LARGE ABELIAN SUBGROUPS OF p-GROUPS

BY

J. L. ALPERIN(1)

For some time now, very little has been known about abelian subgroups of p-groups. We shall try and remedy this situation in a series of papers, of which this is the first. One impetus for doing this was created by several natural conjectures which arose in problems in other areas of group theory. In this paper we shall study p-groups with respect to the existence and nonexistence of abelian subgroups which in one sense or another can be considered as large subgroups. Later work will deal with several other topics.

Our first result is in a negative direction; we shall demonstrate the falsity of the conjecture that every group of order p^n has an abelian subgroup of order $p^{n/2}$. Previously, we announced [1] that the best one could hope for was abelian subgroups of order at least $p^{\cdot 48n}$, but for odd primes we can greatly improve this result by an entirely different method.

THEOREM 1. *If p is an odd prime and n is a positive integer, then there exists a group of order p^{3n+2} all of whose abelian subgroups have order at most p^{n+2}. There exists a group of order 2^{50} all of whose abelian subgroups have order at most 2^{24}.*

This theorem is of course proved by the construction of the required examples. The 2-group described is not as formidable as its order might suggest; it is achieved as the end result of an iteration of several natural and simple constructions. The best known result in a positive direction is Burnside's classic theorem [2] that a group of order p^n has normal abelian subgroups of order p^m with $n \leqq m(m-1)/2$, which is roughly $m \geqq \sqrt{2n}$. Exactly where, between our result and Burnside's, the best possible result lies is an open question.

The last part of Theorem 1 is based in part upon the following result.

THEOREM 2. *If G is a group and H is a group of odd order, then every normal abelian subgroup of $G \operatorname{wr} H$ is contained in the base subgroup. Any abelian subgroup of $G \operatorname{wr} Z_p$, not contained in the base subgroup, has order at most ap, where a is the order of the largest abelian subgroup of G.*

This result has an interest in quite another area. The Sylow p-subgroups of the general linear group, symplectic group, unitary group and orthogonal groups over

Received by the editors June 19, 1963.

(1) This research was partially supported by the Air Force Office of Scientific Research.

finite fields, when p is odd and not the characteristic of the field, are isomorphic with the direct product of iterated wreath products $(\cdots(Z_{p^r} \int Z_p)\cdots) \int Z_p$ [5]. Theorem 2 therefore implies that these Sylow groups have a unique largest normal abelian subgroup and that no other abelian subgroup has order as great.

In a positive direction, we shall next give a simple and short proof of an unpublished theorem of G. Higman. This result was originally proved using canonical forms for pairs of alternating forms, but our proof is quite elementary. This theorem, as it is concerned with forms and vector spaces, looks out of place in this paper, but by means of the well-known connection between alternating forms and groups which are nilpotent of class two [4, p. 17], we will be able to derive a purely group-theoretic consequence.

THEOREM 3. *Let f and g be alternating forms on an n-dimensional vector space V. Then, there is a subspace of dimension $[\frac{1}{2}(n+1)]$ on which both f and g vanish.*

The application to groups is as follows:

COROLLARY. *Let G be a p-group of order p^n, exponent p nilpotency class two with G' of order p^2 and $Z(G)$ of order p^m. Then G has abelian subgroups of order p^s where $s \geqq m + [\frac{1}{2}(n-m+1)]$.*

Theorem 3 and the corollary evoke the obvious question as to what is the case if we have more than two forms or G' has order greater than p^2. To this query, we have no answer but only the feeling that the above results do not hold in generality. An answer to this problem might in fact dispose of the question discussed after the statement of Theorem 1.

