Journal of Number Theory 129 (2009) 2808–2819

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

A Golod–Shafarevich equality and p-tower groups

Cam McLeman

900 State Street, Collins Science Center, Salem, OR 97304, USA

ARTICLE INFO

Article history:
Received 12 November 2008
Revised 1 May 2009
Available online 24 July 2009
Communicated by David Goss

ABSTRACT

Text. All current techniques for showing that a number field has an infinite p-class field tower depend on one of various forms of the Golod–Shafarevich inequality. Such techniques can also be used to restrict the types of p-groups which can occur as Galois groups of finite p-class field towers. In the case that the base field is a quadratic imaginary number field, the theory culminates in showing that a finite such group must be of one of three possible presentation types. By keeping track of the error terms arising in standard proofs of Golod–Shafarevich type inequalities, we prove a Golod–Shafarevich equality for analytic pro-p-groups. As an application, we further work of Skopin [V.A. Skopin, Certain finite groups. Modules and homology in group theory and Galois theory, Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) 31 (1973) 115–139 (in Russian)], showing that groups of the third of the three types mentioned above are necessarily tremendously large.

Video. For a video summary of this paper, please visit http://www.youtube.com/watch?v=13GudVNQUUI.

1. Introduction

All current techniques for showing that a number field has an infinite p-class field tower depend on one of various forms of the Golod–Shafarevich inequality, a purely group-theoretic result relating (among other invariants) the generator rank d and relation rank r of an analytic pro-p-group. Even relatively weak forms of the theorem (e.g., the famous inequality $r > \frac{d^2}{4}$) provide the first examples of fields with infinite p-class field towers. A much stronger form of the inequality due to Koch (see Remark 7) relates finer invariants describing a group's relation structure.

At the heart of the proofs of these stronger forms is the Fox differential calculus, which gives rise to a sequence of inequalities relating various invariants attached to a pro-p-group. Our first contribu-

E-mail address: cmcleman@willamette.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2009.05.014

tion is to introduce and analyze a new set of obstruction invariants, measuring the extent to which these inequalities fail to be equalities. In Section 3, we carry out a standard proof of the Golod–Shafarevich inequality, now with these obstruction invariants in place. In conjunction with a theorem of Jennings on dimension factors of p-groups, this gives our principal result, a new Golod–Shafarevich *equality* (Theorem 6). One immediate corollary (Corollary 8), stemming from lower bounds placed on the obstruction invariants, is a strict improvement of the stronger form of the Golod–Shafarevich inequality mentioned above. A principal benefit of Theorem 6 over similar results is that one can extract information about the *order* of the group in question. We take advantage of this in Section 4, where we apply the theorem to the Galois group of a p-class field tower over a quadratic imaginary number field. In this case, the relation structure for a critical class of such groups is of one of three relation types (see Theorem 9), the last of which is not known to occur for *any* finite p-group. Finally, we provide an application of Theorem 6, using it to put a rather large lower bound on the order of such a group.

2. Background

Let K be a number field, and p a prime number. Denote by $K^{(1)}$ the Hilbert p-class field of K, i.e., the maximal abelian p-extension of K which is unramified at all primes. Class field theory tells us that this is a finite Galois extension of K whose Galois group is isomorphic to the p-primary part of the ideal class group of K. Iterating this procedure constructs the p-class field tower over K:

$$K = K^{(0)} \subset K^{(1)} \subset K^{(2)} \subset K^{(3)} \subset \cdots,$$

where for $i \geqslant 0$, $K^{(i+1)}$ is the Hilbert p-class field of $K^{(i)}$. Let $K^{(\infty)}$ denote the union of the fields in the tower. An important question, open for most number fields, is whether or not K admits a finite extension with class number prime to p – a subtle arithmetic condition which arose, for example, in Kummer's work on the first case of Fermat's Last Theorem for regular primes. This embeddability condition is equivalent to the question of whether or not the p-class field tower over K stabilizes, i.e., whether or not there exists a positive integer $\ell := \ell_p(K)$ such that $K^{(\ell)} = K^{(\ell+1)} = K^{(\ell+2)} = \cdots$. We call the smallest such ℓ the *p-tower length* of K, and set $\ell = \infty$ if no such integer exists. Defining the *p-tower group over K* by $G_K^\infty := \mathrm{Gal}(K^{(\infty)}/K)$, the observation that each extension $K^{(i+1)}/K^{(i)}$ is finite implies that $\ell_p(K)$ is finite if and only if G_K^∞ is. We will thus turn our attention to studying the pro-p-groups G_K^∞, some of the "most mysterious objects in algebraic number theory" [17].

The study of such groups remains in the slightly paradoxical situation that while even the finiteness of G_K^∞ for a given K is difficult to decide, we have rather detailed information on other aspects of its structure. Namely, work of Shafarevich [13] calculates the generator and relation ranks

$$d := \dim_{\mathbb{F}_p} H^1\bigl(G_K^\infty, \mathbb{F}_p\bigr) \quad \text{and} \quad r := \dim_{\mathbb{F}_p} H^2\bigl(G_K^\infty, \mathbb{F}_p\bigr)$$

in terms of arithmetic information of K, and work of Koch [4], Venkov [6], and more recently Vogel [16], give information on the specific form of those relations. The standard, and essentially only, way of demonstrating a p-class field tower to be infinite is by combining these calculations with (one of various forms of) the Golod–Shafarevich inequality, which we turn to next.

