1 \). Hence, one has \( K_2 = K'_2 \), then \( K_3 = K'_3 \) etc. up to \( K_{n+1} = K'_{n+1} \).

In particular the extension \( K'_{n+1}/K \) is unramified and \( \tau_p \in \Phi_{n+1}(G^T_S) \); in other words \( G^T_S/\Phi_{n+1}(G^T_S) \cong G^T_\wp/\Phi_{n+1}(G^T_\wp) \). By Proposition 4 (iii), we get \( \omega(\tau_p) \geq 2^n \). \( \Box \)

6.2.2 Depth and freeness

Recall from Sect. 4.2 that

\[ V_S = \{ x \in K^\times | x \in (K_v^\times)^P \forall v \in S \text{ and } v(x) \equiv 0 \mod p, \forall v \} \]
and set
\[ V^T = \{ x \in K^\times | v(x) \equiv 0 \mod p, \forall v \notin T \} \]
and
\[ V^T_S = \{ x \in K^\times | x \in (K_v^\times)^p \forall v \in S \text{ and } v(x) \equiv 0 \mod p, \forall v \notin T \}. \]

Note \( V^T_\emptyset = V_S, V_S \subseteq V^T_S, S_1 \subseteq S_2 \implies V_{S_2} \subseteq V_{S_2} \text{ and } T_1 \subseteq T_2 \implies V_{T_1} \subseteq V_{T_2}. \)

If we switch fields to some \( L \supseteq K \), we will include the field in the notation to avoid confusion, e.g. \( V^T_L \) or \( V^T_{L,S} \).

Consider
\[ 1 \rightarrow \mathcal{O}_{K,T}^\times/(\mathcal{O}_{K,T}^\times)^p \rightarrow V^T_K/(K^\times)^p \rightarrow Cl^T_K[p] \rightarrow 1, \]
(5)
where \( \mathcal{O}_{K,T}^\times \) denotes the group of \( T \)-units of \( K \) and \( Cl^T_K \) the \( p \)-Sylow subgroup of the \( T \)-class group of \( K \). Put \( K' := K(\mu_p) \) and \( K'_T = K'(\sqrt[p]{V^T}). \) One has Theorem 11 below [9, Chapter V, Corollary 2.4.2] involving the Artin symbol \( \left( \frac{K'_T/K' \times}{\Phi} \right) \) in \( Gal(K'_T/K'). \)

Note that \( S \) and \( T \) are our \( T \) and \( S \) here respectively.

**Theorem 11** (Gras) *Let \( S = \{ p_1, \ldots, p_s \} \) be a tame set of primes of \( K \). There exists a cyclic degree \( p \) extension \( F/K \), unramified outside \( S \), ramified at every prime of \( S \), and where each place of \( T \) splits completely, if and only if for \( i = 1, \ldots, s \), there exist \( a_i \in (\mathbb{Z}/p\mathbb{Z})^\times \) such that*

\[ \prod_{i=1}^s \left( \frac{K'_T/K'}{\mathfrak{p}_i} \right)^{a_i} = 1 \in Gal(K'_T/K'), \]

*where \( \mathfrak{p}_i \mid p_i \) is any prime in \( \mathcal{O}_{K'} \) above \( p_i \).*

Now choose \( p \) of \( K \) whose Frobenius in \( K'_T/K \) has order \( p \) and set \( S = \{ p \} \). This implies that for \( \mathfrak{p} \subset \mathcal{O}_{K'} \) with \( \mathfrak{p} \mid p \) the Frobenius \( x_{\mathfrak{p}} \in Gal(K'_T/K') \) at \( \mathfrak{p} \) is non-trivial.

**Theorem 11** implies that \( d_p G^T_S = d_p G^T_\emptyset \), hence \( \tau_p \) has depth at least 2 in \( G^T_S \) by Lemma 2.

