PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 108, Number 2, February 1990

ON AUTOMORPHISMS OF FREE PRO-p-GROUPS I

WOLFGANG N. HERFORT AND LUIS RIBES

(Communicated by Warren J. Wong)

ABSTRACT. Let F be a (topologically) finitely generated free pro-p-group, and β an automorphism of F. If $p \neq 2$ and the order of β is 2, then there is some basis of F such that β either fixes or inverts its elements. If p does not divide the order of β, then the subgroup of F of all elements fixed by β is (topologically) infinitely generated; however this is not always the case if p divides the order of β.

Let p be a fixed prime number, and let F be a free pro-p-group of finite rank. In this paper we study (continuous) automorphisms of F. The group of automorphisms $\mathrm{Aut}(F)$ of F is, in a natural way, a profinite group. In [9], Lubotzky gives global properties of the group $\mathrm{Aut}(F)$. Our interest here is rather more local; we describe properties of certain types of automorphisms. The group $\mathrm{Aut}(F)$ contains a pro-p-subgroup of finite index; hence the automorphisms of order prime to p must have finite order. In $p \neq 2$, we show that given an automorphism φ of order 2 of a finitely generated pro-p-group G (in particular, a free one), there is a minimal set of generators of G such that φ sends each of the generators in that set to itself or its inverse. As a consequence we can describe all the conjugacy classes of involutions of $\mathrm{Aut}(F)$: they correspond bijectively to those of $\mathrm{GL}(n, p)$, where $\mathrm{rank}\, F = n$.

In [4], Gersten proves that if α is an automorphism of an abstract free group of finite rank, then the elements of the group fixed by α form a subgroup of finite rank also. In contrast, in §3 we show that for a free pro-p-group F of finite rank, the equivalent result need not hold; in fact we prove that if the order of $\beta \in \mathrm{Aut}(F)$ is not divisible by p, and β is not the identity, then the subgroup of the elements of F fixed by β is necessarily infinitely generated (i.e. such a subgroup contains no dense subgroup which is finitely generated as an abstract group). This result depends strongly on the fact that the order of the automorphism does not involve the prime p. In fact, in §4 we

Received by the editors November 17, 1988 and, in revised form, February 13, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20E18; 20F28.

0002-9939/90 $1.00 + $.25 per page

describe nontrivial automorphisms of free pro-p-groups whose fixed subgroups have prescribed finite rank.

1. Notation

We follow the notation of [12] and [10], where basic results about pro-p-groups can be found. Throughout the paper p denotes a prime number. A *pro-p-group* is a projective limit of finite p-groups, or equivalently a compact, totally-disconnected, Hausdorff topological group whose images under continuous homomorphisms into finite groups are p-groups. For a natural number n, the *free* pro-p-group F of rank n is the topological completion of the abstract free group Δ of rank n with respect to the group topology of Δ, whose fundamental system of neighborhoods of the identity element are those normal subgroups N of finite index in Δ, such that Δ/N is a finite p-group. A pro-p-group G is *finitely generated* if it contains a dense subgroup that is finitely generated as an abstract group; otherwise we say that G is infinitely generated. For a finitely generated group G, $d(G)$ denotes the smallest cardinality of a set of generators of G. The *Frattini* subgroup of a pro-p-group G is the intersection of its maximal open subgroups, and it is denoted by $\Phi(G)$; $G/\Phi(G)$ is a vector space over the field with p elements, and its dimension is precisely $d(G)$ (cf. [6]). All subgroups of a pro-p-group are assumed to be closed, unless otherwise stated; and all homomorphisms of pro-p-groups are assumed to be continuous. If G is a pro-p-group, and α an automorphism of G then the fixed subgroup $\mathrm{Fix}_G(\alpha)$ of α in G consists of the subgroup $\{x \in G | x^\alpha = x\}$. We denote by $\hat{\mathbf{Z}}_p$ the additive group of the ring of p-adic integers. If A and B are pro-p-groups, $A \coprod B$ denotes their free pro-p-product (cf., e.g. [2]).

2. Involutions

In this section we study the automorphisms of order 2 of a free pro-p-group of finite rank, where $p \neq 2$. We begin with an auxiliary result.

