PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 103, Number 4, August 1988

ELEMENTARY EQUIVALENCE AND PROFINITE COMPLETIONS: A CHARACTERIZATION OF FINITELY GENERATED ABELIAN-BY-FINITE GROUPS

FRANCIS OGER

(Communicated by Thomas J. Jech)

ABSTRACT. In this paper, we show that any finitely generated abelian-by-finite group is an elementary submodel of its profinite completion. It follows that two finitely generated abelian-by-finite groups are elementarily equivalent if and only if they have the same finite images. We give an example of two finitely generated abelian-by-finite groups G, H which satisfy these properties while $G \times \mathbf{Z}$ and $H \times \mathbf{Z}$ are not isomorphic. We also prove that a finitely generated nilpotent-by-finite group is elementarily equivalent to its profinite completion if and only if it is abelian-by-finite.

The definitions and results of model theory which are used here, and in particular the notions of elementary equivalence and elementary submodel, are given in [**2**]. Anyhow, for the sake of brevity, we denote by G^U the ultrapower G^I/U, for each group G and each ultrafilter U over a set I. Concerning group theory, the reader is referred to [**9** and **10**].

We obtain the following characterization:

THEOREM. *A finitely generated nilpotent-by-finite group is elementarily equivalent to its profinite completion if and only if it is abelian-by-finite.*

This result is a consequence of Theorems 1 and 2 below.

THEOREM 1. *Any finitely generated abelian-by-finite group is an elementary submodel of its profinite completion.*

THEOREM 2. *If G is a finitely generated nilpotent-by-finite, but not abelian-by-finite, group, then there exists an existential sentence, built up from the multiplication symbol, which is false in G and true in the profinite completion of G.*

Theorem 1 generalizes [**7**, Theorem 1.4], which was only valid for finitely generated finite-by-abelian groups. A finitely generated finite-by-abelian group is abelian-by-finite, since its center is a normal subgroup of finite index according to the result of P. Hall which is mentioned in [**10**, p. 12]. On the other hand, the finitely presented abelian-by-finite group $\langle x, y;\ y^2 = 1, y^{-1}xy = x^{-1}\rangle$ is not finite-by-abelian as its center is trivial.

By [**11**, Theorem 2.1 and **6**, Theorem 5.5], the following properties are equivalent for two finitely generated finite-by-abelian groups G, H:

(1) G and H are elementarily equivalent;

Received by the editors July 16, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20A15; Secondary 03C60, 20F18.

(2) G and H have isomorphic profinite completions;
(3) G and H have the same finite images;
(4) $G \times \mathbf{Z} \cong H \times \mathbf{Z}$;
(5) There exists an integer $n \geq 1$ such that $\times^n G \cong \times^n H$.

The result below generalizes the equivalence of (1), (2) and (3) to finitely generated abelian-by-finite groups. It is a consequence of Theorem 1, [**9**, Proposition 4, p. 225] and the remark which follows Corollary 3.4 of [**6**]:

COROLLARY. *The following properties are equivalent for two finitely generated abelian-by-finite groups G, H:*
(1) *G and H are elementarily equivalent;*
(2) *G and H have isomorphic profinite completions;*
(3) *G and H have the same finite images.*

For two finitely generated abelian-by-finite groups G, H, (4) and (5) are equivalent and imply (1), (2) and (3), according to [**3**, Theorem 1, **4**, Theorem 9 and **5**, Theorem 1]. Anyhow, contrary to the case of finitely generated finite-by-abelian groups, the converse is false, as we can see from the following proposition.

PROPOSITION. *Let us consider the finitely presented abelian-by-finite groups:*

$$M = \langle a, b;\ a^{25} = 1,\ b^{-1}ab = a^6\rangle,$$
$$N = \langle c, d;\ c^{25} = 1,\ d^{-1}cd = c^{11}\rangle,$$
$$G = \langle M \times M, y;\ y^2 = 1,\ y^{-1}(u,v)y = (v,u) \text{ for any } u, v \in M\rangle,$$
$$H = \langle N \times N, z;\ z^2 = 1,\ z^{-1}(u,v)z = (v,u) \text{ for any } u, v \in N\rangle.$$

Then, G and H are elementarily equivalent, but $G\times\mathbf{Z}$ and $H\times\mathbf{Z}$ are not isomorphic.