We want to apply this principle to the number field \( K_2 = (K'_T)^{\Phi_2(G^T_\emptyset)} \) bearing in mind the Galois action of \( G^T_\emptyset / \Phi_2(G^T_\emptyset) \).

Let us fix a Galois extension \( L/K \) with Galois group \( H \) inside \( K^T_\emptyset/K \). One has the following consequence of Theorem 11.

**Corollary 2** Suppose that \( V^T_L/(L^\times)^p \) contains a non-trivial free \( \mathbb{F}_p[H] \)-submodule. Then there exists a prime \( p \subset \mathcal{O}_K \) such that \( d_p G^T_L = d_p G^T_{L,S} \text{ where } S = \{ p \}. \)

**Proof** Suppose that \( V^T_L/(L^\times)^p \) has a free \( \mathbb{F}_p[H] \)-submodule \( M \) of rank 1; as the algebra \( \mathbb{F}_p[H] \) is Frobenius, the free submodule \( M \) is a direct factor in \( V^T_L/(L^\times)^p \). By Kummer duality, one deduces that \( Gal(L'_T/L') \) contains a free \( \mathbb{F}_p[H] \)-module of rank 1, generated by some \( g \). By Chebotarev’s density theorem one can choose a prime \( p \subset \mathcal{O}_K \) such that its Frobenius in \( Gal(L'_T/K) \) is in the conjugacy class of \( g \); the prime \( p \) splits completely in \( L'/K \). Put \( S = \{ p \} \). Denote by \( \Omega_0 \) a prime ideal in \( \mathcal{O}_{L'} \) above \( p \) such that \( \left( \frac{L'_T/L'}{\Omega_0} \right) = g. \)

But \( \forall h \in H \) we have \( \left( \frac{L'_T/L'}{\Omega_0^h} \right) = g^{h^{-1}} \), and as \( \langle g \rangle_H \) is a free \( \mathbb{F}_p[H] \)-module, there is no
non-trivial relation between the $\left( \frac{L'_1/L'_1/\Omega^0}{\Omega^0} \right)$'s. By Theorem 11, there is no degree $p$ cyclic extension $F/L$ ramified at some places of $S$, unramified outside $S$, and where each place of $T$ splits completely, and then $d_p G^T_{L,\emptyset} = d_p G^T_{L,S}$. □

**Remark 9** Let $L/K$ be a Galois extension of number fields with Galois group $H$. Let $T$ be a $H$-invariant set of places of $L$. Here are two ways to produce situations where $V^T_L/(L^\times)^p$ has a free-$H$-part:

(i) for large $|T|$ with size depending on $|H|$ (thanks to a bound given by Ozaki [30], see also [16]), we are guaranteed that $\mathcal{O}^\times_{L,T} \otimes \mathbb{F}_p$, and then also $V^T_L/(L^\times)^p$ by (5), contains a non-trivial free $\mathbb{F}_p[H]$-submodule. But the bound for $|T|$ is very bad;

(ii) by Kummer theory, and by an appropriate choice of $T$, we are guaranteed that $V^T_L/(L^\times)^p$ contains a non-trivial free $\mathbb{F}_p[H]$-submodule. This is the method we will use.

### 6.3 A result

We prove the following

**Theorem 12** Let $K$ be a number field. Given $k > 0$, there exists a Chebotarev set of primes $\mathcal{D}$ with the following property: for every $q \in \mathcal{D}$ there are infinitely many primes $p$, coprime to $p$ such that $\omega(\tau_p) \geq k$ in $Gal(K^{[q]}_{\{p\}}/K)$.

As we will see the proof of Theorem 12 can be reduced to the next Proposition.

