CUTTING TOWERS OF NUMBER FIELDS

by

Farshid Hajir, Christian Maire, Ravi Ramakrishna

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, phenomena 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.

Contents

Given a minimal presentation $(\mathscr{P})$ of a finitely generated pro-p group G with d generators and r relations, the well-known criterion of Golod-Shafarevich states that if $1 - dt + rt^2$ vanishes on $]0, 1[$, then G is infinite. In fact one may replace this polynomial with $P_{\mathscr{P}}(t) := 1 - dt + \sum_{k\geqslant 2} r_k t^k$, where r_k is the number of relations in the presentation $(\mathscr{P})$

2000 ***Mathematics Subject Classification.*** — 11R29, 11R37, 11R21.
Key words and phrases. — root-discriminant, asymptotically good extensions, Golod-Shafarevich Theorem.

This work has been done during a visiting scholar position for the second author at Cornell University for the academic year 2017-18, 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. The second author was also 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.

of depth k in the Zassenhaus filtration. We may then employ the same vanishing test for infiniteness. See §1.

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-Venkov [**21**], Kisilevski-Labute [**19**] and Schoof [**33**].

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 $\mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$ 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 kind of results:

(*i*) 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 has Frobenius of finite order. These orders are *not* bounded. Ihara stated his expectation that such examples could exist 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 the 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_{S_p} 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 $\mathrm{K}_{S_p}/\mathrm{K}$ 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 $\mathrm{K}_{S_p}/\mathrm{K}$ such that $\log d_p \mathrm{Cl}_{\mathrm{L}_n} \gg (\log[\mathrm{L}_n : \mathbb{Q}])^\beta$, where $\mathrm{Cl}_{\mathrm{L}_n}$ is the class group of L_n.

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, something that can be difficult to arrange. See [**9**, Chapter IV, §3] for a good explanation.

We also study the question of the depth of the generator $\tau_{\mathfrak{p}}$ of tame inertia in G_S. Let T be a finite set of finite places of K, disjoint from S. Let G_S^T be the quotient of G_S by all the Frobenius elements of places of T. Then we prove that given $k > 0$ there exists infinitely many primes $\mathfrak{q}$ such that for infinitely many primes $\mathfrak{p}$, coprime to $p\mathfrak{q}$, the depth of $\tau_{\mathfrak{p}}$ in $\mathrm{G}_{\{\mathfrak{p}\}}^{\{\mathfrak{q}\}}$ is at least k (see Theorem 5.6).

Our work contains five sections. In §1 we recall the refined Golod-Shafarevich Theorem, and we indicate how we use it. We then develop and apply our cutting strategy: in §2 to obtain the splitting results in the context of asymptotically good extensions; in §3 to obtain the new root discriminant records in infinite towers of number fields; in §4 we cut wild towers. The last section is devoted to the question of the depth of tame inertia in G_S.

Notations:
We fix a rational prime p.
– Given a $\mathbb{Z}$-module M, we denote by d_pM the dimension over $\mathbb{F}_p$ of $\mathbb{F}_p \otimes M$: it is the p-rank of M.

– We fix a number field K. By abuse, we identify prime ideals $\mathfrak{p} \subset \mathscr{O}_{\mathrm{K}}$ and places v of K. For a place v of K, we denote by K_v the completion, and by U_v the local units. For v finite, we denote by π_v an uniformizer and by v the corresponding valuation.
For a prime ideal $\mathfrak{p} \subset \mathscr{O}_{\mathrm{K}}$, we put $\mathrm{N}(\mathfrak{p}) := \#(\mathscr{O}_{\mathrm{K}}/\mathfrak{p})$ its absolute norm.

– We fix now a finite set S of finite places of K. For $\mathfrak{p} \in S$ not dividing p, one assumes that $\mathrm{N}(\mathfrak{p}) \equiv 1 \bmod p$. When all $\mathfrak{p} \in S$ are prime to p we call S *tame*. The set of all $\mathfrak{p} \subset \mathscr{O}_{\mathrm{K}}$ dividing (p) is denoted S_p.
If L/K is a finite extension, we also denote by S the set of places of L above S.

– The maximal pro-p extension of K unramified outside S is denoted K_S. Note $\mathrm{K}_\varnothing$ is the maximal everywhere unramified pro-p extension of K. The Galois group of K_S/K is denoted G_S.

– All cohomology groups of G_S have coefficients in $\mathbb{Z}/p$, and we denote by $d = d(\mathrm{G}_S)$ and $r = r(\mathrm{G}_S)$, $d_pH^i(\mathrm{G}_S)$ for $i = 1, 2$ respectively. Hence, $d(\mathrm{G}_S) = d_p(\mathrm{G}_S/[\mathrm{G}_S, \mathrm{G}_S])$. More generally for a finitely generated pro-p group G, we denote by $d_p\mathrm{G} := d(\mathrm{G})$ its p-rank.

– Set $\delta_{\mathrm{K},p} = \begin{cases} 1 & \mu_p \subset \mathrm{K} \\ 0 & \text{otherwise} \end{cases}$. If K has signature (r_1, r_2), set $\alpha_{\mathrm{K},S} := 2+2\sqrt{r_1 + r_2 + \theta_{\mathrm{K},S}}$ where $\theta_{\mathrm{K},S} = \begin{cases} 0 & S \neq \varnothing \\ \delta_{\mathrm{K},p} & S = \varnothing \end{cases}$. It is well-known that when S is tame: $d(\mathrm{G}_S) > \alpha_{\mathrm{K},S} \Longrightarrow r < d^2/4$. More precisely, if $P(t) = 1 - dt + rt^2$ then $P(t_0) < 0$ for $t_0 = d/2r \in]0, \frac{1}{2}]$.

– For a number field L the root discriminant of L, denoted rd_{L}, is $|\mathrm{Disc}(\mathrm{L})|^{1/[\mathrm{L}:\mathbb{Q}]}$. If J is an infinite algebraic extension of $\mathbb{Q}$, we set $\mathrm{rd}_{\mathrm{J}} := \limsup_{\mathrm{L}} |\mathrm{Disc}(\mathrm{L})|^{1/[\mathrm{L}:\mathbb{Q}]}$ where the limit is taken over all number fields $\mathrm{L} \subset \mathrm{J}$. In the relative setting, e.g L/K, we compute discriminants to K and use the degree of L/K when taking roots.

1. Depth of relations and the Theorem of Golod-Shafarevich

Good references are [**22**, Appendice] and [**20**].

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

Definition 1.1. — Given $x \in \mathrm{G}$, $x \neq 1$, 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:

$$\mathrm{G}_n = \{g \in \mathrm{G}, \omega(g) \geqslant n\},\ n \geqslant 1,$$

and that $I/I^2 \simeq \mathrm{G}/[\mathrm{G},\mathrm{G}]\mathrm{G}^p$, hence, $\mathrm{G}_2 = [\mathrm{G},\mathrm{G}]\mathrm{G}^p$. The sequence G_n is a filtration of open normal subgroups of G.

Proposition 1.2. — *One has the following properties:*

(*i*) *For* $x \in \mathrm{G}$, $\omega(x^p) \geqslant p\omega(x)$. *Hence, if* $x \in \mathrm{G}_n$, *then* $x^p \in \mathrm{G}_{np}$;

(*ii*) *For* $x \in \mathrm{G}_n$ *and* $y \in \mathrm{G}_m$, *one has* $[x,y] \in \mathrm{G}_{n+m}$;

(*iii*) *For* $x, y \in \mathrm{G}$, $\omega(xy) \geqslant \min(\omega(x), \omega(y))$.

Proof. — See §7.4 of [**20**]. □

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

Proposition 1.3. — *The Zassenhaus filtration of a pro-p group* G, *is the minimal filtration on* G *satisfying:*

(*i*) $\omega(\mathrm{G}) \geqslant 1$;

(*ii*) $\omega(x^p) \geqslant p\omega(x)$;

(*iii*) *for all* $\nu > 0$, $\mathrm{G}_\nu := \{x \in \mathrm{G}, \omega(x) \geqslant \nu\}$ *are closed.*

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

1.2. The inequality. — Let G be a finitely generated pro-p group of p-rank d. Let

$$1 \longrightarrow \mathrm{R} \longrightarrow \mathrm{F} \xrightarrow{\varphi} \mathrm{G} \longrightarrow 1$$

be a minimal presentation ($\mathscr{P}$) of G: here F is a free pro-p group on d generators with its Zassenhaus filtration ω.
Suppose that R can be generated by $\{\rho_i, i = 1, \cdots\}$ as a normal subgroup of F. We denote $\mathrm{R} = \langle \rho_i, i = 1, \cdots \rangle^{\mathrm{N}}$. For $k \geqslant 1$, 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 2.7. We denote by

$$P_{\mathscr{P}}(t) := 1 - dt \sum_{k \geqslant 2} r_k t^k \in \mathbb{R}[\![t]\!]$$

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

Theorem 1.4 **(Vinberg [36])**. — *If* G *is finite, then*

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

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

Remark 1.5. — One may have partial information on the depth of the relations. For example, assume that one has only $\omega(\rho_k) \geqslant a_k$ for all k. Then as $1-dt+\sum_{\rho_k} t^{a_k} \geqslant P_{\mathscr{P}}(t)$ (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 '$r \leqslant d^2/4$' that guarantees G is infinite. We say that G *passes the Golod-Shafarevich test* if there exists $t_0 \in]0,1[$ such that $P_{\mathscr{P}}(t_0) < 0$. Observe that if $P_{\mathscr{P}}(t_0) = 0$ then G is infinite, but for many of our applications we need some t_0 such that $P_{\mathscr{P}}(t_0) < 0$. Finally, it is known that if G passes the Golod-Shafarevich test and $d \geqslant 2$, then G is *not* analytic.

1.3. Detecting the depth of an element. — We start with a minimal presentation $(\mathscr{P})$ of G:

$$1 \longrightarrow \mathrm{R} \longrightarrow \mathrm{F} \xrightarrow{\varphi} \mathrm{G} \longrightarrow 1.$$

One has the following result that gives a relation between the Zassenhaus filtrations ω_{F} of F and ω_{G} of G.