We now turn our attention to the last topic discussed here, namely, the existence of normal abelian subgroups. A maximal subgroup of a p-group is always normal so that if a p-group has an abelian subgroup of index p then this subgroup is a normal abelian subgroup. On the other hand, it is well known that if a p-group possesses an abelian subgroup of index p^2 then it also has normal abelian subgroups of index p^2. Furthermore, we shall now prove

THEOREM 4. *If a p-group G, for an odd prime p, possesses an abelian subgroup of index p^3 then it has a normal abelian subgroup of index p^3.*

This result is surprising in two ways: first, the cases of subgroups of index p and p^2 are very special and give no indication that such a result should hold for index p^3, and second, the theorem is false for $p = 2$. In fact, there is a group of order 2^9 which has precisely two abelian subgroups of index eight, neither of which is a normal subgroup. This group may be constructed as follows: Let H be the group of order 2^8 generated by four elements a_1, a_2, b_1, b_2 of order two subject only to the conditions that H be of class two and that $(a_1, a_2) = (b_1, b_2) = 1$. An automorphism t of order two of H can be defined by requiring that it map a_i to b_i and

b_i to a_i for $i = 1,2$. The splitting extension of H by the automorphism t has order 2^9 and is the required group. This example is one group of a family of groups which will be discussed in detail in a later paper.

The organization of the rest of this paper is as follows: The remainder of this section is devoted to a description of notation and relevant previous results. §2 contains the proof of the first statement of Theorem 1, while §3 has the proof of Theorem 2 and the conclusion of the proof of Theorem 1. The next section is concerned with Theorem 3 and the corollary and §5 is devoted to the proof of the final theorem. A last section contains some remarks, suggestions and conjectures.

Let $x, y, x_1, \cdots, x_n$ be elements of a group G. We denote the commutator $(x, y) = x^{-1}y^{-1}xy$ and let $(x_1, \cdots, x_n) = ((x_1, \cdots, x_{n-1}), x_n)$. The conjugate of x by y is x^y. If $S_1, S_2, \cdots$ are subsets of G then $gp(S_1, S_2, \cdots)$ is the subgroup of G generated by the subsets $S_1, S_2 \cdots$. If H and K are subgroups of G then (H, K) is the subgroup of G generated by all the elements (h, k) for $h \in H$, $k \in K$. We let $H^x = x^{-1}Hx$ and H^G be the subgroup of G generated by all the conjugates of H in G. Thus, H^G is the normal closure of H in G. The index of H in G is $(G: H)$ and $N(H)$ and $C(H)$ are the normalizer and centralizer of H in G, respectively.

If p is a prime then G is a p-group if it has order a power of p. In this paper all groups will be assumed finite. If G is a p-group, then we say G has exponent p if $x^p = 1$ for all $x \in G$. We also let $Z(G)$ and G' be the center and derived group of G so $G' = (G, G)$. If $G' \leqq Z(G)$ then we say that G has class two. In this case, if m and n are integers, then $(x^m, y^n) = (x, y)^{mn}$. If G is the product of two normal abelian subgroups, then G is of class two. A p-group G has the important property that if A is a maximal normal abelian subgroup of G then $C(A) = A$. That is, A is a maximal abelian subgroup.

If G and H are two groups then the wreath product W of G and H is denoted by G wr H. It is constructed as follows: Let B be the direct product of as many copies of G as there are elements of H. Therefore, index these copies of G by the elements of H. If $h \in H$ then h induces an automorphism of B by mapping G_{h_1} to $G_{h_1 h}$, sending one element to the corresponding element in the second group. In this way, H may be viewed as a group of automorphisms of B. The splitting extension of B by H, with this action of H on B, is the wreath product W. The subgroup B of W is called the base subgroup of W. The subgroups G_h of the base subgroup will be called the factors of B.

Again, let G and H be any two groups and suppose there is an isomorphism f of $Z(G)$ onto $Z(H)$. The set of all pairs $(g, f(g)^{-1})$, for all $g \in Z(G)$, is a normal subgroup of $G \times H$. The quotient group G/H of G by this normal subgroup is called the central product P of G and H. Usually, the isomorphism f will be clear from the context. Thus, P is the product of two subgroups, one isomorphic with G and one with H. Furthermore, these two subgroups, call them G and H also, commute elementwise. Also, $Z(G) = Z(H) = Z(P)$. Similarly, one can define the central product of more than two groups.