REMARK. The characterization of the models of the theory of a finitely generated finite-by-abelian group which is given in [**7**, Theorem 1.3] is not valid for finitely generated abelian-by-finite groups. In fact, the finitely generated abelian-by-finite group $G = \langle x, y;\ y^2 = 1,\ y^{-1}xy = x^{-1}\rangle$ has a trivial center and the same property is true for any group which is elementarily equivalent to G.

§§1, 2 and 3 are respectively devoted to the proofs of Theorem 1, Theorem 2 and the proposition.

1. Proof of Theorem 1.

LEMMA 1.1. *If M is a finitely generated nilpotent-by-finite group, then there exists an integer $n \geq 1$ such that M^n is nilpotent and torsion-free.*

PROOF OF LEMMA 1.1. Let us consider a nilpotent normal subgroup N of M such that M/N is finite. There exists an integer $r \geq 1$ such that M^r is contained in N. The nilpotent group N is finitely generated according to [**8**, Theorem 1.41] and it follows from [**10**, Exercise 3.10 and Theorem 3.25] that the set $t(N)$ of all torsion elements of N is finite. As M is residually finite by [**9**, Theorem 1, p. 17], there exists an integer $s \geq 1$ such that $M^s \cap t(N) = \{1\}$. For each integer n which is divisible by r and s, we have $M^n \subset N$ and $M^n \cap t(N) = \{1\}$; so, M^n is nilpotent and torsion-free.

NOTATIONS. For each group M, for each ultrafilter U over a set I, for each $x \in M$ and for each $a \in \mathbf{Z}^U$, we denote by x^a the element of M^U which admits

$(x^{a(i)})_{i\in I}$ as a representative, where $(a(i))_{i\in I}$ is a representative of a in $\mathbf{Z}^I$. The element x^a does not depend on the choice of the representative $(a(i))_{i\in I}$.

For each residually finite group M, for each $x \in M$ and for each $a \in \widehat{\mathbf{Z}}$, if $(a(n))_{n\in\mathbf{N}}$ is a sequence of elements of $\mathbf{Z}$ which converges to a in $\widehat{\mathbf{Z}}$, then $(x^{a(n)})_{n\in\mathbf{N}}$ converges in $\widehat{M}$ to an element which we denote by x^a. This element does not depend on the choice of the sequence $(a(n))_{n\in\mathbf{N}}$.

PROOF OF THEOREM 1. We must show that, if G is a finitely generated abelian-by-finite group, then G and $\widehat{G}$ satisfy the same sentences with parameters in G. According to [**2**, Theorem 4.1.9], it is enough to prove that there exist an ultrafilter U and an isomorphism $f\colon G^U \to \widehat{G}^U$ which fixes the elements of G.

By Lemma 1.1, there exists an integer $p \geq 1$ such that G^p is abelian and torsion-free. We consider a basis $\{z_1, \ldots, z_s\}$ of the free $\mathbf{Z}$-module G^p and representatives $y_1, \ldots, y_r$ of the elements of G/G^p in G. Each element of G can be written in a unique way $x = y_a z_1^{a(1)} \cdots z_s^{a(s)}$ with $1 \leq a \leq r$ and $a(1), \ldots, a(s) \in \mathbf{Z}$.

