Journal of Pure and Applied Algebra 30 (1983) 293-299
North-Holland

CANCELLATION AND ELEMENTARY EQUIVALENCE OF GROUPS

Francis OGER

U.E.R. de mathématiques, E.R.A. de logique no. 1021, Université Paris VII, tour 45–55, 5ème étage, 2 place Jussieu, 75251 Paris Cedex 05. France

Communicated by J. Benabou
Received 24 March 1983

If A and B are groups such that $A\times\mathbb{Z}\cong B\times\mathbb{Z}$, then A and B are elementarily equivalent. From this follows the existence of finitely generated torsion-free nilpotent groups which are elementarily equivalent without being isomorphic.

Since 1970, a number of papers were devoted to the investigation of non-isomorphic groups A,B such that $A\times\mathbb{Z}\cong B\times\mathbb{Z}$. It is fair to say that no clear algebraic pattern emerges.

This paper is divided into two parts: In the first, and most important, part we prove the following result, which provides a surprising connection with model theory:

Theorem. *If A and B are groups such that $A\times\mathbb{Z}\cong B\times\mathbb{Z}$, then A and B are elementarily equivalent.*

In the second part we give some examples and applications.

The definition of elementary equivalence and the results of model theory which are used here can be found in [2]. The reader is referred to [7] for group theory.

For subsets X, Y of a group G, we denote by $\langle X\rangle$ the subgroup generated by X and $[X, Y]$ the subgroup generated by

$$\{[x,y]=x^{-1}y^{-1}xy \mid x\in X, y\in Y\}.$$

If X has a single element x, we write $[x, Y]$ instead of $[X, Y]$ and $\langle x, Y\rangle$ instead of $\langle X\cup Y\rangle$. We note $Z(G)$ the center of a group G.

0022-4049/83/$3.00

1. Proof of the theorem

We shall prove that A and B are elementarily equivalent under the following hypotheses:

- A and B are subgroups of a group G and x, y elements of G.
- $\langle x\rangle \cap A = \{1\}$, $[x, A] = \{1\}$ and $\langle x, A\rangle = G$.
- $\langle y\rangle \cap B = \{1\}$ $[y, B] = \{1\}$ and $\langle y, B\rangle = G$.
- $\langle x\rangle$ and $\langle y\rangle$ are isomorphic to $\mathbb{Z}$.

Isomorphic groups are elementarily equivalent. So, from now on, we suppose A and B non-isomorphic.

Lemma 1. *We have $[G, G] \subset A \cap B$; so A, B and $A \cap B$ are normal subgroups of G.*

Proof. Since x is obviously in the center of G, we have $[G, G] = [\langle x, A\rangle, \langle x, A\rangle] = [A, A] \subset A$. Likewise, we have $[G, G] \subset B$.

Lemma 2. (i) *The group $\langle x, y\rangle$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$.*

(ii) *We have $\langle x, y\rangle \cap (A \cap B) = \{1\}$.*

(iii) *The following groups are isomorphic to $\mathbb{Z}$:*

$$\langle x, y\rangle \cap A, \qquad \langle x, y\rangle \cap B, \qquad \langle x, y\rangle/(\langle x, y\rangle \cap A), \qquad \langle x, y\rangle/(\langle x, y\rangle \cap B).$$

Proof. The subgroup $M = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid x^a y^b \in A \cap B\}$ is either isomorphic to $\mathbb{Z}$ or to $\{0\}$ since $\langle (1, 0)\rangle \cap M = \{(0, 0)\}$. As $G/A \cong \mathbb{Z}$ and $G/B \cong \mathbb{Z}$ are torsion-free groups, $G/(A \cap B)$ and $(\mathbb{Z} \times \mathbb{Z})/M$ are also torsion-free. So, if M is isomorphic to $\mathbb{Z}$, $(\mathbb{Z} \times \mathbb{Z})/M$ is isomorphic to $\mathbb{Z}$ and there is a basis $\{(k, l), (m, n)\}$ of $\mathbb{Z} \times \mathbb{Z}$ with $(k, l) \in M$ and $\langle (m, n)\rangle \cap M = \{(0, 0)\}$. We have

