Canad. J. Math. Vol. **70** (1), 2018 pp. 142–172
http://dx.doi.org/10.4153/CJM-2017-032-9

# On the Invariant Factors of Class Groups in Towers of Number Fields

Farshid Hajir and Christian Maire

*Abstract.* For a finite abelian $p$-group $A$ of rank $d = \dim A/pA$, let $\mathbb{M}_A := \log_p |A|^{1/d}$ be its (logarithmic) mean exponent. We study the behavior of the mean exponent of $p$-class groups in pro-$p$ towers $\mathrm{L}/K$ of number fields. Via a combination of results from analytic and algebraic number theory, we construct infinite tamely ramified pro-$p$ towers in which the mean exponent of $p$-class groups remains bounded. Several explicit examples are given with $p = 2$. Turning to group theory, we introduce an invariant $\underline{\mathbb{M}}(G)$ attached to a finitely generated pro-$p$ group $G$; when $G = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$, where $\mathrm{L}$ is the Hilbert $p$-class field tower of a number field $K$, $\underline{\mathbb{M}}(G)$ measures the asymptotic behavior of the mean exponent of $p$-class groups inside $\mathrm{L}/\mathrm{K}$. We compare and contrast the behavior of this invariant in analytic versus non-analytic groups. We exploit the interplay of group-theoretical and number-theoretical perspectives on this invariant and explore some open questions that arise as a result, which may be of independent interest in group theory.

## 1 Introduction

A few hundred years after its definition, the ideal class group continues to be one of the most mysterious objects in number theory. One early lesson, going back to Gauss, was that it is advantageous to study the $p$-Sylow subgroup of the class group of one prime $p$ at a time. The variation of $p$-class groups in pro-$p$ towers of number fields is perhaps the area that has had the most success, thanks to the pioneering work of Iwasawa. Indeed, his insights uncovered a very rich algebraic structure in the behavior of $p$-class groups in layers of a $\mathbb{Z}_p$-extension. In particular, the growth of the generator rank of these $p$-class groups is governed by the invariants $\mu, \lambda, \nu$, which derive from the structure of the associated Iwasawa module. These ideas have been extended to a much broader context of extensions with more general $p$-adic analytic groups, including non-abelian ones (see, for example, Harris [17], Venjakob [39], Coates–Schneider–Sujatha [3], and Perbet [34]).

In this article, we consider the variation of the invariant factors of $p$-class groups, focusing in particular on a notion we call the *mean exponent* in towers of $p$-extensions of number fields. A recurring theme is comparing and contrasting the tame case versus the analytic case; indeed, the Fontaine–Mazur conjecture [7, Conjecture 5a] has influenced and motivated the questions we explore here.

First, let us define the average or mean exponent. Suppose a non-trivial finite $p$-group $A$ has elementary divisors $p^{a_1}, \dots, p^{a_d}$ listed in decreasing order, in other

Received by the editors January 4, 2016; revised January 25, 2017.
Published electronically November 2, 2017.
AMS subject classification: **11R29**, 11R37.
Keywords: class field tower, ideal class group, pro-p group, p-adic analytic group, Brauer-Siegel Theorem.

words

$$A = \mathbb{Z}/p^{a_1} \times \cdots \times \mathbb{Z}/p^{a_d}, \qquad a_1 \geq a_2 \geq \cdots \geq a_d \geq 1,$$

where $d$ is the $p$-rank of $A$. We then define the *(logarithmic) mean exponent* of $A$ to be

$$\mathbb{M}_A := \frac{a_1 + a_2 + \cdots + a_d}{d} = \log_p |A|^{1/d} = \frac{\log_p |A|}{d},$$

where $\log_p(a) = \log(a)/\log(p)$ is the base-$p$ logarithm. Thus, the mean exponent is a *normalized* measure of the size of the group as compared to its rank. Note that for a non-trivial $p$-group $A$, we always have $1 \leq \mathbb{M}_A \leq \log_p |A|$, the minimum value occurring in the case where $A$ is an elementary abelian $p$-group and the maximum value occurring in the case of cyclic $A$. Note also that $\exp(A) = p^{a_1}$ is the exponent of $A$. The mean exponent of the trivial group is defined to be 0.

For a number field $\mathrm{K}$, we denote by $\mathrm{A}(\mathrm{K})$ its $p$-class group, and we put

$$\mathbb{M}(\mathrm{K}, p) := \mathbb{M}(\mathrm{K}) = \mathbb{M}_{\mathrm{A}(\mathrm{K})}$$

to be the "mean exponent" of the $p$-class group of $K$.

Second, let us introduce towers with restricted ramification. Let $\mathrm{K}$ be a number field, $p$ a rational prime number, and $S$, $T$ a disjoint pair of finite sets of places of $\mathrm{K}$. Inside a fixed algebraic closure of $\mathrm{K}$, consider the compositum $\mathrm{K}_S^T$ of all finite Galois extensions of $\mathrm{K}$ of $p$-power degree unramified outside $S$ and in which all the places of $T$ split completely. We call $\mathrm{K}_S^T$ the maximal unramified-outside-$S$ and $T$-split $p$-extension of $\mathrm{K}$, and put $\mathcal{G}_S^T = \mathcal{G}_S^T(\mathrm{K}, p) = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$ for its Galois group over $\mathrm{K}$. If there are no places dividing $p$ in $S$, which we abbreviate as $(S, p) = 1$ and call the tame case, the structure of the groups $\mathcal{G}_S^T$ is rather mysterious. In particular, it is already difficult to determine in any given case whether $\mathcal{G}_S^T$ is finite or not. On the other hand, if $S$ contains all the primes of $\mathrm{K}$ dividing $p$ (the wild case), then the knowledge of $\mathbb{Z}_p$-extensions of $\mathrm{K}$, which give infinite abelian quotients of $\mathcal{G}_S^{\varnothing}$, goes quite far in revealing the structure of the latter group. By contrast, in the tame case, $\mathcal{G}_S^T$ is *FAb*, meaning its subgroups of finite index have finite abelianization, so, in particular, there are no surjections to $\mathbb{Z}_p$. This is a manifestation of a broader philosophy of Fontaine and Mazur [7] that maintains that "geometric" $p$-adic Galois representations with infinite image are always wildly ramified. The dichotomy of the wild and tame cases is punctuated by the expectation that when $(S, p) = 1$, $\mathcal{G}_S^T$ has no infinite $p$-adic analytic quotients.

To illustrate the key ideas, let us fix $p$, and consider a number field $\mathrm{K}$ with infinite Hilbert $p$-class field, *i.e.,* $\mathcal{G}_{\varnothing}^{\varnothing}(\mathrm{K})$ is infinite. Let us fix an infinite Galois extension $\mathrm{L}/\mathrm{K}$ with $\mathrm{K} \subset \mathrm{L} \subseteq K_{\varnothing}^{\varnothing}$. We are primarily interested in estimating $\exp(\mathrm{A}(\mathrm{K}_n))$, for $(\mathrm{K}_n)$ a nested sequence inside $\mathrm{L}$, but finding this difficult, we also study $(\mathbb{M}(\mathrm{K}_n))$, *i.e.,* the variation of the mean exponent of $p$-class groups in the tower $\mathrm{L}/\mathrm{K}$. In particular, for each natural number $n$, we define

$$\mathbb{M}_n(\mathrm{L}/\mathrm{K}) = \min_{[\mathrm{K}':\mathrm{K}]=p^n} \mathbb{M}(\mathrm{K}'),$$

where the minimum is taken over all extensions $\mathrm{K}'/\mathrm{K}$ of degree $p^n$ with $\mathrm{K}' \subset \mathrm{L}$. We then put

$$\underline{\mathbb{M}}(\mathrm{L}/\mathrm{K}) = \liminf_n \mathbb{M}_n(\mathrm{L}/\mathrm{K}),$$

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

which we call the *asymptotic mean exponent* of the tower. This quantity is well defined, but could *a priori* be $\infty$.

Let us note right away that these asymptotic invariants can be defined purely in a group-theoretical context, as follows. Say $\mathcal{G}$ is an infinite finitely generated *FAb* pro-$p$ group. For each $n$, we put

$$\mathbb{M}_n(\mathcal{G}) = \min_{[\mathcal{G}:\mathcal{U}]=p^n} \mathbb{M}_{\mathcal{U}^{\mathrm{ab}}},$$

where the minimum is taken over the open subgroups of index $p^n$. We then put

$$\underline{\mathbb{M}}(\mathcal{G}) = \liminf_n \mathbb{M}_n(\mathcal{G})$$

for the asymptotic mean exponent of $\mathcal{G}$. It is clear that if $\mathcal{G} = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$, with $\mathrm{L} = \mathrm{K}_{\emptyset}^{\emptyset}$, then $\underline{\mathbb{M}}(\mathcal{G}) = \underline{\mathbb{M}}(\mathrm{L}/\mathrm{K})$. Let us also note that we immediately have the estimate $1 \le \underline{\mathbb{M}}(\mathcal{G})$, but a general upper bound would seem to be elusive.

Some of our results in this paper give bounds for $\underline{\mathbb{M}}(\mathrm{L}/\mathrm{K})$ for certain kinds of tame extensions $\mathrm{L}/\mathrm{K}$. In particular, we draw upon a relationship between the number of primes that split in $\mathrm{L}/\mathrm{K}$ and the asymptotic mean exponent of the tower. Thus, for finitely generated infinite *FAb* $\mathcal{G}$ that are realizable as the Galois group of the Hilbert $p$-class tower of number fields, we can bound $\underline{\mathbb{M}}(\mathcal{G})$ from above. These estimates could be of interest in relation to the following question: is every finitely generated *FAb* pro-$p$ group realizable as $\mathrm{Gal}(\mathrm{K}_{\emptyset}^{\emptyset}/\mathrm{K})$ for some number field K? Note that Ozaki [33] has shown that for any *finite* $p$-group $\mathcal{G}$, there exists a number field $K$ such that $\mathcal{G}$ is isomorphic to $\mathrm{Gal}(\mathrm{K}_{\emptyset}^{\emptyset}/\mathrm{K})$).

The following theorem summarizes some of the key results in this paper.

***Theorem 1.1*** (i) *Suppose* $S$ *is a finite set of primes of a number field* K *with* $(S, p) = 1$ *such that* $\mathcal{G} = \mathrm{Gal}(\mathrm{K}_S^{\emptyset}/\mathrm{K})$ *is infinite. Then there exists a constant* $C > 0$ *such that for all open subgroups* $\mathcal{U} \subset \mathcal{G}$, $\mathbb{M}_{\mathcal{U}^{\mathrm{ab}}} \le C[\mathcal{G}:\mathcal{U}]$.

(ii) *With* $K, S, \mathcal{G}$ *as above, suppose* $\mathcal{G}$ *is mild (for example this is the case if* $K, S$ *satisfy the condition of Labute* [21, Theorem 1.6], *and see also Schmidt* [36]*). Then for all* $\varepsilon > 0$*, there exist a constant* $C' > 0$ *and a nested sequence of open subgroups* $\mathcal{U}_i$ *forming an open neighborhood of* $\mathcal{G}$ *such that* $\mathbb{M}_{\mathcal{U}_i^{\mathrm{ab}}} \le C'[\mathcal{G}:\mathcal{U}_i]/(\log[\mathcal{G}:\mathcal{U}_i])^{2-\varepsilon}$.

(iii) *There exist infinitely many pairwise disjoint number fields* K *with infinite* $p$*-class field tower* $\mathrm{K}_{\emptyset}^{\emptyset}/\mathrm{K}$ *but finite asymptotic mean exponent,* i.e., $\underline{\mathbb{M}}(\mathrm{Gal}(\mathrm{K}_{\emptyset}^{\emptyset}/\mathrm{K})) \ne \infty$.

The first two parts of the theorem come relatively easily from standard techniques; they are proved in Proposition 6.7 and Theorem 6.15, respectively. To illustrate the third part, which is proved in § 3.1, consider the following concrete arithmetic example. Namely, fix $p = 2$ and let K be the following compositum of quadratic fields:

$$\mathrm{K} = \mathbb{Q}\big(\sqrt{13035663390876017892 0}, \sqrt{-80285321329764931}\big).$$

Let $\mathrm{L} = \mathrm{K}_{\emptyset}^{\emptyset}$. Then $\mathrm{L}/\mathrm{K}$ is infinite and $\underline{\mathbb{M}}(\mathrm{L}/\mathrm{K}) \le 8.858$. The details of the construction are given in Section 4, but here, let us explain what this example means concretely. Namely, the assertion is that there exists a tower $\mathrm{K} = \mathrm{K}_1 \subset \mathrm{K}_2 \subset \cdots$ inside L such that for all $n$, the 2-class group of $\mathrm{K}_n$ has mean exponent at most 8.858, so, in particular, there is always at least one elementary divisor of size at most $2^8$ all the way up the tower. We should note that the construction of the tower guarantees that the rank of

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

the 2-class groups tends to infinity, so the fact that the mean exponent remains below 9 entails that the number of elementary divisors of size at most $2^8$ becomes arbitrarily large as we climb the tower.

We would like to contrast the third part of the theorem with the generic behavior of the mean exponent of open neighborhoods in analytic pro-$p$ groups. Namely, if $G$ is a uniform pro-$p$ group of dimension $d$ and $\mathcal{U}$ runs over the $p$-central series of $G$, we have $\mathbb{M}_{\mathcal{U}^{\mathrm{ab}}} \geq \frac{1}{d}\log[G:\mathcal{U}]$, hence it tends to infinity; see Corollary 6.5.

The principle behind the above example and others we construct is as follows. We use genus theory to create towers in which the $p$-rank grows linearly with the degree; this is achieved by first having a tower in which many primes split and then composing that tower with a degree $p$ Galois extension the same primes ramify. The linear growth of the rank of the $p$-class group when combined with upper bounds on the class number coming from the generalized Brauer–Siegel theorem of Tsfasman and Vladut gives us the desired upper bound on $\underline{\mathbb{M}}$.

In the more classical case of Iwasawa theory, *i.e.,* in wild towers, there is an algebraic theory of the invariants $\mu, \lambda, \nu$ associated with the Iwasawa module, and having linear growth in the rank is tantamount to having $\mu > 0$. It is curious that in that context also, the phenomenon of linear rank growth appears to be related to having a large set of primes splitting in the tower (see Iwasawa [19]). In a forthcoming work, we will study this relationship further.

The paper is organized as follows. In Section 2, we recall some background, including the work of Tsfasman and Vladut extending the Brauer–Siegel Theorem and some basic results from genus theory. In Section 3, we begin by giving a sketch of our main construction for unramified towers, then enlarge the scope of our study by introducing class groups that classify extensions with prescribed splitting and (tame) ramification. In Section 4, we work out a number of examples in detail, demonstrating how the exact asymptotic formula of Tsfasman and Vladut can be exploited to improve the bounds on the mean exponent. In Section 5, we reflect on the relationship between linear growth for $p$-ranks of class groups and the existence of many primes in the tower that split (almost) completely, together with the implication of these considerations for bounding the asymptotic mean exponent in infinite tame extensions. In Section 6, we turn from number theory to considerations of the asymptotic mean exponent for pro-$p$ groups in general. Finally, in Section 7, we consider a number of questions for further study in group theory, as well as in number theory, that are raised by the considerations of this paper.

## Some Notation and Basic Notions

We fix a prime number $p$. Let $\mathrm{K}$ be a number field of degree $[\mathrm{K}:\mathbb{Q}]$. Assume the following notations:

- $(r_1, r_2)$ is the signature of K, where $r_1$ is the number of real embeddings of K and where $r_2$ is the number of pairs of conjugate complex embeddings; thus, $[\mathrm{K}:\mathbb{Q}] = r_1 + 2r_2$.
- $\mathrm{disc}(\mathrm{K})$ is the discriminant of K (see [23, chapter III], [31, Chapter I]).
- $\mathrm{Rd}_{\mathrm{K}} := |\mathrm{disc}(\mathrm{K})|^{1/[\mathrm{K}:\mathbb{Q}]}$ is the root discriminant of K.

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

- $g = g_{\mathrm{K}} = \log\sqrt{|\operatorname{disc}(\mathrm{K})|}$ is the genus of K.
- $\mathrm{Reg}_{\mathrm{K}}$ is the regulator of K (see [23, Chapter V], [31, Chapter I]).
- $\mathrm{Cl}(\mathrm{K})$ is the Class group of K.
- $h_{\mathrm{K}} = |\mathrm{Cl}(\mathrm{K})|$ is the Class number of K.
- $\mathrm{A}(\mathrm{K})$ is the $p$-Class group of K; it is the $p$-Sylow of $\mathrm{Cl}(\mathrm{K})$.
- $\delta_{\mathrm{K}} = 1$ if K contains the $p$-roots of unity, 0 otherwise.

