ON A THEOREM OF PHILIP HALL

Daniel Gorenstein

Lemma 8.2 of "Solvability of Groups of Odd Order" by W. Feit and J. G. Thompson asserts that every finite p-group P possesses a characteristic subgroup C of class at most 2 with the following properties: (i) $C/3(C)$ is elementary abelian, (ii) $\mathfrak{C}_P(C) = 3(C)$, and (iii) $[P, C] \subseteq 3(C)$. Subgroups of essentially the same type were used by Thompson in an earlier paper "Normal p-complements for Finite Groups". We shall call a subgroup with these properties a critical subgroup of P.

If C is an arbitrary characteristic subgroup of P such that $\mathfrak{C}_P(C) = 3(C)$, it is easily seen that any nontrivial p'-automorphism of P remains nontrivial when restricted to C. This property of critical subgroups together with the restriction on their class are the crucial ones for the applications. However, in the present note we shall show that they can also be used to obtain a rather direct proof of a frequently quoted, unpublished,[1] theorem of Philip Hall which gives the structure of all p-groups having no noncyclic characteristic abelian subgroups.

We recall that a p-group P is said to be *extra-special* if P is of class 2 and $3(P) = P' = \phi(P)$ is of order p. It is convenient to include in the definition the trivial group $P = 1$.

LEMMA 1. *Let P be a p-group which has no noncyclic characteristic abelian subgroups and let C be a critical subgroup of P. Then the following hold:*

(i) *$3(C)$ is cyclic and C is the central product of an extra-special group E and $3(C)$.*

(ii) *If $R = \mathfrak{C}_P(E)$, then $3(C)$ is a self-centralizing normal subgroup of R and $P = ER$.*

Proof. Since C char P, our hypothesis implies that C contains no noncyclic characteristic abelian subgroups, so that, in particular, $Z = 3(C)$ is cyclic. Since $\mathfrak{C}_P(C) = Z$, the lemma follows with $E = 1$ and $R = P$ in case $C = Z$. Hence we may assume that $C \supset Z$, whence C is nonabelian. Since C/Z is elementary, we thus have $C' = \Omega_1(Z)$ is of order p. Assume first that $|Z| > p$.

Set $\bar{C} = C/C'$ and let $\bar{Z}$ be the image of Z in $\bar{C}$. If $\bar{A}$ is a cyclic subgroup of $\bar{C}$ of maximal order containing $\bar{Z}$, then $\bar{C} = \bar{A} \times \bar{E}$, where $\bar{E}$ is elementary, and $|\bar{A} : \bar{Z}| = 1$ or p. In either case $\bar{Z}\bar{E}$ char $\bar{C}$. Hence if E denotes the inverse image of $\bar{E}$ in C and we set $C_1 = EZ$,

---

[1] A proof appears in a set of unpublished lecture notes of Philip Hall.

then C_1 char C and so C_1 char P. But then also C_1 has no noncyclic characteristic abelian subgroups, whence $\mathfrak{Z}(C_1)$ is cyclic. Since $Z \subseteq Z(C_1)$ and $\bar{Z}$ is a maximal cyclic subgroup of the image $\bar{Z}\bar{E}$ of C_1 in $\bar{C}$, we have, in fact, $Z = \mathfrak{Z}(C_1)$. Since $\mathfrak{Z}(E) \subseteq \mathfrak{Z}(C_1) = Z$ and $E \cap Z = C'$, it follows that $\mathfrak{Z}(E) = C'$. Furthermore, $E' \neq 1$, since otherwise $C_1 = Z$ and C would by cyclic. Hence $E' = C'$ and so also $E/E' = E/C' = \bar{E}$ is elementary. But then $\phi(E) = E' = \mathfrak{Z}(E)$ and we conclude that E is extra-special.

Since $[P, C] \subseteq Z$, certainly $[P, E] \subseteq Z$. But $\mho^1(E) \subseteq \mathfrak{Z}(E)$, which implies that, in fact, $[P, E] \subseteq \Omega_1(Z) = C' = \mathfrak{Z}(E)$. Thus every element of P induces by conjugation an automorphism of E which acts trivially on the Frattini factor group $\bar{E}$ of E. It is well-known that any such automorphism of E is inner. Indeed, if $|\bar{E}| = p^k$, the number of such automorphisms is, on the one hand, at most p^k; while, on the other hand, the number of inner automorphisms of E is exactly p^k. From this the assertion follows.