Let V be an n-dimensional vector space over the field F. A bilinear functional f of V into F is called an alternating form if $f(v, v) = 0$ for all $v \in V$. If n is odd, then there is an element $w \in V$ such that $f(w, v) = 0$ for all $v \in V$.

2. **Theorem 1.** In this section we shall only prove the first statement of the theorem; the construction of the 2-group is postponed until the next section. We shall construct the desired groups by a sequence of simple steps. First, we let H_1 be an elementary abelian p-group on generators w, z_x and z_y. This group has an automorphism y of order p which leaves z_x and z_y fixed and sends w to wz_y. Let H_2 be the splitting extension of H_1 by y. The group H_2 has an automorphism x of order p, if $p \neq 2$, which sends y to yw^{-1}, w to wz_x and fixes z_x and z_y. Let H be the splitting extension of H_2 by x.

Thus, H is of order p^5, $Z(H)$ is of order p^2 and generated by z_x and z_y, H' is of order p^3 and generated by $Z(H)$ and w. Also, $H/Z(H)$ is of exponent p. Furthermore, the maximal abelian subgroups of H are the subgroups of order p^3 generated by $Z(H)$ and any element of H not contained in $Z(H)$.

We let G_n be the group which is the central product of n copies of H. Thus G_n has order p^{3n+2} and is generated by $2n$ elements of order p, $x_1, \cdots, x_n, y_1, \cdots, y_n$ subject to the defining relations:

$$\begin{aligned}
(x_i, y_j) &= 1 \qquad \text{if } i \neq j,\\
(x_i, y_i) &= w_i,\\
(w_i, x_i) &= z_x,\\
(w_i, y_i) &= z_y,\\
(z_x, x_i) &= (z_x, y_i) = (z_y, x_i) = (z_y, y_i) = 1.
\end{aligned}$$

The derived group W of G_n is generated by all the w_i, z_x and z_y and has order p^{n+2}. Furthermore, W is abelian. The center $Z(G_n)$ is of order p^2 and is generated by z_x and z_y. The quotient $G_n/Z(G_n)$ is of exponent p.

We shall now prove that every abelian subgroup of G_n is of order at most p^{n+2}. Let A be a maximal abelian subgroup of order $> p^{n+2}$ so that $C(A) = A$ and $Z(G_n) \leqq A$. Therefore, $A \cap W$ is elementary abelian, say of order p^{m+2} and so is generated by $z_x, z_y, u_1, \cdots, u_m$ where

$$u_i = w_1^{a_{i1}} w_2^{a_{i2}} \cdots w_n^{a_{in}}, \qquad i = 1, \cdots, m,$$

with the a_{ij} integers modulo p.

As a first step, we shall compute $C(A \cap W)$. Since $W' = 1$, we have $W \leqq C(A \cap W)$. Suppose $g \in C(A \cap W)$ and

$$g = x_1^{b_1} y_1^{c_1} \cdots x_n^{b_n} y_n^{c_n} w$$

where $w \in W$ and the b_i and c_i are integers modulo p. Since $w \in C(A \cap W)$, we have $g \in C(A \cap W)$ if and only if $h = gw^{-1} \in C(A \cap W)$.

But

$$(u_i, h) = (w_1^{a_{i1}}, x_1^{b_i} y_1^{c_i}) \cdots (w_n^{a_{in}}, x_n^{b_n} y_n^{c_n})$$
$$= z_x^{a_{i1}b_1 + \cdots + a_{in}b_n} z_y^{a_{i1}c_1 + \cdots + a_{in}c_n}$$

so that if $\bar{A}$ is the matrix (a_{ij}) of m rows and n columns and b and c are column vectors of the b_i and c_j then $h \in C(A \cap W)$ if and only if $\bar{A}b = \bar{A}c = 0$.

