THE EXISTENCE OF OUTER AUTOMORPHISMS OF SOME NILPOTENT GROUPS OF CLASS 2

EUGENE SCHENKMAN[1]

In a recent conversation with F. Haimo the question arose as to whether a nilpotent group always possesses an outer automorphism. The object of this note is to show that the answer is in the affirmative for certain nilpotent groups of class 2 and also to show that if the group is finite but not Abelian, then for all primes p when p^k divides the group order it also divides the order of the group of automorphisms.

Some preliminary remarks. We let G' stand for $[G, G]$ the commutator subgroup of G; i.e. the group generated by all commutators $[a, b]=aba^{-1}b^{-1}$ where a and b are elements of G; and also note that nilpotent of class 2 means that G' is in the center of G. From this last fact we readily obtain

(1a) $$[a, bc] = [a, b][a, c],$$

(1b) $$[ab, c] = [a, c][b, c],$$

(1c) $$[a^m, b^n] = [a, b]^{mn},$$

(1d) $$[a, b] = [b, a]^{-1}.$$

E will denote the identity subgroup, e the identity element of G.

We let $G(n)$ denote the subgroup of G generated by the nth powers of the elements of G and assume that for some prime p there is an integer k such that $G(p^k)\subset G'$.

We shall begin with some general results probably well known (cf. for instance [1]), but we have included the proofs for completeness.

THEOREM A. *If G is an Abelian group such that, for some prime p and integer k, $G(p^k)=E$, then G is the direct product of cyclic groups.*

PROOF. If $k=1$ the theorem is true since G is a vector space over the field of p elements. We proceed by induction on k assuming that $G(p)$ is a direct product of cyclic groups, $G(p)=\prod\otimes(x_\alpha)$ where (x_α) designates the cyclic group generated by x_α.

Let y_α be such that $y_\alpha=x_\alpha^{1/p}$. Then the y_α generate a group G_1 which is a direct product, $G_1=\prod\otimes(y_\alpha)$. For $\prod y_\alpha^{n_\alpha}=e$ implies that $\prod y_\alpha^{pn_\alpha} = \prod x_\alpha^{n_\alpha}=e$ whence $x_\alpha^{n_\alpha}=e$ for all α, and hence n_α is a positive power

Presented to the Society, April 23, 1954; received by the editors March 2, 1954.

[1] This research was supported by the U. S Air Force under contract number AF 18(600)-790 monitored by the Office of Scientific Research.

of p; it follows that $\prod x_\alpha^{n_\alpha/p}=e$, whence $x_\alpha^{n_\alpha/p}=e$, and finally $y_\alpha^{n_\alpha}=e$.

Now let G_0 be the maximum subgroup of G such that $G_0(p)=E$; then there is a subgroup $Q=\prod\otimes z_\beta$ such that $G_0=(G_0\cap G_1)\otimes Q$ and finally $G=G_1\otimes Q=(\prod\otimes y_\alpha)\otimes(\prod\otimes z_\beta)$ as can readily be verified.

By a similar method of proof we can obtain the following result.

THEOREM B. *If G is Abelian, $G(p^k)=E$, and if $g_1, \cdots, g_n$ are not in $G(p)$ and if the group they generate is a direct product $(g_1)\otimes \cdots \otimes(g_n)$, then there is an H such that $G=H\otimes(g_1)\otimes \cdots \otimes(g_n)$.*

Letting as usual $\Phi(G)$ denote the intersection of all maximal subgroups of G, we have the following result.

THEOREM C. *If G is nilpotent such that $G(p^k)\subset G'$, then $\Phi(G) = \{G', G(p)\}$, the subgroup of G generated by G' and $G(p)$.*

PROOF. $\Phi(G)\supset G'$ by Theorem 12, p. 114, of [3] and by the same type of argument $\Phi(G)\supset G(p)$. On the other hand if g is not in $\{G', G(p)\}$, then by Theorem B there is a maximal subgroup of G not containing g, and hence g is not in $\Phi(G)$.

Some lemmas on automorphisms.