The multiplication law of G is determined by a set of equalities:

$$[z_i, z_j] = 1 \quad \text{for } 1 \leq i, j \leq s,$$

$$y_i y_j = y_{g(i,j)} z_1^{g(1,i,j)} \cdots z_s^{g(s,i,j)} \quad \text{for } 1 \leq i, j \leq r,$$

$$y_i^{-1} z_j y_i = z_1^{h(1,i,j)} \cdots z_s^{h(s,i,j)} \quad \text{for } 1 \leq i \leq r \text{ and } 1 \leq j \leq s,$$

with $1 \leq g(i,j) \leq r$ for $1 \leq i,j \leq r$, $g(1,i,j), \ldots, g(s,i,j) \in \mathbf{Z}$ for $1 \leq i,j \leq r$ and $h(1,i,j), \ldots, h(s,i,j) \in \mathbf{Z}$ for $1 \leq i \leq r$ and $1 \leq j \leq s$. We have $y_i^{-1} z_j^a y_i = (y_i^{-1} z_j y_i)^a = z_1^{h(1,i,j)a} \cdots z_s^{h(s,i,j)a}$ for $1 \leq i \leq r$, $1 \leq j \leq s$ and $a \in \mathbf{Z}$.

A sequence $(x_n)_{n\in\mathbf{N}}$ of elements of G, with $x_n = y_{a(n)} z_1^{a(1,n)} \cdots z_s^{a(s,n)}$ for each integer n, converges in $\widehat{G}$ if and only if, first, $(a(n))_{n\in\mathbf{N}}$ is stationary and, second, for each integer $1 \leq i \leq s$, $(a(i,n))_{n\in\mathbf{N}}$ converges in $\widehat{\mathbf{Z}}$. In fact, if $(x_n)_{n\in\mathbf{N}}$ converges in $\widehat{G}$, then, for each integer $q \geq 1$, there exists an integer m such that, for each integer $n \geq m$, $x_n x_m^{-1}$ belongs to $G^{pq} \subset (G^p)^q$; for each integer $n \geq m$, we have $a(n) = a(m)$ and $a(1,n) - a(1,m), \ldots, a(s,n) - a(s,m)$ belong to $q\mathbf{Z}$.

So the profinite completion $\widehat{G}$ of G is equal to the set of all elements $x = y_a z_1^{a(1)} \cdots z_s^{a(s)}$ with $1 \leq a \leq r$ and $a(1), \ldots, a(s) \in \widehat{\mathbf{Z}}$, where the multiplication law is given by the following rules:

(1) $z_i^a z_i^b = z_i^{a+b}$ for $1 \leq i \leq s$ and $a, b \in \widehat{\mathbf{Z}}$;

(2) $[z_i^a, z_j^b] = 1$ for $1 \leq i, j \leq s$ and $a, b \in \widehat{\mathbf{Z}}$;

(3) $y_i y_j = y_{g(i,j)} z_1^{g(1,i,j)} \cdots z_s^{g(s,i,j)}$ for $1 \leq i, j \leq r$;

(4) $y_i^{-1} z_j^a y_i = z_1^{h(1,i,j)a} \cdots z_s^{h(s,i,j)a}$ for $1 \leq i \leq r$, $1 \leq j \leq s$ and $a \in \widehat{\mathbf{Z}}$.

For each ultrafilter U over a set I and for each $x \in G^U$ (respectively $\widehat{G}^U$), let us consider a representative $(x_i)_{i\in I}$ of x in G^I (respectively $\widehat{G}^I$). Each element x_i can be written in a unique way $x_i = y_{a(i)} z_1^{a(1,i)} \cdots z_s^{a(s,i)}$ with $1 \leq a(i) \leq r$ and $a(1,i), \ldots, a(s,i) \in \mathbf{Z}$ (respectively $\widehat{\mathbf{Z}}$). There exists a unique element $a \in \{1, \ldots, r\}$ such that $\{i \in I | a(i) = a\}$ belongs to U. We have $x = y_a z_1^{a(1)} \cdots z_s^{a(s)}$, where $a(1), \ldots, a(s)$ are the elements of $\mathbf{Z}^U$ (respectively $\widehat{\mathbf{Z}}^U$) which admit $a(1,i)_{i\in I}, \ldots, a(s,i)_{i\in I}$ as representatives. This decomposition of x is necessarily unique and does not depend on the choice of the representative $(x_i)_{i\in I}$ of x in G^I (respectively $\widehat{G}^I$).

