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

EUGENE SCHENKMAN

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

\[
\begin{align*}
(1a) & \quad [a, bc] = [a, b][a, c], \\
(1b) & \quad [ab, c] = [a, c][b, c], \\
(1c) & \quad [a^n, b^n] = [a, b]^{mn}, \\
(1d) & \quad [a, b] = [b, a]^{-1}.
\end{align*}
\]

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

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

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 \( (x_\alpha) \) designates the cyclic group generated by \( x_\alpha \).

Let \( y_\alpha \) be such that \( y_\alpha = x_\alpha^{1/p} \). Then the \( y_\alpha \) 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 \( \prod x_\alpha^{n_\alpha} = e \) whence \( x_\alpha^{n_\alpha} = e \) for all \( \alpha \), and hence \( n_\alpha \) is a positive power

---

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 $\prod x_{a_i}^{n_{a_i}/p} = e$, whence $x_{a_i}^{n_{a_i}/p} = e$, and finally $x_{a_i}^{n_{a_i}} = e$.

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 $g_1, \ldots, g_n$ 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 $\sigma$ of $H$ which leaves $M \setminus H$ 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 $g^\sigma$ will be defined to be $mh^\sigma$. This defines $g^\sigma$ uniquely; for if $g = m_1h_1 = m_2h_2$, then $m_2^{-1}m_1 = h_2h_1^{-1} = (h_2h_1^{-1})^\sigma = m_2h_2h_1^{-1} = (h_2h_1^{-1})^\sigma$ whence $m_2h_2^\sigma = m_2h_1^\sigma$.

We next check that $(m_1h_1)^\sigma(m_2h_2)^\sigma = (m_1h_1m_2h_2)^\sigma$. 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 $\sigma$ defined by the rule $(ma)^\sigma = ma\sigma z^\sigma$ 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 $a, b, c, \ldots, f$ such that $G/G'$ is the direct product of $(aG'), (bG'), \ldots, (fG')$ whose orders are $k_a, k_b, \ldots, k_f$, so that every element of $G$ is expressed uniquely as $w^a_\alpha y^b_\beta \cdots f^r_\gamma$ where $w \in G'$ and $0 \leq r_\alpha < k_a, \ldots, 0 \leq r_\gamma < k_f$. We then have the following result.

**Lemma 3.** If $z$ commutes with $b, c, \ldots, f$ and the order of $az$ is the
same as the order of $a$, then the mapping $\sigma$ sending $g_1 = w_1 a^{e_1} \cdots f^{e_r}$ into $w_1 (az)^{e_1} \cdots f^{e_r}$ is an automorphism of $G$.

Proof. Clearly $G'$ is left elementwise fixed by $\sigma$. If now $g_2 = w_2 a^{e_2} \cdots f^{e_2}$, then $g_1 g_2 = w_1 w_2 [b^{e_1} \cdots f^{e_1}, a^{e_2} a^{e_2 + e_3} b^{e_3} \cdots f^{e_1} b^{e_2} \cdots f^{e_2}]$; and $(g_1 g_2)^{e} = w_1 w_2 [b^{e_1} \cdots f^{e_1}, a^{e_2}] (az)^{e_1} a^{e_2 + e_3} b^{e_3} \cdots f^{e_1} b^{e_2} \cdots f^{e_2}$. But

$$g_1 g_2 = w_1 (az)^{e_1} b^{e_2} \cdots f^{e_1} w_2 (az)^{e_2} b^{e_3} \cdots f^{e_2}$$

$$= w_1 [b^{e_1} \cdots f^{e_1}, (az)^{e_2}] (az)^{e_1} a^{e_2 + e_3} b^{e_3} \cdots f^{e_1} b^{e_2} \cdots f^{e_2}$$

and hence $\sigma$ is an automorphism since $[b^{e_1} \cdots f^{e_1}, a^{e_2}] = [b^{e_1} \cdots f^{e_1}, (az)^{e_2}]$ by the assumption on $z$ and by (1a) and (1c).