Proposition 1.6. — *The Zassenhaus filtration* ω_{G} *of* G *coincides with the filtration quotient of the Zassenhaus filtration* ω_{F} *of* F*: for all* $g \in \mathrm{G}$, $\omega_{\mathrm{G}}(g) = \max\{\omega_{\mathrm{F}}(x), \ \varphi(x) = g\}$. *Hence, for* $n \geqslant 1$,

$$\mathrm{G}_n \simeq \mathrm{F}_n\mathrm{R}/\mathrm{R} \simeq \mathrm{F}_n/\mathrm{F}_n \cap \mathrm{R}.$$

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

Definition 1.7. — The Frattini series of a pro-p group G is defined by $\Phi_1(\mathrm{G}) = G$ and $\Phi_{n+1}(\mathrm{G}) = \mathrm{G}_n^p[\mathrm{G}_n, \mathrm{G}_n]$.

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

Proposition 1.8. — *Put* $\varphi(x) = g \in \mathrm{G}$ *such that* $\omega_{\mathrm{G}}(g) = \omega_{\mathrm{F}}(x)$. *One has* $\omega_{\mathrm{F}}(x) \geqslant k$ *if and only if,* $g \in \mathrm{G}_k$. *In particular,*

(i) $g \in \mathrm{G}^p[\mathrm{G},\mathrm{G}] \implies \omega_{\mathrm{F}}(x) \geqslant 2$*;*

(ii) $g \in \mathrm{G}_2^p[\mathrm{G},\mathrm{G}_2] \implies \omega_{\mathrm{F}}(x) \geqslant 3$*;*

(iii) $g \in \Phi_n(\mathrm{G}) \implies \omega_{\mathrm{F}}(x) \geqslant 2^{n-1}$.

Proof. — *(i)* Recall that $\mathrm{G}_2 = \mathrm{G}^p[\mathrm{G},\mathrm{G}]$.
(ii) Consider the p-central descending series $\mathrm{G}_{(n)}$. Then $\mathrm{G}_{(n)} \subset \mathrm{G}_n$ for all $n \geqslant 1$ (see for example §7 of [**20**]). Hence, if $g \in \mathrm{G}_{(3)} = \mathrm{G}_2^p[\mathrm{G},\mathrm{G}_2]$, then $g \in \mathrm{G}_3$ which is equivalent to $\omega_{\mathrm{G}}(g) \geqslant 3$, and then $\omega_{\mathrm{F}}(x) \geqslant 3$.
(iii) Clearly $\Phi_2(\mathrm{G}) = \mathrm{G}_2$ and as $\Phi_{n+1}(\mathrm{G}) = (\Phi_n(\mathrm{G}))^p[\Phi_n(\mathrm{G}), \Phi_n(\mathrm{G})] \subset \mathrm{G}_{2^n}$. □

1.4. On some special quotients of a pro-p group G. — We study some *infinite* quotients of G.

Proposition 1.9. — *Take $(x_i)_{i\in I} \in \mathrm{G}$ a family of elements of* G *with $\omega_{\mathrm{G}}(x_i) \geqslant 2$ for all x_i. Put $\Gamma := \mathrm{G}/\langle x_i, i \in I\rangle^{\mathrm{N}}$. Suppose that* G *is given by a minimal presentation $(\mathscr{P})$ with a Golod-Shafarevich polynomial $P_{\mathscr{P}}(t)$. Then for the natural minimal presentation*

$$1 \longrightarrow \langle \mathrm{R}, \langle y_i, i \in I\rangle\rangle^{\mathrm{N}} \longrightarrow \mathrm{F} \xrightarrow{\varphi'} \Gamma \longrightarrow 1$$

of Γ, where y_i are chosen such that $\varphi(y_i) = x_i$ and $\omega_{\mathrm{F}}(y_i) = \omega_{\mathrm{G}}(x_i)$, a Golod-Shafarevich polynomial of Γ for this presentation is $P_{\mathscr{P}}(t) + \sum_{i\in I} t^{\omega_{\mathrm{G}}(x_i)}$.

Proof. — Obvious. □

Much of what we need follows from this easy proposition:

Proposition 1.10. — *Let* G *be a finitely presented pro-p group with a minimal presentation $(\mathscr{P})$ and a Golod-Shafarevich polynomial $P_{\mathscr{P}}(t)$ of* G *(following $(\mathscr{P})$). Suppose that $P_{\mathscr{P}}(t_0) < 0$ for some $t_0 \in]0,1[$. Then for suitable $k \geqslant 2$ and $k' \geqslant 2$ we have $P_{\mathscr{P}}(t_0) + t_0^k < 0$ and $P_{\mathscr{P}}(t_0) + \dfrac{t_0^{k'}}{1-t_0} < 0$.*

(i) Let $\mathfrak{f} \in \mathrm{F}$ be such that $\omega_{\mathrm{F}}(\mathfrak{f}) \geqslant k$. Then the group quotient $\mathrm{F}/\langle R, \mathfrak{f}\rangle^{\mathrm{N}} \simeq \mathrm{G}/\varphi(\langle \mathfrak{f}\rangle^{\mathrm{N}})$ is also infinite.

(ii) Take a sequence $(\mathfrak{f}_i)_i \in \mathrm{F}$, $i \geqslant 0$, such that $\omega_{\mathrm{F}}(\mathfrak{f}_i) \geqslant k' + i$. Then the group quotient $\mathrm{F}/\langle \mathrm{R}, \mathfrak{f}_i, i\rangle^{\mathrm{N}} \simeq \mathrm{G}/\varphi(\langle \mathfrak{f}_i, i\rangle^{\mathrm{N}})$ is also infinite.

Proof. — Let us start with a minimal presentation $1 \longrightarrow \mathrm{R} \longrightarrow \mathrm{F} \xrightarrow{\varphi} \mathrm{G} \longrightarrow 1$ of G.
(i). When one adds a relation of depth at least $k \geqslant 2$, the p-rank does not change. Take now the following minimal presentation $(\mathscr{P}')$ of Γ:

$$1 \longrightarrow \mathrm{R}' \longrightarrow \mathrm{F} \longrightarrow \Gamma \longrightarrow 1,$$

where $\mathrm{R}' = \langle \mathfrak{f}, \rho_i, i\rangle^{\mathrm{N}}$, the ρ_i being some generators of R as normal subgroup of F. Now, a polynomial of Golod-Shafarevich for Γ and $(\mathscr{P}')$ can be written as (thanks to Proposition 1.9) $P_{\mathscr{P}'}(t) = P_{\mathscr{P}}(t) + t^k$. But k is chosen so $P_{\mathscr{P}'}(t_0) < 0$, then Theorem 1.4 gives that Γ is infinite.
(ii). Put $\Gamma := \mathrm{G}/\varphi(\langle \mathfrak{f}_i, i\rangle^{\mathrm{N}})$. First, as the elements $\mathfrak{f}_i$ are in $\mathrm{F}_{k'+i}$, with $k' + i \geqslant 2$, then $d_p\Gamma = d_p\mathrm{G} = d$. As in (i), take now the following minimal presentation $(\mathscr{P}')$ of Γ:

$$1 \longrightarrow \mathrm{R}' \longrightarrow \mathrm{F} \longrightarrow \Gamma \longrightarrow 1,$$

where $\mathrm{R}' = \langle \rho_j, \mathfrak{f}_i, i, j\rangle^{\mathrm{N}}$, the ρ_j being some generators of R as normal subgroup of F. Now, a polynomial of Golod-Shafarevich for Γ and $(\mathscr{P}')$ can be written as (thanks to Proposition 1.9):

$$P_{\mathscr{P}'}(t) \leqslant P_{\mathscr{P}}(t) + t^{k'} \sum_{i\geqslant 0} t^i = P_{\mathscr{P}}(t) + t^{k'} \frac{1}{1-t},$$

which is negative at $t = t_0$ by assumption. Apply Theorem 1.4 as in (i). □

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 $m \in \mathbb{Z}_{\geqslant 2}$ such that

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

Lemma 1.11. — *Let* G *be a finitely presented pro-p group such that* $r < d^2/4$ *and* $2r/d > 1$. *Take* λ *and* m *as above. For* $k \geqslant 0$, *take distincts elements* $\mathfrak{f}_{j,k} \in \mathrm{F}$ *with* $j = 1, \cdots, \lambda^{k+m}$, *such that* $\omega_{\mathrm{F}}(\mathfrak{f}_{j,k}) \geqslant m + k$. *Then the group quotient* $\mathrm{G}/\varphi(\langle \mathfrak{f}_{j,k},\ j, k\rangle^{\mathrm{N}})$ *is also infinite.*

Proof. — Put $\Gamma := \mathrm{G}/\varphi(\langle \mathfrak{f}_{j,k}, j, k\rangle^{\mathrm{N}})$. As before the new relations all have depth at least two so $d_p\Gamma = d_p\mathrm{G} = d$. Take for G the polynomial $P_{\mathscr{P}}(t) = 1 - dt + rt^2$. Here, a Golod-Shafarevich polynomial $P_{\mathscr{P}'}$ of Γ can be taken as

$$P_{\mathscr{P}'}(t) = P_{\mathscr{P}}(t) + \sum_{k\geqslant 0}^{\infty} \lambda^{m+k} t^{m+k}.$$

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

$$P_{\mathscr{P}'}(d/2r) \leqslant 1 - \frac{d^2}{4r} + \frac{\left(\frac{\lambda}{a}\right)^m}{1 - \frac{\lambda}{a}} < 0,$$

and Theorem 1.4 applies. □

In Galois contexts the quotients of Proposition 1.9 and Proposition 1.10 correspond to subextensions, so we will use the term 'cut' to apply both to Galois groups and the corresponding towers of fields.

2. Infinitely many splitting in K_S/K

In this section we address a question of Ihara.

2.1. Wilson's result. — Our main result, Theorem 2.7, builds on a group-theoretic result of Wilson [**37**], the number-theoretic interpretation of which we give below.

