ISRAEL JOURNAL OF MATHEMATICS 107 (1998), 195–227

FINITE EXTENSIONS OF FREE PRO-P GROUPS OF RANK AT MOST TWO

BY

W. N. HERFORT

Institut für Angewandte und Numerische Mathematik, Technische Universität Wien
A-1040 Wien, Austria
e-mail: herfort@uranus.tuwien.ac.at

AND

L. RIBES*

Department of Mathematics and Statistics, Carleton University
Ottawa, Ontario K1S 5B6, Canada
e-mail: lribes@math.carleton.ca

AND

P. A. ZALESSKII**

Institute of Technical Cybernetics, Academy of Sciences of Belarus
6, Surganov St., 220605 Minsk, Belarus
e-mail: pz@uranus.tuwien.ac.at

ABSTRACT

For a pro-p group G, containing a free pro-p open normal subgroup of rank at most 2, a characterization as the fundamental group of a connected graph of cyclic groups of order at most p, and an explicit list of all such groups with trivial center are given. It is shown that any automorphism of a free pro-p group of rank 2 of coprime finite order is induced by an automorphism of the Frattini factor group F/F^*. Finally, a complete list of automorphisms of finite order, up to conjugacy in $\mathrm{Aut}(F)$, is given.

* Supported by an NSERC grant.

** Supported by the Austrian Science Foundation.
Received January 19, 1997

Introduction

Let p be a prime number and G a pro-p group that contains an open free pro-p subgroup F. If G is torsion free, then by the celebrated theorem of Serre [S1], G is also a free pro-p group. However, if G has torsion, the structure of G is not clear even in the case $[G : F] = p$.

The situation for abstract groups is much better. In addition to the abstract version of Serre's theorem due to Serre, Stallings and Swan, the following two theorems describe the structure of virtually free groups:

THEOREM (A. Karrass, A. Pietrowski and D. Solitar [K-P-S]): *Let G be a finitely generated virtually free group. Then G is the fundamental group of a finite graph of finite groups.*

THEOREM (J. L. Dyer and G. P. Scott [D-S]): *Let G be a group having a free subgroup of index p. Then $G = (*_{i\in I}(C_p \times H_i)) * H$, where H_i, H are free groups.*

On this basis (as well as on the basis of the results below) one can state the following conjectures:

CONJECTURE 1: *Let G be a finitely generated virtually free pro-p group. Then G is the fundamental group of a finite graph of finite p-groups in the category of pro-p groups (i.e. isomorphic to the pro-p completion of some abstract fundamental group of a finite graph of finite p-groups).*

CONJECTURE 2: *Let G be a finitely generated pro-p group having a free pro-p subgroup of index p. Then G is a free pro-p product*

$$G \cong \Big(\coprod_{i=1}^{n}(C_p \times H_i)\Big) \coprod H,$$

where H_i, H are free pro-p groups of finite ranks.

In this paper we establish the following results.

THEOREM 1: *Conjectures 1 and 2 are true if G is a finite extension of a free pro-p group F of rank < 3.*

If $\operatorname{rank}(F) = 1$, the easy proof, which relies on the well known structure of $\operatorname{Aut}(\mathbf{Z}_p)$, is given in Lemma 3.7. If $\operatorname{rank}(F) = 2$, the first step of the proof is to make the reduction to the case when G has trivial center. After this one needs to describe all finite extensions of F having trivial center, which is done in the following

THEOREM 2: *Let G be a pro-p group with trivial center. Then G has an open normal free subgroup F of rank 2 if and only if G has one of the following structures:*

(1) *G is a free pro-p group of finite rank.*
(2) *$p = 3$ and $G \cong C_3 \coprod C_3$.*
(3) *$p = 2$ and G has one of the following forms:*
  (a) $G \cong C_2 \coprod C_2 \coprod C_2$;
  (b) $G \cong C_2 \coprod \mathbf{Z}_2$;
  (c) $G \cong C_2 \coprod (C_2 \times \mathbf{Z}_2)$;
  (d) $G \cong C_4 \coprod C_2$;
  (e) $G \cong (C_2 \times C_2) \coprod C_2$;
  (f) $G \cong (C_2 \times C_2) \coprod_{C_2} (C_2 \times C_2) \coprod_{C_2} (C_2 \times C_2)$;
  (g) $G \cong D_4 \coprod_{C_2} (C_2 \times C_2)$ *where D_4 is the dihedral group of order* 8.

Here, C_n denotes the finite cyclic group of order n and $\mathbf{Z}_2$ is the group of 2-adic integers. All free products (with amalgamations) in Theorem 2 are in the category of pro-p groups which (in our situation) can be defined as the pro-p completions of the corresponding abstract constructions. For precise definitions, see e.g. [B-N-W], [R2] and [G-R].

COROLLARY: *Let α be an automorphism of order p^n of a free pro-p group F of rank 2. Then there exists an α-invariant abstract dense free subgroup of rank 2 in F.*

It is known that the automorphism group $\mathrm{Aut}(F_2)$ of a free pro-p group of rank 2 is much more complicated than the automorphism group $\mathrm{Aut}(\Phi_2)$ of the abstract free group Φ_2 of rank 2. Athough $\mathrm{Aut}(\Phi_2)$ is embedded in $\mathrm{Aut}(F_2)$ it is by no means dense there. In fact, V. Romankov [Ro] proved recently that $\mathrm{Aut}(F_n)$, $n > 1$, is (topologically) infinitely generated! Nevertheless Theorem 2 allows us to deduce that there are only a few conjugacy classes of torsion elements in $\mathrm{Aut}(F_2)$. They are described in the following

THEOREM 3: *Let p denote a prime. Let S denote the set of possible orders of torsion elements of* $\mathrm{Aut}(F_2)$, *where F_2 is the free pro-p group of rank* 2.

The conjugacy classes of elements of finite order coprime to p in $\mathrm{Aut}(F_2)$ *are in a natural one-to-one correspondence to the conjugacy classes of elements of order coprime to p in* $\mathrm{GL}_2(p)$.

Let $c(n)$ denote the number of conjugacy classes of automorphisms of order n.

(i) *For $s \in S$ with s coprime to p one has that s divides $p^2 - 1$. Furthermore $c(s) = \phi(s)s$, if s divides $p - 1$, and $c(s) = \phi(s)/2$ if s does not divide $p - 1$.*

Here ϕ denotes the Euler function.

(ii) *If $p = 2$, then $S = \{2, 3, 4\}$. One has $c(2) = 4$, $c(3) = 1$, $c(4) = 1$.*

(iii) *If $p = 3$, then $S = \{2, 3, 4, 8\}$. One has $c(2) = 2$, $c(3) = 1$, $c(4) = 1$, $c(8) = 2$.*

(iv) *If $p > 3$, then $s \in S$ is coprime to p.*

The proofs of all corresponding results for abstract groups (including the abstract analog of Serre's theorem) use a very poweful instrument, namely the theory of ends. There is nothing similar to a theory of ends in the context of a pro-p groups. The proofs in the present paper are based on the combinatorial methods in the category of pro-p groups.

2. Preliminaries

In addition to the above, we list here the notation and conventions that we use. Throughout the paper p denotes a prime number. In general, the groups in this paper are pro-p groups; whenever we deal with abstract groups we shall mention it explicitly. Subgroups of a pro-p group are assumed to be closed, and homomorphisms of pro-p groups are supposed to be continuous. If G is a pro-p group, we denote by G' (the closure of) its commutator subgroup, and by G^* its Frattini subgroup, i.e., $G^* = G^pG'$. We use $H \leq G$ (respectively, $H \leq_o G$, $H < G$, $H \triangleleft G$, etc.) to indicate that H is a subgroup (respectively, an open subgroup, a proper subgroup, a normal subgroup, etc.) of G. If $x, y \in G$, then $x^y = y^{-1}xy$ and $[x, y] = x^{-1}y^{-1}xy$, as usual. For $X, Y \leq G$, $[X, Y]$ denotes the subgroup of G generated by all commutators $[x, y]$ $(x \in X,\ y \in Y)$. If $H \leq G$, then $\mathcal{C}(H)$, $\mathcal{C}_G(H)$ and $\mathcal{N}_G(H)$ denote the center of H, the centralizer of H in G and the normalizer of H in G, respectively. For sets X and Y, we let $X - Y$ denote the difference set.

LEMMA 2.1: *For a pro-p group H let* $\mathrm{Tor}(H)$ *denote the subgroup generated by the torsion elements of H. Let p be a prime number, G a pro-p group and H an open subgroup of G.*

(i) *If* $\mathrm{Tor}(\mathcal{C}(H))$ *is a nontrivial finite group, then* $\mathrm{Tor}(\mathcal{C}(G))$ *is also finite and nontrivial.*

(ii) *If $\mathcal{C}(H)$ is finite nontrivial, so is $\mathcal{C}(G)$.*

Proof: (i) Suppose that this is not the case, and let $H <_o G$ be a counter example to our statement such that the index $[G : H]$ is minimal. If $[G : H] \neq p$, choose K to be an open subgroup of G containing H with $[G : K] = p$. Since $[K : H] < [G : H]$, we have that $\mathrm{Tor}(\mathcal{C}(K))$ is finite and nontrivial, by the minimality of $[G : H]$. Similarly, since $[G : K] < [G : H]$, one concludes that $\mathrm{Tor}(\mathcal{C}(G))$ is finite and nontrivial. This contradiction implies that in our minimal counterexample we must have $[G : H] = p$. Hence H is a normal subgroup of G; this is a consequence of the corresponding property for finite p-groups (cf. Theorem 4.3.2 of [H]), since G/H_G is a finite p-group and $H_G \leq H \leq G$, where $H_G = \bigcap_{g \in G} g^{-1}Hg$ is the core of H in G.

Note that $\mathrm{Tor}(\mathcal{C}(H))$ is normal in G. Consider the natural homomorphism

$$\varphi \colon G \longrightarrow \mathrm{Aut}(\mathrm{Tor}(\mathcal{C}(H)))$$

induced by conjugation, and denote its image by G_0. Then G_0 is finite and it acts on $\mathrm{Tor}(\mathcal{C}(H))$ as follows: if $g \in G$ and $z \in \mathrm{Tor}(\mathcal{C}(H))$, then $z^{\varphi(g)} = g^{-1}zg$. Consider the corresponding semidirect product $\Gamma_0 = \mathrm{Tor}(\mathcal{C}(H)) \rtimes G_0$. Since Γ_0 is a finite p-group and $1 \neq \mathrm{Tor}(\mathcal{C}(H)) \triangleleft_o \Gamma_0$, we deduce that

$$\mathrm{Tor}(\mathcal{C}(H)) \cap \mathcal{C}(\Gamma_0) \neq 1$$

(cf. [H], Theorems 4.3.1 and 4.3.4). Hence there exists some $1 \neq z \in \mathrm{Tor}(\mathcal{C}(H))$ such that for every $g \in G$, $z^{\varphi(g)} = g^{-1}zg = z$; thus $z \in \mathrm{Tor}(\mathcal{C}(G))$, i.e., $\mathrm{Tor}(\mathcal{C}(G)) \neq 1$.