However, A is an abelian subgroup of $C(A \cap W)$. Since A has order greater than p^{n+2}, there is an abelian subgroup (also to be denoted by A) of order p^{n+3} generated by $z_x, z_y, u_1, \cdots, u_m$ and $g_1, g_2, \cdots, g_{n-m+1}$ where

$$g_i = x_1^{r_{i1}} y_1^{s_{i1}} \cdots x_n^{r_{in}} y_n^{s_{in}} v_i, \qquad i = 1, \cdots, n - m + 1,$$

with the r_{ij} and s_{ij} integers modulo p and $v_i \in W$. Since A is abelian, certainly $(g_i, g_j) \equiv 1$ (modulo $Z(G_n)$), which is

$$(x_1^{r_{i1}} y_1^{s_{i1}}, x_1^{r_{j1}} y_1^{s_{j1}}) \cdots (x_n^{r_{in}} y_n^{s_{in}}, x_n^{r_{jm}} y_n^{s_{jn}}) \equiv 1,$$
$$w_1^{r_{i1}s_{j1} - s_{i1}r_{j1}} \cdots w_n^{r_{in}s_{jn} - s_{in}r_{jn}} \equiv 1$$

so

$$r_{ik}s_{jk} - s_{ik}r_{jk} = 0, \qquad k = 1, \cdots, n.$$

From this it follows easily that there are integers modulo p, r_k, s_k, t_{ik} for $i = 1, \cdots, n - m + 1$, $k = 1, \cdots, n$ such that

$$r_{ik} = t_{ik}r_k, \quad s_{ik} = t_{ik}s_k.$$

Indeed, the last of the above equations implies that the row vectors (r_{ik}, s_{ik}), for fixed k and $i = 1, \cdots, n - m + 1$, are linearly dependent in pairs and so span a one-dimensional space.

Let r_i and s_i be the column vectors of the numbers r_{ik} and s_{ik}, respectively. Then, since $g_i \in C(A \cap W)$, $\bar{A}r_i = \bar{A}s_i = 0$, where $\bar{A}$ is as defined before. However, if we now let A_1 be the matrix $(a_{ij}r_j)$ of m rows and n columns $A_2 = (a_{ij}s_j)$ and t_i be the column vector of the t_{ij}, these conditions become $A_1t_i = A_2t_i = 0$, for all i. Next, let B be the matrix of $2m$ rows and n columns whose first m rows are A_1 and whose last m rows are A_2. Then $Bt_i = 0$ for all i, so that B has nullity at least $n - m + 1$. Therefore, if we can show that B has rank at least m, then $m + (n - m + 1) = n + 1 > n$, which is a contradiction.

However, in order to prove that B has rank at least m, we first show that we may assume $r_i \neq 0$ or $s_i \neq 0$ for each $i = 1, \cdots, n - m + 1$. For, if say $r_n = s_n = 0$, then $A \leqq G_{n-1}W$. However, $(G_{n-1}W : G_{n-1}) = p$, so then $A \cap G_{n-1}$ has order at least p^{n+2}. But we may assume that the theorem has already been proved for G_{n-1}, so that this is a contradiction.

We may now choose an m by n submatrix C of B as follows: If $r_i \neq 0$ then the ith column of C consists of the first m entries of the ith column of B and if $r_i = 0$,

so $s_i \neq 0$, then the ith column of C consists of the last m entries of the ith column of B. In this way, the ith column of C is a nonzero multiple of the ith column of $\bar{A}$. Thus C and $\bar{A}$ have the same rank. But $A \cap W/Z(G_n)$ has order p^m so that $\bar{A}$ has rank m. Thus C has rank m so that B has rank at least m and the proof of the theorem is complete.

3. **Wreath products.** Let G be any group and H a group of odd order. Let B be the base subgroup of the wreath product $W = G \operatorname{wr} H$. Suppose that there is a normal abelian subgroup A of W which contains an element $y \notin B$. Then we may express $y = bh$, for $b \in B$, $h \in H$. As a first step, we shall show that it is enough to consider only the case where H is cyclic and generated by h.