Theorem 2.1. — *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* $d_p\mathrm{G}_S > \alpha_{\mathrm{K},S}$*). Then there exists an infinite pro-p extension* $\tilde{\mathrm{K}}/\mathrm{K}$ *in* K_S/K *where all Frobenius elements are torsion.*

Proof. — Let $P_{\mathscr{P}}(t)$ 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 $P_{\mathscr{P}}(t_0) = -\delta < 0$ for some $t_0 \in]0, 1[$. Using Proposition 1.2 (i) and Proposition 1.10 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 $P_{\mathscr{P}}(t) + t^{k_1}$ and $P_{\mathscr{P}}(t_0) + t_0^{k_1} < -\delta/2$. Now add in a suitable relation corresponding to a power of x_2 and the new Golod-Shafarevich polynomial with this relation imposed is $P_{\mathscr{P}}(t) + t^{k_1} + t^{k_2}$ and $P_{\mathscr{P}}(t_0) + t_0^{k_1} + t_0^{k_2} < -\delta/2$. Continuing on with powers of x_3, x_4 etc. the resulting series, $\tilde{P}_{\mathscr{P}}(t)$ satisfies $\tilde{P}_{\mathscr{P}}(t_0) \leqslant -\delta/2 < 0$ so the corresponding quotient of G_S, fixing $\tilde{\mathrm{K}}$,

is infinite. By construction, the Frobenius of any unramified prime in this quotient is torsion. □

Remark 2.2. — For extensions for which Frobenius elements have *uniformly bounded* orders see Checcoli [**4**].

Remark 2.3. — Note that every p-adic analytic quotient of the infinite quotient that appears in Theorem 2.1 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}).

2.2. Main result. —

Definition 2.4. — Let K be a number field and let L/K be a (possibly infinite) algebraic extension. The *root discriminant* of K is $\mathrm{rd_K} := |\mathrm{Disc(K)}|^{1/[\mathrm{K}:\mathbb{Q}]}$. The *root discriminant* of L/K is $\limsup_{\mathrm{J}} |\mathrm{Disc(J)}|^{1/[\mathrm{J:K}]}$ where $\mathrm{L} \supset \mathrm{J} \supset \mathrm{K}$ and $[\mathrm{J} : \mathrm{K}] < \infty$.

Definition 2.5. — An infinite extension L/K is called *asymptotically good* if its root discriminant is finite.

Given an (possibly infinite) extension L/K, and a prime $\mathfrak{p}$ of K, let $f(\mathfrak{p})$ be the residue degree extension of $\mathfrak{p}$ in L/K. Put $\mathscr{T}_{\mathrm{L/K}} = \{\mathfrak{p} \subset \mathscr{O}_{\mathrm{K}} \mid \mathfrak{p} \text{ a prime ideal}, f(\mathfrak{p}) < \infty\}$.
We introduce the estimate given by Ihara in [**17**]. See also Tsfasman-Vladut [**35**].

Theorem 2.6. — *Let* L/K *be an infinite asymptotically good extension. Then (assuming the GRH),*

$$\lim_{X\to\infty} \sum_{\mathfrak{p}\in\mathscr{T}_{\mathrm{L/K}}(X)} \frac{\log \mathrm{N}(\mathfrak{p})}{\sqrt{\mathrm{N}(\mathfrak{p})} - 1} < \infty.$$

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

Theorem 2.1 produces asymptotically good extensions L/K where $\mathscr{T}_{\mathrm{L/K}}$ is maximal, namely it consists of all primes of $\mathscr{O}_{\mathrm{K}}$ 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

$$\mathscr{S}_{\mathrm{L/K}} = \{\mathfrak{p} \subset \mathscr{O}_{\mathrm{K}} \mid \mathfrak{p} \text{ a prime ideal}, f(\mathfrak{p}) = 1\},$$

be the set of prime ideals $\mathfrak{p}$ of K that split completely in L/K. Using Proposition 1.10, we will exhibit an asymptotically good extension $\tilde{\mathrm{K}}$/K for which $\mathscr{S}_{\tilde{\mathrm{K}}/\mathrm{K}}$ is infinite.

Theorem 2.7. — *Let* K *be a number field, and S be a finite set of places of* K *coprime to p. Suppose that $d_p \mathrm{G}_S > \alpha_{\mathrm{K},S}$. Then there exists an infinite pro-p extension* $\tilde{\mathrm{K}}$/K *in* K_S/K *for which:*

(*i*) *the set* $\mathscr{S}_{\mathrm{L/K}}$ *is infinite;*

(*ii*) *the set* $\mathscr{T}_{\mathrm{L/K}}$ *is maximal.*

Proof. — Let $1 \longrightarrow \mathrm{R} \longrightarrow \mathrm{F} \xrightarrow{\varphi} \mathrm{G}_S \longrightarrow 1$ be a minimal presentation of G_S. By hypothesis $r < d^2/4$. Take $P_{\mathscr{P}}(t) = 1 - dt + rt^2$ as a Golod-Shafarevich polynomial, and note that $P_{\mathscr{P}}(d/2r) = 1 - d^2/4r < 0$. We will apply Proposition 1.10 (*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 $i \geqslant 2$, denote by

G_i the image $\varphi(\mathrm{F}_i)$; Proposition 1.6 gives that G_i is also the Zassenhaus filtration of G_S. Now, for $i \geqslant 0$, choose a prime ideal $\mathfrak{p}_i$ of $\mathscr{O}_\mathrm{K}$ such that its Frobenius $x_i \in \mathrm{G}_S$ is in $\mathrm{G}_{k'+i}$ (in fact a conjugacy class there), and such that $\mathfrak{p}_i \notin \{\mathfrak{p}_0, \cdots, \mathfrak{p}_{i-1}\}$. Choose $y_i \in \mathrm{F}_{k'+i}$ such that $\varphi(y_i) = x_i$ so $\omega_\mathrm{F}(y_i) \geqslant k' + i$. The quotient Γ of G_S by the normal subgroup generated by the Frobenius x_i of the primes $\mathfrak{p}_i$, $i \geqslant 0$ is

$$\Gamma \simeq \mathrm{G}_S/\langle x_i, i\rangle^\mathrm{N} \simeq \mathrm{F}/\langle \mathrm{R}, y_i, i\rangle^\mathrm{N}.$$

Denote by $\mathrm{L} \subset \mathrm{K}_S$ the fixed field by $\langle x_i,\ i \geqslant 0\rangle^\mathrm{N}$; $\mathrm{Gal}(\mathrm{L}/\mathrm{K}) \simeq \Gamma$. By Proposition 1.10 (ii), the pro-p extension L/K is infinite, and each prime $\mathfrak{p}_i$ has trivial Frobenius in L and thus splits completely; in other words $\mathscr{S}_{\mathrm{L}/\mathrm{K}}$ is infinite. Observe now that we can take

$$P(t) = 1 - dt + rt^2 + \sum_{m>k} t^m = 1 - dt + rt^2 + \frac{t^k}{1-t}$$

as a Golod-Shafarevich series for L/K; here k has been taken such that $P(t_0) < 0$, where $t_0 = d/2r \in]0, \frac{1}{2}]$. Now it suffices to apply Theorem 2.1 to L/K to obtain a subextension $\tilde{\mathrm{K}}/\mathrm{K}$ of L/K for which $\mathscr{T}_{\mathrm{L}/\mathrm{K}}$ is maximal. Moreover as $\mathscr{S}_{\mathrm{L}/\mathrm{K}} \subset \mathscr{S}_{\tilde{\mathrm{K}}/\mathrm{K}}$, then $\mathscr{S}_{\tilde{\mathrm{K}}/\mathrm{K}}$ is infinite. □

Remark 2.8. — Theorem 2.7 is particulary interesting in the context of Tsfasman-Vladut [**35**]. See also Lebacque [**23**].

In Theorem 2.7 one can say a little bit more about $\mathscr{S}_{\mathrm{L}/\mathrm{K}}$. For a (possibly infinite) Galois extension L/K of a number field K, and for $X \geqslant 0$, put

$$\mathscr{S}_{\mathrm{L}/\mathrm{K}}(X) := \{\mathfrak{p} \in \mathscr{S}_{\mathrm{L}/\mathrm{K}},\ \mathrm{N}(\mathfrak{p}) \leqslant X\},\ \text{and}\ \pi_{\mathrm{L}/\mathrm{K}}(X) = |\mathscr{S}_{\mathrm{L}/\mathrm{K}}(X)|\cdot$$

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

Proposition 2.9. — *If* L/K *is asymptotically good, there exists a constant* $B \geqslant 0$ *such that for* $X \geqslant 2$ *(assuming the GRH),*

$$\pi_{\mathrm{L}/\mathrm{K}}(X) \leqslant CX^{1/2}\left([\mathrm{K}:\mathbb{Q}]\log X + \log|\mathrm{disc}(\mathrm{K})| + B\right),$$

where C *is an absolute constant. When* L/K *is unramified, one can take* $B = 0$.

Proof. — Pass to the limit Theorem 4 of [**34**, §2.4]. □

2.3. Norm of ideals in K_S/K**.** — Suppose G_S tame and infinite. Denote by G_n the Zassenhaus filtration of G_S. Suppose moreover that $r < d^2/4$: the pro-p group G_S is not analytic and then $\mathrm{G}_n \neq \mathrm{G}_{n+1}$ for all n (see [**5**, Chapter 11, Theorem 11.4]).

Remark 2.10. — When G_S is tame and infinite, by the tame Fontaine-Mazur conjecture [**7**, Conjecture (5a)] G_S must not be analytic and then $\mathrm{G}_n \neq \mathrm{G}_{n+1}$ for all n.

Definition 2.11. — Let $\mathrm{G} := \mathrm{G}_S$ be tame and infinite. For a prime $\mathfrak{p} \notin S$, denote by $x_\mathfrak{p}$ the Frobenius at $\mathfrak{p}$ in G_S. Define for $i \geqslant 1$,

$$\mathrm{N}_n := \min\{\mathrm{N}(\mathfrak{p}), x_\mathfrak{p} \in \mathrm{G}_n \backslash \mathrm{G}_{n+1}\}.$$

Recall pro-p extensions of a number field that are tamely ramified at a finite set of places are always asymptotically good. One can produce some asymptotic good extensions where the set of splitting is infinite, and in particular, by our construction, the series $\sum_{n\geqslant 2}\frac{\log \mathrm{N}_n}{\sqrt{\mathrm{N}_n}}$ converges.

