PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 130, Number 12, Pages 3461–3464
S 0002-9939(02)06486-9
Article electronically published on April 22, 2002

DERIVATIONS AND THE PERMUTABILITY OF SUBGROUPS IN POLYCYCLIC-BY-FINITE GROUPS

DEREK J. S. ROBINSON

(Communicated by Steven D. Smith)

Abstract. It is shown that there is an algorithm to decide if two given subgroups of a polycyclic-by-finite group permute. This is accomplished by finding an algorithm which is able to determine if a derivation is surjective.

1. Results

In recent years an extensive body of algorithms has been developed to perform many standard tasks for polycyclic-by-finite groups ([1], [4]). Among these is an algorithm which is able to decide if a given subgroup H of a polycyclic-by-finite group G is permutable, i.e., $HK = KH$ for each subgroup K of G ([1], 7.7). The related problem of deciding whether two given subgroups H and K permute with each other is mentioned in an earlier paper of Lennox and Wilson ([3], Corollary A1). There it is stated that the problem has a positive solution as a consequence of the fact that two subgroups of a polycyclic-by-finite group permute if their images in every finite quotient permute. However, the connection between these results is not clear and it seems probable that the statement was an oversight.

Our main purpose here is to remedy the situation by proving

Theorem A. *There is an algorithm which, when a polycyclic-by-finite group G and finite subsets X and Y of G are given, decides if $HK = KH$ where $H = \langle X\rangle$ and $K = \langle Y\rangle$.*

This result will follow from a theorem about derivations.

Theorem B. *There is an algorithm which, when given a polycyclic-by-finite group Q, a finitely generated abelian group A with an explicit Q-module structure, and a derivation $\delta : Q \to A$, decides if δ is surjective.*

Here it is understood that the Q-module structure is given by specifying the action of the generators of Q on those of A, and that the derivation is given by listing the images of the generators of Q. Finally, we record another algorithmic result about derivations which is a consequence of Theorem A.

Theorem C. *There is an algorithm which, when given a polycyclic-by-finite group Q, a finitely generated abelian group A with an explicit Q-module structure, a derivation $\delta : Q \to A$, and finite subsets X, Y of Q, decides if $H^\delta = K^\delta$ where $H = \langle X\rangle$ and $K = \langle Y\rangle$.*

Received by the editors May 29, 2001 and, in revised form, July 5, 2001.
2000 *Mathematics Subject Classification.* Primary 20F10, 20F16.

Here, of course, H^δ is the set $\{h^\delta | h \in H\}$. Theorem C was suggested by the referee, to whom our thanks are due.

2. Proofs

We begin by establishing a simple reduction lemma.

Lemma. *Let Q be a group, A a Q-module, and B a submodule of A. Let $\delta : Q \to A$ be a derivation and define $Q_0 = \{x \in Q | x^\delta \in B\}$. Then*

(i) *Q_0 is a subgroup of Q;*

(ii) *if $\delta_0 : Q_0 \to B$ and $\overline{\delta} : Q \to A/B$ arise from δ by restriction and composition respectively, the derivation δ is surjective if and only if δ_0 and $\overline{\delta}$ are surjective.*

Proof. Of course (i) is clear, as is the necessity of the conditions in (ii). We assume that these conditions hold and show that δ is surjective. To this end let $a \in A$; then we can write $a = b + x^\delta$ where $b \in B$ and $x \in Q$. Further, $bx^{-1} \in B$, so that $bx^{-1} = x_0^{\delta_0} = x_0^\delta$ for some $x_0 \in Q_0$. Therefore $a = (bx^{-1})x + x^\delta = (x_0^\delta)x + x^\delta = (x_0 x)^\delta \in \mathrm{Im}(\delta)$, as required. □

Proof of Theorem B. We begin by making two reductions.

(i) *Let B be a given Q-submodule of A and define $Q_0 = \{x \in Q | x^\delta \in B\}$. If the algorithm exists for the pairs (Q_0, B) and $(Q, A/B)$, then it exists for (Q, A).*

Let $\overline{\delta} : Q \to A/B$ be the derivation induced from δ. If δ is surjective, then so is $\overline{\delta}$ and by hypothesis this can be decided. Thus we may assume that $\overline{\delta}$ is surjective. Notice that $Q_0 = \mathrm{Ker}\ (\overline{\delta})$, and so by [1], 3.4 and 6.2, we can find a finite presentation for Q_0. Also, let $\delta_0 : Q_0 \to B$ arise from restricting δ to Q_0; then δ_0 will be surjective if δ is, and by hypothesis this is decidable for the pair (Q_0, B). Therefore we may assume that δ_0 is surjective. It now follows from the lemma that δ is surjective.