Finally, we need to prove that $\mathrm{Tor}(\mathcal{C}(G))$ is finite. If $\mathrm{Tor}(\mathcal{C}(G))=\mathrm{Tor}(\mathcal{C}(H))$, this is clear. Otherwise, since $[G : H] = p$, one can find $g_0 \in \mathrm{Tor}(\mathcal{C}(G))$ with

$$\mathcal{C}(G) = \langle \mathcal{C}(G) \cap H,\ g_0 \rangle.$$

Because $[\mathcal{C}(G) : \mathcal{C}(G) \cap H] \leq p$, one infers

$$\mathcal{C}(G) = \langle \mathcal{C}(G) \cap H, g_0 \rangle \leq \langle \mathcal{C}(H), g_0 \rangle;$$

therefore the abelian group

$$\mathrm{Tor}(\mathcal{C}(G)) = \langle \mathrm{Tor}(\mathcal{C}(H)), g_0 \rangle$$

is finite.

Note that part (ii) follows from (i). ∎

LEMMA 2.2: *Let p be a prime number. Assume that a pro-p group G contains a proper open subgroup F which is a free pro-p group of rank 2. Then G has torsion.*

Proof: By a Theorem of Serre [S1], if G were torsion-free, it would be free pro-p, say of rank $d > 1$. Then (cf. [B-N-W]),

$$2 = \mathrm{rank}(F) = [G : F](d - 1) + 1 \geq 3,$$

a contradiction. ∎

Let A and B be pro-p groups and L a common subgroup of them. The amalgamated free pro-p product $A\coprod_L B$ is the push-out of A and B over L in the category of pro-p groups, if in addition the groups A and B are canonically embedded in H (cf. [R2] for more details).

LEMMA 2.3: *Let $G = \langle H, g\rangle$ be a pro-p group generated by a subgroup H and an element $g \notin H$, with $[G : H] < \infty$, and suppose that H is a free pro-p product with amalgamation*

$$H = A_1 \coprod_L A \coprod_{L'} B.$$

(i) *Let X denote any of the free factors of H and assume that X is a finite p-group, and X^g is conjugate to X in H, then there exists some element $g_0 \in \mathcal{N}_G(X) - H$ of finite order.*
(ii) *Assume in addition that $L = L' = A_1 = 1$, i.e. $H = A \coprod B$, $p \neq 2$, both A and B are finite p-groups and $g \in \mathcal{N}_G(H)$. Then there exists some element $g_0 \in \mathcal{N}_G(A) - A$ of finite order.*

Proof: (i) Let $x \in H$ be such that $X^g = X^x$. Then $g_0 = gx^{-1} \in \mathcal{N}_G(X) - H$. Since $[G : H] < \infty$, $g_0^{p^n} \in H$, for some natural number n. So $g_0^{p^n} \in \mathcal{N}_H(X)$, and therefore $g_0^{p^n} \in X$ (cf. [Z-M], Corollary (3.13)). It follows that g_0 has finite order.

(ii) Consider the set $\mathcal{S}$ of conjugacy classes (in H) of maximal finite subgroups of H. Then $\mathcal{S}$ consists of two elements, namely the classes represented by A and B (cf. [H-R1], Theorem 1). Obviously the odd-order group $\langle g\rangle$ acts trivially on the set $\mathcal{S}$. So A^g is a conjugate of A in H. The result then follows from part (i). ∎

Remark: Part (i) of the above Lemma could be proved in more generality. One could take H to be the fundamental group of a finite tree product of pro-p groups and A a finite vertex group; then under the assumptions of the Lemma we reach the same conclusion.

LEMMA 2.4:

(i) *If $p > 3$, $\mathrm{GL}_2(\mathbf{Z}_p)$ contains no nontrivial finite p-subgroups.*
(ii) *Let $A, B \in \mathrm{GL}_2(\mathbf{Z}_3)$ be such that $A^3 = B^3 = I$ and $[A, B] = I$. Then A and B generate a cyclic subgroup of $\mathrm{GL}_2(\mathbf{Z}_3)$.*
(iii) *$\mathrm{GL}_2(\mathbf{Z}_3)$ contains no elements of order 9.*
(iv) *Let H be a maximal abelian finite 2-subgroup of $\mathrm{GL}_2(\mathbf{Z}_2)$. Then H is conjugate to one of the following subgroups:*

(a) *the cyclic group of order* 4

$$\left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\rangle;$$

(b) *the Klein-four subgroup*

$$\left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle;$$

(c) *the Klein-four subgroup*

$$\left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right\rangle.$$

(v) *Let H be a maximal finite nonabelian 2-subgroup of* $\mathrm{GL}_2(\mathbf{Z}_2)$. *Then H is isomorphic to the dihedral group and, up to conjugation, contains*

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Proof: (i) Follows from Lemma 2.5 (iii) in [H-R-Z].

(ii) Let $A, B \in \mathrm{GL}_2(\mathbf{Z}_3)$ be such that $A^3 = B^3$ and $[A, B] = I$. From Lemma 2.5 (ii) in [H-R-Z] one may assume that

$$A = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

Note that $A^2 + A + I = 0$. If $[A, B] = I$, i.e. $AB = BA$, then, by equating matrix entries, one finds that $B = aI - bA$, for suitable $a, b \in \mathbf{Z}_3$. Assume that $B \neq I$; since $B^3 = I$, the minimal polynomial for B must be $T^2 + T + I$. By equating corresponding entries one finds the equations

$$a^2 + a + 1 - b^2 = 0 \quad \text{and} \quad b(2a + b + 1) = 0.$$

These equations have the solutions $(a, b) \in \{(0, -1), (-1, 1)\}$ over $\mathbf{Z}_3$, so that $B \in \{I, A, A^2\}$. Hence (ii) is proved.

(iii) Let $C \in \mathrm{GL}_2(\mathbf{Z}_3)$ be such that $C^9 = I$ but $C^3 \neq I$. By Lemma 2.5 (ii) in [H-R-Z] we may assume that

$$C^3 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

We remark that $[C, C^3] = I$; therefore, as in part (ii), $C = aI - bC^3$, for some $a, b \in \mathbf{Z}_3$. By equating matrix entries, one finds

$$a^3 - b^3 - 3ab^2 = 0 \quad \text{and} \quad 3ab(a+b) + 1 = 0.$$

The second of these equations cannot be solved for numbers $a, b \in \mathbf{Z}_3$, a contradiction. Therefore there is no matrix in $\mathrm{GL}_2(\mathbf{Z}_3)$ of order 9.

(iv) Let H be a maximal finite abelian 2-subgroup of $\mathrm{GL}_2(\mathbf{Z}_2)$. Let $C \in H$ be an involution. According to Lemma 2.5 of [H-R-Z], C is conjugate to one of the following matrices:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Assume

$$C = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

and let $I \neq X \in \mathrm{GL}_2(\mathbf{Z}_2)$. If $[C, X] = I$, then equating matrix entries one deduces that $X = a_X I + b_X C$, for suitable $a_X, b_X \in \mathbf{Z}_2$. Let X have order 2^n. We claim that $n = 1$. Suppose $n > 1$. Consider $Y := X^{2^{n-1}}$. Then $Y \neq I$ and $[C, Y] = I$; so, similarly, there exist $a_Y, b_Y \in \mathbf{Z}_2$ with $Y = a_Y I + b_Y C$. From $I = Y^2 = a_Y^2 I + 2a_Y b_Y C + b_Y^2 I$ one infers

$$a_Y^2 + b_Y^2 - 1 = 0 \quad \text{and} \quad 2a_Y b_Y = 0,$$

so that either $a_Y = 0$ or $b_Y = 0$.

If $b_Y = 0$, then $Y = -I$ since $Y \neq I$. Put $U := X^{2^{n-2}}$. Then, for suitable $a_U, b_U \in \mathbf{Z}_2$ one has $U = a_U I + b_U C$, and so

$$-I = Y = U^2 = (a_U^2 + b_U^2)I + 2a_U b_U C .$$

Hence, by equating entries we get

$$a_U^2 + b_U^2 + 1 = 0 \quad \text{and} \quad 2a_U b_U - 1 = 0 .$$

Here the second equation cannot be solved over $\mathbf{Z}_2$. So the case $b_Y = 0$ cannot happen.

Therefore $a_Y = 0$, and so $Y = \pm C$. Let $Z = X^{2^{n-2}}$. Then $[C, Z] = I$; hence, as before, there exist $a_Z, b_Z \in \mathbf{Z}_2$ with $Z = a_Z I + b_Z C$. Then $Z^2 = (a_Z^2 + b_Z^2)I + a_Z b_Z C = \pm C$ implies

$$a_Z^2 + b_Z^2 = 0 \quad \text{and} \quad a_Z b_Z = \pm 1.$$

The first equation has only the trivial solution $a_Z = b_Z = 0$. Then, however, the second equation cannot be solved, a contradiction. So $n = 1$. Therefore $I = X^2 = a_X^2 I + 2a_X b_X C + b_X^2 I$; one infers that

$$a_X^2 + b_X^2 - 1 = 2a_X b_X = 0,$$

so that either $a_X = 0$ or $b_X = 0$. Therefore $X \in \{I, -I, C, -C\}$, and since X had been chosen to be an arbitrary element of 2-power order commuting with C, we conclude that $H = \{I, -I, C, -C\}$. Thus case (b) holds.

Assume next that

$$C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in H.$$

Let $X \in H$; from $[C, X] = I$, one concludes that

$$X = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix},$$

where $d_i \in \{1, -1\}$, since X has finite 2-power order. Therefore X can have only order 2, and therefore $H = \{I, -I, C, -C\}$, i.e., case (c) holds.

Finally, assume that H contains no involutions that are conjugate to

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Then we may assume that $C = -I$. Since $-I$ is in the center of $\mathrm{GL}_2(\mathbf{Z}_2)$, C is then the only involution contained in H. Therefore, H must be cyclic, since it is abelian. By case (b) the group $\{I, -I\}$ is not a maximal finite abelian subgroup. So H must contain some Y with $Y^2 = C = -I$. By equating matrix entries, and taking into account that Y has order 4 and so it cannot be a diagonal matrix, one shows that Y must have the form

$$Y = \begin{bmatrix} a & b \\ c & -a \end{bmatrix},$$

where $a^2 + bc + 1 = 0$. Considering the latter equation mod $4\mathbf{Z}_2$ one deduces that it can only be solved over $\mathbf{Z}_2$, if either b or c is a unit in $\mathbf{Z}_2$. Without loss of generality we assume that c is a unit. Put

$$T = \begin{bmatrix} c^{-1} & ac^{-1} \\ 0 & 1 \end{bmatrix}.$$

Then

$$T^{-1} Y T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Replacing H by $T^{-1}HT$ if necessary, we may assume that

$$Y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in H.$$

Next pick any X in H with $[X,Y] = I$. Then by equating the matrix entries of XY and YX and using an argument similar to those above, one finds that $X \in \langle Y \rangle$. So case (a) holds.