2.1. **Lemma.** *Let p be a prime number and $\alpha \in \mathrm{GL}(n, F) \approx \mathrm{GL}(V)$, where V is an n-dimensional vector space over the field F, and assume $\alpha^m = 1$, where m is a natural number; if $\mathrm{char}(F) = p > 0$, we assume in addition that $p \nmid m$. Then*

$$\mathrm{Ker}(I + \alpha + \cdots + \alpha^{m-1}) = Im(\alpha - I).$$

Proof. Let V_1 be the eigenspace of α belonging to 1. By Maschke's theorem there exists an α-subspace W of V with $V = V_1 \oplus W$. Denote by α_1 and β the restrictions of α to V_1 and W, respectively. Then $\alpha = \alpha_1 \oplus \beta$. So

$(I+\alpha+\cdots+\alpha^{m-1}) = (I+\alpha_1+\cdots+\alpha_1^{m-1}) \oplus (I+\beta+\cdots+\beta^{m-1})$. Therefore, since $\beta - I_W$ is an isomorphism of W, we have

$$\begin{aligned}
&\operatorname{Ker}(I+\alpha+\cdots+\alpha^{m-1}) \\
&= \operatorname{Ker}(I_{V_1}+\alpha_1+\cdots+\alpha_1^{m-1}) \oplus \operatorname{Ker}(I_W+\beta+\cdots+\beta^{m-1}) \\
&= \operatorname{Ker}(m(\mathrm{id}_{V_1})) \oplus \operatorname{Ker}(I_W+\beta+\cdots+\beta^{m-1})(\beta - I_W) = O_{V_1} \oplus \operatorname{Ker}(\beta^m - I_W) \\
&= O_{V_1} \oplus W = W. \quad \square
\end{aligned}$$

2.2. **Lemma.** *Let $p \neq 2$ be a prime number, and let*

$$1 \longrightarrow V \longrightarrow G \longrightarrow G/V = Q \longrightarrow 1$$

be an exact sequence of pro-p-groups, where V is a finitely generated elementary Abelian p-group. Assume α is an automorphism of G such that $V^\alpha = V$, and suppose that $\alpha^2 = I$. Denote by $\bar{\alpha}$ the automorphism of Q induced by α, and suppose that $q^{\bar{\alpha}} = q^{-1}$ for some $q \in Q$. Then, there exists some $g \in G$ with $gV = q$ and $g^\alpha = g^{-1}$.

Proof. Choose any $x \in G$ such $xV = q$. Then $x^\alpha = vx^{-1}$ for some $v \in V$. Then $x = x^{\alpha^2} = v^\alpha x^{-\alpha} = v^\alpha x v^{-1}$, so that $v = v^{\alpha x}$, i.e. $v \in \operatorname{Ker}(I - \alpha x)$. On the other hand, $(\alpha x)^2 = \alpha x \alpha x = x^\alpha x = vx^{-1}x = v$, so that for every $u \in V$ one has $u^{(\alpha x)^2} = u^v = u$, i.e. $(\alpha x)^2$ is the identity when restricted to V. Now, we are looking for $w \in V$ such that $(wx)^\alpha = (wx)^{-1}$, i.e. $x^{-1}w^{-1} = w^\alpha x^\alpha = w^\alpha v x^{-1}$, and therefore, in additive notation, $w^\alpha + w^x = -v$. Set $w_1 = w^\alpha$ to get $w_1 + w_1^{\alpha x} = -v$. Therefore to prove the existence of w, it suffices to show that $\operatorname{Ker}(I - \alpha x) \leq \operatorname{Im}(I + \alpha x)$ in V. This follows from Lemma 2.1. $\square$

2.3. Theorem. *Let G be a finitely generated pro-p-group, with $p \neq 2$, and let α be an automorphism of G of order 2. Then there is a set of generators $\{x_1, \ldots, x_t, y_1, \ldots, y_s\}$ of G such that $x_i^\alpha = x_i$ and $y_j^\alpha = y_j^{-1}$ $(i = 1, \ldots, t; j = 1, \ldots, s)$. The number $t+s$ may be chosen so that the minimal number of generators $d(G)$ of G is precisely $t+s$.*

Proof. Let $G^1 = \Phi(G) = \Phi^1(G)$ be the Frattini subgroup of G, and set $G^{r+1} = \Phi^{r+1}(G) = \Phi(\Phi^r(G))$. For each $r = 1, 2, \ldots$, consider the natural short exact sequence of finite p-groups

$$0 \longrightarrow G^n/G^{n+1} \longrightarrow G/G^{n+1} \longrightarrow G/G^n \longrightarrow 0.$$