(ii) *We may assume that Q acts faithfully on A.*

First observe that $C = C_Q(A)$ can be found by [1], 4.5. Put $B = \{c^\delta | c \in C\}$. If $x \in Q$ and $c \in C$, then $(xc)^\delta = x^\delta + c^\delta$, from which it follows that B is an additive subgroup of A and that $\mathrm{Im}(\delta) + B \subseteq \mathrm{Im}(\delta)$. In fact, B is a Q-submodule. For if $x \in Q$ and $c \in C$, then $(cx)^\delta = (c^\delta)x + x^\delta$, while in addition $cx = x\overline{c}$ for some $\overline{c} \in C$. Therefore $(cx)^\delta = (x\overline{c})^\delta = x^\delta + \overline{c}^\delta$ and $(c^\delta)x = \overline{c}^\delta \in B$.

Next, δ is surjective if and only if the induced derivation $\overline{\delta} \in \mathrm{Der}\ (Q/C,\ A/B)$ is surjective since $\mathrm{Im}(\delta) + B \subseteq \mathrm{Im}(\delta)$. Note that we have finite presentations for Q/C and A/B; for if $c_1, \dots, c_m$ generate C, then $c_1^\delta, \dots, c_m^\delta$ generate B. Hence we may pass to the pair $(Q/C,\ A/B)$. If the action of Q/C on A/B is not faithful, repeat the argument. Since Q satisfies the maximal condition, we will eventually find a pair with faithful action, and it is enough to decide surjectivity of the derivation for this pair.

(iii) *The final step.*

We show that the algorithm exists by induction on the Hirsch number $h(A)$, which is of course computable. If $h(A) = 0$, then A, and hence Q, is finite and the result is obvious.

Let $h(A) > 0$ and let F denote the Fitting subgroup of Q, which can be found by [1], 5.1. We can decide whether $A/[A, F]$ is finite. Assuming that it is, we will prove that δ *cannot be surjective.* In the first place it follows from [2], Theorems G and H, that $A^F = H^0(F, A)$ and $H^1(F, A)$ are finite. Then the exact sequence $0 \to H^1(Q/F,\ A^F) \to H^1(Q, A) \to H^1(F, A)^Q$ shows that $H^1(Q, A)$ is finite.

Choose a prime p not dividing $m = |H^1(Q, A)|$. Then $m\delta$ is inner, as is $m\delta(p)$ where $\delta(p) : Q \to A/pA$ is the induced derivation. But $H^1(Q, A/pA)$ is a p-group and p does not divide m. Hence $\delta(p)$ is inner and $x^\delta \equiv a(x-1)(\text{mod } pA)$ for some $a \in A$. If δ is surjective, then so is $\delta(p)$ and $a \equiv a(1-x)(\text{mod } pA)$ for some $x \in Q$. This implies that $a \in pA$, whence $A = pA$. But this means that A is finite, a contradiction.

We may therefore assume that $A/[A, F]$ is infinite: let $B/[A, F]$ be its torsion-subgroup. Of course, B can be found and $h(B) < h(A)$. If B is infinite, the algorithm exists for the pairs (Q_0, B) and $(Q, A/B)$ where $Q_0 = \{x \in Q | x^\delta \in B\}$, by induction on $h(A)$. It follows from (i) that the algorithm exists for (Q, A), so we can decide if δ is surjective.

Finally, suppose that B is finite. Since $C_F(A) = 1$, it follows that F is finite, whence so is Q. But now $\text{Im}(\delta)$ is finite and thus δ cannot be surjective since A is infinite. □

Proof of Theorem A. By [1], 3.4, a finite presentation of the subgroup $\langle H, K\rangle$ can be found. Consequently, we may suppose that $G = \langle H, K\rangle$. We show that it is possible to decide if $G = HK$ by induction on $h(G)$, which can be found by [1], 3.5. If $h(G) = 0$, there is nothing to prove since G is finite, so let $h(G) > 0$. By [1], 3.7 we can find an infinite abelian normal subgroup A of G. By induction hypothesis the algorithm exists for the group G/A; thus we may suppose that $G = HAK$.