(v) First note that a nonabelian finite 2-subgroup exists, namely

$$\left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle.$$

Pick any nonabelian maximal finite 2-subgroup H of $\mathrm{GL}_2(\mathbf{Z}_2)$. Then H must contain a nonabelian subgroup of order 8. There are precisely two isomorphism classes of groups of order 8:

$$Q_4 := \langle x, y |\, x^4 = y^4 = 1, x^2 = y^2 = [x,y] \rangle$$

and

$$D_4 := \langle x, y |\, x^4 = y^2 = 1, x^y = x^{-1} \rangle.$$

Claim 1: *Q_4 is not a subgroup of* $\mathrm{GL}_2(\mathbf{Z}_2)$.

Assume the claim to be false. Then, by case (iv)(a) one may assume that

$$X = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

and that

$$Y = \begin{bmatrix} a & b \\ c & -a \end{bmatrix},$$

where $a^2 + bc + 1 = 0$. Here we refer to the proof of case (a), in order to find Y with $Y^2 = -I$. Next note that $-I = X^2 = [X,Y] = XYXY$ implies the matrix equation $-I = (XY)^2$. By equating matrix entries one deduces the equations $a^2 + c^2 = a^2 + b^2 = -1$ and $a(b-c) = 0$. Since $a^2 + c^2 = -1$ cannot be solved for $a, c \in \mathbf{Z}_2$ a contradiction arises.

Claim 2: $H \cong D_4$.

Assume this is false. By Claim 1, H contains a proper subgroup L isomorphic with D_4. Since H is a finite 2-group one finds a subgroup K such that $L \triangleleft K < H$ and $[K:L] = 2$. Let N be the unique cyclic subgroup of L of order 4; then $N \triangleleft K$ and $[L:N] = 2$. Since $\mathrm{Aut}(N)$ has order 2, there exists $k \in K - N$ acting trivially by conjugation on N. Then, however, $\langle k, N \rangle$ would be an abelian subgroup of order 8 contradicting (iv).

CLAIM 3: *Up to conjugation*

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in H.$$

Assume not. Since H is dihedral, it can be generated by two involutions X and Y. As pointed out above, the involutions of $\mathrm{GL}_2(\mathbf{Z}_2)$ are conjugate to

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Since $-I$ is central, by (iv) we may assume that

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Consider the quotient group $\mathrm{GL}_2(\mathbf{F}_2) \cong S_3$ of $\mathrm{GL}_2(\mathbf{Z}_2)$, and let $\pi\colon \mathrm{GL}_2(\mathbf{Z}_2) \longrightarrow \mathrm{GL}_2(\mathbf{F}_2)$ denote the canonical epimorphism. Note that the 2-Sylow subgroup of S_3 has order 2. Since XY has order 4, it is conjugate to

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

so that $X \equiv XY \pmod{\ker(\pi)}$, i.e., $Y \equiv I \pmod{\ker(\pi)}$. Then Y cannot be a conjugate of X. Therefore we conclude from (iv) that Y is conjugate to

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

a contradiction.

This completes the proof of (v). ∎

3. The proof of the theorems

In this section we prove the theorems of the Introduction. We do this by considering a series of special cases.

PROPOSITION 3.1: *Let p be a prime number greater than 3. Let G be a pro-p group with an open normal subgroup F which is a free pro-p group of rank 2. Assume that G has trivial center. Then $G = F$.*

Proof: Assume $G \neq F$. By Lemma 2.2, G has torsion. Pick $g \in G - F$ with $g^p = 1$. Consider the automorphism φ of F defined by $\varphi(x) = g^{-1}xg$ ($x \in F$). Then $\varphi^p = \mathrm{id}_F$; hence by Theorem 6.7 of [H-R-Z], $\varphi = \mathrm{id}_F$. Therefore $\mathcal{C}(\langle g, F\rangle) \neq 1$. Since F has finite index in $\langle g, F\rangle$ and it has trivial center, it follows that $\mathcal{C}(\langle g, F\rangle)$ is finite. According to Lemma 2.1 this implies that $\mathcal{C}(G) \neq 1$, a contradiction. ∎

PROPOSITION 3.2: *Let G be a pro-3 group with a proper open normal subgroup F which is a free pro-3 group of rank 2. Assume that G has trivial center. Then $G \cong C_3 \coprod C_3$.*

Proof: We proceed by contradiction. Let G have a proper open free pro-3 subgroup F of rank 2, and suppose that G is a counterexample to our statement, i.e., assume that $G \not\cong C_3 \coprod C_3$. By Lemma 2.2, there exists an element $g \in G - F$ of order 3. If conjugation by g induces the trivial automorphism on F, then $\mathcal{C}(\langle g, F\rangle) \neq 1$, and so, by Lemma 2.1, $\mathcal{C}(G) \neq 1$, negating one of our hypotheses. Therefore conjugation by g induces a nontrivial automorphism on F, and hence, by Theorem 6.5 of [H-R-Z], $\langle g, F\rangle \cong A \coprod B$, where $A \cong B \cong C_3$. Note that $G \neq \langle g, F\rangle$, since G is a counterexample. Let

$$\langle g, F\rangle < L \leq G$$

with $(L : \langle g, F\rangle) = 3$. By Lemma 2.3, there exists an element of finite order $\ell \in L - \langle g, F\rangle$ that normalizes A, so $\ell \in \mathcal{N}_L(A)$. Then $\ell^3 \in \langle g, F\rangle \cong A \coprod B$; hence ℓ^3 is an element of order at most 3 (cf. [H-R1] Theorem A$'$). Suppose the order of ℓ^3 is 3; then the automorphism induced by ℓ^3 by conjugation on F has order 3, since, as we have pointed out above, otherwise ℓ^3 would centralize F, and this would imply that $\mathcal{C}(G) \neq 1$; therefore ℓ induces on F an automorphism of order 9. Now, the kernel of the natural map

$$\mathrm{Aut}(F) \longrightarrow \mathrm{Aut}(\mathbf{Z}_3 \times \mathbf{Z}_3)$$

is torsion-free (cf. [Lu] Theorem 5.8); hence ℓ induces on $\mathbf{Z}_3 \times \mathbf{Z}_3$ an automorphism of order 9. However, this is not possible by Lemma 2.4 (ii). Thus $\ell^3 = 1$. Since $\ell \in \mathcal{N}_L(A)$, we infer that there exist $1 \neq x \in A$ such that $x^3 = 1$ and $[\ell, x] = 1$. Therefore, by Lemma 2.4 (iii), either ℓx or ℓx^{-1} acts trivially on $F/F' \cong \mathbf{Z}_3 \times \mathbf{Z}_3$, and so, by Theorem 5.8 of [Lu], either ℓx or ℓx^{-1} acts trivially on F. Then, since $\ell x \neq 1 \neq \ell x^{-1}$, either $\langle \ell x, F\rangle$ or $\langle \ell x^{-1}, F\rangle$ has a nontrivial finite center, and thus, by Lemma 2.1, so does G, a contradiction. ∎

Our next results deal with pro-2 groups. We shall prove Theorem 2 for $p = 2$ in several steps, that will depend on the index of F in G. We distinguish three cases: $[G : F] = 2$, $[G : F] = 4$, and $[G : F] = 8$. There is a natural action of G/F on the $\mathbf{Z}_2$-module F/F'. So we have a homomorphism of G/F onto $\bar{G} \leq \mathrm{GL}_2(\mathbf{Z}_2)$.

First we state the following result on the structure of an automorphism of the free abelian pro-2 group $\mathbf{Z}_2 \times \mathbf{Z}_2$.

LEMMA 3.3: *Let $\bar{G}$ be as above.*

(i) *If $|G/F| > |\bar{G}|$ then $\mathcal{C}(G)$ is nontrivial and finite.*

(ii) *If $\bar{G}$ is of order 2 then w.r.t. a certain basis of $\mathbf{Z}_2 \times \mathbf{Z}_2$ it is generated by one of the following elements:*

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

(iii) *If $\bar{G}$ is of order 4 then w.r.t. a certain basis $\bar{G}$ has the following form:*

(a) *the cyclic group of order 4*

$$\left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\rangle;$$

(b) *the Klein-four subgroup*

$$\left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle;$$

(c) *the Klein-four subgroup*

$$\left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right\rangle.$$

(iv) *If $\bar{G}$ has order 8 then $\bar{G} \cong D_4$. One can assume that w.r.t. a certain basis,*

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in \bar{G}.$$

(v) *If $\mathcal{C}(G) = 1$ then $[G : F] \leq 8$.*

Proof of (i): In this case there exists $g \in G - F$ inducing the trivial action on F/F'. Next consider $H := \langle g, F \rangle$. Then H acts trivially on F/F'. By Lemma 2.2, H has torsion and so we may assume that g has finite order. Then g acts trivially on F by Theorem 5.8 in [Lu], and therefore $\mathcal{C}(H)$ is nontrivial and finite. Finally, by Lemma 2.1 (ii) we conclude the result.

Proof of (ii): This follows from Lemma 2.5 in [H-R-Z].

Proof of (iii): This follows from Lemma 2.4 (iv).

Proof of (iv): This follows from Lemma 2.4 (v).

Proof of (v): This follows from (i) together with Lemma 2.4 (iv)+(v).

So the Lemma is proved. ∎

PROPOSITION 3.4: *Let G be a pro-2 group with an open normal subgroup F of index 2 which is a free pro-2 group of rank 2. Assume that G has trivial center. With the notation from Lemma 3.3 one has:*

(a) *If, with respect to a basis of F/F', $\bar{G} = \left\langle \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle$, then*

$$G \cong C_2 \coprod C_2 \coprod C_2;$$

(b) *If, with respect to a basis of F/F', $\bar{G} = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle$, then*

$$G \cong C_2 \coprod \mathbf{Z}_2;$$

(c) *If, with respect to a basis of F/F', $\bar{G} = \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle$, then*

$$G \cong C_2 \coprod (C_2 \times \mathbf{Z}_2).$$

Proof: By Lemma 2.2 the existence of $\alpha \in G$ of order 2 is guaranteed.

(a) By Lemma 3.1 in [H-R-Z], there exists a basis $\{x, y\}$ of F such that $x^\alpha = x^{-1}$ and $y^\alpha = y^{-1}$. Hence, by Lemma 3.2 in [H-R-Z], $G \cong C_2 \coprod C_2 \coprod C_2$.

