Journal of Pure and Applied Algebra 25 (1982) 311–325
North-Holland Publishing Company

COMBINATORIAL GROUP THEORY FOR PRO-p GROUPS

Alexander LUBOTZKY
Department of Mathematics, Bar-Ilan University, Ramat-Gan, Israel

Communicated by H. Bass
Received July 1981

Introduction

Although the category of pro-finite groups forms a natural extension of the category of finite groups, it carries a richer structure in that it has categorical objects and notions which do not exist in the finite case; e.g. projective groups and free product. The existence of such notions in the extended category leads to the definition of the usual notions of combinatorial group theory, such as free groups and defining a group by generators and relations.

Topics in various fields lead to a special consideration of pro-p groups: the tower problem (cf. [21]), Galois theory over p-adic fields and Demuskin groups (cf. [20]), the interpretation of generators and relations by means of cohomology (cf. [19, 21]), the theory of nilpotent groups (cf. [11]) etc. Nevertheless, there is no systematic theory (but see [6]). The aim of this paper is to begin to develop what we call combinatorial group theory for pro-p groups, although combinatorial tools do not seem to be useful here.

The fundamental books on combinatorial group theory, [16] and [15] both begin with free groups, their subgroups and their automorphisms. Accordingly, we study these aspects of pro-p groups. After summarizing (in Section 2) the basic (and mostly well-known) properties of free groups and free products, we prove in Section 3 some results analogous to the theorems of Hall, Greenberg and Howson about finitely generated subgroups of free groups. In Section 5, we describe the automorphism group of finitely generated free pro-p groups, and obtain as a corollary that, contrary to the discrete case, a free pro-p group on two generators has an outer automorphism acting trivially on the commutator quotient.

A central role in our work is played by the Frattini subgroup of a pro-p group; its basic properties are summarized in Section 1. This notion, whose importance to pro-p groups was first noted by Gruenberg [7], enables us to relate combinatorial group theoretic notions to group theoretic ones (see for example 3.1) and so we can replace the combinatorial methods by quite elementary group theoretic methods. Note also that our methods are free from cohomology.

Finally, it is worth noting that the theory of pro-p groups has already contributed to discrete group theory. For example Stalling's theorem [24] and the results in [22] were motivated by analogous results for pro-p groups. Our proposition 4.2 which characterizes the free pro-p group on e generators as *e-freely indexed pro-p group* (see 4.1), was announced in [14]. It motivated Ralph Strebel to characterize the discrete free group on e generators as the residually-finite e-freely indexed discrete group. Moreover, the main result of [12], about automorphisms of discrete free groups, is obtained there *as a consequence* of an analogous result for pro-p groups, in [9]. We anticipate that the future will bring more contributions of this nature.

Some conventions and terminology

Unless we indicate otherwise, we suppose subgroup of pro-finite groups to be closed and morphisms between pro-finite groups to be continuous. If (sub)groups in the ordinary sense are intended, we call them discrete, if there is any possibility of misunderstanding. Furthermore '$\lhd, \leq$' are used for 'normal subgroup of, subgroup of'; 1 denotes the group identity as well as the trivial group. C_p denotes the cyclic group of order p, and F_p the field of order p, while $\hat{Z}_p$ is the group of p-adic integers, $\hat{Z} = \prod_p \hat{Z}_p$ and $N = \{1, 2, 3, \dots\}$. $\bar{H}$ is the closure of a set H, and we shall say that a set X generates (topologically) a group G, if $G = \bar{H}$ where H is the discrete group generated by X. rk(G) is the minimal cardinality of such an X which converges to 1, in the sense that every neighborhood of 1 excludes only finitely many elements of X.

A family of open subgroups $\{H_\alpha\}_{\alpha \in I}$ in a pro-finite group F is said to be a base for (F, H) if $H = \bigcap_{\alpha \in I} H_\alpha$ and every open subgroup K of F, $H \subseteq K \subseteq F$ contains H_α for some $\alpha \in I$.

The following two lemmas will be used frequently without reference:

Lemma A. *If K is a closed subgroup of G and L an open subgroup of K then* (i) *there exists an open subgroup M of G such that $M \cap K = L$,* (ii) *if L is normal in K then there exists an open normal subgroup N such that $N \cap K < L$.*

Proof. (i) By [19, pp. 11–12], $K = \bigcap_{\alpha \in I} H_\alpha$ where $\{H_\alpha\}_{\alpha \in I}$ is the family of all open subgroups of G containing K. So $L = \bigcap_{\alpha \in I} (H_\alpha \cap K)$. $K \setminus L$ is a closed subset of K thus there exists a finite subset $J \subset I$ such that $L = \bigcap_{\beta \in J} (H_\beta \cap K)$. Take $M = \bigcap_{\beta \in J} H_\beta$.

(ii) First take M as in part (i) and then replace it by some open subgroup N of M which is normal in G. Such an N clearly exists.

Lemma B. *If $\{H_\alpha\}_{\alpha \in I}$ is a base for (G, H) and K a subgroup of G then $\{H_\alpha \cap K\}_{\alpha \in I}$ is a base for $(K, K \cap H)$.*

Proof. First, $K \cap H = K \cap (\bigcap_{\alpha \in I} H_\alpha) = \bigcap_{\alpha \in I} (K \cap H_\alpha)$. Now if L an open subgroup of $K, K \cap H \subseteq L \subseteq K$ then there exists M open in G such that $L = M \cap K$ and there exists $\alpha \in I$ such that $H_\alpha \subseteq M$. Thus $H \cap K \subseteq H_\alpha \cap \subseteq L$.

This research was supported by a grant from the United States – Israel Binational Science Foundation (BSF), Jerusalem, Israel.