Theorem 2.12. — *Assume the GRH. Let* K_S/K *be a pro-p and tame extension for which* $d_p\mathrm{G}_S > \alpha_{\mathrm{K},S}$. *Then, considering the Zassenhaus filtration* G_n *of* $\mathrm{G} := \mathrm{G}_S$, *one has along the tower* K_S/K *the estimate: for infinitely many* n,

$$\mathrm{N}_n \gg n^2.$$

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

Definition 2.13. — Set $\mathrm{G} := \mathrm{G}_S$ be tame and infinite, and for a prime $\mathfrak{p}$ denote by $x_\mathfrak{p}$ the Frobenius at $\mathfrak{p}$ in G. Define for $n \geqslant 1$, and $k \in \mathbb{Z}_{\geqslant 1}$,

$$\mathrm{N}_n^{(k)} := \text{the kth smallest norm of a prime } \mathfrak{p} \text{ with } x_\mathfrak{p} \in \mathrm{G}_n\backslash\mathrm{G}_{n+1}.$$

Of course, $\mathrm{N}_n^{(1)} = \mathrm{N}_n$.

Theorem 2.14. — *Assume the GRH. Let* G_S *be the Galois group of a tame p-tower for which* $r < d^2/4$. *Choose* λ *and* m *as for Lemma 1.11. Put* $\beta_{k,m} := \lambda^{k+m}$. *Then for infinitely many* k,

$$\mathrm{N}_k^{(\beta_{k,m})} \gg \lambda^{2k}.$$

Proof. — Set $\mathrm{G} := \mathrm{G}_S$. Observe that here $r-d \geqslant 0$. For $k \geqslant 0$, let us choose λ^{k+m} different prime ideals $\mathfrak{p}_{i,k} \subset \mathscr{O}_\mathrm{K}$ (of smallest norm as possible) such that $x_{\mathfrak{p}_{i,k}} \in \mathrm{G}_{m+k}\backslash\mathrm{G}_{m+k+1}$. The element $x_{\mathfrak{p}_{i,k}}$ is of depth $m+k$. Denote by $\tilde{\mathrm{K}} := \mathrm{K}_S^{\langle\varphi(y_{i,k}),\ i,k\rangle^\mathrm{N}}$. Then Lemma 1.11 implies that $\tilde{\mathrm{K}}/\mathrm{K}$ is infinite: it is an asymptotically good extension where each prime $\mathfrak{p}_{i,k}$ splits completely. Put $\beta_{k,m} := \lambda^{k+m}$. Then by the estimation of Ihara (Theorem 2.6) for $\tilde{\mathrm{K}}/\mathrm{K}$, one has:

$$\sum_{k\geqslant 0}\lambda^{k+m}\frac{\log \mathrm{N}_k^{(\beta_{k,m})}}{\sqrt{\mathrm{N}_k^{(\beta_{k,m})}}} < \infty,$$

which implies that $\mathrm{N}_k^{(\beta_{k,m})} \gg \lambda^{2k+2m}$ for infinitely many k. □

2.4. The case of the center. — Using Proposition 1.10, 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 generator of G_S with Zassenhaus filtration ω_G. Let x be a non-trivial Frobenius element in G_S. Then $\omega_\mathrm{G}([x, a_i]) \geqslant 1 + \omega_\mathrm{G}(x)$. Hence, assuming that G_S passes the Golod-Shafarevich test ($r < d^2/4$), we are guaranteed that when $\omega_\mathrm{G}(x)$ is large then $\Gamma := \mathrm{G}_S/\langle[x, a_i], i = 1, \cdots d\rangle^\mathrm{N}$ is also infinite.

Proposition 2.15. — *The class of the Frobenius element* x *in* Γ *is non-trivial and is in the center* $Z(\Gamma)$ *of* Γ.

Proof. — In Γ, 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 Γ. That $\omega_\mathrm{G}([x, a_i]) > \omega_\mathrm{G}(x)$ implies x is not trivial in Γ. □

Now let us remark that $\langle [x, a_i], i = 1, \cdots, d\rangle \subset \langle x\rangle^{\mathrm{N}}$, hence

$$\Gamma := \mathrm{G}_S/\langle [x, a_i], i = 1, \cdots, d\rangle^{\mathrm{N}} \twoheadrightarrow \Gamma' := \mathrm{G}_S/\langle x\rangle^{\mathrm{N}}.$$

Here for the infiniteness of Γ one has to check if

$$1 - dt + rt^2 + dt^{1+k} \tag{1}$$

has a root in $]0, 1[$. For the quotient Γ', one has to check if

$$1 - dt + rt^2 + t^k \tag{2}$$

has a root in $]0, 1[$. Some easy algebra shows that (2) is stronger than (1): in other words, to prove that Γ is infinite it is better to use the criteria for Γ'. 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 Γ' is infinite and we can only conclude that Γ is infinite as it has Γ' as a quotient. Note:

Proposition 2.16. — *Suppose that all primes in S are coprime to p. The pro-p group Γ is infinite if and only if Γ' is infinite.*

Proof. — Clearly $\#\Gamma' = \infty \implies \#\Gamma = \infty$.
Let N and N′ be the kernels of the maps $\mathrm{G}_S \twoheadrightarrow \Gamma$ and $\mathrm{G}_S \twoheadrightarrow \Gamma'$. If Γ' is finite then $\mathrm{K}_S^{\mathrm{N}'}$ is a number field and $\mathrm{K}_S^{\mathrm{N}}/\mathrm{K}_S^{\mathrm{N}'}$ is a finitely generated tamely ramified abelian p-extension. By class field theory such extensions are always finite so $\mathrm{K}_S^{\mathrm{N}}/\mathrm{K}$ is finite and thus Γ is finite. □

This situation shows that some cuts may be not optimal.

3. 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 $[\mathrm{K} : \mathbb{Q}] = n$, the root discriminant of K, denoted rd_{K}, is $|\mathrm{disc}(\mathrm{K})|^{1/n}$. 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 this lim sup is ∞. 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 $\gamma := \lim_{n\to\infty} \left(\left(\sum_{k=1}^{n} \frac{1}{k}\right) - \log n\right)$. The current GRH lower bounds for infinite towers are $8\pi e^{\gamma} \approx 44.763$ for totally complex fields and $8\pi e^{\gamma+\frac{\pi}{2}} \approx 215.33$ for totally real fields. See [**30**] 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-Sharafevich criterion, and the root discriminants can be bounded by tame ramification theory. Here we improve their results by using our technique of cutting towers.

3.1. Tame towers with finite ramification-exponent. — We will again use Proposition 1.10. The set S will consist of $\mathfrak{p}$ with $\mathrm{N}(\mathfrak{p}) \equiv 1 \bmod p$. Recall that $d = d_p H^1(\mathrm{G}_S) = d_p \mathrm{G}_S$ is the p-rank of G_S and $r = d_p H^2(\mathrm{G}_S)$ is the minimal number of relations of G_S.

Definition 3.1. — Fix $k \geqslant 1$. Denote by $\mathrm{K}_S^{[k]}/\mathrm{K}$ the maximal pro-p extension of K unramified outside S and where the exponent of ramification at $\mathfrak{p} \in S$ is at most p^k so $\mathrm{K}_S^{[\infty]} = \mathrm{K}_S$. Put $\mathrm{G}_S^{[k]} := \mathrm{Gal}(\mathrm{K}_S^{[k]}/\mathrm{K})$.

Remark 3.2. — The extension $\mathrm{K}_S^{[k]}/\mathrm{K}$ is well-defined because inertia groups are cyclic in the tame case.

Proposition 3.3. — *Assume that $r < d^2/4$. Put $k_0 = \lceil \log(\frac{d^2}{4r} - 1)/\log(d/2r) \rceil$. Then, for $k \geqslant \log_p(k_0)$, the extension $\mathrm{K}_S^{[k]}/\mathrm{K}$ is infinite.*

Proof. — We follow the notations of Proposition 1.10. We have chosen k_0 so that $P_{\mathscr{P}'}(t) = 1 - dt + rt^2 + t^{k_0}$ is negative at $t = d/2r$. Take as x a generator of the inertia group at $\mathfrak{p}$ in K_S/K, cut by x^{p^k} and apply Proposition 1.10 (i). □

Recall the root discriminant of a number field K is denoted by rd_K. The interest of extensions as above is the following:

Proposition 3.4. — *In the tower $\mathrm{K}_S^{[k]}/\mathrm{K}$ the root discriminant is bounded by*

$$\mathrm{rd}_\mathrm{K} \cdot \left(\mathrm{N}(\mathfrak{p})^{\frac{1}{[\mathrm{K}:\mathbb{Q}]}}\right)^{1-\frac{1}{p^k}}.$$

Proof. — The result follows from the basic theory of tame ramification. □

In [**13**] it is shown, by taking the limit in the above Proposition, that the root discriminant of $\mathrm{K}_S/\mathrm{K} = \mathrm{K}_S^{[\infty]}/\mathrm{K}$ is bounded by $\mathrm{rd}_\mathrm{K} \cdot \left(\mathrm{N}(\mathfrak{p})^{\frac{1}{[\mathrm{K}:\mathbb{Q}]}}\right)$.
We can now give an answer to a central question of [**12**]:

Theorem 3.5. — *Suppose $S \neq \varnothing$ such that $d_p \mathrm{G}_S > \alpha_{\mathrm{K},S}$. Then there exists a finite extension L/K in K_S/K such that $\mathrm{L}_\varnothing/\mathrm{L}$ is infinite.*

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

3.2. Some set up. — Let K be a number field and S a finite set of finite places of K. Let

$$\mathrm{V}_S = \{x \in \mathrm{K}^\times \mid x \in (\mathrm{K}_v^\times)^p \text{ for } v \in S, \text{ and } v(x) \equiv 0 \bmod p, \forall\, v\}$$

and let Б_S to be the character group of $\mathrm{V}_S/(\mathrm{K}^\times)^p$. Recall the exact sequence

$$0 \to Ш_S^2 \to H^2(\mathrm{G}_S) \to \oplus_{v \in S} H^2(G_{\mathrm{K}_v})$$

where each term on the right is just $\mathbb{Z}/p\mathbb{Z}$ or 0 depending on $\delta_{\mathrm{K}_v,p} = 1$ or 0; observe also that when $\delta_{\mathrm{K},p} \neq 0$, 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

$$d_p\mathrm{G}_S = \left(\sum_{v\in S_p}[\mathrm{K}_v:\mathbb{Q}_v]\right) - \delta_{\mathrm{K},p} + \left(\sum_{v\in S}\delta_{\mathrm{K}_v,p}\right) - (r_1+r_2) + 1 + d_p(\text{Б}_S) \tag{3}$$

and there is a natural injection $Ш^2_S \hookrightarrow \text{Б}_S$ which is an isomorphism if S contains all primes of K dividing p (and infinity for $p = 2$).