(b) Let $\{\bar{x}, \bar{y}\}$ be a basis of F/F' such that $\bar{x}^{\bar{\alpha}} = \bar{y}$, $\bar{y}^{\bar{\alpha}} = \bar{x}$. Let $x \in F$ map canonically onto $\bar{x} \in F/F'$. Then $y = x^\alpha$ maps canonically onto $\bar{y} \in F/F'$. Hence $\langle x, y\rangle F' = F$, and since F' is contained in the Frattini subgroup of F, one has $F = \langle x, y \rangle$, so that $\{x, y\}$ is a basis of F. Then $G \cong C_2 \coprod \mathbf{Z}_2$ (if a is a generator of C_2 and b a generator of $\mathbf{Z}_2$, then a can be identified with α, and b and b^a with x and y respectively).

(c) This case is harder. Since $\alpha|_{F/F'} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, there exists a basis $\{x, y\}$ of F such that $y^\alpha = y^{-1}$ and $x^\alpha = kx$, where $k \in F'$ (cf. Theorem 3.1 in [H-R-Z]).

Next we recall the notation and some facts from Theorem 5.3 in [H-R-Z]. Let Γ be the smallest normal closed subgroup of F containing y; then Γ is a free pro-2 group on a topological basis homeomorphic with $\mathbf{Z}_2$, specifically

$$\Gamma = \coprod_{\lambda \in \mathbf{Z}_2} \langle y^{x^\lambda} \rangle.$$

For $f \in F$ and $\lambda \in \mathbf{Z}_2$, define $c(\lambda, f) = (x^{-\lambda})^\alpha f x^\lambda$, and set

$$Y = \{c(\lambda, y) |\ \lambda \in \mathbf{Z}_2\}.$$

CASE 1: $k \in \Gamma^*$. In this case, it is proved in Theorem 5.3 of [H-R-Z] that the space $Y = \{c(\lambda, y) | \ \lambda \in Z_2\}$ is a topological basis of the free pro-2 group Γ, and α acts on each element u of Y by inverting it; furthermore, $c(\lambda, y) \equiv y^{x^\lambda}$ (mod Γ^*) . By Lemma 3.2 of [H-R-Z]

$$\langle \alpha, \Gamma \rangle = \left(\coprod_{u \in Y} \langle \alpha u \rangle \right) \coprod \langle \alpha \rangle,$$

where the first coproduct is taken over the profinite space Y. Note that the identity element 1 of G is not in Y; define $Y' = Y \cup \{1\}$; then 1 is an isolated point of Y', since Y is compact. Hence we may write

$$\langle \alpha, \Gamma \rangle = \coprod_{u \in Y'} \langle \alpha u \rangle.$$

Since $x^\alpha = kx$, it follows that

$$\alpha^x = x^{-1} k x \alpha \subseteq F' \alpha \subseteq \Gamma \alpha.$$

So $\alpha^x \in \langle \alpha, \Gamma \rangle$. Therefore, by Theorem 2 of [H-R1], α^x must be conjugate in $\langle \alpha, \Gamma \rangle$ to αu for some $u \in Y'$. In fact, we claim that it is conjugate to α. To see this, note first that since $k \in \Gamma^*$, $\alpha^x \equiv \alpha \pmod{\Gamma^*}$; and so $\alpha^x \equiv \alpha \pmod{\langle \alpha, \Gamma \rangle^*}$. Then the claim follows from the fact that $\alpha \not\equiv \alpha u \pmod{\langle \alpha, \Gamma \rangle^*}$ for all $u \in Y$. Thus $\alpha^x = \alpha^g$, for some $g \in \Gamma$. Then $xg^{-1} \in C_G(\alpha) - \Gamma$. Since $G^* = F^*$ (see claim 2 in the proof of Theorem 3.1 in [H-R-Z]), g is in $\langle y \rangle$ modulo F^*; hence $x' = xg^{-1}$ and y form a basis for F. Moreover, $x'^\alpha = x'$ and $y^\alpha = y^{-1}$. Finally we assert that this implies that

$$G = F \rtimes \langle \alpha \rangle \cong (C_2 \times Z_2) \coprod C_2.$$

To see this, let r and t be elements of order 2, and s a generator for $\mathbf{Z}_2$; then

$$(\langle r \rangle \times \langle s \rangle) \coprod \langle t \rangle = \langle s, rt \rangle \rtimes \langle r \rangle,$$

and clearly $s^r = s$ and $(rt)^r = (rt)^{-1}$. Therefore it suffices to check that $\langle s, rt \rangle \cong F$. Note that the minimal number

$$d((\langle r \rangle \times \langle s \rangle) \coprod \langle t \rangle)$$

of (topological) generators of

$$(\langle r \rangle \times \langle s \rangle) \coprod \langle t \rangle$$

is 3, since

$$d((\langle r\rangle \times \langle s\rangle)\coprod\langle t\rangle) = d((\langle r\rangle \times \langle s\rangle) + d(\langle t\rangle)$$

(cf. [Lu], Proposition 2.9). Therefore,

$$d(\langle s, rt\rangle) = 2.$$

Hence $t \notin \langle s, rt\rangle$ and $r \notin \langle s, rt\rangle$. It follows that $\langle s, rt\rangle$ is torsion-free since, being normal, it does not contain any conjugate of t or r (cf. [H-R1], Theorem A′). So,

$$\langle s, rt\rangle \cap \langle r, s\rangle = \langle s\rangle(\langle s, rt\rangle \cap \langle r\rangle) = \langle s\rangle,$$

and

$$\langle s, rt\rangle \cap \langle t\rangle = 1.$$

Since

$$\langle s, rt\rangle \lhd_o (\langle r\rangle \times \langle s\rangle)\coprod\langle t\rangle,$$

it follows from the Kurosh subgroup theorem (cf. [B-N-W]) that

$$\langle s, rt\rangle = \langle s, rt\rangle \cap \langle r, s\rangle \coprod \langle s, rt\rangle \cap \langle t\rangle \coprod T = \langle s\rangle \coprod T,$$

where T is a free pro-p group. Thus, $\langle s, rt\rangle$ is free pro-p of rank 2, and so

$$\langle s, rt\rangle \cong F,$$

as desired.

CASE 2: $k \notin \Gamma^*$. First we recall some facts about the structure of Γ/Γ^* (see section 4 in [H-R-Z] for details). The elements of Γ/Γ^* have the form y^a ($a \in \mathbf{F}_2[[\langle x\rangle]]$), where $\mathbf{F}_2[[\langle x\rangle]]$ is the completed group algebra. The map

$$\mathbf{F}_2[[\langle x\rangle]] \longrightarrow \Gamma/\Gamma^*$$

that sends a to y^a ($a \in \mathbf{F}_2[[\langle x\rangle]]$) is an isomorphism of $\mathbf{F}_2[[\langle x\rangle]]$-modules. Let $\kappa \in \mathbf{F}_2[[\langle x\rangle]]$ correspond to $k^{-x}\Gamma^* \in \Gamma/\Gamma^*$ under this isomorphism, i.e.,

$$y^\kappa \equiv k^{-x} \pmod{\Gamma^*}.$$

Since $\mathbf{F}_2[[\langle x\rangle]]$ is a local ring with unique maximal ideal $\langle x-1\rangle$, there exists a natural number m and a unit u of $\mathbf{F}_2[[\langle x\rangle]]$ such that

$$\kappa = (x-1)^m u.$$

The topological rings $\mathbf{F}_2[[\langle x\rangle]]$ and $\mathbf{F}_2\{\{T\}\}$ (the ring of formal power series in the indeterminate T over $\mathbf{F}_2$) are isomorphic under the correspondence $x \longmapsto T+1$ (cf. [L] Proposition 3.1.4, page 63). Hence

$$\Gamma/\Gamma^*\langle k^{-x}\rangle \cong \mathbf{F}_2[[\langle x\rangle]]/\langle\kappa\rangle \cong \mathbf{F}_2\{\{T\}\}/\langle T^m\rangle.$$

It follows that $1, x-1, \ldots, (x-1)^{m-1}$ form a basis for the $\mathbf{F}_2$-vector space $\mathbf{F}_2[[\langle x\rangle]]/\langle\kappa\rangle$, and therefore, $y, y^x, \ldots, y^{x^{m-1}}$ form a basis for $\Gamma/\Gamma^*\langle k^{-x}\rangle$.

Consider the elements

$$c_1 = y,\ c_2 = c(1,y),\ \ldots,\ c_m = c(m-1,y),$$

where, as above,

$$c(\lambda, f) = (x^{-\lambda})^\alpha f x^\lambda = (kx)^{-1}\lambda f x^\lambda \quad (f \in F, \lambda \in \mathbf{Z}_2).$$

Note that

$$(*) \qquad c(\lambda+1,k)^{-1}c(\lambda,y) = y^{x^\lambda}.$$

Put

$$K = \{c(\lambda,k) \mid \lambda \in \mathbf{Z}_2\} \quad \text{and} \quad C = \{c_1, \ldots, c_m\}.$$

It is proved in Theorem 5.3 of [H-R-Z] that the pointed topological space $U = C \cup K$, with distinguished point $\{1\}$, is a pointed topological basis of the free pro-2 group Γ; moreover, $u^\alpha = u^{-1}$ for all $u \in U$. It follows then as an easy generalization of Lemma 3.2 in [H-R-Z] that

$$\langle\alpha,\Gamma\rangle = \coprod_{u\in U} \langle\alpha u\rangle,$$

where the free pro-2 product is taken over the space U. Given $u \in U$, $(\alpha u)^x \in \langle\alpha,\Gamma\rangle$ has order 2, and so it is a conjugate in $\langle\alpha,\Gamma\rangle$ of $\alpha u'$, for some $u' \in U$ (cf. [H-R1] Theorem 2). Therefore,

$$(\alpha u)^x \equiv \alpha u' \pmod{\Gamma^*},$$

for each $u \in U$ and a corresponding $u' \in U$. In other words, the element x acts continuously on the subspace

$$\alpha U\Gamma^* = \{\alpha u\Gamma^* \mid u \in U\}$$

of Γ/Γ^*.

