Can. J. Math. Vol. **47** (2), 1995 pp. 383–404

FIXED POINTS OF AUTOMORPHISMS OF FREE PRO-p GROUPS OF RANK 2

WOLFGANG N. HERFORT, LUIS RIBES AND PAVEL A. ZALESSKII

ABSTRACT. Let p be a prime number, and let F be a free pro-p group of rank two. Consider an automorphism α of F of finite order m, and let $\mathrm{Fix}_F(\alpha) = \{x \in F \mid \alpha(x) = x\}$ be the subgroup of F consisting of the elements fixed by α. It is known that if m is prime to p and $\alpha = \mathrm{id}_F$, then the rank of $\mathrm{Fix}_F(\alpha)$ is infinite. In this paper we show that if m is a finite power p^r of p, the rank of $\mathrm{Fix}_F(\alpha)$ is at most 2. We conjecture that if the rank of F is n and the order of α is a power of p, then $\mathrm{rank}(\mathrm{Fix}_F(\alpha)) \leq n$.

Introduction. Let p be a prime number, F a free pro-p group of finite rank n, and α a (continuous) automorphism of F. Denote by $\mathrm{Fix}_F(\alpha)$ the subgroup of F consisting of those elements which are fixed by α. In [11] it is proved that if the order of α (as an element of the group $\mathrm{Aut}(F)$) is not divisible by p, then either α is the identity automorphism or otherwise $\mathrm{Fix}_F(\alpha)$ is a free pro-p group of infinite rank. That result is somewhat surprising, taking into account the well-known related fact in the context of abstract groups (*cf.* [5], [1], where it is shown that if Φ is an abstract free group of finite rank and $\alpha \in \mathrm{Aut}(\Phi)$, then $\mathrm{rank}\,\mathrm{Fix}_\Phi(\alpha) \leq \mathrm{rank}\,\Phi$). One feels that this "pathological" situation is due to the fact that α is not in the category of pro-p groups, *i.e.*, the group generated by α is not a pro-p group. Theorem 4.3 in [11] provides a method to construct free pro-p groups F of finite rank, and automorphisms α of F of order a power of p, such that the rank of $\mathrm{Fix}_F(\alpha)$ is at most the rank of F. Now, F can be thought of as a pro-p completion of an abstract free group Φ. In Theorem 1.1 in this paper we show that an automorphism of finite p-power order of the abstract group Φ, induces an automorphism of F of the same order; moreover the group of fixed points of such an automorphism has finite rank. This suggests that if both F and the group generated by α are in the category of pro-p groups, then one should expect a result that reflects the situation in abstract free groups. We are now ready to state a formal conjecture.

CONJECTURE. *Let F be a free pro-p group of finite rank n, and let α be an automorphism of order p^r $(0 \leq r \leq \infty)$. Then the rank of the free pro-p group $\mathrm{Fix}_F(\alpha)$ is at most n.*

Recall that one says that the order of α is p^∞ if the topological subgroup of $\mathrm{Aut}(F)$ generated by α is isomorphic to $\mathbb{Z}_p$, the group of p-adic integers.

In this paper we prove this conjecture in the case when F has rank $n = 2$ and α has finite order.

Received by the editors October 6, 1993.
AMS subject classification: 20E18; 20E36; 22C05.

We show that if $n = 2$ and α has finite order p^r, then α is trivial unless p is 2 or 3 (*cf.* Theorem 6.7). Most of the paper is concerned with the case $p = 2$. When $p = 3$ we show that, up to conjugation, there is only one automorphism of order 3, as in the abstract case. In this case the subgroup of fixed points is trivial (*cf.* Theorem 6.5).

It turns out that one can reduce the proof of the conjecture for $p = 2$, to the case when the order of α is 2. The strategy for the proof is then as follows. First we consider the induced automorphism $\bar{\alpha}$ on the abelianized quotient F/F' of F. It is easy to describe the different possibilities for $\bar{\alpha}$. The important fact is that, if one chooses a convenient basis for the free abelian pro-2 group F/F', then $\bar{\alpha}$ interchanges the elements of such a basis, or it fixes some of them and inverts the others (Lemma 2.5). Then we study the lifting of such a basis to F. One of the main results of this paper is that there exists a basis of F such that α inverts as many elements of that basis as $\bar{\alpha}$ does for the corresponding basis of F/F' (Theorem 3.1). Another key result of the paper is that if α is any involutory automorphism of a free pro-p group with basis $\{x, y\}$, and $\alpha(y) = y^{-1}$, $\alpha(x) = x \pmod{F'}$, then α cannot fix any nontrivial element of the normal closure of y in F (Theorem 5.3), and consequently the rank of $\mathrm{Fix}_F(\alpha)$ is bounded by 1.

In Theorem 6.7 we collect all the information about fixed points of automorphisms of finite p-power order of a free pro-p group of rank 2.

1. **Notation and automorphisms induced from abstract groups.** Throughout the paper p stands for a prime number. A pro-p group is a projective limit of finite p-groups, and we think of it as a topological group. For general facts about pro-p groups one may consult [17], [4], [14]. If G is a pro-p group, we use $d(G)$ to denote the smallest cardinality of a set of generators of an abstract dense subgroup of G. In this paper all homomorphisms among pro-p groups are assumed to be continuous, and all subgroups of pro-p groups are assumed to be closed. The commutator and Frattini subgroups of G are denoted by G' and G^*, respectively. If Y is a subset of a pro-p group G, the normal closure of Y in G is denoted by Y^G; and if Y consists of the element y only, we write instead $(y)^G$. If α is an automorphism of a pro-p group G, we use the notation

$$C_G(\alpha) = \mathrm{Fix}_G(\alpha) = \{x \in G \mid \alpha(x) = x\}.$$

If X is a finite set, let Φ be the free abstract group on X. Then the free pro-p group on X is $F = \varprojlim \Phi/N$, where N runs through the set of those normal subgroups whose index in Φ is a finite power of p. The rank of F is $|X|$. The free pro-p group of rank 1 is the additive group of the p-adic integers, for which we use the standard notation $\mathbb{Z}_p$. For properties of free pro-p groups, as well as the concept of freeness on a (pointed) topological space, one may consult [6]. If F is a free pro-p group on a space X, then F/F^* is a topological vector space over the field $\mathbb{F}_p$ with p elements, with X as a topological basis; we also refer to F/F^* as a free pro-p group on X in the variety of abelian pro-p groups of exponent p.

If $G_1, \ldots, G_n$ are pro-p groups, their free pro-p product $G = G_1 \amalg \cdots \amalg G_n$ is the coproduct of the groups $G_1, \ldots, G_n$ in the category of pro-p groups. For basic properties of free pro-p products, as well as the concept of free products indexed by a topological space, one may consult [7] and [8].

If R is a commutative pro-p ring (for example $\mathbb{Z}_p$ or $\mathbb{F}_p$) and G is a pro-p group, the completed group algebra $R[[G]]$ is the topological algebra $\varprojlim R[G/U]$, where U runs through the open normal subgroups of G, and $R[G/U]$ is the usual group algebra. For properties of $R[[G]]$, one may consult [12].

Let $\bar{\alpha}$ be an automorphism of the abstract free group Φ. Then $\bar{\alpha}$ induces in a natural way a (continuous) automorphism α of its pro-p completion F. In our first result we establish a straightforward consequence for free pro-p groups of a theorem of J. L. Dyer and G. P. Scott that they prove for abstract groups.

THEOREM 1.1. *Let Φ be a free abstract group of finite rank and F its pro-p completion. Let $\bar{\alpha}$ be an automorphism of Φ of finite order p^n, and let α be the automorphism of F induced by $\bar{\alpha}$. Then $F = \mathrm{Fix}_F(\alpha) \amalg L$, for some pro-p subgroup L of F. In particular,* $\mathrm{rank}\big(\mathrm{Fix}_F(\alpha)\big) \leq \mathrm{rank}(F)$.

PROOF. Note that $\mathrm{Fix}_F(\alpha) \leq \mathrm{Fix}_F(\alpha^p)$. Therefore by induction it suffices to prove the result when $n = 1$. Consider the holomorph $\Gamma = \Phi \rtimes \langle\bar{\alpha}\rangle$. By Theorem 1 in [3], Γ admits a decomposition as a free product of abstract groups $\Gamma = (\star\Gamma_\lambda) * \triangle$, where $\triangle$ is a free abstract group and for each λ, $\Gamma_\lambda \cong \mathbb{Z}/p\mathbb{Z} \times \triangle_\lambda$ for some free abstract group $\triangle_\lambda$. Let G be the pro-p completion of Γ. One easily verifies that

$$G = F \rtimes \langle\alpha\rangle = \coprod_\lambda (\mathbb{Z}/p\mathbb{Z} \times H_\lambda) \amalg H,$$

where H and H_λ are the pro-p completions of $\triangle$ and $\triangle_\lambda$ respectively. By Theorem A$'$ in [9], $\langle\alpha\rangle$ must be conjugate to one of the $\mathbb{Z}/p\mathbb{Z}$ appearing in the above free pro-p product decomposition of G, and therefore we may assume that $\langle\alpha\rangle$ is in one of those free factors, say $\mathbb{Z}/p\mathbb{Z} \times H_\lambda$. Now by Theorem B' in [9], the centralizer of α in G is $\mathbb{Z}/p\mathbb{Z} \times H_\lambda = \langle\alpha\rangle \times H_\lambda$. So $\mathrm{Fix}_F(\alpha) = (\langle x\rangle \times H_\lambda) \cap F$, which is a free pro-$p$ factor of F by the main theorem in [2]. ∎

REMARK 1.2. Theorem 1.1 is valid in a more general setting. Specifically, let $\mathcal{C}$ be non-empty class of finite groups closed under taking subgroups, quotients and extensions with abelian kernel. Let $\bar{\alpha}$ be an automorphism of the free abstract group Φ such that $\langle\bar{\alpha}\rangle \in \mathcal{C}$. Denote by F the pro-$\mathcal{C}$ completion of Φ. Then $\mathrm{Fix}_F(\alpha)$ is a free pro-$\mathcal{C}$ factor of F.

