

# Finite Presentations of Pro- $p$ and Discrete Groups

Leigh Humphries, 137067

November 4, 2005

# Contents

<b>1 Preliminaries</b>	<b>5</b>
<b>2 Presentations of pro-<math>p</math> groups</b>	<b>13</b>
<b>3 The Theorems</b>	<b>16</b>
3.1 Proof of Theorem A' . . . . .	23
3.2 Proof Theorem B . . . . .	25
<b>4 The Corollaries</b>	<b>26</b>
<b>5 Consequences and Further Work</b>	<b>29</b>

## Preface

The study of profinite groups is closely associated with the study of Galois groups of algebraic field extensions of infinite degree. Indeed, suppose that  $K$  is an infinite degree Galois extension of a field  $L$ . Then define the Galois group  $\text{Gal}(K/L)$  to be the group of automorphisms of  $K$  fixing  $L$  elementwise. If we consider the family  $\mathcal{F}$  of all intermediate fields  $L \leq F \leq K$ , we can find  $\mathcal{L} \subseteq \mathcal{F}$  such that

$$\mathcal{L} = \{F \mid F \text{ is a finite Galois extension of } L\}$$

From Galois theory, we know that  $|\text{Gal}(K/L)|$  is infinite, but for each  $F \in \mathcal{L}$ ,  $|\text{Gal}(F/L)|$  is finite and  $\text{Gal}(F/L) < \text{Gal}(K/L)$ . We can define a topology in  $\text{Gal}(K/L)$  by taking a base of open neighbourhoods of 1 to be the family of subgroups

$$\mathcal{N} = \{\text{Gal}(K/F \mid F \in \mathcal{L}\}$$

Moreover, since  $K$  is the direct limit of the family  $\mathcal{L}$  the Galois correspondence gives us that  $\text{Gal}(K/L)$  is the *inverse* limit of the family of groups  $\text{Gal}(F/L)$  for every  $F \in \mathcal{L}$ . So  $\text{Gal}(K/L)$  is in fact a profinite group, as defined in Chapter 1, and by giving each of the finite groups  $\text{Gal}(F/L)$  the discrete topology, the group  $\text{Gal}(K/L)$  is given the same topology as above, by virtue of the inverse limit.

The converse to this is also true, not only is a Galois group of a Galois extension of infinite degree a profinite group; every profinite group  $G$  is isomorphic (as a topological group) to a Galois group. (See Wilson, [9] Theorem 3.3.2).

The purpose of this paper is to present the results published by John Wilson [10] in his paper "Finite Presentations of pro- $p$  and discrete groups." (Chapter 3 and Chapter 4), as well as the preliminary material required for the results (Chapters 1 and 2) and the consequences of this paper in the study of profinite groups (Chapter 5). In particular, the main result of the paper is a version of the Golod-Šafarevič theorem 'for a large class of pro- $p$  groups and discrete groups' (Wilson, [10]). This 'large class' includes, for example, all soluble groups. The Golod-Šafarevič inequality is a sufficient condition for the infinitude of finitely generated pro- $p$  groups, that is, if a finitely generated pro- $p$  group fails to satisfy the inequality 1 then it must be an infinite group. As a result, E.S Golod ([4]) used this inequality to provide a counterexample to the General Burnside Problem.

As the title of the paper suggests, we are primarily concerned with presentations of pro- $p$  groups in terms of generators and relations. In general, if a profinite group  $G$  is said to be generated by a subset  $X$ , we do in fact mean  $X$  generates  $G$  *topologically*, that is,  $G$  is the closure (in the appropriate topology) of the abstract group generated by  $X$ , and we write  $d(G)$  for the minimal number of generators of  $G$  (with  $d(G) = \infty$  if  $G$  is not finitely generated). Also, we often need to distinguish between open and closed subgroups of  $G$ . Where this is necessary, we make this distinction by adding a subscripted  $O$  or  $C$  to the relation symbol. (i.e.  $H \triangleleft_O G$  means " $H$  is an *open* normal subgroup of  $G$ "). We will be repeatedly using the fact that for a topological group  $G$ , the map  $x \mapsto x^{-1}$  is continuous, and for a fixed  $g \in G$  the maps  $x \mapsto gx$  and  $x \mapsto xg$  are homeomorphisms. The proofs of these can be found in [9] Lemma 0.3.1.

The theorems themselves are as follows:

**Theorem 1 (Theorem A).** *Let  $G$  be a pro- $p$  group which has finite presentation with  $n$  generators and  $r$  relations, and suppose  $d = d(G) > 1$ . Then either*

$$r \geq n + \frac{1}{4}d^2 - d \quad (1)$$

*or for each finitely generated dense discrete subgroup  $X$  of  $G$  there is a closed normal subgroup  $K$  of  $G$  such that  $XK/K$  is an infinite (finitely generated) torsion group.*

**Theorem 2 (Theorem B).** *Let  $G$  be a discrete group which has a finite presentation with  $n$  generators and  $r$  relations, and let  $d = d(G^{ab})$  (where  $G^{ab}$  is the abelianization of  $G$ ). Then either*

$$r \geq n + \frac{1}{4}(d^2 - 1) - d \quad (2)$$

*or for some prime  $p$ ,  $G$  has a normal subgroup  $K$  such that  $G/K$  is an infinite residually  $p$ -torsion group.*

The proofs of these theorems are provided in Chapter 3.

# 1 Preliminaries

We begin by defining the necessary concepts for the construction of profinite groups. Recall that a directed set is a partially ordered set  $I$  such that for all  $i_1, i_2 \in I$  there is an element  $j \in I$  for which  $i_1 \leq j$  and  $i_2 \leq j$ .

**Definition 1 (Inverse System).** An Inverse System  $(X_i, \varphi_{ij})$  of topological spaces indexed by a directed set  $I$  consists of a family  $(X_i | i \in I)$  of topological spaces and a family  $(\varphi_{ij} : X_j \rightarrow X_i | i, j \in I, i \leq j)$  of continuous maps such that for every  $i$ ,  $\varphi_{ii}$  is the identity map on  $X$ , and  $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$  whenever  $i \leq j \leq k$ .

**Definition 2 (Compatible Family).** Let  $(X_i, \varphi_{ij})$  be an inverse system of topological spaces and let  $Y$  be a topological space. We call a family  $(\psi_i : Y \rightarrow X_i | i \in I)$  of continuous maps compatible if  $\varphi_{ij}\psi_j = \psi_i$  whenever  $i \leq j$ . The condition can be expressed as the requirement that each of the following diagrams commutes:

$$\begin{array}{ccc} & Y & \\ \psi_j \swarrow & & \searrow \psi_i \\ X_j & \xrightarrow{\varphi_{ij}} & X_i \end{array}$$

**Definition 3 (Inverse Limit).** An inverse limit  $(X, \varphi_i)$  of an inverse system of topological spaces  $(X_i, \varphi_{ij})$  is a topological space  $X$  together with a compatible family of continuous maps with the following universal property: Whenever  $(\psi_i : Y \rightarrow X_i)$  is a compatible family of continuous maps from a space  $Y$ , there is a unique continuous map  $\psi : Y \rightarrow X$  such that  $\varphi_i\psi = \psi_i$  for each  $i$ . That is, there is a unique  $\psi$  such that each of the following diagrams is commutative.

$$\begin{array}{ccc} & Y & \\ \psi \swarrow & & \searrow \psi_i \\ X & \xrightarrow{\varphi_i} & X_i \end{array}$$

Note that the above definition applies to topological groups and rings by stipulating that each of the continuous maps are in fact continuous homomorphisms (respectively, ring homomorphisms).

Let  $(X_i, \varphi_{ij})$  be an inverse system and write  $C = \prod_{i \in I} X_i$  and let  $\pi_i$  be the projection map from  $C$  to  $X_i$ . Define  $X = \{c \in C | \varphi_{ij}\pi_j(c) = \pi_i(c), i \leq j\}$ , and  $\varphi_i = \pi_i|_X$  for each  $i$ . Then  $(X, \varphi_i)$  is an inverse limit of  $(X_i, \varphi_{ij})$ , which we denote  $\varprojlim X_i$ . In the case that the  $X_i$  form a set  $J$  we denote this inverse limit  $\varprojlim_j X_j$ . As inverse limits are unique up to isomorphism (see [9], Proposition 1.1.4) we can use this particular construction to prove general facts about profinite group.

We now have all the concepts needed to define pro- $\mathcal{C}$  groups:

**Definition 4 (Pro- $\mathcal{C}$  Group).** Let  $\mathcal{C}$  be a class of finite groups. We call  $F$  a  $\mathcal{C}$  group if  $F \in \mathcal{C}$ . A topological group  $G$  is called a pro- $\mathcal{C}$  group if it is the inverse limit of an inverse system of  $\mathcal{C}$ -groups.

In the above definition, class is meant in the usual sense, with the added condition that it is closed under isomorphism. That is, if  $F_1 \in \mathcal{C}$  and  $F_1 \cong F_2$  then  $F_2 \in \mathcal{C}$ .

Some important classes of this type are:

- The class of all finite groups,
- The class of finite  $p$ -groups (groups of order  $p^k$ , for some  $k$ ), where  $p$  is a fixed prime,
- The class of all finite cyclic groups.

An inverse limits of finite,  $p$ -, and cyclic groups are denoted *profinite*, *pro- $p$*  and *procyclic* groups, respectively. Note also that since  $\mathcal{C}$  is a class of finite groups, any pro- $\mathcal{C}$  group is also a profinite group.

Examples of pro- $\mathcal{C}$  groups include:

- Any  $\mathcal{C}$ -group is a pro- $\mathcal{C}$  group (corresponding to the directed set of just one element).
- Call a map  $\theta : X \rightarrow G$  from a set  $X$  to a profinite group  $G$  1-convergent if and only if  $\theta^{-1}(1)$  contains all but finitely many elements of  $X$ . The free pro- $\mathcal{C}$  group on a set  $X$ ; defined as a pro- $\mathcal{C}$  group  $F$  together with a 1-convergent map  $j : X \rightarrow F$  with the universal property that whenever  $\xi : X \rightarrow G$  is a 1-convergent map to a *profinite* group  $G$ , there is a unique homomorphism  $\bar{\xi} : F \rightarrow G$  such that the following diagram commutes:

$$\begin{array}{ccc} & X & \\ j \swarrow & & \searrow \xi \\ F & \xrightarrow{\bar{\xi}} & G \end{array}$$

The convergence condition ensures that the free pro- $\mathcal{C}$  group on  $X$  is the inverse limit of the free pro- $\mathcal{C}$  groups on the finite subsets of  $X$ . In particular, the free pro- $p$  group is vital to the discussion of presentations of pro- $p$  groups, see Chapter 2

The following theorem gives us a characterization of profinite groups that is useful:

**Theorem 3.** *Let  $G$  be a topological group. The following are equivalent:*

- (i)  $G$  is profinite;
- (ii)  $G$  is isomorphic (as a topological group) to a closed subgroup of a Cartesian product of finite groups;
- (iii)  $G$  is a compact Hausdorff topological group whose open subgroups form a base for the neighbourhoods of the identity.

*Proof.*

(i)  $\Rightarrow$  (ii)

This follows from the fact that since each of the groups  $X_i$  in the inverse limit is Hausdorff (since each  $X_i$  has the discrete topology), the group  $s\varprojlim X_i$  is closed in  $\prod_{i \in I} X_i$ , as  $s\varprojlim X_i = \bigcap_{j > i} \{c \in \prod_{i \in I} X_i \mid \vartheta_{ij} \pi_j(c) = \pi_i(c)\}$  (where the  $\vartheta_{ij}$  are the maps in the inverse system and the  $\pi_i$  are the projection maps). Thus  $s\varprojlim X_i$  is the intersection of closed sets, giving the result.