Remark 3.6. — 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 $d_p\mathrm{G}_S$ in many cases, thus giving $d_p\text{Б}_S$ exactly and the upper bound $r(\mathrm{G}_S) \leqslant \begin{cases} d_p\text{Б}_\varnothing & S = \varnothing \\ d_p\text{Б}_S + |S| - \delta_{\mathrm{K},p} & S \neq \varnothing \end{cases}$.

3.3. Examples and records. — For various computations of H^1s and ray class groups we have used the software packages PARI/GP [**32**] and MAGMA [**3**]. We take always $p = 2$ in this subsection.

3.3.1. 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 $\dim \text{Б}_\varnothing = 16$ so $\dim H^2(\mathrm{G}_\varnothing) = \dim Ш^2_\varnothing \leqslant \dim \text{Б}_\varnothing = 16$. The Golod-Shafarevich polynomial is (at worst) $P(t) = 1 - 8t + 16t^2$. Note $P(1/4) = 0$ so $\mathrm{G}_\varnothing$ is infinite. As Martin's thesis is unpublished, we record his polynomial here: $x^8 - 3297x^6 + 14790x^5 + 3555341x^4 - 24457440x^3 - 1347361755x^2 + 7744222350x + 149856133975$. 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.

3.3.2. The totally complex case. —

• Take $\mathrm{K} = \mathbb{Q}(\sqrt{13}, \sqrt{-3\cdot 5\cdot 17})$. Software gives $d_2\mathrm{G}_\varnothing = 4$ so Equation (3) gives $d_2\text{Б}_\varnothing = 6$. The Golod-Shafarevich polynomial $1 - 4t + 6t^2$ has no root so we cannot conclude $G_\varnothing$ is infinite. There are two primes above 43 in K, both having norm 43^2. Take S to be either of these. We write $S = \{\mathfrak{p}_{43^2}\}$. Software gives that $d_2\mathrm{G}_S = 5$ so $d_2\text{Б}_S = 6$ and $r(\mathrm{G}_S) \leqslant 6 + 1 - 1 = 6$. In this case the Golod-Shafarevich polynomial $1 - 5t + 6t^2$ has a root in $]0,1[$. As $d_2\mathrm{G}_\varnothing = 4 < 5 = d_2\mathrm{G}_S$, the generator of inertia $\tau_{\mathfrak{p}_{43^2}} \in \mathrm{G}_S$ has depth 1 by Proposition 1.8 (*iii*). We cut G_S by the relation $\tau^4_{\mathfrak{p}_{43^2}}$ which has depth at least 4 by Proposition 1.2. As $1 - 5t^2 + 6t^2 + t^4$ has a root in $]0,1[$, the group $\mathrm{G}_S^{[2]}$ is infinite, and in this tower one has:

$$\mathrm{rd}_{\mathrm{K}_S^{[2]}} = \mathrm{rd}_\mathrm{K}\cdot(43^2)^{\frac{1}{4}\cdot(1-\frac{1}{4})} < 235.9351.$$

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

$$\mathrm{rd}_\mathrm{K} < 75.7332,\ d_2G_\varnothing = 7 \text{ and } d_2\text{Б}_\varnothing = 13.$$

The Golod-Shafarevich polynomial $1-7t+13t^2$ has no root so we set S to be the one prime $\mathfrak{p}_9$ above 3. It has norm 9 and software gives $d_2\mathrm{G}_S = d_2\mathrm{G}_\varnothing = 7$ so $\tau_{\mathfrak{p}_9}$ is of depth at least 2 by Proposition 1.8 (*iii*) and $\tau_{\mathfrak{p}_9}^2$ has depth at least 4. One sees that $d_2\text{Б}_S = 12$ and $r(\mathrm{G}_S) \leqslant 12$. As $1-7t+12t^2$ has a root in $]0,1[$, G_S is infinite. After cutting by $\tau_{\mathfrak{p}_9}$, our Golod-Shafarevich polynomial $1-7t+12t^2+t^4$ has a root in $]0,1[$ so $\mathrm{G}_S^{[1]}$ is infinite and

$$\mathrm{rd}_{\mathrm{K}_S^{[1]}} = \mathrm{rd}_\mathrm{K} \cdot (9)^{\frac{1}{12}\cdot(1-\frac{1}{2})} < 82.9940.$$

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 $\mathrm{Gal}(\mathrm{H}/\mathrm{K}) \simeq (\mathbb{Z}/2)^6$ so

$$d_2\mathrm{G}_\varnothing = 6,\ d_2\text{Б}_\varnothing = 6+r_2 = 6+6 = 12 \text{ and } r(G_\varnothing) \leqslant 12.$$

The polynomial $1-6t+12t^2$ is always positive so we cannot conclude that the maximal pro-2 quotient of $\mathrm{G}_\varnothing$ is infinite. Here $\mathrm{rd}_\mathrm{K} < 68.3636$. Now take $S = \{\mathfrak{p}_9\}$, the unique prime above 3 of norm 9. Software gives $d_2\mathrm{G}_S = 7$ so $d_2\text{Б}_S = 12$ and we have the bound $r(\mathrm{G}_S) \leqslant 12+1-1 = 12$. The polynomial $1-7t+12t^2$ has a root in $]0,1[$ so G_S is infinite. As $d_2\mathrm{G}_\varnothing = 6 < 7 = d_2\mathrm{G}_S$, $\tau_{\mathfrak{p}_9}$ has depth 1. We cut by $\tau_{\mathfrak{p}_9}^4$ to get Golod-Shafarevich polynomial $1-7t+12t^2+t^4$ which has a root in $]0,1[$ so $\mathrm{G}_S^{[2]}$ is infinite, and in this tower

$$\mathrm{rd}_{\mathrm{K}_S^{[2]}} = \mathrm{rd}_\mathrm{K} \cdot (9)^{\frac{1}{12}\cdot(1-\frac{1}{4})} < 78.4269.$$

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

3.3.3. 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 $\mathbb{Q}$. It's polynomial is $x^{12}-56966x^{10}+959048181x^8-5946482981439x^6+14419821937918124x^4-1270542597983552994 1x^2+352705306960207836 8989$ and $\mathrm{rd}_K < 770.6432$. All primes above 13 in K have norm 13. Take S to be any one of them. Software gives

$$d_2\mathrm{G}_\varnothing = d_2\mathrm{G}_S = 9,\ d_2\text{Б}_\varnothing = 21 \text{ and } d_2\text{Б}_S = 20.$$

The Golod-Shafarevich polynomial for $\mathrm{G}_\varnothing$ is $1-9t+21t^2$ and has no root in $]0,1[$ so we cannot conclude $G_\varnothing$ 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 $d_2G_\varnothing = d_2\mathrm{G}_S = 9$ we see $\tau_{\mathfrak{p}_{13}}$ has depth at least 2 by Proposition 1.8 (*iii*). We cut by $\tau_{\mathfrak{p}_{13}}^2$ which has depth at least 4. As $1-9t+20t^2+t^4$ has a root in $]0,1[$ $\mathrm{K}_S^{[1]}/\mathrm{K}$ is infinite and

$$\mathrm{rd}_{\mathrm{K}_S^{[1]}} = \mathrm{rd}_\mathrm{K} \cdot (13)^{\frac{1}{12}\cdot(1-\frac{1}{2})} < 857.5662.$$

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

3.3.4. Comments. — In the example above, a hope would be that $\tau_{\mathfrak{p}_{13}}$ has depth greater than two in G_S. In that case we could cut by the relation $\tau_{\mathfrak{p}_{13}}$ and the corresponding Golod-Shafarevich polynomial would be at most $1-9t+20t^2+t^3$ 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 $\tau_{\mathfrak{p}_{13}}$ in G_S. See also the beginning of §5.

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 $\partial(\mathrm{K}) = \log(\mathrm{Rd}_{\mathrm{K}}/\alpha)$ where $\alpha = 44.763$ if K is totally imaginary or $\alpha = 215.33$ if K is totally real. Let us recall the different improvements. The ordered pairs in the table below are $(rd_{\mathrm{K}}, \partial)$.

Signature	Martinet (1978)	Hajir-Maire (2002)	Martin (2006)	new records
tot. compl.	(92.368; 0.7244)	(82.1004; 0.6066)		(78.427; 0.5608)
tot. real	(1058.565; 1.592)	(954.293; 1.488)	(913.493; 1.445)	(857.567; 1.382)

The recent improvement of ∂ in the totally imaginary case is 7.55%, and 4.36% for the totally real case.

4. Cutting of wild towers

4.1. Local abelian extensions. — For this section, our results follow from this main observation: *we can cut wildly ramified towers if we first cut by local commutators*. We also assume throughout this section that in our wild extensions, the assertion of Kuz'min's Theorem holds, that is the pro-2 local Galois groups above (2) are maximal. In the first totally complex example of §4.2 the hypotheses of Kuz'min'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 4.1. — Take $S = S_p$ the set of p-adic places. Denote by $\mathrm{K}_S^{[k],p-ab}/\mathrm{K}$ the maximal pro-p extension unramified outside S, locally abelian at p (and then at all places), and for which the inertia groups at $v|p$ are of exponent dividing p^k. Put $\mathrm{G}_S^{[k],p-ab} = \mathrm{Gal}(\mathrm{K}_S^{[k],p-ab}/\mathrm{K})$.

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

Theorem 4.2. — *Take $p = 2$ and $S = S_p$. In $\mathrm{K}_S^{[1],p-ab}/\mathrm{K}$, the root discriminant is bounded by* $\mathrm{rd}_{\mathrm{K}} \cdot 2^{\frac{\sum_{v|p} f_v\left(2+\frac{1}{e_v}-\frac{1}{2^{e_v f_v}}\right)}{[\mathrm{K}:\mathbb{Q}]}}$.