Indeed, if $y \in A$ then any conjugate of y is in A so that y will commute with any of its conjugates. Therefore, y will have this property in any homomorphic image of any subgroup containing it. On the other hand, if y should commute with all its conjugates then y and these conjugates will generate a normal abelian subgroup. Consequently, in order to be able to reduce to the case where $H = gp(h)$, we need only show that there is a homomorphic image of a subgroup containing y which is isomorphic with $G \operatorname{wr} gp(h)$. However, this is easily accomplished as follows: Let K be the group generated by B and y. Let $B = B_1 \times B_2$ where B_1 is generated by one of the factors of B (isomorphic with G) and all its conjugates under powers of y and B_2 is the product of the remaining factors of B. Then B_2 is a normal subgroup of K and $K/B_2 \cong G \operatorname{wr} gp(h)$.

Now we may suppose that bh is an element of a normal abelian subgroup of $G \operatorname{wr} gp(h)$. If h has order n then we may express $b = b_1 b_2 \cdots b_n$ where b_i is an element of the ith factor of B. Let $c = b_n$ if $b_n \neq 1$ and, if $b_n = 1$, then let c be any nonidentity element of the nth factor of B. Thus,

$$\begin{aligned}(c, bh) &= (c, h)(c, b)^h \\ &= c^{-1}c^h(c, b_1 \cdots b_n)^h \\ &= c_n^{-1}c_1\end{aligned}$$

where $c_n = c$ and c_1 is the element of the first factor of B corresponding to c. Therefore, $((bh)^c)^{bh} = (bh)^c$ implies, since $(bh)^c = bh(bh, c)$,

$$bh((c_1^{-1})^{b_1}c_n^{b_n})^h = bhc_1^{-1}c_n.$$

However, after cancelling the terms bh, the left-hand side has a nonidentity component in the second factor of the base subgroup, while the right-hand side does not, unless $n = 2$. But h has odd order, so this is a contradiction.

We shall now prove the second part of the theorem. Let G be any group and let $W = G \operatorname{wr} Z_p$. Let A be an abelian subgroup of W not contained in the base subgroup B. Then there is $h \in Z_p$ and $b \in B$ such that $bh \in A$, $bh \notin B$. We shall

now examine the centralizer of bh in B. Let $b' = b_1 \cdots b_p$ be an element of B commuting with bh. Then, with the obvious notation,

$$(b_1 \cdots b_p)^{bh} = b_1 \cdots b_p$$

so

$$b_p^b b_1^b \cdots b_{p-1}^b = b_1 \cdots b_p$$

and

$$b_1 = b_p^b, b_2 = b_1^b, \cdots, b_{n-1} = b_{n-2}^b .$$

Thus $b_1 \cdots b_p$ is determined by b once we know that it commutes with bh. But $AB = W$ so $A = gp(A \cap Bg, bh)$ and $A \cap B$ is an abelian subgroup of $C(bh)$. By the above, we see that $A \cap B$ has order at most a, where a is the order of the largest abelian subgroup of G. Hence, A has order at most pa. This proves Theorem 2.

At this point, we can complete the proof of Theorem 1, by construction of the appropriate 2-group. We shall, however, only sketch the proof and leave the tedious details to the interested reader. Let D_8 be a dihedral group of order eight generated by two elements x and y of order two. Let D be the central product of four copies of D_8 so D is generated by eight elements x_i, y_i, $i = 1,2,3,4$, of order two and has order 2^9. Every abelian subgroup of D has order at most 2^5. Let t be the automorphism of order eight of D which sends x_i and y_i to x_{i+1} and y_{i+1}, respectively, for $i = 1,2,3$, and x_4 to y_1, y_4 to x_1. Let H be the splitting extension of D by t. If $d \in D$ then $C_D(dt)$, $C_D(dt^2)$, $C_D(dt^4)$ have orders at most $2^2, 2^3, 2^5$, respectively. Therefore, every abelian subgroup of H has order at most 2^6 while H has order 2^{12}. Therefore, $W = H \operatorname{wr} Z_2$ has order 2^{25} while every abelian subgroup of W has order at most 2^{12}. Indeed, any abelian subgroup of W not in the base subgroup has order at most 2^7, while an abelian subgroup of the base subgroup is a subgroup of a direct product of two abelian subgroups of the factors, namely the projections on the two factors of the base subgroup. Similarly, $G = W \times W$ has order 2^{50} and all abelian subgroups of G have order at most 2^{24}.