(ii)  $\Rightarrow$  (iii)

Suppose  $G$  is isomorphic to a closed subgroup  $\hat{G}$  of  $C = \prod_{i \in I} X_i$  where each  $X_i$  is a finite group, and for each  $i$  write  $K_i$  for the kernel of the projection map  $\pi_i : C \rightarrow X_i$  and write  $N_i = K_i \cap \hat{G}$ . Because each of the  $X_i$  are compact and Hausdorff, so is  $C$  (by Tychonoff's Theorem), and since  $\hat{G}$  is a closed subgroup of  $C$ ,  $\hat{G}$  is also compact. Since  $K_i \triangleleft C$  we have  $N_i \triangleleft \hat{G}$  and since  $\bigcap_{i \in I} K_i = \{1\}$  we have  $\bigcap_{i \in I} N_i = \{1\}$  as well. Hence  $\bigcap (N_i | N_i \triangleleft \hat{G}) = 1$  and the open subgroups of  $\hat{G}$  form a basis for the neighbourhoods of the identity.

(iii)  $\Rightarrow$  (i)

Write  $\hat{G} = \varprojlim (G/N)$  for  $N \triangleleft G$ . That is, the inverse limit of the inverse set of open normal subgroups ordered by reverse inclusion with the natural maps  $(G/K \rightarrow G/L)$  for  $K \leq L$ . There is a natural homomorphism  $\iota : G \rightarrow \prod G/N$  given by  $\iota(g) = (gN)_{N \triangleleft G}$ . Since  $\bigcap \{N | N \triangleleft G\} = 1$ ,  $\iota$  is injective, and  $\iota(G) \leq \hat{G}$ .  $\square$

Note that part (ii) of this characterization implies that the group is totally disconnected, that is, that every connected subspace of a profinite group  $G$  contains at most one element. This follows since each of the finite groups in the inverse system has the discrete topology and is therefore totally disconnected. Since this property is preserved by products and subspaces,  $G$  must also be totally disconnected. Using Theorem 3, we show some elementary topological properties of profinite groups.

**Lemma 1.** *Let  $G$  be a profinite group.*

(i) *Every open set is a union of sets which are both closed and open.*

(ii) *If  $C$  is a subset of  $G$  which is both closed and open and contains 1 then  $C$  contains an open normal subgroup.*

*Proof.*

(i)

Let  $U$  be a non-empty open set and choose  $x \in U$ . For each  $y \in G \setminus \{x\}$  there is a set  $F_y$  with  $x \in F_y$  and  $y \notin F_y$  which is both closed and open, because any set strictly containing  $\{x\}$  is disconnected (since  $G$  is totally disconnected).  $X$  is the union of the open set  $U$  and the open sets  $X \setminus F_y$ , so by compactness there are finitely many elements  $y_1, \dots, y_n$  such that

$$\begin{aligned} X &= U \cup \left( \bigcup_{i=1}^n X \setminus F_{y_i} \right) \\ &= U \cup \left( X \setminus \bigcap_{i=1}^n F_{y_i} \right) \\ \Rightarrow X \setminus U &\subseteq X \setminus \bigcap_{i=1}^n F_{y_i} \\ \Rightarrow U &\supseteq \bigcap_{i=1}^n F_{y_i} \end{aligned}$$

This intersection is both open and closed, since each of the  $F_{y_i}$  are open and closed, and contains  $x$ , since each of the  $F_{y_i}$  contain  $x$ . If we repeat this construction for each  $x \in U$ , and let  $U_x$  be the respective intersections  $\bigcap_{i=1}^n F_{y_i}$  for

$x$  then we find  $U \supseteq \bigcup_{x \in U} U_x$  since  $U$  contains each of the  $U_x$ , and also that  $U \subseteq \bigcup_{x \in U} U_x$  since for any  $x \in U$  there is a  $U_x$  containing  $x$ . Hence  $U = \bigcup_{x \in U} U_x$  is a union open and closed sets.

(ii)

Let  $C$  be an open and closed subset of  $G$  containing 1. For each  $x \in C$ , the set  $W_x = Cx^{-1}$  is an open neighbourhood of 1 such that  $W_x x \subseteq C$ . Since multiplication is continuous (mapping from  $G \times G$  to  $G$ ), the inverse image of  $W_x$  in is an open set  $\overline{W}_x$ . By the definition of the product topology there exist open sets  $L_x, R_x$  (each containing 1) in  $G$  such that  $L_x \times R_x \subseteq \overline{W}_x$ . Hence  $L_x R_x \subseteq W_x$ . Denote  $L_x \cap R_x$  by  $S_x$ . We see that  $S_x$  is open, and  $S_x S_x \subseteq L_x S_x \subseteq L_x R_x \subseteq W_x$ . Since each of  $L_x, R_x$  contain 1,  $1 \in S_x$  and so  $x \in S_x x$ . Hence

$$\begin{aligned} C &\subseteq \bigcup_{x \in C} (C \cap S_x x) \\ &= C \cap \left( \bigcup_{x \in C} S_x x \right) \\ \Rightarrow C &\subseteq \bigcup_{x \in C} S_x x \end{aligned}$$

, and since  $S_x x$  is open for each  $x$ , by compactness we have  $C \subseteq \bigcup_{i=1}^n S_{x_i} x_i$  for  $n < \infty$ . Let  $S = \bigcap_{i=1}^n S_{x_i}$  is open and contains 1, so

$$\begin{aligned} SC &\subseteq S \bigcup_{i=1}^n S_{x_i} x_i \\ &= \bigcup_{i=1}^n S S_{x_i} x_i \\ &\subseteq \bigcup_{i=1}^n S_{x_i} S_{x_i} x_i \\ &\subseteq \bigcup_{i=1}^n W_{x_i} x_i \\ &\subseteq C \end{aligned}$$

So  $S \subseteq C$ .

Let  $T = S \cap S^{-1}$ , where  $S^{-1} = \{x^{-1} | x \in S\}$ . Then we can easily see  $T$  is open, since  $S$  and  $S^{-1}$  are both open,  $T = T^{-1}$ ,  $1 \in T$  and  $T \subseteq S \subseteq C$ . Write  $T^1 = T$  and  $T^n = T T^{n-1}$  for  $n > 1$  and denote by  $H$  the union  $\bigcup_{m > 0} T^m$ . Then if  $T^{n-1} \in C$ ,  $T^n \subseteq T C \subseteq S C \subseteq C$ , so  $T^m \subseteq C$  for every  $m \geq 1$ . We see that  $T^m$  is a union of the form  $\bigcup_{y \in T^{m-1}} T y$ , and is therefore open for any  $m$ . Hence  $H$  is also open, and is the group generated by  $T$  (being the set of words over  $T$ ). Since  $H$  is an open subgroup, it follows from part (i) of Proposition 1 that  $H$  has finite index in  $G$  and therefore has only finitely many conjugates in  $G$ . Each of the conjugates is open, and hence the intersection of the conjugates (since there are only finitely many) is open and is contained in  $C$ , since  $1T1 = T$  is a conjugate contained in  $C$ . Thus  $C$  contains an open normal subgroup.  $\square$

**Proposition 1.** *Let  $G$  be a profinite group.*

- (i) Every open subgroup of  $G$  is closed, has finite index in  $G$ , and contains an open normal subgroup of  $G$ . A closed subgroup of  $G$  is open if and only if it has finite index.
- (ii) A subset of  $G$  is open if and only if it is a union of cosets of open normal subgroups
- (iii) For any subset  $X$  of  $G$

$$\bar{X} = \bigcap_{N \triangleleft_o G} XN$$

In particular, if  $X$  is a subgroup of  $G$  then

$$\bar{X} = \bigcap \{K \mid X \leq K \leq_o G\}$$

- (iv) If  $X$  and  $Y$  are closed subsets of  $G$  then so is the set  $XY$ . If  $X$  is an integer then the set  $\{x^n \mid x \in X\}$  is closed

*Proof.*

(i)

We have seen that the maps defined by  $x \mapsto gx$  and  $x \mapsto xg$ , for a fixed  $g \in G$ , are both homeomorphisms. Thus for an open set  $H \leq G$ , the relative complement  $G \setminus H = \bigcup \{gH : g \notin H\}$  is also open. Hence  $H$  is closed. Also, if  $H$  is open, then  $G$  is the disjoint union of open sets. Hence, by the definition of compactness, there must be finitely many cosets of  $H$  (since no proper sub-cover could contain the entire group). So  $H$  has finite index.

Suppose that  $H$  is closed, then  $G \setminus H$  is the union of closed sets (similar to the open case), and so is closed if  $H$  is of finite index. In which case  $H$  is open.

(ii)

That every union of cosets of open normal subgroups is an open set is clear, since multiplication is continuous. Suppose that  $U$  is a non-empty open subset of  $G$ . Then for any  $x$  in  $U$ ,  $Ux^{-1}$  is an open set containing 1. So by Lemma 1 (i),  $Ux_i$  is a union of subsets which are both open and closed. Since at least one of these subsets contains 1, by Lemma 1 (ii)  $Ux_i$  contains an open normal subgroup  $N_x$ . Hence  $N_x x$  is a coset of an open normal subgroup and  $U = \bigcup_{x \in U} N_x x$ , as required.

(iii)

Let  $y \notin \bar{X}$ , then there exists an open neighbourhood containing  $y$  which is disjoint from  $X$ . From (ii), it follows that there exists an open normal subgroup of  $G$  satisfying  $Ny \cap X = \emptyset$ , thus  $y \notin NX$ , so  $NX \subseteq \bar{X}$ . That  $\bar{X} \subseteq NX$  follows from (i). Also note that if  $H$  is a subgroup of  $G$ , then  $HN \leq_o G$  since  $|N : G| < \infty$  implies  $|HN : G| < \infty$ , and since  $HN$  obviously contains  $H$ , we get that  $\bar{H} = \bigcap \{K \mid H \leq K \leq_o G\}$ .

(iv)

The set  $\{x^n \mid x \in X\}$  is the image of the continuous map  $x \mapsto x^n$  and so is compact, hence closed in  $G$ . Since  $X, Y$  are both closed and  $G$  is compact, it follows that  $X$  and  $Y$  are compact and so is the set  $X \times Y$  in  $G \times G$ . The map  $(x, y) \mapsto xy$  is continuous, so the image of  $X \times Y$  is compact and equal to  $XY$ . Thus  $XY$  is closed.  $\square$

As a corollary to the above, we note that if  $X$  is the trivial group and  $\mathcal{K}$  the set of subgroups of finite index, then

$$\bigcap_{K \in \mathcal{K}} K \subseteq \bigcap \{L \mid L \leq_o G\} = \overline{\{1\}} = \{1\}$$

Since  $\{1\}$  is closed (because  $G$  is Hausdorff). Hence every profinite group is residually finite.

There are two more constructions, the Frattini subgroup of a profinite group and the completion of an abstract group, that need mention before we move on to the discussion of presentations. Call a family  $I$  of normal subgroups of a group  $G$  a *filter base* if for every  $K_1, K_2 \in I$ , there exists  $K_3 \in I$  such that  $K_3 \subseteq K_1 \cap K_2$ .

