ON THE POWER OF A PRIME DIVIDING THE ORDER OF A GROUP OF AUTOMORPHISMS[1]

J. E. ADNEY

1. **Introduction and notation.** A natural question that arises concerning a finite group G and its group of automorphisms $A(G)$ is the relationship between their orders. P. Hall and G. Birkhoff [1] have obtained an upper bound on the order of $A(G)$ in terms of the order of G.

In this paper we shall be concerned with the power of the prime p that divides the order of $A(G)$ for those primes p that divide the order of G. For abelian groups Hilton [2] proved that if p^n divides the order of G, then $p^{n-1}(p-1)$ divides the order of $A(G)$. In the general case Herstein and Adney [3] proved that if p^2 divides the order of G, then p divides the order of $A(G)$. Scott [4] showed that if p^3 divides the order of G, then p^2 divides the order of $A(G)$.

The main theorem proved in this paper is as follows:

THEOREM. *Let G be a group of order $p^n g$ where $(p, g)=1$, p a prime, and let P denote a p-Sylow subgroup belonging to G. If P is abelian, then at least p^{n-1} divides the order of $A(G)$.*

A counterexample to the general conjecture that if p^n is the highest power of p that divides the order of G then p^{n-1} divides the order of $A(G)$ is the following: Let G be the group of all quadratic nonsingular matrices with elements from the Galois field with 19 elements then[2] $[G: 1]=(19^2-1)(19^2-19)$ and $[A(G): 1]=o(G)/3^2$.

NOTATION. In this paper we shall write group for finite group.

If G is a group, we denote by:

$Z(G)$ the center of G,

G' the commutator subgroup of G,

$A(G)$ the group of automorphisms of G,

$I(G)$ the group of inner automorphisms of G and $[G: 1]$ the order of G.

If H is a subgroup of G, we denote by $V_{G\to H}(G)$ the transferred group of G to H[5].

Presented to the Society, December 27, 1954; received by the editors May 16, 1955 and, in revised form, August 20, 1956.

[1] The following comprises part of a Ph.D. thesis written under the direction of Professor Marshall Hall and accepted by the Ohio State University. I wish, at the outset, to acknowledge my deep indebtedness to my former teacher.

[2] The author is indebted to the referee for this counterexample as well as the form of Theorem 2.2.

2. **Preliminaries.** We use the following theorems in the proof of the main theorem of this paper.

THEOREM 2.1. *If the finite group G has an abelian p-Sylow subgroup P, then we have*

$$G = G_1 \cdot P_1, \qquad G_1 \cap P_1 = 1$$

where G_1 is the kernel of the transfer of G into P and P_1 is the image group of G transferred into P. Moreover P_1 contains $P_2 = P \cap Z(G)$.

PROOF. This theorem is an immediate corollary of [**5**, pp. 142–143].

THEOREM 2.2. *Let G be a group, N a normal subgroup, and R a representative subgroup of G modulo N. All automorphisms α of R that satisfy the condition*

$$x^{-1}\alpha(x) \in Z(G) \cap R, \qquad x \in R$$

form a group $A_1 = A(G, N, R)$ of automorphisms of R that is mapped isomorphically onto a group $\bar{A}_1$ of central automorphisms of G by the correspondence: $\alpha \rightarrow \bar{\alpha}$ where $\bar{\alpha}(nr) = n\alpha(r)$ $n \in N$, $r \in R$, and A_1 is obtained from $\bar{A}_1$ by restriction to R. If R is abelian then $\bar{\alpha}$ is inner only if α is the identity.

PROOF. Clearly the α's form a group. By direct verification it follows that $\bar{\alpha}$ is an automorphism of G. Moreover from the definition of $\bar{\alpha}$ and the fact that α is an automorphism the correspondence $\alpha \rightarrow \bar{\alpha}$ is 1-1 and preserves products. This isomorphism together with $\bar{\alpha}(1 \cdot r) = \alpha(r)$ shows that $\bar{A}_1$ restricted to R gives A_1.