2. **Preliminary results.**

LEMMA 2.1. *Let $G = G_1 \amalg G_2$ be the free pro-p product of pro-p groups G_1, G_2. Let α be an automorphism of G of finite order p^n with $\alpha(G_i) = G_i$ for $i = 1, 2$. Then*

$$C_G(\alpha) = \langle C_{G_1}(\alpha), C_{G_2}(\alpha)\rangle \cong C_{G_1}(\alpha) \amalg C_{G_2}(\alpha).$$

PROOF. First assume that G_1 and G_2 are both finite. Let K denote the Cartesian kernel of G, *i.e.*, K is the kernel of the homomorphism

$$\phi\colon G_1 \coprod G_2 \longrightarrow G_1 \times G_2, \quad \text{defined by } \phi(x) = \begin{cases} (x,1) & \text{if } x \in G_1 \\ (1,x) & \text{if } x \in G_2. \end{cases}$$

CLAIM 1. $C_K(\alpha) = \langle [g_1, g_2] \mid g_i \in C_{G_i}(\alpha) \setminus \{1\}, i = 1, 2 \rangle$. Put $X := \big\{[g_1, g_2] \mid g_i \in G_i \setminus \{1\}, i = 1, 2\big\}$. Note that X is a free set of generators for K (*cf.* Theorem 3.4 in [15]). Clearly α acts on X as a permutation. Hence X admits a partition into α-orbits, *i.e.*, one can find a subset $X_1 \subseteq X$, so that

$$X = \bigcup_{j=0}^{p^n-1} \alpha^j(X_1) \cup X_0, \quad X_1 \cap X_0 = \emptyset,$$

where $X_0 := C_X(\alpha) = \{[g_1, g_2] \mid g_i \in C_{G_i}(\alpha), i = 1, 2\}$.

Next observe that the holomorph $H := K \rtimes \langle \alpha \rangle$ admits the free pro-p product decomposition

$$H = \big(\langle \alpha \rangle \times F(X_0)\big) \coprod F(X_1),$$

where $F(X_0)$ and $F(X_1)$ denote the free pro-p group on X_0 and X_1 respectively.

For, define a homomorphism

$$\eta : L = \big(\langle \alpha \rangle \times F(X_0)\big) \coprod F(X_1) \longrightarrow K \rtimes \langle \alpha \rangle$$

by

$$\eta(\alpha) = \alpha, \text{ and}$$
$$\eta(x) = x \quad \text{if } x \in X_0 \cup X_1.$$

The normal subgroup of L generated by $F(X_0)$ and $F(X_1)$ is

$$\Big\langle \Big(F(X) \coprod F(X_1)\Big)^{\alpha^i} \mid i = 0, \ldots, p^n - 1 \Big\rangle = F(X_0) \coprod \coprod_{i=0}^{p^n-1} F(X_1^{\alpha^i}) = F(X) \cong K.$$

Therefore, η is an isomorphism.

From Theorem 3 in [9] we infer that

$$C_K(\alpha) = F(X_0).$$

This proves Claim 1.

It is clear from the definition of K that

$$C_G(\alpha) \leq C_{G_1}(\alpha) C_{G_2}(\alpha) K.$$

Therefore $g \in C_G(\alpha)$ has the form $g = g_1 g_2 k$ with $g_i \in C_{G_i}(\alpha)$ and $k \in K$. Then

$$g_1 g_2 k = g = \alpha(g) = \alpha(g_1)\alpha(g_2)\alpha(k) = g_1 g_2 \alpha(k)$$

implies $k = \alpha(k)$, *i.e.*,

$$C_G(\alpha) \leq C_{G_1}(\alpha)C_{G_2}(\alpha)C_K(\alpha) \leq \langle C_{G_1}(\alpha), C_{G_2}(\alpha)\rangle,$$

by Claim 1. The latter group can be seen to be isomorphic with $C_{G_1}(\alpha) \amalg C_{G_2}(\alpha)$ by applying Lemma 5.3 in [10], and so the lemma is proved for finite groups G_1, G_2.

We turn to the general case. Since α is of finite order, the groups G_i contain α-invariant open normal subgroups forming a basis of neighbourhoods of the identity. Pick open normal α-invariant subgroups $N_i \leq G_i$, $i = 1, 2$. Let N denote the normal closure of $N_1 \cup N_2$ in $G = G_1 \amalg G_2$ and let $\pi_N \colon G \longrightarrow G/N$ stand for the canonical projection. For an element $g \in C_G(\alpha)$ the canonical isomorphism

$$G/N \cong G_1/N_1 \coprod G_2/N_2$$

and the first part of the proof yield the fact that

$$\pi_N(g) \in \Big(\langle C_{G_1/N_1}(\alpha), C_{G_2/N_2}(\alpha)\rangle\Big).$$

It now follows that

$$g \in \langle C_{G_1}(\alpha), C_{G_2}(\alpha)\rangle.$$

This shows that $C_G(\alpha) \leq \langle C_{G_1}(\alpha), C_{G_2}(\alpha)\rangle$. The reverse inclusion is trivial and the isomorphism with $C_{G_1}(\alpha) \amalg C_{G_2}(\alpha)$ again follows from Lemma 5.3 in [10]. ∎

REMARK. One easily extends the result to an infinite number of free factors, or even to a free product of factors indexed by some boolean space.

LEMMA 2.2. *Let $G := \mathbb{Z}_p \amalg F$ be the free pro-p product of the p-adic integers with a pro-p group F. Let α be an automorphism of G and assume that the normal closure of F in G does not contain nontrivial fixed points of α. Then $C_G(\alpha)$ is procyclic.*

PROOF. Let F^G denote the normal closure of F in G and define π to be the canonical projection from G onto G/F^G. Then

$$C_G(\alpha) \cong C_G(\alpha)/C_G(\alpha) \cap F^G \cong C_G(\alpha)F^G/F^G \hookrightarrow G/F^G \cong \mathbb{Z}_p. \qquad ∎$$

LEMMA 2.3. *Let $G := A_1 \amalg \cdots \amalg A_p$ be a free pro-p product of isomorphic pro-p groups A_i. Let $\alpha \in \mathrm{Aut}(G)$ be the automorphism that sends A_i to A_{i+1} (where $1 \leq i \leq p$ and $p + 1$ is identified with 1) in the canonical way. Then $C_G(\alpha) = \{1\}$.*

PROOF. It is enough to remark that the holomorph $\Gamma := G \rtimes \langle\alpha\rangle$ is isomorphic to

$$A_1 \coprod \langle\alpha\rangle,$$

so that Theorem B in [9] implies

$$C_\Gamma(\alpha) = \langle\alpha\rangle.$$

Therefore α has no non-trivial fixed points in G. ∎

Next we turn to some result on linear algebra that will be needed later.

LEMMA 2.4. *Let F be a field, and $V = F \times \cdots \times F$ the n-dimensional F-vector space of n-tuples of elements of F. If $v = (a_1, \ldots, a_n)$, $w = (b_1, \ldots, b_n)$ are in V, let $v \cdot w = \sum_{i=1}^{n} a_i b_i$ be their standard bilinear product. Suppose that $f\colon V \longrightarrow V$ is a function such that $f(v) \cdot v \neq 0$ for every $0 \neq v \in V$. Then the linear span of the set*

$$f(V) = \{f(v) \mid v \in V\}$$

is V.

PROOF. Let W be the linear span of $f(V)$. If $W \neq V$, then choose $u \neq 0$ in V such that $W \cdot u = 0$. If follows that $f(u) \cdot u = 0$, a contradiction. ∎

LEMMA 2.5. *Let $\mathbb{Z}_p$ be the ring of p-adic integers. Let $A \in \mathrm{GL}(2, \mathbb{Z}_p)$ be a matrix with $A^p = 1$. Then*

(i) If $p = 2$ and $A \neq 1$, then A must be conjugate to precisely one of the following matrices

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

(ii) If $p = 3$ and $A \neq 1$, then A must be conjugate to

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

(iii) If $p > 3$, then $A = 1$.

PROOF. (i) First observe that $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ are not conjugate in $\mathrm{GL}(2, \mathbb{Z}_2)$ since they are not conjugate in $\mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$. Let $M = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ be the free abelian pro-2 group of rank 2, and let α be an automorphism with $\alpha^2 = 1$. It suffices to prove that there is a basis $\{m_1, m_2\}$ of M such that either (a) $\alpha(m_1) = m_2$ (and then $\alpha(m_2) = m_1$), or (b) $\alpha(m_1) = \pm m_1$ and $\alpha(m_2) = \pm m_2$. To prove this consider a basis $\{n_1, n_2\}$ of M.

CASE 1. $\alpha(n_1) \neq n_1 \pmod{2M}$ or $\alpha(n_2) \neq n_2 \pmod{2M}$. Hence $\{n_1, \alpha(n_1)\}$ or $\{n_2, \alpha(n_2)\}$ respectively, is a basis of M. Then we get the alternative (a) above.

CASE 2. $\alpha(n_i) = n_i + 2h_i$ for some $h_i \in M$ $(i = 1, 2)$. Since $\alpha^2 = 1$, it follows that $\alpha(h_i) = -h_i$. Hence $\alpha(n_i + h_i) = n_i + h_i$. Next observe that $\{n_1 + h_1, n_2 + h_2, h_1, h_2\}$ generate M, and, since M is pro-2, there are two elements in that set which form a basis for M. It is easily checked that any such basis leads to one of the cases in (b).

(ii) Let $M = \mathbb{Z}_3 \oplus \mathbb{Z}_3$ be the free abelian pro-3 group of rank 2, and let α be an automorphism of order 3. It suffices to prove that there is a basis $\{m_1, m_2\}$ of M such that $\alpha(m_1) = m_2$ and $\alpha(m_2) = -m_1 - m_2$. First observe that in $\mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z})$ there is only one element of order 3 up to conjugation, namely $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Therefore one may choose $m_1 \in M$, such that m_1 and $m_2 = \alpha(m_1)$ form a basis of M. Say $\alpha(m_2) = am_1 + bm_2 (a, b \in \mathbb{Z}_3)$. The matrix of α with respect to this basis is

$$\begin{bmatrix} 0 & a \\ 1 & b \end{bmatrix}.$$

Since $\alpha^3 = 1$, $det(\alpha) = 1$, and so $a = -1$.