Since αK is homeomorphic with $\mathbf{Z}_2$, the points $c_1, c_2, \ldots, c_m$ are the only isolated points of the space U; so, the points $\alpha c_1\Gamma^*, \alpha c_2\Gamma^*, \ldots, \alpha c_m\Gamma^*$ are the only isolated points of $\alpha U\Gamma^*$. Hence x acts by conjugation on the finite subset

$$\{\alpha c_1\Gamma^*, \alpha c_2\Gamma^*, \ldots, \alpha c_m\Gamma^*\}.$$

Next observe that

$$(\alpha c_i)^x = x^{-1}\alpha c_i x = \alpha x^{-\alpha} c_i x = \alpha x^{-\alpha}(x^{1-i})^\alpha y x^{i-1} x = \alpha(x^{-i})^\alpha y x^i = \alpha c_{i+1}.$$

Therefore,

$$(\alpha c_m)^x\Gamma^* = \alpha c_{m+1}\Gamma^* \in \{\alpha c_1\Gamma^*, \alpha c_2\Gamma^*, \ldots, \alpha c_m\Gamma^*\},$$

and so

$$\alpha c_{m+1}\Gamma^* = \alpha c_1\Gamma^*.$$

Hence

$$c_{m+1}\Gamma^* = c_1\Gamma^* \quad \text{in } \Gamma/\Gamma^*.$$

Now, by $(*)$,

$$c_i = c(i,k)y^{x^{i-1}}.$$

So,

$$y = c_1 \equiv c_{m+1} = c(m+1,k)y^{x^m} \equiv k^{-x\frac{x^m-1}{x-1}} y^{x^m} \quad (\mathrm{mod}\ \Gamma^*),$$

where in the last congruence we use the fact that

$$c(\lambda+1,k) = k^{-x\frac{x^\lambda-1}{x-1}}$$

(see page 397 in [H-R-Z]*). Therefore,

$$y^{1-x^m} \equiv y^{\kappa\frac{x^m-1}{x-1}} \quad (\mathrm{mod}\ \Gamma^*).$$

Hence,

$$1 - x^m = \kappa\frac{x^m-1}{x-1} \quad \text{in } \mathbf{F}_2[[\langle x\rangle]].$$

Since $\mathbf{F}_2[[\langle x\rangle]]$ is an integral domain, one deduces that

$$\kappa = -(x-1).$$

* This corrects a misprint on page 397, line 8 of [H-R-Z].

Comparing this with the definition of m, we infer that

$$m = 1.$$

So

$$C = \{c_1\} = \{y\};$$

thus

$$(\alpha y)^x \equiv \alpha y \pmod{\Gamma^*},$$

and $\alpha y \Gamma^*$ is the only isolated point of the topological space $\alpha U \Gamma^*$ and so x must stabilize $\alpha y \Gamma^*$. Hence $(\alpha y)^x$ must be a conjugate of αy in $\langle \alpha, \Gamma \rangle$, say

$$(\alpha y)^x = (\alpha y)^z,$$

where $z \in \langle \alpha, \Gamma \rangle = \langle \alpha y \rangle \Gamma$. Write $z = \alpha y g$, with $g \in \Gamma$. Then

$$(\alpha y)^x = (\alpha y)^z = (\alpha y)^g.$$

So,

$$x g^{-1} \in \mathcal{C}_G(\alpha y) - \Gamma.$$

Next observe that $g \in \langle y, F' \rangle \leq \langle y, F^* \rangle$. Hence xg^{-1} and y are linearly independent mod F^*, i.e., $\{xg^{-1}, y\}$ is a basis for the free pro-2 group F. It follows that

$$G = \langle F, \alpha \rangle = \langle xg^{-1}, y, \alpha y \rangle = \langle xg^{-1}, y \rangle \rtimes \langle \alpha y \rangle,$$

and $\operatorname{order}(\alpha y) = 2$, $(xg^{-1})^{\alpha y} = xg^{-1}$, $y^{\alpha y} = y^{-1}$. Thus,

$$G = F \rtimes \langle \alpha \rangle \cong (C_2 \times Z_2) \coprod C_2,$$

as we established in Case 1. ∎

PROPOSITION 3.5: *Let G be a pro-2 group with an open normal subgroup F of index 4 which is a free pro-2 group of rank 2. Assume that G has trivial center. In the notation of Lemma 3.3:*

(d) $G \cong C_4 \coprod C_2$ *if*

$$\bar{G} = \left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\rangle;$$

(e) $G \cong (C_2 \times C_2) \coprod C_2$ *if*

$$\bar{G} = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle;$$

(f) $G \cong (C_2 \times C_2) \coprod_{C_2} (C_2 \times C_2) \coprod_{C_2} (C_2 \times C_2)$ *if*

$$\bar{G} = \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right\rangle.$$

Proof: Note that there exists a chain of normal subgroups of G

$$F < H < G,$$

so that $[H : F] = 2$. If $\mathcal{C}(H) \neq 1$, then $|\mathcal{C}(H)| = 2$ since $\mathcal{C}(H) \cap F = 1$; and this would imply, according to Lemma 2.1, that $\mathcal{C}(G) \neq 1$, contradicting our assumption. So, $\mathcal{C}(H) = 1$. Hence H is isomorphic to one of the groups (a), (b) or (c) of Proposition 3.4.

Next we proceed to prove a series of claims that will lead to a final proof of the Proposition.

Claim 1: *There exists an element $c \in H$ of order 2 whose conjugacy class in H is fixed by G under conjugation, and $\langle c \rangle$ is a free factor of H.*

Since H is a normal subgroup of G, the group G acts by conjugation on the set $\mathrm{Conj}(H)$ of conjugacy classes of involutions of H. In case (a), there are exactly three such classes (see Theorem A′ in [H-R1]); therefore the image of the action

$$G \longrightarrow \mathrm{Aut}(\mathrm{Conj})(H)) \cong S_3$$

must be of order 1 or 2, since G is a pro-2 group; hence G fixes at least one of the elements of $\mathrm{Conj}(H)$. In case (b), $\mathrm{Conj}(H)$ consists of just one element. Finally, if H is of the form (c), there are exactly two conjugacy classes of involutions in H; let $c_1, c_2 \in H$ be representatives of those classes; note that $\mathcal{C}_H(c_1) \neq \mathcal{C}_H(c_2)$; so no automorphism of H can map the conjugacy class of c_1 to the conjugacy class of c_2; hence, in this case, both conjugacy classes of involutions of H are fixed by the action of G.

Claim 2: *If c is as in Claim 1, there exists some element $g_0 \in G \setminus H$ of finite order such that $[g_0, c] = 1$.*

Since $\langle c \rangle$ is a free factor of H, the conditions of Lemma 2.3 (ii) apply. Hence there exists $g_0 \in G \setminus H$ of finite order such that $g_0 \in \mathcal{N}_G(\langle c \rangle) \setminus H$. Since c has order 2, one deduces that $[g_0, c] = 1$.

Observe that such g_0 has at most order 4 since $[G : F] = 4$ and that $\langle g_0, c, F \rangle = G$.

CLAIM 3: *If g_0 has order 4, then case (d) holds: $G \cong C_4 \coprod C_2$.*

Since $[G:F]=4$, $G=\langle g_0,F\rangle$ and $|\langle g_0,c\rangle|=4$. So $\langle g_0,c\rangle = C_4$ and $g_0^2=c$. Since g_0 has order 4, $\bar{G}$ is naturally isomorphic to $\langle g_0\rangle$. Hence by Lemma 3.3 the automorphism induced by g_0 on F/F' with respect to a certain basis of F is

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Therefore, the matrix of the automorphism of F/F' induced by conjugation by c is

$$\left\langle \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle.$$

Then

$$H \cong C_2 \coprod C_2 \coprod C_2,$$

by Proposition 3.3. Note that the basis of F/F' can be lifted to a basis $\{x,y\}$ of F such that

$$x^c = x^{-1} \quad \text{and} \quad y^c = y^{-1}$$

(cf. Theorem 3.1 in [H-R-Z]). On the other hand, it is clear that

$$H = \langle c, cx, cy\rangle.$$

Now, we know that

$$x^{g_0} \equiv y \pmod{F'} \quad \text{and} \quad y^{g_0} \equiv x^{-1} \pmod{F'},$$

and hence

$$(cx)^{g_0} \equiv cy \pmod{F'} \quad \text{and} \quad (cy)^{g_0} \equiv cx^{-1} \pmod{F'}.$$

Since g_0 fixes the conjugacy class of c, this means that g_0 permutes the conjugacy classes in H of cx and cy.

Consider two cyclic groups $\langle a\rangle$ and $\langle b\rangle$ of orders 4 and 2, respectively. Let

$$\varphi\colon P = \langle a\rangle \coprod \langle b\rangle \longrightarrow G$$

be the epimorphism determined by $\varphi(a)=g_0$ and $\varphi(b)=cx$.

We assert that φ is an isomorphism. To see this, observe first that $\ker(\varphi)$ is torsion-free, for a nontrivial element in P of finite order must be conjugate to either a, a^2, a^3 or b (cf. [H-R1] Theorem A′), and these elements are sent by φ

to g_0, g_0^2, g_0^3 , cx, respectively; but none of these is trivial. Put $L = \varphi^{-1}(F)$. It follows that L is torsion-free, since a torsion element of L must be in the kernel of φ. Note that L is an open normal subgroup of P; hence, by the Kurosh subgroup theorem, L is a free pro-2 group and its rank can be computed by means of the following formula (cf. [B-N-W]):

$$\operatorname{rank}(L) = ([P:L] - [P:L\langle a\rangle]) + ([P:L] - [P:L\langle b\rangle]) - [P:L] + 1 = 2.$$

Therefore $L \cong F$. It follows from the Hopfian property of finitely generated profinite groups that the restriction of φ to L is an isomorphism from L to F (cf. [R1] Proposition 7.6). Thus

$$L \cap \ker(\varphi) = 1.$$

Since $[P:L]$ is finite, this implies that $\ker(\varphi)$ is finite, and being torsion-free, it is trivial. So φ is an isomorphism and

$$G \cong C_4 \coprod C_2 .$$

This proves Claim 3.

Therefore, we may assume from now on that $\operatorname{order}(g_0) = 2$, so that $\langle g_0, c\rangle \cong C_2 \times C_2$. Denote by γ and ρ the automorphisms of F induced by conjugation by g_0 and c, respectively. Then $\langle \gamma, \rho\rangle \cong C_2 \times C_2$ since $\mathcal{C}(G) = 1$. Let $\bar\gamma$ and $\bar\rho$ be the automorphisms of F/F' induced by γ and ρ, respectively. We have

$$\bar G = \langle \bar\gamma, \bar\rho\rangle \cong C_2 \times C_2.$$

According to Lemma 3.3 (iv), there is a basis of F/F' such that one of the following is true:

Case 1: $\bar G = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle;$

Case 2: $\bar G = \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right\rangle;$

Claim 4: *In Case 1, $G \cong (C_2 \times C_2) \coprod C_2$.*

By assumption there exists an element $c_1 \in \langle g_0, c\rangle$ that induces an automorphism on F/F' whose matrix with respect to an appropriate basis is

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Hence, by using Theorem 3.1 of [H-R-Z], this basis can be lifted to a basis $\{x, y\}$ of F such that

$$x^{c_1} = x^{-1} \quad \text{and} \quad y^{c_1} = y^{-1}.$$

Note that

$$H_1 = \langle c_1, F \rangle = \langle c_1, c_1 x, c_2 y \rangle \cong C_2 \coprod C_2 \coprod C_2,$$

by Lemma 3.2 of [H-R-Z], and observe that H_1 has index 2 in G. Also, there exists $c_2 \in \langle g_0, c \rangle - H_1$ such that

$$x^{c_2} \equiv y \quad \text{and} \quad y^{c_2} \equiv x \pmod{F'}\ .$$

Hence

$$F_1 = \langle x, x^{c_2} \rangle$$

is a free pro-2 group with basis $\{x, x^{c_2}\}$, and c_2 permutes the elements of this basis. Furthermore, one easily checks that

$$x^{c_1} = x^{-1} \quad \text{and} \quad (x^{c_2})^{c_1} = (x^{c_2})^{-1}.$$

Thus $G = \langle c_1, c_2, c_1 x \rangle$.

