THE EXISTENCE OF OUTER AUTOMORPHISMS OF SOME GROUPS, II

RIMHAK REE

Developing the idea used in [3], we prove a few results concerning the “size” of the groups of automorphisms of some nilpotent groups.

Theorem 1. If $G$ is a finite $p$-group every element of which satisfies the equation $x^p = e$ (the unit element of $G$), and if $G$ is of order greater than $p^2$, then the order of $G$ divides the order of the group of automorphisms of $G$.

Proof. First we consider the case where $G$ is not abelian. Evidently there exists a normal subgroup $N$ of $G$ which contains the center $Z$ of $G$ such that $G/N$ is cyclic of order $p$. Let $a$ be an element in $G$ such that $aN$ generates the group $G/N$, and let $Z_N$ be the center of $N$. Clearly $Z_N$ is a normal subgroup of $G$, and $Z \leq Z_N$. The mapping $\phi: Z_N \to Z_N$ defined by $\phi(x) = [x, a] = xax^{-1}a^{-1}$ is easily seen to be a homomorphism into. Denote by $\phi(Z_N)$ and $K$ the image and the kernel of $\phi$ respectively. Since $Z_N / K \cong \phi(Z_N)$ and $Z \leq K$, we have

$$\langle Z : 1 \rangle \mid \langle Z_N : \phi(Z_N) \rangle.$$ 

Denote now by $\mathfrak{A}$ and $\mathfrak{I}$ the group of automorphisms of $G$ and the group of inner automorphisms of $G$ respectively. For any $x \in Z_N$ define a mapping $\sigma(x): G \to G$ by

$$(a^ru)^{\sigma(x)} = (ax)^r u,$$

where $u \in N$, and $r$ is an integer modulo $p$. We shall show that $\sigma(x)$ is an automorphism of $G$. We have, for $u, v \in N$,

$$(a^rua^sv)^{\sigma(x)} = (a^{r+s}[a^{-s}, u]uv)^{\sigma(x)} = (ax)^{r+s}[a^{-s}, u]uv,$$

$$(a^ru)^{\sigma(x)}(a^sv)^{\sigma(x)} = (ax)^r u(ax)^{\sigma(x)} = (ax)^{r+s}[ax^{-s}, u]uv.$$ 

Since, however, $(ax)^{-s} = a^{-s}x'$ with $x' \in Z_N$, we have $[(ax)^{-s}, u] = [a^{-s}, u]$. It follows that $(a^rua^sv)^{\sigma(x)} = (a^ru)^{\sigma(x)}(a^sv)^{\sigma(x)}$. If $(a^ru)^{\sigma(x)} = (ax)^{-s}u = e$ then $a^rx' = e$. Hence $r \equiv 0 \pmod{p}$, $u = e$, and $a^ru = e$. Now any element in $G$ is clearly an image under the mapping $\sigma(x)$. Therefore $\sigma(x)$ is an automorphism of $G$. Since $(a^x)^{\sigma(y)} = (ax)^{\sigma(y)} = ayx = a^{\sigma(y)}$ for any $x, y \in Z_N$ and since $x = e$ if $\sigma(x)$ is the identity automorphism of $G$, it follows that the mapping $\sigma: Z_N \to \mathfrak{A}$ is an isomorphism into. We shall show that

Received by the editors, March 5, 1957.
Indeed, if $\sigma(x)$ is an inner automorphism induced by $y = axu \in G$, then $y = y^\sigma(x) = (ax)^r u$ and hence $(ax)^r = a^r$. If $r \equiv 0 \pmod{p}$ then $ax = a$, $x = e$, and hence $\sigma(x) \in \sigma(\phi(Z_N))$. If $r \equiv 0 \pmod{p}$ then $y \in \mathbb{N}$, and since $y^\sigma(x) = yby^{-1} = b$ for all $b \in \mathbb{N}$, we have $y \in Z_N$. Now $ax = a^\sigma(x) = yay^{-1}$, $x = \phi(axay)$, and hence $\sigma(x) \in \sigma(\phi(Z_N))$ and, for any $x$ in $Z_N$, $\sigma(\phi(x))$ is the inner automorphism induced by $axa^{-1}$. Hence (2) is proved. From (2) we have

$$\sigma(Z_N) \mathfrak{S} / \mathfrak{S} \cong \sigma(Z_N) / (\sigma(Z_N) \cap \mathfrak{S})$$

(3)

$$\cong Z_N / \phi(Z_N),$$

since $\sigma$ is an isomorphism into. Since $\sigma(Z_N) : \mathfrak{S}$ divides $(\mathfrak{S} : \mathfrak{S})$, from (1) we have $(Z : 1) | (\mathfrak{S} : \mathfrak{S})$. Hence $(G : 1) = (G : Z)(Z : 1) = (\mathfrak{S} : 1)(Z : 1)$ divides $(\mathfrak{S} : \mathfrak{S})(\mathfrak{S} : 1) = (\mathfrak{S} : 1)$.