1. The Frattini subgroup

1.1. Let G be a pro-finite group. Its Frattini subgroup is denoted by G^*, i.e. G^* is the intersection of the maximal open subgroups of G. Here are some of the properties of G^*:

Proposition. [7] (a) *G^* is a pro-nilpotent characteristic subgroup of G.*

(b) *If T is any subset of G such that $T \cup G^*$ generates G, then T generates G. In particular, if H is a subgroup of G such that $HG^* = G$, then $H = G$.*

(c) $\mathrm{rk}(G) = \mathrm{rk}(G/G^*)$.

1.2. Proposition. [7]. *If G is a pro-p group, then;*

(a) *Every maximal subgroup is normal of index p, $G^* = [G,G]G^p$, and G/G^* is, therefore, an elementary abelian p-group.*

(b) $G = \bigcap_{\psi} \mathrm{Ker}\, \psi$, *where* $\psi \in \mathrm{Hom}(G, C_p)$.

(c) *G is finitely generated iff G^* is open in G, in which case $G/G^* \approx C_p^{\mathrm{rk}(G)}$ and so* $(G:G^*) = p^{\mathrm{rk}(G)}$.

(d) $\mathrm{rk}(G) = \dim H^1(G, F_p) = \dim \mathrm{Hom}(G, F_p)$.

1.3. For a pro-p group G we shall define by induction a series of normal subgroups: $G^{(1)} = G$, $G^{(n+1)} = (G^{(n)})^*$ for $n \geq 1$.

Proposition. *Assume G and H are pro-p groups and $\varphi: G \to H$ an epimorphism. Then;*

(a) *$G^{(n)}$ is a characteristic subgroup of G.*

(b) $\varphi(G^{(n)}) = H^{(n)}$.

(c) $\bigcap_{n=1}^{\infty} G^{(n)} = \{1\}$.

(d) *G is finitely generated iff $G^{(n)}$ is open in G for all n.*

Proof. (a) $G^{(n+1)}$ is characteristic in $G^{(n)}$ and so, by induction, in G.

(b) If φ is an epimorphism, then $\varphi(G^*) = H^*$ (cf. [7]) and so by induction, $\varphi(G^{(n)}) = H^{(n)}$.

(c) This is clearly true for a finite p group. Now let N be an open normal subgroup of G. Then from (b) it follows that $\bigcap_{n=1}^{\infty} G^{(n)} \subseteq N$. As this is true for every N, we deduce $\bigcap_n G^{(n)} = \{1\}$.

(d) This is obtained by induction from Proposition 1.2(c).

1.4. Proposition. *Let G be a pro-p group, K a subgroup of G and $\{K_\alpha\}_{\alpha \in I}$ a base for (G,K). Then $K^* = \bigcap_{\alpha \in I} K_\alpha^*$.*

Proof. Since $H \to H^*$ preserves inclusions for pro-p groups (1.2(a)), $\bigcap_\alpha K_\alpha^* = \bigcap_\beta H_\beta^*$ where (H_β) is the family of all open subgroups containing K, we may thus assume that $(K_\alpha) = (H_\beta)$.

If $K \leq K_\alpha$ then $K^* = [K,K]K^p \subsetneq [K_\alpha, K_\alpha]K_\alpha^p = K_\alpha^*$.

On the other hand, if $x \in \bigcap_\alpha K_\alpha^*$ then in particular $x \in \bigcap_\alpha K_\alpha = K$. Let $\varphi: K \to C_p$ be a homomorphism whose kernel is $N \lhd K$. Denote by $\pi: K \to K/N$ the canonical projection. Then there exists an open normal subgroup M in G such that $M \cap K \leq N$, and

$$\psi: KM \longrightarrow KM/M \simeq K/M \cap K \longrightarrow K/N \xrightarrow{\bar{\varphi}} C_p,$$

where $\bar{\varphi}$ is the unique map satisfying $\bar{\varphi} \circ \pi = \varphi$. Thus we obtain a homomorphism $\psi: KM \to C_p$. KM is an open subgroup containing K, so by our assumption on $x, \psi(x) = 1$. Clearly $\psi|_K = \varphi$ and hence $\varphi(x) = 1$. This shows that $x \in K^*$; the proposition is proved.

1.5. The following lemma was proved by Gaschutz for finite groups, and extended by Jarden and Kiehne in [8] to finitely generated pro-finite groups. For pro-p groups the proof, using the Frattini subgroup, is trivial.

Lemma. *Let $\varphi: G \to H$ be a surjective morphism of pro-finite groups with* $\mathrm{rk}(G) = e$. *Then for each system of generators $\{y_1, \ldots, y_e\}$ of H there exists a system of generators $\{x_1, \ldots, x_e\}$ of G with $\varphi(x_i) = y_i$, $i = 1, \ldots, e$.*

2. Free pro-p groups and free products

2.1. Let F_X be the free discrete group on a set X, and $\mathscr{C}$ a class of finite groups closed under taking subgroups, quotient groups and direct products. Let $\mathscr{L}_\mathscr{C}$ be the family of all normal subgroups N of F for which $X \setminus N$ is finite and $F/N \in \mathscr{C}$. $\mathscr{L}_\mathscr{C}$ serves as a basis of neighborhoods of the identity for a topology on F_X – the pro-$\mathscr{C}$ topology. The completion of F_X with respect to this topology is denoted by $\hat{F}_X(\mathscr{C})$, and is called the free pro-$\mathscr{C}$ group on the set X.

Examples. $\mathscr{C}$ is the class of all finite (respectively nilpotent, p-) groups. In this case $\hat{F}_X(\mathscr{C})$ will be denoted by $\hat{F}_X$ (resp. $\hat{F}_X(\eta), \hat{F}_X(p)$).