Definition 1. Let G be a group and let $\mathbb{F}_p[G]$ be its group ring over $\mathbb{F}_p$. The augmentation map $\varepsilon : \mathbb{F}_p[G] \to \mathbb{F}_p$, given by $\varepsilon(\sum a_i g_i) = \sum a_i$, is a surjective homomorphism whose kernel I is called the *augmentation ideal* of $\mathbb{F}_p[G]$ (or just of G). The *n-th modular dimension subgroup* G_n of G (with respect to p) is

$$G_n = \bigl\{ g \in G \bigm| g - 1 \in I^n(G) \bigr\}.$$

The filtration $G = G_1 \supset G_2 \supset \cdots$ of G by its modular dimension subgroups is called the *Zassenhaus filtration* of G. One checks easily (e.g., [5, Theorem 7.12]) that if $g, h \in G_n$, then $[g,h] \in G_{n+1}$ and

$g^p \in G_{np} \subset G_{n+1}$, so that the quotients G_n/G_{n+1} are $\mathbb{F}_p$-vector spaces for all n. We define the (modular) *dimension factors* of G by $a_n(G) := \dim_{\mathbb{F}_p} G_n/G_{n+1}$.

If G is a d-generated, r-related pro-p-group, we call a presentation

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

minimal if F is a free pro-p-group on d generators and R is generated as a normal subgroup of F by r elements. The most commonly cited form of the Golod–Shafarevich inequality places the lower bound $r > \frac{d^2}{4}$ on the number of relations r required to force a d-generated pro-p-group finite. A more refined version observes that relations lying deeper in the Zassenhaus filtration contribute less to keeping a group finite, and hence more such relations would be required.

Theorem 2. *(See Koch [4].) Suppose $1 \to R \to F \to G \to 1$ is a minimal presentation for a pro-p-group G, and that $R \subset F_m$. If G is finite, then*

$$r > \frac{d^m(m-1)^{m-1}}{m^m}.$$

Remark 3. The bound $r > \frac{d^2}{4}$ now follows from the observation that one has $R \subset F_2$ for any minimal presentation.

The results referenced above combine with the Golod–Shafarevich equality to give a particularly strong answer in the case that the base field K is a quadratic imaginary number field. Let $d_p \operatorname{Cl}(K) := \dim_{\mathbb{F}_p} \operatorname{Cl}(K)/p$ be the p-rank of the class group of K. The calculation of Shafarevich [13, Theorem 1] gives that $r(G_K^\infty) = d(G_K^\infty) = d_p \operatorname{Cl}(K)$, and a result of Koch and Venkov [6, Theorem 2] uses the fact that G_K^∞ is a so-called Schur-σ group to conclude that $R \subset F_3$. The Golod–Shafarevich inequality gives in this case that

$$d > \frac{4d^3}{27}.$$

Since this inequality is violated for $d \geqslant 3$, we find that K has an infinite p-class field tower whenever the p-rank of $\operatorname{Cl}(K)$ is at least 3. Further, it is easy to show that if the p-rank of $\operatorname{Cl}(K)$ is less than or equal to one, then K has a finite p-class field tower. The only remaining case, where $d = r = 2$, will be discussed in Section 4, after we prove a stronger form of the Golod–Shafarevich result.

3. A Golod–Shafarevich equality

Our contribution to the theory will be to introduce and analyze a series of invariants (dubbed e_n below) that one can attach to a finitely-generated pro-p-group to find the source of the “inequality” in the Golod–Shafarevich inequality. These invariants, which admit an interpretation in terms of a non-commutative Jacobian map on formal power series, can be shown to supply a non-trivial error term, leading to a refinement of the inequality. As the beginning of the proof will closely follow that given by Koch in the appendix of [2], we will omit some details until the two proofs differ.

Let G be a d-generated pro-p-group, and consider a minimal presentation

$$1 \longrightarrow R \xrightarrow{\iota} F \xrightarrow{\phi} G \longrightarrow 1$$

of G as a pro-p-group. We choose lifts $\{\sigma_i\}_{i=1}^d$ to F of a minimal generating set for G, and go through an inductive procedure to choose a generating system of relations which is minimal with respect to the Zassenhaus filtration. Namely, define $R_0 = \emptyset$, and for $n \geqslant 1$, let $R_n = R_{n-1} \cup \{\rho_{n,1}, \ldots, \rho_{n,r_n}\}$ where the relations $\rho_{n,1}, \rho_{n,2}, \ldots, \rho_{n,r_n}$ are chosen so that they and R_{n-1} constitute a minimal system of generators for RF_{n+1}/F_{n+1}. In the process, we have also defined invariants r_k representing the number of relations of level k in a minimal presentation for G. Note that $\sum_{k=1}^{\infty} r_k = r$. The completed group ring $\mathbb{F}_p[[F]]$ is isomorphic to the ring $\mathbb{F}_p(d) := \mathbb{F}_p\{\{x_1, \ldots, x_d\}\}$ of formal power series in d non-commuting variables over $\mathbb{F}_p$, the isomorphism being the linear extension of the map sending σ_i to $1 + x_i$.