Now, $m_1 = \alpha^3(m_1) = am_2 + b(am_1 + bm_2)$. So $ab = 1$, and $a + b^2 = 0$. Therefore $b = -1$.

(iii) Let $M = \mathbb{Z}_p \oplus \mathbb{Z}_p$ be the free abelian pro-p group of rank 2. Let $\alpha \in \mathrm{GL}(2, \mathbb{Z}_p)$ be of order p. Consider the induced automorphism $\bar{\alpha}$ on M/pM. Then the matrix of $\bar{\alpha}$ with respect to a certain basis has the form

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

Choose a vector $\bar{z} \neq 0$ of M/pM such that $\bar{\alpha}(\bar{z}) = \bar{z}$. Then for any $\bar{x}$ in M/pM, $\bar{\alpha}(\bar{x}) = \bar{x} + q\bar{z}$, with $q \in \mathbb{Z}/p\mathbb{Z}$. Next choose $x_0 \in M$ such that $\bar{\alpha}(\bar{x}_0) \neq \bar{x}_0$. Then $\alpha(x_0) = x_0 + z_0$, where $z_0 \notin pM$ but z_0 is fixed by α modulo pM. Then

$$\alpha^2(x_0) = x_0 + z_0 + \alpha(z_0) = x_0 + 2z_0 + x_1, \quad \text{where } x_1 \in pM;$$
$$\alpha^3(x_0) = x_0 + 3z_0 + 3x_1 + z_1, \quad \text{where } z_1 \in pM;$$

and in general,

$$x_0 = \alpha^p(x_0) = x_0 + \binom{p}{1} z_0 + \binom{p}{2} x_1 + \binom{p}{3} z_1 + \cdots. \tag{1}$$

Note that for $p > 3$

$$\binom{p}{2} x_1 + \binom{p}{3} z_1 + \cdots \in p^2 M.$$

Since $\binom{p}{1} z_0 \in pM \setminus p^2M$, the expression (1) leads to a contradiction. Hence there is no automorphism α of order p. ∎

3. Lifting inverted elements.

THEOREM 3.1 (LIFTING THEOREM). *Let G be a free pro-2 group of finite rank $n = d_1 + d_2$, where d_1 and d_2 are non-negative integers. Let $\alpha \in \mathrm{Aut}(G)$ be an automorphism of order 2 of G, and assume that the automorphism induced by α on the free abelian pro-2 group G/G' has with respect to a certain basis $\bar{\mathcal{B}}$ of G/G', the matrix form*

$$A = \begin{pmatrix} I_1 & 0 \\ 0 & -I_2 \end{pmatrix},$$

where I_1 and I_2 denote the identity matrices of degree d_1 and d_2 respectively (if $d_1 = 0$, $A = -I_2$). Then G admits a decomposition as a free pro-2 product $G = G_1 \amalg G_2$, with

(i) rank $G_i = d_i$ $(i = 1, 2)$, *and*

(ii) G_2 admits a free basis X such that $\alpha(x) = x^{-1}$ for $x \in X$.

PROOF. Lift the ordered basis $\bar{\mathcal{B}}$ of G/G' to an ordered basis $\mathcal{B}$ of G, and let F_1 and F_2 denote the subgroups of G generated by the first d_1 and the last d_2 elements of $\mathcal{B}$, respectively. Furthermore denote by

$$\Gamma := G \rtimes \langle \alpha \rangle$$

the holomorph.

We first describe the idea of the proof. In Γ we shall exhibit d_2 involutions β_j ($j = 1, \ldots, d_2$), which are neither pairwise conjugates in Γ nor conjugates of α. The elements $\beta_j\alpha \in \Gamma$, ($j = 1, \ldots, d_2$) will turn out to be contained in G already and will serve as the set X of the theorem.

Put $N := \langle G^*, F_1 \rangle$. Let Ξ_Γ (Ξ_G) denote the collection of maximal open subgroups $H \neq G$ in Γ (H_0 in G) which contain N and with $\alpha \notin H$.

We give the proof after establishing the following claims:

1. $\Gamma/G' \cong [(F_1/F_1') \times (F_2/F_2')] \rtimes \langle\alpha\rangle$, where $\alpha(f_2F_2') = -f_2F_2'$ for $f_2 \in F_2$.
2. The Frattini groups Γ^* and G^* satisfy $\Gamma^* = G^*$.
3. For each $H_0 \in \Xi_G$ there is exactly one $H \in \Xi_\Gamma$ with $H_0 = H \cap G$.
4. Let $H \in \Xi_\Gamma$. Then
$$H/G' \cong (F_1/F_1' \times F_2/F_2') \rtimes C_2,$$
where the generating element $c \in C_2$ acts on (F_2/F_2') by inverting the elements. Moreover $d(H) \geq d(G) + 1$.
5. Let $H \in \Xi_\Gamma$. Then H contains an involution β_H.
6. Put $y_H := \beta_H\alpha$. Then $y_H \in G \setminus H$ and $\alpha(y_H) = y_H^{-1}$.
7. The set $\{\beta_H \mid H \in \Xi_\Gamma\}$ contains d_2 linearly independent elements modulo Γ^*.

For 1. This fact follows immediately from the block form of the matrix A.

For 2. Note that $\Gamma' = [G\langle\alpha\rangle, G\langle\alpha\rangle] \leq G^*[G,\alpha]$. Also, if $g \in G$, then $(g\alpha)^2 = g^2[g,\alpha] \in G^*[G,\alpha]$. Therefore, it follows that $\Gamma^* \leq G^*[G,\alpha]$. Finally, by hypothesis, $[G,\alpha] \leq G^*$. Thus $\Gamma^* = G^*$.

For 3. By Claim 2, $\Gamma^* \leq N$. Let $H_0 \in \Xi_G$. Then $H_0 \geq N \geq \Gamma^*$. Observe that H_0/N has codimension 2 in the vector space Γ/N, and in fact
$$\Gamma/H_0 = (G \rtimes \langle\alpha\rangle)/H_0 \cong (G/H_0) \times \langle\alpha\rangle \cong C_2 \times C_2.$$
Pick $g \in G \setminus H_0$. Let $H \geq H_0$ be a maximal (open) subgroup of Γ. Clearly the only possibilities for H are $H = \langle H_0, g\rangle$, $H = \langle H_0, \alpha\rangle$ and $H = \langle H_0, g\alpha\rangle$. If in addition one requires that $H \cap G = H_0$ and $\alpha \notin H$, one must have $H = \langle H_0, g\alpha\rangle$.

For 4. Put $H_0 := G \cap H$. Note that $G' \leq H_0$. Pick $g_H \in G \setminus H$ then $g_H\alpha \in H \setminus G$. Since $H \neq G$ one can choose $g_H \in F_2$ and so
$$(g_H\alpha)^2 = g_H\alpha(g_H) \equiv 1 \bmod G'$$
holds. This finally implies that
$$H/G' \cong (F_1/F_1' \times F_2/F_2') \rtimes C_2,$$
where the generator $g_H\alpha$ of C_2 acts on F_2/F_2' by inverting the elements.

Altogether we found
$$H/G' \cong \Gamma/G'.$$

This together with the simple observation $d(H) \geq d(H/G')$ implies

$$d(H) \geq d(\Gamma/G') \geq d(\Gamma/G^*).$$

Finally note that $d(\Gamma/G^*) = d(F_1) + d(F_2) + 1 = d(G) + 1$ yields the desired estimate for the generation rank of H.

For 5. If not then H must be torsion-free. Since H_0 is a free pro-2 subgroup of index 2 in H it turns out that H is a free pro-2 group (*cf.* p. 413 in [16]). Then H_0 is a subgroup of index 2 in both H and G, and therefore an application of the Schreier formula (*cf.* [2]) yields

$$d(G) = d(H).$$

Therefore Claim 4 yields a contradiction.

For 6. Since $\Gamma/G \cong \langle\alpha\rangle$ and G is torsion-free, it is clear that y_H is in G. Assume $y_H = \beta_H\alpha \in G \cap H$ then $\alpha = y_H^{-1}\beta_H \in H$ contradicts the choice of H. Clearly the elements y_H get inverted by α.

For 7. Consider the vector space $V = G/N$ over $\mathbb{F}_2$ (the field with two elements). Define a bilinear product $v \cdot w$ on V as follows: fix a basis for V, and if $(a_1, \ldots, a_{d_2})$ and $(b_1, \ldots, b_{d_2})$ are the coordinates of v and w with respect to that basis, set

$$v \cdot w = \sum_{i=1}^{d_2} a_i b_i.$$

For $g \in G \setminus N$, denote by V_g the subspace of V consisting of the vectors orthogonal to gN. Let H_g be the unique subgroup of G containing N with $V_g = H_g/N$, and observe that $H_g \in \Xi_G$. By Claim 3 there exists $\bar{H}_g \in \Xi_\Gamma$ such that $\bar{H}_g \cap G = H_g$. Choose $\beta_g = \beta_{\bar{H}_g} \in \Gamma$ as in Claim 5. By Claim 6, $\beta_g\alpha \in G \setminus H_g$. Thus $(gN) \cdot (\beta_g\alpha N) \neq 0$. Define a function

$$f\colon V \setminus \{0\} \longrightarrow V \setminus \{0\}$$

by $f(gN) = \beta_g\alpha N$. By Lemma 2.4 the set $\{\beta_g\alpha N \mid g \in G \setminus N\}$ contains d_2 linearly independent elements. It follows that the set

$$\{\beta_g\alpha\Gamma^* \mid g \in G \setminus N\}$$

contains d_2 linearly independent elements, and thus so does the set

$$\{\beta_g\Gamma^* \mid g \in G \setminus N\}.$$

In order to finish the proof, pick a linearly independent set mod Γ^* of involutions β_i $(i = 1, \ldots, d_2)$. Note that $y_i := \beta_i\alpha$ are linearly independent mod $\Gamma^* = G^*$ (see Claim 1). Put $X := \{y_i \mid i = 1, \ldots, d_2\}$. By Claim 6 α inverts the elements of X and by Claim 7 X is a linearly independent set mod G^*. ■

Before we state a consequence of Theorem 3.1, we need the following auxiliary result.