Let us now fix $S$ and $T$, two disjoint finite sets of places of K.

- Let $\mathrm{K}_S^T$ be the maximal unramified outside $S$ and $T$-split $p$-extension of K, with the convention that for $p = 2$ all real places stay real (see, for example, [12, Appendix] or [25]). Put $\mathcal{G}_S^T = \mathrm{Gal}(\mathrm{K}_S^T/\mathrm{K})$.
- It is well known that the pro-$p$-group $\mathcal{G}_S^T$ is finitely presented (see, for example, [20] or [12, Appendix]): the quantities
$$d(\mathcal{G}_S^T) = \dim_{\mathbb{F}_p} H^1(\mathcal{G}_S^T, \mathbb{F}_p) = d_p H^1(\mathcal{G}_S^T, \mathbb{F}_p),$$
$$r(\mathcal{G}_S^T) = \dim_{\mathbb{F}_p} H^2(\mathcal{G}_S^T, \mathbb{F}_p) = d_p H^2(\mathcal{G}_S^T, \mathbb{F}_p)$$
are finite.
- Let $\mathrm{A}_S^T := \mathcal{G}_S^{T^{ab}}$, the maximal abelian quotient of $\mathcal{G}_S^T$, which corresponds by Class Field Theory to the maximal abelian $S$-ramified (*i.e.*, unramified outside $S$) and $T$-split extension of K.
- For $S = T = \varnothing$, $\mathcal{G}_S^T$ corresponds to the Galois group of the Hilbert $p$-Class Field Tower of K and $\mathrm{A} = \mathrm{A}(\mathrm{K})$ corresponds to its $p$-Class group.
- If $S$ is prime to $p$, the pro-$p$-group $\mathcal{G}_S^T$ is *FAb*; i.e., every open subgroup of $\mathcal{G}_S^T$ has finite abelianization (see, for example, [12, Chapter III]).

We next introduce some basic notation concerning towers of number fields (see [38]).

- A sequence $(\mathrm{K}_n)$, $n \in \mathbb{N} \cup \{0\}$, of number fields, where $\mathrm{K}_0 = \mathrm{K}$, is called a tower if for all $n$, $\mathrm{K}_n \subsetneq \mathrm{K}_{n+1}$, so, in particular, $[\mathrm{K}_n : \mathrm{K}] \to \infty$ with $n$.
- Let L/K be an infinite extension of a number field K and let $(\mathrm{K}_n)$ be a tower in L/K with limit L, *i.e.*, each $\mathrm{K}_n$ is a finite extension of K contained in L and $\bigcup_n \mathrm{K}_n = \mathrm{L}$.
- "Assuming *GRH* in L/K" means that the *Generalized Riemann Hypothesis* holds along the tower (see [2]).

Then put:

- $g_n = g_{\mathrm{K}_n} = \log(\sqrt{|\operatorname{disc}(\mathrm{K}_n)|})$;
- $h_n = |\mathrm{Cl}(\mathrm{K}_n)|$ the class number of $\mathrm{K}_n$;
- $\mathrm{Reg}_n$ = the regulator of $\mathrm{K}_n$;
- $B(\mathrm{L}/\mathrm{K}) = \lim_n \frac{\log(\mathrm{Reg}_n h_n)}{g_n}$.

- We let $\gamma = 0.5772\cdots$ be the Euler constant and put $e = \exp(1) = 2.7182\cdots$.
- For material on Iwasawa Theory, see [41]; for mild pro-$p$-groups see [8, 21]; for analytic pro-$p$-groups, see [4].

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

## 2 Background

### 2.1 The Brauer–Siegel and Tsfasman–Vladut Theorems

We first recall some results due to Tsfasman and Vladut [38] generalizing the Brauer–Siegel theorem. Throughout this work, we will use the Tsfasman–Valdut context of asymptotically exact extensions.

Let $\mathrm{L}/\mathrm{K}$ be an infinite extension of a number field $\mathrm{K}$ and let $(\mathrm{K}_n)$ be a tower in $\mathrm{L}/\mathrm{K}$ with limit $\mathrm{L}$: $\bigcup_n \mathrm{K}_n = \mathrm{L}$.

For every prime number $\ell$ and power $q := \ell^m$ of $\ell$, let us consider the quantity

$$\phi_q = \lim_n \frac{N_n(q)}{g_n},$$

where $N_n(q) = \#\{\text{prime ideal } \mathfrak{q} \subset \mathcal{O}_{\mathrm{K}_n},\ \#\mathcal{O}_{\mathrm{K}_n}/\mathfrak{q} = q\}$. We also put

$$\phi_{\mathbb{R}} = \lim_n \frac{r_1(\mathrm{K}_n)}{g_n} \quad \text{and} \quad \phi_{\mathbb{C}} = \lim_n \frac{r_2(\mathrm{K}_n)}{g_n}.$$

As the sequence $(\mathrm{K}_n)$ is a tower, all the limits exist and depend only on $\mathrm{L}/\mathrm{K}$. In the terminology of [38], the sequence $(\mathrm{K}_n)$ is said to be *asymptotically exact*. It is called *asymptotically good* if $\phi_q > 0$ for some $q$, where $q$ is either a prime power or belongs to $\{\mathbb{R}, \mathbb{C}\}$. In this paper, we will mostly be interested in examples where $\phi_{\mathbb{C}} > 0$. Deeply ramified wild extensions (such as $\mathbb{Z}_p$-extensions) are asymptotically bad. By contrast, assuming $\mathcal{G}_S^{\varnothing}(\mathrm{K}, p)$ is infinite for some finite $S$ with $(S, p) = 1$, any tower inside $\mathrm{K}_S^{\varnothing}/\mathrm{K}$ is asymptotically good. More generally, even if $(S, p) \neq 1$ but $(\mathrm{K}_n)$ is a tower in which the $N$-th higher ramification groups all vanish for some fixed $N$, then the tower is asymptotically good (see [16]).

In [38], Tsfasman and Vladut studied the behavior of the quantity $\log(\mathrm{Reg}_n \cdot h_n)/g_n$ along a tower $(K_n)$ with limit $\mathrm{L}/\mathrm{K}$. They conjectured that the quantity

$$B(\mathrm{L}/\mathrm{K}) = \lim_n \frac{\log(\mathrm{Reg}_n h_n)}{g_n}$$

is well defined, and they proved the following theorem.

***Theorem 2.1*** (Tsfasman–Vladut [38]) (i) *Assuming GRH, the limit $B(\mathrm{L}/\mathrm{K})$ exists and depends only* $\mathrm{L}/\mathrm{K}$, *not on the choice of tower* $(\mathrm{K}_n)$ *with limit L. Moreover, one has the equality:*

$$B(\mathrm{L}/\mathrm{K}) = 1 + \sum_q \phi_q \log \frac{q}{q-1} - \phi_{\mathbb{R}} \log 2 - \phi_{\mathbb{C}} \log 2\pi.$$

*Without assuming GRH, one has the same conclusion if the tower of number fields* $(\mathrm{K}_n)$ *is Galois relative to* K.

(ii) *Assuming GRH,* $B(\mathrm{L}/\mathrm{K}) \le 1.0939$ *for all* $\mathrm{L}/\mathrm{K}$. *If* K *is totally imaginary, then* $B(\mathrm{L}/\mathrm{K}) \le 1.0765$. *Without assuming GRH, one has* $B(\mathrm{L}/\mathrm{K}) \le 1.1589$.

### 2.2 On the $p$-$S$-$T$ Towers

Comprehensive references for the study of extensions with restricted ramification include Koch [20], Gras [12], and Neukirch–Schmidt–Wingberg [32]. We give only a quick sketch of some well-known facts, and refer the reader to those books, which contain much more background and detail.

Let $\mathrm{K}$ be a number field and let $S$ and $T$ be two finite sets of places of $\mathrm{K}$ with $S \cap T = \varnothing$. We assume that $(S,p) = 1$. We recall that the pro-$p$-group $\mathcal{G}_S^T$ is *FAb* and that the $p$-rank $d_p \mathcal{G}_S^T$ of $\mathcal{G}_S^T$ can be computed thanks to Class Field Theory. In particular, one has the following propoition (see *e.g.,* [12, Chapter I §4, Theorem 4.6]).

***Proposition 2.2*** *With notation as above, we have*

$$d_p \mathcal{G}_S^T = d_p \mathrm{A}_S^T \geq |S| - \big( r_1(\mathrm{K}) + r_2(\mathrm{K}) + |T| - \delta_{\mathrm{K}} \big).$$

*A priori*, the pro-$p$-group $\mathcal{G}_S^T$ may be finite or not. A criterion for its infinitude can be obtained as a consequence of Golod–Shafarevich's theorem; the following is their result, in the improved version due to Gaschütz and Vinberg (see Roquette [35]).

***Theorem 2.3*** (Golod–Shafarevich) *If a non-trivial pro-$p$-group $\mathcal{G}$ is finite, then its generator and relation ranks satisfy the following inequality: $r(\mathcal{G}) > d(\mathcal{G})^2/4$.*

The following classical theorem of Shafarevich on the Euler characteristic of $\mathcal{G}_S^T$ is of fundamental importance in this theory (see, for example, [12]):

***Proposition 2.4*** *Assuming as above that $(S,p) = 1$, we have*

$$0 \leq r(\mathcal{G}_S^T) - d(\mathcal{G}_S^T) \leq r_1 + r_2 - 1 + \delta_S + |T|,$$

*where $\delta_S = 1$ if $\mathrm{K}$ contains the $p$-roots of unity and $S$ is empty, and $0$ otherwise.*

The last two propositions together imply that if $S$ is large in comparison to the size of $T$, then $\mathcal{G}_S^T$ is infinite, giving rise to the so-called Golod–Shafarevich criterion. This criterion can be made effective by using genus theory (*cf.* [25] or [12, Chapter IV]) to construct number fields with class group of large $p$-rank. The following is a standard result from genus theory (*cf.* [12, Chapter IV, Example after Corollary 4.5.1]).

***Theorem 2.5*** *Let $\mathrm{K}/\mathrm{k}$ be a cyclic extension of degree $p$. Then*

$$d_p \mathrm{A}(\mathrm{K}) \geq \rho - 1 - \big( r_1(\mathrm{k}) + r_2(\mathrm{k}) - 1 + \delta_k \big),$$

*where $\delta_{\mathrm{k}} = 1$ if $\mathrm{k}$ contains the $p$-roots of unity, and $0$ otherwise, and where $\rho$ is the number of ramified places of $\mathrm{k}$ in $\mathrm{K}/\mathrm{k}$ (eventually archimedean places).*

It is possible to obtain a $T$-split version of Genus Theory and then one can show the following theorem [26].

***Theorem 2.6*** *Let $\mathrm{K}/\mathrm{k}$ be a cyclic extension of degree $p$. Assume that*

$$\rho + i_T \geq 3 + r_1(\mathrm{k}) + r_2(\mathrm{k}) + |T(\mathrm{k})| - 1 + \delta_{\mathrm{k}} + 2\sqrt{r_1(\mathrm{K}) + r_2(\mathrm{K}) + |T(\mathrm{K})| + \delta_{\mathrm{K}}},$$

*where $\rho$ is the number of places ramified in $\mathrm{K}/\mathrm{k}$ (eventually the archimedean places) and where $i_T$ is the number of places of $T$ inert in $\mathrm{K}/\mathrm{k}$. Then $\mathcal{G}^T := \mathcal{G}_\varnothing^T$ is infinite.*

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

***Corollary 2.7*** *Let* $\mathrm{K}/\mathbb{Q}$ *be a real quadratic field and let* $T$ *be a finite set of odd primes of* $\mathbb{Q}$*. Put* $T_{\mathrm{dec}} = \{\ell \in T,\ \ell \text{ splits in } \mathrm{K}/\mathbb{Q}\}$*. If*

$$\rho \geq 4 + |T_{\mathrm{dec}}| + 2\sqrt{3 + |T|},$$

*where* $\rho$ *is the number of primes not in* $T$ *that are ramified in* $\mathrm{K}/\mathbb{Q}$*, then the group* $\mathcal{G}^T$ *is infinite.*

**Proof** We simply remark that a prime of $T$ that is not split in $\mathrm{K}/\mathbb{Q}$ is inert or ramified and then apply Theorem 2.6. ■

# 3 Towers with Bounded Mean Exponent

## 3.1 The Principal Construction

In this subsection, we sketch the key idea for the construction of towers with $p$-class groups of bounded mean exponent in the simpler case of unramified extensions, and in particular, we prove Theorem 1.1(iii). In later subsections, we will explore the mean exponent for more general notions of class groups.

We will need the following lemma.

***Lemma 3.1*** *There is an absolute constant* $C_0 > 0$ *such that for all number fields* $\mathrm{K}$*,* $\log(h_{\mathrm{K}}) \leq C_0 \log|\operatorname{disc}(\mathrm{K})|$.

**Proof** By Brauer's Lemma [23, Lemma 2, Chapter 16], there is an absolute positive constant $C$ such that for all number fields K, $\log(h_{\mathrm{K}} \operatorname{Reg}_{\mathrm{K}}) \leq C \log|\operatorname{disc}(\mathrm{K})|$. We can essentially suppress the contribution of the regulator thanks to Friedman's result [9] that for all number fields K we have $\operatorname{Reg}_{\mathrm{K}} > 0.1$. Thus, by replacing $C$ with a larger constant $C_0$, we have $\log(h_{\mathrm{K}}) \leq C_0 \log|\operatorname{disc}(\mathrm{K})|$. ■

***Proposition 3.2*** *Suppose* $\mathrm{k}$ *is a number field and* $T$ *is a finite set of primes such that* $\mathrm{k}_{\varnothing}^{T}/\mathrm{k}$ *is infinite. Suppose* $t_0 := |T| - (r_1(\mathrm{k}) + r_2(\mathrm{k}) + 1) > 0$*, and that* $\mathrm{k}$ *admits a cyclic degree* $p$ *extension* $K$ *in which all the primes in* $T$ *ramify. Then the Hilbert* $p$*-class field tower of* $\mathrm{K}$ *is infinite with bounded asymptotic mean exponent*

$$\underline{\mathbb{M}}\big(\operatorname{Gal}(\mathrm{K}_{\varnothing}^{\varnothing}/\mathrm{K})\big) < \frac{C_0}{t_0} \log_p |\operatorname{disc}(K)|,$$

*where* $C_0$ *is the constant appearing in Lemma 3.1.*

**Proof** Consider a tower $(\mathrm{k}_n)$ inside $\mathrm{k}_{\varnothing}^{T}/\mathrm{k}$ and let $\mathrm{K}_n = \mathrm{K}\mathrm{k}_n$. To simplify the notation, let $d_n = d(A(\mathrm{K}_n))$ be the $p$-rank of the class group of $\mathrm{K}_n$. By Theorem 2.5 applied to $\mathrm{K}_n/\mathrm{k}_n$, we have

$$d_n \geq |T|[\mathrm{k}_n : \mathrm{k}] - \big(r_1(\mathrm{k}_n) + r_2(\mathrm{k}_n) + 1\big) \geq t_0[\mathrm{K}_n : \mathrm{K}]. \tag{3.1}$$

By the definition of the mean exponent $\mathbb{M}(\mathrm{K}_n)$, we have

$$d_n \mathbb{M}(\mathrm{K}_n) = \log_p |A(\mathrm{K}_n)| \leq \log_p h_n,$$

where $h_n$ is the class number of $K_n$. Now, if we apply Lemma 3.1, we have

$$d_n \mathbb{M}(\mathrm{K}_n) \le \log_p h_n \le C_0 \log_p |\mathrm{disc}(\mathrm{K}_n)|. \tag{3.2}$$

But since $\mathrm{K}_n/\mathrm{K}$ is unramified, $\log_p |\mathrm{disc}(\mathrm{K}_n)| = [\mathrm{K}_n : \mathrm{K}] \log_p |\mathrm{disc}(K)|$. Putting the inequalities (3.1) and (3.2) together, we conclude that

$$t_0 [\mathrm{K}_n : \mathrm{K}] \mathbb{M}(\mathrm{K}_n) \le C_0 [\mathrm{K}_n : \mathrm{K}] \log_p |\mathrm{disc}(\mathrm{K})|,$$

hence $\mathbb{M}(\mathrm{K}_n)$ is bounded from above by $C_0 \log_p |\mathrm{disc}(\mathrm{K})|/t_0$. We conclude that

$$\underline{\mathbb{M}}(\mathrm{K}_\varnothing^\varnothing/\mathrm{K}) \le \frac{C_0}{t_0} \log_p |\mathrm{disc}(\mathrm{K})|. \qquad \blacksquare$$

**Proof of Theorem 1.1(iii)** Suppose $\{\ell_1, \ell_2, \dots, \ell_r\}$ is a large set of primes congruent to 1 mod $p$. Let k be a cyclic degree $p$ extension of $\mathbb{Q}$ in which $\ell_1, \dots, \ell_r$ ramify. Consider primes $q_1 < q_2$ that split completely in $\mathrm{k}(\zeta_p)/\mathbb{Q}$ if $p$ is odd and in $\mathrm{k}(\zeta_4)/\mathbb{Q}$ if $p = 2$. Let k′ be a cyclic degree $p$ extension of $\mathbb{Q}$ in which $q_1$ and $q_2$ ramify. Let $T$ be the union of the primes of k lying over $q_1$ and those lying over $q_2$. As specified in Theorem 2.6, if $r$ is sufficiently large, $\mathrm{k}_\varnothing^T/\mathrm{k}$ is infinite. Now we let $\mathrm{K} = \mathrm{kk}'$. This puts us in the situation of Proposition 3.2, which gives the desired outcome. $\blacksquare$

## 3.2 On the Mean Exponent for $T$-class Groups mod $S$

In this section, we will expand our notion of class group in two directions: we will look at ($p$-parts of) ray class groups of tame conductor (*i.e.,* a conductor that is a finite product of distinct prime ideals co-prime to $p$), and with the underlying ring being the $T$-integers.