The map $\phi : F \to G$ above extends naturally to a surjection (which we also call ϕ)

$$\mathbb{F}_p[[F]] \xrightarrow{\phi} \mathbb{F}_p[[G]],$$

and we label the generators of $\mathbb{F}_p[[G]]$ by $\bar{x}_i = \phi(\sigma_i) - 1$, for $1 \leqslant i \leqslant d$. Letting f_i be the image of $(\rho_i - 1)$ under the identification $\mathbb{F}_p\{\{x_1, \ldots, x_d\}\} \approx \mathbb{F}_p[[F]]$, we have $\ker(\phi) = (f_1, \ldots, f_r)$, and so $\mathbb{F}_p[[G]] \cong \mathbb{F}_p\{\{x_1, \ldots, x_d\}\}/(f_1, \ldots, f_r)$. Let $I = (\bar{x}_1, \ldots, \bar{x}_d)$ denote the augmentation ideal of $\mathbb{F}_p[[G]]$, and define the *level* of an element $f \in \mathbb{F}_p[[G]]$ to be the maximal n such that $f \in I^n$.

The proof of the Golod–Shafarevich theorem centers around the exact sequence of $\mathbb{F}_p[[G]]$-modules

$$\bigoplus_{i=1}^{r} \mathbb{F}_p[[G]] \xrightarrow{J} \bigoplus_{i=1}^{d} \mathbb{F}_p[[G]] \xrightarrow{\psi} \mathbb{F}_p[[G]] \xrightarrow{\varepsilon} \mathbb{F}_p \longrightarrow 0,$$

where we define the three maps as follows:

- ε is the augmentation map, which translates under ϕ to the "evaluation at $(x_1, \ldots, x_d) = (0, \ldots, 0)$" map on power series.
- ψ is the linear map defined by

$$\psi(g_1, \ldots, g_d) = \sum_{i=1}^{d} g_i \bar{x}_i.$$

- To define J we introduce the *Fox partial derivative operators* $\frac{\partial f}{\partial x_j}$ for $f \in I \subset \mathbb{F}_p[[F]]$ by observing that if $f \in I$, then f has no constant term and hence, after collecting the monomials appearing in f according to their last factor, can be written uniquely in the form $f = \sum \frac{\partial f}{\partial x_j} x_j$. Now define J (a "non-commutative Jacobian") by

$$J(g_1, \ldots, g_r) := \left(\sum_{i=1}^{r} g_i \phi\left(\frac{\partial f_i}{\partial x_1}\right), \ldots, \sum_{i=1}^{r} g_i \phi\left(\frac{\partial f_i}{\partial x_d}\right) \right).$$

The sequence remains exact after taking quotients by suitable powers of the augmentation ideal, and we arrive at the exact sequences

$$0 \longrightarrow \ker(J_n) \longrightarrow \bigoplus_{i=1}^{r} \mathbb{F}_p[[G]]/I^{n-\nu(f_i)} \xrightarrow{J_n} \bigoplus_{i=1}^{d} \mathbb{F}_p[[G]]/I^{n-1} \xrightarrow{\psi_n} \mathbb{F}_p[[G]]/I^n \xrightarrow{\bar{\varepsilon}} \mathbb{F}_p \longrightarrow 0.$$

for each $n \geqslant 1$. Define

$$c_n := \dim_{\mathbb{F}_p} \mathbb{F}_p[[G]]/I^n, \qquad e_n := \dim_{\mathbb{F}_p} \ker J_n$$

and set $I^n = \mathbb{F}_p[[G]]$ for $n \leqslant 0$, so that $c_n = e_n = 0$ for $n \leqslant 0$. Finally, recall that r_i was the number of relations of level i for $i \geqslant 1$, and we set $r_0 = 1$ by convention. Taking the alternating sum of dimensions of the exact sequence above, and noting that

$$\dim_{\mathbb{F}_p}\left(\bigoplus_{i=1}^{r} \mathbb{F}_p[[G]]/I^{n-v(f_i)}\right) = \sum_{i=1}^{r} c_{n-v(f_i)} = \sum_{i=1}^{n} r_i c_{n-i},$$

gives the following key result:

Theorem 4 *(Golod–Shafarevich recursion relation). For a d-generated pro-p-group G, and with all other notation as in the above paragraph, we have*

$$\sum_{i=0}^{n} r_i c_{n-i} - d c_{n-1} = 1 + e_n$$

for all $n \geqslant 1$.

Before stating the Golod–Shafarevich equality, we recall the following theorem of Jennings which relates the dimension factors $a_n = \dim_{\mathbb{F}_p} G_n/G_{n+1}$ to the invariants $c_n = \dim_{\mathbb{F}_p} \mathbb{F}_p[[G]]/I^n$ defined above.

Theorem 5. *(See Jennings [3].) Let G be a finitely-generated pro-p-group, and define*

$$b_n := c_{n+1} - c_n = \dim_{\mathbb{F}_p} I^n/I^{n+1}, \qquad P_n(t) := \frac{1-t^n}{1-t^{np}}.$$

Then

$$\prod_{n=1}^{\infty} P_n(t)^{-a_n} = \sum_{n=1}^{\infty} b_n t^n.$$

Collecting all of the above provides us with our desired result.

Theorem 6 *(A Golod–Shafarevich equality). Let G be a d-generated analytic pro-p-group, and take all other notation as above. Then*

$$\sum_{k=2}^{\infty} r_k t^k - dt + 1 = \prod_{n=1}^{\infty} P_n(t)^{a_n} + \frac{\sum_{n=1}^{\infty} e_n t^n}{\sum_{n=1}^{\infty} c_n t^n}$$

for all $0 \leqslant t < 1$.