We shall be interested mainly in the case where $\mathscr{C}$ is the p-groups and X is a finite set of order e. In this case $\hat{F}_X(p)$ will be denoted as $\hat{F}_e(p)$.

2.2. Proposition. *The free pro-p groups $F_X(p)$ and $F_Y(p)$ are isomorphic iff $|X| = |Y|$.*

Proof. If $|X| = |Y|$ the isomorphism is clear. For the opposite direction we use the fact that $|X| = \dim H^1(\hat{F}_X(p), F_p) = \dim \mathrm{Hom}(\hat{F}_X(p), F_p)$.

2.3. Theorem. [21, 7, 19]. *Every closed subgroup of $\hat{F}_X(p)$ is free.*

The standard proofs of this theorem are based on the characterization of free groups as the projective objects in the category of pro-p groups and as the groups of cohomological dimension ≤ 1. If $H \leq \hat{F}_X(p)$ then $\mathrm{cd}(H) \leq \mathrm{cd}(\hat{F}_X(p))$ and so H is also free. Another proof free from cohomology is obtained through a combination of [4, §2.5] and [7, Theorem 2].

The reader is also referred to [17] and [14] for a discussion to what extent Theorem 2.3 is true for other families $\mathscr{C}$.

2.4. We also have the analogue of Schreier's formula:

Proposition. [17, 14]. *If H is an open subgroup of $\hat{F}_e(p)$ of index r then H is isomorphic to $\hat{F}_k(p)$, where $k = 1 + (e-1)r$.*

2.5. We shall describe now the lower central series of $F = \hat{F}_e(p)$. Later we shall use it to describe the automorphism group of F.

Definition. Let G be a pro-finite group. Define by induction, $G_1 = G$, $G_{n+1} = \overline{(G_n, G)}$, $n = 1, 2, \ldots$, where $\overline{(G_n, G)}$ denotes the closure of the group generated by the commutators $a^{-1}b^{-1}ab$, $a \in G_n$, $b \in G$.

The following is well known:

Proposition. *G is pro-nilpotent iff $\bigcap_{n=1}^{\infty} G_n = 1$. In particular this is true for pro-p groups.*

2.6. Let E denote the discrete free group on e generators, and F its pro-p-completion. If E_n is the n-th term of the lower central series of E, then $E_n \subseteq F_n$.

Lemma. (a) $E \cap F_n = E_n$. (b) *E_n is dense in F_n.*

Proof. (a) follows from the fact that E/E_n is residually-p (i.e. the intersection of its normal subgroups of p-power index is trivial) [25, p. 47].

(b) Let $H = \overline{E_n}$. Then every commutator of weight n in elements of E is contained in H. As E is dense in F, this is true for every commutator of weight n. Thus F/H is a pro-p of nilpotency class $\leq n$ so $F_n \subseteq H$.

The opposite inclusion is clear.

2.7. So, F/F_n is the pro-p completion of E/E_n, and F_{n-1}/F_n is the pro-p completion of E_{n-1}/E_n [25, p. 55]. Thus the following information is derived from the results about the discrete case (cf. [16, Ch. 5]):

Proposition. *Let $F=\hat{F}_e(p)$ and $n\geq 1$. Then the quotient group F_n/F_{n+1}, $n=1,2,\dots$, of the lower central series is a free pro-p abelian group of rank $r(e,n)$. Namely, F_n/F_{n+1} is isomorphic to $\hat{Z}_p^{r(e,n)}$ where $r(e,n)$ is given by the Witt formula:*

$$r(e,n)=\frac{1}{n}\sum_{d\mid n}\mu(d)e^{n/d}$$

where μ is the Moebius function.

2.8. Finally, we summarize the basic properties of free products of pro-p groups.

Let G and H be two pro-p groups. Their free product $G*H$ is defined as follows: We take first their free product as discrete groups; call it K. Of course G and H are subgroups in a natural way of K. Now, let $\mathscr{L}$ be the family of all normal subgroups N of K such that

(a) K/N is a finite p-group.

(b) $N\cap G$ (resp.: $N\cap H$) is an open subgroup of G (resp. H).

The completion of K with respect to the topology determined by $\mathscr{L}$ is $G*H$. By standard arguments one can prove that $G*H$ really satisfies the desired universal property (cf. [3]) in the category of the pro-p groups. Note also that the discrete free product of G and H is contained in the pro-p free product.

2.9. The Grusko–Neumann theorem [15, p. 91] which is quite a deep result in the discrete case, becomes trivial in our context.

Proposition. *Let G and H be two finitely generated pro-p groups. Then* $\mathrm{rk}(G*H)=\mathrm{rk}(G)+\mathrm{rk}(H)$.

Proof. If G' and H' are dense subgroups of G and H, respectively, then the group generated by G' and H' is dense in $G*H$, and so $\mathrm{rk}(G*H)\leq\mathrm{rk}(G)+\mathrm{rk}(H)$.

On the other hand, $G\times H$ is a quotient of $G*H$, and so is $G/G^*\times H/H^*$. The last group is just an elementary abelian p-group whose rank is $\mathrm{rk}(G/G^*)+\mathrm{rk}(H/H^*)=\mathrm{rk}(G)+\mathrm{rk}(H)$. Thus $\mathrm{rk}(G*H)\geq\mathrm{rk}(G)+\mathrm{rk}(H)$ and the proposition is proved.

Remark. The stronger version of the Grusko–Neumann result (see [15, III, 3.7]) is also true for pro-p groups, but for our needs below, the above weak version is more appropriate.

