

# A CLASS OF SOLVABLE GROUPS

DANIEL GORENSTEIN AND I. N. HERSTEIN

**1. Introduction.** Numerous studies have been made of groups, especially of finite groups,  $G$  which have a representation in the form  $AB$ , where  $A$  and  $B$  are subgroups of  $G$ . The form of these results is to determine various group-theoretic properties of  $G$ , for example, solvability, from other group-theoretic properties of the subgroups  $A$  and  $B$ .

More recently the structure of finite groups  $G$  which have a representation in the form  $ABA$ , where  $A$  and  $B$  are subgroups of  $G$ , has been investigated. In an unpublished paper, Herstein and Kaplansky (2) have shown that if  $A$  and  $B$  are both cyclic, and at least one of them is of prime order, then  $G$  is solvable. Also Gorenstein (1) has completely characterized  $ABA$  groups in which every element is either in  $A$  or has a *unique* representation in the form  $aba'$ , where  $a, a'$  are in  $A$ , and  $b \neq 1$  is in  $B$ .

In this paper we shall analyse groups of the form  $ABA$  in which  $A$  and  $B$  are cyclic of relatively prime order. The techniques and methods used borrow heavily from those used in the aforementioned paper of Herstein and Kaplansky. The authors became interested in the structure of  $ABA$  groups as an outgrowth of problems they considered while at a conference held at Bowdoin College in the summer of 1957 under the auspices of the Cambridge Research Center of the United States Air Force.

In the body of the paper we shall use the following notation: If  $H$  is a subgroup of  $G$ ,  $o(H)$ ,  $i(H)$ , and  $N(H)$  will denote respectively the order of  $H$ , the index of  $H$  in  $G$ , and the normalizer of  $H$  in  $G$ .

**2. Two preliminary lemmas.** We shall need a result on the transfer homomorphism which is a slight extension of a result of Grün (3, p. 143); in fact, the result is essentially contained in Grün's, but for the sake of completeness we present it here.

LEMMA 1. *Let  $G$  be a finite group, and  $A$  an Abelian subgroup of  $G$  for which  $(o(A), i(A)) = 1$ . Then the transfer of  $G$  into  $A$  maps the intersection of  $A$  with the centre of its normalizer onto itself.*

*Proof.* Since  $(o(A), i(A)) = 1$  it is clear that for any  $p|o(A)$  the  $p$ -Sylow subgroup of  $A$  is a  $p$ -Sylow subgroup of  $G$ .

We first contend that if  $A_1$  is an Abelian subgroup of  $G$  and  $o(A_1) = o(A)$ , then  $A_1$  is a conjugate of  $A$ . Let  $S_p \neq (1)$  be the  $p$ -Sylow subgroup of  $A_1$ .

---

Received June 16, 1958. The work of the second author was supported in part by OOR, Contract No. ORDOR-LO-P-2042/A11472.

Since these are  $p$ -Sylow subgroups of  $G$ , there is a  $y \in G$  such that  $S_p = yS_p'y^{-1}$ . If we replace  $A_1$  by  $yA_1y^{-1}$  we may, without loss of generality, assume that  $S_p \subset A$  and  $S_p \subset A_1$ .

If  $N(S_p) \neq G$ , our contention follows by induction and from the fact that both  $A$  and  $A_1$ , being Abelian, are contained in  $N(S_p)$ . If, on the other hand,  $N(S_p) = G$ , we use induction on  $\bar{G} = G/S_p$  to conclude that  $\bar{A}, \bar{A}_1$ , the images of  $A$  and  $A_1$  in  $\bar{G}$  are conjugate in  $\bar{G}$ . Since both  $A$  and  $A_1$  contain  $S_p$ , their conjugacy in  $G$  follows at once.

From this, and the usual argument made on the centres of Sylow subgroups, we can say that if two elements of  $A$  are conjugate in  $G$  then they are already conjugate in  $N(A)$ .