$$\langle x, y\rangle = \langle x^k y^l, x^m y^n\rangle,$$

$$G = \langle x, A\rangle = \langle x^k y^l, x^m y^n, A\rangle = \langle x^m y^n, A\rangle$$

and

$$G = \langle y, B\rangle = \langle x^k y^l, x^m y^n, B\rangle = \langle x^m y^n, B\rangle$$

with

$$\langle x^m y^n\rangle \cap A = \{1\} \quad \text{and} \quad \langle x^m y^n\rangle \cap B = \{1\}.$$

Therefore, if M is isomorphic to $\mathbb{Z}$, A and B are both isomorphic to $G/\langle x^m y^n\rangle$, contrary to our hypothesis.

So, we have

$$M = \{(0, 0)\}, \ \langle x, y\rangle \cong \mathbb{Z} \times \mathbb{Z} \quad \text{and} \quad \langle x, y\rangle \cap (A \cap B) = \{1\}.$$

Moreover,

$$\langle x, y\rangle/(\langle x, y\rangle \cap A) \cong \langle x, y, A\rangle/A = G/A$$

and

$$\langle x, y\rangle/(\langle x, y\rangle \cap B) \cong \langle x, y, B\rangle/B = G/B$$

are both isomorphic to $\mathbb{Z}$. An obvious argument about ranks of $\mathbb{Z}$-modules shows that $\langle x, y\rangle \cap A$ and $\langle x, y\rangle \cap B$ are also isomorphic to $\mathbb{Z}$.

Lemma 3. *The groups $A/(A\cap B)$, $Z(A)/(Z(A)\cap B)$, $B/(A\cap B)$ and $Z(B)/(A\cap Z(B))$ are isomorphic to $\mathbb{Z}$.*

Proof. We only give the argument for $Z(A)/(Z(A)\cap B)$ since the other proofs are similar. It follows from Lemma 2 that $Z(A)$ is not contained in B, for $\langle x, y\rangle \cap A$ is contained in $Z(A)$. Therefore, $Z(A)/(Z(A)\cap B) \cong \langle Z(A), B\rangle / B \subset G/B$ is isomorphic to $\mathbb{Z}$.

Lemma 4. *There is an integer $p \geq 2$ such that*

$$A/\langle Z(A), A\cap B\rangle \cong B/\langle Z(B), A\cap B\rangle \cong \mathbb{Z}/p\mathbb{Z}.$$

Proof. The group $A/\langle Z(A), A\cap B\rangle$ is cyclic since $A/(A\cap B)$ is isomorphic to $\mathbb{Z}$ and finite since $Z(A)$ is not contained in $A\cap B$. Moreover, we have:

$$\begin{aligned} A/\langle Z(A), A\cap B\rangle &\cong G/\langle x, Z(A), A\cap B\rangle = G/\langle y, Z(B), A\cap B\rangle \\ &\cong B/\langle Z(B), A\cap B\rangle \end{aligned}$$

since $\langle x, Z(A)\rangle = Z(G) = \langle y, Z(B)\rangle$. If the groups $A/\langle Z(A), A\cap B\rangle$ and $B/\langle Z(B), A\cap B\rangle$ were trivial, it would imply

$$A = \langle A\cap B, Z(A)\rangle \cong (A\cap B)\times(Z(A)/(Z(A)\cap B)) \cong (A\cap B)\times\mathbb{Z}$$

and

$$B = \langle A\cap B, Z(B)\rangle \cong (A\cap B)\times(Z(B)/(A\cap Z(B))) \cong (A\cap B)\times\mathbb{Z}.$$

Corollary 5. *If $a\in A$ and $b\in B$ are such that $A=\langle a, A\cap B\rangle$ and $B=\langle b, A\cap B\rangle$, we have*

$$\langle a^p, A\cap B\rangle = \langle Z(A), A\cap B\rangle \quad \text{and} \quad \langle b^p, A\cap B\rangle = \langle Z(B), A\cap B\rangle$$

for the integer p of Lemma 4.