LEMMA 3.2. *Let C and C_i be groups of order 2 generated by α and β_i ($i = 1, \ldots, n$) respectively. Consider the free pro-2 product*

$$G = C_1 \coprod \cdots \coprod C_n \coprod C,$$

and let $H = \langle \beta_1\alpha, \ldots, \beta_n\alpha \rangle$. Then

(i) H is a free pro-2 group of rank n.

(ii) $G = H \rtimes C$.

PROOF. First observe that $H \lhd G$, for $(\beta_i\alpha)^\alpha = \alpha\beta_i = (\beta_i\alpha)^{-1}$, and $(\beta_i\alpha)^{\beta_j} = (\beta_j\alpha)(\beta_i\alpha)^{-1}(\beta_j\alpha)^{-1}$. Hence (ii) follows (for $\alpha \notin H$; otherwise G would be generated by n elements). Next note that $\beta_i \notin H$ and $\alpha \notin H$ (otherwise $H = G$, but $d(H) \leq n$ and $d(G) = n + 1$). Therefore, if $a \in G$, one has $\langle \beta_i \rangle^a \cap H = \langle \alpha \rangle^a \cap H = 1$. It follows from the Kurosh subgroup theorem for pro-2 products of pro-2 groups (*cf.* [2]) that H is a free pro-2 group. Finally, rank $H = n$, for otherwise, $d(G) < n + 1$. ■

THEOREM 3.3. *Let F be the free pro-2 group on n generators, $\alpha \in \mathrm{Aut}(F)$ of order 2 and assume that α inverts the elements of F modulo the commutator-subgroup. Then there exists a finite subset $Y \subset F$ so that Y is a free set of generators of F and for $y \in Y$, $\alpha(y) = y^{-1}$. Moreover, α has no nontrivial fixed points in F.*

PROOF. From Theorem 3.1 one deduces the existence of the subset Y with the desired properties. Next, in the semidirect product $\Gamma = F \rtimes \langle \alpha \rangle$ for $y \in Y$ pick elements $\beta(y) = y\alpha$. By Lemma 3.2,

$$\Gamma \cong \langle \alpha \rangle \coprod \Big(\coprod_{y \in Y} \langle \beta(y) \rangle \Big).$$

The set of fixed points for α inside Γ coincides with $\langle \alpha \rangle$ as was shown in [9] Theorem B. Therefore α cannot have nontrivial fixed points inside F. ■

COROLLARY 3.4. *Let F be a free pro-2 on a boolean space U, and let $\alpha \in \mathrm{Aut}(F)$ be of order 2. Assume that for each $u \in U$ one has $\alpha(u) = u^{-1}$. Then α has no nontrivial fixed points in F.*

PROOF. Let $\mathcal{N}$ be a basis of open neighbourhoods N of 1 consisting of α-invariant open normal subgroups of F. Then (*cf.* [6], Proposition 1.7)

$$F = \varprojlim_{N \in \mathcal{N}} F_N,$$

where F_N is the free pro-2 group on the finite set UN/N. Let α_N be the automorphism of F_N that inverts the elements of UN/N. Then

$$\alpha = \varprojlim_{N \in \mathcal{N}} \alpha_N.$$

Let $f \in F$, and let f_N denote the image of f in F_N under the canonical projection $F \longrightarrow F_N$. Clearly $\alpha(f) = f$, implies that $\alpha_N(f_N) = f_N$ for each $N \in \mathcal{N}$. By Theorem 3.3, $\alpha_N(f_N) = f_N$ if and only if $f_N = 1$. Thus $\alpha(f) = f$ only if $f = 1$. ■

4. **The structure of a certain frattini quotient.** Let $F = F(x, y_1, \ldots, y_n)$ be a free pro-p group of rank $n+1$ with basis $\{x, y_1, \ldots, y_n\}$. Denote by Γ (respectively, $\Gamma_i, i = 1, \ldots, n$) the normal subgroup of F generated by $y_1, \ldots, y_n$ (respectively y_i). Then (*cf.* [6], Theorem 2.1) Γ is a free pro-p group on the space $\{y_i^{x^\lambda} \mid i = 1, \ldots, n; \lambda \in \mathbb{Z}_p\}$ (respectively, Γ_i is a free pro-p group on the space $\{y_i^{x^\lambda} \mid \lambda \in \mathbb{Z}_p\}$). Therefore $\Gamma = \coprod_{i=1}^n \Gamma_i$ (free pro-p product). Let Γ^* and Γ_i^* ($i = 1, \ldots, n$) be the Frattini subgroup of Γ and Γ_i respectively. There is a natural action of the subgroup $\langle x \rangle$ of F on Γ/Γ^* and Γ_i/Γ_i^* ($i = 1, \ldots, n$) by conjugation. These actions turn Γ/Γ^* and Γ_i/Γ_i^* into $\mathbb{F}_p[[\langle x \rangle]]$-modules, and we have an isomorphism of $\mathbb{F}_p[[\langle x \rangle]]$-modules

$$\Gamma/\Gamma^* \cong \Gamma_1/\Gamma_1^* \oplus \cdots \oplus \Gamma_n/\Gamma_n^*.$$

We shall now describe the structure of Γ_i/Γ_i^* as an $\mathbb{F}_p[[\langle x \rangle]]$-module.

LEMMA 4.1. *Γ_i/Γ_i^* is isomorphic to $\mathbb{F}_p[[\langle x \rangle]]$ as an $\mathbb{F}_p[[\langle x \rangle]]$-modules.*

PROOF. Consider the subgroup F_i ($i = 0, 1, 2, \ldots$), defined recursively as follows: $F_0 = F, F_{r+1} = F_r^p l[F_r, F]$. It is easily checked that these subgroups constitute a basis for the open neighbourhoods of 1 in F. Put $\Gamma_i^{(r)} = \Gamma_i \cap F_r$, ($r = 0, 1, \ldots$). Then $\{\Gamma_i^{(r)}\Gamma_i^*/\Gamma_i^* \mid r = 0, 1, \ldots\}$ is a basis of open neighborhoods of the identity in the group Γ_i/Γ_i^*. For $r = 0, 1, 2, \ldots$, define

$$y_i^{(x-1)^r} = y_i^{\binom{r}{0}x^r} y_i^{(-1)\binom{r}{1}x^{r-1}} \cdots y_i^{(-1)^r\binom{r}{r}}.$$

CLAIM 1. The subset $\{y_i^{(x-1)^r}\Gamma_i^* \mid r = 0, 1, \ldots\}$ of Γ_i/Γ_i^* converges to 1. For, observe that $y_i^{(x-1)^r} \equiv [y_i^{(x-1)^{r-1}}, x] \bmod \Gamma^*$, and by an easy induction argument $[y_i^{(x-1)^t}, x] \in \Gamma_i^{(r)}$ ($t, r = 0, 1, \ldots$) if $t \geq r$.

CLAIM 2. The subset $\{y_i^{(x-1)^r}\Gamma_i^* \mid r = 0, 1, \ldots\}$ of Γ_i/Γ_i^* is linearly independent over $\mathbb{F}_p$. Observe first that $\langle y_i^{(x-1)^r}\Gamma_i^* \mid r = 0, 1, \ldots, t\rangle = \langle y_i^{x^r}\Gamma_i^* \mid r = 0, 1, 2, \ldots, t\rangle$, for any natural number t. Therefore it suffices to show that the subset $\{y_i^{x^r}\Gamma_i^* \mid r = 0, 1, \ldots, t\}$ is linearly independent. To see this choose a natural number j such that $t < p^j$. Partition the basis $\{y_i^{x^\lambda} \mid \lambda \in \mathbb{Z}_p\}$ of Γ_i using the cosets of $p^j\mathbb{Z}_p$ in $\mathbb{Z}_p$. Then there exists an epimorphism of pro-p groups

$$\phi: \Gamma_i \longrightarrow \bar{F} = F(\mathbb{Z}_p/p^j\mathbb{Z}_p)$$

(where $\bar{F} = F(\mathbb{Z}_p/p^j\mathbb{Z}_p)$ is the free pro-p group on the finite set $\mathbb{Z}_p/p^j\mathbb{Z}_p$) that sends $y_i^{x^\lambda}$ to $\lambda + p^j\mathbb{Z}_p$. Observe that according to the choice of j, $\phi(y_i^{x^r}) \neq \phi(y_i^{x^s})$ if $r \neq s$ ($r, s, \in \{0, 1, 2, \ldots, t\}$). Since $\bar{F}$ is free pro-p of finite rank, the elements of a basis of $\bar{F}$ are linearly independent modulo $\bar{F}^*$. It follows that $\phi(y_i), \phi(y_i^x), \ldots, \phi(y_i^{x^t})$ are linearly independent modulo $\bar{F}^*$. Since $\phi(\Gamma_i^*) = \bar{F}^*$, one deduces that $y_i, y_i^x, \ldots, y_i^{x^t}$ are linearly independent modulo Γ_i^*, as desired. This ends the proof of Claim 2.

Now note that

$$\Gamma_i/\Gamma_i^* = \varprojlim_r \Gamma_i/\Gamma_i^{(r)}\Gamma_i^*.$$

https://doi.org/10.4153/CJM-1995-021-6 Published online by Cambridge University Press

Therefore, according to the above observation, every element of Γ_i/Γ_i^* can be represented formally as

$$y^{\sum_{r=0}^{\infty} a_i(x-1)^r},$$

where $a_i \in \mathbb{F}_p$. Thus Γ_i/Γ^* can be identified, as a pro-p group, with the additive group of the ring of formal power series

$$\mathbb{F}_p\big\{\{(x-1)\}\big\}$$

on $x-1$ with coefficients in $\mathbb{F}_p$. One knows that this ring is topologically isomorphic with $\mathbb{F}_p[[\langle x\rangle]]$ (*cf.* [12] Proposition 3.1.4, p. 63). Thus Γ_i/Γ_i^* can be identified with the additive group of $\mathbb{F}_p[[\langle x\rangle]]$. Finally, it is clear that the action of $\mathbb{F}_p[[\langle x\rangle]]$ on Γ_i/Γ_i^* induced by conjugation by x, corresponds under this identification, with multiplication in $\mathbb{F}_p[[\langle x\rangle]]$. ■

The following consequence is now clear.