2.10. Kurosh Subgroup Theorem. [3, 5]. *Let K be an open subgroup of $A=G*H$. Then $K=B*F$, where F is a finitely generated free pro-p group and B is a free product of intersections of K with some conjugates in A of G and H.*

Problem. Is the Kurosh subgroup theorem true for *closed* subgroups of free products of *pro-p* groups?

As subgroups of $\hat{F}_e$ are not free in general, one cannot expect the Kurosh subgroup theorem to be true for general pro-finite groups (at least if one takes a direct analogue) but we think it is valid for pro-p groups.

3. Finitely generated subgroups of $\hat{F}_e(p)$

3.1. We shall begin with a lemma which gives the central argument for the next theorem.

Lemma. *Let F be a finitely generated free pro-p group, and H a subgroup of F. Then the following two conditions are equivalent:*

(a) *H is a free factor of F (namely, there exists a subgroup M of K such that the map $H*M\to K$, induced by the inclusions of H and M in F, is an isomorphism).*

(b) $F^*\cap H=H^*$.

Proof. (a)$\Rightarrow$(b) is easy and left to the reader.

(b)$\Rightarrow$(a): (b) implies that the inclusion $H\hookrightarrow F$ induces an inclusion of H/H^* as a subspace of the F_p-vector space F/F^*. Since F/F^* is finite, H/H^* is finite and H is a finitely generated free group. Let $X=\{x_1,\dots,x_r\}$ be a set of free generators for H, and let C be a complementary F_p-subspace of H/H^* in F/F^*. One can find a set $Y=\{y_1,\dots,y_l\}$ of elements in F such that $\{\pi(y_1),\dots,\pi(y_l)\}$ is a basis of C (π is the natural projection $F\to F/F^*$). This yields that $\{\pi(x_1),\dots,\pi(x_r),\pi(y_1),\dots,\pi(y_l)\}$ is a basis for F/F^*. Let M be the (closed) subgroup generated by Y. The map $\varphi:H*M\to F$ extending the inclusions is surjective since $X\cup Y$ generates F. Now $\mathrm{rk}(H*M)=r+l=\mathrm{rk}(F/F^*)=\mathrm{rk}(F)$ and F is a free group, so it is free on $r+l$ generators. This suffices to conclude that φ is an isomorphism.

Remark. We do not know whether the restriction on F to be of finite rank is necessary.

3.2. We are coming to the main result of this section, an analogue of Hall's theorem [15, I, §3.10], from which most of the other results of this section are derived. Note that its proof here is completely different from the proof in the discrete case and in some sense it is even a simpler one.

Theorem. *Let $F=\hat{F}_e(p)$ be the free group on e generators, $e\geq 2$, H a finitely generated subgroup of F, and A a compact subset of F that is disjoint from H. Then H is a free factor of an open subgroup (of finite index) of F disjoint from A.*

Proof. As A is compact and disjoint from H, standard compactness arguments show that one can find an open subgroup G of F such that $H\subseteq G$ and $G\cap A=\emptyset$. So we can replace F by G.

By Proposition (1.4) we know that $H^* = \bigcap H_\alpha^*$, where $\{H_\alpha\}$ is the set of all open subgroups containing H. Thus $H^* = \bigcap (H \cap H_\alpha^*)$. For every α, $H \cap H_\alpha^*$ is a subgroup of finite index in H. H is of finite rank and H^* is, therefore, of finite index in H as well (1.2(c)). Hence there exists $K = H_\alpha$ such that $H^* = H \cap H_\alpha^* = H \cap K^*$. Lemma 3.1 applies now to yield that H is a free factor of K.

Remark. The above proof shows, in fact, that H is free. Thus we obtained a purely group theoretic proof for this special case of Theorem 2.3.

3.3. A pro-p Greenberg theorem can now be deduced.

Proposition. *If a finitely generated subgroup H of $F = \hat{F}_e(p)$ contains a non-trivial normal subgroup of F, then it has finite index in F.*

Proof. By Theorem 3.2, $K = H * M$ has finite index in F. Suppose H has infinite index; then $M \neq 1$. So $H * M$ is a non-trivial free product; in particular, N is a normal subgroup of the discrete free product of H and M (2.8). But for discrete groups it is clear that a free factor cannot contain a normal subgroup of the whole group.

Corollary. [14, 17]. *A finitely generated normal subgroup of $F_e(p)$ is of finite index.*

3.4. Corollary. [1, 14, 17]. *The center of $\hat{F}_e(p)$ ($e \geq 2$) is trivial.*

Proof. If $Z = Z(\hat{F}_e(p))$ is not trivial it is abelian, free, and thus isomorphic to $\hat{Z}_p$, and hence finitely generated. The last corollary implies that Z is of finite index which is a contradiction to 2.4.

3.5. In a way similar to [10] and [15, §I.3], many other results can be derived from Hall's theorem (3.2). As the proofs are really the same as those for the discrete case (when one takes, of course, the right interpetations), we shall just state the results:

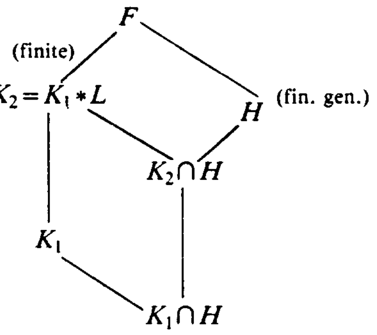
Proposition. *Let $H \neq \{1\}$ be a finitely generated subgroup of $F = \hat{F}_e(p)$. Then the following conditions are equivalent:*

(a) *H is of finite index in F.*
(b) *H contains a non-trivial normal subgroup of F.*
(c) *H intersects non-trivially every non-trivial normal subgroup of F.*
(d) *H intersects non-trivially every non-trivial subgroup of F.*
(e) *H is properly contained in no subgroup of F of infinite rank.*
(f) *H is properly contained in no subgroup of F of rank as great as that of H.*