Proof. Since $A/\langle Z(A), A\cap B\rangle$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, we have $a^p \in \langle Z(A), A\cap B\rangle$ and $\langle a^p, A\cap B\rangle \subset \langle Z(A), A\cap B\rangle$. Then, $\langle a^p, A\cap B\rangle = \langle Z(A), A\cap B\rangle$ follows from

$$|A/\langle a^p, A\cap B\rangle| = |\langle a, A\cap B\rangle/\langle a^p, A\cap B\rangle| = p = |A/\langle Z(A), A\cap B\rangle|.$$

If $b\in B$ is such that $B=\langle b, A\cap B\rangle$, we have $G=\langle y, b, A\cap B\rangle$ and $A = \langle A\cap\langle y, b\rangle, A\cap B\rangle$ since $A\cap B$ is normal in G. So, we can choose $a\in A\cap\langle y, b\rangle$ such that $A=\langle a, A\cap B\rangle$.

For the sequel, we consider elements $a\in A$ and $b\in B$ such that $A=\langle a, A\cap B\rangle$ and $B=\langle b, A\cap B\rangle$, and for which there are integers r, s such that $a=y^r b^s$. Replacing a by a^{-1} if necessary, we may assume $s\geq 0$. We also consider elements $c, d\in A\cap B$, $u\in Z(A)$ and $v\in Z(B)$ such that $a^p = uc$ and $b^p = vd$.

We note that a, b, u, υ are elements of infinite order according to Lemma 3. Each of the elements a, b, c, d commutes with the three others.

Lemma 6. *With these definitions, we have $s \geq 2$.*

Proof. If $s=0$, we have $a \in Z(A)$, contrary to Lemma 4. If $s=1$, there is an isomorphism $f: A \to B$ such that $f(a)=b$ and $f(x)=x$ for each $x \in A \cap B$.

Lemma 7. *The integers p, s are prime to each other.*

Proof. If m is a divisor of p and s, we have

$$a^{p/m} = (y^r b^s)^{p/m} = y^{r(p/m)}(b^p)^{s/m} = y^{r(p/m)}(\upsilon d)^{s/m}$$
$$= (y^{r(p/m)}\upsilon^{s/m})d^{s/m}.$$

Since a and d belong to A, $y^{r(p/m)}\upsilon^{s/m} = a^{p/m}d^{-s/m}$ belongs to $Z(G) \cap A = Z(A)$. Moreover, $d^{s/m}$ belongs to $A \cap B$. So we have $a^{p/m} \in \langle Z(A), A \cap B\rangle$ and $m = \mp 1$.

Lemma 8. *For each integer $n \geq 2$, there are two integers g and h, with g prime to n, and an element $z \in \langle y, \upsilon\rangle$ such that $a = b^g d^h z$.*

Proof. We must find g, h and z such that

$$y^r b^s = a = b^g d^h z = b^g(b^p \upsilon^{-1})^h z = b^{g+ph}\upsilon^{-h} z.$$

It is sufficient to have $s = g + ph$ and $z = y^r \upsilon^h$. So, we have only to find a solution (g, h) of the equation $s = g + ph$, with g and n prime to each other, knowing that s and p are prime to each other.

Let us consider two integers i, j such that $n = ij$, with j prime to s and each prime divisor of i being a divisor of s. As p is prime to s, it is also prime to i. Thus, $g = s + pj$ is prime to i since p and j are prime to i. It is also prime to j since j and s are prime to each other. So, g is prime to n. Moreover, $(g = s + pj,\ h = -j)$ is a solution of $s = g + ph$.

We are going to prove that, for any non-trivial ultrafilter U over $\mathbb{N}$, A^U and B^U are isomorphic. Then, A and B will be elementarily equivalent, according to corollary 4.1.10 of [2].