We are now able to prove the lemma. For let  $a_1$  be an element in the intersection of  $A$  with the centre of  $N(A)$ , we compute the transfer,  $\tau$ , on  $a_1$ . Since  $A$  is Abelian,

$$\tau(a_1) = \prod_{i=1}^r x_i a_1^{f_i} x_i^{-1} \quad \text{where} \quad \sum_{i=1}^r f_i = i(A) \quad \text{and} \quad x_i a_1^{f_i} x_i^{-1} \in A.$$

However, since

$$a_1^{f_i} \quad \text{and} \quad x_i a_1^{f_i} x_i^{-1}$$

are conjugate in  $G$  and are in  $A$  they are conjugate in  $N(A)$ ; since  $a_1$  is in the centre of  $N(A)$  they must be equal. Thus

$$\tau(a_1) = \prod_{i=1}^r a_1^{f_i} = a_1^{i(A)};$$

and since  $(o(A), i(A)) = 1$ , the lemma follows.

The second result we shall need is contained in the following lemma.

**LEMMA 2.** *Suppose a finite group  $G$  admits an automorphism  $\alpha$  of order  $h$  such that every element of  $G$  can be expressed in the form  $\alpha^i(b^j)$  for some fixed element  $b$  of  $G$  of order  $k$ . If  $(h, k) = 1$ , then  $G$  is either Abelian or is the direct product of an Abelian group of odd order with the quaternion group of order 8. If  $\alpha$  leaves only the identity element of  $G$  fixed, then  $G$  is Abelian.*

*Proof.* We proceed by induction on the order of  $G$ .

Suppose, first, that  $\alpha$  leaves some element,  $\neq 1$ , of  $G$  fixed. Then for some  $e, t, \alpha(\alpha^e(b^t)) = \alpha^e(b^t), b^t \neq 1$ . Thus  $\alpha(b^t) = b^t$ . But then for all  $i, j$

$$\alpha^i(b^j) \cdot b^t = \alpha^i(b^j)\alpha^i(b^t) = \alpha^i(b^{j+t}) = b^t\alpha^i(b^j),$$

and so  $b^t$  is in  $Z$ , the centre of  $G$ .

Since the order of every element of  $G$  is a divisor of the order of  $b$ , then  $f$  or any prime  $p, p|o(G)$  implies  $p|k$ . We consider the cases when  $p \nmid k/t$  and  $p|k/t$  separately.

Suppose first that  $p \nmid k/t$ . Let  $\bar{G} = G/(b^t)$  and let  $\bar{\alpha}$  be the automorphism induced by  $\alpha$  on  $\bar{G}$ . If  $\bar{b}$  is the image of  $b$  in  $\bar{G}$ , then every element of  $\bar{G}$  is clearly of the form  $\bar{\alpha}^i(\bar{b}^j)$ . By our induction hypothesis the  $p$ -Sylow subgroup

$\bar{S}_p$  of  $\bar{G}$  is normal in  $\bar{G}$ . Thus the inverse image of  $\bar{S}_p$  in  $\bar{G}$ , is normal in  $G$  and is of the form  $S_p \cdot (b^t)$  for some  $p$ -Sylow subgroup of  $G$ . If  $s \in S_p, x \in G$ , then  $xsx^{-1} = b^{tj}s_1, s_1 \in S_p$ ; since the order  $k/t$  of  $b^t$ , is relatively prime to  $p$ , this implies  $b^{tj} = 1$ , and so  $xS_p x^{-1} = S_p$ , so  $S_p$  is normal in  $G$ .

Furthermore

$$\bar{S}_p = \frac{S_p \cdot (b^t)}{(b^t)} \cong \frac{S_p}{S_p \cap (b^t)} = S_p;$$

by induction  $\bar{S}_p$ , and hence  $S_p$ , is either Abelian or isomorphic to the quaternion group of order 8.

If, on the other hand,  $p|k/t$  then  $b^{k/p}$  is in  $Z$ , and being of prime-power order, must be in all  $p$ -Sylow subgroups of  $G$ . By induction,  $\bar{S}_p$ , the  $p$ -Sylow subgroup of  $\bar{G} = G/(b^{k/p})$  is normal in  $\bar{G}$ , so its inverse image,  $S_p$ , must be normal in  $G$ . Thus  $S_p$  contains all elements of  $G$  whose order is a power of  $p$ . We claim  $S_p$  contains a unique subgroup of order  $p$ . For if  $\alpha^i(b^j)$  is of order  $p$ , then  $j$  is a multiple of  $k/p$ , so  $\alpha^i(b^j) = b^j$  since  $\alpha(b^{k/p}) = b^{k/p}$ ; thus the only subgroup of order  $p$  is  $(b^{k/p})$ . It is well known that a group of prime-power order having only one subgroup of order  $p$  is cyclic if  $p$  is odd and is either cyclic or a generalized quaternion group of order  $2^n$  if  $p = 2$ . Now  $S_2$  is a normal subgroup of  $G$  invariant under  $\alpha$ . Since by assumption  $(h, k) = 1$  and since  $2|k$  if  $S_2 \neq 1$ , we conclude that  $\alpha$  is of odd order. If  $\alpha$  reduces to the identity on  $S_2$ ,  $S_2$  is cyclic. Hence if  $S_2$  is isomorphic to the generalized quaternion group,  $\alpha$  has odd order on  $S_2$ . But for  $n > 3$  the automorphism group of a generalized quaternion group of order  $2^n$  is of order  $2^{n-1}$ . Thus the only possibility in our case is  $n = 3$ , and  $S_2$  is isomorphic to the quaternion group of order 8.