Now let R be abelian. If $\bar{\alpha}$ is an inner automorphism we have

$$\bar{\alpha}(nr) = nrz = gnrg^{-1} = n_1r_1nrr_1^{-1}n_1^{-1} \text{ where } g = n_1r_1.$$

But then

$$z = n^{-1}n_1r_1nr_1^{-1}rn_1^{-1}r^{-1} \in N \text{ since } N \text{ is normal and is abelian.}$$

Hence $z = 1$ and $\alpha(r) = r$.

3. **Construction of central automorphisms.** In the remainder of the paper it is assumed (i) that G is a group of order $p^n g$ where p is a prime, $(g, p) = 1$, and (ii) that a p-Sylow subgroup P of G is abelian. Let $P_1 = V_{G \rightarrow P}(G)$, $[P: 1] = p^n = p^{r+s}$, $[P_1: 1] = p^r$, $[P_2: 1] = p^s$ and let G_1 denote the kernel of the transfer of G into P. If p^m is the highest power of p dividing $[A_1: 1]$ where $A_1 = A(G, G_1, P_1)$ the two previous results show that $p^m \mid [A(G): I(G)]$. Since $p^r \mid [I(G): 1]$ it follows that

$p^{m+r} \mid [A(G):1]$. It is to be shown that $m+r \geqq n-1 = r+s-1$ or $m \geqq s-1$.

The main theorem has now been reduced to a consideration of the automorphisms α of an abelian p-group P_1, with a subgroup P_2 of order p^s, such that $x^{-1}\alpha(x) \in P_2$, for all $x \in P_1$.

We proceed to construct the required automorphisms of P_1 with the repeated application of the following:

Remark. An element of highest order in an abelian p-group may be chosen as a basis element [6].

Consider first $P_2 \subset P_1$. Let $\{a_1, \cdots, a_k\}$ be a basis for P_1 with a_i of order p^{m_i} and let a_1 be an element of highest order in P_1. If P_2 does not contain an element of highest order, then $a_1 \notin P_2$ and we define

$$\alpha(a_1) = a_1 \cdot b \qquad b \in P_2,$$

$$\alpha(a_i) = a_i \qquad i \neq 1.$$

We assert α is an automorphism of P. Suppose

$$(a_1 b)^{x_1} a_2^{x_2} \cdots a_k^{x_k} = 1 \text{ with not all } x_i = 0.$$

In particular $x_1 \neq 0$ for otherwise there would be a dependence among $\{a_2, a_3, \cdots, a_k\}$. Since

$$b \in P_2 \subset P_1,$$

we can write

$$b = a_1^{y_1} a_2^{y_2} \cdots a_k^{y_k}$$

with y_1 a multiple of p, since b is of lower order than a_1. Now we obtain

$$a_1^{x_1 + x_1 y_1} a_2^{x_2 + x_1 y_2} \cdots a_k^{x_k + x_1 y_k} = 1$$

and this implies

$$x_i + x_1 y_i \equiv 0 \pmod{p^{m_i}}.$$

But

$$x_1 + x_1 y_1 \equiv x_1(1 + y_1) \equiv 0 \pmod{p^{m_1}},$$

$$(1 + y_1, p) = 1$$

hence $x_1 = p^{m_1}$. Thus

$$a_2^{x_2} \cdots a_k^{x_k} = 1$$

and hence

$$x_2 = x_3 = \cdots = x_k = 0$$

so that

$$\{a_1 b, a_2, \cdots, a_k\} \text{ is a basis for } P.$$

By direct calculation one can show that for $a, a' \in P_1$

$$\alpha(aa') = \alpha(a)\alpha(a').$$

The product of any two such automorphisms is again an automorphism of the same type. For let

$$\beta(a_1) = a_1 \cdot b', \qquad b' \in P_2,$$
$$\beta(a_i) = a_i, \qquad i \neq 1,$$

then

$$\alpha\beta(a_1) = \alpha(a_1 b') = a_1 b\alpha(b') = a_1 \bar{b}$$

where

$$\bar{b} = b\alpha(b') \in P_2.$$

Therefore the set of automorphisms obtained as b runs over P_2 form a group. By direct calculation α has the same order as the corresponding $b \in P_2$ and we have at least p^s automorphisms.