3.6. Howson's result [15, I, 3.13] also has a pro-p analogue:

Proposition. *The intersection of two finitely generated subgroups of $F=\hat{F}_e(p)$ is itself finitely generated.*

3.7. Lemma. *Let H be a finitely generated subgroup of F, K_2 a subgroup of finite index in F, and K_1 a free factor of K_2. Then $H\cap K_1$ is a free factor of $H\cap K_2$.*



Proof. Assume first that H is open in F. As K_1 is a free factor of K_2, there exists a system of free generators X of K_2 such that $K_1\cap X$ generates K_1 freely. Denote by K_2' (respectively, K_1') the discrete group generated by X (resp. $X\cap K_1$). Clearly K_i is the pro-p completion of K_i' $(i=1,2)$ and K_1' is a free factor of K_2'.

Now, $H\cap K_2$ is of finite index in K_2, as is $H\cap K_2'$ in K_2'. From the Kurosh subgroup theorem for discrete groups [15, III, 3.6] it follows that $H\cap K_1'$ is a free factor of $H\cap K_2'$. Since K_i is the pro-p completion of K_i' and $H\cap K_i'$ is of finite index in K_i', $H\cap K_i$ is the pro-p completion of $H\cap K_i'$, $i=1,2$, (see [14, §1]). Thus $H\cap K_1$ is a free factor of $H\cap K_2$ and Lemma 3.1 yields that $(H\cap K_1)^*=(H\cap K_1)\cap(H\cap K_2)^*$.

Now consider the general case. $H=\bigcap_\alpha H_\alpha$, where $\{H_\alpha\}$ is the family of all open subgroups of F containing H. From the above we have

$$(H_\alpha\cap K_1)^*=(H_\alpha\cap K_1)\cap(H_\alpha\cap K_2)^*.$$

On the other hand, from Proposition (1.4) we get

$$(H\cap K_i)^*=\bigcap_\alpha (H_\alpha\cap K_i)^*,\quad i=1,2.$$

Putting this together gives

$$\begin{aligned}(H\cap K_1)^*&=\bigcap_\alpha (H_\alpha\cap K_1)^*=\bigcap_\alpha ((H_\alpha\cap K_1)\cap(H_\alpha\cap K_2)^*)\\ &=\bigcap_\alpha (H_\alpha\cap K_1)\cap\bigcap_\alpha (H_\alpha\cap K_2)^*\\ &=(H\cap K_1)\cap(H\cap K_2)^*.\end{aligned}$$

Recall that H is finitely generated and $H\cap K_2$ is of finite index in H; hence $H\cap K_2$ is finitely generated. Thus we can use Lemma 3.1, again, to conclude that $H\cap K_1$ is a free factor of $H\cap K_2$.

3.8. Proof of 3.6. Let H_1 and K_1 be two finitely generated subgroups of F. By Theorem 3.2 there exist $K_2 = K_1 * U$ and $H_2 = H_1 * V$ of finite index in F. Lemma 3.7 implies that $H_1 \cap K_1$ is a free factor of $H_1 \cap K_2$ and that $H_1 \cap K_2$ is a free factor of $H_2 \cap K_2$. The latter group is of finite index in F and thus of finite rank. $H_1 \cap K_1$ is therefore of finite rank as well (2.9).

4. Freely indexed groups

4.1. If G is a (pro-finite) group generated by e elements and H is a (open) subgroup of finite index, then

$$\mathrm{rk}(H) \leq 1 + (e-1)(G:H). \qquad (*)$$

Definition. G is called e-freely indexed if $(*)$ is an equality for every H.

This definition and the following theorem are taken from [14].

Theorem. *Let $\mathscr{C}$ be a class of finite groups as in 2.1 which is also closed under taking extensions. Let $e \geq 2$ and N a normal subgroup of $\hat{F}_e(\mathscr{C})$ of infinite index. If $\hat{F}_e(\mathscr{C})/N$ is not an e-freely indexed group then $N \simeq \hat{F}_\omega(\mathscr{C})$ the free pro-$\mathscr{C}$ group of countable rank.*

It is also observed there that $\hat{F}_e$ and $\hat{F}_e(p)$ are e-freely indexed (2.4) while $\hat{F}_e(\eta)$ is not. It turns out that for pro-p groups this property characterizes $\hat{F}_e(p)$.

4.2. Proposition . *If G is an e-freely indexed pro-p group then $G \simeq \hat{F}_e(p)$.*

Proof. By substituting $H = G$ in $(*)$ we see that $\mathrm{rk}(G) = 1 + (e-1)(F:F) = e$. Hence there is an epimorphism $\varphi : F = \hat{F}_e(p) \to G$. Proposition 1.3(b) gives that $\varphi(F^{(n)}) = G^{(n)}$ for every n. So φ induces a system of epimorphisms $\varphi^n : F^{(n)}/F^{(n+1)} \to G^{(n)}/G^{(n+1)}$, $n = 1, 2, \ldots$.

Now, $F^{(1)}/F^{(2)}$ is isomorphic to an elementary abelian group of rank e. But the same is true for $G^{(1)}/G^{(2)}$, since this is also an elementary abelian group and $\mathrm{rk}(G^{(1)}/G^{(2)}) = \mathrm{rk}(G/G^*) = \mathrm{rk}(G) = e$. This shows that φ^1 is an isomorphism, and in particular, the index of $F^{(2)}$ in $F^{(1)}$ is equal to the index of $G^{(2)}$ in $G^{(1)}$. As G is an e-freely indexed group we have

$$r = \mathrm{rk}(G^{(2)}) = 1 + (e-1)[G^{(1)} : G^{(2)}] = 1 + (e-1)[F^{(1)} : F^{(2)}] = \mathrm{rk}(F^{(2)}).$$

Moreover, $\varphi(F^{(2)}) = G^{(2)}$ and $(G^{(2)})^{(i)} \simeq G^{(i+1)}$. An open subgroup of an e-freely indexed group of index l is an r-freely indexed group, where $r = 1 + (e-1)l$ [14, §2.4]. So $F^{(2)}$ and $G^{(2)}$ are r-freely indexed and we can continue as before to show that φ^2 is an isomorphism and by induction that φ^n is an isomorphism for every n.

