CONJUGACY IN NILPOTENT GROUPS

NORMAN BLACKBURN

1. **Statement of the theorem.** The aim of the present note is to investigate possible generalizations of the well-known fact that if a is a nonidentity element of a finitely-generated nilpotent group G, there exists an epimorphism ϕ of G onto a finite group such that $a\phi \neq 1$. The generalization that we consider is the following. Let G be a finitely-generated nilpotent group, and let $w(x_1, \cdots, x_n; a_1, \cdots, a_m)$ be a word in variables $x_1, \cdots, x_n$ and elements $a_1, \cdots, a_m$ of G. If $w=1$ has no solution in G, does there exist an epimorphism ϕ of G onto a finite group H such that $w(x_1, \cdots, x_n; a_1\phi, \cdots, a_m\phi)=1$ has no solution in H? The answer in general is in the negative, as is shown by a counterexample constructed below. However, we shall prove, in answer to a question posed by A. W. Mostowski, that the answer is in the affirmative if $w=x^{-1}axb^{-1}$. Our aim then is to prove the following.

THEOREM. *Let G be a finitely-generated nilpotent group and let a, b be elements of G which are not conjutate in G. Then there is an epimorphism ϕ of G onto a finite group H such that $a\phi$, $b\phi$ are not conjugate in H.*

To construct the counterexample referred to above we use the following lemma.

LEMMA 1. *Let $f(t_1, t_2, \cdots, t_n)$ be a polynomial with integer coefficients in n variables $t_1, t_2, \cdots, t_n$. Then there exists a finitely-generated torsion-free nilpotent group G, a word $w(x_1, x_2, \cdots, x_n; u_0, \cdots, u_r)$ in n variables $x_1, x_2, \cdots, x_n$ and elements $u_0, \cdots, u_r$ of G and an element $u \neq 1$ such that as $x_1, x_2, \cdots, x_n$ run through G the values of $w(x_1, x_2, \cdots, x_n; u_0, \cdots, u_r)$ are the values of $u^{f(\lambda_1, \lambda_2, \cdots, \lambda_n)}$ as $\lambda_1, \lambda_2, \cdots, \lambda_n$ run through all integers.*

In the proof of this we mean by the *degree* of the monomial $t_1^{m_1}t_2^{m_2}\cdots t_n^{m_n}$ the integer $m_1+m_2+\cdots+m_n$. Let r be the greatest degree of the monomials occurring in f with nonzero coefficients. Let G be the split extension of a free Abelian group with basis $u_0, u_1, \cdots, u_r$ by the automorphism v which carries u_i into u_iu_{i-1} $(i=1, 2, \cdots, r)$ and u_0 into itself:

Received by the editors July 5, 1963.

$$u_i^{v} = u_i u_{i-1} \qquad (i = 1, 2, \cdots, r), \qquad u_0^{v} = u_0.$$

Then G is nilpotent of class $r+1$. Also G is finitely-generated and torsion-free. If

$$f(t_1, t_2, \cdots, t_n) = \sum c t_1^{m_1} t_2^{m_2} \cdots t_n^{m_n},$$

define

$$w(x_1, x_2, \cdots, x_n; u_0, u_1, \cdots, u_r) = \prod u_{m_1+m_2+\cdots+m_n}^{c(x_1-1)^{m_1}(x_2-1)^{m_2}\cdots(x_n-1)^{m_n}}$$

Now every element of G is of the form $v^{\lambda}y$, where y lies in the group generated by $u_0, u_1, \cdots, u_r$. Thus to find all the values of w we may substitute $x_i = v^{\lambda_i}y_i$. Then

$$u_j^{x_i-1} = u_j^{v^{\lambda_i}y_i-1} = u_{j-1}^{\lambda_i \binom{\lambda_i}{2}} u_{j-2} \cdots .$$

Hence

$$u_j^{(x_i-1)^m} = u_{j-m}^{\lambda_i^m} u_{j-m-1}^{*} \cdots ,$$

where the asterisk denotes some exponent. Hence

$$u_{m_1+m_2+\cdots+m_n}^{c(x_1-1)^{m_1}(x_2-1)^{m_2}\cdots(x_n-1)^{m_n}} = u_0^{c\lambda_1^{m_1}\lambda_2^{m_2}\cdots\lambda_n^{m_n}},$$

and

$$w(x_1, x_2, \cdots, x_n; u_0, u_1, \cdots, u_r) = u_0^{f(\lambda_1, \lambda_2, \cdots, \lambda_n)},$$

as required.