Now consider the case where $G$ is abelian. The order of $\mathfrak{S}$ for this case is well-known [5, p. 112]. It is equal to $(p^d - 1)(p^d - p) \cdots (p^d - p^{d-1})$, where $p^d$ denotes the order of $G$. Since $d \geq 3$, the theorem follows for $G$ abelian. The proof of Theorem 1 is thus complete.

Now let $G$ be a finitely generated torsion-free nilpotent group. Following [2] we define an $F$-series of $G$ as a finite series $G = F_1 > F_2 > \cdots > F_d > F_{d+1} = \{e\}$ of normal subgroups $F_i$ of $G$ such that $[G, F_i] \leq F_{i+1}$ for all $i$ and such that the factor groups $F_i / F_{i+1}$ are infinite cyclic. It is known [2] that the group $G$ always possesses an $F$-series and that the length $d$ of any $F$-series of $G$ is an invariant of $G$, called the dimension of $G$. Any $d$ elements $f_1, f_2, \cdots, f_d$ in $G$, where $d = \dim G$, are said to form an $F$-basis if the series $G = F_1 > F_2 > \cdots > F_d > \{e\}$, where $F_i$ is the subgroup generated by $f_1, \cdots, f_d$, is an $F$-series of $G$. Given any $F$-basis $f_1, \cdots, f_d$, every element $a$ in $G$ is written uniquely as $a = f_1^{r_1} f_2^{r_2} \cdots f_d^{r_d}$, where $r_1, r_2, \cdots, r_d$ are integers. Thus $G$ becomes a linearly ordered group if we order elements in $G$ lexicographically with respect to $r_1, r_2, \cdots, r_d$. (It was proved in [4] that every linear ordering of $G$ which makes $G$ an ordered group is obtained in this way.) We shall call a linear ordering of $G$ obtained in the above manner regular if the group $F_2$ generated by $f_2, \cdots, f_d$ contains the center of $G$, or if $G$ is abelian.

**Theorem 2.** Let $G$ be a finitely generated torsion-free nilpotent group and let $\prec$ be a linear ordering in $G$ by which $G$ becomes an ordered group. Then the group $\mathfrak{A}$ of automorphisms of $G$ which preserve the ordering $\prec$ is a finitely generated torsion-free nilpotent group. If the ordering $\prec$ is regular and if $\dim G > 2$, then $\dim A \geq \dim G$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. It was shown in [4] that can be obtained from an \( F \)-basis \( f_1, \ldots, f_d \) of \( G \). Denote by \( F_i \) the group generated by \( f_1, \ldots, f_d \). It is clear that the set-theoretic differences \( F_i - F_{i+1} \), \( i = 1, 2, \ldots, d - 1 \), can be characterized as \( C \)-classes in the sense of [4], i.e., classes of comparable elements with respect to the ordering \(<\). Since \( G \) has only a finite number of \( C \)-classes it follows easily that every \( C \)-class \( F_i - F_{i+1} \) and hence every \( F_i \) is invariant under all automorphisms \( \sigma \) of \( G \) which preserve \(<\). We infer that for every \( i \), \( f_i^r \) is of the form \( f_i^r = f_{i+1}^r \cdots f_d^r \), where \( a, \ldots, k \) are integers. In particular, \( f_d^r = f_d \).