***Definition 3.3*** Let $T$ and $S$ be two disjoint finite sets of places of K such that $(S, p) = 1$. The mean $\mathbb{M}_S^T(\mathrm{K})$ of the invariant factors of the abelian group $\mathrm{A}_S^T := \mathcal{G}_S^{T\,ab}$ is defined by

$$\mathbb{M}_S^T(\mathrm{K}) := \mathbb{M}_{\mathrm{A}_S^T} = \frac{a_1 + \cdots + a_d}{d} = \log_p |\mathrm{A}_S^T|^{1/d},$$

where $d = d_p \mathcal{G}_S^T = d_p \mathrm{A}_S^T$ and $\mathrm{A}_S^T \simeq \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_d}\mathbb{Z}$ with: $1 \le a_1 \le \cdots \le a_d$. Note that $\mathbb{M}_S^T(\mathrm{K}) = 0$ if $|\mathrm{A}_S^T| = 1$.

***Remark 3.4*** Note that $\mathbb{M}_S^T$ is well defined because, thanks to the choice of $S$ being away from $p$, the group $\mathcal{G}_S^{T\,ab}$ is finite. Clearly, when $\mathrm{A}_S^T$ is not trivial, we have $\mathbb{M}_S^T(\mathrm{K}) \ge 1$.

***Example 3.5*** (Iwasawa Theory context) (For material for Iwasawa theory, see, for example, [41].) Let $\mathcal{L} = \mathrm{L}/\mathrm{K}$ be a $\mathbb{Z}_p$-extension. Let $\mathrm{K}_n$ be the unique subfield of $\mathcal{L}$ of degree $p^n$ over K. Denote by $\mathrm{X}_S^T$ the projective limit of the $p$-group $\mathrm{A}_S^T(\mathrm{K}_n)$ along $\mathcal{L}$. Then $\mathrm{X}_S^T$ is a $\mathbb{Z}_p[[T]]$-module of finite rank and there exist invariants $\mu, \lambda \ge 0$ such that for $n \gg 0$,

$$\log_p |\mathrm{A}_S^T(\mathrm{K}_n)| = \mu p^n + \lambda n + \nu,$$

with $\nu \in \mathbb{Z}$. Moreover,

$$d_p \mathrm{A}_S^T(\mathrm{K}_n) = s p^n + \lambda + c,$$

where $c \geq 0$ and where $s$ is the $\mathbb{F}_p[[T]]$-rank of the module $\mathbb{F}_p \otimes \mathrm{X}_S^T$.

***Proposition 3.6*** *Along a $\mathbb{Z}_p$-extension $\mathcal{L}$, one has*

$$\mathbb{M}_S^T(\mathrm{K}_n) \sim_{n\to\infty} \begin{cases} \delta \log_p[\mathrm{K}_n:\mathrm{K}] & \text{if } \mu = 0 \text{ and } \lambda \neq 0, \\ \mu/s & \text{if } \mu \neq 0, \\ \nu/c & \text{if } \mu = \lambda = 0, \end{cases}$$

*where $\delta = \lambda/(\lambda + c)$ satisfies $0 < \delta \leq 1$.*

**Proof** The proof is a consequence of the structure theorem of Iwasawa Theory and the fact that $\mu = 0$ if and only if $s = 0$. ■

***Remark 3.7*** Note when $\mu = 0$ and $\lambda \neq 0$, $\mathbb{M}_S^T(\mathrm{K}_n)$ is unbounded. This will be in contrast to the examples of Section 4.

From now on, we want to study the quantity $\mathbb{M}(\mathcal{L})$ in some tower $\mathcal{L}$ when the ramification is tame. First, we have some definitions.

***Definition 3.8*** Let $\mathcal{L} := \mathrm{L}/\mathrm{K}$ be an (infinite) extension and let $T$ and $S$ be two disjoint finite sets of places of K with $(S, p) = 1$. Put

$$\overline{\mathbb{M}}(\mathcal{L}, S, T) := \limsup_n \mathbb{M}_{S,n}^T \quad \text{and} \quad \underline{\mathbb{M}}(\mathcal{L}, S, T) := \liminf_n \mathbb{M}_{S,n}^T,$$

where

$$\mathbb{M}_{S,n}^T = \min_{\mathrm{K}_n} \mathbb{M}_S^T(\mathrm{K}_n),$$

the minimum being taken over all subfields $\mathrm{K}_n$ in $\mathcal{L}$ of degree $p^n$ over K. When $S = T = \varnothing$, we have $\underline{\mathbb{M}}(\mathcal{L}, \varnothing, \varnothing) = \underline{\mathbb{M}}(\mathcal{L})$, where $\underline{\mathbb{M}}(\mathcal{L})$ was defined in the introduction. We also write $\overline{\mathbb{M}}(\mathcal{L}) := \overline{\mathbb{M}}(\mathcal{L}, \varnothing, \varnothing)$.

***Remark 3.9*** We have $\limsup_n \min a_1(\mathrm{K}_n) \leq \overline{\mathbb{M}}(\mathcal{L})$ and $\liminf_n \min a_1(\mathrm{K}_n) \leq \underline{\mathbb{M}}(\mathcal{L})$.

***Definition 3.10*** A tower $(\mathrm{K}_n)$ is said to be exhaustive in $\mathcal{L}$ if:

(i) $\bigcup \mathrm{K}_n = \mathcal{L}$,

(ii) for all $n$, $[\mathrm{K}_{n+1}:\mathrm{K}_n] = p$.

***Proposition 3.11*** *For a subtower $(\mathrm{K}_n)$ of $\mathcal{L}$, $\underline{\mathbb{M}}(\mathcal{L}, S, T) \leq \liminf_n \mathbb{M}_S^T(\mathrm{K}_n)$. If, moreover, the subtower $(\mathrm{K}_n)$ is exhaustive in $\mathcal{L}$, then $\overline{\mathbb{M}}(\mathcal{L}, S, T) \leq \limsup_n \mathbb{M}_S^T(\mathrm{K}_n)$.*

**Proof** The proof follows easily from the definitions. ■

### 3.3 Bounds for Mean Exponents in Tamely Ramified Towers

***Definition 3.12*** For a finite set $S$ of prime ideals of K satisfying $(S, p) = 1$, we put

$$\mathrm{disc}(\mathrm{K}, S) := |\,\mathrm{disc}(\mathrm{K})| \prod_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p}).$$

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

A local computation shows the following proposition.

***Proposition 3.13*** *If $S$ is a finite set of prime ideals of $\mathrm{K}$ satisfying $(S,p)=1$, the root discriminant remains bounded inside $\mathrm{K}_S^{\varnothing}/\mathrm{K}$; in other words, $\mathrm{K}_S^{\varnothing}/\mathrm{K}$ is asymptotically good. Indeed, for a tower $(\mathrm{K}_n)$ in $\mathrm{K}_S^{\varnothing}/\mathrm{K}$, we have*

$$\log|\operatorname{disc}(\mathrm{K}_n)| \leq [\mathrm{K}_n:\mathrm{K}]\log\operatorname{disc}(\mathrm{K},S).$$

**Proof** See, for example, [15, Lemma 5]. ■

***Definition 3.14*** For a prime $\mathfrak{p}$ of $\mathrm{K}$ not dividing $p$, let $a(\mathfrak{p}) := v_p(\mathrm{N}(\mathfrak{p})-1)$ be the $p$-valuation of $\mathrm{N}(\mathfrak{p})-1$, where $\mathrm{N}(\mathfrak{p})$ is the absolute norm of $\mathfrak{p}$.

***Lemma 3.15*** *Let $\mathrm{L}/\mathrm{K}$ be a finite Galois $p$-extension and let $S$ be a finite set of places of $\mathrm{K}$ prime to $p$.*

(i) *If $p>2$, then*

$$|\mathrm{A}_S^T(\mathrm{L})| \leq |\mathrm{A}(\mathrm{L})|\Big(\prod_{\mathfrak{p}\in S} p^{a(\mathfrak{p})}\Big)^{[\mathrm{L}:\mathrm{K}]}.$$

(ii) *For $p=2$, one has*

$$|\mathrm{A}_S^T(\mathrm{L})| \leq |\mathrm{A}(\mathrm{L})|\Big(\prod_{\mathfrak{p}\in S} p^{a^*(\mathfrak{p})}\Big)^{[\mathrm{L}:\mathrm{K}]},$$

*where $a^*(\mathfrak{p}) = a(\mathfrak{p})$ if $\mathrm{N}(\mathfrak{p}) \equiv 1 \bmod 4$ (i.e., if $a(\mathfrak{p})>1$); otherwise, $N(\mathfrak{p}) = 1+2n$, where $n$ is odd and then $a^*(\mathfrak{p}) = v_2(1+n)+1$.*

**Proof** One has to give an upper bound of the tame part of the inertia group of a place $\mathfrak{P}|\mathfrak{p}$ in an abelian extension of $\mathrm{L}$. We recall that this inertia group is a quotient of the multiplicative group of the finite field $\mathbb{F}_{\mathfrak{P}}$ of order $N(\mathfrak{P})$. By multiplicativity, one can assume that $\mathrm{L}/\mathrm{K}$ is a cyclic degree $p$-extension. When $\mathbb{F}_{\mathfrak{P}} = \mathbb{F}_{\mathfrak{p}}$, that means that $\mathfrak{p}$ is split or is ramified in $\mathrm{L}/\mathrm{K}$, then $\prod_{\mathfrak{P}|\mathfrak{p}} p^{a(\mathfrak{P})}$ divides $p^{pa(\mathfrak{p})}$ (with equality if $\mathfrak{p}$ splits). Otherwise, $[\mathbb{F}_{\mathfrak{P}}:\mathbb{F}_{\mathfrak{p}}] = p$, and then one note that if $p$ is odd (or when $p=2$ and $N(\mathfrak{p})\equiv 1 \bmod 4$), then $a(\mathfrak{P}) = a(\mathfrak{p})+1$. Indeed, if $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_q$, then $\mathbb{F}_{\mathfrak{P}} = \mathbb{F}_{q^p}$. Let us write $q = 1+p^k n$, with $(n,p)=1$. Then $\mathbb{F}_{q^p}^{\times}$ is cyclic of order

$$\begin{aligned} q^p-1 &= (q-1)(q^{p-1}+\cdots+q+1)\\ &= p^{k+1}n\big(1+np^{k-1}+\cdots+n(p-1)p^{k-1}+p^kA\big)\\ &= p^{k+1}n\Big(1+\frac{1}{2}n(p-1)p^k+p^kA\Big), \end{aligned}$$

where $A\in\mathbb{Z}$, and then $v_p(q^p-1) = p^{k+1}$ for $p$ odd (and for $p=2$ if $k>1$).

When $p=2$ with $N(\mathfrak{p}) = 1+2n$, $n$ odd, one has $a(\mathfrak{P}) = v_2(1+n)+1$. We leave the remaining details to the reader. ■

***Definition 3.16*** For $p>2$, put $a(S) = \sum_{\mathfrak{p}\in S} a(\mathfrak{p})$. For $p=2$, put $a(S) = \sum_{\mathfrak{p}\in S} a^*(\mathfrak{p})$.

***Remark 3.17*** For $p=2$ observe that if the place $\mathfrak{p}$ splits completely in $\mathrm{L}/\mathrm{K}$, then the "local factor" $a^*(\mathfrak{p})$ can be taken $a^*(\mathfrak{p}) = a(\mathfrak{p})$.

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

***Proposition 3.18*** *Let $S$ be a finite set of places of* $\mathrm{K}$ *with* $(S,p)=1$ *such that* $\mathrm{K}_S^{\varnothing}/\mathrm{K}$ *is infinite. Let* $(\mathrm{K}_n) := \mathcal{L}$ *be a tower in* $\mathrm{K}_S^{\varnothing}/\mathrm{K}$*. Let $T$ and $\Sigma$ be two other sets of places of $K$; we assume that $(\Sigma,p)=1$, but the cases $\Sigma=\varnothing$ and $S=\Sigma$ are allowed. Recall that $h_n$ denotes the class number of* $\mathrm{K}_n$*, and that* $g_n = \log|\operatorname{disc}(\mathrm{K}_n)|^{1/2}$ *denotes its genus. Let* $d_n = d(\mathrm{A}_\Sigma^T(\mathrm{K}_n))$ *be the $p$-rank of* $\mathrm{A}_\Sigma^T(\mathrm{K}_n)$*.*

(i) *We have*

$$\mathbb{M}_{\mathrm{A}_\Sigma^T(\mathrm{K}_n)} \leq \frac{[\mathrm{K}_n:\mathrm{K}]}{d_n}\Big(\log_p \operatorname{disc}(K,S)^{1/2}\cdot\frac{\log(h_n)}{g_n}+a(\Sigma)\Big).$$

(ii) *With $C_0$ denoting the constant from Lemma 3.1, we have*

$$\mathbb{M}_{\mathrm{A}_\Sigma^T(\mathrm{K}_n)} \leq \frac{[\mathrm{K}_n:\mathrm{K}]}{d_n}\big(C_0\log_p \operatorname{disc}(K,S)+a(\Sigma)\big).$$

*If, in addition, there is an $\varepsilon>0$ such that* $d_n \geq \varepsilon[\mathrm{K}_n:\mathrm{K}]$ *for all $n$, then* $\mathbb{M}_{\mathrm{A}_\Sigma^T(\mathrm{K}_n)}$ *is bounded as $n\to\infty$.*

**Proof** Recall that by Proposition 3.13, the genus $g_n = \log|\operatorname{disc}(\mathrm{K}_n)|^{1/2}$ of $\mathrm{K}_n$ satisfies

$$g_n \leq [\mathrm{K}_n:\mathrm{K}]\log\operatorname{disc}(\mathrm{K},S)^{1/2}. \tag{3.3}$$

Thanks to Lemma 3.15, we have

$$\begin{aligned}\log_p|\mathrm{A}_\Sigma^T(\mathrm{K}_n)| &\leq \log_p|A(\mathrm{K}_n)|+[\mathrm{K}_n:\mathrm{K}]a(\Sigma)\leq \log_p h_n+[\mathrm{K}_n:\mathrm{K}]a(\Sigma)\\ &\leq g_n\frac{\log_p(h_n)}{g_n}+[\mathrm{K}_n:\mathrm{K}]a(\Sigma).\end{aligned}$$

Now we apply (3.3) to the right-hand side to find

$$\log_p|\mathrm{A}_\Sigma^T(\mathrm{K}_n)| \leq [\mathrm{K}_n:\mathrm{K}]\Big(\frac{\log\operatorname{disc}(K,S)^{1/2}}{\log p}\cdot\frac{\log(h_n)}{g_n}+a(\Sigma)\Big).$$

It remains only to divide both sides by $d_n$ to obtain the desired inequality. For the second claim, we merely apply the bound from Lemma 3.1 to the bound from the first claim. ■

Before stating the key result of this section, we need a couple of definitions.

***Definition 3.19*** In a tower $(\mathrm{K}_n)$, and fixing auxiliary finite sets $\Sigma$ and $T$ of places of $K$, one says that the $p$-rank $d_n$ of $\mathrm{A}_\Sigma^T(\mathrm{K}_n)$ grows $\varepsilon$-linearly with respect to the degree (for some $\varepsilon>0$) if for $n\gg 0$, $d_n\geq\varepsilon[\mathrm{K}_n:\mathrm{K}]$.