4. **Alternating forms.** Let f and g be two alternating forms on an n-dimensional vector space V. We shall prove, by induction on n, that if $n = 2m$ or $n = 2m - 1$, with integral m, then there is an m-dimensional subspace of V on which f and g vanish. This will prove Theorem 3.

If $n = 2m$, then we can complete the proof by applying the induction hypothesis to any $n - 1 = 2m - 1$-dimensional subspace of V. If $n = 2m - 1$ then there is a nonzero vector v with $f(v,w) = 0$ for all $w \in V$. Let W be an $n-2$-dimensional subspace of V, not containing v, such that $g(v,w) = 0$ for all $w \in W$. This exists since the function $g(v, \cdot)$ is a linear functional of V. Let T be an $m - 1$-dimensional subspace of W on which f and g vanish. This exists by the induction hy-

pothesis. Let U be the m-dimensional subspace spanned by v and T so that f and g vanish on U and the theorem is proved.

Let G be a group as described in the hypothesis of Theorem 2. Then $G/Z(G)$ is an elementary abelian p-group of order p^{n-m} and therefore may be considered as a vector space over the integers modulo p. The subgroup G' is the direct product of two groups of order p, so assume that G' has a basis consisting of the elements z_f and z_g. If $xZ(G)$ and $yZ(G)$ are two cosets of $Z(G)$ in G then (x,y) depends only on the cosets and not on the particular representatives x and y. Thus,

$$(x,y) = z_f^{f(x,y)} z_g^{g(x,y)}$$

where $f(x,y)$ and $g(x,y)$ are integers modulo p. The functions f and g so defined are alternating forms on $G/Z(G)$. Let $H/Z(G)$ be a subspace of $G/Z(G)$ of dimension $[\frac{1}{2}(n-m+1)]$ so chosen that f and g both vanish on $H/Z(G)$. Then H is an abelian subgroup of G of the required order. Since $G' \leqq H$, H is also a normal subgroup.

5. **Subgroups of index p^3.** We shall recall briefly, for the convenience of the reader, the proof of the theorem corresponding to Theorem 4 for subgroups of index p^2. Let A be an abelian subgroup of index p^2 in the p-group G. Let M be a maximal subgroup of G containing A. Then, if A is the unique abelian maximal subgroup of M, A is certainly normal in G. If B is another abelian maximal subgroup of M, then $M = AB$, $A \cap B \leqq 2(M)$ and $(M : A \cap B) = p^2$ so that every maximal subgroup of M is abelian. But at least one maximal subgroup of M is normal in G so that G has a normal abelian subgroup of index p^2.

At this point, we turn to the proof of Theorem 4. Let A be an abelian subgroup of index p^3 in a p-group G. By means of the result of the preceding paragraph, we may assume that A is a normal subgroup of a maximal subgroup M of G. Let $x \in G$, $x \notin M$ so that $G = gp(M,x)$. If $A^x = A$ then A is normal in G and we are done. Therefore, we may assume that $A^x \neq A$. For i, any integer modulo p, let $A_i = x^{-i} A x^i$. Thus, $A = A_0$ and $A_i \neq A_j$ if $i \neq j$. We now divide the proof into the separate discussion of two major cases. We first suppose that the intersection of A_i and A_j, for any i and j with $i \neq j$, has index p in A_i and A_j.