**Definition 5 (Completion).** Let  $G$  be an abstract group and  $I$  a non-empty filter base of normal subgroups of finite index. Call a subset of  $G$  open if and only if it is the union of cosets  $Kg$  of subgroups  $K \in I$ . The completion of  $G$  with respect to  $I$  consists of a profinite group  $\hat{G}$  together with a continuous homomorphism  $j : G \rightarrow \hat{G}$  such that the following property holds:

For every continuous homomorphism  $\theta : G \rightarrow H$  (where  $H$  is a profinite group) there is a unique continuous homomorphism  $\hat{\theta} : \hat{G} \rightarrow H$  such that the diagram

$$\begin{array}{ccc} & G & \\ j \swarrow & & \searrow \theta \\ \hat{G} & \xrightarrow{\hat{\theta}} & H \end{array}$$

commutes.

We are particularly concerned with the *pro- $p$  completion* of  $G$ . That is, the completion of  $G$  with respect to the filter base  $I$  consisting of all normal subgroups of  $p$ -power index. Thus the pro- $p$  completion of  $G$  is in fact a pro- $p$  group. In general, for a class  $\mathcal{C}$  of finite groups which is closed with respect to subgroups and direct products, the the pro- $\mathcal{C}$  completion of  $G$  is defined as the completion with respect to the family of normal subgroups  $K$  such that  $G/K \in \mathcal{C}$ .

The following proposition shows that such constructions exist.

**Proposition 2.** Let  $I$  be a non-empty filter base of normal subgroups and let  $\hat{G} = \varprojlim_I G/K$ . Let  $j$  be the map  $g \mapsto (Kg)$  from  $G$  to  $\hat{G}$ . The pair  $(\hat{G}, j)$  has the properties of the completion of  $G$  with respect to  $I$ .

*Proof.*

First note that  $j$  is continuous, since the product of the  $j$  with the projection maps  $\pi_i : \hat{G} \rightarrow G/K_i$  gives continuous quotient homomorphisms. Let  $\theta : G \rightarrow H$  be a continuous map into a finite group  $H$ . Since  $\theta$  is continuous  $\ker \theta$  is open (since  $\{1\}$  is open) so  $\ker \theta$  contains some  $L \in I$ . Define  $\hat{\theta} : \hat{G} \rightarrow H$  to be the map taking each element in  $\hat{G}$  to its coordinate in  $G/L$  composed with the induced homomorphism  $Lg \mapsto \theta(g)$  from  $G/L$  to  $H$ . Thus  $\hat{\theta}$  is continuous, as each of its components are continuous, and  $\theta = \hat{\theta}j$ .  $\hat{\theta}$  is unique since if  $\varphi$  is a continuous homomorphism satisfying  $\theta = \varphi j$  then  $\hat{\theta}, \varphi$  agree on  $j(G)$ , which is dense in  $\hat{G}$ . Thus  $\varphi = \hat{\theta}$ .  $\square$

**Definition 6** (Frattini Subgroup). *The Frattini Subgroup of a profinite group  $G$ , denoted  $\Phi(G)$  is the intersection of all maximal open subgroups of  $G$ .*

We note that  $\Phi(G)$  is a normal subgroup of  $G$  since conjugation preserves maximality and openness, that is, if  $H \in \Phi(G)$  then  $gHg^{-1} \in \Phi(G)$  for any  $g \in G$  from which it follows that  $g\Phi(G)g^{-1} = \Phi(G)$  for any  $g \in G$ . Thus  $\Phi(G)$  is normal. The Frattini subgroup is particularly useful when studying pro- $p$  groups.

**Proposition 3.** *Let  $G$  be a profinite group,*

- (i)  $\Phi(G) \triangleleft_c G$
- (ii) *Let  $X$  be a subset of  $G$ , then the following are equivalent:*
  - (a)  $X$  generates  $G$  topologically
  - (b)  $X \cup \Phi(G)$  generates  $G$  topologically
  - (c)  $X\Phi(G)/\Phi(G)$  generates  $G/\Phi(G)$  topologically
- (iii) *Let  $H$  be a subgroup of  $G$ , then if  $H\Phi(G) = G$  then  $H = G$ .*
- (iv) *If  $K \triangleleft_c G$  and  $K \leq \Phi(G)$  then  $\Phi(G/K) = \Phi(G)/K$ .*

*Proof.*

(i)

We have seen that  $\Phi(G)$  is normal, and since each open subgroup of  $G$  is closed from Proposition 1,  $\Phi(G)$  is an intersection of closed sets, hence closed.

(ii)

That (a) implies (b) is obvious.

Suppose that  $X \cup \Phi(G)$  generates  $G$  topologically and let  $H$  be the subgroup of  $G$  generated by  $X\Phi(G)$ . Let  $K/\Phi(G)$  be a closed subset of  $G/\Phi(G)$  containing  $H/\Phi(G)$ . Then  $K/\Phi(G) \supseteq H/\Phi(G) = \overline{\langle X\Phi(G) \rangle}/\Phi(G) = \overline{\langle X \cup \Phi(G) \rangle}/\Phi(G)$  hence  $K = G$ . Thus the closure of  $H/\Phi(G) = G/\Phi(G)$  as required.

Suppose that (c) holds, and let  $K$  be an open subgroup of  $G$  containing  $X$ . If  $K \neq G$ , then  $K \leq M$  for some maximal open subgroup  $M$  of  $G$ . Then since  $M \geq K$  and  $M \geq \Phi(G)$

$$\overline{\langle X \rangle}\Phi(G)/\Phi(G) \leq M/\Phi(G)$$

and  $M/\Phi(G) \neq G/\Phi(G)$  since  $M$  is a proper subgroup of  $G$ . This contradicts the assumption, so  $G$  is the only open subgroup containing  $X$ , and therefore the only open subgroup containing  $\langle X \rangle$ . From Proposition 1(iii), it follows that  $\overline{\langle X \rangle} = G$ , as required.

(iii)

Suppose  $H \neq G$ , then since  $H \subseteq \bar{H} = \bigcap (K|H \leq K \leq_o N)$ , there is a maximal open subgroup  $M$  containing  $H$ . But then  $H \leq M$  and  $\Phi(G) \leq M$  so  $H\Phi(G) \leq M$ . The result follows by the contrapositive.

(iv)

Suppose  $M/K$  is a maximal open subgroup of  $G/K$ . Then  $M$  is a maximal open subgroup of  $G$ , and so  $M \geq \Phi(G)$  and  $M/K \geq \Phi(G)/K$ . Hence  $\Phi(G/K) = \bigcap M/K \geq \Phi(G)/K$ . Suppose  $\Phi(G/K) > \Phi(G)/K$ , then there exists a maximal open subgroup  $H$  of  $G$  such that  $H/K \leq M/K$  for every maximal open subgroup  $M/K$  in  $G/K$ . But then  $H$  is clearly not maximal, so  $\Phi(G/K) \leq \Phi(G)/K$ , as required.  $\square$

**Proposition 4.** *Let  $G$  be a pro- $p$  group. Then  $G$  is finitely generated if and only if  $\Phi(G)$  is open in  $G$ .*

*Proof.*

If  $\Phi(G)$  is open  $G/\Phi(G)$  is finite and so there is a finite subset  $X$  of  $G$  such that  $G = X\Phi(G)$ . Hence  $X \cup \Phi(G)$  generates  $G$  and from Proposition 3,  $X$  generates  $G$ .

Now suppose  $G = \overline{\langle X \rangle}$  where  $|X| = d$  is finite. If  $\Phi(G) \leq N \triangleleft_O G$ , then  $G/N$  is finite since  $N$  is open in  $G$ , hence  $G/N$  is an elementary abelian  $p$ -group, and can be generated by  $d$  elements, consequently  $|G : N| \leq p^d$ . We chose a subgroup  $N_0$  among all such subgroups  $N$  such that the index of  $N_0$  is maximal. Then  $N_0 \leq N$  whenever  $\Phi(G) \leq N \triangleleft_O G$ . Since  $\Phi(G)$  is both closed and normal in  $G$ , it follows that

$$\Phi(G) = \bigcap \{N \mid \Phi(G) \leq N \triangleleft_O G\} = N_0$$

Thus  $\Phi(G)$  is open in  $G$ . □

## 2 Presentations of pro- $p$ groups

In his 1902 paper [2], William Burnside presented the following problems:

**Burnside Problem**

Is a finitely generated periodic group of bounded exponent necessarily finite?

**General Burnside Problem:**

Is a finitely generated periodic group necessarily finite?

These problems turned out to be considerably difficult and despite early progress from Burnside and Schur, the difficulty in showing any counterexamples to the problems meant that progress was limited until the 1930s, when the following variant of the Burnside Problem was proposed:

**Restricted Burnside Problem**

Are there only finitely many finite  $m$ -generator groups of exponent  $n$ ?

Since that time, there have been many results showing that specific classes of groups, such as all the Burnside groups  $B(m, q)$  for a fixed  $q$ , (where  $B(m, n) = F_m/F_m^n$ ,  $F_m$  being the free group of rank  $m$ ) are finite, but it was not until 1959 that any counterexamples were forthcoming. Novikov announced the existence of a counterexample (that  $B(m, n)$  is infinite for  $n$  odd,  $> 71$ ), but evidently had problems with the proof. It was not until 1968 that Novikov published a counterexample, with S I Adian, showing that for  $n$  odd,  $n \geq 4381$  (later reduced to  $n \geq 665$ , but still much larger than the original 71)  $B(m, n)$  is infinite. This proof used a complicated inductive construction to show that  $B(m, n)$  is not only infinite, but also has solvable word and conjugacy problems.

In the meantime, Golod and Šafarevič produced the first counterexample to the General Burnside Problem, using the Golod-Šafarevič inequality. Since their group did not have bounded exponent, it wasn't a counterexample to the Burnside Problem itself, but did give the first indication that the problem would have a negative answer, as was later confirmed by the Novikov result. The third problem (the restricted Burnside problem) was solved in 1994 by Efim Zel'manov, who used deep structure theory of Jordan Algebras to give a positive solution. Zel'manov was awarded a Fields medal for the proof.

We now return our attention to the Golod-Šafarevič inequality, and the presentations of pro- $p$  groups.

Let  $E$  be a pro- $p$  group and denote by  $d(E)$  the least cardinality of a generating set of  $E$  (writing  $d(E) = \infty$  if  $E$  is not finitely generated). If  $R$  is a normal subgroup of  $E$  we say that  $R$  is generated as a normal subgroup by a subset  $X$  if  $R$  is the smallest (closed) normal subgroup containing  $X$ . If finitely many such sets  $X$  exist we write  $d_E(R)$  for the least cardinality of  $X$ , otherwise we write  $d_E(R) = \infty$

**Proposition 5.** *Let  $G$  be a profinite group, and let  $\Phi(G)$  be the Frattini Subgroup of  $G$ . Then  $d(G) = d(G/\Phi(G))$ .*

*Proof.*

Suppose  $X$  is a generating set for  $G$ . Then if  $\psi$  is the natural homomorphism  $\psi : G \rightarrow G/\Phi(G)$ , the image of  $X$  is a generating set for  $G/\Phi(G)$ , hence  $d(G) \geq d(G/\Phi(G))$  because  $|X| \geq |\psi(X)|$ . Now let  $Y \subseteq G$  be such that  $\psi(Y)$  is a minimal set of generators of  $G/\Phi(G)$ . Then  $G = \langle Y \cup \Phi(G) \rangle = \langle Y \rangle$  so  $d(G) \leq d(G/\Phi(G))$ .  $\square$

In the special case that a profinite group  $G$  is a pro- $p$  group, we have the following theorem that will be useful in sections 3 and 4

**Proposition 6.** *Let  $G$  is a finitely generated pro- $p$  group, then*

- (i)  $\Phi(G) = G^p[G, G]$  where  $[G, G]$  is the commutator subgroup of  $G$  and  $G^p$  the group generated by  $\{g^p | g \in G\}$ .
- (ii)  $G/\Phi(G)$  is an elementary abelian group (i.e., abelian as an abstract group) with  $|G/\Phi(G)| = p^{d(G)}$  and if  $K$  is a normal subgroup of  $G$ ,  $\Phi(G/K) = K\Phi(G)/K$ .