COROLLARY 4.2. *The* $\mathbb{F}_p[[\langle x\rangle]]$*-module* Γ/Γ^* *is isomorphic to*

$$M = \mathbb{F}_p[[\langle x\rangle]] \times \cdots \times \mathbb{F}_p[[\langle x\rangle]].$$

Under this isomorphism, $(a_1,\ldots,a_n) \in M$*, where* $a_i \in \mathbb{F}_p[[\langle x\rangle]]$*, corresponds to*

$$y_1^{a_1}\cdots y_n^{a_n}.$$

Moreover, conjugation of $y_1^{a_1}\cdots y_n^{a_n}$ *by an element* $a \in \mathbb{F}_p[[\langle x\rangle]]$*, corresponds to the product* $(a_1,\ldots,a_n)a$ *in* M*.*

REMARK 4.3. As pointed out above $\mathbb{F}_p[[\langle x\rangle]]$ is isomorphic as a topological ring, to the ring of formal power series $\mathbb{F}_p\big\{\{T\}\big\}$, under the correspondence $x \longmapsto T+1$. It follows then that $\mathbb{F}_p[[\langle x\rangle]]$ is a local ring with unique maximal ideal $(x-1)\mathbb{F}_p[[\langle x\rangle]] = I$. Moreover, every ideal of $\mathbb{F}_p[[\langle x\rangle]]$ is a power of I, and hence every non-zero ideal of $\mathbb{F}_p[[\langle x\rangle]]$ has finite index in $\mathbb{F}_p[[\langle x\rangle]]$.

Next we describe the additive structure of the ideals of $\mathbb{F}_p[[\langle x\rangle]]$.

The next lemma is a well-known result, although we do not have a specific reference for it.

LEMMA 4.4. *Let* G *be a pro-p group, and let* I_G *be the augmentation ideal of* $\mathbb{F}_p[[G]]$ *generated (as an ideal) by* $\{g-1 \mid g \in G\}$*. Then,* I_G *is in fact freely generated by the pointed topological space* $B_G = \{g-1 \mid g \in G\}$ *with distinguished point* 0*, as an abelian pro-p group of exponent p.*

PROOF. Express G as a projective limit of finite p-groups $G = \varprojlim G_i$. Then $I_G = \varprojlim I_{G_i}$ and $B_G = \varprojlim B_{G_i}$. So we may assume that G is finite. Then $\mathbb{F}_p[[G]] = \mathbb{F}_p[G]$, and the result is obvious. ■

LEMMA 4.5. *Let $k \in \mathbb{F}_p[[\langle x\rangle]] \setminus \{0\}$. Then the closed ideal generated by k, $\langle k\rangle = k\mathbb{F}_p[[\langle x\rangle]]$, is a free pro-p abelian group of exponent p on the pointed topological subspace L with distinguished point* 0, *where*

$$L = \left\{\frac{x^\lambda - 1}{x-1}k \mid \lambda \in \mathbb{Z}_p\right\}.$$

PROOF. First observe that L is actually a well-defined subspace of $\mathbb{F}_p[[\langle x\rangle]]$. Indeed, let $\{n_i\}_{i=1}^\infty$ be a sequence of natural numbers converging to λ in $\mathbb{Z}_p$; then

$$\frac{x^{n_i}-1}{x-1} = 1 + x + \cdots + x^{n_i-1} \in \mathbb{F}_p[[\langle x\rangle]].$$

One easily checks that $\{1+x+\cdots+x^{n_i-1}\}_{i=1}^\infty$ is a Cauchy sequence, and then we can define

$$\frac{x^\lambda - 1}{x-1} = \lim_{i\to\infty}(1+x+\cdots+x^{n_i-1}),$$

which is an element of $\mathbb{F}_p[[\langle x\rangle]]$. Since $\mathbb{F}_p[[\langle x\rangle]] \cong \mathbb{F}_p\{\{T\}\}$ as topological rings (*cf.* [12], Proposition 3.1.4, p. 63), we deduce that $\mathbb{F}_p[[\langle x\rangle]]$ has no zero divisors. Therefore $\langle k\rangle$ is isomorphic to $(x-1)\mathbb{F}_p[[\langle x\rangle]] = I$ as abelian pro-p groups. Thus it suffices to prove that I is freely generated by $\{x^\lambda - 1 \mid \lambda \in \mathbb{Z}_p\}$. This is the content of Lemma 4.4. ∎

5. **Fixed points of involutions.** In this section we shall prove that the subgroup of fixed points of an automorphism α of finite 2-power order of a free pro-2 group of rank 2, has rank at most 2. Before we reach this theorem, we need still some auxiliary results.

LEMMA 5.1. *Let $\phi: F_1 \longrightarrow F_2$ denote a homomorphism of free pro-p groups. Assume that the induced homomorphism between the Frattini quotients $\phi^*: F_1/F_1^* \longrightarrow F_2/F_2^*$ is an isomorphism. Then ϕ is an isomorphism.*

PROOF. Let

$$\pi_i: F_i \longrightarrow F_i/F_i^*$$

denote the canonical projections of F_i onto the Frattini quotient for $i = 1, 2$. Using the facts that $\mathrm{Ker}(\pi_2) = F_2^*$ and that ϕ^* is an isomorphism one deduces from $\pi_2\phi = \phi^*\pi_1$:

$$\phi(F_1)F_2^* = \pi_2^{-1}\pi_2\phi(F_1) = \pi_2^{-1}\phi^*\pi_1(F_1) = \pi_2^{-1}(F_2/F_2^*) = F_2.$$

Therefore

$$F_2 = \phi(F_1)F_2^* = \phi(F_1)$$

implies that ϕ is an epimorphism.

Since F_1 and F_2 are free the short exact sequence

$$\mathrm{Ker}(\phi) \hookrightarrow F_1 \longrightarrow F_2$$

is a split extension and therefore one can find an injective homomorphism $\psi: F_2 \longrightarrow F_1$ with

$$\phi\big(\psi(f_2)\big) = f_2$$

for $f_2 \in F_2$. Put

$$F := \psi(F_2) \subseteq F_1,$$

then $\operatorname{Ker}\phi \cap F = \{1\}$ and $F \operatorname{Ker}\phi = F_1$. Since ϕ^* is an isomorphism we conclude $\operatorname{Ker}\phi \leq F_1^*$. Therefore $FF_1^* = F_1$, and hence $F = F_1$, *i.e.*, ϕ is an isomorphism. ∎

COROLLARY 5.2. *Let F be a free pro-p group, U a closed subset of F (respectively, such that $1 \in U$). Assume that U is naturally homeomorphic to the subspace UF^*/F^* of F/F^*, and that F/F^* is free, in the variety of abelian pro-p groups of exponent p, on the space (respectively, on the pointed space) UF^*/F^*. Then F is a free pro-p group on the space (respectively, the pointed space) U.*

PROOF. Let $\bar{F}$ denote the free pro-p group on the space U. Then, clearly the canonical homomorphism $\bar{F} \longrightarrow \bar{F}/\bar{F}^*$, induces a homeomorphism $U \longrightarrow U\bar{F}^*/\bar{F}^*$, and $U\bar{F}^*/\bar{F}^*$ is a basis for the free pro-p group $\bar{F}/\bar{F}^*$ of exponent p. Then the natural homomorphism $\bar{F} \stackrel{\phi}{\longrightarrow} F$ that sends $u \in U \subset \bar{F}$ to $u \in U \subset F$ induces an isomorphism $\bar{F}/\bar{F}^* \longrightarrow F/F^*$. Then by Lemma 5.1, ϕ is an isomorphism. ∎

THEOREM 5.3. *Let $F = F(x,y)$ be a free pro-2 group of rank 2 on the basis $\{x,y\}$. Let α be an automorphism of F of order 2 such that $\alpha(y) = y^{-1}$ and $\alpha(x) = kx$, where $k \in F'$ (F' is the commutator subgroup of F). Then the normal closure $\Gamma = (y)^F$ of y in F does not contain any non-trivial fixed points under α, i.e.,* $\mathrm{Fix}_F(\alpha) \cap (y)^F = 1$.

PROOF. The idea of the proof is to construct a topological basis U of the free pro-p group Γ such that $\alpha(u) = u^{-1}$, if $u \in U$. Then the result would follow from Corollary 3.4.

By Theorem 2.1 in [6]

$$\Gamma = \coprod_{\lambda \in \mathbb{Z}_2} y^{x^\lambda}.$$

For $f \in F$ and $\lambda \in \mathbb{Z}_2$, define

$$c(\lambda, f) = \alpha(x)^{-\lambda} f x^\lambda.$$

Observe that if $\alpha(f) = f^{-1}$, then $\alpha\big(c(\lambda,f)\big) = c(\lambda,f)^{-1}$. Therefore $\alpha\big(c(\lambda,y)\big) = c\big(\lambda,y\big)^{-1}$, and $\alpha\big(c(\lambda,k)\big) = c(\lambda,k)^{-1}$, since by assumption $\alpha(y) = y^{-1}$, and it is easily checked that $\alpha(k) = k^{-1}[\alpha(x) = kx$ and $\alpha^2 = 1$ implies $x = \alpha(k)kx$, *i.e.*, $\alpha(k)k = 1]$. Consider the subspaces of Γ:

$$K = \{c(\lambda,k) \mid \lambda \in \mathbb{Z}_2\}$$

and

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

Note that K and Y are compact, and that Γ is generated by $K \cup Y$, for $c(\lambda+1,k)^{-1}c(\lambda,y) = y^{x^\lambda}$.