Proof. — Fix a place $v|2$ of K. By Kummer's theory, the quadratic extensions of K_v are parametrized by the classes of $\mathrm{K}_v^{\times}/\mathrm{K}_v^{\times 2} \simeq \langle\pi_v\rangle/\langle\pi_v^2\rangle \times U_v/U_v^2$ 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 π^{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

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

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

Remark 4.3. — One has $\mathrm{G}_{S_p}/\langle[D_v,D_v],v|p\rangle\twoheadrightarrow\mathrm{G}_{S_p}^{ab}:=\mathrm{G}_S/[\mathrm{G}_S,\mathrm{G}_S]$ and then the maximal local abelian extension $\mathrm{K}_{S_p}^{p-ab}/\mathrm{K}$ of $\mathrm{K}_{S_p}/\mathrm{K}$ is infinite (it contains the cyclotomic extension). In order to have a criteria proving that $\mathrm{K}_S^{[k],p-ab}/\mathrm{K}$ is infinite, we need a Golod-Shafarevich polynomial of $\mathrm{K}_S^{p-ab}/\mathrm{K}$ to have a root in $]0,1[$.

4.2. Examples. —

4.2.1. — Take $\mathrm{K}=\mathbb{Q}(\sqrt{-8\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13})$ and $p=2$. Software gives $\mathrm{G}_\varnothing^{ab}\simeq\mathbb{Z}/8\times(\mathbb{Z}/2)^4$, and for $S=\{\mathfrak{p}_2\}$, the unique prime above 2, $\mathrm{G}_S^{ab}\simeq\mathbb{Z}_2^2\times(\mathbb{Z}/2\mathbb{Z})^4$. Also $\mathfrak{p}_2$ is not principal and thus its Frobenius in $G_\varnothing$ has depth 1.
In this totally complex wild case, global duality implies the natural injection $Ш_S^2\hookrightarrow Б_S$ from §3.2 is an isomorphism and $r=r(G_S)=d-1-r_2=4$.
Recall that the decomposition group at $\mathfrak{p}_2$ in G_S has at most 4 generators, as a quotient of $\mathrm{G}_\mathfrak{p}=\mathrm{Gal}(\overline{\mathrm{K}}_\mathfrak{p}/\mathrm{K}_\mathfrak{p})$ this last group being isomorphic to the Demushkin group with 4 generators (here $\overline{\mathrm{K}}_\mathfrak{p}$ is the maximal pro-p extension of the complete field $\mathrm{K}_\mathfrak{p}$). Denote by $\langle x,y,z,t\rangle$ these generators viewed in G_S. The structures of $\mathrm{G}_\varnothing^{ab}=\mathrm{G}_\varnothing/[\mathrm{G}_\varnothing,\mathrm{G}_\varnothing]$ and of G_S^{ab} show that the elements x,y,z,t can be choosen such that t (Frobenius) has depth 1 as does x, in inertia group. The other variables, 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 1.10 to cut the ramification at a certain depth; observe that the ramification in $\mathrm{Gal}(\mathrm{K}_{S_p}^{2-ab}/\mathrm{K})$ is generated by the classes of x,y,z and its quotient $\mathrm{G}_S^{[1],2-ab}$ 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 $\mathrm{K}_S^{[1],2-ab}/\mathrm{K}$ is bounded by $\mathrm{rd}_\mathrm{K} \cdot 2^{9/8} < 755.90358\cdots$, thanks to Theorem 4.2.

4.2.2. — 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,
- $d_2\mathrm{G}_S = 18$, and Equation (3) implies $\text{Б}_S = 0$ so $Ш_S^2 = 0$ as well,
- $r(G_S) \leqslant 17$ 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 square of the generators of the abelian local inertia at the wild places (observe that we can take a generator of order 2), i.e by 12 elements of depth at least 2,
- the fourth of the generators of the inertia at three places dividing 5,
- the square of the generators of the inertia of the other eleven places dividing $3 \cdot 5 \cdot 7$.

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

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

4.3. Cutting a p-rational tower. —

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

Definition 4.4. — 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-Maire [**15**], etc. An easy argument from group theory gives:

Proposition 4.5. — *Let* K *be a p-rational field and let* L/K *be a finite extension in* $\mathrm{K}_{S_p}/\mathrm{K}$. *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 $\mathrm{G}_{S_p}^{ab}$ is torsion-free. The torsion of $\mathrm{G}_{S_p}^{ab}$ can be estimated by class field theory: in particular for p sufficiently large this torsion is isomorphic to the p-part of $\left(\prod_{v \in S_p} U_v\right) / \overline{\mathscr{O}_\mathrm{K}^\times}$ which is easy to compute. After many observations Gras [**8**, Conjecture 7.11] recently made the following conjecture:

Conjecture 4.6 **(Gras)**. — *Given a number field* K*, then for large p,* K *is p-rational.*

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

4.3.2. Results. — First, we obtain:

Theorem 4.7. — *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* $\mathrm{K}/\mathbb{Q}$ *and,* (*ii*) K *is p-rational. Then there exists a number field* L/K *in* $\mathrm{K}_{S_p}/\mathrm{K}$ *such that* $\mathrm{L}_\varnothing/\mathrm{L}$ *is infinite. Note that as Gal*$(\mathrm{L}_{S_p}/\mathrm{L})$ *is a subgroup of the free pro-p group Gal*$(\mathrm{K}_{S_p}/\mathrm{K})$ *then* L *is p-rational.*

Proof. — Let $p > 2$. As p splits completely in K, $\mu_p \nsubseteq \mathrm{K}_v$ and G_v is a free pro-p group on 2 generators x_v, τ_v, where x_v can be chosen as the Frobenius and τ_v as a generator of the inertia group.
Suppose moreover that $\mathrm{G} := \mathrm{G}_{S_p}$ is p-rational. Then we cut the free pro-p group G on $r_2 + 1$ generators by all the commutators $[x_v, \tau_v]$ for all $v|p$, to obtain a pro-p extension $\mathrm{K}_{S_p}^{p-ab}/\mathrm{K}$ 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 $\Gamma := \mathrm{Gal}(\mathrm{K}_{S_p}^{p-ab}/\mathrm{K})$. A naive presentation $(\mathscr{P})$ of Γ allows us to obtain the Golod-Shafarevich polynomial

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

As $r_2 \geqslant 6$, we easily compute that $P_{\mathscr{P}}$ is negative on $]0, 1[$, and so for a large given k, if we cut by the powers $\tau_v^{p^k}$ of τ_v, $v|p$, the extension $\mathrm{K}_S^{[k],p-ab}/\mathrm{K}$ is infinite. As $\mathbb{Z}/p^k$ maps onto the inertia group of all $\mathfrak{p}|p$, one concludes by a changing the base field. □

Recall that if a pro-p group G passes the test of Golod-Shafarevich, then G is not p-adic analytic (when $d \geqslant 3$) and, by Lubotzky-Mann [**24**], the p-rank of the open subgroups U of G tends to infinity with $[\mathrm{G} : U]$. In fact, one has the following due to Jaikin-Zapirain (see [**18**] or [**6**, Theorem 8.3]):

Theorem 4.8 **(Jaikin-Zapirain)**. — *Suppose that a pro-p group G passes the Golod-Shafarevich test. Then there exist infinitely many n such that* $\log_p d_p\mathrm{G}_n \geqslant (\log_p[\mathrm{G} : \mathrm{G}_n])^\beta$, *for some* $\beta \in]0, 1[$, *where* G_n *is the Zassenahaus filtration of* G.

In our context, as corollary, one obtains:

Corollary 4.9. — *Let* K *be a totally imaginary field of degree at least* 12 *over* $\mathbb{Q}$. *Choose* $p > 2$ *such that :* (*i*) *p splits totally in* $\mathrm{K}/\mathbb{Q}$ *and,* (*ii*) K *is p-rational. Then there exists a constant* $\beta > 0$ *and a sequence of p-rational number fields* (L_n) *in* $\mathrm{K}_{S_p}/\mathrm{K}$ *such that*

$$\log d_p\mathrm{Cl}_{\mathrm{L}_n} \gg (\log[\mathrm{L}_n : \mathbb{Q}])^\beta,$$

where $\mathrm{Cl}_{\mathrm{L}_n}$ *is the class group of* L_n.

Proof. — Choose k as in proof of Theorem 4.7 such that $\mathrm{K}_{S_p}^{[k],p-ab}/\mathrm{K}$ is infinite. Put $\mathrm{G} = \mathrm{Gal}(\mathrm{K}_{S_p}^{[k],p-ab}/\mathrm{K})$, and consider G_n the Zassenhaus filtration of G. Let K_n be the subfield of $\mathrm{K}_{S_p}^{[k],p-ab}/\mathrm{K}$ fixed by G_n: by Proposition 4.5 all the fields K_n are p-rational. Take n_0 large enough so that the pro-p extension $\mathrm{K}_{S_p}^{[k],p-ab}/\mathrm{K}_{n_0}$ 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 4.8, for infinitely many $n \geqslant n_0$, we get $\log_p d_p\mathrm{G}_n \geqslant (\log_p[\mathrm{G} : \mathrm{G}_n])^\beta$, for some $\beta \in]0, 1[$. To conclude it suffices to note that for $n \geqslant n_0$ the extension $\mathrm{K}_{S_p}^{[k],p-ab}/\mathrm{K}_n$ is unramified, and then by class field theory one has $d_p\mathrm{Cl}_{\mathrm{K}_n} \geqslant d_p\mathrm{G}_n$. □

5. Depth of ramification

5.1. 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 §3.3.2 where $(d, r) = (9, 21)$.

Suppose that $\mathrm{G}_\varnothing$ has P as Golod-Shafarevich polynomial for a certain minimal presentation $(\mathscr{P})$. Then with $S = \{\mathfrak{p}\}$, $\mathfrak{p}$ coprime to p, and when $\mu_p \subset \mathrm{K}$, the group G_S has parameters $(d, r-1)$, or $(d+1, r)$. If $r > 1$, it is easy to see G_S is infinite in either case. Suppose now that the generator of inertia at $\mathfrak{p}$, $\tau_\mathfrak{p}$, has depth at least k in G_S. If we cut G_S by $\langle \tau_\mathfrak{p} \rangle$, 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 $\tau_\mathfrak{p}$ and observe $\mathrm{K}_\varnothing/\mathrm{K}$ is infinite. For $(d, r) = (9, 21)$ we need $k \geqslant 3$.