*Proof.*

(i)

From Lemma 1, if  $M$  is a maximal open subgroup of  $G$ , we can find  $N \leq M$  such that  $N \triangleleft_O G$ . Suppose  $K/N$  is an open subgroup of  $G/N$  containing  $M/N$ . It follows that  $K$  contains  $M$  and since the natural map  $\varphi : G \rightarrow G/N$  is continuous,  $K$  is open in  $G$ , contradicting the maximality of  $M$ . Thus  $M/N$  is a maximal open subgroup of the finite  $p$ -group  $G/N$ . Since each maximal subgroup in a finite  $p$ -group is normal with index  $p$  (see [8], Chapter 2, Corollary to Theorem 1.6), it follows that  $M \triangleleft G$ , and  $|G : M| = p$ , thus  $G^p[G, G] \leq M$ . Since this is the case for every maximal open subgroup  $M$ , we have

$$\Phi(G) = \bigcap M \geq G^p[G, G]$$

$\Phi(G)$  is closed by Proposition 3, so  $\overline{\Phi(G)} = \Phi(G) \geq \overline{G^p[G, G]}$

Now consider  $Q = G/\overline{G^p[G, G]}$ . Then  $Q$  is a pro- $p$  group with the quotient topology from  $G$ . Therefore  $Q$  is profinite and the intersection  $\bigcap_{N \triangleleft_O Q} N = \{1\}$  from Proposition 1(iii). Suppose  $N \triangleleft_O Q$ , then  $N$  has finite index and so  $Q/N$  is a finite abelian  $p$ -group. Hence  $Q/N$  is cyclic and so  $\Phi(Q/N) = 1$ . Therefore  $\Phi(Q) \leq_{N \triangleleft_O Q} N = 1$  as noted above. Then since  $G^p[G, G] \leq \Phi(G)$  from above, it follows by Proposition 3 (iv) that

$$\Phi(Q) = \Phi(G)/\overline{G^p[G, G]} = 1$$

Hence  $\Phi(G) = \overline{G^p[G, G]}$ . However, if we let  $G^{\{p\}} = \{g^p | g \in G\}$ ,  $G^{\{p\}}$  is closed, since  $G$  is closed, and by Proposition 1.19 in [3],  $[G, G]$  is also closed. Since  $G$  is abelian  $G^p[G, G] = G^{\{p\}}[G, G]$  so  $\Phi(G) = \overline{G^p[G, G]} = G^p[G, G]$ .

(ii)

From (i),  $\Phi(G)$  is generated by all commutators and all  $p$ th powers in  $G$ , so  $G/\Phi(G)$  is elementary Abelian. Being finitely generated,  $G/\Phi(G)$  can be written as a direct product of a direct product finitely many ( $n$ ) cyclic groups of prime power order. This order must be  $p$ , since  $g^p = 1$  for any  $g \in G/\Phi(G)$ , thus  $|G/\Phi(G)| = p^n$  and  $n \leq d(G)$  since  $d(G) = d(G/\Phi(G))$  from Proposition 5. But we can choose a set  $X$  with  $|X| = n$  such that  $X$  maps to a generating set of  $G/\Phi(G)$ , and then  $X$  will generate  $G$  by Proposition 3. Hence  $n \geq d(G)$  by the definition of  $d(G)$ , so  $n = d(G)$ .

Since  $\Phi(G) = [G, G]G^p$ , we have

$$\begin{aligned} \Phi(G/K) &= [G/K, G/K](G/K)^p \\ &= (([G, G]K)/K)((G^p K)/K) \\ &= ([G, G]G^p K)/K \end{aligned}$$

as required. □

**Definition 7 (Presentation).** Let  $G$  be a pro- $p$  group. A presentation of  $G$  is a surjective homomorphism  $\pi : F \rightarrow G$  from a free pro- $p$  group  $F$ . A presentation with  $n$  generators and  $r$  relations is a presentation  $\pi : F \rightarrow G$  with  $d(F) = n$  together with a basis for  $F$  and a set of  $r$  elements which generate  $\ker \pi$  as a normal subgroup of  $F$ .

As one would expect, presentations for a pro- $p$  groups are analogous to presentations for abstract groups and for pro- $p$  groups we can write  $G = \langle X | R \rangle$  where  $X$  is a basis for  $F$ ,  $|X| = n$  and  $R$  is a generating set of  $\ker \pi$  with  $r$  elements. Indeed, when considering the pro- $p$  completion  $\hat{G}$  of an abstract group  $G$ , we find that  $\hat{G}$  has the same presentation (as a pro- $p$  group) as  $G$  (as an abstract group).

**Proposition 7.** Suppose that  $G$  is an abstract group, where  $G = \langle X | R \rangle$ . Then if  $\hat{G}$  is the pro- $p$  completion of  $G$ ,  $\hat{G}$  has the pro- $p$  presentation  $\langle X | R \rangle$ .

*Proof.*

See Proposition 12.1.7 in [9] □

We note that Propostion 7 implies the existence of presentations of  $\mathbb{Z}_p$  (the pro- $p$  completion of the group  $\mathbb{Z} = \langle x | - \rangle$ ) that have one more generator than relations. We will see that these presentations form an important special case for Theorem 2 and the two corollaries.

**Lemma 2.** Let  $G$  be a finitely generated pro- $p$  group and let  $\langle X | R \rangle$  be a presentation of  $G$ , where  $|X| = n$  and  $|R| = r$ . Then there exists a minimal presentation of  $G$ . That is, there exists a presentation of  $G$  with  $d(G)$  generators and  $r - (n - d(G))$  relations.

*Proof.*

We saw in the proof of Proposition 6 that for a pro- $p$  group  $H$ , the quotient  $H/\Phi(H)$  can be regarded as an  $\mathbb{F}_p$ -vector space of dimension  $d(H)$ . Let  $F$  be the free pro- $p$  group of rank  $n$ , and let  $\pi$  be the function  $\pi : F \rightarrow G$  such that  $\ker \pi$  is generated as a normal subgroup of  $F$  by  $R$ . Let  $\Phi(\pi) : F/\Phi(F) \rightarrow G/\Phi(G)$  be the homomorphism induced by  $\pi$  and define  $M$  as the the subgroup of  $F$  such that  $M/\Phi(F) = \ker \Phi(\pi)$ . Then  $M/\Phi(F)$  as a subspace of the  $\mathbb{F}_p$ -vector space  $F/\Phi(F)$ , and is generated by the image of  $R$  in  $F/\Phi(F)$ .

We now have  $\dim(F/\Phi(F)) = n$  and  $\dim(G/\Phi(G)) = d(G)$ , so  $\dim \ker \Phi(\pi) = n - d(G)$ , and if  $r_1\Phi(F), r_2\Phi(F), \dots, r_k\Phi(F)$  is a basis for  $M/\Phi(F)$  with  $r_i \in R$  for  $1 \leq i \leq k$  it follows that  $k = n - d(G)$  and  $\{r_1, \dots, r_k\}$  is a subset of a free basis for  $F$ , since the  $r_i$  are independent modulo  $\Phi(F)$ . Hence  $\bar{F} = \langle F | r_1, \dots, r_k \rangle$  is a free pro- $p$  group on  $d(F) - k = d(G)$  generators, and the image  $S$  of  $R \setminus \{r_1, \dots, r_k\}$  generates the kernel for the presentation  $\pi_1 : \bar{F} \rightarrow G$ . Clearly  $|S| = r - k = r - (n - d(G))$ , as required. □

**Lemma 3.** If  $G$  is a finitely generated discrete group then  $d(\hat{G}) = d_p(G)$ , where  $d_p(G) = \dim_{\mathbb{F}_p}(G/\Phi(G))$ .

*Proof.*

$d(\hat{G}) = d(\hat{G}/\Phi(\hat{G}))$  from Proposition 5. But  $\hat{G}/\Phi(\hat{G}) = \widehat{G/\Phi(G)}$ , so  $d(\hat{G}) = d(\widehat{G/\Phi(G)}) = d(G/\Phi(G)) = d_p(G)$ , since  $G/\Phi(G)$  is an  $\mathbb{F}_p$ -vector space (i.e. the  $d(G/\Phi(G))$  generators form a basis). □

### 3 The Theorems

In this chapter we prove Theorems A and B from Wilson's paper. However, before proving the theorems themselves Wilson proves an auxiliary Lemma and introduces the Zassenhaus filtration and the completed group algebra of a free pro- $p$  group. Note that for most of the following, the ring  $\mathbb{F}_p$  could be replaced with any pro- $p$  ring.

We note that  $\mathbb{F}_p$  (the field with  $p$  elements) is a pro- $p$  ring, corresponding to the inverse system  $(\mathbb{F}_p, \text{Id}_{\mathbb{F}_p})$  indexed by the directed set with just one element. We define a formal power series over  $\mathbb{F}_p$  in non-commuting indeterminates  $y_1, y_2, \dots, y_d$  as an expression

$$\sum_{w \in W} \lambda_w w$$

where  $\lambda_w \in \mathbb{F}_p$  for each  $w$  and

$$W = \{1\} \cup \{y_{i_1} y_{i_2} \dots y_{i_r} \mid r \text{ finite, } 1 \leq i_j \leq d \text{ for each } j\}$$

We call the set  $W$  the set of monomials in  $y_1, \dots, y_d$ . Addition and multiplication of formal power series and multiplication of a formal power series by an element of  $\mathbb{F}_p$  are defined in the usual way, and the set of formal power series over  $\mathbb{F}_p$  forms a  $\mathbb{F}_p$ -algebra.

We call a  $\mathbb{F}_p$ -algebra a *profinite  $\mathbb{F}_p$ -algebra* if it is the inverse limit of an inverse system of finite  $\mathbb{F}_p$ -algebras and  $\mathbb{F}_p$ -algebra homomorphisms. If  $G$  is a profinite group (in particular, a pro- $p$  group) then the *Completed Group Algebra* of  $G$  over  $\mathbb{F}_p$ , denoted  $F_p[[G]]$  is a profinite  $\mathbb{F}_p$ -algebra containing  $G$  in its group of units and defined by the following universal property: Each continuous group homomorphism from  $G$  to the group of units  $E^\times$  of a profinite  $\mathbb{F}_p$ -algebra  $E$  extends uniquely to a continuous  $\mathbb{F}_p$ -algebra homomorphism from  $F_p[[G]]$  to  $E$ .