So, for each ultrafilter U over a set I, G^U (respectively $\widehat{G}^U$) is the set of all elements $x = y_a z_1^{a(1)} \cdots z_s^{a(s)}$ with $1 \leq a \leq r$ and $a(1), \ldots, a(s) \in \mathbf{Z}^U$ (respectively $\widehat{\mathbf{Z}}^U$), where the multiplication law is obtained by replacing $\widehat{\mathbf{Z}}$ by $\mathbf{Z}^U$ (respectively $\widehat{\mathbf{Z}}^U$) in the rules (1), (2), (3), (4) above; we prove these rules in G^U (respectively $\widehat{G}^U$) by applying the same rules to representatives in G^I (respectively $\widehat{G}^I$) of the elements that we consider.

As $\mathbf{Z}$ is an elementary submodel of its profinite completion, we obtain elementarily equivalent structures by interpreting, in $\mathbf{Z}$ and $\widehat{\mathbf{Z}}$, each element of $\mathbf{Z}$ by a constant. So, according to [**2**, Theorem 6.1.15], there exist an ultrafilter U and an isomorphism $f\colon \mathbf{Z}^U \to \widehat{\mathbf{Z}}^U$ which fixes the elements of $\mathbf{Z}$. We define an isomorphism $\bar{f}\colon G^U \to \widehat{G}^U$ which fixes the elements of G by $\bar{f}(y_a z_1^{a(1)} \cdots z_s^{a(s)}) = y_a z_1^{f(a(1))} \cdots z_s^{f(a(s))}$ for $1 \leq a \leq r$ and $a(1), \ldots, a(s) \in \mathbf{Z}^U$.

2. Proof of Theorem 2. First, we reduce ourselves to the case of finitely generated torsion-free nilpotent groups:

If G is a finitely generated nilpotent-by-finite group, then, by Lemma 1.1, there exists an integer $p \geq 1$ such that G^p is nilpotent and torsion-free. We have $\widehat{G}^p = \widehat{G^p}$ according to [**9**, Lemma 3, p. 223].

Proposition 2.1 of [**6**] implies the existence of an integer $q \geq 1$ such that each element of G^p can be written $x = x_1^p \cdots x_q^p$ with $x_1, \ldots, x_q \in G$. The group G satisfies the positive sentence $(\forall u_1 \cdots \forall u_{q+1})(\exists v_1 \cdots \exists v_q)(u_1^p \cdots u_{q+1}^p = v_1^p \cdots v_q^p)$. This sentence is also true in $\widehat{G}$ since, by [**6**, Theorem 3.3], $\widehat{G}$ is an image of an elementary extension of G. So, the formula $\theta(x) = (\exists u_1 \cdots \exists u_q)(x = u_1^p \cdots u_q^p)$ defines G^p in G and $\widehat{G}^p$ in $\widehat{G}$.

To any existential sentence

$$\varphi = (\exists v_1 \cdots \exists v_n)\psi(v_1, \ldots, v_n),$$

where ψ is a quantifier-free formula, we associate the sentence

$$\bar{\varphi} = (\exists v_1 \cdots \exists v_n)(\theta(v_1) \wedge \cdots \wedge \theta(v_n) \wedge \psi(v_1, \ldots, v_n))$$

which is equivalent to an existential sentence. The sentence $\bar{\varphi}$ is false in G and true in $\widehat{G}$ as soon as φ is false in G^p and true in $\widehat{G}^p = \widehat{G^p}$.

