A NOTE ON THE AUTOMORPHISM GROUP
OF A $p$-GROUP

RALPH FAUDREE

The relation between the order of a $p$-group and its automorphism group has been the subject of several papers, see [1], [2], and [4]. The existence of outer-automorphisms of a finite $p$-group was proved by Gaschütz [3], but the question of the size of the automorphism group of a $p$-group still remains. In this paper we will prove that the order of the automorphism group of a finite nonabelian nilpotent class two group is divisible by the order of the group. It should be noted that the above result is stated in [4], but the proof is invalid; see [2].

In this paper $G$ will denote a finite nonabelian nilpotent class two $p$-group. $Z$, $G'$, $\Phi$ and $A(G)$ will denote the center, derived subgroup, Frattini subgroup and automorphism group of $G$. $S$ will denote a set of elements $\{a, b, \ldots, f\} \subset G$ such that $G/G'=(a \cdot G') \times \cdots \times (f \cdot G')$. Let $k_a \geq k_b \geq \cdots \geq k_f$ and $k'_a, \ldots, k'_f$ be the orders of $a, b, \ldots, f$ modulo $G'$ and $Z$ respectively. If $r$ is a rational number then $\lceil r \rceil = \max \{1, r\}$.

**Lemmas on automorphisms.** The following lemma can be found in [4]. The lemma as stated in [4] is incorrect and leads to the error of that paper, but the proof is correct for the lemma as stated below.

**Lemma 1.** If $z$ in $G$ commutes with $a, b, c, e, \ldots, f$, $(dz)^{k_d} = d^{k_d}$ and $G = Gp(a, b, \ldots, dz, \ldots, f)$ then the map sending $w a \cdots f$ into $w a^{r_a} \cdots (dz)^{r_d} \cdots f^{r_f}$ $(0 \leq r_a \leq k_a, w \in G')$ determines an automorphism of $G'$.

The following lemma is slightly more general than a lemma in [1], but the proof is the same so it is not included here.

**Lemma 2.** Suppose

(i) $G' = (u) \times U$ where $|u| = m_1 > m' \geq \exp U$,

(ii) $[g, h] = u$ and $h^{m_1, m''} = 1$,

(iii) $m'' = m'$ if $p$ is odd and $m'' = \max \{2, m'\}$ if $p = 2$.

Let $H = Gp(g, h)$ and $L = \{x \in G \mid [g, x], [h, x] \in U\}$. Then $G = HL$ and the correspondence

Received by the editors August 6, 1967.

Supported by NSF Grant GP 7029.
defines an automorphism \( \sigma \) of \( G \) which leaves the elements of \( Z \) fixed. \( \sigma \) has order \( \frac{m_1}{m''} \) modulo the central automorphisms of \( G \).

The following is well known.

**Lemma 3.** The normal subgroup \( N \) of \( A(G) \) of all automorphisms leaving every coset of \( G \) with respect to \( \Phi \) fixed is a \( p \)-group.

**Theorem.** If \( G \) is a finite nonabelian nilpotent class two \( p \)-group, then the order of \( G \) divides the order of \( A(G) \).

**Proof.** We can assume that \([a, b] = w_1\), \( G' = (w_1) \times \cdots \times (w_n)\) where \(|w_i| = m_i\) \((1 \leq i \leq n)\) and \( m_1 \geq m_2 \geq \cdots \geq m_n\). Note that \( k_a \geq k_b \geq m_1\).

If \( m_1|k_d\), then the map sending \( g = w^{a_1} \cdots d^{r_1} \cdots f^{r_1} \) into \( w^{a_1} \cdots (d \cdot d^{m_1})^{r_1} \cdots f^{r_1} \) \((w \in G, t = 1, \cdots, k_d/m_1)\) is an automorphism of \( G \) leaving \( d \) invariant by Lemma 1. Also by Lemma 1 there is an automorphism sending \( w^{a_1} \cdots f^{r_1} \) into \( w^{a_1} \cdots (d \cdot w^{m_1})^{r_1} \cdots f^{r_1} \) where \( q_j = \left\lfloor m_j/k_d \right\rfloor \) and \( u = 1, \cdots, m_j/q_j \). There are \( \min\{k_d, m_j\} \) such automorphisms.

Let \( T \) be the subgroup of automorphisms of \( G \) generated by the above central automorphisms. Then

\[
|T| = \prod_{d \in \Phi} \left( \left\lfloor k_d/m_1 \right\rfloor \cdot \prod_{i=1}^n \min\{k_d, m_i\} \right) \geq k_a \cdots k_f \cdot m_2 \cdot m_3 \cdots m_n.
\]

It is therefore sufficient to exhibit a subgroup \( U \) of \( A(G) \) such that \( UT \) is a \( p \)-group and \(|UT: T| \geq m_1/m_2\).

We will define five automorphisms \( \sigma_1, \sigma_2, \tau_1, \tau_2 \) and \( \theta \) of \( G \), let \( U = Gp(\sigma_1, \sigma_2, \tau_1, \tau_2, \theta) \) and verify that \( U \) satisfies the above properties. Let \( H = Gp(T, \sigma_1, \sigma_2) \) and \( R = Gp(T, U) \). In every case \( R \) will be a subgroup of \( N \) or an extension of a subgroup of \( N \) by an element of order \( p \), so \( R \) will be a \( p \)-group by Lemma 3.