***Definition 3.20*** Given a real number $A$, a number field $\mathrm{K}$ of signature $(r_1,r_2)$, and a finite set $S$ of places of $K$ coprime to $p$, let us define

$$\alpha(A,\mathrm{K},S)=A\log\sqrt{\operatorname{disc}(\mathrm{K},S)}-\frac{r_1}{2}(\gamma+1+\log\pi)-r_2(\gamma+\log 2).$$

***Theorem 3.21*** *We maintain all the hypotheses and notation of Proposition 3.18. We assume that there exists $\varepsilon>0$ such that* $d_n\geq\varepsilon[\mathrm{K}_n:\mathrm{K}]$ *for all $n$. If the conditions of*

*Theorem 2.1 apply to* $(\mathrm{K}_n)$, *then*

$$\limsup_n \mathbb{M}_{\mathrm{A}_\Sigma^T(\mathrm{K}_n)} \leq \frac{1}{\varepsilon}\Big(\frac{\alpha(B(\mathcal{L}),\mathrm{K},S)}{\log p} + a(\Sigma)\Big).$$

*Consequently,*

$$\underline{\mathbb{M}}(\mathcal{L},\Sigma,T) \leq \frac{1}{\varepsilon}\Big(\frac{\alpha(B(\mathcal{L}),\mathrm{K},S)}{\log p} + a(\Sigma)\Big).$$

*If, moreover, the tower* $(\mathrm{K}_n)$ *is exhaustive in* $\mathcal{L}$, *then one can replace* $\underline{\mathbb{M}}$ *by* $\overline{\mathbb{M}}$.

**Proof** We begin with the inequality of Proposition 3.18 but introduce the contribution of the regulator, as follows:

$$\mathbb{M}_{\mathrm{A}_\Sigma^T(\mathrm{K}_n)} \leq \frac{[\mathrm{K}_n:\mathrm{K}]}{d_n}\Bigg(\frac{\log\mathrm{disc}(K,S)^{1/2}}{\log p}\Big(\frac{\log(h_n\,\mathrm{Reg}_n)}{g_n} - \frac{\log(\mathrm{Reg}_n)}{g_n}\Big) + a(\Sigma)\Bigg).$$

By hypothesis, we have $[\mathrm{K}_n:\mathrm{K}]/d_n \leq 1/\varepsilon$. By Theorem 2.1, $\log(h_n\,\mathrm{Reg}_n)/g_n$ tends to $B(\mathcal{L})$. The last ingredient is a theorem of Zimmert [42] (we use the enhanced version proved by Tsfasman and Vladut [38, Theorem 7.4]):

$$\liminf_n \log(\mathrm{Reg}_n)/g_n \geq (\log\sqrt{\pi e} + \gamma/2)\phi_{\mathbb{R}} + (\log 2 + \gamma)\phi_{\mathbb{C}}.$$

Recalling the definition of $\phi_{\mathbb{R}}, \phi_{\mathbb{C}}$, and noting that $r_i(\mathrm{K}_n) = [\mathrm{K}_n:\mathrm{K}]r_i(\mathrm{K})]$ for $i = 1, 2$, we find, after applying Proposition 3.13, that

$$\phi_{\mathbb{R}} \geq \frac{r_1(K)}{\log\sqrt{\mathrm{disc}(\mathrm{K},S)}} \quad\text{and}\quad \phi_{\mathbb{C}} \geq \frac{r_2(K)}{\log\sqrt{\mathrm{disc}(\mathrm{K},S)}}.$$

Putting all of this together and taking $\limsup_n \mathbb{M}_{\mathrm{A}_\Sigma^T(\mathrm{K}_n)}$, we obtain the bound sought. ∎

We will state the following immediate corollary of the theorem, since it will be the form in which we will apply it most frequently.

***Corollary 3.22*** *Suppose in the theorem, we have* $S = \Sigma = T = \varnothing$. *Then, assuming the conditions of Theorem 2.1 apply to a tower* $\mathcal{L}$ *inside* $\mathrm{K}_\varnothing^\varnothing/\mathrm{K}$, *we have*

$$\begin{aligned}\underline{\mathbb{M}}(\mathcal{G}_\varnothing^\varnothing) &\leq \underline{\mathbb{M}}(\mathcal{L},\varnothing,\varnothing)\\ &\leq \frac{1}{\varepsilon\log(p)}\Big(\frac{B(\mathcal{L})}{2}\log|\mathrm{disc}(\mathrm{K})| - \frac{r_1}{2}(\gamma+1+\log\pi) - r_2(\gamma+\log 2)\Big).\end{aligned}$$

***Remark 3.23*** The comparison of Corollary 3.22 to Proposition 3.2 illustrates how the Tsfasman–Vladut theorem allows us to give an improved upper bound for the mean exponent.

## 4 Refined Estimates. The Tsfasman–Vladut Method

We want to illustrate the previous section with a few examples where we have optimized the quantity $B(\mathrm{L}/\mathrm{K})$ by employing the techniques of Tsfasman and Vladut [38].

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

### 4.1 Tsfasman–Vladut Machinery

Let us fix an asymptotically exact extension $\mathcal{L} := \mathrm{L}/\mathrm{K}$. Estimating the constant $B(\mathrm{L}/\mathrm{K})$ given by Theorem 2.1 is an interesting problem, involving certain kinds of optimization. Indeed the quantity for which we would like to have a tight upper bound is the sum

$$\sum_q b_q\phi_q - b_0\phi_{\mathbb{R}} - b_1\phi_{\mathbb{C}}$$

satisfying the three following conditions:

(a) $\phi_q > 0$ ;
(b) $\sum_m m\phi_{\ell^m} \leq \phi_{\mathbb{R}} + 2\phi_{\mathbb{C}}$ for all $\ell$;
(c) $\sum_q a_q\phi_q + a_0\phi_{\mathbb{R}} + a_1\phi_{\mathbb{C}} \leq 1$,

where

$$b_q = \log\frac{q}{q-1}, \qquad a_q = \frac{\log q}{\sqrt{q}-1},$$
$$a_0 = \log 2\sqrt{2\pi} + \pi/4 + \gamma/2, \qquad a_1 = \log(8\pi) + \gamma,$$
$$b_0 = \log 2, \qquad b_1 = \log 2\pi.$$

One now replaces each $\phi_q$ by a variable $x_q$, and the problem becomes a question of linear optimization. For convenience, we put $x_0 = \phi_{\mathbb{R}}$ and $x_1 = \phi_{\mathbb{C}}$.

One studies the quantity $\sum_q b_q x_q - b_0x_0 - b_1x_1$ when $x_0$ and $x_1$ are fixed (*i.e.*, when, for example, one has a totally real tower or a totally complex tower). Similarly, one can exploit knowledge of any finite place that is totally split in $\mathcal{L}$. One can also use some information coming from the base field K: typically if the base field has no place of norm $\ell$, then $x_\ell$ would be fixed and equals 0.

Denote by $\Sigma = \{q_1, \dots, q_r\}$ a set of powers of prime numbers for which one fixes $x_{q_i}$. We want to give an upper bound as small as possible of the quantity

$$\sum_{q\notin\Sigma} b_q x_q,$$

with the conditions

(a)′ $x_q > 0$,
(b)′ $\sum_m m x_{q^m} \leq x_0 + 2x_1$,
(c)′ $\sum_{q\notin\Sigma} a_q x_q \leq 1 - \sum_{q\in\Sigma} a_q x_q$.

As explained in [38], there are two reductions: first, one can assume that $x_{\ell^*}$ attains the maximum for condition (b)′, where $\ell^*$ is the smallest power of $\ell$ for which $x_{\ell^*} \neq 0$; then try to optimize inequality (c)′ for the smallest powers $\ell^*$.

Now let $\ell_0^*$ the smallest power such that

$$\sum_{\ell^*<\ell_0^*} (x_0 + 2x_1 - \varepsilon_{\ell^*})a_{\ell^*} \leq 1 - \Big(a_0x_0 + a_1x_1 + \sum_{q\in\Sigma} a_q x_q\Big),$$

where $\varepsilon_{\ell^*} \leq x_0 + 2x_1$ is a constraint of $\ell$ related to the base field.

Let $\alpha \in [0,1)$ such that

$$\alpha(x_0 + 2x_1 - \varepsilon_{\ell_0^*})a_{\ell_0^*} = 1 - a_0x_0 - a_1x_1 - \sum_{q\in\Sigma} a_q x_q - \sum_{\ell^*<\ell_0^*} (x_0 + 2x_1 - \varepsilon_{\ell^*})a_{\ell^*}.$$

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

***Proposition 4.1*** *One has*

$$\sum_q b_q \phi_q \ \leq \ \sum_{q \in \Sigma} b_q x_q + \sum_{\ell^* < \ell_0^*} (x_0 + 2x_1 - \varepsilon_{\ell^*}) b_{\ell^*} + \alpha (x_0 + 2x_1 - \varepsilon_{\ell_0^*}) b_{\ell_0^*}.$$

## 4.2 Strategy for Construction of Examples

Below we will study some examples built with the following strategy. First, for $p = 2$, let $\mathrm{k}/\mathbb{Q}$ be a real quadratic field. Suppose that for the set $T$ of places of $\mathbb{Q}$, the 2-tower $\mathrm{k}_\varnothing^T/\mathrm{k}$ is infinite (to achieve this, we apply Corollary 2.7). Consider then $\mathrm{K} := \mathrm{k}(\sqrt{-D})$, where $D = \prod_{\mathfrak{p} \in T} \mathfrak{p}$; put $\mathcal{L} := \mathrm{K}\mathrm{k}_\varnothing^T$. Take an exhaustive tower $(\mathrm{k}_n)_n$ of $\mathrm{k}_\varnothing^T/\mathrm{k}$; then $\mathrm{K}_n := \mathrm{k}_n\mathrm{K}$ is an exhaustive tower of $\mathcal{L}$. Moreover, $(\mathrm{K}_n)$ is a subtower of $\mathrm{K}_\varnothing^T$. And then, by Corollary 3.22, one obtains bounds for $\overline{\mathbb{M}}(\mathcal{L})$ and $\underline{\mathbb{M}}(\mathrm{K}_\varnothing^\varnothing/\mathrm{K})$.

## 4.3 Examples

In all of the examples below, we fix $p = 2$, since in this case, we can employ ramification at infinity in conjunction with the genus theory bounds.

***Example 4.2*** Let $\mathrm{k} = \mathbb{Q}(\sqrt{8 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23})$. Thanks to Corollary 2.7, the number field k has an infinite 2-extension $\mathrm{k}^T/\mathrm{k}$ ($S = \varnothing$), where $T = \{\ell_9\}$ is the set containing the only place above 3 (of norm 9). Put $\mathrm{K} = \mathrm{k}(\sqrt{-3})$. Denote by $(\mathrm{k}_n)$ a tower of $\mathrm{k}^T$; put $\mathrm{K}_n = \mathrm{K}\mathrm{k}_n$, $\mathrm{L} = \bigcup_n \mathrm{K}_n$, and $\mathrm{L}/\mathrm{K} := \mathcal{L}$. Then by Genus Theory (*cf.* Theorem 2.5) along $\mathrm{k}^T/\mathrm{k}$, one obtains that

$$d_n = d_2\mathrm{A}(\mathrm{K}_n) \geq [\mathrm{K}_n : \mathrm{K}] - 1.$$

If we apply Corollary 3.22, we find

$$\underline{\mathbb{M}}(\mathrm{K}_\varnothing^\varnothing/\mathrm{K}) \leq \overline{\mathbb{M}}(\mathcal{L}) \leq \frac{1}{22 \cdot \log 2}\Big( B \log \sqrt{|\operatorname{disc}(\mathrm{K})|} - (\gamma + \log 2)\Big) \approx 30.683 \cdots,$$

where one has taken $B \approx 1.0938$. But we can do better by applying the refined results of Tsfasman and Vladut. The base field K is of degree 4 over $\mathbb{Q}$. The tower we consider is totally complex and by construction the prime $\ell^* = 9$ (over 3 with norm 9) splits completely in the considered tower. Here, $g_\mathrm{K} = \log(\sqrt{8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23})$. In order of increasing size of the norm, one has ideals of norm: 4, 7, 7, 9, 13, 13, 19, 19, 25, 31, 37, 43, 43, 43, 43 etc.

One fixes the following conditions $x_0 = 0$, $x_1 = r_2/g = 2/g$, $x_2 = 0$, $x_3 = 0$, $x_5 = 0$, $x_9 = 1/g = x_1/2$. One considers $\Sigma = \{9\}$. Moreover, $x_4 \leq 1/g = x_1/2$, $\varepsilon_{2^*} = x_1$ and $x_{25} \leq 1/g$. One has

$$g - 2(\gamma + \log(8\pi)) - \frac{\log 9}{\sqrt{9} - 1} - 2\Big(\frac{\log 7}{\sqrt{7} - 1} + \frac{\log 13}{\sqrt{13} - 1} + \frac{\log 19}{\sqrt{19} - 1}\Big) \\ - \Big(\frac{\log 4}{\sqrt{4} - 1} + \frac{\log 25}{\sqrt{25} - 1}\Big) - 4\frac{\log 31}{\sqrt{31} - 1} < \frac{\log 37}{\sqrt{37} - 1},$$

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

and then $\ell_0^* = 37$. One obtains

$$B(\mathrm{L}/\mathrm{K}) \leq 1 - \frac{r_2}{g}\log 2\pi + \frac{1}{g}\Big(\log(4/3) + \log(9/8) + \log(25/24) \\ + 2\log(7/6) + 2\log(13/12) + 2\log(19/18) + 4\log(31/30) + 4\alpha\log(37/36)\Big),$$

where

$$4\alpha\frac{\log 43}{\sqrt{43}-1} = g - 2(\log 8\pi + \gamma) - \frac{\log 9}{2} - \log 4 - \frac{\log 25}{\sqrt{25}-1} \\ - 2\Big(\frac{\log 7}{\sqrt{7}-1} + \frac{\log 13}{\sqrt{13}-1} + \frac{\log 19}{\sqrt{19}-1} + 2\frac{\log 31}{\sqrt{31}-1}\Big).$$

and then $B(\mathrm{L}/\mathrm{K}) \approx 0.878\cdots$, and

$$\underline{\mathbb{M}}(\mathrm{K}_{\varnothing}^{\varnothing}/\mathrm{K}) \leq \overline{\mathbb{M}}(\mathcal{L}) \leq 24.100.$$

***Example 4.3*** Let k be the real quadratic field of discriminant $D$ where $D$ is the the product of the elements in the set

$$U = \{47, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, \\ 107, 109, 113, 127, 131, 137, 139, 149, 151\}.$$

Let $T_{\mathrm{in}} = \{3, 7, 29, 31, 37, 41, 43, 53\}$ and $T_{\mathrm{dec}} = \{2, 5, 11, 13, 17, 19, 23\}$; put $T = T_{\mathrm{in}} \cup T_{\mathrm{dec}}$; $|T| = 22$. The places of $T_{\mathrm{in}}$ are inert in $\mathrm{k}/\mathbb{Q}$ and the places of $T_{\mathrm{dec}}$ are totally decomposed in $\mathrm{k}/\mathbb{Q}$. One uses Corollary 2.7: the number field k has an infinite $T$-split 2-tower $\mathrm{k}^T/\mathrm{k}$. Consider now the number field $\mathrm{K} = \mathrm{k}(\sqrt{-D})$, where $D = \prod_{\ell \in T}\ell$ and put $\mathrm{L} = \mathrm{K}\mathrm{k}^T$. Then for all number fields $\mathrm{K}_n$ along $\mathrm{L}/\mathrm{K}$, one has

$$d_2\mathrm{A}(\mathrm{K}_n) \geq 22[\mathrm{K}_n : \mathrm{K}] - 1.$$

Then

$$\mathbb{M}(\mathrm{K}_n) \leq \frac{1}{22\log 2}\cdot\Big(B\log\sqrt{|d_{\mathrm{K}}|} - (\gamma + \log 2)\Big) \approx 9.662\cdots$$