From now on, we suppose G nilpotent and torsion-free. Then, Theorem 2 is proved through a series of lemmas:

LEMMA 2.1. *In G, there are elements x, y, z such that $[x,y] = z \neq 1$, $[x,z] = 1$ and $[y,z] = 1$.*

PROOF. As G is nilpotent and nonabelian,

$$Z_1(G) = \{x \in G \mid [x,y] = 1 \text{ for each } y \in G\}$$

is strictly contained in

$$Z_2(G) = \{x \in G \mid [x,y] \in Z_1(G) \text{ for each } y \in G\}.$$

For each element $x \in Z_2(G) - Z_1(G)$, there exists an element $y \in G$ such that $[x,y] \neq 1$. We have $[x,z] = 1$ and $[y,z] = 1$ for $z = [x,y]$.

LEMMA 2.2. *Let x, y, z be elements of G such that $[x,y] = z \neq 1$, $[x,z] = 1$ and $[y,z] = 1$. Denote by N the group which is obtained by equipping the set $\widehat{\mathbf{Z}}^3$ with the product $(a_1,b_1,c_1)(a_2,b_2,c_2) = (a_1+a_2, b_1+b_2, c_1+c_2-b_1a_2)$. Then, the map $(a,b,c) \to x^a y^b z^c$ is an injective homomorphism from N to $\widehat{G}$.*

PROOF. N can be identified with the profinite completion of the nilpotent group M which is obtained by equipping $\mathbf{Z}^3$ with the product $(a_1,b_1,c_1)(a_2,b_2,c_2) = (a_1+a_2, b_1+b_2, c_1+c_2-b_1a_2)$. The map $(a,b,c) \to x^a y^b z^c$ is a continuous homomorphism from N to $\widehat{G}$. The restriction of this map to M is an injective homomorphism from M to G. So, Lemma 2.2 follows from [**9**, Proposition 3, (iii), p. 222].

LEMMA 2.3. *For each set P of prime numbers, there exists an element $a \in \widehat{\mathbf{Z}}$ such that, for each integer $n \geq 1$, $a \in n\widehat{\mathbf{Z}}$ if and only if n has no divisor in P.*

PROOF. Consider, for each integer $n \geq 1$, the set E_n of all elements $x \in \widehat{\mathbf{Z}}$ such that, for each integer $m \leq n$, x belongs to $m\widehat{\mathbf{Z}}$ if and only if m has no divisor in P. The set E_n is nonempty since it contains the product of the integers $m \leq n$ which have no divisor in P. It is closed in $\widehat{\mathbf{Z}}$ as a—necessarily finite—union of classes modulo $n!\widehat{\mathbf{Z}}$.

So, $(E_n)_{n\in\mathbf{N}^*}$ is a decreasing sequence of nonempty closed subsets in the compact space $\widehat{\mathbf{Z}}$, and the intersection of this sequence is also nonempty. If a is an element of this intersection, then, for each integer $n \geq 1$, a belongs to $n\widehat{\mathbf{Z}}$ if and only if n has no divisor in P. This completes the proof of Lemma 2.3.

In a group, the equalities $[x,y] = 1$ and $[x,y] = z$ are respectively equivalent to the atomic formulas $xy = yx$ and $xy = yxz$. So, the following two lemmas imply the existence of existential sentences built up from the multiplication symbol which are false in G and true in $\widehat{G}$:

LEMMA 2.4. *For each integer $n \geq 1$, there exist elements $x_1, \ldots, x_{3n} \in \widehat{G}$ such that*

(1) $[x_i, x_{i+n}] = x_{i+2n} \neq 1$ *for* $1 \leq i \leq n$;
(2) $[x_i, x_j] = 1$ *for any integers* $1 \leq i \leq j \leq 3n$ *such that* $i \geq n+1$ *or* $j - i \neq n$.