CASE 1. $k \in \Gamma^*$. Then $c(\lambda,y) \equiv y^{x^\lambda} \pmod{\Gamma^*}$, and clearly if $\lambda, \lambda' \in \mathbb{Z}_2$ with $\lambda \neq \lambda'$, then $c(\lambda,y) \not\equiv c(\lambda',y) \pmod{\Gamma^*}$. Therefore according to Lemma 5.2 Y is a basis for Γ. So in this case we may put $U = Y$.

CASE 2. $k \notin \Gamma^*$. Then for a natural number n we have

$$c(n+1,k) = (kx)^{-n-1}kx^{n+1} = k^{-x-x^2-\cdots-x^n} = k^{-x\frac{x^n-1}{x-1}}.$$

Write $\lambda = \lim_{i\to\infty}(n_i+1)$ in $\mathbb{Z}_2$, where each n_i is a natural number. Then

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

Using the notation of Corollary 4.2, say that

$$k^{-x} = y^\kappa$$

for some $\kappa \in \mathbb{F}_p[[\langle x\rangle]]$. Thus $c(\lambda,k)$ corresponds to $\frac{x^\lambda-1}{x-1}\kappa$ in Γ/Γ^*.

Observe that since $k \notin \Gamma^*$, we have $\kappa \neq 0$. Therefore by Lemma 4.5, the pointed space $\{\frac{x^\lambda-1}{x-1}\kappa \mid \lambda \in \mathbb{Z}_2\}$ with distinguished point 0, is a basis for the ideal $\langle\kappa\rangle$ of $\mathbb{F}_2[[\langle x\rangle]]$ considered as a pro-2 group of exponent 2. It follows that the pointed space

$$K = \{c(\lambda,k) \mid \lambda \in \mathbb{Z}_2\}$$

is a free basis for the subgroup of Γ that K generates (*cf.* Lemma 5.2). On the other hand $\langle\kappa\rangle$ has finite index in $\mathbb{F}_2[[\langle x\rangle]]$, since $\kappa \neq 0$ (*cf.* Remark 4.3). As pointed out above, $K \cup Y$ generates Γ. Thus there exists a finite subset $\{c_1,\ldots,c_r\}$ of Y such that $\{c_1,\ldots,c_r\} \cup K$ is a basis for Γ. So $U = \{c_1,\ldots,c_r\} \cup K$ satisfies the desired properties. ∎

THEOREM 5.4. *Let $F = F(x,y)$ be a free pro-2 group of rank 2, and let α be an automorphism of F of finite order 2. Then the subgroup $\mathrm{Fix}_F(\alpha)$ of the elements of F fixed by α is of rank at most 1.*

PROOF. The proof consists of a case by case study of the possible automorphisms $\bar\alpha$ induced by α on the abelianized group F/F'. According to Lemma 2.5 one may choose a suitable basis $\bar{\mathcal{B}} = \{b_1,b_2\}$ of F/F' such that $\bar\alpha$ is of one of the following types (we identify $\bar\alpha$ with its matrix form with respect to the basis $\bar{\mathcal{B}}$).

CASE 1.

$$\bar\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then $\bar\alpha$ is the identity automorphism of F/F'. Now, by Theorem 5.8 in [13],

$$\mathrm{Ker}\Big(\mathrm{Aut}(F) \longrightarrow \mathrm{Aut}(F/F')\Big)$$

is a torsion-free group. Since α is in this kernel and its order is 2, this case is not possible.

CASE 2.

$$\bar{\alpha} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

By Theorem 3.1, there exists a basis $\{x, y\}$ of F such that $\alpha(y) = y^{-1}$ and $\alpha(x) = kx$, where $k \in F'$. From Theorem 5.3 we deduce that the normal closure $(y)^F$ of y in F does not contain non-trivial fixed elements of α. Finally, this implies according to Lemma 2.2, that the subgroup of fixed points of α in F is cyclic.

CASE 3.

$$\bar{\alpha} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then by Theorem 3.1, there exists a basis $\{x, y\}$ of F such that $\alpha(x) = x^{-1}$ and $\alpha(y) = y^{-1}$. Consider the free pro-2 product of three groups of order two:

$$G = \langle \beta_1 \rangle \coprod \langle \beta_2 \rangle \coprod \langle \alpha \rangle.$$

By Lemma 3.2,

$$G = \langle \beta_1 \alpha, \beta_2 \alpha \rangle \rtimes \langle \alpha \rangle \cong F \rtimes \alpha.$$

Then

$$\mathrm{Fix}_F(\alpha) \cong C_G(\alpha) \cap \langle \beta_1 \alpha, \beta_2 \alpha \rangle.$$

Now, by Theorem B$'$ in [9], $C_G(\alpha) = \langle \alpha \rangle$. Thus $\mathrm{Fix}_F(\alpha) = 1$.

CASE 4.

$$\bar{\alpha} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let $\{x, y\}$ be any basis of F. Then $\alpha(x) = yk$ where $k \in F'$. Put $\bar{y} = yk$. Then $\langle x, \bar{y} \rangle = F$, and therefore $\{x, \bar{y}\}$ is a basis of F. Moreover, since $\alpha^2 = 1$, $\alpha(\bar{y}) = \alpha^2(x) = x$. Thus by Lemma 2.3, $\mathrm{Fix}_F(\alpha) = 1$. ∎

6. **The conjecture for the case** rank$(F) = 2$. In this section we classify the subgroups of fixed points of automorphisms of finite order of a free pro-p group of rank 2. We begin with a series of results that will lead to a description of the structure of an extension of a free pro-3 group of rank 2 by a group of order 3.

Let F be a free pro-3 group of rank 2, α an automorphism of F of order 3, and let $\Gamma = F \rtimes \langle \alpha \rangle$ be the holomorph.

LEMMA 6.1. *(i) The action of α on F/F^* is nontrivial.*
(ii) The minimal number of generators $d(\Gamma)$ of Γ is 2.

PROOF. Observe that the automorphism induced on F/F' by α is not trivial (*cf.* [13], Theorem 5.8). Hence it follows from Lemma 2.5 that there is a basis $\{c_1, c_2\}$ of F/F^* such that $\alpha(c_1) = c_2, \alpha(c_2) = -c_1 - c_2$. It follows that $\Gamma/\Gamma^* \cong C_3 \times C_3$.

LEMMA 6.2. *Let L be a subgroup of Γ of index 3. Then if $d(L) \geq 3$, L has torsion.*

PROOF. Suppose L is torsion-free; then L is a free pro-3 group since it contains the free pro-3 subgroup $F \cap L$ of finite index $(F : F \cap L) = 3$ (*cf.* p. 413 in [16]). Therefore by Schreier's formula (*cf.* [2]), $d(L) = d(F) = 2$. Hence if $d(L) \geq 3$, L has torsion. ∎

LEMMA 6.3. *Let φ be an automorphism of the $\mathbb{F}_3$-vector space V of dimension 3, with Jordan form*

$$\textit{either} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \textit{or} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Consider the group $G = V \rtimes \langle \varphi \rangle$. Then $d(G) \geq 3$.

PROOF. Obvious. ∎

PROPOSITION 6.4. *Let $\Gamma = F \rtimes \langle \alpha \rangle$ be as above. Then Γ has a subgroup L of index 3 such that $d(L) \geq 3$ and $\alpha \notin L$.*

PROOF. Consider the quotient Γ/Γ^{**} of Γ modulo its second Frattini subgroup. If T is a subgroup of Γ, we shall denote by $\bar{T}$ its image in Γ/Γ^{**}. It sufficies to prove that Γ has a subgroup L of index 3 such that $d(\bar{L}) \geq 3$ and $\alpha \notin \bar{L}$. Since $d(\Gamma) = 2$, $(\Gamma : \Gamma^*) = 3^2$; hence $(F : \Gamma^*) = 3$, and so $\operatorname{rank}(\Gamma^*) = 4$ by Schreier's formula (*cf.* [2]). It follows that $\bar{\Gamma}^*$ is a four-dimensional $\mathbb{F}_3$-vector space $|\bar{F}| = 3^5$ and $|\bar{\Gamma}| = 3^6$. Next we describe the action of $\bar{F}$ on $\bar{\Gamma}^*$. Throughout the proof we shall use the additive notation for the operation in $\bar{\Gamma}^*$ whenever convenient. Let $f \in \bar{F} \setminus \bar{\Gamma}^*$. Then f acts on $\bar{\Gamma}^*$ as a nontrivial automorphism φ of order 3. There are three possible Jordan normal forms for the matrix of φ, say with respect to the basis v_1, v_2, v_3, v_4:

$$\Phi_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \Phi_3 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \Phi_3 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

In fact the second and third possibilities are not valid. For if the matrix is Φ_3, then $\bar{F}' = \langle v_1 \rangle, \bar{F}^* = \langle v_1, f^3 \rangle$; and therefore $(\bar{F} : \bar{F}^*) \geq 3^3$ since $|\bar{F}| = 3^5$, contradicting the fact that $d(F) = 2$. On the other hand if the matrix of φ is Φ_2, then $f^3 \in \operatorname{Cent}(\bar{F}) = \langle v_1, v_3 \rangle = \bar{F}'$. Now, $\bar{F}^* = \langle f^3 \rangle \bar{F}' = \bar{F}'$, and consequently $|\bar{F}^*| = 3^2$. So $|\bar{F}/\bar{F}^*| = 3^3$, again contradicting the fact that $d(F) = 2$.