**Proposition 13** Let $L/K$ be a given finite $p$-extension with Galois group $H$. There exists a positive density set $\Theta_1$ of primes $q$ of $K$, all coprime to $p$ and all split completely in $L/K$, such that for all $t \in \mathbb{N}$ and for all sets $T = \{q_1, \cdots, q_t\} \subset \Theta_1$ of $t$ different primes, one has

$$
\bigoplus_{i=1}^t \mathbb{F}_p[H] \hookrightarrow V^T_L/(L^\times)^p.
$$

**Proof** Put $L' = L(\mu_p)$, and $\Delta = Gal(L'/L)$. Let us start with the following lemma:

**Lemma 3** There exists a positive density set $\Theta_1$ of primes $q$ of $K$, all coprime to $p$, such that for all $t \in \mathbb{Z}_{>0}$ and for all sets $T = \{q_1, \cdots, q_t\} \subset \Theta_1$ of $t$ different primes, one has $\mathbb{F}_p \otimes G^{ab}_{L',T} \hookrightarrow \bigoplus_{i=1}^t \mathbb{F}_p[H][\Delta]$ as $Gal(L'/K)$-modules. Moreover the $q_i$'s are chosen to split completely in $L/K$.

**Proof** First, we choose a set of primes $\Sigma$ of $L'$, $Gal(L'/K)$-invariant, such that $G^{\Sigma,ab}_{L',\emptyset} = \{1\}$. We can do this by choosing $\Sigma$ to consist of primes whose Frobenii generate the finite abelian group $G^{ab}_{L',\emptyset}$. Put $F = L'(\sqrt[\Sigma]{\mathcal{O}^\times_{L',\Sigma}})$. The extension $F/K$ is Galois and let $\Theta_1$ be the Chebotarev set of places of $K$ that split completely in $F/K$. The splitting implies that for each $v \in \Theta_1$ one has the equality of completions $K_v = L'_v = L'_v(\sqrt[\Sigma]{\mathcal{O}^\times_{L',\Sigma}})$, so $\mathcal{O}^\times_{L',\Sigma} \subset U^p_v$ and $\mu_p \subset K_v$. Take now $T = \{v_1, \cdots, v_t\}$ a set of $t$ different places of $\Theta_1$ all coprime to $p$. By class field theory one has:

$$
\mathbb{F}_p \otimes G^{\Sigma,ab}_{L',T} \simeq \prod_{w|v \in T} U_w \otimes_{\mathcal{O}^\times_{L',\Sigma}} \prod_{w|v \in T} U^p_w \simeq \prod_{w|v \in T} U_w/U^p_w.
$$

\(\Box\) Springer
As all places of $T$ split completely in $L'/K$, then
\[
\prod_{w|T} U_w/U_w^p \cong \bigoplus_{i=1}^t \mathbb{F}_p[H][\Delta].
\]

One concludes by noting that $\mathbb{F}_p \otimes G_{L'/T}^{ab} \to \mathbb{F}_p \otimes G_{L'/T}^{\Sigma,ab} \cong \bigoplus_{i=1}^t \mathbb{F}_p[H][\Delta]$. \hfill \Box

**Proof** The Kummer radical $R_T$ of the maximal $p$-elementary extension of $L'$, unramified outside $T$, is a subgroup of $V_{L'}^T/(L'^x)^p$ (remember that $T$ is coprime to $p$). Hence by Lemma 3 we get
\[
\bigoplus_{i=1}^t (\mathbb{F}_p[H][\Delta])^* \hookrightarrow R_T \subset V_{L'}^T/(L'^x)^p,
\]
where $*$ denotes the reflection action following $\Delta$. By taking the $\Delta$-invariant, Proposition 13 holds by noting that $\left(V_{L'}^T/(L'^x)^p\right)^\Delta \cong (V_{L'}^T/L'^x)^p$. \hfill \Box

**Proof** (of Theorem 12). Given $k > 0$, write $n = \lfloor \log_2 k \rfloor$. Let $L = (K_p)^{\Phi_n(G_{\Theta})}$ and put $H = \text{Gal}(L/K)$. By Proposition 13, choose a prime $q$, coprime to $p$ and that splits completely in $L/K$, such that $\mathbb{F}_p[H] \hookrightarrow V_{L'}^T/(L'^x)^p$ where $T = \{q\}$. So $V_{L'}^T/(L'^x)^p$ contains a free non-trivial $\mathbb{F}_p[H]$-submodule. Then by Corollary 2, there exists a prime $p \subset \mathcal{O}_K$ such that $d_p G_{L',\Theta}^{T} = d_p G_{L',S}^{T}$, where $S = \{p\}$.

