ELEMENTARY EQUIVALENCE OF PROFINITE GROUPS

by

Moshe Jarden, Tel Aviv University*

and

Alexander Lubotzky, The Hebrew University of Jerusalem**

Dedicated to Dan Segal on the occasion of his 60th birthday

Abstract. There are many examples of non-isomorphic pairs of finitely generated abstract groups that are elementarily equivalent. We show that the situation in the category of profinite groups is different: If two finitely generated profinite groups are elementarily equivalent (as abstract groups), then they are isomorphic. The proof applies a result of Nikolov and Segal which in turn relies on the classification of the finite simple groups. Our result does not hold any more if the profinite groups are not finitely generated. We give concrete examples of non-isomorphic profinite groups which are elementarily equivalent.

MR Classification: 12E30

Directory: \Jarden\Diary\JL

3 June, 2008

* Supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation.

** Supported by the ISF and the Landau Center for Analysis at the Hebrew University of Jerusalem.

Introduction

Let $\mathcal{L}$(group) be the first order language of group theory. One says that groups G and H are **elementarily equivalent** and writes $G \equiv H$ if each sentence of $\mathcal{L}$(group) which holds in one of these groups holds also the other one. There are many examples of pairs of elementarily equivalent groups which are not isomorphic. For example, the group $\mathbb{Z}$ is elementarily equivalent to every nonprincipal ultrapower of it although it is not isomorphic to it. Less trivial examples are given by the following result: If G and H are groups satisfying $G \times \mathbb{Z} \cong H \times \mathbb{Z}$, then $G \equiv H$ [Oge91] (see [Hir69] for an example of non-isomorphic groups G and H satisfying $G \times \mathbb{Z} \cong H \times \mathbb{Z}$.) More generally, Nies points out in [Nie03, p. 288] that for every infinite finitely generated abstract group G there exists a countable group H such that $G \equiv H$ but $G \ncong H$. See also related results of Zil'ber in [Zil71] and Sabbagh and Wilson in [SaW91]. One of the consequences of the solution of Tarski's problem is that all finitely generated free nonabelian groups are elementarily equivalent [Sel03, Thm. 3]. We refer the reader to [FrJ05, Chap. 7] for notions and results in logic and model theory that we use here.

The goal of this note is to show that the situation is quite different in the category of profinite groups. Note that in this category "homomorphism" means "continuous homomorphism" and we say that a profinite group G is **finitely generated** if G has a dense finitely generated abstract subgroup; more generally we use the convention of [FrJ05, Chaps. 1, 17, and 22] for profinite groups. However, whenever we say that two profinite groups are elementarily equivalent, we mean that they are elementarily equivalent as abstract groups, i.e. in the sense defined in the preceding paragraph.

THEOREM A: *Let G and H be elementarily equivalent profinite groups. If one of the groups is finitely generated, then they are isomorphic.*

The proof of Theorem A uses tools developed by Nikolov and Segal in their proof of the following deep result: Every abstract subgroup H of a finitely generated profinite group G with $(G : H) < \infty$ is open [NiS03 or NiS07]. Among others, that result relies on the classification of finite simple groups.

Theorem A does not remain true if neither of the groups G and H is finitely

generated. An example to this situation appears in our second main result:

THEOREM B: *Every two free pro-p Abelian groups of infinite rank are elementarily equivalent.*

The proof of Theorem B in Section 2 is based on the fact that every closed subgroup of a free Abelian pro-p group F is again a free Abelian pro-p group. An essential ingredient in the proof is a separation property saying that if $\mathrm{rank}(F) = \infty$ and $x_1, \ldots, x_n \in F$, then F can be presented as a direct sum $F = F_0 \oplus F_1$ such that $\mathrm{rank}(F_0) = \aleph_0$, $\mathrm{rank}(F_1) \geq \aleph_0$, and $x_1, \ldots, x_n \in F_0$.

The referee pointed out to us that Theorem B follows also from a deep result of Szmielew [Szm] that gives a general criterion for Abelian groups to be elementarily equivalent. This approach is explained in Section 3.

We thank the referee for calling our attenion to the work of Smielew as well as for mentioning the results of Nies, Zil'ber, and Sabbagh-Wilson.

1. Finitely Generated Profinite Groups

Profinite groups do not behave well under the usual model theoretic constructions, for example under ultra products. However, we may still speak in $\mathcal{L}$(group) about finite quotients of finitely generated profinite groups. The first steps toward this goal is done in the following observation:

LEMMA 1.1: *For each positive integer n and each finite group A of order at most n there exists a sentence θ of $\mathcal{L}$(group) such that for every group G of order at most n the sentence θ holds in G if and only if A is a quotient of G.*

Proof: It suffices to prove that for every positive integer n and for every group A of order d dividing n there exists a sentence θ of $\mathcal{L}$(group) with the following property: for every group G of order n the sentence θ holds in G if and only if G has a normal subgroup M such that $G/M \cong A$.

