Can. J. Math., Vol. XXIII, No. 6, 1971, pp. 1023–1039

ISOMORPHIC SUBGROUPS OF FINITE p-GROUPS. II

GEORGE GLAUBERMAN

1. Introduction and notation. Suppose that we are given an isomorphism ϕ between two subgroups of index p in a finite p-group P. Let $N(\phi)$ be the largest subgroup of P fixed by ϕ. By a result of Sims [**2**, Proposition 2.1], $N(\phi)$ is a normal subgroup of P. In [**2**], we showed that $P/N(\phi)$ has nilpotence class at most two if $p = 2$, and at most three if p is odd. We then applied this result to investigate certain cases of the following question. Suppose that P is contained in a finite group G and that some subgroup of index p in P is a normal subgroup of G. Let α be an automorphism of P. Then, does α fix some non-identity normal subgroup of P that is normal in G?

In this paper, we consider *characteristic* subgroups of P rather than normal subgroups. For ϕ as above, we use the following notation:

(1.1) (a) *p is a prime;*
(b) *P is a finite p-group;*
(c) *Q and R are subgroups of index p in P;*
(d) *ϕ is an isomorphism of R onto Q;*
(e) $Q^* = N(\phi)$;
(f) *c is the nilpotence class of P/Q^*.*

We also consider the following hypothesis:

(1.2) (a) $P \subseteq G$;
(b) $Q \trianglelefteq G$;
(c) *G is generated by a subset $\mathscr{H}$ enjoying the property that, for every $h \in \mathscr{H}$, P is conjugate to P^h in $\langle P, P^h\rangle$.*

Note that (1.2) is satisfied when P is a Sylow subgroup of G or when G is generated by two conjugates of P.

For every group G and every positive integer i, let G_i be the ith term of the lower central series of G. Thus,

$$G_1 = G \text{ and } G_{i+1} = [G_i, G], \text{ for } i \geqq 1.$$

If G is a finite p-group for some prime p, let

$$\Omega_i(G) = \langle x | x \in G \text{ and } x^{p^i} = 1\rangle \text{ and } \mho^i(G) = \langle x^{p^i} | x \in G\rangle,$$

for $i = 1, 2, 3, \ldots$. In addition, define $\mathscr{A}(G)$ to be the set of all Abelian subgroups of maximal order in G and $J(G)$ to be the subgroup of G generated by the elements of $\mathscr{A}(G)$ (the *Thompson* subgroup of G).

Received March 12, 1971.

https://doi.org/10.4153/CJM-1971-107-9 Published online by Cambridge University Press

We obtain the following results:

THEOREM 1. *Assume* (1.1). *Then P satisfies at least one of the following conditions*:

(i) $\Omega_1(Z(P)) = \Omega_1(Z(Q)) = \Omega_1(Z(R))$;

(ii) (a) $p = 2$ *and* $P_{c+2}\mho^{c+1}(P) = Q_{c+2}\mho^{c+1}(Q) = R_{c+2}\mho^{c+1}(R)$, *or*

(b) $p = 3$ *and* $P_{c+2}\mho^{2}(P) = Q_{c+2}\mho^{2}(Q) = R_{c+2}\mho^{2}(R)$, *or*

(c) $p \geqq 5$ *and* $P_{c+2}\mho^{1}(P) = Q_{c+2}\mho^{1}(Q) = R_{c+2}\mho^{1}(R)$;

(iii) $J(P) = J(Q) = J(R)$;

(iv) P/Q^* *is Abelian.*

COROLLARY 1. *Let p be a prime, P be a finite p-group, and Q be a subgroup of index p in P. Then P and Q satisfy at least one of the following conditions*:

(A) *There exists a characteristic subgroup K of P enjoying the following properties*:

(A1) *Whenever ϕ satisfies* (1.1), *then $K \subseteq R$ and $\phi(K) = K$.*

(A2) *Let $\bar{P} = P/K$. Then $\bar{P}_4\mho^3(\bar{P}) = 1$, if $p = 2$, $\bar{P}_5\mho^2(\bar{P}) = 1$, if $p = 3$, and $\bar{P}_5\mho^1(\bar{P}) = 1$, if $p \geqq 5$.*