This last result implies that $P = ER$, where $R = \mathfrak{C}_P(E)$. In particular, $C = E(C \cap R)$, $Z \subseteq R$, and $R \cap E = \Omega_1(Z)$. Hence $\bar{C} = \bar{B} \times \bar{E}$, where $\bar{B}$ is the image of $C \cap R$ in $\bar{C}$. But we know that $\bar{C} = \bar{A} \times \bar{E}$ with $\bar{A}$ cyclic; and it follows that $C \cap R$ is cyclic. But then $C \cap R \subseteq \mathfrak{Z}(C)$, whence $C \cap R = Z$. Thus $C = C_1 = EZ$ is the central product of an extra-special group and a cyclic group. Furthermore, $\mathfrak{C}_R(Z)$ centralizes both Z and E and so $\mathfrak{C}_R(Z) \subseteq \mathfrak{C}_P(C) = Z$. Hence Z is a self-centralizing normal subgroup of R and the lemma is proved when $|Z| > p$. However, if $|Z| = p$, then C itself is extra-special, and the preceding argument shows that $P = C$, so the lemma holds in this case as well.

The effect of this lemma is to reduce the problem of classifying p-groups which have no noncyclic characteristic abelian subgroups to a study of p-groups which contain a self-centralizing cyclic normal subgroup. For $m \geq 4$, we denote by D_m, Q_m, and S_m respectively the dihedral, generalized quaternion, and semi-dihedral groups of order 2^m. (Here $S_m = \langle x, y \mid x^{2^{m-1}} = y^2 = 1$ and $y^{-1}xy = x^{-1+2^{m-2}}\rangle$). We also introduce the groups $M_m(p) = \langle x, y \mid x^{p^{m-1}} = y^p = 1, y^{-1}xy = x^{1+p^{m-2}}\rangle$. We note for future use that $\Omega_i(M_m(p))$ is abelian of type (p^i, p), $1 \leq i \leq m - 2$, if p is odd or $m \geq 4$.

We next prove:

LEMMA 2. *Let P be a noncyclic p-group which contains a self-centralizing cyclic normal subgroup H of order p^n, $n \geq 2$. If $n = 2$, then P is extra-special of order p^3. If $n > 2$, then one of the following holds:*

(i) $p = 2$ and P is isomorphic to D_{n+1}, Q_{n+1}, or S_{n+1};

(ii) $M = \mathfrak{C}_P(\mho^1(H))$ is isomorphic to $M_{n+1}(p)$ and $\Omega_1(M)$ char P.

Proof. Since $\mathfrak{C}_P(H) = H$, $\bar{P} = P/H$ is isomorphic to a nontrivial p-subgroup of $A = \text{Aut } H$. The structure of A is well-known. First of all, if $n = 2$, an S_p-subgroup of A has order p, whence $|P| = p^3$. But then $\mathfrak{Z}(P) = P' = \phi(P)$ is of order p and so P is extra-special. (In fact, P is either dihedral, quaternion, or isomorphic to $M_3(p)$). Hence we may suppose $n > 2$ for the balance of the proof.

Now set $H = \langle x \rangle$. If $p = 2$, then A is abelian of type $(2^{n-2}, 2)$ with basis α, β, where $x\alpha = x^5$ and $x\beta = x^{-1}$; while if p is odd, an S_p-subgroup of A is cyclic of order p^{n-1} with generator α, where $x\alpha = x^{1+p}$. In the first case, set $\gamma = \alpha^{2^{n-3}}$ and in the second case, set $\gamma = \alpha^{p^{n-2}}$. Then $x\gamma = x^{1+p^{n-1}}$ in both cases. Furthermore, one computes directly that γ generates the subgroup of A which acts trivially on $\mho^1(H) = \langle x^p \rangle$.

Put $M = \mathfrak{C}_P(\mho^1(H))$. Then it follows from the preceding paragraph that either $|M : H| = p$ and $M = \langle x, y \rangle$, where $y^{-1}xy = x^{1+p^{n-1}}$, or else $p = 2$, $M = H$, $|P : H| = p$ and $P = \langle x, y \rangle$, where $y^{-1}xy = x^{-1}$ or $y^{-1}xy = x^{-5^{2^{n-3}}} = x^{-1+2^{n-1}}$. In the first and third cases it is possible to choose y so that $y^p = 1$, while in the second case, so that either $y^2 = 1$ or $y^2 = x^{2^{n-1}}$. We conclude that either M is isomorphic to $M_{n+1}(p)$ or that P is isomorphic to D_{n+1}, Q_{n+1}, or S_{n+1}.