Consider groups $\langle a_1 \rangle$, $\langle a_2 \rangle$ and $\langle a_3 \rangle$, each of order 2, and the epimorphism

$$\varphi\colon (\langle a_1 \rangle \times \langle a_2 \rangle) \coprod \langle a_3 \rangle \longrightarrow G$$

determined by $\varphi(a_1) = c_1$, $\varphi(a_2) = c_2$ and $\varphi(a_3) = c_1 x$. We assert that φ is an isomorphism. To see this, remark first that $\ker(\varphi)$ is torsion-free since an element of finite order of $\langle a_1 \rangle \times \langle a_2 \rangle) \coprod \langle a_3 \rangle$ must be conjugate to either a_1, a_2, $a_1 a_2$ or a_3 (cf. Theorem A$'$ in [H-R1]); and hence φ cannot map such an element to 1. Since F is torsion-free, it follows that $\varphi^{-1}(F)$ is also torsion-free. Note that $\varphi^{-1}(F)$ is a normal subgroup of $\langle a_1 \rangle \times \langle a_2 \rangle) \coprod \langle a_3 \rangle$ of index 4. Therefore, by the Kurosh subgroup theorem for pro-2 products, $\varphi^{-1}(F)$ is a free pro-2 group of rank 2 (cf. [B-N-W]). Hence the restriction of φ to $\varphi^{-1}(F)$ is an isomorphism from $\varphi^{-1}(F)$ to F (cf. [R1] Proposition 7.6). So $\varphi^{-1}(F) \cap \ker(\varphi) = 1$. Since $[G : \varphi^{-1}(F)] = 4$ and $\ker(\varphi)$ is torsion-free, one deduces that $\ker(\varphi) = 1$, as asserted.

Claim 5: *In Case 2, $G \cong (C_2 \times C_2) \coprod_{C_2} (C_2 \times C_2) \coprod_{C_2} (C_2 \times C_2)$.*

By assumption there are elements $c_1, c_2 \in \langle g_0, c \rangle$ such that the automorphisms they induce on F/F' can be represented by matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

respectively, with respect to a convenient common basis for the free abelian pro-2 group F/F'. Clearly

$$\langle c_1, c_2\rangle = \langle g_0, c\rangle.$$

Consider the automorphism induced on F by conjugation by c_1; by Theorem 3.1 in [H-R-Z] the basis of F/F' can be lifted to a basis $\{x, y_0\}$ of F such that

$$(**) \qquad x^{c_1} = x \quad \text{and} \quad y_0^{c_1} = y_0^{-1}\ .$$

By Proposition 3.3 (c), we have

$$L = \langle F, c_1\rangle = (\langle c_1\rangle \times \langle x\rangle) \coprod \langle c_1 y_0\rangle.$$

Put $L_1 = \langle c_1, x\rangle = \langle c_1\rangle \times \langle x\rangle$; then

$$L = L_1 \coprod \langle c_1 y_0\rangle.$$

By Theorem B$'$ of [H-R1],

$$\mathcal{C}_L(c_1) = L_1.$$

Now,

$$L_1^{c_2} = (\mathcal{C}_L(c_1))^{c_2} = \mathcal{C}_L(c_1^{c_2}) = \mathcal{C}_L(c_1) = L_1.$$

Hence $x^{c_2} = c_1^i x^r$ ($i = 0, 1; r \in \mathbf{Z}_2$). But on the other hand, taking into account the form of the matrix of the action of c_2 on F/F', we have that $x^{c_2} = x^{-1}f'$, for some $f' \in F'$. It follows that $i = 0$, $f' = 1$ and $r = -1$, i.e., $x^{c_2} = x^{-1}$.

Exchanging the roles of c_1 and c_2 one finds a basis $\{x_0, y\}$ of F such that

$$(***) \qquad y^{c_2} = y, \quad y^{c_1} = y^{-1}.$$

One deduces that $\{x, y\}$ is a basis for the group F ; for otherwise, $y = xx^*$, where $x^* \in F^*$, the Frattini subgroup of F; this would imply that $\{y, y_0\}$ is a basis of F and hence that the matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

are similar over the ring $\mathbf{Z}_2$, a contradiction.

Let A be the free pro-2 product with amalgamation

$$A = (\langle a_1\rangle \times \langle a_2\rangle) \coprod_{a_1 = a_3} (\langle a_3\rangle \times \langle a_4\rangle) \coprod_{a_4 = a_6} (\langle a_5\rangle \times \langle a_6\rangle),$$

where $a_i, i = 1, \dots, 6$ are elements of order 2. Note that $A = \langle a_1, a_2, a_4, a_5\rangle$. Let

$$\varphi\colon \{a_1, a_2, a_4, a_5\} \longrightarrow \{c_1, c_2x, c_2, c_1y\}$$

be a map defined as follows:

$$\varphi(a_1) := c_1, \quad \varphi(a_2) := c_2x, \quad \varphi(a_4) := c_2, \quad \varphi(a_5) := c_1y.$$

Next extend φ by setting

$$\varphi(a_3) := \varphi(a_1), \quad \varphi(a_6) := \varphi(a_4).$$

By using the formula (**) one verifies that $\varphi(\{a_1, \dots, a_6\})$ satisfies the same relations as $\{a_1, \dots, a_6\}$. So φ extends to an epimorphism from A to G. We shall prove that φ is an isomorphism. First note that $\ker(\varphi)$ is torsion-free for, according to Theorem (3.11) in [Z-M], any nontrivial element of finite order in A must be conjugate to an element of the set $\{a_i, i = 1, \dots, 6\} \cup \{a_1a_2, a_3a_4, a_5a_6\}$, and clearly none of these elements is in $\ker(\varphi)$. It follows that $\varphi^{-1}(F)$ is torsion-free since F is torsion-free.

Recall (cf. [R2]) that A is the pro-2 completion of the abstract free product with amalgamation

$$A_0 = (\langle a_1\rangle \times \langle a_2\rangle) \star_{a_1=a_3} (\langle a_3\rangle \times \langle a_4\rangle) \star_{a_4=a_6} (\langle a_5\rangle \times \langle a_6\rangle).$$

Define a tree with three vertices $\{v_1, v_2, v_3\}$ connected with two edges $\{e_1, e_2\}$ such that e_i connects v_i with v_{i+1} for $i = 1, 2$. Define a tree of groups with $G(v_1) := \langle a_1\rangle \times \langle a_2\rangle$, $G(v_2) := \langle a_3\rangle \times \langle a_4\rangle$, $G(v_3) := \langle a_5\rangle \times \langle a_6\rangle$, $G(e_1) := \langle a_1 = a_3\rangle$, $G(e_2) := \langle a_4 = a_6\rangle$.

In this way A_0 can be naturally identified with the fundamental group of this tree of groups.

Since $\varphi^{-1}(F)$ is an open subgroup of A, it is the pro-2 completion of $A_0 \cap \varphi^{-1}(F)$. We claim that $A_0 \cap \varphi^{-1}(F)$ is a free abstract group of rank 2. Since $A_0 \cap \varphi^{-1}(F) \triangleleft A_0$ and $A_0 \cap \varphi^{-1}(F)$ intersects trivially with the free factors in A_0, we conclude from Proposition 11, p.120 in [S2] that $A_0 \cap \varphi^{-1}(F)$ is a free subgroup of index 4 in A_0.

According to a theorem of Serre (see [S2], Exercise 3 on p.103) we have

$$\begin{aligned}\operatorname{rank}(A_0 \cap \varphi^{-1}(F)) &= 1 + [A_0 : A_0 \cap \varphi^{-1}(F)]\left(\sum_{i=1}^{2} \frac{1}{|G(e_i)|} - \sum_{i:=1}^{3} \frac{1}{|G(v_i)|}\right)\\ &= 1 + 4\left(\left(\frac{1}{2} + \frac{1}{2}\right) - \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right)\right) = 2.\end{aligned}$$

Thus the subgroup $\varphi^{-1}(F)$ of A is free pro-2 of rank 2. Therefore, the restriction of φ to $\varphi^{-1}(F)$ maps the free pro-2 group $\varphi^{-1}(F)$ onto the free pro-2 group F, and so it is an isomorphism (cf. Proposition 7.6 in [R1]). It follows that $\ker(\varphi) \cap \varphi^{-1}(F) = 1$; hence $\ker(\varphi)$ is finite, and thus $\ker(\varphi) = 1$, since it is torsion-free. Therefore φ is an isomorphism. ∎

PROPOSITION 3.6: *Let G be a pro-2 group with an open normal subgroup F of index 8 which is a free pro-2 group of rank 2. Assume $\mathcal{C}(G) = 1$. Then, in the notation of Lemma 3.3, $\bar{G} \cong D_4$ and $G \cong D_4 \coprod_{C_2} (C_2 \times C_2)$.*

Proof: Since G/F is a finite 2-group, there exist intermediate subgroups

$$F < H < G$$

such that $[H : F] = 4$ and $[G : H] = 2$ (cf. [H] Theorem 4.3.2) and $H \triangleleft G$. By Lemma 2.1, $\mathcal{C}(H) = 1$. Then H is isomorphic to one of the groups (d), (e) or (f) of Proposition 3.5. Since $[G : H] = 2$ one can find $g \in G - H$ so that $G = \langle g, H\rangle$. Observe that the group H contains a maximal finite subgroup X such that X^g is conjugate in H to X (cf. [Z-M], Theorem (3.11)): namely, in case (d), $X \cong C_4$ is a free factor of H; in case (e), $X \cong C_2 \times C_2$ is a free factor of H; in case (f), G acts on the set of conjugacy classes of maximal finite subgroups of H by permutation; since there are exactly three of them, we conclude that one of them is fixed. We fix X to be the free amalgamated factor which belongs to this conjugacy class.