(B) *Whenever ϕ satisfies* (1.1), *then $P/N(\phi)$ is Abelian.*

THEOREM 2. *Let p be a prime, P be a finite p-group, and Q be a subgroup of index p in P. Then there exists a characteristic subgroup K of P that satisfies the following conditions*:

(a) *Whenever G is a group that satisfies* (1.2), *then $K \trianglelefteq G$.*

(b) *Let $\bar{P} = P/K$. Then $\bar{P}_4\mho^3(\bar{P}) = 1$, if $p = 2$, $\bar{P}_5\mho^2(\bar{P}) = 1$, if $p = 3$, and $\bar{P}_5\mho^1(\bar{P}) = 1$, if $p \geqq 5$.*

Some variations on Theorem 2 are given in Theorems 3.4 and 6.5.

Let us reconsider the question mentioned in the first paragraph. Suppose that P is a Sylow p-subgroup of G and that $C_G(Q) \subseteq Q$. If there exists a non-identity characteristic subgroup K of P that is normal in G, then K is fixed by α, regardless of the choice of α. Assume that $SL(2, p)$ is not involved in G. By results of J. Thompson and of the author [**1**, p. 19],

$$G = \langle C_G(Z(P)), N_G(J(P))\rangle.$$

If $J(P) \subseteq Q$, then $J(P) = J(Q)$ (by Lemma 2.1) and we can let $K = J(P)$. If $J(P) \nsubseteq Q$, then $P = J(P)Q$ and $N_G(J(P)) = N_G(P) \subseteq N_G(Z(P))$. Hence, we may take $K = Z(P)$, if $J(P) \nsubseteq Q$.

Thus, Theorem 2 is of interest mainly when $SL(2, p)$ is involved in G. Actually, Theorem 2 raises two much more general questions:

1. Can we find K if we remove the restriction that $|P/Q| = p$?

2. Can we find K independently of Q, even at the cost of slightly weakening condition (b) of Theorem 2?

The answers to these questions appear to depend on further investigation or discovery of 'interesting' characteristic subgroups of p-groups.

In general, we use the notation of our previous paper [**2**], to which we will refer as I. In particular, all groups considered in this paper are finite. We require the following additional notation. Let G be a group. For any subsets S and T of G, let $S - T$ be the set of all elements of S that lie outside T. Suppose that p is a prime and that G is a finite p-group. Then G is a *regular* p-group [**4**, Kap. III, § 10] if, for every $x, y \in G$,

$$x^p y^p \equiv (xy)^p, \text{ modulo } \mho^1(\langle x, y\rangle').$$

Acknowledgement. We thank Bowdoin College, the Institute for Advanced Study, the National Science Foundation, and the Sloan Foundation for their partial support during the writing of this article. We also thank Bowdoin College for the opportunity to present most of this work during the Bowdoin Finite Groups Seminar in the summer of 1970.

2. Preliminary results. We require a number of elementary results.

LEMMA 2.1 *Let G be a finite p-group.*
(a) *If $A \in \mathscr{A}(G)$, then $A = C_G(A)$.*
(b) *If $J(G) \subseteq H \subseteq G$, then $J(G) = J(H)$.*
(c) *If $H \subseteq G$ and $J(G) \cong J(H)$, then $J(G) = J(H)$.*

Proof. These statements are elementary consequences of the definitions. (For a proof of (a) and (b), see [**3**, pp. 271–272]. The proofs of (b) and (c) are similar.)

LEMMA 2.2. *Suppose that G is a group and that $H, K, L \trianglelefteq G$. Then*

$$[H, K, L] \subseteq [K, L, H][L, H, K].$$

Proof. Let $N = [K, L, H][L, H, K]$. For every subgroup X of G, let $\bar{X} = XN/N$. Then $[\bar{K}, \bar{L}, \bar{H}] = [\bar{L}, \bar{H}, \bar{K}] = 1$. By Lemma 2.6 of I, we have $[\bar{H}, \bar{K}, \bar{L}] = 1$.