Proof. Since G is analytic, the power series $\sum c_n t^n$ converges absolutely on the unit interval [10], and since $e_n \leqslant r c_n$ by definition of the vector space whose dimension it measures, so does $\sum e_n t^n$. Absolute convergence now allows us to re-write

$$\left(\sum_{k=0}^{\infty} r_k t^k - dt\right)\left(\sum_{n=1}^{\infty} c_n t^n\right) = \sum_{n=1}^{\infty}\sum_{i=0}^{n}(r_i c_{n-i} - d c_{n-1}) t^n = \sum_{n=1}^{\infty}(1+e_n)t^n,$$

the second equality following from Theorem 4. Further, we have $r_0 = 1$ and $r_1 = 0$, and so we can re-write $\sum_{k=0}^{\infty} r_k t^k - dt = \sum_{k=2}^{\infty} r_k t^k - dt + 1$. Solving the previous equation for this quantity gives

$$\sum_{k=2}^{\infty} r_k t^k - dt + 1 = \frac{\sum_{n=1}^{\infty}(1+e_n)t^n}{\sum_{n=1}^{\infty} c_n t^n} = \frac{t}{(1-t)} \cdot \frac{1}{\sum_{n=1}^{\infty} c_n t^n} + \frac{\sum_{n=1}^{\infty} e_n t^n}{\sum_{n=1}^{\infty} c_n t^n},$$

and the result now follows from

$$\frac{t}{1-t} \cdot \frac{1}{\sum_{n=1}^{\infty} c_n t^n} = \frac{1}{\sum_{n=0}^{\infty} b_n t^n} = \prod_{n=1}^{\infty} P_n(t)^{a_n},$$

the last step being Theorem 5. $\square$

Remark 7. Koch's proof in the appendix of [2] gives $\sum r_k t^k - dt + 1 > 0$, which is obtained from the theorem above by noting that $e_n \geqslant 0$ for all n, and that $P_n(t) > 0$ for all $t \in (0,1)$. Either of these versions implies Theorem 2. One simply observes that the assumption that $R \subset F_m$ implies $r_k = 0$ for all $k < m$, and that the right-hand side of the equation in Theorem 6 is strictly positive, giving

$$\sum_{k=2}^{\infty} r_k t^k - dt + 1 = \sum_{k=m}^{\infty} r_k t^k - dt + 1 \geqslant r_m t^m - dt + 1 > 0.$$

This last inequality is violated at $t = (\frac{d}{mr})^{1/(m-1)}$ if $r \leqslant d^m \frac{(m-1)^{m-1}}{m^m}$.

For a finite p-group G, we have $I^n = 0$ for sufficiently large n [5, Lemma 7.9], and so

$$c_n = \dim_{\mathbb{F}_p} \mathbb{F}_p[G]/I^n = \dim_{\mathbb{F}_p} \mathbb{F}_p[G] = |G|$$

for all sufficiently large n. More explicitly, Jennings' theorem implies that b_n $(= c_{n+1} - c_n)$ is zero for all $n > N := (p-1)\sum n a_n$ (the degree of the polynomial $\prod P_n(t)^{-a_n}$), implying that the sequence $\{c_n\}$ stabilizes after c_N. The Golod–Shafarevich recursion relation

$$\sum_{i=0}^{n} r_i c_{n-i} - d c_{n-1} = 1 + e_n$$

in turn implies that $1 + e_n = (r + 1 - d)|G|$ for all sufficiently large n, and hence that the term $\frac{\sum e_n t^n}{\sum c_n t^n}$ appearing on the right-hand side of the Golod–Shafarevich equality is non-zero for any group with $r \geqslant d$ (e.g., finite groups). In the author's PhD thesis [11], this observation is used to give an improvement on the version of the Golod–Shafarevich inequality described in Remark 7:

Corollary 8. *Let G be a finite p-group, let $N = (p-1)\sum_{n=1}^{\infty} n a_n$, let m be the level of the deepest relation defining G, and take all other notation as in Theorem* 6. *Then*

$$\sum_{k=2}^{\infty} r_k t^k - dt + 1 > \prod_{n=1}^{\infty} P_n(t)^{a_n} + (1 - d + r)\left(1 - \frac{1}{|G|}\right) t^{N+m} > 0,$$

for all $0 \leqslant t < 1$.

4. Quadratic imaginary number fields

As discussed in the introduction, the problem of determining the finiteness of the p-tower group G_K^∞ is largely solved in the case that K is a quadratic imaginary number field and p is an odd prime. Namely, the problem is almost completely decided by $d(G)$, which is computable as the p-rank of the class group of K: If $d \leqslant 1$, G_K^∞ is finite, and if $d \geqslant 3$, G_K^∞ is infinite. We are thus left with the case of $d = r = 2$, and the Golod–Shafarevich equality (or Koch's form of the inequality given in Remark 7) yields further information in this case. Namely, since $e_n \geqslant 0$ and $P_n(t) > 0$ for all n and $t \in (0, 1)$, Theorem 6 gives for all $t \in (0, 1)$ the inequality

$$t^{m_1} + t^{m_2} - 2t + 1 > 0,$$

where $m_1 \leqslant m_2$ are the levels of the two relations in a minimal presentation of G. Further, we have that m_1 and m_2 are both odd (again by [6]) and greater than one (since $r_1 = 0$). It is now easily checked that there are only three choices for the pair (m_1, m_2) for which the inequality is not violated, i.e., three possible relation structures for G_K^∞ under the assumption that the group is finite.