We set $m = \frac{n}{d}$ and choose an injective map α: $\{1, \ldots, d\} \to A$. Then the desired

sentence θ will be the following one:

$$(\exists x_1)\cdots(\exists x_m)(\exists g_1)\cdots(\exists g_d)\Big[[\bigwedge_{i\neq j} x_i \neq x_j]\wedge\big[\bigwedge_{i,j=1}^{m}\bigvee_{k=1}^{m} x_ix_j = x_k\big]$$
$$\wedge\big[(\forall g)\bigwedge_{i=1}^{m}\bigvee_{j=1}^{m} g^{-1}x_ig = x_j\big]$$
$$\wedge(\forall g)[\bigvee_{i=1}^{d}\bigvee_{j=1}^{m} g = g_ix_j]\wedge\big[\bigwedge_{i\neq j}\bigwedge_{k=1}^{m} g_i \neq g_jx_k\big]$$
$$\wedge\big[\bigwedge_{i,j=1}^{d}\bigvee_{k=1}^{m} g_ig_j = g_{\alpha^{-1}(\alpha(i)\alpha(j))}x_k\big]\Big]$$

The part of θ included in the first two brackets states that the subset $M = \{x_1, \ldots, x_m\}$ of G is a subgroup of order m, the part in the third brackets says that M is normal, the third line means that $G = \bigcup\!\!\!\cdot_{i=1}^{d} g_iM$, and finally the content of the fourth line is that the map $g_iM \mapsto \alpha(i)$ is an isomorphism $G/M \cong A$. ∎

Let $w(\mathbf{x})$ be a word in the sense of group theory in the variables $\mathbf{x} = (x_1, \ldots, x_m)$ [FrJ05, Sec. 17.5]. For each group G let $w(G)$ be the subgroup generated (in the abstract sense) by the elements $w(\mathbf{g})$ with $\mathbf{g} \in G^m$. The identity $w(g_1, \ldots, g_m)^x = w(g_1^x, \ldots, g_m^x)$ in G implies that $w(G)$ is normal in G. Every element of G of the form $w(g_1, \ldots, g_m)^{\pm 1}$ is said to be a w**-value**. We write $\mathrm{length}_w(G) \leq r$ if each element of $w(G)$ is a product of r w-values. We say that w is a d**-locally finite word** if each group G which is generated by d elements and satisfies $w(G) = 1$ is finite.

LEMMA 1.2: *Let $w(x_1, \ldots, x_d)$ be a word and r a positive integer. Then there exists a map*

$$\varphi(y_1, \ldots, y_n) \mapsto \varphi'(y_1, \ldots, y_n)$$

from the set of all formulas in $\mathcal{L}$(group) into itself such that for each group G with $\mathrm{length}_w(G) \leq r$ and for all $y_1, \ldots, y_n \in G$ we have:

$$(1) \qquad G \models \varphi'(y_1, \ldots, y_n) \Longleftrightarrow G/w(G) \models \varphi(y_1w(G), \ldots, y_nw(G))$$

Proof: Given a word $u(y_1, \ldots, y_n)$, we map the formula $u(y_1, \ldots, y_n) = 1$ onto the

formula

$$(2) \qquad (\exists \mathbf{g}_1)\cdots(\exists \mathbf{g}_r) \bigvee_{\boldsymbol{\varepsilon}\in\{\pm 1\}^r} [u(y_1,\ldots,y_n) = w(\mathbf{g}_1)^{\varepsilon_1}\cdots w(\mathbf{g}_r)^{\varepsilon_r}]$$

where $\exists \mathbf{g}_i$ is an abbreviation for $(\exists g_{i1})\cdots(\exists g_{im})$ and $\boldsymbol{\varepsilon} = (\varepsilon_1,\ldots,\varepsilon_r)$. Indeed, if G is a group with $\mathrm{length}_w(G) \le r$ and $y_1,\ldots,y_n \in G$, then (2) holds in G if and only if $u(y_1,\ldots,y_n) \in w(G)$ if and only if $u(y_1 w(G),\ldots,y_n w(G)) = 1$ in $G/w(G)$.

We continue the definition of $'$ by induction on the structure of formulas letting $'$ commute with negation, disjunction, and existential quantification. ∎

The following insight precedes Theorem 1.2 of [NiS03] and is attributed to Oates-Powell. The reader may also find a short proof in [FrJ05, p. 514].

LEMMA 1.3: *For every finite group A generated by d elements there exists a d-locally finite word w such that $w(A) = 1$.*

In contrast, the following result of Nikolov-Segal is deep. Among others it applies the classification of finite simple groups.