PROOF. We consider elements $x, y, z \in G$ such that $[x,y] = z \neq 1$, $[x,z] = 1$ and $[y,z] = 1$, a partition $P = P_1 \cup \cdots \cup P_n$ of the set P of all prime numbers into n nonempty subsets and, for each integer $1 \leq i \leq n$, an element $a(i) \in \widehat{\mathbf{Z}}$ such that, for each integer $q \geq 1$, $a(i)$ belongs to $q\widehat{\mathbf{Z}}$ if and only if q has no prime divisor in P_i. We write $x_i = x^{a(i)}$, $x_{i+n} = y^{a(i)}$ and $x_{i+2n} = z^{a(i)^2}$ for each integer $1 \leq i \leq n$. Then, we use Lemma 2.2 to prove that $x_1, \ldots, x_{3n}$ satisfy properties (1) and (2) of Lemma 2.4.

For each integer $1 \leq i \leq n$, we have

$$[x_i, x_{i+n}] = [x^{a(i)}, y^{a(i)}] = z^{a(i)^2} = x_{i+2n} \neq 1.$$

For any integers $1 \leq i, j \leq n$ such that $i \neq j$, we have $a(i)a(j) = 0$ since $a(i)a(j)$ belongs to $q\widehat{\mathbf{Z}}$ for each integer $q \geq 1$; it follows

$$[x_i, x_{j+n}] = [x^{a(i)}, y^{a(j)}] = z^{a(i)a(j)} = 1.$$

Finally, for any integers $1 \leq i, j \leq n$, we have

$$[x_i, x_j] = [x^{a(i)}, x^{a(j)}] = 1, \quad [x_{i+n}, x_{j+n}] = [y^{a(i)}, y^{a(j)}] = 1,$$
$$[x_{i+2n}, x_{j+2n}] = [z^{a(i)}, z^{a(j)}] = 1, \quad [x_i, x_{j+2n}] = [x^{a(i)}, z^{a(j)}] = 1,$$
$$[x_{i+n}, x_{j+2n}] = [y^{a(i)}, z^{a(j)}] = 1.$$

DEFINITION. For each finitely generated nilpotent group M, there exists a series of subgroups $\{1\} = M_0 \subset M_1 \subset \cdots \subset M_n = M$ with M_{i-1} normal in M_i and M_i/M_{i-1} cyclic for $1 \leq i \leq n$. The number of integers i such that M_i/M_{i-1} is infinite does not depend on the choice of the series. It is called *Hirsch number* of M, according to [**9**, p. 16].

LEMMA 2.5. *For each integer n which is larger than the Hirsch number of G, there are no elements $x_1, \ldots, x_{3n} \in G$ which satisfy properties* (1) *and* (2) *of Lemma* 2.4.

PROOF. Let us consider elements $x_1, \ldots, x_{3n} \in G$ which satisfy these properties. The subgroup of G which is generated by $x_1, \ldots, x_n$ is abelian. For any integers $a(1), \ldots, a(n) \in \mathbf{Z}$, we have $x_1^{a(1)} \cdots x_n^{a(n)} = 1$ if and only if $a(1) = \cdots = a(n) = 0$. In fact, if $x_1^{a(1)} \cdots x_n^{a(n)}$ is equal to 1, then, for each integer $1 \leq i \leq n$, we have $1 = [x_1^{a(1)} \cdots x_n^{a(n)}, x_{i+n}] = x_{i+2n}^{a(i)}$ and, therefore, $a(i) = 0$. So, $x_1, \ldots, x_n$ generate a free abelian subgroup which has rank n as a $\mathbf{Z}$-module. According to [**9**, p. 16], this is impossible if n is larger than the Hirsch number of G.

3. Proof of the proposition. The groups M, N are elementarily equivalent according to [**1**, Corollary] and [**6**, Theorem 5.5]. Theorem 6.1.15 of [**2**] implies the existence of an ultrafilter U such that M^U and N^U are isomorphic. We have $G^U = \langle M^U \times M^U, y;\ y^2 = 1,\ y^{-1}(u,v)y = (v,u)$ for any $u, v \in M^U\rangle$ and $H^U = \langle N^U \times N^U, z;\ z^2 = 1,\ z^{-1}(u,v)z = (v,u)$ for any $u, v \in N^U\rangle$. To any isomorphism $\varphi\colon M^U \to N^U$, we can associate an isomorphism $\Phi\colon G^U \to H^U$ defined by $\Phi(y) = z$ and $\Phi(u,v) = (\varphi(u), \varphi(v))$ for any $u, v \in M^U$. Consequently, the elementary equivalence of G and H follows from [**2**, Theorem 4.1.9].