Theorem 9 *(Koch–Venkov). If G is a finite 2-generated and 2-related p-group with relations in odd levels m_1 and m_2 with $m_1 \leqslant m_2$, then we have*

$$(m_1, m_2) \in \{(3, 3), (3, 5), (3, 7)\}.$$

Definition 10. For ease of reference, we will call a pro-p-group which satisfies the hypotheses of this theorem a *KV-group*, and call the pair (m_1, m_2) the *Zassenhaus type* (or just *Z-type*) of the group. By the discussion before the theorem, all finite non-cyclic p-tower groups are KV-groups, and so we will focus our attention on this class of groups.

The classification of Z-types for KV-groups provides hope for computationally showing a given p-tower group to be infinite, by showing that any relations defining it lie deeper than the third level. For example, the author [12] used work of Vogel [16] to show that the vanishing of certain traces of Massey products on the $\mathbb{F}_p$-cohomology of G_K^∞ implies the infinitude of the group. Before moving on, we pause to remark on the current state of knowledge on abstract pro-p-groups of these three Z-types (as always, with p odd):

- **Z-Type (3,3):** All known finite non-cyclic p-tower groups, dating back to the earliest examples from Scholz and Taussky [15], are of this Z-type. Recently, Bartholdi and Bush [1] constructed and analyzed an infinite series of 3-groups of Z-type $(3, 3)$ whose derived lengths tend to infinity, providing the first explicit candidates for p-tower KV-groups of length greater than two.
- **Z-Type (3,5):** Skopin [14] has found a family of finite examples of Z-type $(3, 5)$, and Koch and Venkov [6] were able to find some infinite examples (using a variant of the Golod–Shafarevich inequality). No group in either of these families has been shown to occur as a p-tower group.
- **Z-Type (3,7):** No finite p-groups of this Z-type are known. Skopin [14] has placed a lower bound on the size of a small family of such groups. We will expand the scope of this result in Theorem 17 by showing that *any* pro-p-group of this type must be particularly large.

Returning to Corollary 8 (and recalling the notation therein), we remark that since KV-groups are of one of only those three possible Z-types, we can take $m = 7$ for any such group. Further, since N depends only on p and the series $\{a_n(G)\}$, Corollary 8 gives a strict strengthening of the Golod–Shafarevich inequality without referring to any new invariants of the group beyond the dimension factors (one can replace the constant in front of t^{N+m} with $\frac{p-1}{p}$ so that no knowledge of the order of the group is required). Motivated by this observation, we will return to the implications of the Golod–Shafarevich equality to groups of Z-type $(3, 7)$ after extracting more detailed information about dimension factors of pro-p-groups.

4.1. Bounds on dimension factors

Of principal importance in determining dimension factors is the following theorem of Lazard giving an explicit description of the modular dimension subgroups G_n in terms of the lower central series (defined recursively by $\gamma_1(G)=G$, $\gamma_n(G)=[G,\gamma_{n-1}(G)]$).

Theorem 11. *(See Lazard [9].) For any group G and any prime p, the n-th dimension subgroup G_n of G is given by*

$$G_n=\prod_{ip^j\geqslant n}\gamma_i(G)^{p^j}.$$

As a simple consequence, since a surjection of groups $H\twoheadrightarrow K$ induces a surjection $\gamma_n(H)\twoheadrightarrow\gamma_n(K)$ for all n, we obtain the following as an immediate corollary of Lazard's theorem.

Corollary 12. *A surjection of groups $H\to K$ induces surjections*

$$H_n/H_{n+1}\longrightarrow\!\!\!\!\!\rightarrow K_n/K_{n+1}$$

for all $n\geqslant 1$. In particular, surjections $H\twoheadrightarrow G$ and $G\twoheadrightarrow K$ give the inequalities

$$a_n(H)\geqslant a_n(G)\geqslant a_n(K).$$

We will apply the corollary to bound various dimension factors of a KV-group G from both above and below. The lower bound is easiest:

Proposition 13. *Let G be a p-tower KV-group with abelianization of type (p^a,p^b) with $1\leqslant a\leqslant b$. Then*

$$a_n(G)\geqslant\begin{cases}2 & \text{if } n=p^c \text{ and } 0\leqslant c\leqslant a-1,\\ 1 & \text{if } n=p^c \text{ and } a\leqslant c\leqslant b-1.\end{cases}$$

Proof. We apply Corollary 12 to the surjection $G\to G^{ab}\approx\mathbb{Z}/p^a\mathbb{Z}\oplus\mathbb{Z}/p^b\mathbb{Z}$. For any abelian group H, we have $\gamma_i(H)=1$ for $i\geqslant 2$, and so the Lazard product formula for H_n reduces to

$$H_n=\prod_{p^j\geqslant n}\gamma_1(H)^{p^j}=H^{p^{\lfloor\log_p n\rfloor}}.$$

In particular $H_n=H_{n+1}$ unless n is a power of p, so only dimension factors with p-power indices p^c can be non-trivial. Applying this to $H=G^{\mathrm{ab}}\approx\mathbb{Z}/p^a\mathbb{Z}\oplus\mathbb{Z}/p^b\mathbb{Z}$, we have

$$a_{p^c}(G)\geqslant a_{p^c}\left(G^{ab}\right)=\dim_{\mathbb{F}_p}G^{\mathrm{ab}}_{p^c}/G^{\mathrm{ab}}_{p^c+1}=\dim_{\mathbb{F}_p}\left[\frac{p^c\mathbb{Z}/p^a\mathbb{Z}}{p^{c+1}\mathbb{Z}/p^a\mathbb{Z}}\oplus\frac{p^c\mathbb{Z}/p^b\mathbb{Z}}{p^{c+1}\mathbb{Z}/p^b\mathbb{Z}}\right].$$