Hence to complete the proof of the lemma, we need only show in the first instance that $\Omega_1(M)$ char P. Let $\bar{M}$ be the image of M in $\bar{P}$. If $\bar{P}$ is cyclic, then $\bar{M} = \Omega_1(\bar{P})$. Since $\Omega_1(P)$ maps into $\Omega_1(\bar{P})$, it follows that $\Omega_1(P) \subseteq \Omega_1(M)$, whence $\Omega_1(M) = \Omega_1(P)$ char P. On the other hand, if $\bar{P}$ is noncyclic, then $p = 2$ and P necessarily contains an element which inverts x. But then $\mho^1(H) = \langle x^2 \rangle \subseteq P'$. But $P' \subseteq H$ as $\bar{P}$ is abelian and so P' is cyclic. Hence $\mho^1(H)$ char P' char P and consequently $M = \mathfrak{C}_P(\mho^1(H))$ char P. But then $\Omega_1(M)$ char P in this case as well.

From these two lemmas, we can now easily derive our main result:

THEOREM (*P. Hall*). *If P is a p-group with no noncyclic characteristic abelian subgroups, then P is the central product of subgroups P_1 and P_2, where P_1 is extra-special and either P_2 is cyclic or $p = 2$ and P_2 is dihedral, generalized quaternion, or semi-dihedral.*

Proof. Let C be a critical subgroup of P and set $Z = \mathfrak{Z}(C)$. We may assume $P \supset C$, otherwise the theorem follows from Lemma 1. By Lemma 1, Z is cyclic, $C = EZ$, where E is extra-special, and $P = ER$, where $R = \mathfrak{C}_P(E)$, $\mathfrak{C}_R(Z) = Z$, and $R \supset Z$. In particular, $|Z| > p$.

Consider first the case $C = Z$. Then $R = P$. If $|Z| = p^2$, then P is extra-special of order p^3 by Lemma 2. On the other hand, if $|Z| \geqq p^3$, then by the same lemma either P is dihedral, generalized quaternion, or semi-dihedral, or else P contains a subgroup M isomorphic to $M_m(p)$ for some m with $\Omega_1(M)$ char P. Since $\Omega_1(M)$ is abelian of type (p, p), this latter case is impossible and so the theorem follows in all cases when $C = Z$.

Assume then that $C \supset Z$, so that $E \neq 1$ and $E' = \Omega_1(Z)$. If $|Z| = p^2$, then R is extra-special of order p^3, in which case $R/\Omega_1(Z)$ is elementary of type (p, p). But then $P/\Omega_1(Z)$ is elementary and it follows that P itself is extra-special. Thus we may suppose that $|Z| = p^n$, $n \geqq 3$. If R is dihedral, generalized quaternion, or semi-dihedral, the theorem follows with $P_1 = E$ and $P_2 = R$, so we may also assume that R is not of this form. But then if $M = \mathfrak{C}_R(\mho^1(Z))$, M is isomorphic to $M_{n+1}(p)$ by Lemma 2. Furthermore, $\mathfrak{C}_P(\mho^1(Z)) = EM$. On the other hand, $\mho^1(Z)$ char Z char P, and so EM char P. Thus to complete the proof of the theorem, it will suffice to show that EM possesses a noncyclic characteristic abelian subgroup.

Set $F = \Omega_1(EM)$. We shall argue that $\mathfrak{Z}(F)$ is noncyclic. Since M centralizes E and $E \cap M = E'$ is of order p, an element of F of order p is the product of elements of E and M each of order at most p^2. It follows from this that $F \subseteq E\Omega_2(M)$. But $\Omega_2(M)$ is abelian of type (p^2, p) since $|M| \geqq p^4$ and so $F \cap M \subseteq \mathfrak{Z}(F)$. Since $\Omega_1(M) \subseteq F \cap M$ and $\Omega_1(M)$ is abelian of type (p, p), we conclude that $\mathfrak{Z}(F)$ is noncyclic, and the theorem is proved.

When p is odd one can also show that the extra-special subgroup P_1 of P is necessarily of exponent p.

BIBLIOGRAPHY

1. W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 771–1029.
2. J. G. Thompson, *Normal p-complements for finite groups*, Math. Zeit. **72** (1960), 332–354.

NORTHEASTERN UNIVERSITY
BOSTON, MASSACHUSETTS