Now write $H_0 = H \cap KA$, $K_0 = HA \cap K$ and $G_0 = HA \cap KA$; thus $G_0 = H_0A = K_0A$. Observe that $G = HK$ is valid if and only if $A \subseteq HK$, i.e., $A \subseteq H_0K_0$ or equivalently $G_0 = H_0K_0$. It follows that $G = HK$ if and only if $G_0 = \langle H_0, K_0\rangle$ and $H_0K_0 = K_0H_0$. By [1], 6.3 it is possible to find H_0, K_0 and G_0. Certainly it is decidable if $G_0 = \langle H_0, K_0\rangle$, so that we may assume this holds. Consequently, the triple (G, H, K) may be replaced by (G_0, H_0, K_0), i.e., we may assume that

$$G = HA = KA.$$

Next $H \cap A \lhd G$ and $K \cap A \lhd G$ and a finite presentation of $G/(H \cap A)(K \cap A)$ can be found. Thus nothing is lost in assuming that $H \cap A = 1 = K \cap A$.

We are now in a position to introduce derivations. For each h in H there is a unique element h^δ in A such that $hh^\delta \in K$. Furthermore, $\delta : H \to A$ is a derivation. Now a finite presentation of H can be found and the H-module structure of A is known. Also the images of the generators x_i of H under δ can be found by enumerating elements x_ia with a in A and checking to see if $x_ia \in K$; when such an a appears, it will be x_i^δ. Finally, $G = HK$ holds if and only if δ is surjective, which is decidable by Theorem B. □

Proof of Theorem C. First observe that an equivalent formulation of the theorem is that one can decide whether $aH = aK$ for any $a \in A$. Indeed, if this is decidable and δ is given, put $A^* = A \oplus \langle u\rangle$ where u has infinite order, and make A^* into a Q-module via $u \cdot x = u + x^\delta$ where $x \in Q$. Then $h^\delta = k^\delta$ if and only if $u \cdot h = u \cdot k$. Conversely, let $a \in A$ be given and define a derivation $\delta : Q \to A$ by $x^\delta = a(x-1)$. Then $ah = ak$ if and only if $h^\delta = k^\delta$. We can therefore concentrate on deciding whether $aH = aK$. Next, it is easy to show that $aH = aK$ if and only if $aH = aJ = aK$ where $J = \langle H, K\rangle$. Since a finite presentation of J can be found, we may assume that $K = Q$. Finally, $aH = aQ$ is equivalent to $Q = C_Q(a)H$, and by Theorem A this is decidable since $C_Q(a)$ can be found by [1], 6.1. □

In conclusion, we remark that Theorem C implies Theorem A, so that the two results have the same logical status. To see this, first recall that every polycyclic group is isomorphic with a subgroup of some $GL_n(\mathbb{Z})$. Thus in the situation of Theorem A we may assume that G is generated by a finite set of matrices in $GL_n(\mathbb{Z})$. Write M for the ring of all $n \times n$ integral matrices and make M into a $(G \times G)$-module via $m \cdot (x, y) = x^{-1}my$, $(m \in M,\ x, y \in G)$. Without loss of generality, we can assume that $G = \langle H,\ K\rangle$. Then $HK = KH$ holds if and only if $G = HK$, i.e., if $1_n(H \times K) = 1_n(G \times G)$, which is decidable by Theorem C.

References

1. G. Baumslag, F. B. Cannonito, D. J. S. Robinson and D. Segal, *The algorithmic theory of polycyclic-by-finite groups*, J. Algebra **142** (1991), 118-149. MR **92i:**20036
2. J. C. Lennox and D. J. S. Robinson, *Soluble products of nilpotent groups*, Rend. Sem. Mat. Univ. Padova **62** (1980), 261-280. MR **81j:**20050
3. J. C. Lennox and J. S. Wilson, *A note on permutable subgroups*, Arch. Math. (Basel) **28** (1977), 113-116. MR **58:**11135
4. D. Segal, *Decidable properties of polycyclic groups*, Proc. London Math. Soc. (3) **61** (1990), 497-528. MR **91h:**20050

Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 West Green Street, Urbana, Illinois 61801

E-mail address: robinson@math.uiuc.edu