LEMMA 2.3. *Suppose that G is a group and that $H, K \trianglelefteq G$. Assume that $G = HK$ and that $[H, K] \subseteq H'$. Then, for $i = 1, 2, 3, \ldots$,*
(a) *$[H_i, K] \subseteq H_{i+1}$,*
(b) *$[K_i, H] \subseteq H_{i+1}$, and*
(c) *$G_i = H_i K_i$.*

Proof. We use induction on i. By hypothesis, (a), (b), and (c) are true for $i = 1$. We will make frequent use of Lemma 2.2.

Suppose that $i \geqq 1$ and that (a), (b), and (c) are true for i. We prove them for $i + 1$.

(a) Here,

$$[H_{i+1}, K] = [H_i, H, K] \subseteq [H, K, H_i][H_i, K, H] \subseteq [H_2, H_i][H_{i+1}, K] \subseteq H_{i+1},$$

by induction.

(b) By (a) and induction,

$$[K_{i+1}, H] = [K_i, K, H] \subseteq [K, H, K_i][H, K_i, K] \subseteq [H_2, K_i][H_{i+1}, K] \subseteq [H, K_i, H][K_i, H, H]H_{i+2} \subseteq H_{i+2}.$$

(c) By (a), (b), and induction,

$$G_{i+1} = [G_i, G] = [H_iK_i, HK] = [H_i, H][H_i, K][K_i, H][K_i, K] \subseteq H_{i+1}K_{i+1}.$$

Thus, $G_{i+1} = H_{i+1}K_{i+1}$. This completes the proof of Lemma 2.3.

Suppose that P and ϕ satisfy (1.1) and that $N(\phi) = 1$. Then we define integers t, u, v and elements $x_1, \ldots, x_t$ of P as in Section 3 of I. Here, $p^t = |P|$; if P is Abelian, $u = t$; if P is not Abelian, u is the smallest positive integer such that $[x_i, x_{u+i}] \neq 1$ for some i; and $v = t - u$. For every $x \in P$, there exist unique elements $e(1), \ldots, e(t)$ of $\mathbf{Z}_p$ such that $x = x_1^{e(1)} \ldots x_t^{e(t)}$. Moreover, $\phi(x_i) = x_{i+1}$, for $i = 1, 2, \ldots, t - 1$.

If P and ϕ satisfy (1.1), then ϕ induces an isomorphism ϕ' of R/Q^* onto Q/Q^*, and $N(\phi') = 1$. In this case, we will define t, u, v, and $x_1, \ldots, x_t$ for P/Q^* as in the preceding paragraph. We use this notation in the next result.

LEMMA 2.4. *Assume* (1.1). *Suppose that P/Q^* is not Abelian. Then*
(a) $Z(P/Q^*) = \langle x_{v+1}, \ldots, x_u\rangle$ *and* $Z(Q/Q^*) = \langle x_{v+1}, \ldots, x_{u+1}\rangle$, *and*
(b) *if* $x \in (P/Q^*) - (Q/Q^*)$ *and* $y \in Z(Q/Q^*) - Z(P/Q^*)$, *then*

$$\langle [x, y]\rangle = \langle [x_1, x_{u+1}]\rangle \subseteq Z(P/Q^*).$$

Proof. This follows from Lemma 3.5 and Proposition 3.4(b) of I.

LEMMA 2.5. *Assume* (1.1). *Suppose that G is a group that contains P and that ψ is an isomorphism of P into G. Assume that the restriction of ψ to R is equal to ϕ. Then $N(\phi) \trianglelefteq \langle P, \psi(P)\rangle$.*

Proof. This follows directly from Lemma 2.4 of I.

LEMMA 2.6. *Suppose that H is a normal subgroup of a group G. Let A be the set of all automorphisms of G that centralize H and G/H. Then A is Abelian.*

Proof. Suppose that $\alpha, \beta \in A$ and that $g \in G$. Let $h = g^{-1}g^\alpha$ and $k = g^{-1}g^\beta$. Then $h, k \in H$ and $g^\alpha = gh$, $g^\beta = gk$. Let $f = gkg^{-1}$. Then $f \in H$, $k = g^{-1}fg$, and

$$k = k^\alpha = (g^{-1}fg)^\alpha = h^{-1}g^{-1}fgh = h^{-1}kh.$$

Thus, $hk = kh$. Now, $g^{\alpha\beta} = (gh)^\beta = gkh = ghk = g^{\beta\alpha}$.