Since G/G^1 is a vector space over $\mathbf{F}_p$ (the field with p elements), there are elements $x_1(1), \ldots, x_t(1)$, $y_1(1), \ldots, y_s(1)$ in G such that $t+s = \dim(G/G_1) = d(G)$, and for each i and j one has $x_i(1)^\alpha \equiv x_i(1)$ and $y_j(1)^\alpha \equiv y_j(1)^{-1}$ modulo G^1 (this is clear since $\bar{\alpha}^2 = I$ and $2 \neq p$, where $\bar{\alpha}$ denotes the automorphism of G/G^1 induced by α). Therefore, by Satz 18.6, p. 131, in [8] and an induction argument applied to the above exact sequences, we deduce that for

each n there exist elements $x_1(n), \dots, x_t(n)$ of G such that $x_i(n+1) \equiv x_i(n)$ modulo G^n, and $x_i(n)^\alpha \equiv x_i(n)$ modulo G^n, and $x_i(n)^a \equiv x_i(n)$ modulo G^n $(i = 1, \dots, t;\ n = 0, 1, \dots)$. On the other hand from Lemma 2.2 and an induction process, we get elements $y_1(n), \dots, y_s(n)$ of G such that $y_j(n+1) \equiv y_j(n)$ modulo G^n, and $y_j(n)^\alpha \equiv y_j(n)^{-1}$ modulo G^n $(j = 1, \dots, s;\ n = 1, 2, \dots)$. Note that $x_i(n)$ and $y_j(n)$ are congruent to $x_i(1)$ and $y_j(1)$, respectively, modulo G^1, and therefore $x_1(n), \dots, x_t(n), y_1(n), \dots, y_s(n)$ generate G for each $n = 1, 2, \dots$. Put $x_i = (x_i(1), x_i(2), \dots)$ and $y_j = (y_j(1), y_j(2), \dots) \in \lim_{\leftarrow} G/G^n = G$. It is now plain that $x_1, \dots, x_t, y_1, \dots, y_s$ generate G and that $x_i^\alpha = x_i$ and $y_j^\alpha = y_j^{-1}$ $(i = 1, \dots, t;\ j = 1, \dots, s)$, as desired. □

2.4. **Lemma.** (cf. [1], Theorem 6). *Let p be a prime number and let G be a finitely generated pro-p-group with minimal number of generators $d(G) = n$. Consider the natural homomorphism*

$$\pi\colon \operatorname{Aut}(G) \longrightarrow \operatorname{Aut}(G/\Phi(G)) \approx \operatorname{GL}(n, p),$$

where $\Phi(G)$ is the Frattini subgroup of G. Then $\operatorname{Ker}(\pi)$ is a pro-p-group.

Proof. We think of $\operatorname{Aut}(G)$ as a profinite group, $\operatorname{Aut}(G) = \lim_{\leftarrow} \operatorname{Aut}(G/\Phi^r(G))$. Let $\beta \in \operatorname{Ker}(\pi)$ and suppose that p does not divide the order (in the profinite sense; cf. [11] or [10]) of $<\beta>$. If $x_1, \dots, x_n$ is a set of generators for G, it follows from Lemma 1.3 in [5] that $\beta(x_i k_i) = x_i k_i$, for some $k_i \in \Phi(G)$ $(i = 1, \dots, n)$; and since $x_1 k_1, \dots, x_n k_n$ is also a set of generators for G, one gets that β is the identity. It follows that $\operatorname{Ker}(\pi)$ is a pro-p-group. □

2.5. **Corollary.** *Let F be a free pro-p-group of* rank n. *Consider the natural epimorphism $\pi\colon \operatorname{Aut}(F) \longrightarrow \operatorname{Aut}(F/\Phi(F)) \approx \operatorname{GL}(n, p)$, $\Phi(F)$ being the Frattini subgroup of F. Then,* (i) *every element $\bar{y}$ of $\operatorname{Aut}(F/\Phi(F))$ of order q, with $p \nmid q$, can be lifted to an automorphism α of order q of F; and* (ii) *if $p \neq 2$, π defines a* 1-1 *correspondence between the conjugacy classes of involutions of $\operatorname{Aut}(F)$ and the conjugacy classes of involutions of $\operatorname{GL}(n, p)$.*

Proof. (i) Let $\gamma \in \operatorname{Aut}(F)$ be such that $\pi(\gamma) = \bar{y}$. The order of the procyclic group $<\gamma>$ is then divisible by q. Then $<\gamma>$ contains an element α of order q. It follows then from Lemma 2.4 that $\pi(\alpha) = \bar{y}$.