Therefore the matrix of φ is Φ_1. It follows that $\bar{F}' = \langle v_1, v_2 \rangle$ and $\bar{F}^* = \langle v_1, v_2, f^3 \rangle$. Since $|\bar{F}'| = 3^2$ and $(\bar{F} : \bar{F}^*) = 3^2$, we have that $F^* \neq \bar{F}'$. Therefore we can assume $v_4 = f^3$. Clearly $\bar{F}' \cap \operatorname{Cent}(\bar{F}) = \langle v_1 \rangle$. Since $\bar{\Gamma}$ is a nonabelian 3-group and $\bar{F}'$ is a normal subgroup of $\bar{\Gamma}$, it follows that $\bar{F}' \cap \operatorname{Cent}(\bar{\Gamma}) \neq 1$, and thus $\bar{F}' \cap \operatorname{Cent}(\bar{\Gamma}) = \langle v_1 \rangle$. Next we claim that f and $\alpha f \alpha^{-1}$ form a basis of $\bar{F}$. It suffices to check that their images in $\bar{F}/\bar{F}^*$ form a basis, or equivalently, that $f \not\equiv \alpha f \alpha^{-1} \pmod{\bar{F}^*}$ (note that $\alpha f \alpha^{-1} \not\equiv f^2 \pmod{\bar{F}^*}$ since α has order 3). Now $\bar{\Gamma}/\bar{F}^* \cong \bar{F}/\bar{F}^* \rtimes \langle \alpha \rangle$, where the action of α on $\bar{F}/\bar{F}^*$ is nontrivial by Lemma 6.1. Since the order of $\bar{\Gamma}/\bar{F}^*$ is 3^3, one gets that $\operatorname{Cent}(\bar{\Gamma}/\bar{F}^*)$

is cyclic of order 3, and therefore $\mathrm{Cent}(\bar{\Gamma}/\bar{F}^*) = \bar{\Gamma}^*/\bar{F}^*$. Since $f \in \bar{F}/\bar{\Gamma}^*, f$ is not fixed by α in $\bar{\Gamma}/\bar{F}^*$, as desired.

Put $f_1 = f, f_2 = \alpha f_1 \alpha^{-1}$, and define x such that $\alpha f_2 \alpha^{-1} = x f_1^{-1} f_2^{-1}$. Then $(\alpha^{-1} f_1)^3 = \alpha^{-1} f_1 \alpha^{-1} f_1 \alpha^{-1} f_1 = a^{-1} f_1 \alpha \alpha f_1 \alpha^{-1} f_1 = x f_1^{-1} f_2^{-1} f_2 f_1 = x$. Remark that by Lemma 2.5(ii), $x \in \bar{F}'$. We now distinguish two cases.

CASE 1. $x \in \mathrm{Cent}(\bar{\Gamma})$.

Observe that $x = tw_1$, for some $t \in \mathbb{F}_3$. Put $w_1 = v_1, w_2 = v_2, w_3 = f_2 f_1^{-1}, w_4 = v_4 = f_1^3$. Note that $f_2 f_1^{-1} \notin \bar{F}^* = \langle w_1, w_2, w_4 \rangle$. Thus $\{w_1, w_2, w_3, w_4\}$ is a basis of $\bar{\Gamma}^*$. Observe that $\bar{F}' = \langle w_1, w_2 \rangle$.

Next we compute the matrices of φ and α with respect to this new basis. Clearly, $\varphi(w_1) = w_1, \varphi(w_2) = w_1 + w_2$ and $\varphi(w_4) = w_4$. Suppose $\varphi(w_3) = aw_1 + bw_2 + cw_3 + dw_4$, where $a, b, c, d \in \mathbb{F}_3$. Since $\bar{F}/\bar{F}'$ is abelian, $w_3 \equiv f_1 w_3 f_1^{-1} = \varphi(w_3) \equiv cw_3 + dw_4 \pmod{\bar{F}'}$, and so $c = 1, d = 0$. Thus the matrix of φ is

$$\Phi = \begin{bmatrix} 1 & 1 & a & 0 \\ 0 & 1 & b & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

To compute the matrix of α note first that $\alpha(w_1) = w_1$, for as pointed out before $w_1 = v_1$ is in the centre of $\bar{\Gamma}$. Since $\langle w_1, w_2 \rangle / \langle w_1 \rangle$ is a minimal normal subgroup of $\bar{\Gamma}/\langle w_1 \rangle$, it is central, and therefore one has $\alpha(w_2) = w_2 + rw_1$, where $r \in \mathbb{F}_3$. Now,

$$\begin{aligned} \alpha(w_3) &= \alpha(f_2 f_1^{-1})\alpha^{-1} = x f_1^{-1} f_2^{-1} f_2^{-1} = x f_1^{-1} (w_3 f_1)^{-1} (w_3 f_1)^{-1} \\ &= x f_1^{-1} f_1^{-1} w_3^{-1} f_1^{-1} w_3^{-1} = x f_1^{-3} f_1 w_3^{-1} f_1^{-1} w_3^{-1} \\ &= x - w_4 + (-w_3 - bw_2 - aw_1) - w_3 = (t-a)w_1 - bw_2 + w_3 - w_4. \end{aligned}$$

And finally,

$$\begin{aligned} \alpha(w_4) &= \alpha f_1^3 \alpha^{-1} = f_2^3 = (w_3 f_1)^3 = w_3 f_1 w_3 f_1 w_3 f_1 w_3 f_1 w_3 f_1^{-1} f_1^3 f_1^{-1} w_3 f_1 \\ &= w_3 + aw_1 + bw_2 + w_3 + w_4 + \varphi(aw_1 + bw_2 + w_3) = bw_1 + w_4. \end{aligned}$$

Hence the matrix of α with respect to the basis w_1, w_2, w_3, w_4 is

$$A = \begin{bmatrix} 1 & r & t-a & b \\ 0 & 1 & -b & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}.$$

Consider $\bar{\Gamma}/\langle w_1 \rangle$. Then $(\alpha^{-1} f_1)^3 = x \equiv 1 \pmod{\langle w_1 \rangle}$. The matrices Φ and A indicate that the centralizers of φ and α in $\bar{\Gamma}/\langle w_1 \rangle$ contain the images of w_2 and w_4. One deduces that $\alpha^{-1} f_1$ also centralizes the images of w_2 and w_4. Then the Jordan normal form of the action induced by $\alpha^{-1} f_1$ on $\bar{\Gamma}^*/\langle x \rangle$ is

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

It follows from Lemma 6.3 that for $\bar{L} = \langle \alpha^{-1} f_1 \rangle \bar{\Gamma}^*$, $d(\bar{L}) \geq 3$. Finally note that $\alpha \notin \bar{L}$, for otherwise $\bar{L} = \bar{\Gamma}$.

CASE 2. $x \notin \mathrm{Cent}(\bar{\Gamma})$.

Define a new basis w_1, w_2, w_3, w_4 of $\bar{\Gamma}^*$ as follows. Put $w_1 = v_1$ or $-v_1$ depending on whether $\varphi(x) = x + v_1$ or $\varphi(x) = x - v_1$ respectively; put $w_2 = x$; $w_4 = v_4 = (f_1)^3$; $w_3 = f_2 f_1^{-1}$. Note that $\bar{F}' = \langle w_1, w_2 \rangle$ and $\bar{F}^* = \langle w_1, w_2, w_4 \rangle$. By Lemma 6.1, $w_3 = f_2 f_1^{-1} \notin \bar{F}^*$. Thus w_1, w_2, w_3, w_4 is a basis of $\bar{\Gamma}^*$. Next we compute the matrices of φ and α with respect to this new basis. Clearly, $\varphi(w_1) = w_1, \varphi(w_2) = w_1 + w_2$ and $\varphi(w_4) = w_4$. Suppose $\varphi(w_3) = aw_1 + bw_2 + cw_3 + dw_4$, where $a, b, c, d \in \mathbb{F}_3$. Since $\bar{F}/\bar{F}'$ is abelian, $w_3 \equiv f_1 w_3 f_1^{-1} = \varphi(w_3) \equiv cw_3 + dw_4 \pmod{\bar{F}'}$, and so $c = 1, d = 0$. Thus the matrix of φ is

$$\Phi = \begin{bmatrix} 1 & 1 & a & 0 \\ 0 & 1 & b & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Since $\bar{\Gamma}$ is a finite 3-group and $\bar{F}'$ is normal in $\bar{\Gamma}$, $\bar{F}' \cap \mathrm{Cent}(\bar{\Gamma}) \neq 1$; since $\bar{F}' = \langle w_1, w_2 \rangle$, $\bar{F}' \cap \mathrm{Cent}(\bar{F}) = \langle w_1 \rangle$. Hence $\bar{F}' \cap \mathrm{Cent}(\bar{\Gamma}) = \langle w_1 \rangle$. Therefore $\alpha(w_1) = w_1$. Since $(\alpha^{-1} f_1)^3 = x = w_2$, $\alpha^{-1} f_1$ centralizes w_2. So $\alpha(w_2) = \varphi(w_2) = w_1 + w_2$. Next

$$\begin{aligned} \alpha(w_3) &= \alpha(f_2 f_1^{-1})\alpha^{-1} = x f_1^{-1} f_2^{-1} f_2^{-1} = x f_1^{-1} (w_3 f_1)^{-1} (w_3 f_1)^{-1} \\ &= x f_1^{-1} f_1^{-1} w_3^{-1} f_1^{-1} w_3^{-1} = x f_1^3 f_1 w_3^{-1} f_1^{-1} w_3^{-1} \\ &= w_2 - w_4 + (-w_3 - bw_2 - aw_1) - w_3 = -aw_1 + (1-b)w_2 + w_3 - w_4. \end{aligned}$$

Finally,

$$\begin{aligned} \alpha(w_4) &= \alpha f_1^3 \alpha^{-1} = f_2^3 = (w_3 f_1)^3 = w_3 f_1 w_3 f_1 = w_3 f_1 w_3 f_1^{-1} f_1^3 f_1^{-1} w_3 f_1 \\ &= w_3 + aw_1 + bw_2 + w_3 + w_4 + \varphi(aw_1 + bw_2 + w_3) = bw_1 + w_4. \end{aligned}$$

So the matrix of α is

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

Then

$$\Phi A = \begin{bmatrix} 1 & -1 & 1-b & b \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}, \quad A\Phi = \begin{bmatrix} 1 & -1 & b & b \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}.$$

Note $\bar{\Gamma}/\bar{\Gamma}^*$ is abelian and so $A\Phi = \Phi A$. Therefore $1 - b = b$, and so $b = -1$. It follows that

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

Next compute

$$\begin{aligned}[f_1^{-1}, f_2^{-1}] &= f_1 f_2 f_1^{-1} f_2^{-1} = f_1 w_3 f_1 f_1^{-1} (w_3 f_1)^{-1} \\ &= f_1 w_3 f_1^{-1} w_3^{-1} = a w_1 - w_2 + w_3 - w_3 = a w_1 - w_2.\end{aligned}$$

So in $\bar{\Gamma}/\langle w_1\rangle$, $[f_1^{-1}, f_2^{-1}] \equiv -w_2 = -x$. Hence $(f_1\alpha)^3 = f_1\alpha f_1\alpha f_1\alpha = f_1\alpha f_1\alpha^{-1}\alpha^{-1} f_1\alpha = f_1 f_2 x f_1^{-1} f_2^{-1} \equiv 1$, since x centralizes $\bar{\Gamma}/\langle w_1\rangle$.