There remains the case when  $\alpha$  leaves no element of  $G$ , other than 1, fixed. In this situation it is known that for each prime  $p$ ,  $\alpha$  must leave some  $p$ -Sylow subgroup, say,  $S_p$ , fixed. Since an element of  $S_p$  is of the form  $\alpha^i(b^j)$ , it follows readily that  $S_p$  consists of all the elements of  $G$  whose order is a power of  $p$ .  $S_p$  is then the unique  $p$ -Sylow subgroup of  $G$  and so is normal in  $G$ , and  $G$  is the direct product of its Sylow subgroups. We still must show that  $S_p$  is either Abelian or the quaternion group of order 8. Thus we may, without loss of generality, assume that  $S_p = G$ .

Suppose then that  $k = p^s$ . We compute the number of elements in  $G$ . Let  $r_i$  be the least positive integer such that

$$\alpha^{r_i}(b^{p^i}) \in (b^{p^i}).$$

It is clear that the number of elements in  $G$ , of order exactly  $p^{s-i}$ , is  $r_i(p^{s-i} - p^{s-i-1})$ ,  $i < s$ , and so

$$(2.1) \quad o(G) = p^n = r_0(p^s - p^{s-1}) + r_1(p^{s-1} - p^{s-2}) + \dots + r_{s-1}(p - 1) + 1.$$

However, the elements of order  $p$  in the centre of  $G$  form a characteristic subgroup of  $G$ , and so the elements of the form

$$\alpha^i(b^{p^{s-1}j})$$

(that is, all the elements of order  $p$ ), form a subgroup of  $G$  (in  $Z$ ) of order  $p^m$ , containing  $r_{s-1}(p-1)+1$  elements. So

$$(2.2) \quad p^m = r_{s-1}(p-1)+1.$$

Combining (2.1) and (2.2) we have

$$p^n - p^m = r_0(p^s - p^{s-1}) + \dots + r_{s-2}(p^2 - p).$$

If  $m > 1$ , then  $p^2$  divides the left-hand side, and so must divide the right-hand side; but then  $p|r_{s-2}$ . Since  $r_{s-2}|h$ , and  $1 = (h, k) = (h, p^s)$ , this is impossible. So  $m = 1$ , and we can conclude that  $G$  has exactly one subgroup of order  $p$ . We conclude, as above, that  $G$  is either cyclic or isomorphic to the quaternion group of order 8.

The final statement of the lemma follows at once from the fact that the quaternion group has a unique element of order 2 and hence each of its automorphisms leaves this element fixed.

**3. The case  $N(A) = A$ .** In this section we shall prove the following result concerning the structure of  $ABA$  groups:

**THEOREM 1.** *Let  $G$  be an  $ABA$  group, in which  $A$  and  $B$  are cyclic subgroups of relatively prime orders  $h$  and  $k$  respectively. Then if  $A$  is its own normalizer in  $G$ ,  $G$  contains a normal subgroup  $T$  with  $A \cap T = 1$ . Furthermore  $T$  is either Abelian or the direct product of an Abelian group of odd order with the quaternion group of order 8. In particular,  $G$  is solvable, and of order  $hkw$ , where  $w|k^v$  for some integer  $v$ .*

*Proof.* We shall prove first that the Sylow subgroups of  $A$  are, in fact, Sylow subgroups of  $G$ . The proof is by induction on the order of  $G$ .