Denote by \( \mathfrak{A}_t \), \( t = 1, 2, \ldots \), the subgroup of \( \mathfrak{A} \) consisting of all \( \sigma \in \mathfrak{A} \) such that \( f_i^r \equiv f_i \pmod{F_{i+1}} \) for \( i = 1, 2, \ldots, d \) (we set \( F_{d+1} = F_{d+2} = \cdots = \{e\} \)). Then what we have shown above can be expressed as \( \mathfrak{A} = \mathfrak{A}_1 \), and obviously we have \( \mathfrak{A}_d = 1 \). We shall now show that \( [\mathfrak{A}, \mathfrak{A}_t] \leq \mathfrak{A}_{t+1} \) for all \( t \), and that the factor groups \( \mathfrak{A}_t/\mathfrak{A}_{t+1} \) are free abelian groups of finite ranks. Let \( \sigma \in \mathfrak{A}_t \), \( \rho \in \mathfrak{A}_t \). Then for any fixed \( i \) we have \( f_i^r \equiv f_i x, f_i^r \equiv f_i y \pmod{F_{i+1}} \), where \( x \in F_{i+1}, y \in F_{i+1} \). Since \( x^\sigma \equiv x^\rho \equiv x, y^\rho \equiv y \pmod{F_{i+1}} \), we have easily

\[
\begin{align*}
 f_i^{\sigma, \rho} &= f_i y^{-1} x^{-1} y x \pmod{F_{i+1}}. 
\end{align*}
\]

But from \( [G, F_{i+1}] \leq F_{i+1} \) we have \( y^{-1} x^{-1} y x \in F_{i+1} \). Hence \( f_i^{\sigma, \rho} \equiv f_i \pmod{F_{i+1}} \) for all \( i \). This proves \( [\mathfrak{A}, \mathfrak{A}_t] \leq \mathfrak{A}_{t+1} \). In order to prove that \( \mathfrak{A}_t/\mathfrak{A}_{t+1} \) is a free abelian group of finite rank, let \( \sigma \in \mathfrak{A}_t \) and set

\[
\begin{align*}
 f_i^\sigma &= f_i^{a_i} \pmod{F_{i+1}},
\end{align*}
\]

where \( a_1, \ldots, a_d \) are integers. It is easily seen that the mapping \( \sigma \rightarrow (a_1, \ldots, a_d) \) is a homomorphism of \( \mathfrak{A}_t \) into the additive group \( M \) of all \( d \)-tuples of integers (with the addition defined componentwise), and that the kernel of the homomorphism is exactly \( \mathfrak{A}_{t+1} \). Therefore \( \mathfrak{A}_t/\mathfrak{A}_{t+1} \) is isomorphic to a subgroup of \( M \). Our assertion is now clear.

By refining the series \( \mathfrak{A} \supseteq \mathfrak{A}_2 \supseteq \cdots \supseteq \mathfrak{A}_d \), we obtain easily an \( F \)-series of \( \mathfrak{A} \), and hence \( \mathfrak{A} \) is a finitely generated torsion-free nilpotent group. Thus the first part of the theorem is proved.

We now proceed to prove the second part. If \( G \) is abelian, then \( \mathfrak{A} \) is isomorphic to the multiplicative group of all \( d \times d \) triangular matrices with integral entries and with 1's on the principal diagonal. By arguing the same way as in the above, we see easily that \( \dim \mathfrak{A} = d(d-1)/2 \), where \( d = \dim G \). Since we assume \( d > 2 \), we have \( \dim \mathfrak{A} \geq \dim G \), and hence the second part is proved for \( G \) abelian.

If \( G \) is not abelian, we proceed as in the proof of Theorem 1 by setting \( a = f_1, N = F_2 \). Let \( Z, Z_N, \phi, \) and \( K \) be as in the proof of Theorem
1. It is known [2] that \( G/Z \) is torsion-free. Therefore \( Z_N/K \cong \phi(Z_N) \) and \( Z \leq K \) imply

\[
\dim Z \leq \dim Z_N - \dim \phi(Z_N).
\]

We shall show that the automorphisms \( \sigma(x) \) of \( G \) defined by \((a^ru)^{\sigma(r)} = (ax)^ru\), where \( u \in N \), preserve the ordering \(<\) obtained from the \( F \)-basis \( f_1, \ldots, f_d \). This is seen as follows: \( a^ru > e \) implies \( r > 0 \) or \( r = 0 \) and \( u > e \). If \( r > 0 \) then \((a^ru)^{\sigma(r)} = (ax)^ru = a^x'ru > e\), since \( x'u \in N \). If \( r = 0 \) then \((a^ru)^{\sigma(r)} = u > e\). Thus \( \sigma(x) \) preserves the ordering \(<\).