The first factor is non-trivial only for $0\leqslant c\leqslant a-1$ and the second factor is non-trivial only for $0\leqslant c\leqslant b-1$, giving the result. $\square$

For an upper bound, we relate the dimension factors of a group G to the (more easily calculable) mod p quotients of its lower central factors. Define

$$g_n(G):=\dim_{\mathbb{F}_p}\frac{\gamma_n(G)}{\gamma_n(G)^p\gamma_{n+1}}.$$

The relation to the dimension factors is then given by

Lemma 14. *For any finitely-generated pro-p-group G, we have $a_n(G) \leqslant g_n(G)$ for all $n < p-1$.*

Proof. Write γ_i for $\gamma_i(G)$. It suffices to demonstrate a surjection of $\mathbb{F}_p$ vector spaces $\gamma_n/\gamma_n^p\gamma_{n+1} \to G_n/G_{n+1}$. The assumption that $p > n$ renders most of the terms in Lazard's product formula for G_n redundant. Namely, noting the inclusions $\gamma_i \leqslant \gamma_j$ for $i \geqslant j$ and $\gamma_i^{p^j} \leqslant \gamma_i^{p^k}$ for $j \geqslant k$, we claim that the product simplifies to

$$G_n = \prod_{ip^j \geqslant n} \gamma_i^{p^j} = G^p\gamma_n.$$

To see this, observe that any factor in the product must either have $i \geqslant n$, in which case that factor is contained in γ_n, or $j \geqslant 1$, in which case the factor is contained in $\gamma_1^p = G^p$. Similarly, since $p > n+1$, repeating the argument gives $G_{n+1} = G^p\gamma_{n+1}$. Now the kernel of the natural quotient map

$$\gamma_n \longrightarrow\!\!\!\!\!\rightarrow \frac{\gamma_n}{(G^p \cap \gamma_n)\gamma_{n+1}} \simeq \frac{G^p\gamma_n}{G^p\gamma_{n+1}} = \frac{G_n}{G_{n+1}}$$

clearly contains $\gamma_n^p\gamma_{n+1}$, giving the desired surjection. □

This result in hand, we now recall that any KV-group G admits a presentation $F/\langle\rho_1, \rho_2\rangle$ where ρ_1 is of level 3 with respect to the Zassenhaus filtration and ρ_2 is of level i for some $i \in \{3, 5, 7\}$. Regardless of the level of ρ_2, G is thus a quotient of the one-relator pro-p-group $\widetilde{G} := F/\langle\rho_1\rangle$ whose single relation lies in level 3. Such groups were studied extensively by Labute, especially in regard to their lower central series. Important to our upper bound will be his calculation of the lower central factors of a d-generated one-relator pro-p-group with one relation in level k [7]:

$$g_n(\widetilde{G}) = \frac{1}{n}\sum_{j|n} \mu\left(\frac{n}{j}\right)\left[\sum_{0 \leqslant i \leqslant \lfloor \frac{j}{k} \rfloor} (-1)^i \frac{j}{j+(1-k)i}\binom{j+(1-k)i}{i} d^{j-ki}\right],$$

where μ denotes the Moebius function. For a KV-group G, combining Corollary 12 (applied to the natural surjection $\widetilde{G} \to G$) and Lemma 14 gives the chain of inequalities $a_n(G) \leqslant a_n(\widetilde{G}) \leqslant g_n(\widetilde{G})$, proving the following proposition.

Proposition 15. *Let G be a KV-group. Then for $n < p - 11$ we have*

$$a_n(G) \leqslant \frac{1}{n}\sum_{j|n} \mu\left(\frac{n}{j}\right)\left[\sum_{0 \leqslant i \leqslant \lfloor \frac{j}{3} \rfloor} (-1)^i \frac{j}{j-2i}\binom{j-2i}{i} 2^{j-3i}\right].$$

For $p > 7$, this gives the following table of upper bounds for the first few dimension factors of a p-tower KV-group:

$n =$	1	2	3	4	5	6	7	8	9
$a_n \leqslant$	2	1	1	1	2	2	4	5	8

We can refine this slightly for groups of Z-type $(3, 7)$.

Lemma 16. *For $p > 7$ and a KV-group G of Z-type $(3, 7)$, we have $a_7(G) \leqslant 3$.*

Proof. Consider a minimal presentation $1 \to R \to F \to G \to 1$, and choose generators ρ_1, ρ_2 for R of respective levels 3 and 7. Let $\widetilde{G} = F/\langle \rho_1 \rangle$. We have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \langle \rho_1 \rangle / (\langle \rho_1 \rangle \cap F_8) \arrow[r] \arrow[d, hook] & F_7/F_8 \arrow[r] \arrow[d, equal] & \widetilde{G}_7/\widetilde{G}_8 \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & R/(R \cap F_8) \arrow[r] & F_7/F_8 \arrow[r] & G_7/G_8 \arrow[r] & 0
\end{tikzcd}$$

of finite-dimensional $\mathbb{F}_p$-vector spaces. By assumption that ρ_1 and ρ_2 form a minimal system of generators for $RF_8/F_8 \approx R/(R \cap F_8)$ (in particular, since $\rho_2 \notin \langle \rho_1 \rangle \cap F_8$), we have $\dim_{\mathbb{F}_p} R/(R \cap F_8) = \dim_{\mathbb{F}_p} \langle \rho_1 \rangle / (\langle \rho_1 \rangle \cap F_8) + 1$. This then gives $a_7(G) \leqslant a_7(\widetilde{G}) - 1 = 3$ by the previous proposition. $\square$

Finally, we return to the implications of the Golod–Shafarevich equality for p-tower of Z-type $(3, 7)$. A key motivation is that the polynomial $t^7 + t^3 - 2t + 1$ has a minimum value of about 0.02 on the unit interval, implying that the Golod–Shafarevich inequality *nearly* prohibits analytic groups of this Z-type from occurring. While the Golod–Shafarevich results do not rule out the existence of such groups, we instead obtain a rather large lower bound on their orders.