Now let $x \neq 1$ be an element of F. By 1.3(c) there exists n such that $x \in F^{(n)}$ but $x \notin F^{(n+1)}$. Thus $\varphi^n(xF^{(n+1)})$ is a non-trivial element of $G^{(n)}/G^{(n+1)}$. But $\varphi^n(xF^{(n+1)}) = \varphi(x)G^{(n+1)}$. This shows that $\varphi(x) \notin G^{(n+1)}$ and in particular $\varphi(x) \neq 1$. We see, therefore, that φ is injective (as well as surjective). Both groups are compact and so φ is an isomorphism.

4.3. Corollary. *If* $1 \neq N \lhd \hat{F}_e(p)$, $e \geq 2$ *of infinite index then* $N \simeq \hat{F}_\omega(p)$.

Proof. $\hat{F}_e(p)/N$ is not isomorphic to $\hat{F}_e(p)$ and so it is not e-freely indexed so by Theorem 4.1, $N \simeq \hat{F}_\omega(p)$.

Remark. Note that the last corollary is also a consequence of Theorem 2.3 and Corollary 3.3.

4.4. Corollary. *If* G *is a pro-nilpotent e-freely indexed group and* $e \geq 2$ *then* $G \simeq \hat{F}_e(p)$ *for some prime* p.

Proof. $G = \prod_p G_p$, a product of its Sylow subgroups. But a non-trivial direct product of pro-finite groups is never e-freely indexed if $e \geq 2$ [13]. Thus $G = G_p$ for some prime p, i.e. it is a pro-p group and so it is isomorphic to $\hat{F}_e(p)$.

On the other hand, in [14] many examples of pro-finite e-freely indexed groups were presented. Some of them are far from being free.

Finally we mention that Ralph Strebel answered affirmatively a question posed in [14] and proved that a residually finite discrete e-freely indexed group is isomorphic to F_e – the discrete free group on e generators. So once again we see an example of a phenomenon in which the pro-p group theory is more similar to discrete groups than to the general pro-finite group theory.

5. Automorphisms of free pro-p groups

5.1. Let G be a pro-finite group and $A = \mathrm{Aut}(G)$ be the group of the continuous automorphisms of G with the topology of uniform convergence. A is a Hausdorff totally disconnected topological group, but not necessarily compact. If G is finitely generated, A is also compact and thus a pro-finite group [23]. From now on we shall assume that G is finitely generated.

5.2. If $\mathscr{C}$ is a class of finite groups, as in 2.1, and $\hat{F}_e(\mathscr{C})$ the free pro-$\mathscr{C}$ group on e generators, then we have the following property. The reader can see in [2] that this property is not valid for the discrete free group F_e.

Proposition. *Let K be a characteristic subgroup of $F = \hat{F}_e(\mathscr{C})$. The natural map*

$$\pi : \mathrm{Aut}(F) \to \mathrm{Aut}(F/K),$$

(obtained by taking the induced automorphism) is surjective.

Proof. Assume F is freely generated by $x_1, \dots, x_e$. So F/K is generated by $x_1K, \dots, x_eK$. If $\varphi \in \mathrm{Aut}(F/K)$, write $b_i = \varphi(x_iK)$, $i = 1, \dots, e$. The set $\{b_1, \dots, b_e\}$ generates F/K, thus by Gaschutz's Lemma (1.5), we can find a set of generators $\{a_1, \dots, a_e\}$ in F such that $b_i = a_iK$, $i = 1, \dots, e$. The correspondence $x_i \to a_i$, $i = 1, \dots, e$ extends uniquely to an endomorphism Ψ which is an epimorphism and therefore [19, p. 68] an automorphism of F. It is clear that $\pi(\Psi) = \varphi$.

5.3. Again, let G be an arbitrary pro-finite group and G_n, $n = 1, 2, 3, \dots$, the lower central series of G (2.5). Denote $K_n = \mathrm{Ker}(\mathrm{Aut}(G) \to \mathrm{Aut}(G/G_{n+1}))$.

Thus we have a series of normal subgroups $\cdots K_2 \lhd K_1 \lhd A$.

Lemma. *For every $i, j \in N$, $\overline{[K_i, K_j]} \subseteq K_{i+j}$; in particular $\overline{[K_1, K_i]} \subseteq K_{i+1}$.*

Proof. The proof is exactly like that in [2, Theorem 1.1, p. 240].

5.4. Corollary. *G is pro-nilpotent iff K_1 is pro-nilpotent.*

Proof. G modulo its center $Z(G)$ acts as inner automorphisms on G. All the inner automorphisms act trivially on the commutator quotient. $G/Z(G)$ is, therefore, a subgroup of K_1. Hence if K_1 is pro-nilpotent, so is G.

On the other hand, if G is pro-nilpotent then $\bigcap_{n=1}^{\infty} G_n = 1$ (2.5). So $\bigcap_{n=1}^{\infty} K_n = 1$. But from the lemma one easily sees that K_n contains $(K_1)_n$. This implies that $\bigcap_{n=1}^{\infty} (K_1)_n = 1$. Use again 2.5 to conclude that K_1 is pro-nilpotent.