(ii) Let α and β be conjugate involutions in $\operatorname{Aut}(F)$, then obviously $\pi(\alpha)$ and $\pi(\beta)$ are conjugate in $\operatorname{GL}(n, p)$, and by Lemma 2.4 $\pi(\alpha)$ and $\pi(\beta)$ are also of order 2, since $p \neq 2$. Conversely, suppose α and β are involutions in $\operatorname{Aut}(F)$, and $\pi(\alpha)$ and $\pi(\beta)$ are conjugate in $\operatorname{GL}(n, p)$. Say $\bar{\delta}^{-1}\pi(\alpha)\bar{\delta} = \pi(\beta)$, where $\bar{\delta} \in \operatorname{GL}(n, p)$. Let $\delta \in \operatorname{Aut}(F)$ be such that $\pi(\delta) = \bar{\delta}$. Then, $\pi(\delta^{-1}\alpha\delta) = \pi(\beta)$. Put $\gamma = \delta^{-1}\alpha\delta$. By Theorem 2.3, there exist generating sets $\{x_i, \dots, x_t, y_1, \dots, y_s\}$ and $\{u_1, \dots, u_t, v_1, \dots, v_s\}$ of F, such that $x_i^\beta = x_i$, $y_j^\beta = y_j^{-1}$, $u_i^\gamma = u_i$ and $v_j^\gamma = v_j^{-1}$ $(i = 1, \dots, t; j = 1, \dots, s)$; moreover $t + s = n$, and so these generating sets are actually bases

of F. Let ρ be the automorphism of F defined by $u_i^\rho = x_i$ and $v_j^\rho = y_j$ $(i = 1, \dots, t; j = 1, \dots, s)$. Then $\rho^{-1}\gamma\rho = \beta$, since $x_i^{\rho^{-1}\gamma\rho} = x_i^\beta$ and $y_j^{\rho^{-1}\gamma\rho} = y_j^\beta$ $(i = 1, \dots, t;\quad j = 1, \dots, s)$. □

2.6. **Corollary.** *Let p be a prime number and F a free pro-p-group of* rank n. *Then the index of a p-Sylow subgroup of* $\mathrm{Aut}(F)$ *is* $(p^n-1)(p^{n-1}-1)\cdots(p-1)$.

Proof. This follows from Lemma 2.4, and the following facts: $|\mathrm{GL}(n,p)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$ (cf. [8], Hilfssatz 6.2, p. 178), and

$$\pi\colon \mathrm{Aut}(F) \longrightarrow \mathrm{Aut}(F/\Phi(F)) \approx \mathrm{GL}(n,p)$$

is an epimorphism. □

3. Fixed subgroups

In this section we study the subgroup of fixed elements of a free pro-p-group under certain automorphisms. If Δ is an abstract free group of finite rank, and β is an automorphism of Δ, then the subgroup of those elements of Δ fixed by β has finite rank (cf. [4], Theorem 9.8). In Theorem 3.2 we show that for certain types of automorphisms of free pro-p-groups, their fixed subgroups are infinitely generated (see §1 for a precise definition of finite generation).

3.1. **Lemma.** *Let F be a free pro-p-group of* rank n. *Suppose $\alpha, \beta \in \mathrm{Aut}(F)$ are both of order m, $p \nmid m$, and assume that the induced automorphisms $\bar\alpha$, $\bar\beta \in \mathrm{Aut}(F/\Phi(F))$ are conjugate in $\mathrm{Aut}(F/\Phi(F))$, where $\Phi(F)$ is the Frattini subgroup of F. Then α, β are conjugate in $\mathrm{Aut}(F)$.*

Proof. Note first that $\bar\alpha$ and $\bar\beta$ are also of order m by Lemma 2.4. To prove the result we may assume that $\bar\alpha = \bar\beta$, since the natural homomorphism $\pi\colon \mathrm{Aut}(F) \longrightarrow \mathrm{Aut}(F/\Phi(F))$ is onto. Then $\beta = \gamma\alpha$, where $\gamma \in \mathrm{Ker}(\pi)$ which is a pro-p-group by Lemma 2.4. Therefore $\langle\alpha,\gamma\rangle$ is a semidirect product $\langle\alpha,\gamma\rangle = \langle\gamma,\gamma^\alpha,\dots,\gamma^{\alpha^{n-1}}\rangle \rtimes \langle\alpha\rangle$ of a pro-p-group and a cyclic group $\langle\alpha\rangle$ of order m. It follows that $\langle\alpha\rangle$ and $\langle\beta\rangle = \langle\gamma\alpha\rangle$ are Hall subgroups of order m of the prosolvable group $\langle\alpha,\gamma\rangle$, and therefore are conjugate (cf. [3]). Hence, there exists $g \in \langle\gamma,\gamma^\alpha,\dots,\gamma^{\alpha^{m-1}}\rangle$ such that $\langle\alpha\rangle^g = \langle\beta\rangle$. Thus, for some $k = 1, \dots, m-1$, we have $\alpha^g = \beta^k$; and so $\bar\beta = \bar\alpha = \bar\beta^k$. It follows that $k = 1$, i.e. $\alpha^g = \beta$. □