PROPOSITION 1.4 ([NiS03, Thm. 2.1]): *For each d-locally finite word $w(x_1,\ldots,x_m)$ there exists a positive integer r such that $\mathrm{length}_w(G) \le r$ for each finite group G generated by d elements.*

If G is a profinite group and w is a word, then $w(G)$ may be properly contained in its closure. However, if $\mathrm{length}_w(G) < \infty$, the two groups coincide. This is the content of the following lemma.

LEMMA 1.5: *If $w(x_1,\ldots,x_m)$ is a word, r is a positive integer, and G is a profinite group with $\mathrm{length}_w(G) \le r$, then $w(G)$ is closed in G.*

Proof: For all $\varepsilon_1,\ldots,\varepsilon_r \in \{\pm 1\}$ the map $(\mathbf{g}_1,\ldots,\mathbf{g}_r) \mapsto w(\mathbf{g}_1)^{\varepsilon_1}\cdots w(\mathbf{g}_r)^{\varepsilon_r}$ from $(G^m)^r$ into G is continuous. Hence, its image in G is closed. Thus, $w(G)$ is a union of finitely many closed sets, so $w(G)$ is closed. ∎

If w and r are as in Proposition 1.4 and G is a profinite group generated by d elements, then each finite quotient $\bar{G}$ of G is generated by d elements. Hence, by

Proposition 1.4, each element of $w(\bar{G})$ is a product of r w-values of $\bar{G}$. A compactness argument proves that each element of $w(G)$ is a product of r w-values of G, that is $\mathrm{length}_w(G) \leq r$.

Now consider generators $x_1, \ldots, x_d$ of G as a profinite group. Denote the abstract subgroup of G generated by $x_1, \ldots, x_d$ by G_0. Then, $w(G_0) \triangleleft G_0$, $w(G_0/w(G_0)) = 1$, and $G_0/w(G_0)$ is generated as an abstract group by d elements, hence $G_0/w(G_0)$ is finite. Therefore, $(G_0 w(G) : w(G)) \leq (G_0 : w(G_0)) < \infty$, so $G_0 w(G) = \bigcup_{i=1}^{n} g_i w(G)$ for some positive integer n and elements $g_1, \ldots, g_n \in G$. Since by Lemma 1.5 $w(G)$ is closed, also $G_0 w(G)$ is closed. Since G_0 is dense in G, we conclude that $G_0 w(G) = G$. It follows that $(G : w(G)) < \infty$, so $w(G)$ is open.

These arguments prove the following result:

PROPOSITION 1.6: *For each d-locally finite word $w(x_1, \ldots, x_m)$ there exists a positive integer r such that for each profinite group G generated by d elements,* $\mathrm{length}_w(G) \leq r$. *Moreover, $w(G)$ is an open normal subgroup of G.*

We are now in a position to prove Theorem A. Let $\mathrm{Im}(G)$ be the set of finite quotients (up to an isomorphism).

THEOREM 1.7: *Let G and H be elementarily equivalent profinite groups. Suppose one of them is finitely generated. Then $G \cong H$.*

Proof: Suppose for example G is finitely generated. In addition we assume that $G \ncong H$. By [FrJ05, Prop. 16.10.7], $\mathrm{Im}(G) \neq \mathrm{Im}(H)$. Hence, $\mathrm{Im}(H) \not\subseteq \mathrm{Im}(G)$ or $\mathrm{Im}(H) \subset \mathrm{Im}(G)$ (we use $\subset$ for proper inclusions). In the latter case $\mathrm{Im}(G) \not\subseteq \mathrm{Im}(H)$ and H is a quotient of G, in particular H is finitely generated. Thus, it suffices to deal with the case where $\mathrm{Im}(H) \not\subseteq \mathrm{Im}(G)$, that is H has a finite quotient A that is not a quotient of G.

Let d be a positive integer such that both G and A are generated as profinite groups by d elements. Lemma 1.3 gives a d-locally finite word $w(x_1, \ldots, x_m)$ with $w(A) = 1$. Proposition 1.6 gives a positive integer r such that $\mathrm{length}_w(G) \leq r$ and $w(G)$ is open and normal in G.

If we knew that also H is generated by d elements, we could derive the same conclusion for H from Proposition 1.6. Nevertheless, since at this point of the proof

we do not know that $\mathrm{rank}(H) \leq d$, we prove the properties of H using the assumption $H \equiv G$.