Let  $S_p$  be a  $p$ -Sylow subgroup of  $A$ . Since  $A$  is Abelian,  $N(S_p) \supset A$ . If  $x = a_1b_1a_2 \in N(S_p)$  with  $b_1 \in B$ ,  $a_1, a_2 \in A$ , then clearly  $b_1 \in N(S_p) \cap B$ . If  $B_1 = B \cap N(S_p)$ , then obviously  $N(S_p)$  is of the form  $AB_1A$ ; thus if  $N(S_p)$  is a proper subgroup of  $G$ , it follows by induction that the order of  $N(S_p)$  is  $hk_1w_1$ , where  $k_1 = o(B_1)$  and  $w_1|k_1^v$  for some integer  $v$ . Since  $(h, k_1) = 1$ , we see then that  $S_p$  is a  $p$ -Sylow subgroup of  $N(S_p)$ . But  $S_p$  must then be a  $p$ -Sylow subgroup of  $G$ , since the normalizer of a proper subgroup of a  $p$ -group is always a strictly larger subgroup.

On the other hand, if  $N(S_p) = G$ , then  $S_p$  is normal in  $G$ , and we consider  $\bar{G} = G/S_p = \bar{A}\bar{B}\bar{A}$ , where  $\bar{A}, \bar{B}$  are the images of  $A$  and  $B$ . Furthermore  $N(\bar{A}) = \bar{A}$ ; for  $N(\bar{A}) > \bar{A}$  would clearly imply  $N(A) > A$  since  $S_p$  is contained in  $A$ . Hence we can apply our induction hypothesis to  $\bar{G}$ , and we obtain  $o(\bar{G}) = \bar{h}\bar{k}\bar{w}$ , where  $\bar{w}|k^v$  and  $\bar{h} = o(\bar{A})$ . Thus  $p \nmid o(\bar{G})$ , and so  $S_p$  is a Sylow subgroup of  $G$ .

Since this holds for every  $p|h$ , it follows that the order and index of  $A$  are relatively prime. Since  $A$  is Abelian, we may apply Lemma 1 to conclude that the transfer  $\tau$  of  $G$  into  $A$  maps the intersection of  $A$  with the centre

of its normalizer onto itself. But by assumption,  $A$  is the centre of its normalizer, and so  $\tau$  maps  $G$  homomorphically onto  $A$ .

Let  $T$  be the kernel of  $\tau$ ; since  $\tau$  maps  $A$  onto itself,  $A \cap T = 1$ ; since the order of  $B$  is relatively prime to the order of  $A$ ,  $B \subset T$ . If  $a, b$  are generators of  $A, B$  respectively, it is clear that  $T$  consists precisely of the elements of  $G$  of the form  $a^i b^j a^{-i}$ , where  $i, j$  are arbitrary. Now the mapping  $\alpha$  defined on  $T$  by  $\alpha(x) = axa^{-1}$  is an automorphism of  $T$ , and every element of  $T$  is of the form  $a^i(b^j)$ . Therefore by Lemma 2,  $T$  is of the form stated in the theorem.

Since every element of  $T$ , being of the form  $\alpha^i(b^j)$ , has order a divisor of  $k$ ,  $o(T) = kw$  where  $w|k^\nu$  for some integer  $\nu$ . Since  $G/T = A$ , and  $A$  is cyclic of order  $h$ ,  $G$  is solvable of order  $hkw$ . This completes the induction and the proof of the theorem.

**COROLLARY.** *A Sylow subgroup of  $G$  is either Abelian or isomorphic to the quaternion group of order 8.*

**4. The main theorem.**

**THEOREM 2.** *Let  $G$  be an  $ABA$  group in which  $A$  and  $B$  are cyclic subgroups of relatively prime orders  $h$  and  $k$  respectively. Then*

1.  $G$  is solvable.
2. The  $p$ -Sylow subgroups of  $G$ , for odd  $p$ , are Abelian;
3. The 2-Sylow subgroup of  $G$  is either Abelian or isomorphic to the quaternion group of order 8.
4. The order of  $G$  is  $hkw$ , where  $w|k^\nu$  for some integer  $\nu$ .