3.2. **Theorem.** *Let F be a free pro-p-group of finite* rank $n \geq 2$. *Let $\alpha \in \mathrm{Aut}(F)$ be of finite order $m \neq 1$, with $p \nmid m$. Then $\mathrm{Fix}_F(\alpha) = \{x \in F \mid x^\alpha = x\}$ is infinitely generated.*

Before we prove this theorem, we need the following result.

3.3. **Lemma.** *Let F be a free pro-p-group of finite* rank n, *and let α be an automorphism of F. Assume α has finite order m, and $p \nmid m$. Let $G = \mathrm{Fix}_F(\alpha)$, and suppose $F = G \coprod T$ (a free pro-p-product), for some subgroup T of F. Then there exists an α-invariant subgroup S of F such that $F = G \coprod S$.*

Proof. Consider the $\mathbf{F}_p$-vector space $V = F/\Phi(F)$ of dimension n, where $\Phi(F)$ is the Frattini subgroup of F, and $\mathbf{F}_p$ is the field with p elements. Let $\bar{\alpha}$ be the automorphism induced by α on V. Then $V_1 = G\Phi(F)/\Phi(F)$ is an $\bar{\alpha}$-subspace of V. By Maschke's theorem there exists an $\bar{\alpha}$-subspace V_2 of V such that $V = V_1 \oplus V_2$. We may assume that $T\Phi(F)/\Phi(F) = V_2$ (otherwise, let $\overline{T}$ be a subgroup of F such that $\operatorname{rank}(\overline{T}) = \dim(V_2) = \operatorname{rank}(T)$ and $\overline{T}\Phi(F)/\Phi(F) = V_2$; then F is generated by G and T; so the epimorphism $F = G \coprod T \longrightarrow F =< G, \overline{T} >$ that sends G to G identically and T to $\overline{T}$ isomorphically, must be an isomorphism by Proposition 7.6, Ch. I in [10]; thus $F = G \coprod \overline{T}$ and so we may substitute T by $\overline{T}$). Define an automorphism β of F so that β be the identity on G and send T to T as follows: if $x_1, \ldots, x_t$ is a basis for T, then $\beta(x_i) = \alpha(x_i)f_i$ where $f_i \in \Phi(F) \cap T$. It follows that $\operatorname{ord}(\beta) = \operatorname{ord}(\alpha)$, and the automorphisms $\bar{\alpha}$ and $\bar{\beta}$ induced by α and β on V, coincide. Therefore, by Lemma 3.1 there exists an automorphism γ of F with $\beta = \gamma^{-1}\alpha\gamma$. Consider the subgroup S of F defined by $S = T^{\gamma^{-1}}$. Then $S^{\alpha} = T^{\gamma^{-1}\alpha\gamma\gamma^{-1}} = T^{\gamma^{-1}} = S$, i.e. S is an α-invariant subgroup of F. Now for $x \in G = \operatorname{Fix}_F(\alpha)$ one has $x^{\gamma^{-1}\alpha} = x^{\beta\gamma^{-1}} = x^{\gamma^{-1}}$; hence, $x^{\gamma^{-1}} \in G$, i.e. G is γ^{-1}-invariant. Thus $F = (G \coprod T)^{\gamma^{-1}} = G \coprod S$. □

Proof of Theorem 3.2. We proceed by induction on the number k of prime divisors of m.