Claim A: $\mathrm{length}_w(H) \leq r$. Indeed let $s \geq r$ be a positive integer. Then for all $\mathbf{g}_1, \ldots, \mathbf{g}_s \in G^m$ and all $\varepsilon_1, \ldots, \varepsilon_s \in \{\pm 1\}$ there exist $\mathbf{x}_1, \ldots, \mathbf{x}_r \in G^m$ and $\delta_1, \ldots, \delta_r \in \{\pm 1\}$ such that $w(\mathbf{g}_1)^{\varepsilon_1} \cdots w(\mathbf{g}_s)^{\varepsilon_s} = w(\mathbf{x}_1)^{\delta_1} \cdots w(\mathbf{x}_r)^{\delta_r}$. Since $H \equiv G$, the same statement holds for H. Thus, each element of $w(H)$ has the form $w(\mathbf{h}_1)^{\varepsilon_1} \cdots w(\mathbf{h}_r)^{\varepsilon_r}$ for some $\mathbf{h}_1, \ldots, \mathbf{h}_r \in H^m$ and $\varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\}$. In other words, $\mathrm{length}_w(H) \leq r$, as claimed.

Claim B: *$w(H)$ is open in H; moreover, $(H : w(H)) = (G : w(G))$.* Indeed, by Claim A and Lemma 1.5, $w(H)$ is closed in H. Hence, it suffices to prove the equality of the indices. To this end observe that $n = (G : w(G)) < \infty$. Hence, there are $g_1, \ldots, g_n$ with $G = \bigcup_{i=1}^{n} g_i w(G)$. In other words, each element of G belongs to exactly one of the cosets $g_i w(G)$. Since $\mathrm{length}_w(G) \leq r$, this is an elementary statement θ on G. It follows from $G \equiv H$ that θ holds in H. Since, by Claim A, $\mathrm{length}_w(H) \leq r$, we conclude that $(H : w(H)) = n$.

End of Proof: By the beginning of the proof, H has an open normal subgroup N with $H/N \cong A$. By the choice of w, $w(H/N) = w(A) = 1$. The identity

$$w(h_1 N, \ldots, h_m N) = w(h_1, \ldots, h_m) N$$

therefore implies that $w(H) \leq N$. Hence, A is a quotient of the finite group $H/w(H)$. On the other hand, by assumption, A is not a quotient of the finite group $G/w(G)$.

Since by Claim B, $|G/w(G)| = |H/w(H)|$, Lemma 1.1 gives a sentence θ of $\mathcal{L}(\mathrm{group})$ that holds in $H/w(H)$ but not in $G/w(G)$. By Claim A and Lemma 1.2 it is possible to translate θ to a sentence of $\mathcal{L}(\mathrm{group})$ that holds in H but not in G. This contradiction to the elementary equivalence of G and H proves that $G \cong H$. ∎

2. Free pro-p Abelian groups of Infinite Rank

We give examples of pairs of elementarily equivalent profinite groups which are not isomorphic. More precisely, we prove that all free pro-p Abelian groups of infinite rank

are elementarily equivalent to each other. Naturally, if their ranks are unequal they are not isomorphic. Here, the **rank** of a profinite group G is the cardinality of any set of generators that converge to 1. If $\mathrm{rank}(G) = \infty$, then $\mathrm{rank}(G)$ is also the cardinality of the set of all open normal subgroups of G [FrJ05, Prop. 17.1.2].

We work exclusively in the category $\mathrm{AbPro}(p)$ of Abelian pro-p groups (written additively). The free group of rank m in $\mathrm{AbPro}(p)$ is just $\mathbb{Z}_p^m$. This group is torsion-free. Conversely, each torsion-free abelian pro-p group is isomorphic to $\mathbb{Z}_p^m$ for some cardinal number m [RiZ00, Them. 4.3.3]. Hence, each closed subgroup of a free Abelian pro-p group is a free Abelian pro-p group. This implies that if two closed subgroups of a free Abelian pro-p groups have the same rank, they are isomorphic.

Every partition $X = Y \cup Z$ of a basis X of a free Abelian pro-p group F defines a decomposition $F = G \oplus H$ into a direct sum of the closed subgroups generated by X and Y, respectively. In particular, if $\mathrm{rank}(F) \geq \aleph_0$, then $F = F_0 \oplus F_1$ with $\mathrm{rank}(F_0) = \aleph_0$ and $\mathrm{rank}(F_1) \geq \aleph_0$.

LEMMA 2.1: *Let F be an Abelian pro-p group and M a closed subgroup containing pF. Then F has a closed subgroup H such that $H + pF = M$ and $H \cap pF = pH$.*

Proof: Denote the collection of all closed subgroups H of F with $H + pF = M$ by $\mathcal{H}$. In particular, $M \in \mathcal{H}$. If $\{G_i \mid i \in I\}$ is a descending chain in $\mathcal{H}$ (that is, one of every two groups in $\mathcal{H}$ contains the other) and $G = \bigcap_{i \in I} G_i$, then $G + pF = \bigcap_{i \in I}(G_i + pF) = M$ [FrJ05, Lemma 1.2.2(b)]. By Zorn's lemma, $\mathcal{H}$ has a minimal element H, that is H properly contains no group belonging to $\mathcal{H}$.