In this case, suppose that A_2 is a subgroup of $A_0 A_1$. Then $A_i \leqq A_0 A_1$ for all i. In fact, if $A_{i-1} \leqq A_0 A_1$, then

$$A_i = A_{i-1}^x \leqq (A_0 A_1)^x = A_1 A_2 \leqq A_1 A_0 A_1 = A_0 A_1.$$

Therefore, $A^G \leqq A_0 A_1$ so that $A^G = A_0 A_1$. For this reason, $A_0 \cap A_1 \leqq Z(A^G)$. If $A_0 \cap A_1 \neq Z(A^G)$ then $Z(A^G)$ is a normal abelian subgroup of G and is of index at most p^3 in G. Thus, $A_0 \cap A_1 = Z(A^G)$. Let H be a normal subgroup of G, of index p in A^G, containing $Z(A^G)$. Therefore, H is abelian and of index p^3 in G.

Therefore, we may assume that $A_2 \not\leqq A_0A_1$. Now $(M:A_0A_1) = p$ so $A_1 \not\leqq A_0A_1$ implies that $M < A_0A_1A_2$. Consequently,

$$p^2 = (M:A_2) = ((A_0A_1)A_2:A_2) = (A_0A_1:A_0A_1 \cap A_2).$$

Also, $(A_0A_1:A_0) = (A_0:A_0 \cap A_2) = p$ so that $(A_0A_1:A_0 \cap A_2) = p^2$. However, $A_0 \cap A_2 \leqq A_0A_1 \cap A_2$, and both these subgroups have index p^2 in A_0A_1. Thus, $A_0A_1 \cap A_2 = A_0 \cap A_2$. Similarly, $A_0A_1 \cap A_2 = A_1 \cap A_2$. Therefore, $A_0 \cap A_2 = A_0 \cap A_1 \cap A_2$. Hence, since $A_0 \cap A_1 \cap A_2 \leqq Z(A_0A_1A_2) = Z(M), (M:Z(M)) \leqq p^3$. Also $Z(M)$ is a normal subgroup of G. Let H be a normal subgroup of G, of index p^2 in M and containing $A_0 \cap A_1 \cap A_2$. Then H is abelian and of index p^3 in G. This completes the proof of the first case.

We may now assume that $(A_j:A_i \cap A_j) = p^2$ for some i and j. Conjugating this equation by x^{-i}, we may assume that $i = 0$, so $(A:A \cap A_j) = p$.[2] Therefore, $M = AA_j$ and $Z(M) \geqq A \cap A_j$. If $Z(M) > A \cap A_j$ then $(M:Z(M)) \leqq p^3$ so that if H is a normal subgroup of G containing $Z(M)$ as a subgroup of index p, then H is abelian and $(G:H) \leqq p^3$. Hence, we may suppose that $Z(M) = A \cap A_j$.

If $A/Z(M)$ is cyclic then $A_j/Z(M)$ is cyclic since $Z(M)$ is normal in G and $A_j = x^{-j}Ax^j$. In this case let $A = gp(Z(M), a)$, $A_j = gp(Z(M), b)$. Since $M = AA_j$, M is of class two, so $a^{p^2} \in Z(M)$ implies $(a^{p^2}, b) = 1$ so

$$(a^p, b^p) = (a, b)^{p^2} = (a^{p^2}, b) = 1$$

and $L = gp(Z(M), a^p, b^p)$ is abelian. But $M/Z(M)$ is the direct product of two cyclic groups of order p^2 so that $L/Z(M)$ is the subgroup of $L/Z(M)$ of all elements of order at most p. Therefore, L is a normal subgroup of G and is of index p^3 in G.

Therefore, we may now suppose that $A/Z(M)$ is elementary abelian of order p^2. Thus, $A_j/Z(M)$ will also be elementary abelian and $M/Z(M)$ is elementary abelian of order p^4. If $x \in G$ and $x \notin M$ then x induces on $M/Z(M)$, by conjugation, an automorphism of order p. This may be considered as a linear transformation T of order p on a four-dimensional vector space over the integers modulo p. There are four possibilities for the Jordan form of T on $M/Z(M)$: one block of dimension two and two blocks of dimension one, two blocks of dimension two, one block of dimension three and one block of dimension one, or one four-dimensional block if $p \neq 3$. The case of four one-dimensional blocks cannot arise since A is not normal in G.