But, as $q$ splits completely in $K$, observe now that $(K_p)^{\Phi_n(G_{\Theta})} = (K_p^T)^{\Phi_n(G_{\Theta}^T)}$. Then by Lemma 2, we get that the depth of $\tau_p \in G_{S}^{\Theta} = \text{Gal}(K_{S}^{\Theta}/K)$ is at least $2^n \geq k$. \hfill \Box

**Remark 10** The reader may wonder why one can’t, for instance in the totally real example of Sect. 3.3.2, simply apply Theorem 12 for some $p$ whose $\tau_p$ will have depth 3 for some $q$. The difficulties are that first $G_{[p]}^{[q]}$ may have many more relations imposed by the splitting condition, and second if one removes the splitting condition, the kernel of the map $G_{[p]} \to G_{[p]}^{[q]}$ might contain elements of depth 2, so the preimage of $\tau_p$ may have depth 2.

**References**

1. Andozski, I.V.: On some classes of closed pro-$p$-groups. Math. USSR 9(no4), 663–691 (1965)
2. Anick, D., Dicks, W.: A mnemonic for the graded-case Golod–Shafarevich inequality. arXiv:abs/1508.03231 (2015)
3. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. 24, 235–265 (1997)
4. Checcoli, S.: Fields of algebraic numbers with bounded local degrees and their properties. Trans. Am. Math. Soc. 365(4), 2223–2240 (2013)
5. Dixon, J.D., Du Sautoy, M.P.F., Mann, A., Segal, D.: Analytic pro-$p$-Groups, Cambridge Studies in Advances Mathematics, vol. 61. Cambridge University Press, Cambridge (1999)
6. Ershov, M.: Golod–Shafarevich groups: a survey. Int. J. Algebra Comput. 22(5), 68 (2012)
7. Fontaine, J.-M., Mazur, B.: Geometric Galois representations. In: Elliptic Curves, Modular Forms, and Fermat’s Last Theorem (Hong Kong, 1993), Ser. I. Internat. Press, Cambridge, MA, Number Theory, pp 41–78 (1995)
8. Gras, G.: Les $\Theta$-régulateurs locaux d’un nombre algébrique?: conjectures $p$-adiques. Can. J. Math. 68, 571–624 (2016)
9. Gras, G.: Class Field Theory. Springer Monographs in Mathematics. Springer, Berlin (2003)
10. Gras, G., Jaulent, J.-F.: Sur les corps de nombres réguliers. Math. Z. 202, 343–365 (1989)
11. Greenberg, R.: Galois representations with open images. Ann. Math. Québec 40(1), 83–119 (2016)
12. Hajir, F., Maire, C.: Unramified subextensions of ray class field towers. J. Algebra 249(2), 528–543 (2002)
13. Hajir, F., Maire, C.: Tamely ramified towers and discriminant bounds for number fields. Compos. Math. 128, 35–53 (2001)
14. Hajir, F., Maire, C.: Tamely ramified towers and discriminant bounds for number fields II. J. Symbol. Comput. 33, 415–423 (2002)
15. Hajir, F., Maire, C.: Prime decomposition and the Iwasawa mu-invariant. Math. Proc. Camb. Philos. Soc. 166, 599–617 (2019)
16. Hajir, F., Maire, C.: Analytic Lie extensions of number fields with cyclic fixed points and tame ramification. http://front.math.ucdavis.edu/1710.09214 (2017)
17. Ihara, Y.: How many primes decompose completely in an infinite unramified Galois extension of a global field?? J. Math. Soc. Jpn. 35(no4), 693–709 (1983)