By definition, $pH \leq H \cap pF$. Assume toward contradiction that $pH < H \cap pF$. Then $(H \cap pF)/pH$ is a nontrivial closed subgroup of H/pH. The latter group is isomorphic to $\mathbb{F}_p^h$, where $h = \mathrm{rank}(H)$ [FrJ05, Lemma 22.7.4]. Hence, H has an open subgroup H_0 of index p such that $(H \cap pF : H_0 \cap pF) = p$. That group satisfies $H_0 + (H \cap pF) = H$, so $H_0 + pF = M$. This contradiction to the minimality of H proves that $H \cap pF = pH$. ∎

PROPOSITION 2.2: *Let F be a free Abelian pro-p group and G a closed subgroup. Then G is a direct summand of F if and only if $G \cap pF = pG$.*

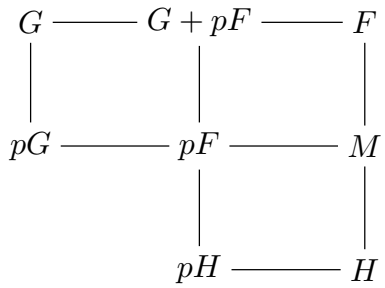
Proof: First suppose $F = G \oplus H$, where G and H are closed subgroups of F. Then $pG \leq pF$. On the other hand, let G_0 be an open normal subgroup of G of index p. Adding the quotient map $G \to G/G_0$ to the trivial map $H \to G/G_0$ gives an epimorphism $F \to G/G_0$ with kernel F_0 such that $G \cap F_0 = G_0$. In particular, $pF \leq F_0$, so $G \cap pF \leq G_0$. Since pG is the intersection of all those G_0, we have $G \cap pF \leq pG$. Combining this conclusion with our first one, we get $G \cap pF = pG$.

Conversely, suppose $G \cap pF = pG$. By [FrJ05, Lemma 22.7.4], $F/pF \cong \mathbb{F}_p^m$ with $m = \operatorname{rank}(F)$. Hence, by [FrJ05, Lemma 22.7.2], F has a closed subgroup M containing pF such that $F/pF = (G + pF/pF) \oplus M/pF$. In other words, $G + pF + M = F$ and $(G + pF) \cap M = pF$.

By Lemma 2.1, F has a closed subgroup H such that $pF \cap H = pH$ and $pF + H = M$. Hence, $G + H + pF = G + M + pF = F$. Since pF is the Frattini subgroup of F [FrJ05, Lemma 22.7.4],

$$G + H = F. \tag{1}$$

The groups appearing in the last two paragraphs fit into the following diagram:



By the preceding two paragraphs, $G \cap H \leq (G + pF) \cap M = pF$. Hence, $G \cap H \leq G \cap pF = pG$ and $G \cap H \leq pF \cap H = pH$. Thus, for each $x \in G \cap H$ there are $g \in G$ and $h \in H$ such that $pg = x = ph$. Since F is torsion-free, $g = h$. Therefore, $G \cap H \leq p(G \cap H)$. Proceeding inductively, we find that $G \cap H \leq p^n(G \cap H)$ for all n. Since F is an Abelian pro-p group, this implies that $G \cap H = 0$. Together with (1) we conclude that $F = G \oplus H$, as desired. ∎

PROPOSITION 2.3: *Let F be a free Abelian pro-p group of infinite rank.*

(a) *For all* $x_1, \ldots, x_n \in F$ *there exists a direct decomposition* $F = F_0 \oplus F_1$ *such that* $\operatorname{rank}(F_0) = \aleph_0$, $\operatorname{rank}(F_1) \geq \aleph_0$, *and* $x_1, \ldots, x_n \in F_0$.

(b) *For each direct decomposition* $F = G \oplus E$ *with* $\operatorname{rank}(G) = \aleph_0$ *and* $\operatorname{rank}(E) \geq \aleph_0$ *and for each* $y \in F$, *the profinite group* F *has a direct summand* H *of rank* $\aleph_0$ *that contains* $\langle G, y\rangle$ *and has a direct decomposition* $H = G \oplus D$ *with* $\operatorname{rank}(D) = \aleph_0$.