LEMMA 1. *If M and H are subgroups of G so that for $m\in M$, $h\in H$, $[m, h]=e$, and if $G=MH$, then any automorphism σ of H which leaves $M\cap H$ elementwise fixed can be extended to be an automorphism of G.*

PROOF. If g is in G then $g=mh$ where $m\in M$, $h\in H$, and g^σ will be defined to be mh^σ. This defines g^σ uniquely; for if $g=m_1h_1=m_2h_2$, then $m_2^{-1}m_1=h_2h_1^{-1}=(h_2h_1^{-1})^\sigma=h_2^\sigma(h_1^{-1})^\sigma$ whence $m_1h_1^\sigma=m_2h_2^\sigma$.

We next check that $(m_1h_1)^\sigma(m_2h_2)^\sigma=(m_1h, m_2h_2)^\sigma$. This can be seen since the left member reduces to $m_1h_1^\sigma m_2h_2^\sigma=m_1m_2h_1^\sigma h_2^\sigma$ and the right member to $(m_1m_2h_1h_2)^\sigma=m_1m_2h_1^\sigma h_2^\sigma$.

LEMMA 2. *If M is a normal subgroup of an arbitrary group so that the coset aM is of order n and so that $G=M(a)$, and if z in M is in the center of G such that $z^n=e$, then the mapping σ defined by the rule $(ma^r)^\sigma=ma^rz^r$ is an automorphism of G.*

The verification is left to the reader.

In what follows we let G' be in the center of G and let G be generated by $a, b, c, \cdots, f$ such that G/G' is the direct product of (aG'), (bG'), $\cdots$, (fG') whose orders are k_a, k_b, $\cdots$, k_f, so that every element of G is expressed uniquely as $wa^{r_a}b^{r_b}\cdots f^{r_f}$ where $w\in G'$ and $0\leqq r_a<k_a, \cdots, 0\leqq r_f<k_f$. We then have the following result.

LEMMA 3. *If z commutes with $b, c, \cdots, f$ and the order of az is the* *same as the order of a, then the mapping σ sending $g_1 = w_1 a^{r_a} \cdots f^{r_f}$ into $w_1(az)^{r_a} \cdots f^{r_f}$ is an automorphism of G.*

PROOF. Clearly G' is left elementwise fixed by σ. If now $g_2 = w_2 a^{s_a} \cdots f^{s_b}$, then $g_1 g_2 = w_1 w_2 [b^{r_b} \cdots f^{r_f}, a^{s_a}] a^{r_a + s_a} b^{r_b} \cdots f^{r_f} b^{s_b} \cdots f^{s_f}$; and $(g_1 g_2)^\sigma = w_1 w_2 [b^{r_b} \cdots f^{r_f}, a^{s_a}](az)^{r_a + s_a} b^{r_b} \cdots f^{r_f} b^{s_b} \cdots f^{s_f}$. But

$$\begin{aligned} g_1^\sigma g_2^\sigma &= w_1 (az)^{r_a} b^{r_b} \cdots f^{r_f} w_2 (az)^{s_a} b^{s_b} \cdots f^{s_f} \\ &= w_1 w_2 [b^{r_b} \cdots f^{r_f}, (az)^{s_a}](az)^{r_a + s_a} b^{r_b} \cdots f^{r_f} b^{s_b} \cdots f^{s_f} \end{aligned}$$

and hence σ is an automorphism since $[b^{r_b} \cdots f^{r_f}, a^{s_a}] = [b^{r_b} \cdots f^{r_f}, (az)^{s_a}]$ by the assumption on z and by (1a) and (1c).

LEMMA 4. *Let $\Phi(G)$ be the Φ subgroup of the finite p-group G and let A be the group of automorphisms of G. Then the normal subgroup N (cf. [3, p. 48]) of A of all the automorphisms leaving every coset of G with respect to $\Phi(G)$ fixed is a p-group.*

PROOF. There is a series of characteristic subgroups of G, $G = G_1, G_2, \cdots, G_n \neq E, G_{n+1} = E$, such that G_{i+1} is the group generated by $[G_{i_0}, G]$ and $G_i(p)$ where i_0 is the largest number less than or equal to i so that G_{i_0} is a member of the descending central series.