The following theorem demonstrates the link between the above objects:

**Theorem 4.** *Let  $P$  be the formal power series algebra over  $\mathbb{F}_p$  in non-commuting indeterminates  $y_1, \dots, y_d$ , and write  $x_i = 1 + y_i$  for  $1 \leq i \leq d$ . Then the profinite subgroup  $F$  of  $P^\times$  (the group of units of  $P$ ) generated by  $x_1, \dots, x_d$  is the free pro- $p$  group with basis  $x_1, \dots, x_d$ , and  $P$  is the completed group algebra  $\mathbb{F}_p[[F]]$  of  $F$ .*

*Proof.*

We have noted that  $\mathbb{F}_p$  is a pro- $p$  ring. Hence this theorem is a special case of Theorem 7.3.3 on page 121 of [9].  $\square$

Let  $F$  be as in the above theorem. Define the ideal  $I_1$  to be the set of power series in  $\mathbb{F}_p$  that have no constant term (that  $I_1$  is an ideal is clear), and define  $I_n = I_1^n$ ,  $n \geq 2$ . That is, any element of  $I_n$  has  $\lambda_w = 0$  for every  $w$  which is the product of less than  $n$  elements of  $\{y_1, \dots, y_d\}$ . Then we define the *Zassenhaus filtration* of  $F$  as the descending chain

$$F = F_1 \geq F_2 \geq F_3 \geq \dots$$

of (closed) normal subgroups of  $F$  where, for each  $n$

$$F_n = \{g \in F; g - 1 \in I_n\}$$

We say that an element  $g \in F \setminus \{1\}$  has degree  $n$  with respect to this filtration if  $g \in F_n \setminus F_{n+1}$ .

**Lemma 4.** *Let  $F$  be the free pro- $p$  group on  $d$  generators.*

(a)  $\Phi(F) \leq F_2$

(b) *If  $G \cong F/R$  and  $d(G) = d$  then  $R \leq F_2$*

*Proof.*

(a)

Let  $s_1, s_2$  be elements of  $I_1$ . Then  $s_1s_2 - s_2s_1 \in I_2$ , by definition of  $I_2$  and so  $P/I_2$  is commutative. Therefore if  $u_1, u_2 \in F$ , then  $u_1^{-1}u_2^{-1}u_1u_2 \equiv u_1^{-1}u_2^{-1}u_2u_1 \equiv 1$  modulo  $I_2$ . Also,  $u_1^p = u_1 - 1 + 1 = u_1^p - 1^p + 1 = (u_1 - 1)^p + 1$  since each of the coefficients of the terms  $\pm u^j$  for  $1 < j < p$  is divisible by  $p$  and hence 0 in  $P$ . Thus  $u^p \in I_p \leq I_2$ . Since  $\Phi(F) = F^p[F, F]$  (Proposition 6,  $\Phi(F) \leq 1 + I_2$ ).

(b)

We know from Proposition 6(ii) that  $|G/\Phi(G)| = p^{d(G)}$  and  $|F/\Phi(F)| = p^d$ . Thus if we consider the diagram:

$$\begin{array}{ccc} F & \xrightarrow{\pi} & G \\ | & & | \\ p^d | & & | p^d \\ | & & | \\ \Phi(F) & \xrightarrow{\pi'} & \Phi(G) \end{array}$$

We find that

$$\begin{aligned} F/\Phi(F) &\cong G/\Phi(G) \\ &\cong (F/R)/\Phi(F/R) \\ &\cong (F/R)/(R\Phi(F)/R) \\ &\cong F/R\Phi(F) \end{aligned}$$

so  $R \leq \Phi(F) \leq 1 + I_2$  from part (a). □

Wilson uses the following Lemma (Lemma 5) to prove Theorem A'. We prove a variant, Lemma 6, part (b) of which leads to Wilson's Lemma.

**Lemma 5.** *Let  $F$  be a free pro- $p$  group on  $d$  generators and let  $\{S_n; n \geq 2\}$  be a family of disjoint finite subsets such that  $S_n$  consists of elements of degree at least  $n$  for each  $n$  (relative to the Zassenhaus filtration). Let  $R$  be the (closed) normal subgroup of  $F$  generated by  $\bigcup\{S_n; n \geq 2\}$ , and define the real power series  $\psi(t)$  by*

$$\psi(t) = 1 - dt + r_2t^2 + r_3t^3 + \dots$$

where  $r_n = |S_n|$  for each  $n$ . Suppose that  $\psi(t)$  is convergent for  $0 < t < 1$ , if the group  $G = F/R$  is finite, then  $\psi(t) > 0$  for  $0 < t < 1$ .

For the following we let  $\delta(v)$  denote the smallest integer  $n$  such that  $v \in I_n \setminus I_{n+1}$  and define  $\delta(0) = \infty$ .

**Lemma 6.** *Let  $S$  be a subset of  $I_1$ . Define  $S_k = \{v \in S | \delta(v) = k\}$  and suppose that each  $S_k$  is finite. We write  $s_k = |S_k|$  and let  $J$  be the closed ideal of  $R$  generated by  $S$ .*

(a) Set  $c_k = \dim(P/(J + I_{k+1}))$  for  $k \geq 0$ . Then

$$c_k - 1 \geq dc_{k-1} - \sum_{j=1}^k s_{jk} c_{k-j} \quad (3)$$

for  $k \geq 1$ .

(b) Define the power series

$$\sigma_S(t) = \sum_{i \geq 1} s_i t^i$$

and let  $t$  be an element of  $[0,1]$  such that  $\sigma_S(t)$  converges. If  $I_n \leq J$  for some  $n$  then  $\psi(t) > 0$ .

*Proof.*

We first show that (b) follows from (a).

Let

$$\gamma(t) = \sum_{k=0}^{\infty} c_k t^k$$

then by multiplying (3) by  $t^k$  and summing over  $k$ , we get

$$\begin{aligned} \sum_{k=0}^{\infty} (c_k t^k - t^k) &\geq \sum_{k=1}^{\infty} \left( dc_{k-1} t^k - t^k \sum_{j=1}^k s_{jk} c_{k-j} \right) \\ \Rightarrow \sum_{k=0}^{\infty} c_k t^k - \sum_{k=0}^{\infty} t^k &\geq t \sum_{k=0}^{\infty} dc_k t^k - \sum_{k=1}^{\infty} \sum_{j=1}^k s_{jk} c_{k-j} t^k \\ \Rightarrow \gamma(t) - (1-t)^{-1} &\geq dt\gamma(t) - \left( \sum_{j=1}^{\infty} s_j t^j \sum_{k=0}^{\infty} c_k t^k \right) \\ &= dt\gamma(t) - \sigma_S(t)\gamma(t) \end{aligned}$$

From which it follows

$$\gamma(t)(1 - dt + \sigma_S(t)) \geq (1-t)^{-1} \quad (4)$$

Provided  $\gamma(t)$  and  $\sigma_S(t)$  converge.

Define  $b_k$  such that

$$b_k = \begin{cases} 1; & k = 0 \\ c_k - c_{k-1}; & k \geq 1 \end{cases}$$

and set  $\beta(t) = \sum_{k=0}^{\infty} b_k t^k$ . Since there is an  $n$  such that  $I_n \leq J$ , then  $c_n - c_{n-1} = \dim(P/(J + I_{n+1})) - \dim(P/(J + I_n)) = \dim(P/J) - \dim(P/J) = 0$ . So  $\beta(t)$  is a polynomial. Also,

$$\begin{aligned} \sum_{i=0}^k b_i &= 1 + \sum_{i=1}^k (c_i - c_{i-1}) \\ &= 1 + \sum_{i=1}^k c_i - \sum_{i=0}^{k-1} c_i \\ &= 1 + c_k - c_0 \\ &= 1 + c_k - \dim(P/(J + I_1)) \\ &= c_k \end{aligned}$$

since  $P/(J+I_1)$  is the ring power series with only constant terms, that is  $P/(J+I_1) = \mathbb{F}_p$ . Then  $\sum_{k=0}^{\infty} c_k t^k = \sum_{k=0}^{\infty} \sum_{i=0}^k b_k t^k = \sum_{k=0}^{\infty} b_k \sum_{k=0}^{\infty} t^k = \beta(t)(1-t)^{-1}$ . Hence  $\gamma(t)$  is a rational function with no poles on  $[0, 1)$  and is therefore convergent on  $[0, 1)$ . So if  $\sigma_S(t)$  converges on  $[0, 1)$  (4) gives us

$$\begin{aligned} \gamma(t)(1-dt+\sigma_S(t)) &\geq (1-t)^{-1} \\ \Rightarrow \frac{\beta(t)}{1-t}(1-dt+\sigma_S(t)) &\geq (1-t)^{-1} \\ \Rightarrow 1-dt+\sigma_S(t) &\geq \frac{1}{\beta(t)} \\ \Rightarrow 1-dt+\sigma_S(t) &> 0 \end{aligned}$$

Since  $\beta(t)$  has purely positive coefficients (because  $J+I_{k+1} \leq J+I_k$ ), and is therefore positive on  $[0, 1)$ .

Recall that Abel's Convergence Theorem (see [1], Theorem 13-33) states that if a real power series converges for some positive value of the argument then the domain of uniform convergence extends up to and including the point and the sum is continuous up to and including the point. In particular, if  $f(z) = \sum_{n=0}^{\infty} \alpha_n x^n$ , and  $f(1)$  is convergent then  $f(1) = \lim_{x \rightarrow 1^-} f(x)$ . Applying this to  $\sigma_S(t)$  gives us that if  $\sigma_S(1)$  is convergent then  $\sigma_S(1) = \lim_{t \rightarrow 1^-} \sigma_S(t)$ , and so  $1-d+\sigma_S(1) > 0$  by continuity. This closes the interval  $[0, 1]$  and completes the proof of (b).

Now we prove (a). First we observe that if  $v \in I_1$  then we can find uniquely determined elements  $u_1, \dots, u_d \in P$  such that  $v = \sum_{i=1}^d u_i y_i$ . We see this by considering each indeterminate  $y_i$  and 'factoring'  $v$  with respect to that indeterminate by removing each monomial that does not end with  $y_i$  and then right multiplying the series by  $y_i^{-1}$  term by term. Thus we obtain a series  $u_i = \sum_{w_i \in W_*} \lambda_{w_i} w_i$  such that  $u_i y_i$  gives every term in  $v$  ending with  $v$ . When we consider this for all  $d$  indeterminates  $y_i$ , the sum  $\sum_{i=1}^d u_i y_i$  clearly gives us the series  $v$  except for any constant terms  $v$  may have. But since  $v \in I_1$ ,  $v$  has no constant terms and so  $\sum_{i=1}^d u_i y_i = v$ .