For two elements $z \in G^U$ and $\alpha \in \mathbb{Z}^U$, we note z^α the element of G^U which admits $(z_n^{\alpha_n})_{n\in\mathbb{N}}$ as a representative, where $(z_n)_{n\in\mathbb{N}}$ and $(\alpha_n)_{n\in\mathbb{N}}$ are any representatives of z and α in $G^{\mathbb{N}}$ and $\mathbb{Z}^{\mathbb{N}}$. If z_1 commutes with z_2 in G^U, we have

$$(z_1 z_2)^\alpha = z_1^\alpha z_2^\alpha \quad \text{for any } \alpha \in \mathbb{Z}^U.$$

The subgroup $E = \bigcap_{n\in\mathbb{N}^*} n\mathbb{Z}^U$ of $\mathbb{Z}^U$ is *divisible* (for each $x \in E$ and each $n \in \mathbb{N}^*$, there is a $y \in E$ such that $x = ny$). A subgroup S of $\mathbb{Z}^U$ is said to be a *supplementary* of E in $\mathbb{Z}^U$ if and only if $S \cap E = \{1\}$ and $\langle S, E\rangle = \mathbb{Z}^U$. The divisibility of E and the existence of a supplementary of E in $\mathbb{Z}^U$ are classical since the groups involved are abelian (for a more general treatment, see Proposition 5.4 and Theorem 5.3 of [6]).

Lemma 9. *Let S and T be supplementaries of E in $\mathbb{Z}^U$. The subgroups $u^E = \{u^\alpha \mid \alpha \in E\}$ and $C = \{a^\alpha z \mid \alpha \in S$ and $z \in (A \cap B)^U\}$ of A^U are such that $u^E \cap C = \{1\}$, $[u^E, C] = \{1\}$ and $\langle u^E, C\rangle = A^U$. In the same way, $v^E = \{v^\alpha \mid \alpha \in E\}$ and $D = \{b^\alpha z \mid \alpha \in T$ and $z \in (A \cap B)^U\}$ are such that $v^E \cap D = \{1\}$, $[v^E, D] = \{1\}$ and $\langle v^E, D\rangle = B^U$. Any isomorphism $f: C \to D$ induces an isomorphism $f': A^U \to B^U$ with $f'(u^\alpha) = v^\alpha$ for each $\alpha \in E$ and $f'(x) = f(x)$ for each $x \in C$.*

Proof. Every element of A^U is a product $a^\alpha z$ with $\alpha \in \mathbb{Z}^U$ and $z \in (A \cap B)^U$. For each $\alpha \in \mathbb{Z}^U$, there are $\beta \in S$ and $\gamma \in E$ such that $\alpha = \beta + \gamma$, and $\delta \in E$ such that $\gamma = p\delta$. It follows that

$$a^\alpha z = a^\beta (a^p)^\delta z = a^\beta (uc)^\delta z = u^\delta a^\beta (c^\delta z)$$

with $\delta \in E$, $\beta \in S$ and $c^\delta z \in (A \cap B)^U$. Moreover, for each $\alpha \in E$, if $u^\alpha = a^{p\alpha} c^{-\alpha}$ belongs to C, we have $p\alpha \in E \cap S$ and $\alpha = 0$.

To end the proof, it is enough to observe that the maps $\alpha \to u^\alpha$ from E onto u^E and $\alpha \to v^\alpha$ from E onto v^E are isomorphisms; this easily follows from the previously noted fact that the elements u and v of G are of infinite order.

Lemma 10. *If S is a supplementary of E in $\mathbb{Z}^U$ and if $g \in \mathbb{Z}^U$ has a representative $(g_n)_{n \in \mathbb{N}}$ such that g_n is prime to $n!$ for each integer n, then $T = gS$ is a supplementary of E in $\mathbb{Z}^U$ and the map $S \to T: q \to gq$ is an isomorphism.*

Proof. Let us consider an element $q \in S - \{0\}$ and a representative $(q_n)_{n \in \mathbb{N}}$ of q in $\mathbb{Z}^{\mathbb{N}}$. There is an integer $k \geq 2$ such that $q \notin k\mathbb{Z}^U$ and, therefore, $\{n \in \mathbb{N} \mid q_n \notin k\mathbb{Z}\} \in U$. For this integer k, $\{n \in \mathbb{N} \mid g_n q_n \notin k\mathbb{Z}\}$ contains $\{n \in \mathbb{N} \mid n \geq k$ and $q_n \notin k\mathbb{Z}\}$ since g_n is prime to k for each $n \geq k$. So $\{n \in \mathbb{N} \mid g_n q_n \notin k\mathbb{Z}\}$ belongs to U and gq cannot belong to E since it does not belong to $k\mathbb{Z}^U$.