We now use the strategy of Tsfasman and Vladut to optimize $B(\mathrm{L}/\mathrm{K})$. Each place of $T$ splits totally in $\mathrm{L}/\mathrm{K}$: the associated parameters $\phi_{\ell^*}$ are then fixed. More precisely, for every $\ell \in T_{\mathrm{in}}$, we have $\phi_\ell = 0$, $\phi_{\ell^2} = 1/g$ and $\phi_{\ell^i} = 0$ for $i > 2$; for $\ell \in T_{\mathrm{dec}}$, one fixes $\phi_\ell = 2/g$ and $\phi_{\ell^i} = 0$ for $i > 1$. Moreover, for $\ell \leq 150$, $\phi_{\ell^*} \leq 2/g$. In fact, one can be more precise: only the primes of $R = \{47, 49, 61, 103, 113, 127, 131, 139\}$ split (and ramify); the others are inert (with $67^2$ the smallest norm). One remarks that the sum

$$A = g - 2(\gamma + \log 8\pi) - 2\sum_{\ell \in T_{\mathrm{dec}}}\frac{\log\ell}{\sqrt{\ell}-1} - \sum_{\ell \in T_{\mathrm{in}}}\frac{\log\ell^2}{\ell - 1} - 2\sum_{\ell \in R}\frac{\log\ell}{\sqrt{\ell}-1} \approx 103.774$$

is smaller than $4\sum_{\ell \leq 67^2}^{*}\log\ell/\sqrt{\ell} - 1$ where the last sum is taken over the splitting places in $\mathrm{K}/\mathbb{Q}$ (*i.e.*, 127 such places). One finds $\ell_0^* = 3877$, and, to finish,

$$A - 4\sum_{153 \leq \ell < 3877}^{*}\frac{\log\ell}{\sqrt{\ell}-1} \approx 0.528.$$

Here, $\alpha \approx 0.980$

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

After making the computation of the default, one obtains

$$\sum_q b_q \phi_q \le 3.348,$$

and then $B(\mathrm{L}/\mathrm{K}) \le 1.01421\cdots$ and

$$\underline{\mathbb{M}}(\mathrm{K}_\emptyset^\emptyset/\mathrm{K}) \le \overline{\mathbb{M}}(\mathcal{L}) \le \frac{1}{\log 2} 6.306\cdots \approx 9.098\cdots.$$

***Example 4.4*** Let

$$\mathrm{k} = \mathbb{Q}(\sqrt{8\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41\cdot 43\cdot 47\cdot 53}).$$

Let $T_{\mathrm{in}} = \{71, 79, 83, 97, 101\}$ et $T_{\mathrm{dec}} = \{59, 61, 67, 73\}$; $T = T_{\mathrm{in}} \cup T_{\mathrm{dec}}$; $|T| = 13$. Put $\mathrm{K} = \mathrm{k}(\sqrt{-59\cdot 61\cdot 67\cdot 71\cdot 73\cdot 79\cdot 83\cdot 97\cdot 101})$. The number field k has an infinite 2-tower $\mathrm{k}^T$; put $\mathrm{L} = \mathrm{K}\mathrm{k}^T$. Along the extension L/K, one has

$$d_2 \mathrm{A}(\mathrm{K}_n) \ge 13[\mathrm{K}_n : \mathrm{K}] - 1.$$

By looking at the primes $\ell \le 100$, one sees that

$$x_2 = x_3 = x_7 = x_{19} = x_{29} = x_{31} = x_{41} = x_{47} = x_{53} = 0.$$

Here, $\ell_0^* = 1249$ and so there are 47 primes that are splitting in $\mathrm{K}/\mathbb{Q}$ and with norm less than $\ell_0^*$. One finds that $\alpha \approx 1.020$,

$$\sum_q b_q \phi_q \le 2.192\cdots,$$

and $B(\mathrm{L}/\mathrm{K}) \le 0.951\cdots$. To conclude,

$$\underline{\mathbb{M}}(\mathrm{K}_\emptyset^\emptyset/\mathrm{K}) \le \overline{\mathbb{M}}(\mathcal{L}) \le \frac{1}{\log 2} 6.139\cdots \approx 8.857.\cdots$$

***Example 4.5*** Take $p = 2$. Let $\mathrm{k} = \mathbb{Q}(\sqrt{2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 43})$. Put $T_{\mathrm{dec}} = \{59, 61\}$ and $T_{\mathrm{in}} = \{37, 47, 53, 67, 89\}$; $|T| = 9$. Let us consider $\mathrm{K} = \mathrm{k}(\sqrt{-37\cdot 47\cdot 53\cdot 59\cdot 61\cdot 67\cdot 89})$. Along the extension L/K, one has

$$d_2 \mathrm{A}(\mathrm{K}_n) \ge 9[\mathrm{K}_n : \mathrm{K}] - 1.$$

Here,

$$x_2 = x_3 = x_7 = x_{13} = x_{31} = x_{37} = x_{47} = 0, \quad \ell_0^* = 647, \quad \text{and } \alpha \approx 0.072.$$

Then $\sum_q b_q \phi_q \le 1.993\cdots$, $B(\mathrm{L}/\mathrm{K}) \le 0.9733\cdots$, and $\underline{\mathbb{M}}(\mathrm{K}_\emptyset^\emptyset/\mathrm{K}) \le \overline{\mathbb{M}}(\mathcal{L}) \le 9.657\cdots$.

***Example 4.6*** Take $p = 2$. Let

$$\mathrm{k} = \mathbb{Q}(\sqrt{8\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41\cdot 43\cdot 47\cdot 53\cdot 59\cdot 61\cdot 67\cdot 71\cdot 73}).$$

Put $T_{\mathrm{dec}} = \{79, 83, 89, 97, 107, 109, 137\}$ and $T_{\mathrm{in}} = \{101, 103, 113, 127, 131, 149, 157, 173\}$. Let $D$ be the product of the elements in $T_{\mathrm{dec}}$ and $T_{\mathrm{in}}$ and let $\mathrm{K} = \mathrm{k}(\sqrt{D})$. Here, $d_2\mathrm{A}(\mathrm{K}_n) \ge 20[\mathrm{K}_n : \mathrm{K}] - 1$. Finally, for this example, $\ell_0^* = 1069$, $B(\mathcal{L}) \le 1.013\cdots$, and thus

$$\underline{\mathbb{M}}(\mathrm{K}_\emptyset^\emptyset/\mathrm{K}) \le \overline{\mathbb{M}}(\mathcal{L}) \le 10.022\cdots.$$

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

# 5 Linear Growth of the $p$-class Rank

## 5.1 The Mean $\mathbb{M}$ and a Question of Ihara

The examples of the previous section show how primes that split completely can be used to produce towers with linear growth for the $p$-rank of the class group, which then places constraints on the asymptotic mean $\underline{\mathbb{M}}$. In particular, with the help of Proposition 2.2, we have the following result.

***Proposition 5.1*** *Let $S$ and $T$ be two sets of places of $\mathrm{K}$, $(S,p)=1$. For all subfields $\mathrm{K}_n$ of $\mathrm{K}_S^T$, one has*

$$d_p \mathrm{A}_T(\mathrm{K}_n) \geq [\mathrm{K}_n : \mathrm{K}]\Big(|T| - \big(r_1(\mathrm{K}) + r_2(\mathrm{K})\big)\Big).$$

*Note that by the Golod–Shafarevich criterion (see Theorem 2.3 and Proposition 2.4), $\mathrm{K}_S^T/\mathrm{K}$ is infinite once $|S|$ is large as compared to $|T|$, and in this case*

$$\underline{\mathbb{M}}(\mathrm{K}_S^T/\mathrm{K}, T, \varnothing) \leq \frac{1}{|T| - (r_1(\mathrm{K}) + r_2(\mathrm{K}))}\Big(\frac{\alpha(B(\mathrm{K}_S^T/\mathrm{K}), \mathrm{K}, S)}{\log p} + a(T)\Big),$$

*where $a(T)$ is given in Definition 3.14 and 3.16.*

**Proof** The proof is an application of Theorem 3.21 with $\varepsilon = |T| - (r_1(\mathrm{K}) + r_2(\mathrm{K}))$. ■

At this point, let us recall a question of Ihara [18]:

***Question 5.2*** What can one say about the number of primes that decompose completely in an infinite unramified Galois extension?

The importance of the above question for the invariant $\mathbb{M}$ is illustrated in the following corollary.

***Corollary 5.3*** *Suppose that in the pro-$p$-extension $\mathrm{K}_S/\mathrm{K}$, with $(S,p)=1$, the set $\mathcal{T}$ of places that split completely in this tower is infinite. Then for all $\varepsilon > 0$, by taking large $T \subset \mathcal{T}$, one obtains*

$$1 \leq \underline{\mathbb{M}}(\mathrm{K}_S/\mathrm{K}, T, \varnothing) \leq \frac{a(T)}{|T|} + \varepsilon.$$

*If, moreover, the set $\mathcal{T}$ contains infinitely many primes $\mathfrak{p}$ with $a(\mathfrak{p}) = 1$, then, by choosing $T$ to consist only of such primes, we can arrange $\underline{\mathbb{M}}(\mathrm{K}_S/\mathrm{K}, T, \varnothing)$ to be as close to 1 as desired.*

## 5.2 Ershov's Trick

Thanks to a result of Schmidt [36], the phenomenon of Proposition 5.1, which we derived from number theory considerations, can be obtained via a clever idea due to Ershov [5] using pro-$p$-group presentations.

Let $\mathrm{K}$ be a number field and $S_0$ a finite set of places of $\mathrm{K}$, $(S_0, p) = 1$. We assume that $\delta_{\mathrm{K}} = 0$ and that $\mathrm{A}_{\mathrm{K}}$ is trivial. By [36], one can choose a finite set $\Sigma$ of places of $\mathrm{K}$ such that

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

(a) $(\Sigma, p) = 1$, $S_0 \subset \Sigma$;
(b) the natural map $H^2(\mathcal{G}_\Sigma, \mathbb{F}_p) \xrightarrow{\sim} \oplus_{v\in\Sigma} H^2(\mathcal{G}_v, \mathbb{F}_p)$ is an isomorphism;
(c) the pro-$p$-group $\mathcal{G}_\Sigma$ is of cohomological dimension 2 and

$$\chi(\mathcal{G}_\Sigma) := 1 - d_p H^1(\mathcal{G}_\Sigma, \mathbb{F}_p) + d_p H^2(\mathcal{G}_\Sigma, \mathbb{F}_p) = r_1(\mathrm{K}) + r_2(\mathrm{K}).$$

Put $d = d_p\mathcal{G}_\Sigma$ and $k = |\Sigma|$. As $\mathrm{A}_\mathrm{K}$ is trivial, $d \le k$.

By (b), the relations of $\mathcal{G}_\Sigma$ are all local. In fact, by following the proof of [36, Theorem 6.1], one can show that there exists a subset $S \subseteq \Sigma$ containing $S_0$ with the following property. Letting $T = \Sigma - S$ and $t = |T|$, there exists a basis of generators $(x_i)$ of $\mathcal{G}_\Sigma$ such that for $i = 1, \dots, t$, every element $x_i$ is a generator of the inertia group in $\mathrm{K}_\Sigma/\mathrm{K}$ of one place of $T$. (The set $S$ allows us to kill a certain Shafarevich group.) The quantities $t$ and $d$ can be as large as we want.

Hence, the group $\mathcal{G}_\Sigma$ can be described by generators and relations as

$$\left\langle x_1, \dots, x_d \;\middle|\; [x_1, F_1]x_1^{p\lambda_1}, \dots, [x_t, F_t]x_t^{p\lambda_t},\ r_{t+1}, \dots, r_k \right\rangle,$$

where the elements $F_i$ are lifts of the Frobenius of the places $v_i \in S$, and $\lambda_i$ belongs to $\mathbb{Z}_p$ (for $p = 2$, $\lambda_i \in 2\mathbb{Z}_2$) and where we recall that $k = d_pH^2(\mathcal{G}_\Sigma, \mathbb{F}_p) = |\Sigma|$. Note that the relations $[x_i, F_i]x_i^{p\lambda_i}$, $i = 1, \dots, t$ are the local conditions.

Then take a minimal presentation of $\mathcal{G} := \mathcal{G}_\Sigma$ as follows:

$$1 \longrightarrow R \longrightarrow \mathrm{F} \longrightarrow \mathcal{G} \longrightarrow 1,$$

where $R$ is the normal subgroup of $\mathrm{F}$ generated by the relations

$$\left\langle [x_1, F_1]x_1^{p\lambda_1}, \dots, [x_t, F_t]x_t^{p\lambda_t},\ r_{t+1}, \dots, r_k \right\rangle.$$

Let $\mathcal{H}$ be the normal subgroup of $\mathrm{F}$ generated by the elements $x_1, \dots, x_t, F_1, \dots, F_t$. By maximality, the subgroup $\mathcal{H}R$ corresponds to $\mathcal{G}_S^T$. Put $\Gamma = \mathcal{G}_S^T$.

Now let $\Gamma_i$ be an open subgroup of $\Gamma$ and let $\mathrm{F}_i$ be the normal subgroup of $\mathrm{F}$ containing $\mathcal{H}R$ and satisfying $\mathrm{F}/\mathrm{F}_i \simeq \Gamma/\Gamma_i \simeq \mathcal{G}/\mathcal{G}_i$, where $\mathcal{G}_i$ corresponds to $\mathrm{F}_i/R$. Now by Schreier's formula one has

$$d_p\mathrm{F}_i - 1 = [\mathrm{F}:\mathrm{F}_i](d_p\mathcal{G} - 1),$$

by recalling that $d_p\mathcal{G} = d_p\mathrm{F}$. One then has the exact sequence

$$1 \longrightarrow \mathrm{F}_i^p[\mathrm{F}_i, \mathrm{F}_i]R/\mathrm{F}_i^p[\mathrm{F}_i, \mathrm{F}_i] \longrightarrow \mathrm{F}_i/\mathrm{F}_i^p[\mathrm{F}_i, \mathrm{F}_i] \longrightarrow \mathrm{F}_i/\mathrm{F}_i^p[\mathrm{F}_i, \mathrm{F}_i]R \longrightarrow 1,$$

where $\mathrm{F}_i/R \simeq \mathcal{G}_i$. Now, by construction, as $\mathrm{F}_i$ contains $\mathcal{H}$, the first generators of $R$ are in $\mathrm{F}_i^p[\mathrm{F}_i, \mathrm{F}_i]$. One sees very quicky that the quotient $\mathrm{F}_i^p[\mathrm{F}_i, \mathrm{F}_i]R/\mathrm{F}_i^p[\mathrm{F}_i, \mathrm{F}_i]$ is topologically generated by the elements of the form $yzy^{-1}$, where $y$ is a representative of a class of $\mathrm{F}/\mathrm{F}_i$ and $z \in \{r_{t+1}, \dots, r_k\}$: indeed, $R \subset \mathrm{F}_i$. Thus,

$$d_p(\mathcal{G}_i) \ge [\mathcal{G}:\mathcal{G}_i](d - 1 - k + t) + 1,$$

and as $1 - d + k = \chi(\mathcal{G}_\Sigma) = r_1(\mathrm{K}) + r_2(\mathrm{K})$, one obtains

$$\frac{d_p(\mathcal{G}_i)}{[\mathcal{G}:\mathcal{G}_i]} \ge t - \big(r_1(\mathrm{K}) + r_2(\mathrm{K})\big).$$

Here, $\mathcal{G}_i = \mathcal{G}_\Sigma(\mathrm{K}_i)$, where $\mathrm{K}_i$ is the fixed field of $\mathcal{G}_i$ inside the tower $\mathrm{K}_\Sigma/\mathrm{K}$.

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

### 5.3 On Schreier's Bound

Recall again the principle behind the construction of the examples of Section 4. Take $p = 2$. Let k be a real quadratic field having an infinite 2-extension $\mathrm{k}^T/\mathrm{k}$. Put $t = |T| - (r_1 + r_2)$. Let K/k be an imaginary quadratic extension in which all places of $T$ are ramified. Let $(\mathrm{k}_n)$ be an exhaustive tower in $\mathrm{k}^T/\mathrm{k}$ and consider the tower $(\mathrm{Kk}_n)$ of K, which is evidently inside $\mathrm{K}^T/\mathrm{K}$. By Genus Theory applied to each quadratic extension $\mathrm{K}_n/\mathrm{k}_n$, $d_p\mathrm{A}(\mathrm{K}_n) \geq [\mathrm{K}_n : \mathrm{K}]t - 1$. In [14], it was proved that in fact

$$d_p\mathrm{A}(\mathrm{K}_n) \geq [\mathrm{K}_n : \mathrm{K}]t + 1.$$

At this level, we recall that Genus Theory allows us a lower bound of the $p$-rank of a subgroup of $\mathrm{A}(\mathrm{K}_n)$ without taking into account the contribution of $\mathrm{A}(\mathrm{k}_n)$, *i.e.*,

$$d_p\mathrm{A}(\mathrm{K}_n) \geq [\mathrm{K}_n : \mathrm{K}]t - 1 + \alpha_n,$$

with $\alpha_n \leq d_p\mathrm{A}(\mathrm{k}_n)$ measuring the added contribution to the rank coming from the injection of $\mathrm{A}(\mathrm{k}_n)$ into $\mathrm{A}(\mathrm{K}_n)$ (see [25]).