LEMMA 2.7. *Suppose that S is a Sylow p-subgroup of a finite group G and that P is a weakly closed subgroup of S with respect to G. Then*:
(a) *For every $g \in G$, P is conjugate to P^g in $\langle P, P^g\rangle$.*
(b) *For every p-subgroup T of G that contains P, P is weakly closed in T with respect to G.*

(c) *Suppose that* $P \subseteq H \subseteq G$ *and that* $N \trianglelefteq H$.
Then PN/N *is weakly closed in some Sylow* p*-subgroup of* H/N *with respect to* H/N.

Proof. Special cases of parts (a) and (b) are proved in Lemmas 7.1 and 7.2 of I. However, the proofs are valid in the general case. Part (c) follows from part (b) by Lemma 7.9 of I.

We require a number of results on powers of products. For the following two results, we denote by $\binom{m}{n}$ the binomial coefficient whose value is $m!/n!(m-n)!$, for integers m, n such that $1 \leqq n \leqq m$.

PROPOSITION 2.8. (P. Hall-Petrescu). *Let* G *be a group generated by two elements* x, y. *Then there exist elements* $C_i \in G_i$ $(i = 1, 2, 3, \ldots)$ *such that, for every positive integer* m,

$$x^m y^m = (xy)^m C_2^{\binom{m}{2}} \ldots C_{m-1}^{\binom{m}{m-1}} C_m.$$

Proof. This is proved in [**4** p. 317] for a free group on two generators. Since G must be a homomorphic image of such a free group, the result follows.

COROLLARY 2.9. *Let* p *be a prime and* G *be a* p*-group generated by two elements* x, y. *Then*
(a) $x^p y^p \equiv (xy)^p$, *modulo* $\mho^1(G_2)G_p$, *and*
(b) $x^{p^2} y^{p^2} \equiv (xy)^{p^2}$, *modulo* $\mho^2(G_2)\mho^1(G_p)G_{p+2}$.

Proof. For $i = 1, 2, \ldots, p-1$, $\binom{p}{i}$ is divisible by p, and $\binom{p^2}{i}$ is divisible by p^2. Furthermore, $\binom{p^2}{i}$ is divisible by p for $i = p$ and $i = p + 1$. Apply Proposition 2.8.

Corollary 2.9(a) yields the next result:

LEMMA 2.10. *If* p *is a prime,* G *is a* p*-group, and* $G_p = 1$, *then* G *is a regular* p*-group.*

LEMMA 2.11. *Suppose that* p *is a prime and that* G *is a regular* p*-group.*
(a) *For all* $x \in \Omega_1(G)$, $x^p = 1$.
(b) *If* $x, y \in G$, *then* $x^p = y^p$ *if and only if* $(xy^{-1})^p = 1$.

Proof. This is proved in [**4**, pp. 324–327].

LEMMA 2.12. *Suppose that* p *is a prime and that* G *is a* p*-group generated by two elements* x, y. *Assume that* $x^p = 1$. *For all* $i \geqq 2$,

$$\mho^1(G_i) \subseteq G_{i+p-1}.$$

Proof. We use induction on i. Let $H = \langle x, G_2 \rangle$. Then $H_p \subseteq G_{p+1}$. So, by Lemma 2.10, H/G_{p+1} is a regular p-group. Now, $H \trianglelefteq G$. Let $H^* = \langle x^g | g \in G \rangle$.

Then $H^* \trianglelefteq G$, $H^* \subseteq H$, and G/H^* is cyclic. Hence, $H^* \supseteq G_2$ and $H^* = H$. Therefore, H and H/G_{p+1} are generated by elements of order p. By Lemma 2.11, H/G_{p+1} has exponent 1 or p. So $\mho^1(G_2) \subseteq G_{p+1}$.