It remains to prove that $G \times \mathbf{Z}$ and $H \times \mathbf{Z}$ are not isomorphic. For this part of the proof, we write $g(u,v) = (v,u)$ for any $u, v \in M$ and $h(u,v) = (v,u)$ for any $u, v \in N$. If $x_1, \ldots, x_n$ are elements of a group A, we denote by $\langle x_1, \ldots, x_n\rangle$ the subgroup of A which is generated by $x_1, \ldots, x_n$.

LEMMA 3.1. *We have* $[G,G] = \langle (b, b^{-1}),\ (a, a^{-1}),\ (a^5, 1)\rangle$ *and* $[H,H] = \langle (d, d^{-1}),\ (c, c^{-1}),\ (c^5, 1)\rangle$.

PROOF OF LEMMA 3.1 (FOR G). The subgroup $[G,G]$ is generated by the elements:

$$[u,v] \quad \text{for } u, v \in M \times M,$$

$$\begin{aligned}[u, yv] &= u^{-1}v^{-1}y^{-1}uyv = u^{-1}v^{-1}g(u)v = u^{-1}g(u)g(u)^{-1}v^{-1}g(u)v \\ &= (u^{-1}g(u))[g(u), v] \quad \text{for } u, v \in M \times M,\end{aligned}$$

$$\begin{aligned}[yu, yv] &= u^{-1}y^{-1}v^{-1}y^{-1}yuyv = u^{-1}y^{-1}v^{-1}uyv = u^{-1}g(v^{-1}u)v \\ &= u^{-1}g(v)^{-1}g(u)v = u^{-1}g(u)g(u)^{-1}g(v)^{-1}g(u)g(v)g(v)^{-1}v \\ &= (u^{-1}g(u))[g(u), g(v)](v^{-1}g(v))^{-1} \quad \text{for } u, v \in M \times M.\end{aligned}$$

So, $[G,G]$ is generated by $[M \times M, M \times M] = [M,M] \times [M,M] = \langle a^5 \rangle \times \langle a^5 \rangle$ and the elements $x^{-1}g(x)$ for $x \in M \times M$. Moreover, we have

$$(u,v)^{-1}g(u,v) = (u^{-1},v^{-1})(v,u) = (u^{-1}v, v^{-1}u) = (u^{-1}v, (u^{-1}v)^{-1})$$

for any $u, v \in M$ and $(u, u^{-1}) = (1,u)^{-1}g(1,u)$ for each $u \in M$. So, an element of G can be written $x^{-1}g(x)$ with $x \in M \times M$ if and only if it can be put in the form (u, u^{-1}) with $u \in M$.

PROOF OF THE PROPOSITION (END). $K = \langle (a, a^{-1}), (a^5, 1) \rangle$ (respectively $L = \langle (c, c^{-1}), (c^5, 1) \rangle$) is the set of all elements $x \in [G,G]$ (respectively $x \in [H,H]$) such that $x^{25} = 1$; $[G,G]/K$ and $[H,H]/L$ are isomorphic to $\mathbf{Z}$. If f is an isomorphism from $G \times \mathbf{Z}$ to $H \times \mathbf{Z}$, then the restriction of f to $[G,G] = [G \times \mathbf{Z}, G \times \mathbf{Z}]$ is an isomorphism from $[G,G]$ to $[H,H] = [H \times \mathbf{Z}, H \times \mathbf{Z}]$; the restriction of f to K is an isomorphism from K to L and f induces an isomorphism from $[G,G]/K$ to $[H,H]/L$. So, we have $f(b,b^{-1}) = (du, d^{-1}v)$ or $f(b,b^{-1}) = (d^{-1}u, dv)$ with $u, v \in \langle c \rangle$.