In any case, we deduce from Lemma 2.3 that there exists an element $g_0 \in \mathcal{N}_G(X) \setminus H$ of finite order. Therefore, $T = \langle g_0, X\rangle$ is a group of order 8, and $G = F \rtimes T$. Note $T \cong \bar{G} \cong D_4$. By Lemma 2.4 (v) we may assume that

$$K := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in \bar{G}.$$

Let $\bar{H}_1$ denote a normal subgroup of index 2 containing the matrix K. Let H_1 denote the preimage of $\bar{H}_1$. Then by Proposition 3.5 (f)

$$H_1 \cong (C_2 \times C_2) \coprod_{C_2} (C_2 \times C_2) \coprod_{C_2} (C_2 \times C_2).$$

There exists $t \in T - H_1$. Let $A = \langle c_1, c_2\rangle$ denote the middle factor in the decomposition of H_1 above where c_1, c_2 are generators of the amalgamating subgroups.

We claim that t leaves the conjugacy class of A invariant. In order to prove this consider the set of the conjugacy classes of maximal abelian finite subgroups of H_1. By Theorem (3.11) in [Z-M] each of the three factors represents precisely one such conjugacy class. Next note that c_1, c_2 are the only involutions in H_1 up to conjugation having infinite centralizers in H_1. Therefore the only factor having two involutions with infinite centralizers is precisely A. Hence t leaves this conjugacy class invariant.

By Lemma 2.3 (ii) one finds $g_1 \in (G - H_1) \cap \mathcal{N}_G(A)$. Note that $g_1^2 \in H_1 \cap \mathcal{N}_G(A) = A$, where the latter equality follows from Corollary (3.13) in [Z-M]. So $L := \langle A, g_1 \rangle$ has order 8. Since $L \cap F = 1$ we conclude $L \cong \bar{G} \cong D_4$. So L is not abelian and since, as remarked above, c_1 and c_2 are the only involutions having infinite centralizers, we conclude that $c_1^{g_1} = c_2$.

Therefore the conjugacy classes of the first and the last factor in the decomposition of H_1 are permuted by g_1. Let $A_1 := \langle c_1, c_0 \rangle$ now denote the first factor. Then $G = \langle A_1, g_1 \rangle$.

Define

$$B := \langle b_1, b_2 |\, b_1^2 = b_2^4 = 1, b_2^{b_1} = b_2^{-1} \rangle \coprod_{b_1 = b_3} \langle b_3, b_4 |\, b_3^2 = b_4^2 = [b_3, b_4] = 1 \rangle.$$

Note that $d(B) = 3$.

Let

$$\phi : \{b_1, b_2, b_4\} \longrightarrow \{c_1, g_1, c_0\}$$

be a map defined as follows:

$$\phi(b_1) := c_1, \quad \phi(b_2) := g_1, \quad \phi(b_4) := c_0.$$

Note that ϕ extends to an epimorphism from B onto G.

Recall that B is the pro-2 completion of the abstract free product

$$B_0 := \langle b_1, b_2 |\, b_1^2 = b_2^4 = 1, b_2^{b_1} = b_2^{-1} \rangle *_{b_1 = b_3} \langle b_3, b_4 |\, b_3^2 = b_4^2 = [b_3, b_4] = 1 \rangle.$$

Since $\phi^{-1}(F)$ is an open subgroup of B, it is the pro-2 completion of $B_0 \cap \phi^{-1}(F)$. We claim that $B_0 \cap \phi^{-1}(F)$ is a free abstract group of rank 2. Since $B_0 \cap \phi^{-1}(F) \triangleleft B_0$ and it intersects trivially with the free factors in B_0, an application of the Kurosh subgroup theorem yields that $B_0 \cap \phi^{-1}(F)$ is a free subgroup of index 8 in B_0.

Moreover by exercise 2) on p.57 in [S2] one has

$$\operatorname{rank}(B_0 \cap \phi^{-1}(F)) = 1 - 4 + (4 - 1) + (4 - 2) = 2.$$

Therefore $d(\phi^{-1}(F)) = 2$. Hence the restriction of ϕ to $\phi^{-1}(F)$ maps the free pro-2 group $\phi^{-1}(F)$ onto the free pro-2 group F, and so it is an isomorphism (cf. Proposition 7.6 in [R1]). It follows that $\ker(\phi) \cap \phi^{-1}(F) = 1$; hence $\ker(\phi)$ is finite, and thus $\ker(\phi) = 1$, since it is torsion free. Therefore ϕ is an isomorphism. ∎

We are finally in a position to finish the proof of Theorem 2.

Proof of Theorem 2: We simply put together the results of this section. Assume $F \neq G$. Then Proposition 3.1 proves the Theorem for $p > 3$, Proposition 3.2 for $p = 3$, Proposition 3.4 for $p = 2$ in case $[G : F] = 2$, Proposition 3.5 for $p = 2$ in case $[G : F] = 4$, and Proposition 3.6 for $p = 2$ in case $[G : F] = 8$. Finally Lemma 3.3 (v) shows that if $p = 2$ and $[G : F] \geq 16$, then $\mathcal{C}(G) \neq 1$, so that, in fact, this case does not arise under the conditions of the Theorem. These cover all cases, and thus the theorem follows. ∎

Proof of the Corollary: Let $G := F \rtimes \langle \alpha \rangle$ be the holomorph. We claim that $\mathcal{C}(G) = 1$. Indeed, assume $1 \neq g \in \mathcal{C}(G)$. Since $\mathcal{C}(F) = 1$ one can find $k \in \mathbf{N}$ and $f \in F$ with $g = f\alpha^k$. Since $[g, \alpha] = 1$ one has $[f, \alpha] = 1$ and so $(f\alpha^k)^{p^n} = f^{p^n} = 1$, so that $f = 1$. Hence $\alpha^k = 1$, i.e., $g = 1$, a contradiction arises. So the claim holds.

Thus G has the form as stated in Theorem 2. Therefore by Theorem (3.11) in [Z-M] α is conjugated to an element of one of the factors of G. Assume w.l.o.g. that α is contained in one of the factors. Let G_0 denote the abstract group obtained from the construction of G by replacing $\coprod$ by $*$ and $\mathbf{Z}_2$ through $\mathbf{Z}$. Note that G is the pro-p completion of G_0 and so G_0 can be considered as a dense subgroup of G containing α. Therefore $G_0 \cap F$ is an abstract free dense α-invariant subgroup. ∎

Lemma 3.7: *Let G be a pro-p group which is a finite extension of $\mathbf{Z}_p$. Suppose that the center of G is torsion free. Then either $G \cong \mathbf{Z}_p$ or it is the dihedral pro-2 group $G \cong C_2 \coprod C_2$.*

Proof: Let $p > 2$. If G has an element g of finite order, then since $\mathrm{Aut}(\mathbf{Z}_p) \cong \mathbf{Z}_p \times C_{p-1}$ the element g must centralize $\mathbf{Z}_p$. Hence by Lemma 2.1 the center of G is nontrivial. This means that G is torsion free and therefore isomorphic to $\mathbf{Z}_p$.

Let $p = 2$. If G is torsion free, then $G \cong \mathbf{Z}_2$ and we are done. Suppose G has torsion. Consider $C = C_G(\mathbf{Z}_2)$. We claim $[G : C] = 2$. Indeed C is torsion free, since otherwise we have a contradiction by Lemma 2.1, so $C \cong \mathbf{Z}_2$. Therefore C admits a unique automorphism of order 2 ($\mathrm{Aut}(\mathbf{Z}_2) \cong \mathbf{Z}_2 \times C_2$). This implies that the product of any two elements $g, h \in G - C$ belongs to C, since gh centralizes C. It follows that $[G : C] = 2$ and $G = C \rtimes C_2 \cong C_2 \coprod C_2$. ∎

Proof of Theorem 1: If the center of G is torsion free, we are done by Theorem 2 and Lemma 3.7. Assume G has a finite central subgroup C. We shall argue by induction on the index $[G : F]$. Consider the epimorphism $f : G \longrightarrow G/C$. Since $[G/C : f(F)] < [G : F]$, by the inductive hypothesis $G/C = \Pi_1(\mathcal{H}, \Delta)$ is the pro-p fundamental group of a finite graph Δ of finite p-groups. Define a graph of groups $(\mathcal{G}, \Delta)$ by setting $\mathcal{G}(m) = f^{-1}(\mathcal{H}(m))$ for all $m \in \Delta$ with embeddings of the edge groups into the vertex groups defined in an obvious way. Then using the universal property of the fundamental group (see (3.2) in [Z-M]) it is easy to check that $G \cong \Pi_1(\mathcal{G}, \Delta)$. ∎

Proof of Theorem 3: The first statement of the Theorem follows from Lemma 3.1 in [H-R2].

We turn to the proof of (i)–(iii).

Proof of (i): By the first statement of the Theorem it is enough to consider the conjugacy classes in $\mathrm{GL}_2(p)$ of elements whose order is prime to p. These conjugacy classes can be represented as follows (see [G], p. 404):

(a) diagonal matrices with entries in $\mathbf{F}_p$;

(b) upper triangular matrices with equal elements on the diagonal;

(c) companion matrices of quadratic irreducible polynomials over $\mathbf{F}_p$.

We next count the conjugacy classes of matrices of order s:

For (a) there are exactly $\phi(s)s$ such matrices.

For (b) we just note that all elements of that form are of order divisible by p.

For (c) we use 2.47. Theorem (ii) in [L-N]. One finds, in our case, that the cyclotomic polynomial of a primitive sth root of unity over $\mathbf{F}_p$ factors into exactly $\phi(s)/d$ distinct monic irreducible polynomials of the same degree d, where d is the least positive integer such that $p^d \equiv 1 \pmod{s}$ holds. In our situation $d = 2$, so that s divides $p^2 - 1$ but must not divide $p - 1$.

Summarizing, we find that the number of conjugacy classes of matrices of order s dividing $p - 1$ is $\phi(s)s$; and if s does not divide $p - 1$, $\phi(s)/2$.

Proof of (ii): Here $p = 2$.

Claim 1: *I.* f $s \in S$, there exists $k \in \mathbf{N}$ with $s = 2^k 3$.

This follows from Lemma 2.5 (i) in [H-R2] together with Theorem 5.8 in [Lu].

Claim 2: $6 \notin S$.

Let $\alpha, \gamma \in \mathrm{Aut}(F_2)$ have orders 3 and 2 respectively and assume that $[\alpha, \gamma] = 1$. First consider the action of α and γ induced on F_2/F_2'. By Lemma 3.3, we may assume that in F_2/F_2' we have chosen a basis such that γ has one of the following forms:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

On the other hand, one can check that there are no matrices of order 3 which commute with the first two matrices. So γ must have the form of the last matrix.