Now let σ be an automorphism of G so that $a^\sigma = a\phi_a$ where $\phi_a \in \Phi(G)$. Then since $\Phi(G) = G_2$ by Theorem C, the Φ subgroup of G/G_n is Φ/G_n and hence by an induction argument there is a power of p, namely p^k, so that $a^{\sigma^{p^k}} = az_a$ where z_a is in G_n. But if τ is any automorphism of A so that $a\tau = az_a$ with z_a in G_n and hence in the center of G, then $\tau^p = 1$; for z_a is a product of commutators and pth powers and hence $z_a^\tau = z_a$ since each commutator and each pth power is fixed under τ as is readily checked. Hence $a^{\tau^p} = a$ and $\sigma^{p^{k+1}} = 1$. Thus every element of N is of p-power order and the lemma is proved.

The main theorems.

THEOREM 1. *If G is a finite non-Abelian group of prime power order whose commutator subgroup is in the center, then the order of G divides the order of the group of automorphisms of G.*

PROOF. Let $a, b, \cdots, f$ be generators of G with the properties stated in connection with Lemma 3, and so arranged that $[a, b] = w_1$ is an element of maximum order m_1 in G'. Let $w_1, \cdots, w_n$ of orders $m_1, \cdots, m_n$ be a basis for G' so chosen that $m_1 \geqq m_2 \geqq m_i$ for $i = 3, \cdots, n$. Then the order of G is $m_1 m_2 \cdots m_n k_a \cdots k_f$.

Now if d is one of the chosen generators and if m_1 divides k_d, then for w in G' the map sending $g = wa^{r_a} \cdots d^{r_d} \cdots f^{r_f}$ into $wa^{r_a} \cdots (d \cdot d^{tm_1})^{r_d} \cdots f^{r_f}$ for $t = 0, 1, \cdots, k_d/m_1$ is an automorphism by

Lemma 3 which leaves the subgroup (d) invariant. There are k_d/m_1 such automorphisms for the generator d.

By Lemma 2 there is an automorphism sending $wa^{r_a} \cdots d^{r_d} \cdots f^{r_f}$ into $wa^{r_a} \cdots (dw_j^{uq_j})^{r_d} \cdots f^{r_f}$ where $q_j = \max(1, m_j/k_d)$ and $u = 0, 1, \cdots, m_j/q_j$. There are $\min(k_d, m_j)$ such automorphisms for the generator d and for $j = 1, \cdots, n$.

We note now that $c, \cdots, f$ can be so chosen that they commute with a and b modulo $(w_2) \otimes \cdots \otimes (w_n)$. For if d is one of the generators $c, \cdots, f$ suppose $[a, d] \equiv [a, b]^s$ and $[d, b] \equiv [a, b]^t$ modulo $(w_2) \otimes \cdots \otimes (w_n)$. Then $[a, db^{m_1-s}a^{m_1-t}] \equiv e \equiv [db^{m_1-s}a^{m_1-t}, b]$ and $db^{m_1-s}a^{m_1-t}$ can replace d as the generator with the required property.

Now if $q = \max(p, k_b/k_a, m_2)$, then b^q commutes with $b, c, \cdots, f$; then for $u = 0, 1, \cdots, k_b/q$ there are k_b/q elements ab^{uq} and since the orders of these are powers of p between k_a and $k_a m_1$, there are $h+1$ possibilities for the orders where $p^h = m_1$. Hence by replacing a by one of the ab^{uq} if necessary there are by Lemma 3 at least $k_b/q(h+1)$ distinct automorphisms sending $g = wa^{r_a} \cdots f^{r_f}$ into $w(ab^{uq})^{r_a} \cdots f^{r_b}$. Similarly if $r = \max(p, k_b/k_a, m_2)$, interchanging the roles of a and b there are at least $k_a/r(h+1)$ more distinct automorphisms.