Moreover, we have $(a,1)^5 \neq 1$ and $(a,1)^{25} = 1$, whence $f(a,1)^5 \neq 1$ and $f(a,1)^{25} = 1$, and therefore $f(a,1) = (c^m, c^n)$ with m or n not divisible by 5. The equality $(b,b^{-1})^{-1}(a,1)(b,b^{-1}) = (a,1)^6$ implies $f(b,b^{-1})^{-1}(c^m,c^n)f(b,b^{-1}) = (c^{6m}, c^{6n})$. The hypotheses $f(b,b^{-1}) = (du, d^{-1}v)$ and $f(b,b^{-1}) = (d^{-1}u, dv)$ with $u, v \in \langle c \rangle$ respectively imply

$$\begin{aligned}(c^{6m}, c^{6n}) &= (du, d^{-1}v)^{-1}(c^m, c^n)(du, d^{-1}v) = (u^{-1}d^{-1}c^m\, du, v^{-1}dc^n d^{-1}v) \\ &= (u^{-1}c^{11m}u, v^{-1}c^{16n}v) = (c^{11m}, c^{16n})\end{aligned}$$

and

$$\begin{aligned}(c^{6m}, c^{6n}) &= (d^{-1}u, dv)^{-1}(c^m, c^n)(d^{-1}u, dv) = (u^{-1}dc^m d^{-1}u, v^{-1}d^{-1}c^n dv) \\ &= (u^{-1}c^{16m}u, v^{-1}c^{11n}v) = (c^{16m}, c^{11n}),\end{aligned}$$

whence a contradiction in both cases since m or n is not divisible by 5.

NOTE ADDED IN PROOF (May 10, 1988). Since the completion of this manuscript, we have obtained some generalizations which will appear in Archiv der Mathematik under the title *Elementary equivalence of a polycyclic-by-finite group and its profinite completion.* We prove that Theorem 2 is true for polycyclic-by-finite groups and not only for finitely generated nilpotent-by-finite groups. It follows that a polycyclic-by-finite group is elementarily equivalent to its profinite completion if and only if it is abelian-by-finite.

REFERENCES

1. G. Baumslag, *Residually finite groups with the same finite images*, Compositio Math. **29** (1974), 249–252.
2. C. C. Chang and H. J. Keisler, *Model theory*, Studies in Logic no. 73, North-Holland, Amsterdam, 1973.
3. R. Hirshon, *The cancellation of an infinite cyclic group in direct products*, Arch. Math. **26** (1975), 134–138.
4. ____, *Some cancellation theorems with applications to nilpotent groups*, J. Austral. Math. Soc. Ser. A **23** (1977), 147–165.
5. ____, *The equivalence of* $\times^t C \cong \times^t D$ *and* $J \times C \cong J \times D$, Trans. Amer. Math. Soc. **249** (1979), 331–340.

6. F. Oger, *Equivalence élémentaire entre groupes finis-par-abéliens de type fini*, Comment. Math. Helv. **57** (1982), 469–480.
7. ——, *The model theory of finitely generated finite-by-abelian groups*, J. Symbolic Logic **49** (1984), 1115–1124.
8. D. Robinson, *Finiteness conditions and generalized soluble groups*, t. 1, Ergeb. Math. Grenzgeb., vol. 62, Springer-Verlag, Berlin and New York, 1972.
9. D. Segal, *Polycyclic groups*, Cambridge Univ. Press, Cambridge, 1983.
10. R. B. Warfield, Jr., *Nilpotent groups*, Lecture Notes in Math., vol. 513, Springer-Verlag, Berlin and New York, 1976.
11. ——, *Genus and cancellation for groups with finite commutator subgroup*, J. Pure Appl. Algebra **6** (1975), 125–132.

DÉPARTEMENT DE MATHÉMATIQUES, UNIVERSITÉ PARIS VII, 75.251 PARIS CEDEX 05, FRANCE