In order to show that $\mathbb{Z}^U = \langle E, T\rangle$, we consider an element $q \in \mathbb{Z}^U$ and a representative $(q_n)_{n \in \mathbb{N}}$ of q in $\mathbb{Z}^{\mathbb{N}}$. For each $n \in \mathbb{N}$, there is an integer $h_n \in \mathbb{Z}$ such that $g_n h_n - q_n \in n!\mathbb{Z}$. The element $h \in \mathbb{Z}^U$ which admits $(h_n)_{n \in \mathbb{N}}$ as a representative is such that $gh - q \in E$. There is an element $i \in S$ such that $h - i \in E$. Then, we have $gi - q = gh - q - g(h - i) \in E$, hence the lemma.

Now, we come to the proof of $A^U \cong B^U$. For each $n \in \mathbb{N}$, we consider two integers $g(n)$, $h(n) \in \mathbb{Z}$, with $g(n)$ prime to $n!$, and an element $z(n) \in \langle y, v\rangle$ such that $a = b^{g(n)} d^{h(n)} z(n)$. The existence of $g(n)$, $h(n)$ and $z(n)$ follows from Lemma 8. We note g, h the elements of $\mathbb{Z}^U$ and z the element of $Z(G^U)$ which admit $(g(n))_{n \in \mathbb{N}}$, $(h(n))_{n \in \mathbb{N}}$ and $(z(n))_{n \in \mathbb{N}}$ as representatives. We have $a = b^g d^h z$.

We also consider a supplementary S of E in $\mathbb{Z}^U$. According to Lemma 10, $T = gS$

is a supplementary of E in $\mathbb{Z}^L$. It follows from Lemma 9 that we only need to build up an isomorphism f from

$$C = \{a^\alpha w \mid \alpha \in S \text{ and } w \in (A \cap B)^U\} \quad \text{to}$$
$$D = \{b^\alpha w \mid \alpha \in T \text{ and } w \in (A \cap B)^U\}.$$

We define f by

$$f(a^\alpha w) = (az^{-1})^\alpha w = (b^g d^h)^\alpha w = b^{g\alpha}(d^{h\alpha} w)$$

for each $\alpha \in S$ and each $w \in (A \cap B)^U$. It follows from Lemma 10 that f is bijective. So, it suffices to show that f is an homomorphism.

For any $\alpha, \alpha' \in S$ and any $w, w' \in (A \cap B)^U$, we have

$$(a^\alpha w)(a^{\alpha'} w') = a^{\alpha+\alpha'}([a^{\alpha'}, w^{-1}]ww')$$

with $[a^{\alpha'}, w^{-1}]ww' \in (A \cap B)^U$,

$$f((a^\alpha w)(a^{\alpha'} w')) = (az^{-1})^{\alpha+\alpha'}([a^{\alpha'}, w^{-1}]ww')$$

and

$$\begin{aligned} f(a^\alpha w) f(a^{\alpha'} w') &= (az^{-1})^\alpha w (az^{-1})^{\alpha'} w' \\ &= (az^{-1})^{\alpha+\alpha'}[(az^{-1})^{\alpha'}, w^{-1}]ww' \\ &= (az^{-1})^{\alpha+\alpha'}([a^{\alpha'}, w^{-1}]ww') \end{aligned}$$

since z belongs to $Z(G^U)$, which completes the proof of the theorem.