Question 5.1. — *Suppose G_S is infinite. To simplify, take $S = \{\mathfrak{p}\}$ with $\mathfrak{p}$ coprime to p. How deep can the generator $\tau_\mathfrak{p}$ of tame inertia be in G_S?*

5.2. Add a splitting condition. —

5.2.1. Detect the level of inertia. — Let S and T be finite disjoint sets of primes of K. We denote by K_S^T the maximal pro-p subextension of K_S/K where all places of T split completely. Put $\mathrm{G}_S^T = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$. Consider the Frattini series $\Phi_n(\mathrm{G}_\varnothing^T)$ and $\Phi_n(\mathrm{G}_S^T)$. Set $\mathrm{K}_n := (\mathrm{K}_\varnothing^T)^{\Phi_n(\mathrm{G}_\varnothing^T)}$. We abuse notation and set $\omega := \omega_{\mathrm{G}_S^T}$.
If L/K is a finite subextension of $\mathrm{K}_S^T/\mathrm{K}$, we denote by $\mathrm{G}_{\mathrm{L},S}^T$ the Galois group $\mathrm{Gal}(\mathrm{L}_S^T/\mathrm{L})$.
To simplify, we assume that $S = \{\mathfrak{p}\}$ where $\mathfrak{p} \subset \mathscr{O}_\mathrm{K}$ is coprime to p. Let $\tau_\mathfrak{p} \in \mathrm{G}_S^T$ be a generator of the inertia group at $\mathfrak{p}$ in $\mathrm{K}_S^T/\mathrm{K}$.

Lemma 5.2. — *If $d_p\mathrm{G}_{\mathrm{K}_n,\varnothing}^T = d_p\mathrm{G}_{\mathrm{K}_n,S}^T$ for some n, then $\omega(\tau_\mathfrak{p}) \geqslant 2^n$.*

Proof. — For $m \geqslant 1$, write $\mathrm{K}'_m = (\mathrm{K}_S^T)^{\Phi_m(\mathrm{G}_S^T)}$. If, for $i \leqslant n+1$, we had a p-extension of K_i unramified outside S but actually ramified there, we could take its composite with the unramified extension $\mathrm{K}_n/\mathrm{K}_i$ to contradict the equality of our hypothesis. Thus $d_p\mathrm{G}_{\mathrm{K}_i,\varnothing}^T = d_p\mathrm{G}_{\mathrm{K}_i,S}^T$ for all $i \leqslant n+1$. Hence, one has $\mathrm{K}_2 = \mathrm{K}'_2$, then $\mathrm{K}_3 = \mathrm{K}'_3$ etc. up to $\mathrm{K}_{n+1} = \mathrm{K}'_{n+1}$. In particular the extension $\mathrm{K}'_{n+1}/\mathrm{K}$ is unramified and $\tau_\mathfrak{p} \in \Phi_{n+1}(\mathrm{G}_S^T)$; in other words $\mathrm{G}_S^T/\Phi_{n+1}(\mathrm{G}_S^T) \simeq \mathrm{G}_\varnothing^T/\Phi_{n+1}(\mathrm{G}_\varnothing^T)$. By Proposition 1.8 (*iii*), we get $\omega(\tau_\mathfrak{p}) \geqslant 2^n$. □

5.2.2. Depth and freeness. — Recall from §3.2 that

$$\mathrm{V}_S = \{x \in \mathrm{K}^\times | x \in (\mathrm{K}_v^\times)^p \ \forall v \in S \text{ and } v(x) \equiv 0 \bmod p, \ \forall v\}$$

and set

$$\mathrm{V}^T = \{x \in \mathrm{K}^\times |\ v(x) \equiv\ 0 \bmod p, \ \forall v \notin T\}$$

and

$$\mathrm{V}_S^T = \{x \in \mathrm{K}^\times | x \in (\mathrm{K}_v^\times)^p \,\forall\, v \in S \text{ and } v(x) \equiv\ 0 \bmod p, \ \forall v \notin T\}.$$

Note $\mathrm{V}_S^\varnothing = \mathrm{V}_S$. If we switch fields to some $\mathrm{L} \supseteq \mathrm{K}$, we will include the field in the notation to avoid confusion, e.g. V_L^T or $\mathrm{V}_{\mathrm{L},S}^T$. One has

$$1 \longrightarrow \mathscr{O}_{\mathrm{K},T}^\times/(\mathscr{O}_{\mathrm{K},T}^\times)^p \longrightarrow \mathrm{V}_\mathrm{K}^T/(\mathrm{K}^\times)^p \longrightarrow \mathrm{Cl}_\mathrm{K}^T[p] \longrightarrow 1, \tag{4}$$

where $\mathscr{O}_{\mathrm{K},T}^\times$ denotes the group of T-units of K and Cl_K^T the p-Sylow subgroup of the T-class group of K. Put $\mathrm{K}' := \mathrm{K}(\mu_p)$ and $\mathrm{K}'_{(T)} = \mathrm{K}'(\sqrt[p]{\mathrm{V}^T})$. One has [**9**, Chapter V,

Corollary 2.4.2] involving the Artin symbol $\left(\frac{\mathrm{K}'_{(T)}/\mathrm{K}'}{\cdot}\right)$ in $\mathrm{Gal}(\mathrm{K}'_{(T)}/\mathrm{K}')$. Note that S and T there are our T and S here respectively.

***Theorem 5.3* (Gras).** — *Let $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$ be a tame set of primes of* K. *There exists a cyclic degree p extension* F/K*, unramified outside S, totally ramified at S, and where each place of T splits completely, if and only if for $i = 1, \cdots, s$, there exist $a_i \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that*

$$\prod_{i=1}^{s} \left(\frac{\mathrm{K}'_{(T)}/\mathrm{K}'}{\mathfrak{P}_i}\right)^{a_i} = 1 \ \in \mathrm{Gal}(\mathrm{K}'_{(T)}/\mathrm{K}'),$$

where $\mathfrak{P}_i|\mathfrak{p}_i$ is any prime in $\mathscr{O}_{\mathrm{K}'}$ above $\mathfrak{p}_i$.

Now choose $\mathfrak{p}$ of K whose Frobenius in $\mathrm{K}'_{(T)}/\mathrm{K}$ has order p and set $S = \{\mathfrak{p}\}$. This implies that for $\mathfrak{P} \subset \mathscr{O}_{\mathrm{K}'}$ with $\mathfrak{P}|\mathfrak{p}$ the Frobenius $x_{\mathfrak{P}} \in \mathrm{Gal}(\mathrm{K}'_{(T)}/\mathrm{K}')$ at $\mathfrak{P}$ is nontrivial. Theorem 5.3 implies that $d_p\mathrm{G}_S^T = d_p\mathrm{G}_\varnothing^T$, hence $\tau_{\mathfrak{p}}$ has depth at least 2 in G_S^T by Lemma 5.2. We want to apply this principle to the number field $\mathrm{K}_2 = (\mathrm{K}_\varnothing^T)^{\Phi_2(\mathrm{G}_\varnothing^T)}$ bearing in mind the Galois action of $\mathrm{G}_\varnothing^T/\Phi_2(\mathrm{G}_\varnothing^T)$.

Let us fix a Galois extension L/K with Galois group H inside $\mathrm{K}_\varnothing^T/\mathrm{K}$. One has the following consequence of Theorem 5.3.

Corollary 5.4. — *Suppose that $\mathrm{V}_\mathrm{L}^T/(\mathrm{L}^\times)^p$ has a non trivial free $\mathbb{F}_p[H]$-submodule. Then there exists a prime $\mathfrak{p} \subset \mathscr{O}_\mathrm{K}$ such that $d_p\mathrm{G}_{\mathrm{L},\varnothing}^T = d_p\mathrm{G}_{\mathrm{L},S}^T$ where $S = \{\mathfrak{p}\}$.*

Proof. — Suppose that $\mathrm{V}_\mathrm{L}^T/(\mathrm{L}^\times)^p$ 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 $\mathrm{V}_\mathrm{L}^T/(\mathrm{L}^\times)^p$. By Kummer duality, one deduces that $\mathrm{Gal}(\mathrm{L}'_{(T)}/\mathrm{L}')$ 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 $\mathfrak{p} \subset \mathscr{O}_\mathrm{K}$ such that its Frobenius in $\mathrm{Gal}(\mathrm{L}'_{(T)}/\mathrm{K})$ is in the conjugacy class of g; the prime $\mathfrak{p}$ splits completely in L'/K. Put $S = \{\mathfrak{p}\}$. Denote by $\mathfrak{Q}_0$ a prime ideal in $\mathscr{O}_{\mathrm{L}'}$ above $\mathfrak{p}$ such that $\left(\frac{\mathrm{L}'_{(T)}/\mathrm{L}'}{\mathfrak{Q}_0}\right) = g$. But $\forall h \in H$ we have $\left(\frac{\mathrm{L}'_{(T)}/\mathrm{L}'}{\mathfrak{Q}_0^h}\right) = g^{h^{-1}}$, and as $\langle g\rangle_H$ is a free $\mathbb{F}_p[H]$-module, there is no nontrivial relation between the $\left(\frac{\mathrm{L}'_{(T)}/\mathrm{L}'}{\mathfrak{Q}_0^h}\right)$'s. By Theorem 5.3, 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 $d_p\mathrm{G}_{\mathrm{L},\varnothing}^T = d_p\mathrm{G}_{\mathrm{L},S}^T$. □

Remark 5.5. — 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 $\mathrm{V}_\mathrm{L}^T/(\mathrm{L}^\times)^p$ has a free-H-part:

- (*i*) for large $|T|$ with size depending on $|H|$ (thanks to a bound given by Ozaki [**31**], see also [**16**]), we are guaranteed that $\mathscr{O}_{\mathrm{L},T}^\times \otimes \mathbb{F}_p$, and then also $\mathrm{V}_\mathrm{L}^T/(\mathrm{L}^\times)^p$ by (4), contains a nontrivial 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 $\mathrm{V}_\mathrm{L}^T/(\mathrm{L}^\times)^p$ contains a nontrivial free $\mathbb{F}_p[H]$-submodule. This is the method we will use.

5.3. A result. — We prove the following

Theorem 5.6. — *Let* K *be a number field. Then given* $k > 0$ *there exists infinitely many primes* $\mathfrak{q}$*, such that for infinitely many primes* $\mathfrak{p}$*, coprime to* $p\mathfrak{q}$*, one has* $\omega(\tau_{\mathfrak{p}}) \geqslant k$ *in* $\mathrm{Gal}(\mathrm{K}^{\{\mathfrak{q}\}}_{\{\mathfrak{p}\}}/\mathrm{K})$.

As we will see the proof of Theorem 5.6 can be reduced to the next Proposition.