Case I. Assume $k = 1$ and $m = q$, a prime different from p. First note that $G = \operatorname{Fix}_F(\alpha) \neq 1$, for otherwise the group $\langle\alpha\rangle$ would act elementwise fixed point free on F; therefore by Corollary 3.7 of [5], F would be nilpotent, contradicting the fact that F is free pro-p of rank at least 2. Suppose that $G = \operatorname{Fix}_F(\alpha)$ were finitely generated. Then by Theorem 3.2 in [9], there would exist an open subgroup U of F such that $U = G \coprod T$ (free pro-p-product), where T is a certain subgroup of F. We may assume that U is α-invariant (for otherwise one can substitute U by $V = U \cap U^{\alpha} \cap \cdots \cap U^{\alpha^{q-1}}$; note that by the Kurosh subgroup theorem, cf. [2], the group G is still a free factor of the group V). By Lemma 3.3, we may assume that T is α-invariant. Assume first that $T = 1$, then G is a proper open subgroup of F of index p^t, say. Let $\bar{\alpha}$ denote the induced automorphism on the free Abelian pro-p-group F/F'. Note that $\bar{\alpha}$ cannot be the identity automorphism, for otherwise one readily deduces from Lemma 1.3 in [5] that α is also the identity. Say $\bar{x} \in F/F'$ with $\bar{\alpha}(\bar{x}) \neq \bar{x}$. Then, using additive notation, one has $\bar{\alpha}(p^t\bar{x}) = p^t\bar{x}$ (since $G = \operatorname{Fix}_F(\alpha)$ has index p^t in F); so $p^t(\bar{\alpha}(\bar{x}) - \bar{x}) = 0$, and hence $\bar{\alpha}(\bar{x}) = \bar{x}$, a contradiction. Therefore, we must have that $T \neq 1$. Consider now the Cartesian subgroup L of $U = G \coprod T$ (i.e. the subgroup of U generated by the set of commutators $\{[g,t] | 1 \neq g \in G,\ 1 \neq t \in T\}$). Then L is α-invariant, and $\operatorname{Fix}_L(\alpha) \neq 1$, again by Corollary 3.7 in [5]. But $\operatorname{Fix}_L(\alpha) = L \cap \operatorname{Fix}_F(\alpha) = L \cap G = 1$, a contradiction. Therefore $G = \operatorname{Fix}_F(\alpha)$ is infinitely generated when $m = q$ is a prime number.

Case II. $k = 1$ and $m = q^s$, where $s \geq 1$ and q is a prime number different from p. To see that $\mathrm{Fix}_F(\alpha)$ is infinitely generated, it suffices to show that $\mathrm{Fix}_F(\alpha) \neq 1$, for then the proof proceeds as in Case I. If $s = 1$, we are in the previous case; hence, assume that $s > 1$; then by Case I, $\mathrm{Fix}_F(\alpha^{q^{s-1}})$ is infinitely generated. Choose $x, y \in \mathrm{Fix}_F(\alpha^{q^{s-1}})$ so that $\langle x, y\rangle$ is not procyclic. Then

$$\Phi = \langle x, x^{\alpha}, x^{\alpha^2}, \ldots, x^{\alpha^{q^{s-1}-1}}, y, y^{\alpha}, y^{\alpha^2}, \ldots, y^{\alpha^{q^{s-1}-1}}\rangle$$

is a subgroup of $\mathrm{Fix}_F(\alpha^{q^{s-2}})$ of rank at least 2. Note that $\alpha^{q^{s-2}}$ induces on Φ an automorphism which is either the identity or of order q; and thus $\mathrm{Fix}_{\Phi}(\alpha^{q^{s-2}})$ (using again Case I if necessary) has rank at least 2; therefore, $\mathrm{Fix}_F(\alpha^{q^{s-2}})$ has rank greater or equal to 2. Continuing this process we deduce that $\mathrm{Fix}_F(\alpha) \neq 1$ (in fact it has rank at least 2), as desired. Hence, $\mathrm{Fix}_F(\alpha)$ is infinitely generated, if m involves one prime.

Case III. Assume that the result is true for $k = r$ as our induction hypothesis, and consider the case $m = h_1 \cdots h_r h_{r+1}$, where each h_i is a power of a prime number, and the primes are all different. Put $\beta = \alpha^{h_{r+1}}$. Then the order of β involves only r primes, and so by the induction hypothesis $\mathrm{Fix}_F(\beta)$ is infinitely generated. Note $\mathrm{Fix}_F(\alpha) \leq \mathrm{Fix}_F(\beta)$. If $\mathrm{Fix}_F(\alpha) = \mathrm{Fix}_F(\beta)$, then $\mathrm{Fix}_F(\alpha)$ is infinitely generated as desired. Otherwise, $\mathrm{Fix}_F(\alpha) \neq \mathrm{Fix}_F(\beta)$ and hence there exists $f \in \mathrm{Fix}_F(\beta) - \mathrm{Fix}_F(\alpha)$.