To obtain the counterexample we apply Lemma 1 to some polynomial f, such as $(1-2t)(1-3t)$ or $t_1^2+55t_2^2-5$, with the property that $f=0$ has no integer solutions but $f \equiv 0$ (m) has a solution for every integer m. Let G be the group and w the word obtained from Lemma 1. Then $w=1$ has no solution in G since $f=0$ has no integer solutions. But let ϕ be any epimorphism of G onto a finite group H and let m be the order of $u\phi$. A solution of $f \equiv 0$ (m) yields immediately a solution of $w(x_1, x_2, \cdots, x_n; u_0\phi, u_1\phi, \cdots, u_r\phi) = 1$ in H.

2. **Lemmas.** To prove the theorem we need two lemmas. For any group G and any positive integer m we denote by G^m the group generated by all mth powers of elements of G.

LEMMA 2. *For each prime p and for each positive integer c there exists an integer $d_p(c)$ such that if G is a nilpotent group of class at most c,*

every element of G^{p^n} (for any $n \geqq d_p(c)$) is a $p^{n-d_p(c)}$th power.[1]

Let

$$d_p(c) = (c+1)\nu - p - p^2 - \cdots - p^{\nu-1},$$

where p^ν is the highest power of p which does not exceed c. Thus for $c>1$,

$$d_p(c) = d_p(c-1) + \nu.$$

The lemma is proved by induction on c and is trivial for $c=1$. Now let $x_1, x_2, \cdots, x_r$ be elements of a nilpotent group G of class $c>1$. By a formula of P. Hall [1, Theorem 6.3], we have for $n \geqq d_p(c)$,

$$x_1^{p^n} x_2^{p^n} \cdots x_r^{p^n} = (x_1 x_2 \cdots x_r)^{p^n} y_2^{\binom{p^n}{2}} y_3^{\binom{p^n}{3}} \cdots y_{p^n},$$

where y_j lies in the jth term of the lower central series of G. Now the binomial coefficient

$$\binom{p^n}{p^l u},$$

where $(u, p)=1$, is divisible by p^{n-l}. Also either $y_{p^l u}=1$ or $p^l u \leqq c$ and $l \leqq \nu$, since the class of G is c. Hence

$$y_j^{\binom{p^n}{j}}$$

is always a $p^{n-\nu}$th power, and we may write

$$x_1^{p^n} x_2^{p^n} \cdots x_r^{p^n} = z_1^{p^{n-\nu}} z_2^{p^{n-\nu}} \cdots z_c^{p^{n-\nu}}.$$

Here $z_2, z_3, \cdots$ lie in the derived group of G. Hence by [1, Lemma 1.3], the group T generated by $z_1, z_2, \cdots, z_c$ is of class less than c. Hence by the inductive hypothesis this element is a $p^{n-\nu-d_p(c-1)}$th power, as required.

LEMMA 3. *Let a be an element of a finitely-generated torsion-free nilpotent group G and let H be the centraliser of a in G. Let p be a prime. Then there exists an integer $e=e(G)$ such that if $n \geqq e$, the centraliser of aG^{p^n} in G/G^{p^n} is contained in $HG^{p^{n-e}}/G^{p^n}$.*

It is a simple consequence of [1, Lemma 1.9 and Lemma 4.7, Corollary] that G possesses a series of normal subgroups

[1] This is very slightly stronger than a result of Malcev (Izvestiya Akad. Nauk. SSSR Ser. Mat. 13 (1949), 201–212). I am indebted to the referee for bringing this reference to my attention.

$$1 = Z_0 < Z_1 < \cdots < Z_r = G,$$

such that G/Z_i is torsion-free and Z_{i+1}/Z_i is an infinite cyclic subgroup of the centre of G/Z_i. We prove Lemma 3 by induction on r. The lemma is trivial if $H=G$ (taking $e=0$). Otherwise $r>1$. Let H_1/Z_1 be the centraliser of aZ_1 in G/Z_1. By the inductive hypothesis there exists an integer $e'=e(G/Z_1)$ such that if $n\geqq e'$ the centraliser of $aG^{p^n}Z_1$ in $G/G^{p^n}Z_1$ is contained in $H_1G^{p^{n-e'}}/G^{p^n}Z_1$.