If, on the other hand, P_2 contains an element of highest order in P_1, say a_1, we choose a basis for

$$P_1\{a_1, a_2, \cdots, a_k\}.$$

We can write $P_1 = \{a_1\} \times H_1$ where $\{a_1\}$ denotes the cyclic group of order p^{m_1} generated by a_1. By a proper choice of a basis for P_2 we can write $P_2 = \{a_1\} \times K_1$ such that $K_1 \subset H_1$.

Suppose now that $a_2 \in H_1$ is an element of highest order in H_1. Also suppose that K_1 does not contain an element of highest order of H_1. Then since $a_2 \notin K_1$, a_2 of order p^{m_2}, we define

$$\alpha(a_2) = a_2 \cdot b, \qquad b \in K_1,$$
$$\alpha(a_i) = a_i, \qquad i \neq 1, 2$$

and $\alpha(a_1)$ any of the $p^{m_1-1}(p-1)$ automorphisms of $\{a_1\}$. Apply the previous argument to H_1 and K_1. Since the direct product of automorphisms of the direct factors of a group is a subgroup of the automorphism group of the group itself, we have, therefore, p^{s-1} automorphisms. We can construct an additional automorphism of order p of P_1 by defining:

$$\beta(a_2) = a_2 \cdot a_1^{p^{m_1-1}},$$
$$\beta(a_i) = a_i, \qquad i \neq 2$$

β is an automorphism of P_1. Suppose

$$a_1^{x_1}(a_2 \cdot a_1^{p^{m_1-1}})^{x_2} a_3^{x_3} \cdots a_k^{x_k} = 1$$

with not all $x_i = 0$. In particular, $x_2 \neq 0$, for otherwise we would have a dependence among

$$a_1, a_3, \cdots, a_k.$$

Simplifying we get

$$a_1^{x_1 + x_2 p^{m_1-1}} a_2^{x_2} \cdots a_k^{x_k} = 1$$

but this implies

$$x_1 + x_2 p^{m_1-1} \equiv 0 \pmod{p^{m_1}}, \qquad x_i \equiv 0 \pmod{p^{m_i}}, \qquad i = 2, \cdots, k.$$

However, since $x_2 \neq 0$, we have a contradiction. Also β is of order p since $\{a_1\}$ is fixed elementwise by β and $a_1^{p^{m_1-1}}$ is of order p. β involves both direct factors, hence it is not one of the previously constructed automorphisms whence p^s automorphisms have been constructed. However, if $a_2 \in K_1$, to P_1 and P_2, respectively. We have $H_2 \subset H_1$ and $K_2 \subset K_1$ so that

$$H_1 = \{a_2\} \times H_2,$$
$$K_1 = \{a_2\} \times K_2$$

where $K_2 \subset H_2$. As before, we construct the automorphisms of H_1 (in the role of P_1) and since H_1 is a direct factor of P_1 the automorphisms will be automorphisms of P_1, using H_1 exclusively. In fact, since

$$P_1 = \{a_1\} \times H_1 \text{ we have } A(P_1) \supset A(\{a_1\}) \times A(H_1).$$

Also since we have p^{m_1} automorphisms using a_1 exclusively, we have the required p^s automorphisms.

Suppose we have

$$P_1 = \{a_1\} \times \{a_2\} \times \cdots \times \{a_i\} \times H_i,$$
$$P_2 = \{a_1\} \times \{a_2\} \times \cdots \times \{a_i\} \times K_i$$

where $K_i \subset H_i$ and

$$P_1 \supset H_1 \supset \cdots \supset H_i,$$
$$P_2 \supset K_2 \supset \cdots \supset K_i.$$

Also a_j is an element of highest order in

$$H_j,\ K_j, \qquad \text{for } j = 1, 2, \cdots, i-1.$$

Now either K_i contains an element of highest order of H_i or K_i does not contain an element of highest order of H_i. In the latter case let a_{i+1} be an element of highest order in H_i; hence, $a_{i+1} \notin K_i$ and we define

$$\begin{aligned} \alpha(a_{i+1}) &= a_{i+1}b, & b &\in K_i, \\ \alpha(a_t) &= a_t, & t &= i+2, \cdots, k \end{aligned}$$

and $\alpha(a_t)$ is any of the p^{m_t-1} automorphisms of the cyclic group generated by a_t $(t=1, 2, \cdots, i)$. For each a a further automorphism may be constructed as follows: Define

$$\begin{aligned} \gamma(a_r) &= a_r \cdot a_1^{p^{m_1-1}}, & r &= 1, 2, \cdots, i+1, \\ \gamma(a_t) &= a_t, & &\text{for } t \neq r. \end{aligned}$$

Hence we have the required p^s automorphisms by application of the previous arguments.