18. Jaikin-Zapirain, A.: Subgroup growth of Golod–Shafarevich groups, Appendix of Kazhdan quotients of Golod–Shafarevich groups by M. Ershov. Proc. Lond. Math. Soc. 102(4), 599–636 (2011)
19. Kisilevski, H., Labute, J.: On a Sufficient Condition for the $p$-Class Tower of a CM-Field to be Infinite, Théorie des Nombres (Quebec, PQ, 1987), pp. 556–560. de Gruyter, Berlin (1989)
20. Koch, H.: Galois Theory of p-Extensions. Springer Monographs in Mathematics. Springer, Berlin (2002)
21. Koch, H., Venkov, B.: The $p$-tower of class fields for an imaginary quadratic field, (Russian) Modules and representations. Zap. Naucn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. 46, 5–13 (1974)
22. Lazard, M.: Groupes analytiques $p$-adiques. IHES. Publ. Math. 26, 389–603 (1965)
23. Lebacque, P.: Quelques résultats effectifs concernant les invariants de Tsfasman–Vladut. Ann. Inst. Fourier 65(1), 63–99 (2015)
24. Lubotzky, A., Mann, A.: Powerful $p$-groups. II. p-adic analytic groups. J. Algebra 105, 506–515 (1987)
25. Martin, J.: Building infinite ray-class towers with specific signatures and small bounded root discriminant, Cornell Ph.D., (2006)
26. Martinet, J.: Tours de corps de classes et estimations de discriminants. Invent. math. 44, 65–73 (1978)
27. Movahhedi, A.: Sur les $p$-extensions des corps $p$-rationnels, Université Paris VII Ph.D., (1988)
28. Movahhedi, A., Nguyen Quang Do, T.: Sur l’arithmétique des corps de nombres $p$-rationnels. Séminaire de Théorie des Nombres, Paris 1987-88, Progress in Mathematics, vol. 81, pp. 155–200. Birkhäuser, Boston (1990)
29. Odlyzko, A.M.: 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(2), 119–141 (1990)
30. Ozaki, M.: Construction of maximal unramified $p$-extensions with prescribed Galois groups. Invent. Math. 83, 649–680 (2011)
31. Schoof, R.: Infinite class field towers of quadratic fields. J. Reine Angew. Math. 372, 209–220 (1986)
32. Serre, J.-P.: Cohomologie Galoisienne, cinquième édition, révisée et complétée. Springer Lect. Notes Math. 5, 20 (1997)
33. Tsfasman, M., Vladut, S.: Infinite global fields and the generalized Brauer–Siegel theorem. Dedicated to Yuri I. Manin on the occasion of his 65th birthday. Mosc. Math. J. 2(2), 329–402 (2002)
34. Vinberg, E.B.: On a theorem concerning on infinite dimensionality of an associative algebra. Izv. Akad. Nauk SSSR Ser. Mat. 29, 208–214 (1965). (english transl., Amer. Mat. Soc. Transl. (2) 82, 237-242 (1969))
35. Wilson, J.S.: Finite presentations of pro-$p$ groups and discrete groups. Invent. Math. 105(1), 177–183 (1991)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
Affiliations

Farshid Hajir\(^1\) · Christian Maire\(^2\) · Ravi Ramakrishna\(^3\)

✉️ Ravi Ramakrishna
ravi@math.cornell.edu

Farshid Hajir
hajir@math.umass.edu

Christian Maire
christian.maire@univ-fcomte.fr

1 Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA 01003, USA

2 FEMTO-ST Institute, University Bourgogne Franche-Comté, CNRS, 15B avenue des Montboucons, 25000 Besancon, France

3 Department of Mathematics, Cornell University, Ithaca, NY 14853, USA