In the first case, we can choose four elements y_i, $i = 1,2,3,4$, which generate M together with $Z(M)$, such that

$$y_1^x = y_1y_2, y_2^x = y_2, y_3^x = y_3, y_4^x = y_4.$$

Since A is not a normal subgroup of G, it is easy to see that we may assume

that A is generated by y_1, y_3 and $Z(M)$. Thus, $(y_1, y_3) = 1$. Conjugating this equation by x we obtain

$$1 = (y_1y_2, y_3) = (y_1, y_3)(y_2, y_3) = (y_2, y_3).$$

Therefore, $gp(Z(M), y_2y_3)$ is a normal abelian subgroup of G and of index p^3 in G.

In the second case, we may similarly choose y_i such that

$$y_1^x = y_1y_2,\ y_2^x = y_2,\ y_3^x = y_3y_4,\ y_4 = y_4.$$

Furthermore, we may assume that either $A = gp(Z(M), y_1, y_4)$ or $A = gp(Z(M), y_1, y_3)$. If the first possibility occurs then $(y_1, y_4) = 1$ so that $(y_1y_2, y_4) = 1$ which implies $(y_2, y_4) = 1$. Hence, $gp(Z(M), y_2, y_4)$ is a normal abelian subgroup of G of index p^3 in G. If the second possibility happens then $(y_1, y_3) = 1$ so that successive conjugations by x give us

$$(y_1y_2, y_3y_4) = (y_1y_2^2, y_3y_4^2) = 1$$

or

$$(y_1, y_4)(y_2, y_3)(y_2, y_4) = 1,$$

$$(y_1, y_4)^2(y_2, y_3)^2(y_2, y_4)^4 = 1$$

and thus $(y_2, y_4)^2 = 1$. Since $p \neq 2$ this implies that $(y_2, y_4) = 1$ and $gp(Z(M), y_2, y_4)$ is the desired group.

The constructions of the desired abelian normal subgroup in the other two cases of the Jordan form are entirely similar to the above argument. However, their greater length and repetitious character stimulates us to omit these laborious details and leave them for the interested reader. This completes the proof of Theorem 4.

6. **Concluding remarks.** There is an entirely different method of constructing the p-group described in Theorem 1; this second way offers some hope for generalization and improvement of the result. At least it suggests a systematic attack rather than the search for a particular example. Let A_n be the group of all n by n matrices with "ones" on the main diagonal, zeros elsewhere, except in the last $n-2$ rows of the first two columns, where there are arbitrary elements of the field of p elements. The abelian group A_n acts naturally on an n-dimensional vector space V_n. The groups G_n, which we constructed, are a nonsplit extension of V_{n+2} by A_{n+2}. This suggests the study of all extensions of V_n by certain p-subgroups of the general linear group over the integers modulo p.

With regard to Theorem 4, we conjecture that if a p-group has an abelian subgroup of index p^n then it has an abelian normal subgroup of index p^n, unless p is one of a finite number of primes. The technique used to prove Theorem 4

might well be carried on to prove this conjecture for $n = 4$ or perhaps $n = 5$. But a radically new idea would be necessary to prove the result for general n. This makes the conjecture an interesting problem, and a good point to close on.

References

1. J. L. Alperin, *Two p-group counterexamples*, Abstract 579–15, Notices Amer. Math. Soc. **8** (1961), 160.

2. W. Burnside, *On some properties of groups whose orders are powers of primes*, Proc. London Math. Soc. (2) **11** (1912), 225–245; ibid. (2) **13** (1913), 6–12.

3. P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. (2) **36** (1932), 29–95.

4. P. Hall and G. Higman, *On the p-length of p-soluble groups*, Proc. London Math. Soc. (3) **6** (1956), 1–42.

5. A. J. Weir, *Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p*, Proc. Amer. Math. Soc. **6** (1955), 529–533.

Massachusetts Institute of Technology,
Cambridge, Massachusetts