Suppose that $i \geqq 2$ and that $\mho^1(G_i) \subseteq G_{i+p-1}$. We wish to prove that $\mho^1(G_{i+1}) \subseteq G_{i+p}$. By considering G/G_{i+p}, if necessary, we may assume that $G_{i+p} = 1$. Since

$$(G_i)_p \subseteq G_{pi} \subseteq G_{i+p} = 1,$$

G_i is regular, by Lemma 2.10. Take any $w \in G_i$ and $z \in G$. By induction, $w^p \in G_{i+p-1} \subseteq Z(G)$. Hence,

$$1 = [w^p, z] = w^{-p}(w^z)^p.$$

Thus, $w^p = (w^z)^p$. By Lemma 2.11, $(w^{-1}w^z)^p = 1$. So

$$[w, z] = w^{-1}w^z \in \Omega_1(G_i).$$

Since w and z are arbitrary, $G_{i+1} = [G_i, G] \subseteq \Omega_1(G_i)$. By Lemma 2.11, G_{i+1} has exponent 1 or p. Hence, $\mho^1(G_{i+1}) = 1 \subseteq G_{i+p}$, as desired.

LEMMA 2.13. *Let p be a prime and Q be a subgroup of index p in a finite p-group P. Suppose that $x \in P - Q$ and that $x^p = 1$. Then*:

(a) *For $1 \leqq i \leqq p$, $P_i\mho^1(P) = P_i\mho^1(Q)$.*

(b) *If $p = 2$, then $P_3\mho^2(P) = P_3\mho^2(Q)$ and $P_4\mho^3(P) = P_4\mho^3(Q)$.*

(c) *If $p = 3$ and $1 \leqq i \leqq 5$, then $P_i\mho^2(P) = P_i\mho^2(Q)$.*

Proof. Take $x \in P - Q$ such that $x^p = 1$. For every $z \in P - Q$ and $i \geqq 1$, there exists $y \in Q$ such that $\langle z^{p^i}\rangle = \langle (xy)^{p^i}\rangle$. Now choose an arbitrary element y of Q and let $S = \langle x, y\rangle$.

(a) Suppose that $1 \leqq i \leqq p$. By Corollary 2.9, $(xy)^p \equiv x^py^p \equiv y^p$, modulo $\mho^1(S_2)S_p$. Since $S_2 \subseteq Q$ and $S_p \subseteq P_p \subseteq P_i$, $(xy)^p \in \mho^1(Q)P_i$. As y is arbitrary, $\mho^1(P) \subseteq P_i\mho^1(Q)$. Therefore,

$$P_i\mho^1(P) = P_i\mho^1(Q).$$

(b) Suppose that $p = 2$. By Corollary 2.9 and Lemma 2.12, $(xy)^4 \equiv x^4y^4 \equiv y^4$, modulo S_3. Consequently, $\mho^2(P) \subseteq P_3\mho^2(Q)$ and $P_3\mho^2(P) = P_3\mho^2(Q)$. Take $z \in S_3$ such that $(xy)^4 \equiv y^4z$, modulo S_4. Then $(xy)^8 \equiv y^8z^2$, modulo S_4. By Lemma 2.12, $\mho^1(S_3) \subseteq S_4$. Hence,

$$P_4\mho^2(P) = P_4\mho^2(Q).$$

(c) Suppose that $p = 3$ and that $1 \leqq i \leqq 5$. By Corollary 2.9 and Lemma 2.12, $(xy)^9 \equiv x^9y^9 \equiv y^9$, modulo S_5. Therefore,

$$P_i\mho^2(P) = P_i\mho^2(Q).$$

3. Statement of main results. In this section, we state the main results of the paper and derive the results of § 1 from them.

LEMMA 3.1. *Assume* (1.1). *Then* ϕ *falls into at least one of the following cases*:
(i) $\Omega_1(Z(P)) = \Omega_1(Z(Q))$,
(ii) $C_P(Q) \not\subseteq Q^*$ *and* $\Omega_1(Z(P)) \neq \Omega_1(Z(Q))$,
(iii) $J(P) = J(Q)$,
(iv) $Z(P) \subset Z(Q) \subseteq Q^*$ *and* $J(P) \neq J(Q)$.