*Proof.* If  $N(A) = A$ , the theorem follows immediately from Theorem 1 and its corollary. We may therefore assume that  $N(A) > A$ . If  $a, b$  denote, as above, generators of  $A$  and  $B$ , there is an element of the form  $a^i b^j a^e$  in  $N(A)$  with  $b^j \neq 1$ , whence  $b^j$  itself is in  $N(A)$ . Let  $r$  be the least positive integer such that  $b^r \in N(A)$ . Then  $r|k$ , and we have for some integer  $\lambda$

$$(4.1) \quad b^r a b^{-r} = a^\lambda, \quad \text{where } \lambda^{k/r} \equiv 1 \pmod{h}.$$

Let  $p$  be a prime dividing  $k/r$  and define  $\gamma_p$  as the least multiple of  $r$  such that  $k/r$  is a power of  $p$ . Set

$$B_p = (b^{\gamma_p}).$$

In the first part of the proof we shall establish the following statement:

*The normalizer  $N(B_p)$  of  $B_p$  is of the form  $A_p B A_p$  for a suitable subgroup  $A_p$  of  $A$ , and furthermore  $B_p$  is in the centre of  $N(B_p)$ .*

We shall need one preliminary result. Since  $r|\gamma_p$ , we have

$$(4.2) \quad b^{\gamma_p} a b^{-\gamma_p} = a^{\lambda^p}, \quad \lambda_p^{k/\lambda_p} \equiv 1 \pmod{h}$$

for some integer  $\lambda_p$ . Let  $u_p = (\lambda_p - 1, h)$ . We assert that

$$\left(u_p, \frac{h}{u_p}\right) = 1.$$

For suppose a prime  $q | (\lambda_p - 1)$ . It is sufficient to show that if  $q^\epsilon | h$ , then  $q^\epsilon | (\lambda_p - 1)$ . Since  $k/\gamma_p = p^s$  for some integer  $s$ , (4.2) implies that

$$\lambda_p^{p^s} \equiv 1 \pmod{h}$$

and hence

$$\lambda_p^{p^\epsilon} \equiv 1 \pmod{q^\epsilon}.$$

Write  $\lambda_p = 1 + xq^\delta$ , where  $(x, q) = 1$ . Then  $(1 + xq^\delta)^{p^\epsilon} \equiv 1 \pmod{q^\epsilon}$  and so  $p^\epsilon xq^\delta + yq^{2\delta} \equiv 0 \pmod{q^\epsilon}$  for some integer  $y$ . Since  $p | k$  and  $q | h$ , and  $(h, k) = 1$ ,  $p \neq q$  and hence  $\delta \geq \epsilon$ .

We now return to  $N(B_p)$ . Suppose that  $a^i b^j a^\epsilon \in N(B_p)$ . Then

$$a^i b^j a^\epsilon b^{\gamma_p} a^{-\epsilon} b^{-j} a^{-i} = b^{\gamma_p m}$$

for some integer  $m$ .

Applying (4.2) to this relation, we obtain

$$(4.3) \quad a^i b^j a^{\epsilon(1-\lambda_p)} b^{-j} a^{-i\lambda_p} = b^{\gamma_p(m-1)}.$$

Suppose first that

$$\frac{h}{u_p} \mid e.$$

Since  $u_p | (\lambda_p - 1)$ , (4.3) reduces to

$$a^{i(1-\lambda_p)} = b^{\gamma_p(m-1)}$$

and their common value is 1, since  $a$  and  $b$  have relatively prime order. But  $u_p = (1 - \lambda_p, h)$ , and so

$$\frac{h}{u_p} \mid i;$$

moreover,

$$m \equiv 1 \pmod{\frac{k}{\gamma_p}},$$

and hence  $a^i b^j a^\epsilon$  commutes with  $b^{\gamma_p}$ .

Conversely, every element of the form

$$\frac{h}{a^{u_p}} i b^j \frac{h}{a^{u_p}} e$$

is in  $N(B_p)$  and commutes with  $b^{\gamma_p}$ . To complete the proof of our assertion, we shall show that every element of  $N(B_p)$  is of this form. We have just shown this to be the case if

$$\frac{h}{u_p} \mid e.$$

Suppose, on the other hand, that  $e(1 - \lambda_p) \not\equiv 0 \pmod{h}$ . Then (4.3) yields the relation

$$b^j a^{e(1-\lambda_p)} b^{-j} = a^{-i} b^{\gamma_p(m-1)} a^{i\gamma_p},$$

and hence  $b^j a^{e(1-\lambda_p)} b^{-j}$  is in  $N(A)$ . But this element has order dividing  $h$ ; since  $(h, k) = 1$ , all the elements of  $N(A)$  of order dividing  $h$  are already in  $A$ . Thus

$$(4.4) \quad b^j a^{e(1-\lambda_p)} b^{-j} = a^{e(1-\lambda_p)\rho}$$

for some integer  $\rho$ .