Lemma 4. Let $\Phi(G)$ be the $\Phi$ 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 $G$, $G = G_1, G_2, \cdots, G_n = E$, such that $G_{i+1}$ is the group generated by $[G_i, G]$ 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 $\sigma$ 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 $\Phi$ subgroup of $G/G_n$ is $\Phi/G_n$ and hence by an induction argument there is a power of $p$, namely $p^k$, so that $a^{\sigma = k} = az_a$ where $z_a$ is in $G_n$. But if $\tau$ is any automorphism of $A$ so that $\tau a = az_a$ 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 $p$th powers and hence $z_a^{\tau} = z_a$ since each commutator and each $p$th power is fixed under $\tau$ as is readily checked. Hence $a^{\tau = a}$ 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 $m_1 \geq m_2 \geq m_i$ for $i = 3, \cdots, n$. Then the order of $G$ is $m_1 m_2 \cdots m_n k_0 \cdots k_f$.

Now if $d$ is one of the chosen generators and if $m_1$ divides $k_d$, then for $w$ in $G'$ the map sending $g = w a^{e_0} \cdots d^{e_d} \cdots f^{e_r}$ into $w a^{e_0} \cdots (d, d^{e_1})^{e_d} \cdots f^{e_r}$ for $i = 0, 1, \cdots, k_d/m_1$ 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 \(wa^{r_1} \cdots d^{r_u} \cdots f^{r_1}\) into \(wa^{r_1} \cdots (dw^{u})^{r_d} \cdots f^{r_1}\) where \(q_j = \max (1, m_j/k_d)\) and \(u = 0, 1, \ldots , m_j/q_j\). There are \(\min (k_d, m_j)\) such automorphisms for the generator \(d\) and for \(j = 1, \ldots , n\).

We note now that \(c, \ldots , f\) 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 \(c, \ldots , f\) suppose \([a, d] = [a, b]^k\) and \([d, b] = [a, b]^t\) modulo \((w_2) \otimes \cdots \otimes (w_n)\). Then \([a, db^{m_1-t}a^{m_1-t}] = e = [db^{m_1-t}a^{m_1-t}, b]\) and \(db^{m_1-t}a^{m_1-t}\) 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 \(b, c, \ldots , f\); then for \(u = 0, 1, \ldots , k_b/q\) there are \(k_b/q\) elements \(ab^{u_q}\) 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 \(ab^{u_q}\) if necessary there are by Lemma 3 at least \(k_b/q(h+1)\) distinct automorphisms sending \(g = wa^{r_1} \cdots f^{r_1}\) into \(w(ab^{u_q})^{r_1} \cdots f^{r_1}\). 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 \(k_a \cdots k_f (m_2 \cdots m_n) x m_2 y\) 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 \(m_2^2 x y \geq m_1\), which is true except for \(m_1 = 8, 16, 32\) and 64 when \(m_2 \geq p\). For then \(m_2^2 \geq m_1\) unless \(m_1 \geq p^3\); but in this case \(p^{(m_1)^{1/2}} > m_1\) whence \((m_1)^{1/2} > h+1, m_1/m_2 > (m_1/m_2)^{1/2}(h+1))\) and finally \(x\) and \(y\) being both greater than or equal to \(m_1/[m_2(h+1)]\) we see that \(xy \geq m_1/m_2^2\).

We consider now the case where \(m_2 = 1\) and first let \(m_1 = p^{2k}\) for \(k = 1, 2, 3, \ldots \). Then \(p^k > h+1\) (except when \(m_1 = 4, 9, 16\)) and \(p^{2k-1}/(h+1) > p^{k-1}\) whence \(x\) and \(y\) are greater than or equal to \(p^k\) and \(xy \geq m_1\). 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 \(xy \geq m_1/p\). 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 \(m_2 \geq p\).
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 \(b\), \(ba\), \(b^3a\), and \(b^{n-1}\) 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 \(G(p^k) \subseteq G'\), 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 automorphism.

We shall suppose that \(k\) is the smallest integer such that \(G(p^k) \subseteq G'\). Let \(z\) in \(G'\) have maximum order \(p^r\); then \(r \leq k\) since \(G(p^k) \subseteq G'\) 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 \(g \in \Phi(G)\) such that \(g^s \in G'\). 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 con-
tain $h$. 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 $\prod g_2^q g_2$, and then by (1b) and (1c), $[h, g] = \prod [h_i, g]^q$, 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 $p^r$ 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 $P' \subseteq P \cap G'$; 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 $p^{t+s}$, then there must be a relation of the form $h^p^r = k^p^r$ mod $G'$ where $t > U \geq V < S$. Then if $w = (kh^{-p_{m-1}})$, $w^p = k^p h^{-p_{m-1}} \in G'$. But since $[h, w] = [h, k] = [h, k]^r \in P'$. Hence $P' = P \cap G'$.

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 $Q \cap P = G'$ 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**