Proof of (a): We start with the case where $n = 1$ and $x_1 = x$. Since F is an Abelian pro-p group, $\bigcap_{k=0}^{\infty} p^k F = 0$. Hence, there exist $k \geq 0$ and $y \in F$ with $x = p^k y$ and $y \notin pF$. Let A be the closed subgroup of F generated by y. If $a \in A \cap pF$, then $a = \alpha y$ for some $\alpha \in \mathbb{Z}_p$ and $a = pf$ for some $f \in F$. If $\alpha \in \mathbb{Z}_p^{\times}$, then $y = \alpha^{-1} pf \in pF$. It follows from this contradiction that $\alpha \in p\mathbb{Z}_p$, so $a \in pA$. Thus, $A \cap pF = pA$. By Proposition 2.2, F has a closed subgroup B with $F = A \oplus B$. Since $\operatorname{rank}(A) = 1$, we have $\operatorname{rank}(B) \geq \aleph_0$. Hence, $B = B_0 \oplus B_1$ with $\operatorname{rank}(B_0) = \aleph_0$ and $\operatorname{rank}(B_1) \geq \aleph_0$. Set $F_0 = A \oplus B_0$ and $F_1 = B_1$. Then $F = F_0 \oplus F_1$, $\operatorname{rank}(F_0) = \aleph_0$, $\operatorname{rank}(F_1) \geq \aleph_0$, and $x \in F_0$.

Now suppose $n \geq 2$. An induction hypothesis gives a direct decomposition $F = A_0 \oplus A_1$ such that $\operatorname{rank}(A_0) = \aleph_0$, $\operatorname{rank}(A_1) \geq \aleph_0$, and $x_1, \ldots, x_{n-1} \in A_0$. We write $x_n = x_{n0} + x_{n1}$ with $x_{n0} \in A_0$ and $x_{n1} \in A_1$. The preceding paragraph gives a direct decomposition $A_1 = A_{10} \oplus A_{11}$ such that $\operatorname{rank}(A_{10}) = \aleph_0$, $\operatorname{rank}(A_{11}) \geq \aleph_0$, and $x_{n1} \in A_{10}$. Set $F_0 = A_0 \oplus A_{10}$ and $F_1 = A_{11}$. Then $\operatorname{rank}(F_0) = \aleph_0$, $\operatorname{rank}(F_1) \geq \aleph_0$, and $x_1, \ldots, x_n \in F_0$, as desired.

Proof of (b): By assumption $y = g + e$ with $g \in G$ and $e \in E$. By (a) there exists a direct decomposition $E = D \oplus D'$ such that $\operatorname{rank}(D) = \aleph_0$, $\operatorname{rank}(D') \geq \aleph_0$, and $e \in D$. We set $H = G \oplus D$ to get $\operatorname{rank}(H) = \aleph_0$, $F = H \oplus D'$, $G \leq H$, and $y = g + e \in G + D = H$, as desired. ∎

PROPOSITION 2.4: *Let* F *be a free Abelian pro-*p *group. Then for each free decomposition* $F = G \oplus E$ *with* $\operatorname{rank}(G) = \aleph_0$ *and* $\operatorname{rank}(E) \geq \aleph_0$, *for all* $x_1, \ldots, x_n \in G$, *and for each* $y \in F$ *the profinite group* F *has a direct summand* H *of rank* $\aleph_0$ *that contains* $\langle G, y\rangle$ *and there exists an isomorphism* $\alpha\colon H \to G$ *that fixes* $x_1, \ldots, x_n$.

Proof: Proposition 2.3(a) gives a direct decomposition $G = G_0 \oplus G_1$ with $\operatorname{rank}(G_0) =$

$\aleph_0$, $\mathrm{rank}(G_1) = \aleph_0$, and $x_1, \ldots, x_n \in G_0$. Proposition 2.3(b) supplies direct decompositions $F = H \oplus E'$ and $H = G \oplus D$ such that $y \in H$ and $\mathrm{rank}(D) = \aleph_0$. Thus, $\mathrm{rank}(G_1 \oplus D) = \aleph_0$ and $H = G_0 \oplus (G_1 \oplus D)$. Therefore, there exists an isomorphism α: $H \to G$ whose restriction to G_0 is the identity map and which maps $G_1 \oplus D$ onto G_1. In particular, $\alpha(x_i) = x_i$ for $i = 1, \ldots, n$. ∎

We are now ready to prove Theorem B of the introduction.

THEOREM 2.5: *For all infinite cardinals l and m the free Abelian pro-p groups $\mathbb{Z}_p^l$ and $\mathbb{Z}_p^m$ are elementarily equivalent.*

Proof: It suffices to consider the case where $l = \aleph_0$ and $m > \aleph_0$. Each sentence θ of $\mathcal{L}(\mathrm{group})$ is logically equivalent to a sentence of the form

$$(Q_1 X_1) \cdots (Q_n X_n) \varphi_0(X_1, \ldots, X_n),$$

where each Q_i is either the existential quantifier $\exists$ or the universal quantifier $\forall$ and $\varphi_0(X_1, \ldots, X_n)$ is a quantifier free formula of the form

$$\bigvee_{i \in I} \bigwedge_{j \in J} u_{ij}(X_1, \ldots, X_n) = 1 \wedge v_{ij}(X_1, \ldots, X_n) \neq 1,$$

where I and J are finite sets and u_{ij}, v_{ij} are words in $X_1, \ldots, X_n$.