Using (4.4), we can rewrite the element

$$a^i b^j a^e = a^i b^j a^{-xe(1-\lambda_p)} a^{e+xe(1-\lambda_p)\rho}$$

as

$$a^{i-xe(1-\lambda_p)\rho} b^j a^{e+xe(1-\lambda_p)\rho}.$$

Since

$$\left(1 - \lambda_p, \frac{h}{u_p}\right) = 1,$$

we can find an integer  $x$  such that

$$e + xe(1 - \lambda_p) \equiv 0 \pmod{\frac{h}{u_p}}.$$

If, for this  $x$ , we set  $i' = i - xe(1 - \lambda_p)\rho$  and  $e' = e + xe(1 - \lambda_p)$ , we have  $a^i b^j a^e = a^{i'} b^{j'} a^{e'}$ , where

$$\frac{h}{u_p} \mid e';$$

and hence

$$a^i b^j a^e = a^{\frac{m h}{u_p}} b^j a^{\frac{n h}{u_p}}.$$

If

$$A_p = (a^{u_p}),$$

we have thus proved that  $N(B_p) = A_p B A_p$ , and that  $B_p$  is in the centre of  $N(B_p)$ .

**5. Continuation of the proof.** The proof now proceeds by induction on the order of  $G$ , but we add the following statement to our induction hypothesis: if  $p \nmid k$  then some  $p$ -Sylow subgroup of  $G$  consists of all the elements of the form  $a^{s i} b^{t j} a^{-s t}$  for suitable integers  $s, t$  where  $i, j$  are arbitrary.

There are three cases to consider, which we take up in succession.

*Case 1.*  $N(B_p) = G$ . In this case  $B_p$  is in the centre of  $G$ , and we define  $\tilde{G} = G/B_p = \tilde{A} \tilde{B} \tilde{A}$ , where  $\tilde{A}$  has order  $h$  and  $\tilde{B}$  has order  $\gamma_p$ . By induction,  $\tilde{G}$  is solvable of order  $h\gamma_p w$ , where  $w \mid \gamma_p^r$ ; so  $G$  is solvable and its order is

$$(h\gamma_p w) \frac{k}{\gamma_p} = hkw$$

where  $w|\gamma_p^r|k^r$ .

Hence the order of  $A$  is relatively prime to its index in  $G$ . Thus the Sylow subgroups of  $G$ , for any prime dividing  $h$ , are cyclic.

Furthermore, the Sylow subgroups  $\tilde{S}_q$  of  $\tilde{G}$  for primes  $q$  which divide  $\gamma_p$  are of the form  $\{\tilde{a}^s \tilde{b}^t \tilde{a}^{-s}\}$  for suitable integers  $s$  and  $t$ . If  $q \neq p$ , then it follows as in the proof of Lemma 2 that the elements

$$\{a^{si} b^{\frac{k}{\gamma_p} j} a^{-st}\}$$

form a  $q$ -Sylow subgroup of  $G$  which maps isomorphically on  $\tilde{S}_q$ . If  $q = p$ , it follows again as in the proof of Lemma 2 that the complete inverse image of a suitable  $p$ -Sylow subgroup  $\tilde{S}_p$  of  $\tilde{G}$  is a  $p$ -Sylow subgroup of  $G$  and is of the form  $\{a^{si} b^{tj} a^{-st}\}$  for suitable  $s, t$ . Thus for each prime  $p$  dividing  $k$  a  $p$ -Sylow subgroup  $S_p$  of  $G$  is of the required form. If  $\alpha$  denotes the automorphism of  $S_p$  defined by  $\alpha(x) = a^s x a^{-s}$  for  $x$  in  $S_p$ , then every element of  $S_p$  is of the form  $a^t (b^{tj})$ . Hence by Lemma 2,  $S_p$  is either Abelian or isomorphic to the quaternion group of order 8. Our induction is therefore complete in the case  $N(B_p) = G$ .

We may therefore assume  $N(B_p) < G$ .