Proof. Assume that ϕ violates (i), (ii), and (iii), and observe that ϕ satisfies (iv).

For our next result, we use the following restrictions on integers d, m, and n.

(3.1) (a) *If* $p = 2$, *then* $m = d = 3$ *and* $n = 2$, *or* $m = 4$ *and* $n = 3$.
(b) *If* $p = 3$, *then* $m = d = 3$ *and* $n = 1$, *or* $d \leqq m \leqq 5$ *and* $n = 2$.
(c) *If* $p \geqq 5$, *then* $d \leqq m \leqq 5$ *and* $n = 1$.

THEOREM 3.2. *Assume* (1.1). *If case* (i) *of Lemma* 3.1 *occurs, then* $\Omega_1(Z(P)) = \Omega_1(Z(Q)) = \Omega_1(Z(R))$.

Suppose that case (ii) *occurs. Let* $d = c + 1$, *if* $[P, Z(Q)] \not\subseteq Q^*$ *or* $[P, Z(R)] \not\subseteq Q^*$, *and let* $d = c + 2$, *otherwise. Suppose that* d, m, *and* n *satisfy* (3.1). *Then* $P_i = Q_i = R_i$, *for all* $i \geqq d$, *and*

$$P_m\mho^n(P) = Q_m\mho^n(Q) = R_m\mho^n(R).$$

If case (iii) *occurs, then* $J(P) = J(Q) = J(R)$.
If case (iv) *occurs, then* P/Q^* *is Abelian and*

$$Q^* = C_P(Z(Q^*)).$$

Remark. Since P/Q^* is Abelian when $c = 1$, in case (ii) we always have $3 \leqq d \leqq 4$, if $p = 2$, and $3 \leqq d \leqq 5$, if p is odd.

It is easy to verify cases (i) and (iii) of Theorem 3.2. (See Lemma 2.1 for case (iii).) The proofs of cases (ii) and (iv) are given in §§ 4 and 5.

Note that Theorem 3.2 yields Theorem 1. To obtain Corollary 1 from Theorem 1, let K be a characteristic subgroup of P that is maximal with respect to property (A1); since 1 satisfies (A1), K must exist. If K satisfies (A2), we are done. Assume that K violates (A2). Take any ϕ that satisfies (1.1). Then $\phi(K) = K$ and $K \subseteq Q^*$. Hence, ϕ induces an isomorphism ϕ' of R/K onto Q/K. By the maximal choice of K, $\Omega_1(Z(P/K)) \neq \Omega_1(Z(Q/K))$. Similar arguments show that ϕ' violates conditions (i), (ii), and (iii) of Theorem 1. Therefore, $(P/K)/N(\phi')$ is Abelian. Since $N(\phi') = Q^*/K$, P/Q^* is Abelian.

THEOREM 3.3. *Let* p *be a prime*, P *be a finite* p-*group*, *and* Q *be a subgroup of index* p *in* P. *Let* $\hat{Q} = \bigcap_{\alpha \in \mathrm{Aut} P} Q^\alpha$. *Then* P *satisfies at least one of the following conditions*:
(i) $\Omega_1(Z(P)) = \Omega_1(Z(Q))$;
(ii) (a) $p = 2$ *and* $P_4\mho^3(P) = Q_4\mho^3(Q)$, *or*
(b) $p = 3$ *and* $P_5\mho^2(P) = Q_5\mho^2(Q)$, *or*
(c) $p \geqq 5$ *and* $P_5\mho^1(P) = Q_5\mho^1(Q)$;
(iii) $J(P) = J(Q)$;
(iv) $\hat{Q} \trianglelefteq G$, *for every group* G *that satisfies* (1.2).

Note that in Theorem 3.3 and in the next theorem, $\hat{Q}$ is a characteristic subgroup of P and $P/\hat{Q}$ is an elementary Abelian group. To obtain Theorem 2 from Theorem 3.3, let K be a characteristic subgroup of P that is maximal with respect to the condition (a) of Theorem 2. By Theorem 3.3, we obtain condition (b) of Theorem 2.