All of the above automorphisms are in the normal subgroup of the group of automorphisms of G described in Lemma 4 which will then be at least of order $k_a \cdots k_f(m_2 \cdots m_n)^2 m_2 xy$ where x and y are the least powers of p greater than $k_b/q(h+1)$ and $k_a/r(h+1)$ and where $(m_2 \cdots m_n)^2 m_2$ is 1 if G^2 is cyclic.

But this order is as large as the order of G if $m_2^2 xy \geqq m_1$, which is true except for $m_1 = 8$, 16, 32 and 64 when $m_2 \geqq p$. For then $m_2^2 \geqq m_1$ unless $m_1 \geqq p^3$; but in this case $p^{(m_1)^{1/2}} > m_1 p = p^{h+1}$ whence $(m_1)^{1/2} > h+1$, $m_1/m_2 > (m_1/m_2^2)^{1/2}(h+1)$, and finally x and y being both greater than or equal to $m_1/[m_2(h+1)]$ we see that $xy \geqq m_1/m_2^2$.

We consider now the case where $m_2 = 1$ and first let $m_1 = p^{2k}$ for $k = 1, 2, 3, \cdots$. Then $p^k > h+1$ (except when $m_1 = 4$, 9, and 16) and $p^{2k-1}/(h+1) > p^{k-1}$ whence x and y are greater than or equal to p^k and $xy \geqq m_1$. Next let $m_1 = p^{2k+1}$ for $k = 0, 1, 2, \cdots$; then except when $m_1 = 2$ or 8, $p^{k+1} > (h+1)$ and $p^{2k+1}/p(h+1) > p^{k-1}$ whence $xy \geqq m_1/p$. But by replacing 1 for p in the expression for one of the numbers r, or q by 1, we can obtain one more automorphism of p power order not in the subgroup of automorphisms already considered, which with that subgroup generates a p-group of order at least equal to that of G.

Hence we have proved the theorem except in the exceptional cases when $m_1 = 2$, 4, 8, 9, or 16 when $m_2 = 1$; and $m_1 = 8$, 16, 32, or 64 when $m_2 \geqq p$.

For the proofs in these cases it is possible to apply Lemma 3. Thus for $m_1=2$, if a^2 and b^2 are in G' then two of the three elements a, b, and ab have the same order; for definiteness let them be a and ab. Then there is an automorphism of order 2 leaving b fixed and sending a into ab. If on the other hand b^2 is not in G', let n be minimal so that b^n is in G'; then two of the elements b, ba, and $b^{n-2}ba=bb^{n-2}a$ have the same order and again there is an automorphism of order 2 not in the subgroup of automorphisms previously considered. Thus the theorem follows for $m_1=2$.

When $m_1=8$ if a^8 and b^8 are in G', then two of the elements a, b, ab, ab^2, and ab^3 have the same order and there is at least an automorphism of order 4 of the type holding b fixed and sending a into ab or ab^2. If b^8 is not in G', then letting n be minimal so that b^n is in G' we see that two of the elements b, ba, b^3a, b^5a, and $b^{n-1}a$ have the same order and there is an automorphism of order at least 4 holding b fixed and sending ab into ab^3 or ab^5 or ab^{n-1} (i.e., a into ab^2 or ab^4 or ab^{n-2}). By a similar method, considering b, bc, bc^2, bc^3, and bc^4 where c is a power of a so that cG' has the same or lower order than bG', it is possible to find an automorphism of order at least 2 so that a is fixed. Then the group consisting of these automorphisms together with those previously described has order at least equal to that of G, proving the theorem when $m_1=8$.

We omit the details of the few remaining cases since no new ideas are involved.

COROLLARY. *If G is a finite non-Abelian group whose commutator subgroup is in the center, then the order of G divides the order of the group of automorphisms of G.*

THEOREM 2. *If G is a p-group, if G' is in the center of G, and $G(p^k) \subset G'$, then G has an outer automorphism.*

PROOF. We shall assume to the contrary that all the automorphisms of G are inner and on the basis of this assumption will exhibit an outer autmorphism.