By Theorem 3.1 in [H-R-Z] one finds a basis $\{x, y\}$ of F_2 with $x^\gamma = x^{-1}$ and $y^\gamma = y^{-1}$. Since α acts fixed point free on F_2/F_2^*, we conclude that $F_2 = \langle x, x^\alpha \rangle$. By assumption, α and γ commute; therefore the elements x^α and x^{α^2} get inverted by γ. So one can choose $y = x^\alpha$. Next consider the action of α and γ on $\Phi := F_2/[F_2, F_2']$. Since every nontrivial automorphism α of $F_2/F_2' \cong \mathbf{Z}_2 \times \mathbf{Z}_2$ of order 3 satisfies the matrix equation $\alpha^2 + \alpha + I = 0$, there exists $k \in \Phi'$ with $x^{\alpha^2} = y^\alpha = x^{-1}y^{-1}k$. Here and up to the end of the proof of Claim 2 we denote the images of x and y in Φ by the same letters respectively. Note that $\Phi' = \langle [x, y] \rangle \cong \mathbf{Z}_2$ and so α and γ act trivially on Φ'. Since α and γ commute one immediately finds $y^{\gamma\alpha} = (y^{-1})^\alpha = yxk^{-1}$. On the other hand $y^{\alpha\gamma} = x^{-\gamma}y^{-\gamma}k = xyk$. Therefore $[x, y] = k^{-2}$. Since $[x, y]$ is a generator of Φ', and $k^{-2} \in (\Phi')^*$, a contradiction arises. Thus $\mathrm{Aut}(F_2)$ cannot contain an automorphism of order 6, i.e., $6 \notin S$.

Claim 3: $\{2, 4\} \subseteq S$.

This follows from Theorem 2(3).

Claim 4: $S = \{2, 3, 4\}$.

This follows immediately from Claims 1, 2 , 3 and Lemma 2.4 (iv)+(v) together with Theorem 5.8 in [Lu].

Claim 5: $c(2) = 4$.

Let α be an automorphism of F_2 of order 2. By Proposition 3.4 there are exactly three types (a), (b), and (c) of $G := F_2 \rtimes \langle \alpha \rangle$ which correspond to the three conjugacy classes of induced automorphisms on F_2/F_2' listed in Lemma 3.3.

If (a) holds, then by Theorem 3.3 in [H-R-Z] there is a basis $\{x, y\}$ of F_2 such that $x^\alpha = x^{-1}$ and $y^\alpha = y^{-1}$. Therefore such an α is unique up to conjugation in $\mathrm{Aut}(F_2)$.

If (b) holds, then there exists $x \in F_2$ such that $F = \langle x, x^\alpha \rangle$. Therefore such an α is unique up to conjugation in $\mathrm{Aut}(F_2)$.

If (c) holds, then $G := C_2 \coprod (C_2 \times \mathbf{Z}_2) = \langle c_1 \rangle \coprod (\langle c_2 \rangle \times \langle z \rangle)$, and so there exists $f \in F_2$ with $\alpha^f = c_i$ for exactly one $i \in \{1, 2\}$.

Therefore α is conjugate in $\mathrm{Aut}(F_2)$ to the automorphism induced by conjugation with c_1 or c_2. So we can assume that $\alpha \in \{c_1, c_2\}$. Note that z or αz belongs to F_2 and let y denote this element. Pick a basis $\{x := c_1 c_2, y\}$ of F_2.

If $\alpha = c_2$ then α fixes y and inverts x, and there is only one such α up to conjugation in $\mathrm{Aut}(F_2)$.

If $\alpha = c_1$ then α cannot have fixed points in F_2 since $C_G(c_1) = \langle c_1 \rangle$ by Theorem B in [H-R1]. Note that $x^\alpha = x^{-1}$, $y^\alpha = y^x$. Such an α is unique up to conjugation in $\mathrm{Aut}(F_2)$.

Claim 6: $c(3) = 1$.

Since $\mathrm{GL}_2(2) \cong S_3$ contains only one conjugacy class of elements of order 3, the claim follows from the first statement of the Theorem.

Claim 7: $c(4) = 1$.

Let $\alpha \in \mathrm{Aut}(F_2)$ have order 4. So, by Proposition 3.5 (d), $G = C_4 \coprod C_2 = \langle c_1 \rangle \coprod \langle c_2 \rangle$. Hence there exists $f \in F_2$ with $\alpha^f = c_1$ by Theorem A in [H-R1]. Therefore α is conjugate in $\mathrm{Aut}(F_2)$ to the automorphism induced by conjugation with c_1. Note that G contains precisely one free pro-2 subgroup of index 4, namely F_2. Let $x := \alpha^2 c_2$, $y := \alpha c_2 \alpha$, then $F_2 = \langle x, y \rangle$ and $x^\alpha = y$, $y^\alpha = x^{-1}$. Thus there is only one such α up to conjugation in $\mathrm{Aut}(F_2)$.

This completes the proof of (ii).

Proof of (iii):

Claim 1: *If $s \in S$, there exists $k \in \mathbf{N}$ with $s = 2^k 3$.*

The proof of this follows from Lemma 2.5 (ii) in [H-R2] together with Theorem 5.8 in [Lu].

Claim 2: $6 \notin S$.

Let $\alpha, \gamma \in \mathrm{Aut}(F_2)$ have orders 3 and 2 respectively and assume $[\alpha, \gamma] = 1$.

First consider the action of α and γ induced on F_2/F_2'. By Maschke's Theorem one may assume that γ corresponds to a diagonal matrix

$$\left\langle \begin{bmatrix} \varepsilon_1 & 0 \\ 0 & \varepsilon_2 \end{bmatrix} \right\rangle$$

where $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$. We now show that both of them are -1. Suppose not; then from $[\alpha, \gamma] = I$ one deduces that α with respect to the same basis must have a diagonal form contradicting the fact that α is of order 3. Thus γ inverts every element of F_2/F_2'.

By Theorem 2 (2), $G \cong \langle\alpha\rangle \coprod \langle\beta\rangle \cong C_3 \coprod C_3$. We fix a basis $\{x, y\}$ of F_2 such that $x^\alpha = y$ and $y^\alpha = x^{-1}y^{-1}$ (in fact put $x := \beta\alpha^{-1}, y := \alpha^{-1}\beta$).

Next consider the action of α and γ on $\Phi := F_2/[F_2, F_2']$. For the rest of proving Claim 2 we denote the images of x, y in Φ by the same letters respectively. There exists $k \in \Phi'$ with $x^\gamma = x^{-1}k$. Note that α and γ act trivially on Φ'. Since α and γ commute one immediately finds $y^\gamma = y^{-1}k$ and so $y^{\gamma\alpha} = (y^{-1}k)^\alpha = yxk$. On the other hand $y^{\alpha\gamma} = x^{-\gamma}y^{-\gamma} = xyk^{-2}$. Therefore $[x, y] = k^3$ follows. Since $[x, y]$ is a generator of Φ', and $k^3 \in (\Phi')^*$, a contradiction arises.

Hence $\mathrm{Aut}(F_2)$ cannot contain an automorphism of order 6.

Claim 3: $\{2, 4, 8\} \subseteq S$.

This follows from (i).

Claim 4: $S = \{2, 3, 4, 8\}$.

The existence of an automorphism of order 3 follows from Theorem 2(2), so the claim follows from Claim 3 and (i).

Claim 5: $c(2) = 2$, $c(4) = 1$, $c(8) = 2$.

This immediately follows from (i).

Claim 6: $c(3) = 1$.

Let $\alpha \in \mathrm{Aut}(F_2)$ have order 3. By Theorem 2 (2) we have $G = F_2 \rtimes \langle\alpha\rangle = \langle c_1\rangle \coprod \langle c_2\rangle \cong C_3 \coprod C_3$. So F is the unique normal subgroup of index 3 in G which is a free pro-3 group. By Theorem A in [H-R1] one finds $f \in F_2$ with $\alpha^f \in \{c_1, c_2\}$. Therefore α is conjugate in $\mathrm{Aut}(F_2)$ to the automorphism induced by conjugation with either c_1 or c_2. W.l.o.g. we assume $\alpha = c_1$. Put $x := c_2\alpha^{-1}$, $y := \alpha^{-1}c_2$, then $x^\alpha = y$ and $y^\alpha = x^{-1}y^{-1}$ and there is only one such α up to conjugacy in $\mathrm{Aut}(F_2)$.

The proof of (iv) follows from Theorem 5.8 in [Lu] and Lemma 2.5(iii) in [H-R-Z]. ∎

References

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

[D-S] J. L. Dyer and G. P. Scott, *Periodic automorphisms of free groups*, Communications in Algebra **3(3)** (1975), 195–201.

[G] J. A. Green, *The characters of the finite general linear groups*, Transactions of the American Mathematical Society **80** (1955), 402–447.

[G-R] D. Gildenhuys and L. Ribes, *A Kurosh subgroup theorem for free pro-C-products of pro-C-groups*, Transactions of the American Mathematical Society **186** (1973), 309–329.

[H] M. Hall, *The Theory of Groups*, Macmillan, New York, 1959.

[H-R1] W. Herfort and L. Ribes, *Torsion elements and centralizers in free products of profinite groups*, Journal für die reine und angewandte Mathematik **358** (1985), 155–161.

[H-R2] W. Herfort and L. Ribes, *On automorphisms of free pro-p groups I*, Proceedings of the American Mathematical Society **108** (1990), 287–295.

[H-R-Z] W. Herfort, L. Ribes and P. Zalesskii, *Fixed points of automorphisms of free pro-p groups of rank 2*, Canadian Journal of Mathematics **47** (1995), 383–404.

[K-P-S] A. Karrass, A. Pietrowski and D. Solitar, *Finite and infinite cyclic extensions of free groups*, Journal of the Australian Mathematical Society **16** (1973), 458–466.

[L] M. Lazard, *Groupes analytiques p-adiques*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **26** (1965), 389–603.

[L-N] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1986.

[Lu] A. Lubotzky, *Combinatorial group theory for pro-p groups*, Journal of Pure and Applied Algebra **25** (1982), 311–325.

[R1] L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's Papers in Pure and Applied Mathematics, Kingston, 1970.

[R2] L. Ribes, *On amalgamated products of profinite groups*, Mathematische Zeitschrift **123** (1971), 357–364.

[Ro] V. A. Roman'kov, *Infinite generation of automorphism groups of free pro-p groups*, Siberian Mathematical Journal **34** (1993), 727–732.

[S1] J-P. Serre, *Sur la dimension cohomologique des groupes profinis*, Topology **3** (1965), 413–420.

[S2] J-P. Serre, *Trees*, Springer-Verlag, Berlin, 1980.

[Z-M] P. Zalesskii and O. Mel'nikov, *Subgroups of profinite groups acting on trees*, Mathematics of the USSR-Sbornik **63** (1989), 405–424.