5.5. In case G is a pro-p group we have some more information: K_1 is a pro-p group. Moreover, the classical result about finite pro-p groups stating that an automorphism of finite p-group acting trivially on the Frattini quotient is of p-power order can be extended to obtain the following (see [1]).

Proposition. *Let G be a finitely generated pro-p group. Then $K_0 = \mathrm{Ker}(\mathrm{Aut}(G) \to \mathrm{Aut}(G/G^*))$ is a pro-p group. In particular $\mathrm{Aut}(G)$ has a pro-p subgroup of finite index.*

5.6. We come now to our primary concern: Fix $e \geq 2$, and let $G = F = \hat{F}_e(p)$. If K_n is defined as above, we have by 5.2 that $\mathrm{Aut}(F)/K_n \simeq \mathrm{Aut}(F/F_{n+1})$ and by 5.4 that $\bigcap_{n=1}^{\infty} K_n = 1$. Thus we get:

Proposition. (a) $\mathrm{Aut}(F) = \varprojlim_n \mathrm{Aut}(F/F_n)$. (b) $\mathrm{Aut}(F)/K_1 \simeq \mathrm{GL}(e, \hat{Z}_p)$.

5.7. We are going to describe now that structure of Aut(F) by describing the quotients K_{n-1}/K_n for $n=2,3,\ldots$. As noted above A/K_n is identified with the group of the automorphism of F/F_{n+1}, and K_{n-1}/K_n consists of those automorphisms which induce the identity on F/F_n.

Let α be such an automorphism and let $x_1,\ldots,x_e$ a fixed set of generators for F/F_{n+1}. Then $\alpha(x_i)\equiv x_i \pmod{F_n/F_{n+1}}$, $i=1,\ldots,e$. Thus there exists $z_i\in F_n/F_{n+1}$, such that $\alpha(x_i)=x_iz_i$, $i=1,\ldots,e$. On the other hand, if $(z_1,\ldots,z_e)\in(F_n/F_{n+1})^e$, then the set $\{x_1z_1,\ldots,x_ez_e\}$ is a set of generators for F/F_{n+1} (since $z_i\in(F/F_{n+1})^*$, see 1.1). So there exists an automorphism $\alpha=\alpha_{(z_1,\ldots,z_e)}$ of F/F_{n+1} such that $\alpha(x_i)=x_iz_i$, $i=1,\ldots,e$.

Lemma. *The correspondence* $(z_1,\ldots,z_e)\to\alpha_{(z_1,\ldots,z_e)}$ *is an isomorphism of* $(F_n/F_{n+1})^e$ *onto* K_{n-1}/K_n.

Proof. It follows from the above that this correspondence is bijective. So we have only to prove that this is a homomorphism. (The continuity of this correspondence can be checked easily from the definition.)

Let $(\mathbf{z})=(z_1,\ldots,z_e)$ and $(\mathbf{z}')=(z_1',\ldots,z_e')\in(F_n/F_{n+1})^e$, and let α and α' be the corresponding automorphisms. We have to show that

$$\alpha\circ\alpha'(x_i)=x_iz_iz_i' \quad \text{for } i=1,\ldots,e. \tag{$*$}$$

In 2.6(b) we note that the n-th term, E_n, of the lower central series of the discrete free group for e generators E is dense in F_n, and so the set of standard words in the letters $x_1,\ldots,x_e$ is dense in F_n/F_{n+1}. As the correspondence $(z_1,\ldots,z_e)\to\alpha_{(z_1,\ldots,z_e)}$ is continuous, it will be sufficient to prove ($*$) for ($\mathbf{z}'$) whose components z_i' ($i=1,\ldots,e$) are standard words in $x_1,\ldots,x_e$. Moreover, every such word is a product of finitely many commutator words of weight n in the generators $x_1,\ldots,x_e$.

So let $z_i'=w_i'(x_1,\ldots,x_e)$, $i=1,\ldots e$, where w_i' is a word in $x_1,\ldots,x_e$.

$$\alpha\circ\alpha'(x_i)=\alpha(\alpha'(x_i))=\alpha(x_iz_i')=\alpha(x_i)\alpha(z_i')=x_iz_i\alpha(z_i'),\quad 1\le i\le e.$$

Thus the proof will be complete once we prove that $\alpha(z_i')=z_i'$.

$$\begin{aligned}\alpha(z_i')&=\alpha(w_i'(x_1,\ldots,x_e))=w_i'(\alpha(x_1),\ldots,\alpha(x_e))\\&=w_i'(x_1z_1,\ldots,x_ez_e)=w_i'(x_1,\ldots,x_e)w_i'(z_1,\ldots,z_e).\end{aligned}$$

The last equality follows from the fact that z_j ($1\le j\le e$), are in the center of the group F/F_{n+1}. Now w_i' is a product of commutator words, and all the z_j's commute, so $w_i'(z_1,\ldots,z_e)=1$ for $i=1,\ldots,e$, and thus:

$$\alpha(z_i')=w_i'(x_1,\ldots,x_e)=z_i',\quad i=1,\ldots,e.$$

This completes the proof of the lemma, whose idea of proof is based on [18; §5].

5.8. Summarizing all this and 2.7 together we obtain:

Theorem. *Let $F=\hat{F}_e(p)$ $(e\geq 2)$ and $A=\mathrm{Aut}(F)$. Then A has a descending series of pro-p normal subgroups $K_n \lhd A$, $n=1,2,\ldots$ such that:*

(a) $K_n=\mathrm{Ker}(\mathrm{Aut}(F)\to\mathrm{Aut}(F/F_n))$.

(b) $\bigcap_{n=1}^{\infty} K_n=\{1\}$.