Remark that the centralizers of φ and α in $\bar{\Gamma}/\langle w_1\rangle$ contain the images of w_2 and w_4. One deduces that $f_1\alpha$ also centralizes the images of w_2 and w_4. Then the Jordan normal form of the action induced by $f_1\alpha$ on $\bar{\Gamma}^*/\langle w_4\rangle$ is

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

It follows from Lemma 6.3 that for $\bar{L} = \langle f_1\alpha\rangle\Gamma^*, d(\bar{L}) \geq 3$. Finally note that $\alpha \notin \bar{L}$, for otherwise $\bar{L} = \bar{\Gamma}$. ■

THEOREM 6.5. *Let F be a free pro-3 group of rank 2. Let α be an automorphism of F of order 3. Then the holomorph $\Gamma = F \rtimes \langle\alpha\rangle$ is a free pro-3 product $\langle\alpha\rangle \amalg \langle\gamma\rangle$, where γ is an element of order 3.*

PROOF. By Proposition 6.4 and Lemma 6.2 there exists a subgroup L of index 3 in Γ such that $\alpha \notin L$ and there is an element $\gamma \in L$ of order 3. Then α and γ generate Γ, since $\Gamma = \Gamma^*\langle\alpha,\gamma\rangle$. Consider the free pro-3 product $\langle\alpha\rangle \amalg \langle\gamma\rangle$ and the natural epimorphism.

$$\rho\colon \langle\alpha\rangle \coprod \langle\gamma\rangle \longrightarrow \Gamma = \langle\alpha,\gamma\rangle.$$

Let $K = \ker(\rho)$. Recall that the torsion element of $\langle\alpha\rangle \amalg \langle\gamma\rangle$ must be conjugate to either an element from $\langle\alpha\rangle$ or $\langle\gamma\rangle$ (*cf.* [9], Theorem 1). It follows that K is torsion-free (in fact it is free). Since F has index 3 in Γ, $\rho^{-1}(F)$ has index 3 in $\langle\alpha\rangle \amalg \langle\gamma\rangle$, and by the main theorem in [2], $\rho^{-1}(F)$ is free pro-3 of rank 2. Observe that the restriction σ of ρ to $\rho^{-1}(F)$ is an epimorphism $\sigma\colon \rho^{-1}(F) \longrightarrow F \cong \rho^{-1}(F)/K \cap \rho^{-1}(F)$. Since $\rho^{-1}(F)$ and F are free pro-3 groups of rank 2, it follows that σ is an isomorphism (*cf.* Proposition 7.6 in [14]). Thus $K \cap \rho^{-1}(F) = 1$. We deduce that K is finite, and since it is torsion-free, it must be trivial. ■

COROLLARY 6.6. *Let F be a free pro-3 group of rank 2. Let α be an automorphism of F of order 3. Then* $\mathrm{Fix}_F(\alpha) = 1$

PROOF. Let $\alpha(x) = x$, for some $x \in F$. Then x centralizes α in $\langle\alpha\rangle \amalg \langle\gamma\rangle$. Thus $x \in \langle\alpha\rangle$ by Theorem B′ in [9]. Hence $x = 1$. ■

In the following result we put together all the information about the subgroup of fixed points of automorphisms of finite order for free pro-p groups of rank 2.

THEOREM 6.7. *Let p be a prime number, F a free pro-p group of rank 2, and α a non trivial automorphism of F of finite order m. Then*

(i) *If $p \nmid m$, then $\mathrm{Fix}_F(\alpha)$ is a free pro-p group of infinite rank;*

(ii) *If $p = 2$, and m is even, then the rank of $\mathrm{Fix}_F(\alpha)$ is at most 1;*

(iii) *If $p = 3$, and m is a multiple of 3, then $\mathrm{Fix}_F(\alpha) = 1$;*

(iv) *If $p > 3$, there is no automorphism of F whose order is a multiple of p.*

PROOF. (i) This is the content of Theorem 3.2 in [11].

(ii) and (iii) Let p be 2 or 3, and assume p divides m. Then $\alpha^{m/p}$ has order p. Observe that $\mathrm{Fix}_F(\alpha) \leq \mathrm{Fix}_F(\alpha^{m/p})$, and therefore the results follow from Theorem 5.4 or Theorem 6.5.

(iv) One knows that the kernel of $\mathrm{Aut}(F) \longrightarrow \mathrm{Aut}(F/F') = \mathrm{GL}(2, \mathbb{Z}_p)$ is torsion-free (*cf.* Theorem 5.8 in [12]). Thus the result is a consequence of Lemma 2.5(iii). ∎

This theorem settles the conjecture that we stated in the introduction for the case $\mathrm{rank}(F) = 2$, and automorphisms of order a finite power of p. Theorem 6.7 could mislead the reader into thinking that the conjecture can be extended to all automorphisms whose order is a multiple of p. Next we present an example to show that such an extension is not possible.

EXAMPLE 6.8. Let $F = F(x, y, z)$ be the free pro-2 group of rank 3. Consider the automorphisms α and β of F defined a follows:

$$\alpha(x) = x,\ \alpha(y) = y,\ \alpha(z) = z^{-1};\quad \beta(x) = y,\ \beta(y) = x^{-1}y^{-1},\ \beta(z) = z.$$

Then α has order 2, β has order 3, and $\alpha\beta = \beta\alpha$. Hence the order of the automorphism $\alpha\beta$ is 6. Then $\mathrm{Fix}_F(\alpha\beta) = \mathrm{Fix}_F(\alpha) \cap \mathrm{Fix}_F(\beta)$, by Lemma 2.4 in [11]. By Lemma 2.1, $\mathrm{Fix}_F(\alpha) = \langle x, y\rangle$. Again by Lemma 2.1, $\mathrm{Fix}_F(\beta) = \mathrm{Fix}_{\langle x,y\rangle}(\beta) \amalg \langle z\rangle$. Therefore, $\mathrm{Fix}_F(\alpha\beta) = \mathrm{Fix}_{\langle x,y\rangle}(\beta)$, which has infinite rank by Theorem 6.7(i).

We end this paper with a result about free pronilpotent groups of rank 2 that follows immediately from Theorem 6.7.

THEOREM 6.9. *Let F be a free pronilpotent group of rank 2, and let α be an automorphism of F of finite order. For a prime number p, denote by F_p the p-Sylow subgroup of F. Then the following conditions are equivalent.*

(i) *The rank of $\mathrm{Fix}_F(\alpha)$ is finite.*

(ii) *$\mathrm{Fix}_F(\alpha)$ is cyclic;*

(iii) *The restriction α_p of α to F_p is the identity mapping if $p \geq 5$, and if $p = 2$ or 3, then α_p is either the identity mapping or the order of α_p is divisible by p.*

ACKNOWLEDGEMENTS. The first author acknowledges the support of NSERC, Canada under the Austria-Canada exchange programs.

The second author was partially supported by NSERC grant 8221.

All three authors thank the Technische Universität Wien and Carleton University for their hospitality during the preparation of this paper.

REFERENCES

1. M. Bestvina and M. Handel M, *Train tracks and automorphisms of free groups*, Ann. of Math. **135**(1992), 1–51.
2. D. Binz, J. Neukirch and G. H. Wenzel, *A subgroup theorem for free products of profinite groups*, J. Algebra **19**(1971), 104–109.
3. J. L. Dyer and G. P. Scott, *Periodic automorphisms of free groups*, Comm. Algebra (3) **3**(1975), 195–201.
4. M. D. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, 1986.
5. S. M. Gersten, *Fixed points of automorphisms of free groups*, Invent. Math. **84**(1986), 91–119.
6. D. Gildenhuys and C. K. Lim, *Free pro-C groups*, Math. Z. **125**(1972), 233–254.
7. D. Gildenhuys and L. Ribes, *A Kurosh subgroup theorem for free pro-C groups*, Trans Amer. Math. Soc. **186**(1973), 309–329.
8. ———, *Profinite groups and Boolean graphs*, J. Pure Appl. Algebra **12**(1987), 21–47.
9. W. Herfort and L. Ribes, *Torsion elements and centralizers in free products of profinite groups*, J. Reine Angew. Math. **358**(1985), 155–182.
10. ———, *Frobenius subgroups of free products of prosolvable groups*, Monatsh. Math. **108**(1989), 165–182.
11. ———, *On automorphisms of free pro-p groups I*, Proc. Amer. Math. Soc. **108**(1989) 287–295.
12. M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. IHES **26**(1965).
13. A. Lubotzky, *Combinatorial Group Theory for Pro-p Groups*, J. Pure Appl. Algebra **25**(1982), 311–325.
14. L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's Papers in Pure and Appl. Math., Queen's Univ., Kingston, Ontario, 1970.
15. ———, *The Cartesian subgroup of a free product of profinite groups*, Contemp. Math. **109**(1990), 147–158.
16. J-P. Serre, *Sur la dimension cohomologique des groupes profinis*, Topology **3**(1965), 413–420.
17. ———, *Cohomologie Galoisienne*, Springer-Verlag, Berlin, 1965.

Institute f. Angew. und Numer. Mathematik
Technische Universität Wien
A-1040 Wien
Austria
e-mail: herfort@uranus.tuwien.ac.at

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

Institute of Techn. Cybernetics
Academy of Sciences
220605 Minsk
Byelorussia
e-mail: mahaniok%bas10.basnet.minsk.by@demos.su