*Case 2.  $p \neq 2$ .* By our induction hypothesis some  $p$ -Sylow subgroup  $S_p$  of  $N(B_p)$  is of the form

$$\{a^{\frac{h}{u_p} \sigma i} b^{\gamma_1 j} a^{-h/u_p \sigma i}\}$$

for some integers  $\sigma$  and  $\gamma_1$ , and is Abelian. Since  $B_p$  is in the centre of  $N(B_p)$ ,  $B_p \subset S_p$  and hence  $\gamma_1 | \gamma_p$ . We shall prove first that  $S_p$  is cyclic. Suppose  $b^{\gamma_1}$  has order  $p^\delta$ . Then clearly  $S_p$  is Abelian of type  $(p^\delta, p^\delta, \dots, p^\delta)$ . But since

$$a^{h/u_p}$$

commutes with  $b^{\gamma_1}$ ,  $B_p$  is the only subgroup of its order in  $S_p$ , and hence  $S_p$  is cyclic.

Since  $S_p$  is cyclic,  $B_p$  is a characteristic subgroup of  $S_p$ , and so  $N(S_p) \subset N(B_p)$ . If  $S_p$  were not a  $p$ -Sylow subgroup of  $G$ , its normalizer would contain a strictly larger  $p$ -group than  $S_p$ . But since  $S_p$  is a  $p$ -Sylow subgroup of  $N(B_p)$  and since  $N(S_p) \subset N(B_p)$ , it must be that  $S_p$  is in fact a  $p$ -Sylow subgroup of  $G$ .

But now by a theorem of Grün (or by Lemma 1), the transfer  $\tau$  of  $G$  into the Abelian Sylow subgroup  $S_p$  maps  $G$  onto the intersection of  $S_p$  with the centre of its normalizer. But  $B_p$  is contained in the centre of its normalizer. Thus  $\tau$  maps  $G$  homomorphically on  $(b^{\gamma_2})$  where  $\gamma_1 | \gamma_2 | \gamma_p$ . Since the order of  $A$  is relatively prime to that of  $B$ ,  $A$  is contained in the kernel  $H$  of  $\tau$ . Also  $H$  contains some proper subgroup  $B^*$  of  $B$ , and hence  $H$  is of the form  $AB^*A$ . Since  $G/H$  has order  $k/\gamma_2$ ,  $B^*$  is of order  $\gamma_2$ . Thus for any prime different from  $p$ , the Sylow subgroups of  $H$  are Sylow subgroups of  $G$ , and hence by induction

are of the required form. As we have already seen  $S_p$  itself is cyclic and of the required form. By induction  $H$  is solvable and  $o(H) = h\gamma_2 w$  where  $w|\gamma_2^v$  for some integer  $v$ . Since  $H$  and  $G/H$  are solvable,  $G$  is solvable and the order of  $G$  is  $o(G/H)o(H)$ . Thus  $o(G) = (h\gamma_2 w)k/\gamma_2 = hkw$ , where  $w|\gamma_2^v|k^v$ . It follows at once that the Sylow subgroups of  $G$ , for any prime dividing  $h$ , is cyclic. The proof is complete in this case.

*Case 3.*  $p = 2$ . If  $S_2$  is Abelian, or if an odd prime divides  $k/r$ , the above proof holds without change. There remains then but one case to consider: namely, when  $k/r = 2^s$  and the 2-Sylow subgroup  $S_2$  of  $N(B_2)$  is isomorphic to the quaternion group of order 8. In this case  $\gamma_p = \gamma_2 = r$  and  $B_2 = (b^r)$ .

Since the quaternion group has no element of order 8,  $8 \nmid k$ . On the other hand, suppose  $2 \nmid r$ . Then  $\bar{N} = N(B_2)/B_2$  is of the form  $\bar{A}_2 \bar{B} \bar{A}_2$ , where  $\bar{B}$  has order  $r$ . Then by our induction hypothesis,  $o(\bar{N}) = o(\bar{A}_2)o(\bar{B})\bar{w} = o(\bar{A}_2)r\bar{w}$ , where  $\bar{w}|r^v$ , and so  $o(\bar{N})$  would be odd. But then  $S_2 = B_2$ , contrary to our assumption that  $S_2$  is the quaternion group. Hence we must have  $2|r$ . Since  $k/r$  is a power of 2 and  $8 \nmid k$ , it follows that  $r/2$  is odd and  $k/r$  is 2.

We are thus reduced to considering the following situation:

$$(5.1) \quad b^r a b^{-r} = a^\lambda, \quad 2|r, \quad r/2 \text{ is odd, and } k/r = 2.$$

Let  $(\lambda - 1, h) = u$ . If  $u = 1$ , then  $N(B_2) = B$  (since  $N(B_2)$  is of the form  $\{a^{h/u} b^j a^{-h/u} \}$ ). But then again  $S_2$  would be cyclic. So we may assume that  $u > 1$ .

