A NOTE ON THE AUTOMORPHISM GROUP OF A p-GROUP[1]

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', Φ and $A(G)$ will denote the center, derived subgroup, Frattini subgroup and automorphism group of G. S will denote a set of elements $\{a, b, \cdots, f\} \subset G$ such that $G/G' = (a\cdot G') \times \cdots \times (f\cdot G')$. Let $k_a \geqq k_b \geqq \cdots \geqq k_f$ and $k_a', \cdots, k_f'$ be the orders of $a, b, \cdots, f$ modulo G' and Z respectively. If r is a rational number then $[[r]] = \max\{1, r\}$.

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 $a, b, c, e, \cdots, f$, $(dz)^{k_d} = d^{k_d}$ and $G = Gp(a, b, \cdots, dz, \cdots, f)$ then the map sending $wa^{r_a} \cdots f^{r_f}$ into $wa^{r_a} \cdots (dz)^{r_d} \cdots f^{r_f}$ $(0 \leqq r_a \leqq k_a, w \in G')$ 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* $|u| = m_1 > m' \geqq \exp U$,

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

(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.

[1] Supported by NSF Grant GP 7029.

$$g \to gh^{m''}, \qquad h \to h, \qquad x \to x, \qquad x \in L,$$

defines an automorphism σ of G which leaves the elements of Z fixed. σ has order 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 Φ 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 $|w_i| = m_i$ $(1 \leqq i \leqq n)$ and $m_1 \geqq m_2 \geqq \cdots \geqq m_n$. Note that $k_a \geqq k_b \geqq m_1$.

If $m_1 | k_d$, then the map sending $g = wa^{r_a} \cdots d^{r_d} \cdots f^{r_f}$ into $wa^{r_a} \cdots (d \cdot d^{tm_1})^{r_d} \cdots f^{r_f}$ $(w \in G,\ t = 1, \cdots, k_d/m_1)$ is an automorphism of G leaving (d) invariant by Lemma 1. Also by Lemma 1 there is an automorphism sending $wa^{r_a} \cdots f^{r_f}$ into $wa^{r_a} \cdots (dw_j^{uq_j})^{r_d} \cdots f^{r_f}$ where $q_j = [[m_j/k_d]]$ 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

$$|T| = \prod_{d \in s} \left([[k_d/m_1]] \cdot \prod_{j=1}^{n} \min\{k_d, m_j\} \right) \geqq k_a \cdots k_f \cdot m_2^2 \cdot m_3 \cdots m_n.$$

It is therefore sufficient to exhibit a subgroup U of $A(G)$ such that UT is a p-group and $[UT\colon T] \geqq m_1/m_2$.

We will define five automorphisms σ_1, σ_2, τ_1, τ_2 and θ 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

$$a^{k_a} = w_1^{t_a} \bmod(w_2 \times \cdots \times w_n), \qquad b^{k_b} = w_1^{t_b} \bmod(w_2 \times \cdots \times w_n),$$

and $k_a = lk_b$ where t_a and t_b are powers of p.

The map

$$a \to b^{m_1} a,$$
$$d \to d, \qquad \forall d \in S \backslash \{a\}$$

determines a central automorphism σ_1 of G by Lemma 1 for m_1

$=\max\{m_1, k_bm_1/k_at_b, k_bm_2/k_a\}$. The smallest power of σ_1 in T is k_b/m_1. Likewise the map

$$b \to ba^{l_a},$$
$$d \to d, \qquad \forall d \in S\backslash\{b\}$$

determines a central automorphism σ_2 of G if

$$l_a = \max\{m_1, k_am_1/k_bt_a, k_am_2/k_b\}.$$

The smallest power of σ_2 in T is $\min\{k_a/m_1, k_bt_a/m_1, k_b/m_2\}$.

By Lemma 2 there is an automorphism τ_1 leaving b fixed which has order

$$\min\{[[m_1t_b/k_b]], [[m_1^2/k_bm_2]] \text{ and possibly } m_1/2 \text{ if } p=2\}$$

modulo the central automorphisms of G. By the same lemma there is an automorphism τ_2 of G leaving a fixed which has order

$$\min\{[[m_1t_a/k_a]], [[m_1^2/k_am_2]], \text{ and possibly } m_1/2 \text{ if } p=2\}$$

modulo the central automorphisms of G.

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

To make the orders of σ_1, σ_2, τ_1 and τ_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. $t_a=rt_b$, $r\geqq l$,

III. $t_a=rt_b$, $1<r<l$.

In case I if you replace b by a^{-lr_b}, 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^{-r/l_a}, $t_a=m_1$ 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 $ba^{-l/r}$, 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 σ_1 and τ_1, in case II consideration of the orders of σ_2 and τ_2, and in case III consideration of the orders of σ_2 and τ_1 modulo appropriate subgroups give $[R: T]\geqq m_1/m_2$.

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 τ_1 has order m_1/m_2 modulo H and hence $[R: T]\geqq m_1/m_2$. If $m_2=1$, $t_a\geqq 2$, $m_1>2$ then consideration of the orders of τ_2 and τ_1 give that $[R: T]\geqq m_1$. Assume $m_2=1$ and $t_a=1$. There is no loss of generality in assuming $t_b=m_1/2$.

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 θ of order m_1 modulo T, and thus $[R: T] \geqq m_1$. If $m_1 = 2$ and $a^2 = b^2 = w_1$, the map $a \to b$ and $b \to a$ determines an automorphism θ of G. If $m_1 = 2$ and $a^2 = w$, $b^2 = 1$, the map $a \to a$, $b \to ab$ determines an automorphism θ. In either case the above definition of θ gives $[R: T] \geqq m_1$.

Assume $k_a > m_1$, $k_b = m_1$ and $m_2 = 1$. In case II, consideration of the orders of σ_2 and τ_2 give $[R: T] \geqq m_1$ and in case III, consideration of the orders of σ_2 and τ_1 give $[R: T] \geqq m_1$. Case I can be handled just as in the previous paragraph.

References

1. J. E. Adney and Ti Yen, *Automorphisms of a p-group*, Illinois J. Math. **9** (1965), 137–143.

2. C. Godino, *Outer automorphisms of certain p-groups*, Proc. Amer. Math. Soc. **17** (1966), 922–929.

3. W. Gaschütz, *Nichtabelsche p-Gruppen besitzen aüssere p-Automorphisms*, J. Algebra **4** (1966), 1–2.

4. E. Schenkman, *Outer automorphisms of some nilpotent groups*, Proc. Amer. Math. Soc. **6** (1955), 6–11.

University of Illinois