Fix  $k \geq 1$ , write  $\bigcup_{j \leq k} S_j = \{z_1, \dots, z_m\}$ . That is, the  $z_i$  are all the elements belonging to some set  $I_n \setminus I_{n+1}$  for  $n \leq k$ . We order the  $z_i$  such that  $\delta(z_{i+1}) \geq \delta(z_i)$  and set  $k_i = \delta(z_i)$  for each  $i$ . Define

$$\bar{A} = \bigoplus_{i=1}^m P/(J+I_{k-k_i+1})$$

and let  $\bar{B}$  be the direct sum of  $d$  copies of  $P/(J+I_k)$ . Since  $\sum_{j=1}^k = m$  we get

$$\sum_{j=1}^k s_j c_{k-j} = \sum_{i=1}^m c_{k-k_i}$$

Since for the first  $s_1$  elements  $u$  of the right hand series,  $k_u = k_1 = 1$ , for the second second  $s_2$  elements of the series  $k_u = k_2 = 2$  and so on, due to the

ordering of the union above. Since  $c_k = \dim(P/(J + I_{k+1}))$ , we have

$$\begin{aligned} \sum_{i=1}^m c_{k-k_i} &= \sum_{i=1}^m \dim(P/(J + I_{k-k_i+1})) \\ &= \dim\left(\bigoplus_{i=1}^m P/(J + I_{k-k_i+1})\right) \\ &= \dim \bar{A} \end{aligned}$$

Hence we need to prove

$$c_k - 1 \geq dc_{k-1} - \dim \bar{A}$$

We do this by showing the existence of an exact sequence

$$\bar{A} \xrightarrow{\varphi} \bar{B} \xrightarrow{\psi} I_1/(J + I_{k+1}) \xrightarrow{\vartheta} 0$$

of  $\mathbb{F}_p$  vector spaces and linear maps, since this will give

$$\begin{aligned} dc_{k-1} &= \sum_{i=1}^d c_{k-1} \\ &= \sum_{i=1}^d \dim(P/(J + I_k)) \\ &= \dim\left(\bigoplus_{i=1}^d P/(J + I_k)\right) \\ &= \dim \bar{B} \\ &= \dim \operatorname{im} \psi + \dim \ker \psi \\ &= \dim \ker \vartheta + \dim \operatorname{im} \varphi \\ &= \dim(I_1/(J + I_{k+1})) + \dim \operatorname{im} \varphi \\ &= \dim(P/(J + I_{k+1})) - 1 + \dim \operatorname{im} \varphi \\ &= c_k - 1 + \dim \operatorname{im} \varphi \\ &\leq c_k - 1 + \dim \bar{A} \end{aligned}$$

Define  $A = \bigoplus_m P$ , and  $B = \bigoplus_d P$ . That is  $A$  and  $B$  represent the direct sums of  $m, d$  copies of  $P$  respectively. We construct the following commutative diagram:

$$\begin{array}{ccccc} A & \xrightarrow{\Phi} & B & \xrightarrow{\Psi} & I_1 \\ \downarrow q_1 & & \downarrow q_2 & & \downarrow q_3 \\ \bar{A} & \xrightarrow{\varphi} & \bar{B} & \xrightarrow{\psi} & I_1/(J + I_{k+1}) \end{array}$$

Where the vertical maps  $q_1, q_2, q_3$  are the obvious ones coming from the quotient. We define a surjective linear map

$$\Psi : B \rightarrow I_1; \quad (u_1, \dots, u_d) \mapsto \sum_{i=1}^d u_i y_i$$

and a linear map

$$\Phi : A \rightarrow B; \quad (v_1, \dots, v_m) \mapsto (w_1, \dots, w_d)$$

where  $w_1, \dots, w_d$  are the elements of  $P$  uniquely determined by  $\sum_{j=1}^m m v_j z_j = \sum w_i y_i$  as described above. It is clear that if  $u_1, \dots, u_d \in J + I_k$  then  $\sum_{i=1}^d u_i y_i \in J + I_k$ , from the definition of  $I_k$ . So if  $\alpha = (u_1, \dots, u_d) \in B$  then

$$\begin{aligned} \alpha &\in \ker q_2 \\ \Rightarrow \alpha &\in \bigoplus_d J + I_k \\ \Rightarrow \Psi(\alpha) &\in J + I_{k+1} \\ \Rightarrow q_3(\Psi(\alpha)) &= 0_{I_1/(J+I_{k+1})} \\ \Rightarrow \alpha &\in \ker(q_3\Psi) \end{aligned}$$

Therefore  $\ker q_2 \leq \ker(q_3\Psi)$ , and  $\Psi$  induces a surjective linear map  $\psi$  such that the right hand square is commutative. Since each  $z_j \in I_1$ , we can write  $z_j = \sum_{i=1}^d g_{ij} y_i$  for each  $j \leq m$ . Then if  $v_j \in J + I_{k-k_j+1}$  for each  $j \leq m$  we have

$$\begin{aligned} \sum_{j=1}^m v_j z_j &= \sum_{i=1}^d \left( \sum_{j=1}^m v_j g_{ij} y_i \right) \\ &= \sum_{i=1}^d \left( \sum_{j=1}^m v_j g_{ij} \right) y_i \end{aligned}$$

and  $v_1 g_{i1} \in J + I_k$  (since  $k_1 = 1$ ) so  $\sum_{j=1}^m v_j g_{ij} \in J + I_k$ . Hence if  $\beta = (v_1, \dots, v_m) \in \ker q_1$  then

$$\begin{aligned} \Phi(\beta) &= \sum_{i=1}^d w_i y_i \\ &= \sum_{i=1}^d \left( \sum_{j=1}^m v_j g_{ij} \right) y_i \\ \Rightarrow w_i &\in J + I_k \\ \Rightarrow q_2(\Phi(\beta)) &= 0 \\ \Rightarrow \beta &\in \ker(q_2\Phi) \end{aligned}$$

Therefore  $\ker q_1 \leq \ker q_2\Phi$ , so  $\Phi$  induces a linear map  $\varphi$  such that the left hand square is commutative.

For any element  $a = (v_1, \dots, v_m) \in A$  we have

$$\begin{aligned} \Phi(a) &= (w_1, w_2, \dots, w_d) \text{ where } \sum_{j=1}^m v_j z_j = \sum_{i=1}^d w_i y_i \\ \Rightarrow \Psi\Phi(a) &= \sum_{i=1}^d w_i y_i \\ &= \sum_{j=1}^m v_j z_j \end{aligned}$$

and since each of the  $z_j \in S$ ,  $\Psi\Phi(a) \in J$ . Hence  $\psi\varphi q_1(a) = q_3\Psi\Phi(a) = 0$  and since  $q_1$  is surjective,  $\text{im } q_1 = \bar{A}$ . Therefore  $\psi\varphi(a) = 0$  and so  $\text{im } \varphi \leq \ker \psi$ .

We now need only check that  $\ker \psi \leq \text{im } \varphi$ . Let  $\bar{b} \in \ker \psi$  such that  $\bar{b} = q_2(u_1, \dots, u_d)$ . So  $0 = \psi q_2(u_1, \dots, u_d)$  and  $\sum_{i=1}^d u_i y_i \in J + I_{k+1}$ . We now write

$$J + I_{k+1} = \sum_{j \leq m} Pz_j + J_1 + I_{k+1}$$

where  $J_1$  is the ideal generated by the elements  $z_j y_i$  with  $j \leq m$ ,  $i \leq d$ . Let  $\sum_{i=1}^d u_i y_i = \sum_{j \leq m} v_j z_j + f$  with  $f \in J_1 + I_{k+1}$ , so from the above remark we can write  $f = \sum_{i=1}^d h_i y_i$  with  $h_i \in J + I_k$  for each  $i$ , and we also write  $\sum_{j=1}^d v_j z_j = \sum_{i=1}^m u'_i y_i$ . Hence we have  $\sum_{i=1}^d u_i y_i = \sum_{i=1}^d (u'_i + h_i) y_i$  and so  $u_i = u'_i + h_i$  for each  $i$ . Therefore

$$\begin{aligned} \bar{B} = q_2(u_1, \dots, u_d) &= q_2(u'_1, \dots, u'_d) + q_2(h_1, \dots, h_d) \\ &= q_2(u'_1, \dots, u'_d) \text{ since } h_i \in \ker q_2 \\ &= q_2\Phi(v_1, \dots, v_m) \text{ from the definition of } \Phi \\ &= \varphi q_1(v_1, \dots, v_m) \\ &\in \text{im } \varphi \end{aligned}$$

So  $\ker \psi \leq \text{im } \varphi$ . Hence we have the required exact sequence

$$\bar{A} \xrightarrow{\varphi} \bar{B} \xrightarrow{\psi} I_1/(J + I_k) \longrightarrow 0$$

and the result follows.  $\square$

Wilson proves Theorem A as a special case of a more general theorem, which he denotes Theorem A'.

**Theorem 5** (Theorem A'). *Suppose that  $G = F/R$  where  $F$  is the free pro- $p$  group of rank  $d > 1$  and where  $R$  is the (closed) normal subgroup generated by  $U = \{u_1, u_2, \dots, u_r\}$ . If  $U$  is contained in  $F_{m'}$  (where  $m \geq 2$  and  $(F_i)$  is the Zassenhaus filtration of  $F$ ), and if*

$$r < \frac{(m-1)^{m-1}}{m^m} d^m \quad (5)$$

*then for each finitely generated dense discrete subgroup  $X$  of  $G$  there is a closed normal subgroup  $K$  of  $G$  such that  $XK/K$  is an infinite torsion group.*

To show that Theorem A is a special case of Theorem A' we use Lemma 2<sup>1</sup> to take the presentation of  $G$  to be  $\langle X'|R' \rangle$  where  $|X'| = d(G)$  and  $|R'| = r - (n - d(G))$ , and applying Theorem A' where  $m = 2$  (since  $R \leq F_2$  by Lemma 4) gives that if

$$\begin{aligned} r - (n - d) &< \frac{1}{4} d^2 \\ \iff r &< n + \frac{1}{4} d^2 - d \end{aligned}$$

<sup>1</sup>Wilson quotes this lemma incorrectly, saying that  $G$  has a presentation with  $d(G)$  generators and  $r - (d(G) - n)$  relations. Clearly this would result in a smaller group than  $G$  (or equal if  $d(G) = n$ , as it would have fewer generators and more relations. He does, however, use the lemma correctly.

Then for each finitely generated dense discrete subgroup  $Y$  of  $G$  there is a closed normal subgroup  $K$  of  $G$  such that  $XK/K$  is an infinite torsion group. This is obviously Theorem A.

### 3.1 Proof of Theorem A'

Let  $\varepsilon \geq 0$  and condition the function

$$\psi_\varepsilon(t) = 1 - dt + rt^m + \frac{\varepsilon t^m}{1-t}$$

We show that  $\psi_0(t_1) < 0$  for some  $t_1 \in (0, 1)$ . Note that if  $t_0 = \left(\frac{d}{mr}\right)^{\frac{1}{m-1}}$  then

$$\begin{aligned} \psi_0(t_0) &= 1 - d \left(\frac{d}{mr}\right)^{\frac{1}{m-1}} + r \left(\frac{d}{mr}\right)^{\frac{m}{m-1}} \\ &= 1 - \left(\frac{d^m}{mr}\right)^{\frac{1}{m-1}} + \left(\frac{d}{mr}\right)^{\frac{m}{m-1}} \\ &= 1 - d^{\frac{m}{m-1}} \left( \left(\frac{1}{mr}\right)^{\frac{1}{m-1}} + \left(\frac{1}{mr}\right)^{\frac{m}{m-1}} \right) \end{aligned}$$

From (5) we get

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

Hence

$$\begin{aligned} \psi_0(t_0) &< 1 - \frac{(rm^m)^{\frac{1}{m-1}}}{m-1} \left( \left(\frac{1}{mr}\right)^{\frac{1}{m-1}} + \left(\frac{1}{mr}\right)^{\frac{m}{m-1}} \right) \\ &= 1 - \frac{1}{m-1} \left( \left(\frac{rm^m}{mr}\right)^{\frac{1}{m-1}} + \left(\frac{r^{\frac{1}{m}}m}{mr}\right)^{\frac{m}{m-1}} \right) \\ &= 1 - \frac{1}{m-1} \left( (m^{m-1})^{\frac{1}{m-1}} + \left(\frac{r^{\frac{1}{m}}}{r}\right)^{\frac{m}{m-1}} \right) \\ &= 1 - \frac{1}{m-1} \left( m + (r^{-\frac{m-1}{m}})^{\frac{m}{m-1}} \right) \\ &= 1 - \frac{m+1}{m-1} \\ &= 1 - \left( 1 + \frac{2}{m-1} \right) \\ &< 0 \end{aligned}$$

Suppose that there does not exist  $t_1$  such that  $\psi_0(t_1) < 0$ . Then  $t_0$  must be greater than 1, so  $d > mr$ , and

$$0 \leq \psi_0(1) = 1 - d + r$$

by the continuity of  $\psi_0$ , but

$$\begin{aligned} 1 - d + r &< 1 - d + \frac{d}{m} \\ &< 1 - d \left(1 - \frac{1}{m}\right) \\ &\leq 1 - \frac{d}{2} \\ &\leq 0 \end{aligned}$$

Since  $m, d \geq 2$ . Hence  $0 \leq \psi_0(1) < 0$ , a contradiction. Therefore there exists  $t_1 \in (0, 1)$  with  $\psi_0(t_1) < 0$  and by continuity there is a positive  $\varepsilon$  such that  $\psi_\varepsilon(t_1) < 0$ . Now choose  $q \in \mathbb{Z}$  such that  $q\varepsilon \geq 1$ .