(c) *A/K_1 is isomorphic to* $\mathrm{GL}(e,\hat{Z}_p)$.

(d) *K_{n-1}/K_n is isomorphic to the free abelian pro-p group of rank $e\cdot r(e,n)$ where $r(e,n)=n^{-1}\sum_{d\mid n}\mu(d)e^{n/d}$ (μ is the Moebius function).*

5.9. It is well known that an automorphism of the discrete free group on two generators which acts trivially on the commutator quotient is inner (cf. [15, I.4.5]. This is not true any more for $\hat{F}_e(P)$, not even for $e=2$.

Proposition. *There exist outer automorphisms of $F=\hat{F}_e(p)$ which induce the identity on F/F_2.*

Proof. In the above notation we have to prove that the inclusion $\hat{F}_e(p)\to K_1$ is not an isomorphism. A simple computation (and 5.8, of course) shows that $\mathrm{rk}(K_1/K_2)=\frac{1}{2}e^2(e-1)$. This is greater than e, for $e\geq 3$. Thus it is clear, and not surprising, that for $e\geq 3$, K_1 is not isomorphic to $\hat{F}_e(p)$.

Consider now the case $e=2$. If $K_1=\hat{F}_2(p)=F$, then $\mathrm{rk}(K_1)=2$ and since K_1/K_2 is a free abelian pro-p group of rank $\mathrm{rk}(K_1/K_2)=\frac{1}{2}2^2\cdot(2-1)=2$, we get that $K_2=(K_1)_2=F_2$. From the definition of K_n and from the fact that F_n/F_{n+1} is in the center of F/F_{n+1}, we get that $F_n\subsetneq K_n$, and in particular, $F_3\subsetneq K_3$. But $\mathrm{rk}(F_2/F_3)=r(2,2)=1$, while $\mathrm{rk}(K_2/K_3)=2\cdot\mathrm{rk}(F_3/F_4)=2\cdot r(2,3)=4$. This contradicts the assumption $F=K_1$.

Remark. The last proof shows that at least for $e=2$, the series K_n $(n=1,2,\ldots)$ is not the lower central series of K_1.

References

[1] M.P. Anderson, Exactness properties of pro-finite functors, Topology 13 (1974) 229–239.

[2] S. Andreadakis, On the automorphisms of free groups and free nilpotent groups, Proc. London Math. Soc. 15 (1965) 239–268.

[3] E. Binz, J. Neukirch and G.H. Wenzel, A subgroup theorem for free products of profinite groups, J. Algebra 19 (1971) 104–109.

[4] J. Cossey, O.H. Kegel and L.G. Kovacs, Maximal Frattini extensions, Arch. der Math. 35 (1980) 210–217.

[5] D. Gildenhuys and L. Ribes, A Kurosh subgroup theorem for free pro-$\mathscr{C}$-products of pro-$\mathscr{C}$-groups, A.M.S. Trans. 186 (1973) 309–329.

[6] D. Gildenhuys and L. Ribes, Profinite groups and Boolean graphs, J. Pure and Appl. Algebra 12 (1978) 21–47.

[7] K.W. Gruenberg, Projective profinite groups, J. London Math. Soc. 42 (1967) 155–165.

[8] M. Jarden and U. Kiehne, The elementary theory of algebraic fields of finite corank, Inventiones Math. 30 (1975) 275–294.
[9] M. Jarden and J. Ritter, Normal automorphisms of absolute Galois groups of p-adic fields, Duke Math. J. 47 (1980) 47–56.
[10] A. Karrass and D. Solitar, On finitely generated subgroups of a free group, Proc. A.M.S., 22 (1969) 209–213.
[11] M. Lazard, Sur les groupes nilpotents et les anneaux de Lie, Annales Sci. l'Ecole Norm. Sup. (3) 71 (1954) 101–190.
[12] A. Lubotzky, Normal automorphisms of free groups, J. Algebra 63 (1980) 494–498.
[13] A. Lubotzky, Free quotients and the congruence kernel of SL_2, J. Algebra, to appear.
[14] A. Lubotzky and L. Van-den-Dries, Subgroups of free pro-finite groups and large subfields of $\bar{Q}$, Israel J. Math. 39 (1981) 25–45.
[15] R.C. Lydon and P.E. Schupp, Combinatorial Group Theory (Springer, Berlin–Heidelberg–New York, 1977).
[16] W. Magnus, A. Karrass and D. Solitar, Combinatorial Group Theory (Wiley, New York, 1966).
[17] D.V. Mel'nikov, Normal subgroups of free profinite groups, Mat. USSR Izvestiya 12 (1) (1978) 1–20.
[18] A.W. Mostowski, On automorphisms of relatively free groups, Fund. Math. 50 (1961–62) 403–411.
[19] L. Ribes, Introduction of profinite groups and Galois cohomology, Queens Papers in Pure and Applied Mathematics, No. 24 (1970).
[20] J.P. Serre, Structure de certains pro-p groups, Semin. Bourbaki, No. 252 (1968).
[21] J.P. Serre, Cohomologie Galoisienne, Lecture Notes in Math. No. 5 (Springer, Berlin–Göttingen–Heidelberg, 1964).
[22] J. Shapiro and J. Sonn, Free factor groups of one-relator groups, Duke Math. J. 41 (1974) 83–88.
[23] J. Smith, On products of pro-finite groups, Illinois J. Math. 13 (1969) 680–688.
[24] J.R. Stallings, On torsion free groups with infinitely many ends, Ann. of Math. 87 (1961) 312–334.
[25] R.B. Warfield, Nilpotent Groups, Lecture Notes in Math. No. 513, (Springer, Berlin–New York, 1976).