Proposition 5.7. — *Let* L/K *be a given finite* p*-extension with Galois group* H*. There exists a positive density set* Θ_1 *of primes* $\mathfrak{q}$ *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* $T = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_t\} \subset \Theta_1$ *of* t *different primes, one has*

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

Proof. — Put $\mathrm{L}' = \mathrm{L}(\mu_p)$, and $\Delta = \mathrm{Gal}(\mathrm{L}'/\mathrm{L})$. Let us start with the following lemma

Lemma 5.8. — *There exists a positive density set* Θ_1 *of primes* $\mathfrak{q}$ *of* K*, all coprime to* p*, such that for all* $t \in \mathbb{Z}_{\geqslant 0}$ *and for all sets* $T = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_t\} \subset \Theta_1$ *of* t *different primes, one has* $\mathbb{F}_p \otimes \mathrm{G}^{ab}_{\mathrm{L}',T} \twoheadrightarrow \bigoplus_{i=1}^{t} \mathbb{F}_p[H][\Delta]$ *as* $\mathrm{Gal}(\mathrm{L}'/\mathrm{K})$*-modules. Moreover the* $\mathfrak{q}_i$*'s split completely in* L/K*.*

Proof. — First, let us choose a set of places Σ of L', $\mathrm{Gal}(\mathrm{L}'/\mathrm{K})$-invariant, such that $G^{\Sigma,ab}_{\mathrm{L}',\varnothing} = \{1\}$. Put $\mathrm{F} = \mathrm{L}'(\sqrt[p]{\mathscr{O}^{\times}_{\mathrm{L}',\Sigma}})$. The extension F/K is Galois and let Θ_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 $\mathrm{K}_v = \mathrm{L}'_v = \mathrm{L}'_v(\sqrt[p]{\mathscr{O}^{\times}_{\mathrm{L}',\Sigma}})$, so $\mathscr{O}^{\times}_{\mathrm{L}',\Sigma} \subset U_v^p$ and $\mu_p \subset \mathrm{K}_v$. Take now $T = \{v_1, \cdots, v_t\}$ a set of t different places of Θ_1 all coprime to p. By class field theory one has:

$$\mathbb{F}_p \otimes \mathrm{G}^{\Sigma,ab}_{\mathrm{L}',T} \simeq \frac{\prod_{w|v\in T} U_w}{\mathscr{O}^{\times}_{\mathrm{L}',\Sigma} \prod_{w|v\in T} U_w^p} \simeq \prod_{w|v\in T} U_w/U_w^p.$$

As all places of T split completely in L'/K, then

$$\prod_{w|v\in T} U_w/U_w^p \simeq \bigoplus_{i=1}^{t} \mathbb{F}_p[H][\Delta].$$

One concludes by noting that $\mathbb{F}_p \otimes \mathrm{G}^{ab}_{\mathrm{L}',T} \twoheadrightarrow \mathbb{F}_p \otimes \mathrm{G}^{\Sigma,ab}_{\mathrm{L}',T} \simeq \bigoplus_{i=1}^{t} \mathbb{F}_p[H][\Delta]$. □

The Kummer radical R_T of the maximal p-elementary extension of L', unramified outside T, is a subgroup of $\mathrm{V}^T_{\mathrm{L}'}/(\mathrm{L}'^{\times})^p$ (remember that T is coprime to p). Hence by Lemma 5.8 we get

$$\bigoplus_{i=1}^{t} \big(\mathbb{F}_p[H][\Delta]\big)^{*} \hookrightarrow R_T \subset \mathrm{V}^T_{\mathrm{L}'}/(\mathrm{L}'^{\times})^p,$$

where $*$ denotes the reflection action following Δ. By taking the Δ-invariant, Proposition 5.7 holds by noting that $\big(\mathrm{V}^T_{\mathrm{L}'}/(\mathrm{L}'^{\times})^p\big)^{\Delta} \simeq (\mathrm{V}^T_{\mathrm{L}}/\mathrm{L}^{\times})^p$. □

Proof. — (of Theorem 5.6). Given $k > 0$, write $n = \lceil \log_2 k \rceil$. Let $\mathrm{L} = (\mathrm{K}_\varnothing)^{\Phi_n(\mathrm{G}_\varnothing)}$ and put $H = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$. By Proposition 5.7, choose a prime $\mathfrak{q}$, coprime to p and that splits completely in L/K, such that $\mathbb{F}_p[H] \hookrightarrow \mathrm{V}_\mathrm{L}^T/(\mathrm{L}^\times)^p$ where $T = \{\mathfrak{q}\}$. So $\mathrm{V}_\mathrm{L}^T/(\mathrm{L}^\times)^p$ contains a free nontrivial $\mathbb{F}_p[H]$-submodule. Then by Corollary 5.4, there exists a prime $\mathfrak{p} \subset \mathscr{O}_\mathrm{K}$ such that $d_p\mathrm{G}_{\mathrm{L},\varnothing}^T = d_p\mathrm{G}_{\mathrm{L},S}^T$ where $S = \{\mathfrak{p}\}$.

But, as $\mathfrak{q}$ splits completely in K, observe now that $(\mathrm{K}_\varnothing)^{\Phi_n(\mathrm{G}_\varnothing)} = (\mathrm{K}_\varnothing^T)^{\Phi_n(\mathrm{G}_\varnothing^T)}$. Then by Lemma 5.2, we get that the depth of $\tau_\mathfrak{p} \in \mathrm{G}_S^T = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$ is at least $2^n \geqslant k$. □

Remark 5.9. — The reader may wonder why one can't, for instance in the totally real example of §3.3.2, simply apply Theorem 5.6 for some $\mathfrak{p}$ whose $\tau_\mathfrak{p}$ will have depth 3 for some $\mathfrak{q}$. The difficulties are that first $\mathrm{G}_{\{\mathfrak{p}\}}^{\{\mathfrak{q}\}}$ may have many more relations imposed by the splitting condition, and second if one removes the splitting condition, the kernel of the map $\mathrm{G}_{\{\mathfrak{p}\}} \twoheadrightarrow \mathrm{G}_{\{\mathfrak{p}\}}^{\{\mathfrak{q}\}}$ might contain elements of depth 2, so the preimage of $\tau_\mathfrak{p}$ may have depth 2.

References

[1] I.V. Andozski, *On some classes of closed pro-p-groups*, Math. USSR **9** (1965), no4, 663-691.

[2] D. Anick and W. Dicks, *A mnemonic for the graded-case Golod-Shafarevich inequality*, arxiv 2015, https://arxiv.org/abs/1508.03231.

[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235-265.

[4] S. Checcoli, *Fields of algebraic numbers with bounded local degrees and their properties*, Trans. Amer. Math. Soc. **365** (2013), no. 4, 2223–2240.

[5] J.D. Dixon, M.P.F. Du Sautoy, A. Mann and D. Segal, *Analytic pro-p-groups*, Cambridge studies in advances mathematics 61, Cambridge University Press, 1999.

[6] M. Ershov, *Golod-Shafarevich groups: a survey*. Internat. J. Algebra Comput. **22** (2012), no. 5, 68 pp.

[7] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, In Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995.

[8] G. Gras, *Les Θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques*, Canadian Journal of Math. **68** (2016), 571-624.

[9] G. Gras, Class Field Theory, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003.

[10] G. Gras and J.-F. Jaulent, *Sur les corps de nombres réguliers*, Mathematische Zeitschrift **202** (1989), 343- 365.

[11] R. Greenberg, *Galois representations with open images*, Annales Math. Québec **40** (2016), issue 1, 83-119.

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

[13] F. Hajir and C. Maire, *Tamely ramified towers and discriminant bounds for number fields*, Compositio Math. **128** (2001), 35-53.

[14] F. Hajir and C. Maire, *Tamely ramified towers and discriminant bounds for number fields II*, Journal of Symbolic Computation **33** (2002), 415-423.

[15] F. Hajir and C. Maire, *Prime decomposition and the Iwasawa mu-invariant*, Math. Proc. of the Cambridge Philosophical Soc. **166** (2019), 599-617.

[16] F. Hajir and C. Maire, *Analytic Lie extensions of number fields with cyclic fixed points and tame ramification*, arxiv 2017, http://front.math.ucdavis.edu/1710.09214.

[17] Y. Ihara, *How many primes decompose completely in an infinite unramified Galois extension of a global field ?*, J. Math. Soc. Japon **35** (1983), no4, 693-709.

[18] A. Jaikin-Zapirain, *Subgroup growth of Golod-Shafarevich groups*, Appendix of *Kazhdan quotients of Golod-Shafarevich groups* by M. Ershov, Proceedings of the London Mathematical Society **102** (4) (2011), 599-636.

[19] J. Labute and H. Kisilevski, *On a sufficient condition for the p-class tower of a CM-field to be infinite*, Théorie des nombres (Quebec, PQ, 1987), 556–560, de Gruyter, Berlin, 1989.

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

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

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

[23] P. Lebacque, *Quelques résultats effectifs concernant les invariants de Tsfasman-Vladut*, Ann. Inst. Fourier **65** (2015), no. 1, 63–99.

[24] A. Lubotzky and A. Mann, *Powerful p-Groups. II. p-Adic Analytic Groups*, J. Algebra **105** (1987), 506-515.

[25] J. Martin, *Building Infinite Ray-Class Towers with Specific Signatures and Small Bounded Root Discriminant*, Cornell Ph.D., 2006.

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

[27] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, Université Paris VII Ph.D., 1988.

[28] A. Movahhedi and T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels*, Séminaire de Théorie des Nombres, Paris 1987–88, 155–200, Progr. Math., 81, Birkhäuser Boston, Boston, MA, 1990.

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

[30] 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.

[31] M. Ozaki, *Construction of maximal unramified p-extensions with prescribed Galois groups*, Inventiones math. **83** (2011), 649-680.

[32] The PARI Group, PARI/GP version `2.9.4`, Univ. Bordeaux, 2018, http://pari.math.u-bordeaux.fr/.

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

[34] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, IHES Publ. Math. **54** (1981), 323-401.

[35] M. Tsfasman and S. Vladut, 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** (2002), no 2, 329-402.

[36] 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.

[37] J.S. Wilson, *Finite presentations of pro-p groups and discrete groups*, Invent. Math. **105** (1991), no. 1, 177–183.

June 1, 2020

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