In the other direction, thanks to Schreier's inequality, one has

$$d_p\mathrm{A}(\mathrm{K}_n) \leq \big( d_p\mathrm{A}(\mathrm{K}) - 1 \big) [\mathrm{K}_n : \mathrm{K}] + 1,$$

and then

$$t\,[\mathrm{K}_n : \mathrm{K}] \leq d_p\mathrm{A}(\mathrm{K}_n) - 1 \leq \big( d_p\mathrm{A}(\mathrm{K}) - 1 \big) [\mathrm{K}_n : \mathrm{K}],$$

which naturally raises the following question, which was raised in [14].

***Question 5.4*** Is it possible to create an example as above having an optimal inequality, *i.e.*, such that $d_pA(\mathrm{K}) - 1 = t$?

In [14], it was shown that a sequence of examples can be created with the ratio $(d_p\mathrm{A}(\mathrm{K}) - 1)/t$ tending to 1. In the remainder of this section, we will make an attempt to find examples with small $(d_p\mathrm{A}(\mathrm{K}) - 1) - t$ by considering some ray class groups.

We take $p = 2$. To recall a theorem due to Gras and Munnier (see [12, section I.4, or chapter VI] or [13]), we fix the notation. Let $\mathrm{F}' := \mathrm{F}(\sqrt{E}, \sqrt{A})$ be the governing field of a number field $F$, where $E$ is the group of units of F, where $A = \{a_1, \ldots, a_d\}$, ${\mathcal{A}_i}^2 = a_i\mathcal{O}_\mathrm{F}$, $(\mathcal{A}_i)_i$ being a system of generators of $\mathrm{A}(\mathrm{F})[2]$.

***Theorem 5.5*** (Gras–Munnier) *Let $T = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ be a set of places of* K*, with* $\mathrm{N}\mathfrak{p}_i \equiv 1 \bmod p$. *There exists an extension* L/F *cyclic of degree* 2*, exactly and totally ramified at $T$ if and only if, for $i = 1, \ldots, t$, there exists $a_i \in \mathbb{F}_p^\times$, such that*

$$\prod_{i=1}^{t} \Big( \frac{\mathrm{F}'/\mathrm{F}}{\mathfrak{P}_i} \Big)^{a_i} = 1 \in \mathrm{Gal}(\mathrm{F}'/\mathrm{F}),$$

*where $\mathfrak{P}_i$ is an ideal of $L$ above $\mathfrak{p}_i$.*

Now, take $\ell$ to be a prime with $\ell \equiv 1 \bmod 32$. Let F be the totally real subfield of $\mathbb{Q}(\zeta_\ell)$ of degree 16 over $\mathbb{Q}$. Let $\{-1, \varepsilon_1, \ldots, \varepsilon_r\}$ be a basis of $E/E^2$. Note that the extension $\mathrm{F}'/\mathbb{Q}$ is a Galois extension and contains F (here F′ is the governing field defined above). By the Chebotarev Density Theorem, we can find an odd prime $q$ that splits completely in $\mathrm{F}'/\mathbb{Q}$. Now by Theorem 5.5, for all primes $\mathfrak{q}_i$ of F above $q$,

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

there exists a cylic 2-extension exactly $\{\mathfrak{q}_i\}$-ramified. We conclude that the 2-rank of the 2-class group $\mathrm{A}_S(\mathrm{K})$ is at least 16, where $S$ is the set of places of K above $q$. Moreover, by the condition above $q$, one has that $-1$ is a square in $\mathbb{Q}_q$; that means that $q \equiv 1 \bmod 4$. Now, again by applying the Chebotarev Density Theorem, take $p_1$ that splits completely in the extension $\mathrm{F}_S^{ab}(\sqrt{-1})/\mathbb{Q}$ as well as another prime $p_2$ that splits completely in $\mathrm{F}_S/\mathbb{Q}$ but which is inert in $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$.

Let $T$ be the set of places of F above $\{p_1, p_2\}$. Then the 2-rank of $\mathcal{G}_S := \mathrm{Gal}(\mathrm{F}_S/\mathrm{F})$ and the 2-rank of $\mathcal{G}_S^T := \mathrm{Gal}(\mathrm{F}_S^T/\mathrm{F})$ are the same and are at least 16. Now, $r(\mathcal{G}_S^T) \le 48$ (see Proposition 2.4) and, by the Golod-Shafarevich Theorem (see Theorem 2.1) the tower $\mathrm{F}_S^T/\mathrm{F}$ is infinite, and then the tower $\mathbb{Q}_\Sigma^T/\mathbb{Q}$ is infinite too, where $\Sigma = \{q, \ell\}$.

Put $\mathrm{K} = \mathbb{Q}(\sqrt{-p_1p_2})$. The primes $\ell$ and $q$ are split in K/$\mathbb{Q}$. As $p_2 \equiv 3 \bmod 4$, one has $\mathrm{d}_2\mathrm{A}_K = 1$ and the 2-rank of the ray class group of K with modulus $q\ell$ is at most 5. Now consider the compositum $\mathrm{L} := \mathbb{Q}_\Sigma^T\mathrm{K}$. Thanks to Schreier's inequality and to Genus Theory, one has for all number fields $\mathrm{K}_n$ in L/K:

$$2[\mathrm{K}_n : \mathrm{K}] \le d_2\mathrm{A}_\Sigma(\mathrm{K}_n) - 1 \le 4[\mathrm{K}_n : \mathrm{K}].$$

By assuming a hypothesis, we can improve the above estimate. Indeed, the 2-group $\mathcal{G} := \mathrm{Gal}(\mathrm{F}/\mathbb{Q})$ acts on the elementary abelian 2-group $\mathcal{H} := \mathrm{Gal}(\mathrm{F}'/\mathrm{F})$. Hence, there exists a subgroup $\mathcal{H}_0$ of $\mathcal{H}$ of order 2 on which $\mathcal{G}$ acts trivially.

For the remainder of this section, suppose that $\mathcal{H}_0$ can be chosen such that $\mathcal{H}_0 \not\subseteq \mathrm{Gal}(\mathrm{F}'/\mathrm{F}(\sqrt{-1}))$.

By the Chebotarev Density Theorem, take an odd prime $q$ such that its Frobenius in $\mathrm{Gal}(\mathrm{F}'/\mathbb{Q})$ is a generator of $\mathcal{H}_0$.

***Lemma 5.6*** *Let $\mathfrak{q}_i \ne \mathfrak{q}_j$ be two primes of* F *above $q$. Then $((\mathrm{F}'/\mathrm{F})/\mathfrak{q}_i) = ((\mathrm{F}'/\mathrm{F})/\mathfrak{q}_j)$.*

**Proof** The primes $\mathfrak{q}_i$ and $\mathfrak{q}_j$ are conjugate: there exists $g \in \mathcal{G}$ such that $\mathfrak{q}_j = \mathfrak{q}_i^g$. We are done thanks to the property of the Artin Symbol: $((\mathrm{F}'/\mathrm{F})/\mathfrak{q}_i^g) = g \cdot ((\mathrm{F}'/\mathrm{F})/\mathfrak{q}_i) \cdot g^{-1}$ and the fact that $\mathcal{G}$ acts trivially on $\mathcal{H}_0$. ■

Now by Theorem 5.5, for all pairs of primes $\mathfrak{q}_i \ne \mathfrak{q}_j$ of F above $q$, there exists a cylic 2-extension exactly $\{\mathfrak{q}_i, \mathfrak{q}_j\}$-ramified. Then, this implies that the 2-rank of the 2-class group $\mathrm{A}_S(\mathrm{K})$ is at least 15, where $S$ is the set of places of K above $q$. Moreover, by the condition above $q$, one has that $-1$ is not a square in $\mathbb{Q}_q$, which means that $q \equiv 3 \bmod 4$. We now put $\mathrm{K} = \mathbb{Q}(\sqrt{-p_1p_2})$ and proceed exactly as before; the 2-rank of the ray class group of K with modulus $q\ell$ is at most 4 if $q$ is inert in K/$\mathbb{Q}$ or 5 if $q$ splits.

***Lemma 5.7*** *Here, $d_2\mathrm{A}_\Sigma(\mathrm{K}) \le 4$.*

**Proof** One has only to look at the case where $q$ splits in K/$\mathbb{Q}$. Let $\alpha \in \mathrm{K}$ be the square of the unique non-trivial class $C$ of $\mathrm{A}_\mathrm{K}$: $C^2 = (\alpha)$. Consider the morphism

$$\theta \colon \langle -1, \alpha \rangle \longmapsto \frac{\mathbb{F}_{\mathfrak{l}_1}^\times}{\mathbb{F}_{\mathfrak{l}_1}^{\times 2}} \times \frac{\mathbb{F}_{\mathfrak{l}_2}^\times}{\mathbb{F}_{\mathfrak{l}_2}^{\times 2}} \times \frac{\mathbb{F}_{\mathfrak{q}_1}^\times}{\mathbb{F}_{\mathfrak{q}_1}^{\times 2}} \times \frac{\mathbb{F}_{\mathfrak{q}_2}^\times}{\mathbb{F}_{\mathfrak{q}_2}^{\times 2}},$$

where $\mathfrak{l}_i$ and $\mathfrak{q}_i$ are the primes of K above $q\ell$ and where $\mathbb{F}_{\mathfrak{q}_i}$ (resp. $\mathbb{F}_{\mathfrak{l}_i}$) is the residue field of $\mathfrak{q}_i$ (resp. of $\mathfrak{l}_i$). Then one has the formula (see [26] or see [12]): $d_2\mathrm{A}_{\mathrm{K},\Sigma} =$

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

$d_2 \mathrm{A}_\mathrm{K} + |\Sigma| - d_2 \operatorname{Im}(\theta)$. Now as $q \equiv -1 \bmod 4$, the image of $\theta$ is at least of order 2, and then we are done. ■

Now consider the compositum $\mathrm{L} := \mathbb{Q}_\Sigma^T \mathrm{K}$. Thanks to Schreier's inequality and to Genus Theory, one has for all number fields $\mathrm{K}_n$ in L/K:

$$2[\mathrm{K}_n : \mathrm{K}] \leq d_2 \mathrm{A}_\Sigma(\mathrm{K}_n) - 1 \leq 3[\mathrm{K}_n : \mathrm{K}].$$

# 6 Invariant Factors in Pro-$p$-groups

For this section the main reference is [4]. We begin with a straightforward observation.

***Proposition 6.1*** *Let $\mathcal{G}$ be a torsion-free* FAb *pro-p-group. Let $(\mathcal{U})$ be a basis of open subgroups of $\mathcal{G}$. Then the sequence of the exponents $e(\mathcal{U}^{ab})$ of $\mathcal{U}^{ab}$ is not bounded.*

**Proof** Suppose that there exists an integer $k$ such that for all open subgroups $\mathcal{U}$, $e(\mathcal{U}^{ab}) \leq k$. Take $1 \neq x \in \mathcal{G}$. Then $\langle x^k \rangle \mathcal{U} \subset [\mathcal{U}, \mathcal{U}]$; that means,

$$\langle x^k \rangle = \bigcap_{\mathcal{U}} \langle x^k \rangle \mathcal{U} \subset \bigcap_{\mathcal{U}} [\mathcal{U}, \mathcal{U}] = \{1\}.$$

In other words, $x^k = 1$ and, as $\mathcal{G}$ is torsion-free, $x = 1$, which is a contradiction. ■

Our work in the previous sections on exponents of $p$-class groups leads us now to defining the following invariant for finitely generated *FAb* pro-$p$ groups.

***Definition 6.2*** Let $\mathcal{G}$ be a *FAb* pro-$p$-group of finite type. For any open subgroup $\mathcal{U}$ of $\mathcal{G}$, since $\mathcal{U}^{\mathrm{ab}}$ is finite, $\mathbb{M}_{\mathcal{U}^{\mathrm{ab}}}$ is well defined. For $n \geq 1$, we put

$$\mathbb{M}_n(\mathcal{G}) := \min_{[\mathcal{G} : \mathcal{U}] = p^n} \mathbb{M}_{\mathcal{U}^{\mathrm{ab}}},$$

and then define the asymptotic mean exponent of $\mathcal{G}$ to be

$$\underline{\mathbb{M}}(\mathcal{G}) := \liminf_n \mathbb{M}_n(\mathcal{G}).$$

In the remainder of this section, we will show how to estimate the asymptotic mean exponent in two special cases.

## 6.1 In Analytic Pro-$p$-groups

As noted by Gärtner [11], the exponents of open subgroups of an infinite $p$-adic analytic pro-$p$-group tend to infinity. To be more precise, let $\mathcal{G}$ be an analytic pro-$p$-group of dimension $d$. Then $\mathcal{G}$ has an open uniform subgroup $\mathcal{U}$ (of rank $d$). Put $\mathcal{U}_1 = \mathcal{U}$ and consider for $i \geq 1$, $\mathcal{U}_{i+1} = \mathcal{U}_i^p [\mathcal{U}_i, \mathcal{U}]$ the $p$-central descending series of $\mathcal{U}$. (For $p = 2$, take $\mathcal{U}_{i+1} = \mathcal{U}_i^4 [\mathcal{U}_i, \mathcal{U}]$.)

***Definition 6.3*** A pro-$p$-group $\mathcal{U}$ is uniform if

(i) $\mathcal{U}/\mathcal{U}^p$ is abelian and

(ii) for all $i \geq 1$, the map

$$\begin{array}{ccc} \mathcal{U}_i/\mathcal{U}_{i+1} & \longrightarrow & \mathcal{U}_{i+1}/\mathcal{U}_{i+2} \\ x & \longmapsto & x^p \end{array}$$

is an isomorphism.

***Proposition 6.4*** *Let $p$ be an odd prime, and let $\mathcal{U}$ be a uniform pro-$p$-group. Then for each $n$, $\mathcal{U}_n^{\mathrm{ab}}$ has rank $d$ and maps onto $(\mathbb{Z}/p^n\mathbb{Z})^d$.*

**Proof** Take $n > 1$. Let $x \in \mathcal{U}_n$ be an element of a minimal family of generators of $\mathcal{U}_n$: the element $x$ is not trivial in the quotient $\mathcal{U}_n/\mathcal{U}_n^p[\mathcal{U}_n, \mathcal{U}]$. As $\mathcal{U}$ is uniform, one has $\mathcal{U}_n^p[\mathcal{U}_n, \mathcal{U}] = \mathcal{U}_{n+1}$ and then $x$ is not trivial in $\mathcal{U}_n/\mathcal{U}_{n+1}$. Suppose now that the order $p^k$ of $x$ in $\mathcal{U}_n/\mathcal{U}_{n+1}$ is smaller than $p^{n-1}$, *i.e.*, $x^{p^k} \in [\mathcal{U}_n, \mathcal{U}]$ with $k < n$. Then as $[\mathcal{U}_n, \mathcal{U}] \subset \mathcal{U}_{2n}$, one has $x^{p^k} \in \mathcal{U}_{2n}$. But as $\mathcal{U}$ is uniform, for all $m$ the following isomorphism holds:

$$\mathcal{U}_n/\mathcal{U}_{n+1} \xrightarrow{x \mapsto x^{p^m}} \mathcal{U}_{n+m}/\mathcal{U}_{n+m+1}.$$

The integer $k$ being supposed smaller than $n$, we find $x^{p^{n-1}} = 1$ in $\mathcal{U}_{2n-1}/\mathcal{U}_{2n}$ and then $x = 1$ in $\mathcal{U}_n/\mathcal{U}_{n+1}$, which is a contradiction. Hence, every element of a generator basis of $\mathcal{U}_n$ is of order at least $p^n$. ■

***Corollary 6.5*** *Let $\mathcal{G}$ be a uniform analytic pro-$p$-group of dimension $d$. Consider the sequence $\mathbb{M}_{\mathcal{G}_n^{\mathrm{ab}}}$ of mean exponents for the abelianizations of terms of the $p$-central series. We have*

$$\mathbb{M}_{\mathcal{G}_n^{\mathrm{ab}}} \geq n = \frac{1}{d} \log_p [\mathcal{G} : \mathcal{G}_n].$$