Theorem 17. *Let $p > 7$, and suppose G is a pro-p-group of Z-type $(3, 7)$ whose abelianization is of type (p^a, p^b) with $1 \leqslant a \leqslant b$. Then $|G| \geqslant p^{21+a+b} \geqslant p^{23}$.*

Proof. Using that $e_n \geqslant 0$ for all n, the Golod–Shafarevich equality implies that

$$t^7 + t^3 - 2t + 1 > \prod_{n=1}^{\infty} P_n(t)^{a_n}$$

for all $t \in (0, 1)$. We abbreviate $P_n(t)$ by P_n, and begin by breaking up the right-hand product (making use of Proposition 13 and that $a_1 = d = 2$ in the process):

$$\prod_{n=1}^{\infty} P_n^{a_n} = P_1^2 P_2^{a_2} \cdots P_9^{a_9} \cdot \prod_{c=1}^{a-1} P_{p^c}^2 \cdot \prod_{c=a}^{a+b-1} P_{p^c} \cdot {\prod}' P_n^{a_n}$$

where the primed product at the end consists of all terms not explicitly pulled out in one of the other displayed factors. (The reason for specifically pulling out the first nine terms will become clear by the end of the proof). The products with p-power indices now telescope to give

$$\begin{aligned}
\prod_{n=1}^{\infty} P_n^{a_n} &= \left(\frac{1-t}{1-t^p} \right)^2 P_2^{a_2} \cdots P_9^{a_9} \cdot \left(\frac{(1-t^p)^2}{(1-t^{p^a})(1-t^{p^b})} \right) \cdot {\prod}' P_n^{a_n} \\
&\geqslant (1-t)^2 \left(1-t^2\right)^{a_2} \cdots \left(1-t^9\right)^{a_9} {\prod}' \left(1-t^n\right)^{a_n}.
\end{aligned}$$

Since $|G| = p^{\sum a_n}$, we now search for the sequence $a_2, a_3, \ldots$ of dimension factors which gives the smallest value of $A := \sum a_n$ subject to this last inequality and whose terms satisfy the constraints of Proposition 15 and Lemma 16. Since $(1 - t^m) \geqslant (1 - t^n)$ on the unit interval whenever $m \geqslant n$, we note that of all the sequences which sum to A, the one with the smallest value of $\prod (1 - t^n)^{a_n}$ is the one with $a_1 = A$, $a_i = 0$ for $i \geqslant 2$. Elementary calculus or a graphing calculator shows that for $A = 2$, the inequality $t^7 + t^3 - 2t + 1 > (1 - t)^2$ is violated at $t = 0.5$. Thus we must have $A > 2$, but now the restriction that $a_1 \leqslant 2$ implies that the minimal possible solution occurs when $a_1 = 2$,

$a_2 = A - 2$. A similar argument rules out $A = 3$, and since $a_2 \leqslant 1$, the minimal solution must have a_3 also non-trivial. We now repeat, incrementing the next smallest dimension factor until either the Golod–Shafarevich equality is satisfied, or we reach the upper bound on that factor prescribed by Proposition 15 or Lemma 16. The process terminates after incrementing a_9 to 6, which one can verify by calculating that

$$t^7 + t^3 - 2t + 1 > (1-t)^2\left(1-t^2\right)\left(1-t^3\right)\left(1-t^4\right)\left(1-t^5\right)^2\left(1-t^6\right)^2\left(1-t^7\right)^3\left(1-t^8\right)^5\left(1-t^9\right)^5$$

is violated for $t = 0.55$, whereas the analogous inequality with $a_9 = 6$ holds for all $t \in (0,1)$. Recalling that this sequence of dimension factors (including those of p-power index dealt with earlier in the proof) was the sequence which gave the *minimal* possible value of A, we conclude that for any p-tower KV-group of Z-type $(3,7)$, we have

$$\sum_{n=1}^{\infty} a_n \geqslant 2+1+1+1+2+2+3+5+6+2(a-1)+(b-a) = 21+a+b. \qquad \square$$

Remark 18. The explicit bound $|G| \geqslant p^{23}$ might suggest that to find candidates for quadratic imaginary number fields whose p-tower group is of Z-type $(3,7)$, it would be prudent to search for fields with very large p-class groups (but still, of course, with p-rank 2). The bound $|G| \geqslant p^{21+a+b}$, however, shows that this is not the case. In particular, since we have assumed that $|G^{ab}| = p^{a+b}$, the theorem implies (via the inequality $|G'| \geqslant p^{21}$) that it is the commutator subgroup which contains the bulk of this newfound size.