We may further assume that no subgroup of  $A$  is normal in  $G$ , for the theorem follows easily by induction in this case. In particular, this implies, as in the proof of Theorem 1, that the order of  $A$  is relatively prime to its index.

From (5.1), we have  $\lambda^2 - 1 \equiv 0 \pmod{h}$ , and hence  $u(\lambda + 1) \equiv 0 \pmod{h}$ . Thus  $b^r a^u b^{-r} = a^{u\lambda} = a^{-u}$ , and similarly  $b^r a^{-u} b^{-r} = a^u$ . Now as we have already seen,  $b^r$  commutes with  $a^{h/u}$ . But  $N(A)$  is generated by  $a$  and  $b^r$ , and hence  $a^{h/u} \neq 1$  is in the centre of  $N(A)$ . Since the order of  $A$  is relatively prime to its index, it follows from Lemma 1 that the transfer of  $G$  into  $A$  maps the intersection of  $A$  with the center of its normalizer onto itself. Thus  $(a^{h/u})$  is mapped onto itself by the transfer map. Hence the kernel  $H$  of the transfer of  $G$  into  $A$  consists of all elements of the form  $a^i b^j a^{-i+eu}$ . Suppose now that  $x = a^i b^j a^{-i+eu}$  is an element of order 2 in  $H$ . Thus  $1 = x^2 = a^i b^j a^{-i+eu} a^i b^j a^{-i+eu}$ , whence

$$(5.2) \quad b^j a^{eu} b^j = a^{-eu}.$$

Conjugating this relation by  $b^r$  we obtain  $b^j a^{-eu} b^j = a^{eu}$ . Thus  $b^j a^{eu} b^j b^j a^{-eu} b^j = a^{-eu} a^{eu} = 1$ , and so

$$(5.3) \quad a^{eu} b^{2^j} a^{-eu} = b^{-2^j}.$$

Thus  $a^{2^e u} b^{2^j} a^{-2^e u} = b^{2^j}$ . But  $(2, h) = 1$ , so that we must have  $a^{eu} b^{2^j} a^{-eu} = b^{2^j}$ . Equation (5.3) now yields that  $b^{4^j} = 1$ . Consequently  $k|4j$ ; that is  $k/4 = (r/2)|j$ . Thus  $x^2 = 1$  implies that

$$x = a^i b^{\frac{r}{2}m} a^{-i+eu}.$$

Suppose next that  $j = r/2$ . Then (5.2) becomes  $b^{\frac{1}{2}r}a^{eu}b^{\frac{1}{2}r} = a^{-eu}$ , so that  $b^{\frac{1}{2}r}a^{eu}b^{-\frac{1}{2}r} = a^{-eu}b^{-r} = a^{-eu}b^r$  since  $k = 2r$ ; but now the element on the right-hand side of this relation is of order 2, while that on the left-hand side is not, which is a contradiction. Similarly,  $j = -\frac{1}{2}r$  is impossible.

We have thus proved that if  $x = a^i b^j a^{-i+eu}$  is an element of order 2 in  $H$ , then  $j = r$ , and so  $x$  is of the form  $b^r a^{e/u}$ . Since  $H$  is normal in  $G$ , and since  $b^r a^u$  is of order 2,  $b(b^r a^u)b^{-1}$  is of order 2 and is in  $H$ . It follows that  $b(b^r a^u)b^{-1} = b^r a^{mu}$  for some integer  $m$ , and hence  $ba^u b^{-1} = a^{mu}$ . Thus  $a^u$  generates a normal subgroup of  $G$ , in contradiction to our present assumption that no subgroup of  $A$  is normal in  $G$ . This contradiction completes the proof of the theorem.

## REFERENCES

1. D. Gorenstein, *A Class of Frobenius Groups*, Can. J. Math., 11 (1959), 39–47.
2. I. N. Herstein and I. Kaplansky, *Groups of Cyclic Length Three*, project document No. 13, Summer Mathematical Conference, Bowdoin College, Brunswick, Maine (1957).
3. H. Zassenhaus, *The Theory of Groups*, New York, 1949).

*Clark University*  
*and*  
*Cornell University*