**Proof** This follows immediately from the previous Proposition. ■

***Remark 6.6*** ([4, Chapter 13]) Let us replace $\mathbb{Z}_p$ by the complete local regular Noetherien ring $R = \mathbb{Z}_p[[T_1, \dots, T_k]]$ with residue field $\mathbb{F}_p$ and dimension $k+1$; here $\mathfrak{m} = (p, T_1, \dots, T_k)$ is the maximal ideal of $R$. Let $\mathrm{Grad}(R) = \bigoplus_{i \geq 0} \mathfrak{m}^i/\mathfrak{m}^{i+1}$ be the graded algebra; put $c_i = \dim_{\mathbb{F}_p} \mathfrak{m}^i/\mathfrak{m}^{i+1}$. Following the terminology of [4], consider $\mathcal{G}$ an $R$ standard and perfect group of dimension $d$. For example $\mathrm{Sl}_n^1(R) := \ker(\mathrm{Sl}_n(R) \to \mathrm{Sl}_n(\mathbb{F}_p))$ is such a group for $p > 2$. In particular, $\mathcal{G} = \mathfrak{m}^d$ as an analytic variety on which there is a formal group law $F$. Let us consider the filtration of $\mathcal{G}$: $\mathcal{G}_n \simeq (\mathfrak{m}^n)^d$, $n \geq 1$. Then, for all integers $m, n \geq 1$, $[\mathcal{G}_m, \mathcal{G}_n] = \mathcal{G}_{m+n}$ ($\mathcal{G}$ is perfect) and there is an isomorphism of groups $\mathcal{G}_n^{ab} \simeq \left(\mathfrak{m}^n/\mathfrak{m}^{2n}\right)^d$, where the formal law on the quotient $\mathfrak{m}^n/\mathfrak{m}^{2n}$ becomes the addition. As the quotients $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ are $p$-elementary, one has

$$v_p\big([\mathcal{G} : \mathcal{G}_n]\big) = \log_p [R : \mathfrak{m}^n] = c_1 + c_2 + \cdots + c_{n-1}.$$

By using the Hilbert–Samuel–Serre polynomial $H = CX^{k+1} + \cdots$ of $\operatorname{Grad}(R)$, $C > 0$ (*i.e.*, $\deg(H) = k+1$), we have

$$\begin{aligned} v_p\big([\mathcal{G}:\mathcal{G}_n]\big) &\sim_n dH(n-1) \sim_n Cdn^{k+1}, \\ v_p\big(|\mathcal{G}_n^{ab}|\big) = v_p\big([\mathcal{G}_n:\mathcal{G}_{2n}]\big) &\sim_n d\big(H(2n-1) - H(n-1)\big) \\ &\sim_n cd(k+1)n^{k+1}(2^{k+1}-1). \end{aligned}$$

(For material for the Hilbert–Samuel–Serre polynomial; see, for example, [28].) To finish, we want to bound the $p$-rank $d_p\mathcal{G}_n$ of $\mathcal{G}_n$: $d_p\mathcal{G}_n = d \cdot d_p(\mathfrak{m}^n/(p\mathfrak{m}^n + \mathfrak{m}^{2n}))$. First, we have the exact sequence

$$0 \longrightarrow (p^{n-1}\mathfrak{m} + \cdots + p\mathfrak{m}^{n-1})/p\mathfrak{m}^n \longrightarrow \mathfrak{m}^n/(p\mathfrak{m}^n + \mathfrak{m}^{2n}) \longrightarrow \overline{\mathfrak{m}}^n/\overline{\mathfrak{m}}^{2n} \longrightarrow 0,$$

where $\overline{\mathfrak{m}}$ is the maximal ideal of $\mathbb{F}_p[[T_1, \dots, T_k]]$. Now the natural homomorphism

$$\begin{array}{ccc} \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \times \cdots \times \overline{\mathfrak{m}}^{n-1}/\overline{\mathfrak{m}}^n & \longrightarrow & p^{n-1}\mathfrak{m} + \cdots + p\mathfrak{m}^{n-1} \mod p\mathfrak{m}^n \\ (\overline{x}_1, \dots, \overline{x}_{n-1}) & \longmapsto & p^{n-1}x_1 + \cdots px_{n-1} \mod p\mathfrak{m}^n \end{array}$$

allows us to obtain

$$d_p\mathcal{G}_n \le a_1 + \cdots + a_{2n-1},$$

where $a_i = d_p\overline{\mathfrak{m}}^{i-1}/\overline{\mathfrak{m}}^i$. The local ring $\mathbb{F}_p[[T_1, \dots, T_k]]$ is of dimension $k$, and then, if $\overline{H} = C'X^k + \cdots$ is the Hilbert-Samuel of the graded algebra $\mathbb{F}_p[[T_1, \dots, T_k]]$ with $C' > 0$, we have for $n \gg 0$:

$$d_p\mathcal{G}_n \ll n^k.$$

Finally, one obtains

$$\mathbb{M}_{\mathcal{G}_n^{\mathrm{ab}}} \gg n \gg \big(\log_p[\mathcal{G}:\mathcal{G}_n]\big)^{1/(k+1)}.$$

## 6.2 Bounding $\underline{\mathbb{M}}(\mathcal{G}_S^T)$ for Tame $S$

First, thanks to Proposition 3.18, for the Galois group $\mathcal{G} = \mathcal{G}_S^T$ of a tame tower $\mathrm{K}_S^T/\mathrm{K}$, we have

$$\underline{\mathbb{M}}(\mathcal{G}) \le c(\mathrm{K}, S, T) \limsup_{\mathcal{U}} \frac{[\mathcal{G}:\mathcal{U}]}{d(\mathcal{U})},$$

where $c(\mathrm{K}, S, T)$ is a quantity that depends only on $\mathrm{K}, S, T$. So, we must consider the rate of growth of the generator rank of open subgroups of $\mathcal{G}$ with respect to their index. Recall that the *rank gradient* of $\mathcal{G}$ (see, for example, [5]) is defined to be

$$\rho(\mathcal{G}) = \liminf_{\mathcal{H}} \frac{d(\mathcal{H}) - 1}{[\mathcal{G}:\mathcal{H}]},$$

where the infimum is taken over all open subgroups $\mathcal{H} \subset \mathcal{G}$. Note that when $\mathcal{U} \subset \mathcal{V}$, Schreier's formula gives the inequality

$$\frac{d(\mathcal{U}) - 1}{[\mathcal{G}:\mathcal{U}]} \le \frac{d(\mathcal{V}) - 1}{[\mathcal{G}:\mathcal{V}]}$$

showing that the sequence $[\mathcal{G}:\mathcal{U}_i]/d(\mathcal{U}_i)$ is increasing for a nested sequence $(\mathcal{U}_i)$ of open subgroups. For groups with positive rank gradient $\varepsilon$, the $p$-rank of open subgroups grows $\varepsilon$-linearly with the index (compare Definition 3.19).

In the general case, lacking any knowledge of the behavior of $d(\mathcal{U})$, we nonetheless have the following result (Theorem 1.1(i)).

***Proposition 6.7*** *Suppose $S$ is a finite set of primes of a number field $\mathrm{K}$ with $(S,p)=1$. Let $\mathcal{G}=\mathcal{G}_S^T$. There is a constant $C>0$ such that for any open subgroup $\mathcal{U}$ of $\mathcal{G}$, we have $\mathbb{M}_{\mathcal{U}^{\mathrm{ab}}}\leq C[\mathcal{G}:\mathcal{U}]$.*

**Proof** We simply apply Proposition 3.18, merely noting that $d(\mathcal{U})\geq 1$. ■

***Question 6.8*** Is the conclusion of Proposition 6.7 true for every *FAb* pro-$p$-group of finite type?

In the main result of this section, for certain special subgroups $\mathcal{U}$ of $\mathcal{G}$, we give lower bounds for $d(\mathcal{U})$, which allows us to estimate $\mathbb{M}_{\mathcal{U}^{\mathrm{ab}}}$. The main references are[4, §11 and §12].

First of all, a key result is a theorem of Jennings, which asserts that for any group $\mathcal{G}$ there exists a connection between the enveloping algebra associated with a certain graduated algebra $\mathrm{Grad}(\mathcal{G})$ of $\mathcal{G}$ and the restricted enveloping algebra of $\mathbb{F}_p[\mathcal{G}]$ graded by the powers of the augmentation ideal $I$. Here, $\mathrm{Grad}(\mathcal{G}):=\oplus_{i\geq 0}D_i/D_{i+1}$, where $D_i=(1+I^i)\cap\mathcal{G}$; put $b_i:=d_pD_i/D_{i+1}$. The filtration $(D_n)$ is called the *Zassenhaus filtration* of $\mathcal{G}$; this filtration satisfies these mains properties:

$$D_1=\mathcal{G},\quad D_n=D_{n^*}^p\prod_{i+j=n}[D_i,D_j],\quad D_n^p\subset D_{np},\quad\text{and }\ [D_n,D_m]\subset D_{n+m},$$

where $n^*=\lceil n/p\rceil$. Hence, $D_i/D_{i+1}\simeq(\mathbb{Z}/p\mathbb{Z})^{b_i}$.

The relationship between these two associative algebras gives a link between the $b_i$ and the $c_j:=d_pI^j/I^{j+1}$. More precisely, if $U(T):=\sum_{n\geq 0}c_nT^n$ is the Hilbert Poincaré series of the graded algebra $\mathbb{F}_p[[\mathcal{G}]]$, then

$$U(T)=\prod_{i\geq 1}\Big(\frac{T^{pi}-1}{T^i-1}\Big)^{b_i}.$$

In particular, when $\mathcal{G}$ is analytic, the $p$-rank of its open subgroups is bounded and then, the integers $b_i$ should often vanish. In fact, one has the spectacular result that $b_i=0$ for a single integer $i$ if and only if the pro-$p$-group is analytic. The following beautiful lemma is a consequence of all of this.

***Lemma 6.9*** *Suppose $\varepsilon>0$. If $\mathcal{G}$ is not analytic, then there exist infinitely many $n$ such that*

$$d_pD_{2^n}\geq(1-\varepsilon)\log_p[\mathcal{G}:D_{2^n}],$$

*where $D_{2^n}$ runs in the Zassenhaus filtration $(D_k)$ of $\mathcal{G}$.*

**Proof** This is [4, lemma 11.8]. ■

***Definition 6.10*** A finitely generated pro-$p$ group $\mathcal{G}$ is said to be of *Golod–Shafarevich type* if all the relations are of degree 2 and $d^2\geq 4r$ where $d,r$ are the generator rank and relation rank of $\mathcal{G}$, respectively, (*cf.* Theorem 2.3).

***Remark 6.11*** A pro-$p$-group of Golod–Shafarevich type with relation rank $r > 1$ is not analytic, (*cf.* [24, 37]). If a pro-$p$ group is mild with respect to the Zassenhaus filtration, and all its relations are of degree 2, then it is of Golod–Shafarevich type (and of cohomological dimension 2); see [21].

***Proposition 6.12*** *Suppose that the conditions of Theorem 2.6 hold for a number field* K*, so that $\mathcal{G} = \mathcal{G}_{\varnothing}^{T}$ is infinite. Then there exists a constant $C$ and infinitely many $n$ such that*

$$\mathbb{M}_{D_{2^n}^{\mathrm{ab}}} \leq C \frac{[\mathcal{G}:D_{2^n}]}{\log_p [\mathcal{G}:D_{2^n}]},$$

*where $D_{2^n}$ runs in the Zassenhaus filtration $(D_k)$ of $\mathcal{G}$.*

**Proof** The conditions of Theorem 2.6 entail that $\mathcal{G}$ is of Golod–Shafarevich type, and hence is not analytic. The desired conclusion is therefore a consequence of Lemma 6.9 and Proposition 3.18. ■

To finish, let us improve the lower bound of Lemma 6.9. To simplify, assume that $p > 2$.

Let

$$1 \longrightarrow R \longrightarrow F \longrightarrow \mathcal{G} \longrightarrow 1,$$

be a minimal presentation of $\mathcal{G}$: the pro-$p$-group $F$ is free and generated by $d$ elements $x_1, \ldots, x_d$. We assume that $\mathcal{G}$ is finitely presented: the dimension over $\mathbb{F}_p$ of $H^2(\mathcal{G}, \mathbb{F}_p)$ is finite. Let $\rho_1, \ldots, \rho_r \in F$ be a system of generators of $R/R^p[F, R]$. For $i = 1, \ldots, r$, let $a_i$ be the degree of $\rho_i$ following the Zassenhaus filtration of $F$.

***Definition 6.13*** For two formal series with real coefficients, we say that $\sum_n \alpha_n T^n \geq \sum_n \alpha'_n T^n$ if for all $n$, $\alpha_n \geq \alpha'_n$.

***Proposition 6.14*** *Let $\mathcal{G}$ be a finitely presented pro-p-group. Let $U(t)$ be the Hilbert Poincaré series of the graded algebra $\mathbb{F}_p[[\mathcal{G}]]$. Then*

$$U(T) \geq \frac{1}{1 - dT + \sum_{i=1}^{r} T^{a_i}},$$

*with equality if $\mathcal{G}$ is of cohomological dimension at most* 2.

**Proof** The proof is essentially a result of Brumer [1]. First let us consider the natural short exact sequence

$$0 \longrightarrow \mathrm{I}(\mathcal{G}) \longrightarrow \mathbb{F}_p[[\mathcal{G}]] \longrightarrow \mathbb{F}_p \longrightarrow 0,$$

where $\mathrm{I}(\mathcal{G})$ is the augmentation ideal of the complete algebra $\mathbb{F}_p[[\mathcal{G}]]$. The topological generators of $\mathcal{G}$ are in $\mathrm{I}(\mathcal{G})$ and therefore all of degree 1. For a minimal presentation

$$1 \longrightarrow R \longrightarrow F \longrightarrow \mathcal{G} \longrightarrow 1,$$

of $\mathcal{G}$, Brumer (see [1, (5.2.1)]) shows that there is a short exact sequence

$$0 \longrightarrow R/R^p[R,R] \xrightarrow{f} \mathrm{I}(F)/\mathrm{I}(F)\mathrm{I}(R) \xrightarrow{g} \mathrm{I}(\mathcal{G}) \longrightarrow 0,$$

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

where $f(r) = r-1 \bmod \mathrm{I}(F)\mathrm{I}(R)$. Now, the quotient $\mathrm{I}(F)/\mathrm{I}(F)\mathrm{I}(R)$ is a free $\mathbb{F}_p[[\mathcal{G}]]$-module on the generators $x_1-1,\dots,x_d-1$, and then we have the following relation on the Hilbert Poincaré series:

$$P(T) - dTU(T) + U(T) - 1 = 0,$$

where $P(T)$ is the series of $R/R^p[R,R]$ and where $U(T)$ is the series of $\mathbb{F}_p[[\mathcal{G}]]$. As

$$\mathbb{F}_p[[\mathcal{G}]]\cdot\rho_1 \oplus \cdots \oplus \mathbb{F}_p[[\mathcal{G}]]\cdot\rho_r \overset{\varphi}{\twoheadrightarrow} R/R^p[R,R],$$

and since the elements $\rho_i$ are of degree $a_i$, one has

$$P(T) \le \Big(\sum_{i=1}^{r} T^{a_i}\Big)U(T).$$

Now, the equality comes from the fact that the pro-$p$-group $\mathcal{G}$ is of cohomological dimension at most 2 if and only if the map $\varphi$ is an isomorphism (see [1, Proposition 5.3]). ■

***Theorem 6.15*** *Let* L/K *be a tamely ramified pro-*$p$*-extension with Galois group* $\mathcal{G}$*. Suppose that* $\mathcal{G}$ *is of Golod–Shafarevich type and of cohomological dimension* 2*. Then for every* $\varepsilon>0$*, there exists a constant* $C$ *and infinitely many* $n$ *such that*

$$\mathbb{M}_{D_{2^n}^{\mathrm{ab}}} \le C\frac{[\mathcal{G}:D_{2^n}]}{(\log_p[\mathcal{G}:D_{2^n}])^{2-\varepsilon}},$$

*where* $D_{2^n}$ *runs in the Zassenhaus filtration* $(D_k)$ *of* $\mathcal{G}$*.*

***Remark 6.16*** In the inequality of the previous theorem, the constant depends on $\varepsilon$ and on the set of primes ramifying in L/K. We note that Labute ([21, Theorem 1.6]) was the first to give a sufficient condition for mildness of $\mathcal{G}_S^T$; thanks to the work of Schmidt [36], for any K, by choosing $S$ large enough, one can arrange that the group $\mathcal{G}_S^T$ is of cohomological dimension 2 and mild, and hence meets the conditions of the Theorem 6.15. (See also the work of Labute [21], Labute and Mináč [22], Forré [8], Gärtner [10], Vogel [40], etc.) We wish to highlight the fact that the preceding theorem combines some results from analytic number theory (Brauer–Siegel), arithmetic (the results of Schmidt and the fact that the root discriminant is bounded), and group theory! In fact, better bounds for the growth of $p$-rank of open subgroups of Golod–Shafarevich pro-$p$ groups can be found in the literature [5, 6], but the interest of Theorem 6.15 is the arithmetic flavor of the proof.

**Proof** We want to give a lower bound of $d_pD_{2^n}$. First, as $[D_{2^n},D_{2^n}] \subset D_{2^{n+1}}$, we should have in mind the fact that $d_pD_{2^n} \ge d_pD_{2^n}/D_{2^{n+1}}$.