5. Concluding remarks

The proof of Theorem 17 suggests that we can hope to better understand finite groups of Z-type (3,7) by considering abstract sequences of invariants which conform to the bounds given by the various results on such a group's dimension factors. Namely, for a sequence $a_1, a_2, \ldots$ of non-negative integers (and a fixed prime p), we could define invariants b_n, c_n, and e_n for $n \geqslant 1$ by mirroring their definitions as found in the text:

$$\sum_{n=0}^{\infty} b_n t^n = \prod_{n=1}^{\infty} P_n(t)^{a_n}, \qquad c_n = b_{n+1} - b_n,$$
$$e_n = c_n - 2c_{n-1} + c_{n-3} + c_{n-7} - 1.$$

We will say the original sequence $\{a_n\}$ is *potentially KV* if its terms satisfy the bounds given by Proposition 15 and Lemma 16, and if the corresponding sequences c_n and e_n are non-negative and stabilize for sufficiently large n. Certainly a necessary condition for the existence a finite p-group of Z-type (3,7) is the existence of such a sequence. While it may be tempting to view Theorem 17 as a first step toward proving the non-existence of such a group or sequence, the following example, found in collaboration with Ray Puzio, shows that this interpretation is premature.

Example 19. For $p = 17$, the sequence

$$\{a_n\}_{n=1}^{15} = \{2,1,1,1,2,2,3,3,4,4,6,5,7,5,4\}$$

is potentially KV. In other words, a pro-p-group G with dimension factors a_n defined by the above sequence satisfies all of the combinatorial criteria above to be a KV-group of Z-type $(3,7)$.

It seems difficult, at the present, to determine whether or not this example actually occurs as the sequence of dimension factors of a pro-p-group, though we note that by the proof of Proposition 13 the abelianization of such a group would necessarily be isomorphic to $\mathbb{Z}/17\mathbb{Z} \oplus \mathbb{Z}/17\mathbb{Z}$. Further, by summing the sequence, we see that such a group would have order 17^{50}, well beyond the bound guaranteed by Theorem 17 (and larger than the monster group!).

Finally, we wish to remark on a possible alternate interpretation for the sequence of invariants e_n appearing in the Golod–Shafarevich equality. A result of Labute [8, Theorem 5.1g], shows that for a mild pro-p-group, one has

$$\sum r_k t^k - dt + 1 = \sum b_n t^n,$$

which after applying Jennings' theorem to the right-hand side, is precisely the Golod–Shafarevich inequality in the case that $e_n = 0$ for all n. This suggests a further interpretation of the e_n as a measure of the non-mildness of a pro-p-group G. As a toy example of this interpretation, the fact that for a finite p-group G we have $e_n = |G| - 1 \neq 0$ for all sufficiently large n (see the discussion after Remark 7) might suggest that finite p-groups are "highly non-mild."

Acknowledgments

The author would like to thank William McCallum for his guidance and support, Ray Puzio for his insights on recursion relations, the reviewer for several improvements, and Kirti Joshi, Dinesh Thakur, and Klaus Lux for endless valuable conversations.

Supplementary material

The online version of this article contains additional supplementary material.
Please visit doi:10.1016/j.jnt.2009.05.014.

References

[1] L. Bartholdi, M.R. Bush, Maximal Unramified 3-Extensions of Imaginary Quadratic Fields and $SL_2(\mathbb{Z}_3)$, 2006.
[2] Klaus Haberland, Galois Cohomology of Algebraic Number Fields, VEB Deutscher Verlag der Wissenschaften, Berlin, 1978.
[3] S.A. Jennings, The structure of the group ring of a p-group over a modular field, Trans. Amer. Math. Soc. 50 (1941) 175–185.
[4] Helmut Koch, Zum Satz von Golod–Schafarewitsch, Math. Nachr. 42 (1969) 321–333 (in German).
[5] Helmut Koch, Galois Theory of p-Extensions, Translated from the 1970 German original by Franz Lemmermeyer, Springer-Verlag, Berlin, 2002, xiv+190 pp.
[6] H. Koch, B. Venkov, The p-Tower of Class Fields for an Imaginary Quadratic Field, Zap. Naučn. Sem. Leningrad Otdel. Mat. Inst. Steklov. (LOMI), vol. 46, 1974 (in Russian).
[7] John P. Labute, On the descending central series of groups with a single defining relation, J. Algebra 14 (1970) 16–23.
[8] John Labute, Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$, J. Reine Angew. Math. 596 (2006) 155–182.
[9] Michel Lazard, Sur les groupes nilpotents et les anneaux de Lie, Ann. Sci. Ecole Norm. Sup. 71 (3) (1954) 101–190.
[10] Michel Lazard, Groupes analytiques p-adiques, Publ. Math. Inst. Hautes Études Sci. 26 (1965) 389–603.
[11] Cameron McLeman, A Golod–Shafarevich Equality and p-tower Groups, PhD dissertation, University of Arizona, 2008.
[12] Cameron McLeman, p-tower groups over quadratic imaginary number fields, Ann. Sci. Math. Quebec 32 (2) (2009).
[13] I. Shafarevich, Extensions with prescribed ramification points, Publ. Math. Inst. Hautes Études Sci. 18 (1963) 71–95.
[14] V.A. Skopin, Certain finite groups. Modules and homology in group theory and Galois theory, Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) 31 (1973) 115–139 (in Russian).
[15] A. Scholz, O. Taussky, Die Hauptideale der kubischen Klassenkörper imaginär-quadritscher Zahlkörper, J. Reine Angew. Math. 171 (1934) 19–41.
[16] Denis Vogel, Massey products in the Galois cohomology of number fields, PhD dissertation, Ruprecht–Karls Universität, Heidelberg, 2004.
[17] K. Wingberg, On the maximal unramified p-extension of an algebraic number field, J. Reine Angew. Math. 440 (1993) 129–156.