Consider the subgroup H generated by $\mathrm{Fix}_F(\alpha)$ and the elements $f, f^{\alpha}, \ldots, f^{\alpha^{q_{r+1}-1}}$. Note that $\alpha^{q_{r+1}}$ leaves f fixed, and therefore, α induces an automorphism on H of order dividing h_{r+1} and which is not the identity. From $\mathrm{Fix}_F(\alpha) \geq \mathrm{Fix}_H(\alpha) \geq \mathrm{Fix}_H(\alpha)$, we deduce $\mathrm{Fix}_F(\alpha) = \mathrm{Fix}_H(\alpha)$. Then $\mathrm{Fix}_F(\alpha)$ must be infinitely generated, for suppose that $\mathrm{Fix}_F(\alpha)$ were finitely generated; then H would be also finitely generated, and since h_{r+1} involves only one prime, we could apply to H the Case II considered above to get that $\mathrm{Fix}_H(\alpha) = \mathrm{Fix}_F(\alpha)$ is infinitely generated, a contradiction. □

4. Automorphisms whose orders involve p

In this section we describe a method to construct nonidentity automorphisms α as free pro-p-groups of finite rank such that the fixed subgroup of α has prescribed finite rank. By Theorem 3.2, the order of α must involve the prime p.

4.1. **Lemma.** *Let β be an automorphism of a finitely generated profinite group G, and let H be a finitely generated β-invariant subgroup of G. Consider the profinite groups* $\mathrm{Aut}(G)$ *and* $\mathrm{Aut}(H)$ *of continuous automorphisms of G and H, respectively. Then the order of the restriction $\bar{\beta} = \beta_{|H}$, as an element of* $\mathrm{Aut}(H)$, *divides the order of β, as an element of* $\mathrm{Aut}(G)$.

Proof. Note that the profinite structure of $\mathrm{Aut}(G)$ (respectively, of $\mathrm{Aut}(H)$) is given by $\mathrm{Aut}(G) = \varprojlim \mathrm{Aut}(G/G_n)$ (respectively, $\mathrm{Aut}(H) = \varprojlim \mathrm{Aut}(H/H_n)$), where for each natural number n, G_n (respectively, H_n) is the intersection of the subgroups of G (respectively, of H) of index at most n. The order of β (in the profinite sense, see, e.g. [12]) is the l.c.m. $\{\beta_n | n \in \mathbf{N}|\}$, where β_n is the image of β in $\mathrm{Aut}(G/G_n)$. Observe that each β_n induces an automorphism $\bar{\beta}_n$ of H/H_n, which is precisely the image of $\bar{\beta}$ in $\mathrm{Aut}(H/H_n)$. Since $\mathrm{Aut}(G/G_n)$ and $\mathrm{Aut}(H/H_n)$ are finite, it follows that the order of $\bar{\beta}_n$ divides the order of β_n; and therefore, the order of $\bar{\beta}$ divides the order of β. □

4.2. **Lemma.** *Let G be a finitely generated profinite group, γ an automorphism of G of finite order m, β an automorphism of G of order (not necessarily finite) relatively prime to m. Assume that γ and β commute, and put $\alpha = \beta\gamma$. Then $\mathrm{Fix}_G(\alpha) = \mathrm{Fix}_G(\gamma) \cap \mathrm{Fix}_G(\beta)$.*

Proof. Note first that $\alpha^m = \gamma^m \beta^m$. Let $x \in \mathrm{Fix}_G(\alpha)$. Then $x = x^{\alpha^m} = x^{\beta^m}$. So β induces an automorphism $\bar{\beta}$ of $H = \langle x, \ x^\beta, \ldots, x^{\beta^{m-1}} \rangle \leq G$, whose order divides m. On the other hand, by Lemma 4.1, the order of β must be a divisor of order (β). Therefore, $\bar{\beta}$ has order 1, i.e. $x^\beta = x$. It follows that $x^\gamma = x^{\alpha\beta^{-1}} = x$; and hence, $x \in \mathrm{Fix}_G(\gamma) \cap \mathrm{Fix}_G(\beta)$, i.e., $\mathrm{Fix}_G(\alpha) \leq \mathrm{Fix}_G(\gamma) \cap \mathrm{Fix}_G(\beta)$. The reverse containment is obvious. □