If $x\in H_1$, then $[a, x]\in Z_1$ and Z_1 is contained in the centre of G. Hence if $x, y\in H_1$,

$$[a, xy] = [a, y][a, x]^y = [a, x][a, y].$$

The mapping $x\to[a, x]$ is thus a homomorphism of H_1 into Z_1 with kernel H. If z is an element which generates Z_1, the image of this homomorphism is generated by z^k for some integer k, and if x is an element of H_1 such that $[a, x]=z^k$, then H_1 is generated by x and H. If $k=0$, we take $e=e'$. For in this case $H_1=H$, so for $n\geqq e$ the centraliser of aG^{p^n} in G/G^{p^n} is contained in $H_1G^{p^{n-e'}}/G^{p^n}=HG^{p^{n-e}}/G^{p^n}$.

If $k\neq 0$, let p^κ be the highest power of p which divides k and put $e=e(G)=e'+\kappa+d_p(c)$, where c is the class of G and $d_p(c)$ is defined as in Lemma 2. Suppose that $n\geqq e$ and $[a, b]\in G^{p^n}$. Then $bG^{p^n}Z_1$ certainly lies in the centraliser of $aG^{p^n}Z_1$; hence $b\in H_1G^{p^{n-e'}}$. Hence $b\in tG^{p^{n-e'}}$ for some $t\in H_1$, and $[a, t]\in G^{p^{n-e'}}$. From above, $t=sx^l$ for some $s\in H$, and

$$[a, x^l] = [a, s^{-1}t] = [a, t] \in G^{p^{n-e'}}.$$

But $[a, x^l]=z^{kl}$. Hence by Lemma 2,

$$z^{kl} = u^{p^{n-e'-d_p(c)}}$$

for some $u\in G$. Since G/Z_1 is torsion-free, it follows that $u\in Z_1$, and hence that kl is divisible by $p^{n-e+\kappa}$. Thus l is divisible by p^{n-e}, so that $b\in HG^{p^{n-e}}$.

3. **Proof of the theorem.** We prove the theorem in the case when G is torsion-free by induction on the same integer r as was used in the proof of Lemma 3. Thus if $G>1$ and $Z=\{z\}$ is a cyclic subgroup of the centre of G such that G/Z is torsion-free, we suppose that the theorem is true in G/Z. Let a, b be nonconjugate elements of G. If aZ, bZ remain nonconjugate in G/Z, the result follows at once from the inductive hypothesis. Otherwise b is conjugate to an element of the form az^k, for some integer k. However a and az^k are not conjugate in G.

Let H/Z be the centraliser of aZ in G/Z. As in Lemma 3, the mapping $u \to [a, u]$ is a homomorphism of H into Z, and the image is of the form $\{z^l\}$ for some integer $l \geqq 0$. Now l does not divide k, for otherwise $z^k = [a, u]$ for some $u \in H$ and $a^u = az^k$, which is not the case. Hence there exists a prime power p^m which divides l but does not divide k. Let $e = e(G/Z)$ be defined as in Lemma 3, and put $n = m + e + d_p(c)$, where c is the class of G and $d_p(c)$ is defined as in Lemma 2. By [1, Lemma 4.4, Corollary], G/G^{p^n} is a finite homomorphic image of G. If aG^{p^n}, bG^{p^n} are conjugate, then aG^{p^n}, $az^kG^{p^n}$ are conjugate. Suppose then that $a^x \equiv az^k \pmod{G^{p^n}}$. Then x lies in the centraliser of aZG^{p^n} and so, by Lemma 3, $x \in HG^{p^{n-e}}$. Thus $x \in tG^{p^{n-e}}$ for some $t \in H$ and $a^t \equiv az^k \pmod{G^{p^{n-e}}}$. But from the definition of l, $a^t = az^{lq}$ for some integer q. Hence $z^{lq-k} \in G^{p^{n-e}}$. By Lemma 2, $z^{lq-k} = v^{p^{n-e-d_p(c)}}$ for some $v \in G$. Hence $v \in Z$ and $lq \equiv k (p^m)$. Thus $k \equiv 0 \ (p^m)$, a contradiction. Hence aG^{p^n}, bG^{p^n} are not conjugate, as required.