Set $F = \mathbb{Z}_p^m$ and notice that if $x_1, \ldots, x_n \in F$ and $F \models \varphi_0(x_1, \ldots, x_n)$, then $G \models \varphi_0(x_1, \ldots, x_n)$ for each closed subgroup G of F that contains $x_1, \ldots, x_n$. Indeed, the truth of $\varphi_0(x_1, \ldots, x_n)$ in G depends only on the multiplication laws in F and the restriction of the latter to G coincides with the multiplication laws in G. In particular, $G \models \varphi_0(x_1, \ldots, x_n)$ for each direct summand G of F of rank $\aleph_0$ that contains $x_1, \ldots, x_n$.

Now suppose $n \geq 2$, $\varphi(X_1, \ldots, X_n)$ is an arbitrary formula of $\mathcal{L}(\mathrm{group})$, and from $F \models \varphi(x_1, \ldots, x_n)$ for $x_1, \ldots, x_n \in F$ it follows that $G \models \varphi(x_1, \ldots, x_n)$ for each direct summand G of F of rank $\aleph_0$ that contains $x_1, \ldots, x_n$. We prove the same statement for the formula $(QX_n)\varphi(X_1, \ldots, X_{n-1}, X_n)$, where Q is either $\exists$ or $\forall$.

First suppose Q is $\exists$ and let $x_1, \ldots, x_{n-1}$ be elements of F with

$$F \models (\exists X_n)\varphi(x_1, \ldots, x_{n-1}, X_n). \tag{2}$$

By Proposition 2.3(a), F has a direct summand G of rank $\aleph_0$ that contains $x_1, \ldots, x_{n-1}$. By (2) there exists $x_n \in F$ with $F \models \varphi(x_1, \ldots, x_{n-1}, x_n)$. By Proposition 2.4, F has a direct summand H of rank $\aleph_0$ that contains $\langle G, x_n \rangle$ and there exists an isomorphism α: $H \to G$ that fixes $x_1, \ldots, x_{n-1}$. The assumption on φ implies that $H \models \varphi(x_1, \ldots, x_{n-1}, x_n)$. Hence, $G \models \varphi(x_1, \ldots, x_{n-1}, \alpha(x_n))$. Consequently, $G \models (\exists X_n)\varphi(x_1, \ldots, x_{n-1}, X_n)$, as desired.

Now suppose $Q = \forall$ and let $x_1, \ldots, x_{n-1}$ be elements of F with

$$F \models (\forall X_n)\varphi(x_1, \ldots, x_{n-1}, X_n).$$

Thus, for each $x_n \in G$ we have $F \models \varphi(x_1, \ldots, x_{n-1}, x_n)$, so $G \models \varphi(x_1, \ldots, x_{n-1}, x_n)$. It follows that $G \models (\forall X_n)\varphi(x_1, \ldots, x_{n-1}, X_n)$, as desired.

Induction on n now proves that if θ holds in F, then θ holds in each direct summand of F of rank $\aleph_0$. Since there are such summands, $\mathbb{Z}_p^{\aleph_0} \models \theta$. Consequently, $\mathbb{Z}_p^{\aleph_0} \equiv \mathbb{Z}_p^m$. ∎

3. Elementary Equivalence of Abelian Profinite Groups

Theorem 2.5 is a consequence of a comprehencive result of Szmielew that gives a simple criterion for two Abelian groups to be elementarily equivalent in terms of a few invariants of the groups.

Following Szmielew we consider a prime number l, a positive integer k, and an Abelian additive group A. We say that elements $x_1, \ldots, x_n \in A$ are **linearly independent modulo** l^k if for all $a_1, \ldots, a_n \in \mathbb{Z}$ the equality $\sum_{i=1}^n a_i x_i = 0$ implies $a_i \equiv 0 \mod l^k$ for each i. We say that $x_1, \ldots, x_n$ are **strongly linearly independent modulo** l^k if for all $a_1, \ldots, a_n \in \mathbb{Z}$ the congruence $\sum_{i=1}^n a_i x_i \equiv 0 \mod l^k A$ implies that $a_i \equiv 0 \mod l^k$ for each i.