We now list all the elements  $\bar{s}_1, \bar{s}_2, \dots$  of  $X$  and choose for each  $\bar{s}_i$  a preimage  $s_i \in F$ . Set  $v_i = s_i^{p^{iq+m}}$  for each  $i$ . Then, calculating in the formal power series ring  $A$  (see above), we see that

$$(s_i - 1)^{p^{iq+m}} = \sum_{k=0}^{p^{iq+m}} \binom{p^{iq+m}}{k} s_i^{p^{iq+m}-k} + (-1)^k$$

But for  $k \neq 0$  or  $p^{iq+m}$  the coefficient  $\binom{p^{iq+m}}{k} = 0$  in  $A$ . Hence

$$(s_i - 1)^{p^{iq+m}} = s_i^{p^{iq+m}} - 1 = v_i - 1$$

Moreover, since the  $s_i \in F$ ,  $s_i$  is a word over the alphabet  $\{1+x_1, 1+x_2, \dots, 1+x_d\}$ . Hence, regarded as a power series, each  $s_i$  has constant term 1, and so  $(s_i - 1) \in I$ . Therefore

$$v_i - 1 = (s_1 - 1)^{p^{iq+m}} \in I_{p^{iq+m}} \leq I_{iq+m}$$

and since  $p$  is prime,  $v_i \notin I_n$  for  $n < iq + m$ . Thus  $v_i$  has degree  $iq + m$  with respect to the Zassenhaus filtration. Now consider the set  $S = U \cup \{v_i; i \geq 1\}$ . Since  $U \subset F_m$ , all the elements of  $U$  have degree at least  $m$ . Thus we can write  $S = U \cup_{i \in \mathbb{N}} \{v_i\}$ , where each of the  $v_i$  are disjoint from each other and  $U$ , so that  $S$  satisfies the conditions for the set  $\{S_n; n \geq 2\}$  in Lemma 5 (note that for  $n = 2 \dots m - 1$  the set  $S_n$  is empty). Let  $R_+$  be the (closed) normal subgroup of  $F$  generated by  $S$  and suppose that the quotient group  $F/R_+$  is finite. Then from Lemma 5,  $\phi(t_1) > 0$  where

$$\phi(t) = 1 - dt + r_2 t^2 + r_3 t^3 + \dots = 1 - dt + r t^m + t^m \sum_{i=1}^{\infty} t^{qi} \quad (6)$$

Since  $r_j = |S_j|$  and we have seen that  $|S_j| = 0$  for  $j = 2 \dots m - 1$ , also  $|S_m| = |U| = R$  and  $|S_j| = |\{v_j\}| = 1$  for  $j = iq + m$ .<sup>2</sup> However, for  $t \in (0, 1)$  we have  $t^q \leq t^k$  for  $k < q$  so

$$\begin{aligned} qt^q &\leq 1 + t + t^2 + \dots + t^{q-1} \\ \Rightarrow t^q &\leq \frac{1}{q}(1 + t + \dots + t^{q-1}) \\ &\leq \varepsilon(1 + t + \dots + t^{q-1}) \end{aligned}$$

<sup>2</sup>In the paper, Wilson leaves out the  $t^m$  coefficient for the sum in equation (6). This appears to be a typographical error.

since  $\varepsilon \geq \frac{1}{q}$ . Combining this with (6) we get

$$\begin{aligned}\phi(t) &\leq 1 - dt + rt^m + \varepsilon t^m \sum_{k=0}^{\infty} t^k \\ &= 1 - dt + rt^m + \frac{\varepsilon t^m}{1-t} \\ &= \psi_\varepsilon(t)\end{aligned}$$

But we have shown that  $\phi_\varepsilon(t_1) < 0$ , for  $t_1 \in (0, 1)$ . It follows from this contradiction that  $F/R_+$  must be infinite. Since  $U \subset S$ ,  $R_+ \geq R$  and  $F/R_+ \leq F/R$ , so  $G$  is infinite as well. Moreover, for each element  $s_i, s_i^{p^{iq+m}} \in S$  and so  $\bar{s}_i^{p^{iq+m}} = 1_{F/R_+}$  by homomorphism. Hence the image in  $F/R_+$  of the subgroup  $X$  of  $G$  is periodic, and since  $X$  is dense in  $G$ , the image of  $X$  must be infinite as well. Finally, taking  $K$  as the kernel of the map from  $G$  to  $F/R_+$  makes  $K$  normal, and  $XK/K$  is the image of  $X$  in  $F/R_+$ . This completes the proof.

### 3.2 Proof Theorem B

Suppose that  $G$  is a discrete group which has a finite presentation with  $n$  generators and  $r$  relations, and let  $d = d(G/[G, G])$  (where  $[G, G]$  is the commutator subgroup of  $G$ , so that  $G/[G, G] = G^{ab}$ ).

Because  $G/[G, G]$  is a finitely generated abelian group, we can write

$$G/[G, G] = (\mathbb{Z})^m \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \dots \oplus \mathbb{Z}_{n_k}$$

Where  $n_1 | n_2 | \dots | n_k$ . In particular, this representation gives the least number of generators for  $G/[G, G]$  (i.e.  $d(G/[G, G]) = m + k$ ) Thus there exists a prime  $p$  (any prime that divides  $n_1$ ) such that  $p | n_i$  for all  $i$ , and we can write

$$G/[G, G]G^p = (\mathbb{Z})^m \oplus \mathbb{Z}_{n_1/p} \oplus \mathbb{Z}_{n_2/p} \oplus \dots \oplus \mathbb{Z}_{n_k/p}$$

and so  $d(G/[G, G]G^p) = m + k = d(G/[G, G])$ .

Let  $\hat{G}$  be the pro- $p$  completion of  $G$ . From Lemma 3 we have  $d(\hat{G}) = d(G/[G, G]G^p)$ . We noted above that there exist presentations of  $\mathbb{Z}_p$  with one more generator than relations.  $\mathbb{Z}$  is abelian and has presentation  $\langle x | - \rangle$ , so  $d(\mathbb{Z}^{ab}) = 1$  and so Theorem A implies that

$$r \geq r + 1 + \frac{1}{4} - 1 = r + \frac{1}{4}$$

Clearly this is a contradiction, but the quotient of  $\mathbb{Z}$  by any subgroup  $K$  is finite,  $\mathbb{Z}/K$  is not an infinite residually finite  $p$ -torsion group. So we add an extra summand  $-\frac{1}{4}$  to equation 1 to include these presentations of  $\mathbb{Z}_p$ .

Using this modification and applying Theorem A to  $d(\hat{G})$ , we have either

$$r \geq n + \frac{1}{4}(d^2 - 1) - d$$

or there is a closed normal subgroup  $\bar{K}$  of  $\hat{G}$  such that the image of  $G$  in  $\hat{G}/\bar{K}$  is an infinite torsion group. Since  $\hat{G}/\bar{K}$  is a pro- $p$  group, the image must be a  $p$ -torsion group, and is residually finite from Theorem 1(iii)

## 4 The Corollaries

To prove the two corollaries in Wilson's paper we use the Lemma 7. For this Lemma we make use of a *right transversal* to a closed subgroup  $H$  of  $G$ , defined as a closed subset of  $G$  containing precisely one element from each right coset  $gH$  in  $G$ . We also need the following theorem:

**Theorem 6.** *Let  $F$  be the free pro- $\mathcal{C}$  group on the set  $X$  and let  $H$  be an open subgroup of  $F$ . Then there is a right transversal  $T$  to  $H$  in  $F$  such that  $H$  is the free pro- $\mathcal{C}$  group with basis*

$$\{t_1xt_2^{-1} \mid x \in X, t_1, t_2 \in T, t_1xt_2^{-1} \in H \setminus 1\}$$

Moreover, if  $X$  is finite, then the ranks  $r_F = |X|$  and  $r_H$  satisfy  $|F : H|(r_F - 1) = r_H - 1$ .

*Proof.*

The proof of this theorem can be found in [9], Theorem 5.4.4 □

**Lemma 7.** *Let  $G$  be a group (pro- $p$  or discrete) having a presentation with  $n$  generators and  $r$  relations, and let  $H$  be a subgroup of finite index  $h$ . Then  $H$  has a presentation with  $hn - (h - 1)$  generators and  $hr$  relations.*

*Proof.*

Let  $\pi : F \rightarrow G$  be a presentation with  $F$  free of rank  $d$  and let  $R = \ker \pi$  be generated as a normal subgroup by  $u_1, u_2, \dots, u_r$  (as in the definition of a presentation). Then let  $F_1$  be the preimage of  $H$  in  $F$  and denote the induced map from  $F_1$  to  $H$  by  $\pi_1$ . Then  $R = \pi_1^{-1}(1)$  ( $= \ker \pi_1$ ) is a normal subgroup of  $F_1$ , and  $|F : F_1| = h$ , since  $|F/R : F_1/R| = h$ . So by Theorem 6 (below)  $F_1$  is free of rank  $hn - (h - 1)$ . Let  $\{t_1, t_2, \dots, t_h\}$  be a left transversal of  $H$  in  $F$ , so  $F = \bigcup_{i=1}^h t_i F_1$  since there is exactly one  $t_i$  for each of the  $h$  cosets of  $H$ . So for any  $f \in F$ , there is some  $t_i$  such that  $fF_1 = t_i F_1$  and hence some  $k \in F_1$  such that  $t_i k = f$ . So for any conjugate  $f^{-1}u_j f$  with  $f$  in  $R$ , there is a conjugate of some  $t_i^{-1}u_j t_i$  under an element of  $F_1$  (namely  $k$ ). Hence  $R$  is generated by  $R_1 = \{t_j^{-1}u_i t_j \mid i \leq r, j \leq h\}$ , and  $|R_1| = hr$  as required. □

Wilson presents two corollaries of the main results:

**Corollary 1 (Corollary A).** *Let  $G$  be a finitely presented pro- $p$  group and assume that there do not exist a closed subgroup  $K$  of  $G$  and a finitely generated discrete subgroup  $X$  of  $G$  normalizing  $K$  such that  $XK/K$  is an infinite torsion group. Then*

- (i) *there is a constant  $k > 0$  such that  $d(H) \leq k|G : H|^{\frac{1}{2}}$  for each open subgroup  $H$  of  $G$ , and*
- (ii) *if  $N$  is any (closed) normal subgroup of  $G$  such that  $G/N \cong \mathbb{Z}_p$ , then  $N$  is finitely generated*

**Corollary 2 (Corollary B).** *Let  $G$  be a finitely presented discrete group and assume that there do not exist a prime  $p$  and subgroups  $X, K$  such that  $K \triangleleft X$  and  $X/K$  is an infinite finitely generated residually finite  $p$ -torsion group. Then there is a constant  $k > 0$  such that  $d(H^{ab}) \leq k|G : H|^{\frac{1}{2}}$  for each subgroup of finite index in  $G$ .*

Note that Corollary 2 is essentially Corollary 1(i) in the case of discrete groups, each of which we now prove.