Now by hypothesis,

$$\prod_{i\ge1}\Big(\frac{T^{p^i}-1}{T^i-1}\Big)^{b_i} = \frac{1}{1-dT+rT^2} = \frac{1}{(1-\alpha T)(1-\beta T)},$$

with $\alpha \ge \beta$, $\alpha \ge 2$, and $\beta > 1$. Indeed, as $\mathcal{G}^{ab}$ is finite, $r \ge d$.

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

By taking logarithms, one obtains

$$\sum_{i\geq 1} b_i \sum_{k\geq 1} \frac{1}{k}(T^{ki} - T^{pki}) = \sum_{i\geq 1} \frac{1}{i}(\alpha^i + \beta^i)T^i.$$

Take $m$ with $(m,p) = 1$. Then by looking the coefficients at $T^m$,

$$\alpha^m + \beta^m = \sum_{i|m} ib_i.$$

This equality at $m = 2^n$ and at $m = 2^{n-1}$ allows us to give

$$b_{2^n} = 2^{-n}\big(\alpha^{2^n} - \sqrt{\alpha^{2^n}} + \beta^{2^n} - \sqrt{\beta^{2^n}},\big)$$

and then there is a constant $C > 1$ such that for all large enough $n$, we have

$$b_{2^n} \geq C\frac{\alpha^{2^n}}{2^n}.$$

Let us conserve the notation of [4] and put $i_n = \log_p[\mathcal{G}:D_{2^n}]$. As

$$d_p D_{2^n} \geq d_p D_{2^n}/D_{2^{n+1}} = \log_p |D_{2^n}/D_{2^{n+1}}|,$$

one has the inequality $i_{n+1} \leq d_n + i_n$, where $d_n = d_p D_{2^n}$. Now, for $n \gg 0$,

$$\begin{aligned} i_{n+1} &= \log_p[\mathcal{G}:D_{2^{n+1}}] = \log_p[\mathcal{G}:D_{2^n}] + \log_p[D_{2^n}:D_{2^n+1}] + \log_p[D_{2^n+1}:D_{2^{n+1}}] \\ &\geq b_{2^n} \geq C\frac{\alpha^{2^n}}{2^n}. \end{aligned}$$

Let $n_0$ be an integer. Suppose that for all $n \geq n_0$, $d_n \leq i_n^{2-\varepsilon}$. Then $i_{n+1} \leq 2i_n^{2-\varepsilon}$ and by induction,

$$i_{n+1} \leq 2^{1+(2-\varepsilon)+\cdots+(2-\varepsilon)^{n-n_0}}\, i_{n_0}^{(2-\varepsilon)^{n+1-n_0}}.$$

Hence, for $n \gg n_0$,

$$C\frac{\alpha^{2^n}}{2^n} \leq i_{n+1} \leq 2^{\frac{(2-\varepsilon)^{n+1-n_0}-1}{1-\varepsilon}}\, i_{n_0}^{(2-\varepsilon)^{n+1-n_0}},$$

which is a contradiction for large $n$.

Hence, there exist infinitely many $n$ such that $d_p D_{2^n} \geq (\log_p[\mathcal{G}:D_{2^n}])^{2-\varepsilon}$ and if $\mathcal{G}$ is the Galois group of a tamely ramified tower,

$$\mathbb{M}_{D_{2^n}^{\mathrm{ab}}} \ll \frac{[\mathcal{G}:D_{2^n}]}{(\log_p[\mathcal{G}:D_{2^n}])^{2-\varepsilon}}. \qquad \blacksquare$$

*Remark 6.17* Calculations of the above type with Poincaré series can be found, for example, in [29, 30].

# 7 Final Remarks

## 7.1 On a Question of Structure

We have been looking for towers in which the $p$-rank of class groups has linear growth. In the Iwasawa context, abelian as well as non-abelian (for the latter, see, for example, [34]), there is an underlying algebraic structure thanks to which the linear growth

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

of the rank corresponds exactly to having positive $\mu$-invariant. Can we detect any evidence of a similar algebraic structure in the tame case?

In this paper we produce our examples as follows. First, we consider an infinite extension $\mathrm{k}_S^T/\mathrm{k}$ with $T$ non-trivial, and then take its compositum with a finite $p$-extension $\mathrm{K}/\mathrm{k}$ inside $\mathrm{k}_T$. In this manner, one obtains a subextension $\mathrm{L} := \mathrm{K}\mathrm{k}_S^T$ of $\mathrm{k}_{\{S\cup T\}}^{\varnothing}$. It is in the extension $\mathrm{L}/\mathrm{K}$ that we can force linear growth of the $p$-class groups $(\mathrm{A}_n)_n$. Put $\mathcal{G} = \mathrm{Gal}(\mathrm{k}_S^T/\mathrm{k}) \simeq \mathrm{Gal}(\mathrm{L}/\mathrm{K})$. By a result of Schmidt [36], by choosing $S$ large enough, one can assume that the group $\mathcal{G}$ is of cohomological dimension 2 and mild. Let $\Lambda := \mathbb{F}_p[[\mathcal{G}]]$ be the Iwasawa algebra associated with $\mathcal{G}$. As $\mathcal{G}$ is mild, the ring $\Lambda$ is without zero divisor, but note that it is probably not Noetherian. Let $\mathrm{X} := \lim_{\leftarrow_n} \mathrm{A}_n$ be the projective limit of the studied arithmetic object $\mathrm{A}_n$. The limit X is a finitely generated $\Lambda$-module ([27]).

***Question 7.1*** Is the linear growth of $A_n$ produced by this method related to a natural algebraic structure of “Iwasawa module” X ?

## 7.2 How Small Can the Mean Exponent be in Tame Towers?

We have shown that there exist asymptotically good infinite towers in which the mean exponent is bounded above. On one hand, it is natural to ask the following question.

***Question 7.2*** Can we find asymptotically good pro-$p$ towers $\mathcal{L}$ for which $\underline{\mathbb{M}}(\mathcal{L})$ is arbitrarily close to 1?

On the other hand, our constructions are rather special, so we have the following question.

***Question 7.3*** Are there asymptotically good infinite pro-$p$ towers in which the mean exponent of $p$-class groups is not bounded?

As a start on Question 7.2, we note that in Section 4, we have developed some examples of the following type:

$$\mathrm{K} = \mathbb{Q}(\sqrt{p_1\cdots p_t}, \sqrt{-p_{t+1}\cdots p_{t+s}}).$$

Here, $\mathrm{k}^T/\mathrm{k}$ is infinite where $\mathrm{k} = \mathbb{Q}(\sqrt{p_1\cdots p_t})$ and $T = \{p_{t+1},\dots,p_{t+s}\}$. These examples give $s$-linear growth for $p$-class groups where the base field K has genus $g \approx \log(p_1\cdots p_t p_{t+1}\cdots p_{t+s})$. Letting $n = t+s$, we note that as $n$ becomes large, one has $g \lesssim p_n$, where $p_n$ is, in the optimal case, the $n$-th prime number, *i.e.*, $g \sim n\log(n)$. But on the other side, to force the infinitude of $\mathrm{k}^T/\mathrm{k}$, which we need, we must apply Corollary 2.7, which requires $s \sim n$. Thus, the best we can expect via this method for bounding $\underline{\mathbb{M}}(\mathrm{K}_{\varnothing}^{\varnothing}/\mathrm{K})$ is only $\underline{\mathbb{M}}(\mathrm{K}_{\varnothing}^{\varnothing}/\mathrm{K}) \lesssim \log(n)$.

***Question 7.4*** What is the biquadratic field (following the above method) with the smallest upper bound on the value of $\underline{\mathbb{M}}(\mathrm{K}_{\varnothing}^{\varnothing}/\mathrm{K})$?

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

### 7.3 Concluding Summary

In this paper, we have introduced the logarithmic mean exponent of a finite abelian $p$-group as an invariant that balances the cardinality of the group against its rank, and studied its behavior in the context of $p$-class groups of number fields varying in towers with restricted ramification. By a mixture of results from algebraic and analytic number theory, we have constructed tame towers for which the mean exponent is bounded, and shown that, by contrast, the mean exponent for some open subgroups of $p$-adic analytic groups tend to infinity. We hope that further study of the mean exponent will shed light on properties that distinguish Galois groups of tame versus wild extensions.

**Acknowledgements** The second author would like to thank UMass Amherst for its hospitality during several visits, as well as the Région Franche-Comté for making his travel possible. He also thanks NTU Singapore for providing a stimulating research atmosphere on a visit there. The authors are grateful to Ján Mináč for interesting discussions and encouragements. They also want to thank the anonymous referee for the careful reading of the paper and for her/his comments.

## References

[1] A. Brumer, *Pseudocompact algebras, profinite groups and class formations.* J. Algebra **4**(1966), 442–470. http://dx.doi.org/10.1016/0021-8693(66)90034-2

[2] J. W. S. Cassels and A. Fröhlich [eds], *Algebraic number theory.* Proceedings of the instructional conference held at the University of Sussex, Brighton, September 1–17, 1965, Academic Press, New York, 1967.

[3] J. Coates, P. Schneider, and R. Sujatha, *Modules over Iwasawa algebras*. J. Inst. Math. Jussieu **2**(2003), no. 1, 73–108. http://dx.doi.org/10.1017/S1474748003000045

[4] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p-groups*. Cambridge Studies in Advanced Mathematics, 61, Cambridge University Press, Cambridge, 1999. http://dx.doi.org/10.1017/CBO9780511470882

[5] M. Ershov, *Golod-Shafarevich groups: a survey*. Internat. J. Algebra Comput. **22**(2012), no. 5, 1230001. http://dx.doi.org/10.1142/S0218196712300010

[6] ———, *Kazhdan quotients of Golod-Shafarevich groups*. Proc. Lond. Math. Soc. **102**(2011), no. 4, 599–636. http://dx.doi.org/10.1112/plms/pdq022

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

[8] P. Forré, *Strongly free sequences and pro-p-groups of cohomological dimension* 2. J. reine angew. Math. **658**(2011), 173–192. http://dx.doi.org/10.1515/CRELLE.2011.067

[9] E. Friedman, *Analytic formulas for the regulator of a number field*. Invent. Math. **98**(1989), no. 3, 599–622. http://dx.doi.org/10.1007/BF01393839

[10] J. Gärtner, *Mild pro-p-groups with trivial cup-product*. PhD thesis, University of Heidelberg, 2011.

[11] ———, *On p-class groups and the Fontaine-Mazur conjecture*. Math. Res. Lett. **21**(2014), 469–477. http://dx.doi.org/10.4310/MRL.2014.v21.n3.a5

[12] G. Gras, *Class field theory.* Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003. http://dx.doi.org/10.1007/978-3-662-11323-3

[13] G. Gras and A. Munnier, *Extensions cycliques T-totalement ramifiées*. Publ. Math. UFR Sci. Tech. Besançon, 1999.

[14] F. Hajir, *On the growth of p-class groups in p-class field towers.* J. Algebra **188**(1997), no. 1, 256–271. http://dx.doi.org/10.1006/jabr.1996.6849

[15] F. Hajir and C. Maire, *Tamely ramified towers and discriminant bounds for number fields*. Compositio Math. **128**(2001), no. 1, 35–53. http://dx.doi.org/10.1023/A:1017537415688

[16] ———, *Extensions of number fields with bounded ramification of bounded depth*. Int. Math. Res. Not. **13**(2002), 677–696. http://dx.doi.org/10.1155/S1073792802106015

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press

[17] M. Harris, *p-adic representations arising from descent on abelian varieties*. Compositio Math. **39**(1979), no. 2, 177–245; with correction: Compositio Math. **121**(2000), 105–108. http://dx.doi.org/10.1023/A:1001730616194

[18] Y. Ihara, *How many primes decompose completely in an infinite unramified Galois extension of a global field?*. J. Math. Soc. Japan **35**(1983), no. 4, 693–709. http://dx.doi.org/10.2969/jmsj/03540693

[19] K. Iwasawa, *On the $\mu$-invariants of $\mathbb{Z}_\ell$-extensions*. In: Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, Kinokuniya, Tokyo, 1973, pp. 1–11.

[20] H. Koch, *Galoissche Theorie der p-Erweiterungen*. Springer-Verlag, Berlin-New York, 1970.

[21] J. Labute, *Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$*. J. Reine Angew. Math. **596**(2006), 155–182. http://dx.doi.org/10.1515/CRELLE.2006.058

[22] J. Labute and J. Mináč, *Mild pro-2-groups and 2-extensions of $\mathbb{Q}$ with restricted ramification*. J. Algebra **332**(2011), 136–158. http://dx.doi.org/10.1016/j.jalgebra.2011.01.019

[23] S. Lang, *Algebraic number theory.* Second ed., Graduate Texts in Mathematics, 110, Springer-Verlag, New York, 1994 http://dx.doi.org/10.1007/978-1-4612-0853-2

[24] M. Lazard, *Groupes analytiques p-adiques*. Inst. Hautes Études Sci. Publ. Math. **26**(1965), 389–603.

[25] C. Maire, *Finitude de tours et p-tours T-ramifiées modérées, S-décomposées*. J. Théor. Nombres Bordeaux **8**(1996), 47–73. http://dx.doi.org/10.1007/s00209-009-0652-2

[26] ———, *T-S- capitulation*. In: Théorie des nombres, Années 1994/95–1995/96, Publ. Math. Fac. Sci. Besançon, 1997.

[27] ———, *Sur la structure galoisienne de certaines pro-p-extensions de corps de nombres*. Math. Z. **267**(2011), no. 3–4, 887–913. http://dx.doi.org/10.1007/s00209-009-0652-2

[28] H. Matsumura, *Commutative ring theory.* Cambridge Studies in Advanced Mathematics, 8, Cambridge University Press, Cambridge, 1989.

[29] M. McLeman, *A Golod-Shafarevich equality and p-tower groups.* J. Number Theory **129**(2009), no. 11, 2808–2819. http://dx.doi.org/10.1016/j.jnt.2009.05.014

[30] J. Mináč, M. Rogelstad, and N. D. Tân, *Dimensions of Zassenhaus filtration subquotients of some pro-p-groups*. Israel J. Math. **212**(2016), 825–855. http://dx.doi.org/10.1007/s11856-016-1310-0

[31] J. Neukirch, *Algebraic number theory.* Grundlehren der Mathematischen Wissenschaften, 322, Springer-Verlag, Berlin, 1999. http://dx.doi.org/10.1007/978-3-662-03983-0

[32] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields,* Grundlehren der Mathematischen Wissenschaften, 323, Springer-Verlag, Berlin, 2008. http://dx.doi.org/10.1007/978-3-540-37889-1

[33] M. Ozaki, *Construction of maximal unramified p-extensions with prescribed Galois groups.* Invent. Math. **183**(2011), no. 3, 649–680. http://dx.doi.org/10.1007/s00222-010-0289-0

[34] G. Perbet, *Sur les invariants d'Iwasawa dans les extensions de Lie p-adiques.* Algebra Number Theory **5**(2011), no. 6, 819-848. http://dx.doi.org/10.2140/ant.2011.5.819

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

[36] A. Schmidt, *Über pro-p-fundamentalgruppen markierter arithmetischer kurven.* J. Reine Angew. Math. **640**(2010), 203–235. http://dx.doi.org/10.1515/CRELLE.2010.025

[37] J.-P. Serre, *Cohomologie galoisienne.* Lecture Notes in Mathematics, 5, Springer-Verlag, Berlin-New York, 1965.

[38] M. Tsfasman and S. Vladut, *Infinite global fields and the generalized Brauer-Siegel theorem*. Mosc. Math. J. 2(2002), no. 2, 329–402.

[39] O. Venjakob, *On the structure theory of the Iwasawa algebra of a p-adic Lie group*. J. Eur. Math. Soc. (JEMS) **4**(2002), 271–311. http://dx.doi.org/10.1007/s100970100038

[40] D. Vogel, *Massey products in the Galois cohomology of number fields*, PhD Heidelberg, 2004.

[41] L. C. Washington, *Introduction to cyclotomic fields.* Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1999. http://dx.doi.org/10.1007/978-1-4612-1934-7

[42] R. Zimmert, *Ideale kleiner Norm in Idealklasse une eine Regulatorabschätzung*. Invent. Math. **62**(1981), no. 3, 367–380. http://dx.doi.org/10.1007/BF01394249

*Department of Mathematics & Statistics, University of Massachusetts, Amherst MA 01003, USA*
*e-mail*: hajir@math.umass.edu

*Laboratoire de Mathématiques, Université Bourgogne Franche-Comté et CNRS (UMR 6623), 16 route de Gray, 25030 Besançon cédex, France*
*e-mail*: christian.maire@univ-fcomte.fr

https://doi.org/10.4153/CJM-2017-032-9 Published online by Cambridge University Press