There is no loss of generality in assuming

\[
a^{k_a} = w_1^{t_a} \mod (w_2 \times \cdots \times w_n), \quad b^{k_b} = w_1^{t_b} \mod (w_2 \times \cdots \times w_n),
\]

and \( k_a = l k_b \) where \( t_a \) and \( t_b \) are powers of \( p \).

The map

\[
a \to b^{m_1} a,
\]

\[
d \to d, \quad \forall d \in S \setminus \{a\}
\]

determines a central automorphism \( \sigma_1 \) of \( G \) by Lemma 1 for \( m_1 \).
The smallest power of $c_1$ in $T$ is $k_b/m_1$. Likewise the map
\[
\begin{align*}
  b &\rightarrow ba^{l_a}, \\
  d &\rightarrow d, \quad \forall d \in S \setminus \{b\}
\end{align*}
\]
determines a central automorphism $c_2$ of $G$ if
\[
l_a = \max\{m_1, k_a m_1/k_b t_a, k_a m_2/k_b\}.
\]
The smallest power of $c_2$ in $T$ is $\min\{k_a/m_1, k_b t_a/m_1, k_b/m_2\}$.

By Lemma 2 there is an automorphism $\tau_1$ leaving $b$ fixed which
has order
\[
\min\{[[m_1 t_b/k_b]], [[m_2/k_b m_2]] \text{ and possibly } m_1/2 \text{ if } p = 2\}
\]
modulo the central automorphisms of $G$. By the same lemma there is
an automorphism $\tau_2$ of $G$ leaving $a$ fixed which has order
\[
\min\{[[m_1 t_a/k_a]], [[m_2/k_a m_2]], \text{ and possibly } m_1/2 \text{ if } p = 2\}
\]
modulo the central automorphisms of $G$.

The automorphism $\theta$ will be the identity for the most general cases
and will be defined differently for each exceptional case.

To make the orders of $c_1$, $c_2$, $\tau_1$ and $\tau_2$ as large as possible we want
to choose $a$ and $b$ such that $t_a$ and $t_b$ are maximal. Consider the following
three cases for the relationship between $t_a$ and $t_b$
I. $t_b = rt_a$,
II. $t_a = rt_b$, $r \geq l$,
III. $t_a = rt_b$, $1 < r < l$.

In case I if you replace $b$ by $a^{-l_\tau}$, then $t_b = m_1$ unless $p = 2$, $k_a = k_b = m_1$, and $r = l = 1$; then $t_b = m_1/2$. In case II if you replace $a$ by $b^{-l_\tau}$, $t_a = m_1$ unless $p = 2$, $k_a = k_b = m_1$ and $r = l = 1$; then $t_b = m_1/2$. In case III if you replace $b$ by $ba^{-l_\tau}$, then $t_b = m_1/r$.

We will now consider all values of $k_a$, $k_b$, $m_1$, $m_2$ and $p$ except when $p = 2$ and $k_a = k_b = m_1$, or $p = 2$, $k_a > m_1$, $k_b = m_1$ and $m_2 = 1$. In case I consideration of the orders of $c_1$ and $\tau_1$, in case II consideration of the orders of $c_2$ and $\tau_2$, and in case III consideration of the orders of $c_2$ and $\tau_1$ modulo appropriate subgroups give $[R: T] \geq m_1/m_2$.

Now consider the case where $k_a = k_b = m_1$ and $p = 2$. Due to symmetry we must consider only case I. If $m_2 > 1$ then $\tau_1$ has order $m_1/m_2$ modulo $H$ and hence $[R: T] \geq m_1/m_2$. If $m_2 = 1$, $t_a \geq 2$, $m_1 > 2$ then consideration of the orders of $\tau_2$ and $\tau_1$ give that $[R: T] \geq m_1$. Assume $m_2 = 1$ and $t_a = 1$. There is no loss of generality in assuming $t_b = m_1/2$.  

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Then using the construction given in Lemma 2 it can be shown that the map \( a \to ba \) and \( b \to b \) determines an automorphism \( \theta \) of order \( m_1 \) modulo \( T \), and thus \([R: T] \geq m_1\). If \( m_1 = 2 \) and \( a^2 = b^2 = w_1 \), the map \( a \to b \) and \( b \to a \) determines an automorphism \( \theta \) of \( G \). If \( m_1 = 2 \) and \( a^2 = w, \ b^2 = 1 \), the map \( a \to a, \ b \to ab \) determines an automorphism \( \theta \). In either case the above definition of \( \theta \) gives \([R: T] \geq m_1\).

Assume \( k_a > m_1, \ k_b = m_1 \) and \( m_2 = 1 \). In case II, consideration of the orders of \( \sigma_2 \) and \( \tau_2 \) give \([R: T] \geq m_1\) and in case III, consideration of the orders of \( \sigma_2 \) and \( \tau_1 \) give \([R: T] \geq m_1\). Case I can be handled just as in the previous paragraph.

References