*Proof of Corollary 1(i):*

Let  $G$  satisfy the conditions for Corollary A with a presentation having  $n$  generators and  $r$  relations. Let  $H$  be an open subgroup of  $G$  with index  $h$  that is not isomorphic<sup>3</sup> to  $\mathbb{Z}_p$ . Then by Lemma 7,  $H$  has a presentation with  $hn - (h - 1)$  generators and  $hr$  relations. We see that the conditions for Corollary 1(i) rule out the second alternative of Theorem A, so if we apply Theorem A to  $H$  we must have

$$\begin{aligned}
hr &\geq hn - (h - 1) + \frac{1}{4}d(H)^2 - d(H) \\
\Rightarrow 4(hr - (hn + h)) &\geq d(H)^2 - 4d(h) + 4 \\
\Rightarrow 4h(r - n + 1) &\geq (d(H) - 2)^2 \\
\Rightarrow 2h^{\frac{1}{2}}(r - n + 1)^{\frac{1}{2}} &\geq d(H) - 2 \\
\Rightarrow h^{\frac{1}{2}}(2(r - n + 1)^{\frac{1}{2}} + 2) &\geq d(H) \\
\Rightarrow h^{\frac{1}{2}}(2(r - n + 1)^{\frac{1}{2}} + 2) &\geq d(H) \\
\Rightarrow d(H) &\leq kh^{\frac{1}{2}} \\
&= k|G : H|^{\frac{1}{2}}
\end{aligned}$$

Now suppose that  $H$  is isomorphic to  $\mathbb{Z}_p$ , we have seen that  $d(H) = 1$ , so the conclusion  $d(H) \leq k|G : H|^{\frac{1}{2}}$  is immediate since  $|G : H| \geq 1$ . This concludes the proof.  $\square$

The proof of Corollary 2, which Wilson omits, is very similar.

*Proof of Corollary 2:*

Let  $G$  satisfy the conditions of Corollary 2 (ruling out the second part of Theorem B), where  $G$  has  $n$  generators and  $r$  relations. Then let  $H$  be a subgroup of  $G$  with index  $h$ . By Lemma 7  $H$  has a presentation with  $hn - (h - 1)$  generators and  $hr$  relations. Applying Theorem B to  $H$  gives:

$$\begin{aligned}
hr &\geq hn - (h - 1) + \frac{1}{4}(d(H^{\text{ab}})^2 - 1) - d \\
\Rightarrow 4(hr - hn + h) + 1 &\geq d(H^{\text{ab}})^2 - 4d(H^{\text{ab}}) + 4 \\
\Rightarrow 4h(r - n + 1) + 1 &\geq (d(H^{\text{ab}}) - 2)^2 \\
\Rightarrow (4h(r - n + 1) + 1)^{\frac{1}{2}} &\geq d(H^{\text{ab}}) - 2 \\
\Rightarrow ((2h^{\frac{1}{2}}(r - n + 1)^{\frac{1}{2}} + 1)^2)^{\frac{1}{2}} &\geq d(H^{\text{ab}}) - 2 \\
\Rightarrow 2h^{\frac{1}{2}}(r - n + 1)^{\frac{1}{2}} + 1 &\geq d(H^{\text{ab}}) - 2 \\
\Rightarrow 2h^{\frac{1}{2}}(r - n + 1)^{\frac{1}{2}} + 3 &\geq d(H^{\text{ab}}) \\
\Rightarrow h^{\frac{1}{2}}(2(r - n + 1)^{\frac{1}{2}} + 3) &\geq d(H^{\text{ab}})
\end{aligned}$$

Since  $h \geq 1$ . Letting  $k = 2(r - n + 1)^{\frac{1}{2}} + 3$  concludes the proof.  $\square$

---

<sup>3</sup>Wilson does not prove the  $\mathbb{Z}_p$  case separately, instead he claims "clearly we can assume that  $G$  has no subgroups isomorphic to  $\mathbb{Z}_p$ " with no further justification or reference. Regardless of the validity of this assumption, the proof of the special case is easy.

Note that in the proof of Corollary 2 it was not necessary to consider the special cases from Corollary 1(i), since these were taken into account when proving Theorem B.

The proof of Corollary 1(ii) is somewhat different and uses the following results about the completed group algebra of  $\mathbb{Z}_p$ .

Suppose  $T$  is an infinite procyclic pro- $p$  group. That is,  $T \cong \mathbb{Z}_p$  (again,  $\mathbb{Z}_p$  is the pro- $p$  completion of the integers). Then  $d(T) = 1$ , so if  $A$  is the completed group algebra of  $T$  over  $\mathbb{F}_p$ ,  $A$  is isomorphic to the ring of formal power series in a single indeterminate over  $\mathbb{F}_p$  (from Theorem 4). Hence  $A$  is a principal ideal domain whose proper quotients are all finite.

Now let  $G$  be the split extension of a free  $A$ -module  $M$  of rank 1 by  $T$ . i.e.  $G = M \rtimes T$  where  $M \cong A$ . This forms a group  $(M, T)$  with operation defined by  $(r_1, t_1)(r_2, t_2) = (r_1t_2 + r_2, t_1t_2)$  ( $M$  is also a  $T$ -module). We see that  $T$  is generated by a single element  $t_0$  (since  $T$  has presentation  $\langle t_0 | - \rangle$  as a pro- $p$  group) and  $M$  is generated by an element  $m_0$  and  $t_0$ . Hence  $G$  is a metabelian pro- $p$  group generated by two elements. Also consider the subgroup  $MT^{p^m}$  for each integer  $m$ .  $|T : T^{p^m}| = p^m$ , so by Proposition 7.6.3 in [9],  $T$  is a free  $\mathbb{F}_p[[T^{p^m}]]$ -module of rank  $p^m$ . Hence as a module for the completed group algebra of  $T^{p^m}$ ,  $M$  is free of rank  $p^m$ . Thus  $G_m$  can be generated by  $(t_0)^p$  from  $T^m$  as well as  $p^m$  elements of  $M$ . Since these generators generate  $G_m$  freely,  $d(G_m) = p^m + 1$ .

However,  $|G : G_m| = p^m$  so from Corollary 1(i)  $G$  cannot be the image of a finitely presented pro- $p$  group satisfying the conditions of Corollary 1

*Proof of Corollary 1(ii):*

Suppose that  $G$  satisfies the hypotheses of Corollary 1, and let  $G/N \cong \mathbb{Z}_p$  where  $N$  is not finitely generated. Then  $N/\Phi(N)$  is infinite (since  $d(N/\Phi(N)) = d(N) = \infty$ ) but  $N/\Phi(N)$  is generated as a normal subgroup of  $G$ , since  $\mathbb{Z}_p$  is finitely presented as a pro- $p$  group. Therefore, by Proposition 7.6.3 of [9],  $N/\Phi(N)$  is a finitely generated module of the completed group algebra of  $T$ , where  $T$  is a complement to  $N$  in  $G$ . Since  $T$  is isomorphic to  $\mathbb{Z}_p$ , being a transversal to  $N$  of  $G$ , the completed group ring of  $T$  is isomorphic to  $A$  above. Hence  $A/(N/\Phi(N))$  is finite, so  $N/\Phi(N) = U \oplus V$  where  $U, V$  are  $A$ -submodules and  $V$  is free of rank 1. Then if we write  $U = L/\Phi(N)$ , we find

$$\begin{aligned} G/L &\cong (G/\Phi(N))/(L/\Phi(N)) \\ &\cong (G/\Phi(N))/U \\ \Rightarrow (G/L)/V &\cong (G/\Phi(N))/(N/\Phi(N)) \\ &\cong \mathbb{Z}_p \end{aligned}$$

Hence  $G/L$  is an extension of a free  $A$ -module  $V$  by  $\mathbb{Z}_p$  and the contradiction follows from the above paragraph. Hence  $N$  must be finitely generated.

## 5 Consequences and Further Work

The theorems in Wilson's paper provides relatively little new material for further study. The Golod-Šafarevič condition for pro- $p$  groups is not only well known, but similar levels of generalizations pre-date this paper in the literature. Indeed, Lubotsky [6] details a version of the theorem by Roquette which is not only similar in strength but is also proved as a special case to the more general Theorem A' ([6] Proposition 1.3).

So it is clear that Wilson's focus in this paper is on Corollaries A and B. However, although these corollaries improve the bound for the growth of the subgroups  $H$  (and  $H^{ab}$ ) there has, in practice, been little work done using these results.

There is, however, one area in the paper that has seen significant interest. Wilson conjectures, on page 178, that groups that fail the inequalities given in Theorems 1 and 2 (and are hence infinite) contain free pro- $p$  subgroups of rank 2 (i.e. a free nonabelian pro- $p$  group). He also suggests that "proving this is likely to be difficult".

In [11], Wilson and Zel'manov show that a group that fails the inequalities (1), (2) do indeed contain an abstract free nonabelian subgroup, while in [12], Zel'manov proved the conjecture for a free *pro- $p$*  nonabelian subgroup. Both proofs used techniques from the theory of Lie Algebras. The link between Lie algebras and pro- $p$  groups coming from the ability of some pro- $p$  groups to be interpreted not only as a finitely generated free  $\mathbb{Z}_p$  module, but by then defining an additional operation, the module can be turned into a Lie algebra on  $\mathbb{Z}_p$ . See Chapter 4 of [3] for an introduction.

Wilson later published an alternative proof of the conjecture, but found that it contained a crucial error after the journal had gone to print. Despite this, the fact that the conjecture is true is an important result in the theory of profinite groups, giving us a deeper understanding of the structure of these 'large' groups.

## References

- [1] Apostol T., *Mathematical Analysis*, Addison-Wesley, Reading, 1960
- [2] Burnside, W., On unsettled questions in the theory of discontinuous groups, *Quarterly Journal of Pure and Applied Mathematics*, **33** (1902), p.230-238
- [3] Dixon, J. D., Du Sautoy M. P. F., Mann, A., Segal, D., *Analytic Pro- $p$  Groups*, 2nd Edition, Cambridge University Press, Cambridge, 1999.
- [4] Golod, E. S., On nil-algebras and residually finite  $p$ -groups, *Izv. Akad. Nauk SSSR*, **28** (1964), p.273-276
- [5] Ivanov, S. V., On the Burnside Problem on periodic groups, *Bulletin of the American Mathematical Society*, **27** (1992), p.257-260
- [6] Lubostky, A., Group Presentation  $p$ -adic Analytic Groups and Lattices in  $SL_2(\mathbb{C})$ , *The Annals of Mathematics*, **118** (1983), p.115-130
- [7] Ribes, L., Zalesskii P., *Profinite Groups*, Springer-Verlag, Berlin, 2000
- [8] Suzuki, M., *Group Theory I*, Springer-Verlag, Berlin, 1982.
- [9] Wilson, J. S., *Profinite Groups*, Clarendon Press, Oxford, 1998.
- [10] Wilson, J. S., Finite presentation of pro- $p$  and discrete groups, *Inventiones Mathematicae*, **105** (1991), p.177-183
- [11] Wilson, J. S. and Zel'manov, E., Identities for Lie Algebras of pro- $p$  groups, *Journal of Pure and Applied Algebra*. **81** (1992), p.103-109
- [12] Zel'manov, E., On Groups Satisfying the Golod-Shafarevich Condition, in Sautoy, Segal, Shalev (Eds) *New Horizons in pro- $p$  Groups*, Birkhäuser Boston, 2000, p.223-232