Also every inner automorphism preserves the ordering \(<\). Since \( G \) is linearly ordered, we can prove (2) by observing that \( \sigma(x)^r = a^r \) with \( r \neq 0 \) implies \( ax = a, x = e \). From (2) we have (3) as before. By (3) and a theorem of Hirsch [1, Theorem 2.23], we may prove easily that \( \dim Z_N - \dim \phi(Z_N) \leq \dim A - \dim Z \). Then from (4) it follows that \( \dim Z \leq \dim A - \dim Z \). Since \( \dim G - \dim Z = \dim Z \), we have the desired result \( \dim G \leq \dim A \). Thus Theorem 2 is proved.

The method of proof used in the above may be applied to similar but more general nilpotent groups, namely nilpotent groups \( G \) which have decreasing series of normal subgroups \( G = G_1 \supset G_2 \supset \cdots \supset G_d \supset \{e\} \) such that \([G, G_i] \leq G_i+1 \) for all \( i \) and such that \( G_i/G_i+1 \) are all isomorphic to the additive group of an integral domain.

By analyzing the main points of the above method we can prove more:

**Theorem 3.** Let \( p \) be a prime. If a group \( G \) possesses a normal subgroup \( N \) of index \( p \) whose center \( Z_N \neq \{e\} \) is of order \( < p^p \) and if every element \( \neq e \) in \( Z_N \) is of order \( p \), then there exists an outer automorphism of \( G \).

**Proof.** Let \( a \in G \) be such that \( aN \) generates the group \( G/N \). The mapping \( \alpha: Z_N \rightarrow Z_N \) defined by \( \alpha(x) = axa^{-1} \) is an automorphism of \( Z_N \) of order \( p \). Define a homomorphism \( \beta \) of \( Z_N \) into itself by

\[
\beta(x) = x\alpha(x)\alpha^2(x) \cdots \alpha^{p-1}(x).
\]

Then we see easily that \((ax)^p = \beta(x)a^p\). The argument used in the proof of Theorem 1 shows that for any \( x \in Z_N \) such that \( \beta(x) = e \) there exists an automorphism \( \sigma(x) \) of \( G \) such that \( a^{\sigma(r)} = ax \) and \( u^{\sigma(x)} = u \) for all \( u \in N \). Further \( \sigma(x) \) is an inner automorphism of \( G \) if and only if \( x = (1-\alpha)y \) with \( y \in Z_N \), where \( 1 \) denotes the identity automorphism of \( Z_N \). Therefore our theorem is proved if we can derive a contradiction from the assumption that \( x \in Z_N \) is of the form \( x = (1-\alpha)y \), \( y \in Z_N \), whenever \( \beta(x) = e \). Now every element \( \neq e \) of the abelian group \( Z_N \) is of order \( p \). Hence \( 1 = \alpha^p \) implies \( (1-\alpha)^p = 0 \), where \( 0 \)
denotes the homomorphism of $Z_N$ into itself which carries every element into $e$. Hence

$$\beta = 1 + \alpha + \cdots + \alpha^{p-1} = (1 - \alpha)^{p-1}. \quad (5)$$

Now, for $i=1, 2, \cdots, p$, let

$$Z_i = \{x \mid x \in Z_N, (1 - \alpha)^i x = e\}.$$

Then we have $Z_i \supseteq Z_{i-1}$. We shall show that the equality can not hold. Suppose $Z_i = Z_{i-1}$ for some $i > 0$. Now for any $x \in Z_N$ we have

$$(1 - \alpha)^i((1 - \alpha)^{p-i}x) = (1 - \alpha)^{p-i}x = e.$$  

Thus the assumption $Z_i = Z_{i-1}$ implies that

$$(1 - \alpha)^{i-1}((1 - \alpha)^{p-i}x) = (1 - \alpha)^{p-i}x = e$$

for all $x \in Z_N$. Therefore from (5) it follows that $\beta(x) = e$, and hence, by our assumption, that every $x \in Z_N$ is of the form $x = (1 - \alpha)y$. From this it follows easily that every element $x \in Z_N$ is of the form $x = (1 - \alpha)^{p}z = e$. Therefore $Z_N = \{e\}$, contradicting our assumption $Z_N \not= \{e\}$. Therefore $Z_i \not= Z_{i-1}$. Similarly we may prove $Z_1 \not= \{e\}$. Now from the fact that the series $Z_N = Z_p > Z_{p-1} > \cdots > Z_1 > \{e\}$ is strictly decreasing it follows that the order of $Z_N$ is $\geq p^p$. This again contradicts our assumption that the order of $Z_N$ is $< p^p$. This completes the proof.

References


The University of British Columbia