2. Examples and applications

The reader is referred to R. Hirshon's works and especially to the introduction of [3] for the algebraic properties of non-isomorphic groups A, B such that $A \times \mathbb{Z} \cong B \times \mathbb{Z}$. It is well known that if A and B are such groups, they are infinite and non-abelian.

Two examples are quoted in the introduction of [3]. Another one, given on pages 154–155, concerns finitely generated torsion-free nilpotent groups. According to our theorem, this provides an example of finitely generated torsion-free nilpotent groups which are elementarily equivalent without being isomorphic.

Many other examples concern finitely generated groups with finite commutator subgroups. R.B. Warfield proves in [8] that two finitely generated groups with finite commutator subgroups A, B have the same finite images if and only if $A \times \mathbb{Z}$ and $B \times \mathbb{Z}$ are isomorphic. Non-trivial examples of that situation can be found, for instance, in [1, p. 249] and in [5, p. 104].

In [6], we show that two finitely generated groups with finite commutator subgroups A, B are elementarily equivalent if and only if they have the same finite images, and therefore if and only if $A \times \mathbb{Z}$ and $B \times \mathbb{Z}$ are isomorphic.

The theorem of the present paper only provides a partial generalization of this result. As a matter of fact, two finitely generated groups A, B can be elementarily equivalent while $A \times \mathbb{Z}$ and $B \times \mathbb{Z}$ are not isomorphic.

In order to see this, we consider an example, which was given in [4], of a finitely generated group A such that $Z(A)=\{1\}$, $A\cong A\times A\times A$ and $A\not\cong A\times A$. The elementary equivalence of A and $B=A\times A$ follows from Proposition 6.3.13.(ii) of [2] since each of the two groups A, B is isomorphic to a direct factor of the other.

We have $Z(A\times\mathbb{Z})=Z(B\times\mathbb{Z})=\mathbb{Z}$ since $Z(A)=Z(B)=\{1\}$. So, any isomorphism $f:A\times\mathbb{Z}\to B\times\mathbb{Z}$ would map $Z(A\times\mathbb{Z})=\mathbb{Z}$ onto $Z(B\times\mathbb{Z})=\mathbb{Z}$ and induce an isomorphism from $A\cong(A\times\mathbb{Z})/\mathbb{Z}$ to $B\cong(B\times\mathbb{Z})/\mathbb{Z}$. Therefore, $A\times\mathbb{Z}$ and $B\times\mathbb{Z}$ are not isomorphic.

As a conclusion, we also mention Theorem 1 of [3]: If a group C satisfies the maximal condition for normal subgroups and if $A\times C\cong B\times C$, then $A\times\mathbb{Z}\cong B\times\mathbb{Z}$. Therefore, A and B are elementarily equivalent, according to our theorem.

On the other hand, if A and B are the two finitely generated groups that we introduced when we considered the example of [4], we have $A=\{1\}\times A\cong B\times A$ while $\{1\}$ and B are not elementarily equivalent.

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, Vol. 73 (North-Holland, Amsterdam, 1973).

[3] R. Hirshon, Some cancellation theorems with applications to nilpotent groups, J. Austral. Math. Soc. 23 (Series A) (1977) 147–165.

[4] J.M.T. Jones, On isomorphisms of direct powers, in: Word Problems II, Studies in Logic, Vol. 95 (North-Holland, Amsterdam, 1980) 215–245.

[5] G. Mislin, Nilpotent groups with finite commutator subgroups, in: Localization in Group Theory and Homotopy Theory, Lecture Notes in Mathematics, Vol. 418 (Springer-Verlag, Berlin, 1974) 103–120.

[6] F. Oger, Equivalence élémentaire entre groupes finis-par-abéliens de type fini, Comment. Math. Helv. 57 (1982) 469–480.

[7] D. Robinson, Finiteness Conditions and Generalized Soluble Groups, Ergebnisse der Mathematik und Ihrer Grenzgebiete, Vol. 62 (Springer-Verlag, Berlin, 1972).

[8] R.B. Warfield, Genus and cancellation for groups with finite commutator subgroup, J. Pure App. Algebra 6 (1975) 125–132.