In the general case the torsion subgroup T of G is finite [1, Theorem 4.5, Corollary], and we proceed by induction on the order of T. If $T = 1$, G is torsion-free, and the theorem is already proved. Otherwise let Z be a subgroup of the centre of G of prime order p. If a, b are nonconjugate elements of G, and a, b remain nonconjugate modulo Z, the result follows at once from the inductive hypothesis. Suppose then that b is conjugate to az for some generator z of Z. Then a and az are not conjugate in G.

Suppose first that there is another prime divisor q of the order of T. Let Z_1 be a subgroup of the centre of G of order q. If a, az are conjugate modulo Z_1, we have

$$a^x = azz_1,$$

for some element x of G and some generator z_1 of Z_1. Since z, z_1 lie in the centre of G, it follows at once that $a^{x^q} = az^q$, and so if $qq' + pp' = 1$, $a^{x^{qq'}} = az$. This is impossible, and so a, az are not conjugate modulo Z_1. Hence the result follows from the inductive hypothesis.

Finally, then, suppose that T is a p-group. Let $e = e(G/T)$ be defined as in Lemma 3, let p^m be the exponent of T and set $n = m + e + d_p(c)$, where c is the class of G and $d_p(c)$ is defined as in Lemma 2. If $v \in T \cap G^{p^{n-e}}$, then by Lemma 2, $v = w^{p^m}$ for some $w \in G$. Hence $w \in T$ and $w^{p^m} = 1$. Thus $T \cap G^{p^{n-e}} = 1$. Suppose that aG^{p^n}, bG^{p^n} are conjugate. Then there is an element x of G such that $a^x \equiv az \pmod{G^{p^n}}$. Hence $xG^{p^n}T$ lies in the centraliser of $aG^{p^n}T$. If H/T is the centraliser of aT in G/T, it follows from Lemma 3 that $x \in HG^{p^{n-e}}$. Hence $x \in tG^{p^{n-e}}$ for some $t \in H$. Thus $a^t \equiv az \pmod{G^{p^{n-e}}}$, or $[t, a]z \in G^{p^{n-e}}$. But since $t \in H$, $[t, a] \in T$. Since $T \cap G^{p^{n-e}} = 1$, we have $[a, t] = z$, or

$a^t = az$, a contradiction. Hence aG^{p^n}, bG^{p^n} are not conjugate, and the theorem is proved.

REFERENCE

1. P. Hall, *Nilpotent groups*, Canadian Mathematical Congress, University of Alberta, Alberta, Canada, 1957.

THE UNIVERSITY, MANCHESTER, ENGLAND

SOME REMARKS ON THE DIOPHANTINE EQUATION $x^3+y^3+z^3=x+y+z$

HUGH MAXWELL EDGAR

In order to avoid certain trivial solutions of the Diophantine equation $x^3+y^3+z^3=x+y+z$ we initially assume $x \geqq y \geqq 0$, $z<0$ and $x \neq -z$. All letters will indicate rational integers throughout, with the exception of k, t, M which denote rational numbers. S. L. Segal [1] has shown that if $x=y$ then only finitely many solutions are forthcoming. Generalizing the method of Segal slightly we prove the following result:

THEOREM 1. *If A, B, C and D are given nonzero integers satisfying $(A, B)=(C, D)=1$ and $C \mid A^2$ then the Diophantine equation*

$$A(Cx^3 - Dx) = B(z^3 - z) \tag{1}$$

has just a finite number of solutions (x, z). An upper bound for the number of solutions is given by

$$c \mid B(A^2D^3 - CB^2)A^3C^3, \quad 5\sum(2\sigma(c)+1) \tag{2}$$

where $\sigma(n)$ denotes the sum of the positive divisors of the natural number n.

PROOF. If $(x, z)=d$ then we write $x=ad$, $z=bd$ with $(a, b)=1$. Upon substituting for x and z in the given equation and dividing by d we obtain the equation

$$(ACa^3 - Bb^3)d^2 = ADa - Bb \tag{3}$$

from which it follows that $ADa-Bb=cd^2$ for some suitable c. Upon writing

Received by the editors July 25, 1963.