4.3. **Theorem.** *Let p be a prime number, and let $m \geq 1$ be an integer dividing $p-1$. Assume $r \geq 1$ and $n \geq 0$ are integers. Then there exist a free pro-p-group F and an automorphism α of F such that $\mathrm{Fix}_F(\alpha)$ has rank n, and the order of α is mp^r.*

Proof. Consider a free pro-p-group F of rank $p^r + n$, that we write in the form $F = G \coprod L$, where G and L are free pro-p-groups of rank p^r and n, respectively. Define the group $m = \langle x \rangle \coprod (L \times C)$ to be the free pro-p-product of the groups $\langle x \rangle \approx \hat{\mathbf{Z}}_p$ and $L \times C$, where $C = \langle y \rangle$ is a finite cyclic group of order p^r. Let K be the normal closure of x and L in M; then $K = \langle x^{y^i}, \ L | i = 0, \ldots, p^r - 1 \rangle$. On the other hand, consider the semidirect product $F \rtimes C$, where y acts on F as the automorphism β that sends L to L identically and sends G to G by $x_i^\beta = x_j$, with $j = i + 1$ modulo p^r, where $\{x_i | i = 1, \ldots, p^r - 1\}$ is a basis for G. Define a homomorphism $\varphi: M \longrightarrow F \rtimes C$ by $\varphi(x) = x_1$, $\varphi(y) = y$ and φ sends L to L identically. Clearly $\varphi(K) = F$; then since F is free pro-p and K can be generated by rank(F) elements, the restriction of φ to K is an isomorphism of K onto F, and so $M = \langle x \rangle \coprod (L \times C) = K \rtimes C \approx F \approx C$. We claim that $\mathrm{Fix}_F(\beta) = L$. To see this we think of β as being the automorphism of $K \approx F$ induced by the inner automorphism of M determined by y. Now, $k^y = k$ if and only if $k \in L \times C$ (cf. [7], Theorem 2), i.e. the elements of K that commute with y are those in $K \cap (L \times C) = L$.

Since $\mathrm{Aut}(\hat{\mathbf{Z}}_p) \approx C_{p-1} \times \hat{\mathbf{Z}}_p$ if $p \neq 2$, and $\mathrm{Aut}(\hat{\mathbf{Z}}_2) \approx C_2 \times \hat{\mathbf{Z}}_2$ (cf. [11], p. 17), there exists an element $\mu \in \hat{\mathbf{Z}}_p$ whose multiplicative order is m. Let

$z_1, \ldots, z_n$ be a basis of L. Define now an automorphism γ of order m of F as follows: $x_i^\gamma = x_i^\mu$ for every $i = 1, \ldots, p^r$, and $z_j^\gamma = z_j$ for every $j = 1, \ldots, n$. It is plain that order $(\gamma) = m$, and since β and γ commute, the automorphism $\alpha = \beta\gamma$ of F has order mp^r. Finally, $\mathrm{Fix}_F(\alpha) = L$, by Lemma 4.2 □

References

1. M. P. Anderson, *Exactness properties of profinite completion of functors*, Topology **13** (1974), 229–239.
2. E. Binz, J. Neukirch and G. H. Wenzel, *A subgroup theorem for free products of profinite groups*, J. Algebra **19** (1971), 104–109.
3. E. D. Bolker, *Inverse limits of solvable groups*, Proc. Amer. Math. Soc. **14** (1963), 147–152.
4. S. M. Gersten, *Fixed points of automorphisms of free groups*, Adv. in Math. **64** (1987), 51–85.
5. D. Gildenhuys, W. Herfort and L. Ribes, *Profinite Frobenius groups*, Arch. Math. **33** (1979), 518–528.
6. K. Gruenberg, *Projective profinite groups*, J. London Math. Soc (3) **42** (1967), 155–165.
7. W. Herfort and L. Ribes, *Torsion elements and centralizers in free products of profinite groups*, J. Reine Angew. Math. **358** (1985), 155–161.
8. B. Huppert, *Endliche Gruppen* I, Springer, Berlin, 1967.
9. A. Lubotzky, *Combinatorial group theory for pro-p-groups*, J. Pure Appl. Algebra **25** (1982), 311–325.
10. L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's Papers in Pure and Appl. Math. **24**, Berlin, (1970).
11. J-P. Serre, *A course in arithmetic*, Springer, Berlin, 1973.
12. ____, *Cohomologie Galoisienne*, Lecture Notes in Math., vol. 5, Springer-Verlag, 1965.

Institut für Angewandte und Numerische Mathematik, Technische Universität Wien, A-1040 Wien, Austria

Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario K1S 5B6, Canada