Let $\rho^{(1)}[l,k](A)$ be the maximal number of elements of A of order l^k that are linearly independent modulo l^k. Let $\rho^{(2)}[l,k](A)$ be the maximal number of elements of A that are strongly linearly independent modulo l^k. Finally, let $\rho^{(3)}[l,k](A)$ be the maximal number of elements of order l^k that are strongly linearly independent modulo l^k. We write ∞ for $\rho^{(i)}[l,k](A)$ if there is an unbounded number of elements of A satisfying the i-th condition, $i = 1, 2, 3$.

In addition, we say that A is of the **first kind** if there exists a positive integer n such that $nA = 0$. Otherwise, we say that A is of the **second kind**.

The following deep result of Szmielew gives a criterion for Abelian groups to be elementarily equivalent.

PROPOSITION 3.1 ([Szm55, Thm. 5.2]): *Abelian groups A and B are elementarily equivalent (in the language $\mathcal{L}$(group)) if and only if they are of the same kind and $\rho^{(i)}[l,k](A) = \rho^{(i)}[l,k](B)$ for $i = 1, 2, 3$, each prime number l, and all positive integers k.*

Note that if A is torsion-free, than A is of the second kind and $\rho^{(i)}[l,k](A) = 0$ for $i = 1, 3$. This leads to the following special case of Proposition 3.1.

COROLLARY 3.2: *Torsion-free Abelian groups A and B are elementary equivalent if and only if $\rho^{(2)}[l,k](A) = \rho^{(2)}[l,k](B)$ for each prime number l and all $k \in \mathbb{N}$.*

We apply Corollary 3.2 to Abelian profinite group and choose a set S of prime numbers. For each $p \in S$ we choose an infinite cardinal m_p. Then we set $A_{S,m} = \prod_{p \in S} \mathbb{Z}_p^{m_p}$.

THEOREM 3.3: *For a fixed set S of prime numbers all profinite Abelian groups $A_{S,m}$ are elementarily equivalent.*

Proof: First we observe that $A_{S,m}$ is torsion-free, so may apply the criterion given by Corollary 3.2. Then we note that if P is a pro-p Abelian group and $l \neq p$, then $l^k P = P$ for all $k \in \mathbb{N}$. Hence, $\rho^{(2)}[l,k](A) = 0$ if $l \notin S$. If $l \in S$, then $A_{S,m}/l^k A_{S,m} \cong (\mathbb{Z}/l^k\mathbb{Z})^{m_l}$, so $\rho^{(2)}[l,k](A) = \infty$. It follows from Corollary 3.2 that if $(m'_p)_{p \in S}$ is another set of infinite cardinals, then $A_{S,m} \equiv A_{S,m'}$, as claimed. ∎

The special case of Theorem 3.3, where S consists of a unique prime number p gives Theorem 2.5.

References

[FrJ05] M. D. Fried and M. Jarden, *Field Arithmetic, Second Edition, revised and enlarged by Moshe Jarden,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2005.

[Hir69] R. Hirshon, *On cancellation in groups,* American Mathematical Monthly **76**, 1969, 1037–1039.

[NiS03] N. Nikolov and D. Segal, *Finite index subgroups in profinite groups,* Comptes Rendus de l'Académie des Sciences **337** (2003), 303–308.

[NiS07] N. Nikolov and D. Segal, *On finitely generated profinite groups. I. Strong completeness and uniform bounds,* Annals of Mathematics **165** (2007), 171–238.

[Nie03] A. Nies, *Separating classes of groups by first-order sentences,* International Journal of Algebra and Computation **13** (2003), 287–302.

[Oge91] F. Oger, *Cancellation and elementary equivalence of groups,* Journal of Pure and Applied Algebra **30** (1983), 293-299.

[RiZ00] L. Ribes and P. Zalesskii, *Profinite Groups,* Ergebnisse der Mathematik III **40**, Springer, Berlin, 2000.

[SaW91] G. Sabbagh and J. Wilson, *Polycyclic groups, finite images, and elementary equivalence,* Archiv der Mathematik **57** (1991), 231–227.

[Sel03] Z. Sela, *Diophantine geometry over groups and the elementary theory of free and hyperbolic group,* Bulletin of the Symbolic Logic Volume **9** (2003), 51–70.

[Szm55] W. Szmielew, *Elementary properties of Abelian groups,* Fundamenta Mathematica **41** (1955), 203–271.

[Zil71] B. Zil'ber, *An example of two elementarily equivalent, but nonisomorphic finitely generated metabelian groups,* Algebra i Logika **10** (1971), 309–315.

Moshe Jarden
School of Mathematics, Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel
e-mail: jarden@post.tau.ac.il

Alexander Lubotzky
Institute of Mathematics, The Hebrew University of Jerusalem
Givat Ram, Jerusalem 91094, Israel
e-mail: alexlub@math.huji.ac.il