We shall suppose that k is the smallest integer such that $G(p^k)\subset G'$. Let z in G' have maximum order p^r; then $r\leqq k$ since $G(p^k)\subset G'$ implies $G'(p^k)=E$ in view of (1c).

Now let s be the smallest integer greater or equal to r so that there is a $g\notin\Phi(G)$ such that $g^{p^s}\in G'$. Then by Theorem B, $G=M(g)$ where M is normal in G and G/M has order p^s. Hence Lemma 2 asserts that there is an automorphism, which is determined by an element h since by assumption it is inner, such that $[h, g]=z$ and $[h, m]=e$ for $m\in M$. Now M can be changed if necessary so as to contain h. For if $M(h)$ contains M properly, then $M(h)$ contains g^q for some smallest number q, and then by Theorem B, $M(h)=(g^q)\otimes(h)\otimes M_1$ and $G=(g)\otimes(h)\otimes M_1$ so that $(h)\otimes M_1$ has the desired property.

Now h is not in $\Phi(G)$ since in that event, by Theorem C, h would be of the form $\prod_i h_i^p g_2$ where $g_2\in G'$, and then by (1b) and (1c), $[h, g]=[\prod_i h_i^p g_2, g]=\prod_i [h_i, g]^p$, which would contradict the maximality of the order of z in G' since the orders of $[h_i, g]$ are at most as great as that of $[h, g]=z$. Hence $G=N(h)$ where N is normal in G and G/N has order p^t. But p^t is at least equal to p^s by the choice of s and because of (1c) and the fact that z has order p^r.

Again by Lemma 2 there is a k so that, for $n\in N$, $[k, n]=e$ and $[k, h]=z^{-1}$ or $[h, k]=z$. Since $G=M(g)$, $k=mg^r$ and $z=[h, k]=[h, mg^r]=[h, g]^r=z^r$ whence $r=1$ and $k=mg$. Then $G=M(g)=M(k)$.

Now if P is the group generated by h and k, then we shall show that P/P' is of order p^{t+s}. First $P'=P\cap G'$. For clearly $P'\subset P\cap G'$; on the other hand if $d\in P\cap G'$ then by our assumption there is an f such that $[f, k]=d$. But since $f=nh^r$ where n is in N, $[f, k]=[h^r, k]=[h, k]^r\in P'$. Hence $P'=P\cap G'$.

Next we observe that if P/P' is of order less than p^{r+s}, then there must be a relation of the form $h^{p^u}=k^{p^v}$ mod G' where $t>U\geqq V<S$. Then if $w=(kh^{-p^{u-v}})$, $w^{p^v}=k^{p^v}h^{-p^u}\in G'$. But since $[h, w]=[h, k]=z$, w is not in $\Phi(G)$ for the same reason that $h\notin\Phi(G)$, and hence the existence of w contradicts the way s was chosen since $v<s$. We conclude that P/P' is of order p^{t+s}.

Let $Q=M\cap N$. Then, mod G', Q has index p^{t+s} in G; but P has order p^{t+s} mod G'. Furthermore $Q\cap P\subset G'$ and hence $G=QP$. Also $P'=P\cap G'$ so that $P'=P\cap Q$. Finally $[q, p]=e$ for $q\in Q$, $p\in P$. Then by Theorem 1, P has an outer automorphism leaving P' elementwise fixed; this can be extended to be an automorphism of G by Lemma 1, and the proof of the theorem is completed.

It would be of interest to know whether Theorem 2 is valid if the class of nilpotency of the group is arbitrary.

Bibliography

1. I. Kaplansky, *Infinite Abelian groups*, Ann Arbor, University of Michigan, 1954.

2. W. R. Scott, *On the order of the automorphism group of a finite group*, Proc. Amer. Math. Soc. vol. 5 (1954) pp. 23–24.

3. H. Zassenhaus, *The theory of groups*, trans. from the German, New York, 1949.

Louisiana State University and
The Institute for Advanced Study