If, however, K_i contains an element of highest order of H_i, say a_{i+1}, then, as before, we have

$$\begin{aligned} P_1 &= \{a_1\} \times \cdots \times \{a_{i+1}\} \times H_{i+1}, \\ P_2 &= \{a_1\} \times \cdots \times \{a_{i+1}\} \times K_{i+1} \end{aligned}$$

where $K_{i+1} \subset H_{i+1}$. But $P_2 \subset P_1$; hence we have for some $i \leqq k$ the first case of $H_{i+1} \neq 1$ and $K_{i+1} = 1$. Finally, if

$$P_2 = P_1 = P \cap Z(G),$$

then

$$G = G_1 \times P_1 \text{ and } A(G) \supseteq A(G_1) \times A(P_1).$$

Now

$$p^{s-1} \mid [A(P_1):1] \text{ by } [\mathbf{1}] \text{ and } p^r \mid [(G):1].$$

Since $I(G)$ fixes P_1 elementwise, we have $p^{r+s-1} = p^{n-1} \mid [A(G):1]$.

It should be noted that the results of this section include Theorem 1 of Scott [4].

Bibliography

1. G. Birkhoff and P. Hall, *On the order of groups of automorphisms*, Trans. Amer. Math. Soc. vol. 39 (1936) pp. 498–499.

2. H. Hilton, *On the order of the group of automorphisms of an Abelian group*, Messenger of Math. (2) vol. 38 (1909) pp. 132–134.

3. I. N. Herstein and J. E. Adney, *A note on the automorphism group of a finite group*, Amer. Math. Monthly vol. 59 (1952) pp. 309–310.

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

5. H. Zassenhaus, *The theory of groups* (English trans.), New York, 1949.

6. W. Burnside, *Theory of groups*, Cambridge, 1897.

THE OHIO STATE UNIVERSITY

A NOTE ON FINITE UNIONS OF IDEALS AND SUBGROUPS

NEAL H. MCCOY

1. **Introduction.** From the theory of ideals in a *commutative* ring R it follows easily that an ideal I of R is contained in the (set-theoretic) union of a finite number of prime ideals P_i $(i=1, 2, \cdots, n)$ of R if and only if I is contained in some *one* of the ideals P_i. A simple direct proof of this will be found in [2, p. 186]. Recently, Behrens [1, p. 171] has shown that the same result holds for the case in which neither commutativity nor associativity is assumed in R.

It is easy to see that if an ideal I of a ring R is contained in the union $A_1 \cup A_2$ of *any two* ideals A_1 and A_2, it must be contained in one of them. For suppose that $I \subseteq A_1 \cup A_2$ and that $I \not\subseteq A_1$. Then there exists an element a_2 of $I \cap A_2$ such that $a_2 \notin A_1$. If $x \in I \cap A_1$, then $x+a_2 \notin A_1$ and therefore $x+a_2 \in A_2$ and $x \in A_2$. That is, $I \cap A_1 \subseteq A_2$ and we have $I \subseteq A_2$. As a matter of fact, this result remains valid if I, A_1, and A_2 are subgroups of an arbitrary group. These observations were pointed out to me by Bailey Brown who also raised several questions about possible generalizations, some of which are partially answered in this note.

The following simple example, due to R. E. Johnson, shows that the above result about the union of two ideals no longer holds when we pass to the union of three ideals. Let R be the ring whose additive group is the direct sum of two two-element cyclic groups, with every products equal to zero. Thus the elements of R may be written as (0, 0), (0, 1), (1, 0), and (1, 1) with componentwise addition modulo 2. Then $A_1 = \{(0, 0), (0, 1)\}$, $A_2 = \{(0, 0), (1, 0)\}$, and $A_3 = \{(0, 0), (1, 1)\}$ are ideals in R, and R is contained in the union of these three

Received by the editors September 30, 1956.