(3.2) (a) $P \subseteq G$.
(b) $Q \trianglelefteq G$.
(c) *For some Sylow p-subgroup S of G, P is a weakly closed subgroup of S with respect to G.*

THEOREM 3.4. *Let p be a prime, P be a finite p-group, and Q be a subgroup of index p in P. Let $\hat{Q} = \bigcap_{\alpha \in \mathrm{Aut} P} Q^{\alpha}$. Then P satisfies at least one of the following conditions*:
(i) $\Omega_1(Z(P)) = \Omega_1(Z(Q))$;
(ii) (a) $p = 2$ *and* $P_3\mho^2(P) = Q_3\mho^2(Q)$, *or*
(b) $p = 3$ *and* $P_4\mho^2(P) = Q_4\mho_2(Q)$, *or*
(c) $p \geqq 5$ *and* $P_3\mho^1(P) = Q_3\mho^1(Q)$;
(iii) $J(P) = J(Q)$;
(iv) *whenever G is a group that satisfies* (3.2), *then* $Z(P) \trianglelefteq G$ *or* $\hat{Q} \trianglelefteq G$.

Assuming Theorem 3.4, we obtain the following result:

COROLLARY 3.5. *Let p be a prime, P be a finite p-group, and Q be a subgroup of index p in P. Then P satisfies at least one of the following conditions*:
(a) *whenever G is a group that satisfies* (3.2), *then there exists a non-identity characteristic subgroup K of P such that $K \trianglelefteq G$*;
(b) $p = 2$ *and* $P_3\mho^2(P) = 1$, *or* $p = 3$ *and* $P_4\mho^2(P) = 1$, *or* $p \geqq 5$ *and* $P_3\mho^1(P) = 1$.

Proof. Assume that P violates (b). Let L be a characteristic subgroup of P that is maximal with respect to the property that $L \trianglelefteq G$ whenever G satisfies (3.2). If $L \neq 1$, we have (a). Assume that $L = 1$. By the maximal choice of L, the groups P and Q must violate conditions (i), (ii), and (iii) of Theorem 3.4. Therefore, for every G that satisfies (3.2), $Z(P)$ or $\hat{Q}$ is a normal subgroup of G. Since P violates (b), $Z(P) \neq 1$ and $\hat{Q} \neq 1$. Hence, we obtain (a).

4. Case (ii). We now treat case (ii) of Lemma 3.1 and obtain case (ii) of Theorem 3.2.

THEOREM 4.1. *Assume* (1.1) *and assume that $C_P(Q) \not\subseteq Q^*$. Then*:
(a) *We have $P = C_P(Q^*)Q$.*
(b) *For all $i \geqq c + 2$, $P_i = Q_i = R_i$, and ϕ fixes P_i.*
(c) *If $[P, Z(Q)] \not\subseteq Q^*$ or $[P, Z(R)] \not\subseteq Q^*$, then $P_{c+1} = Q_{c+1} = R_{c+1}$, and ϕ fixes P_{c+1}.*

Proof. Suppose that $C_P(Q^*) \subseteq Q$. Since ϕ fixes Q^*, $\phi^{-1}(C_P(Q^*)) \subseteq C_P(Q^*)$. So $C_P(Q^*) \subseteq N(\phi) = Q^*$. Then $C_P(Q) \subseteq Q^*$, contrary to hypothesis. This proves (a).

Since $\phi(R_i) = Q_i$ and $R_i \subseteq P_i$, for all i, it now suffices to prove that $P_i = Q_i$, for all $i \geqq c + 2$, and that $P_{c+1} = Q_{c+1}$ in case (c). Take $x_1, \ldots, x_t \in P/Q^*$ as in Lemma 2.4. Let y_1 be an element of x_1, and let $y_i = \phi^{i-1}(y_1)$, for $i = 2, 3, \ldots, t$. Take $x \in C_P(Q) - Q^*$.

Suppose that $x \notin Q$. Then $C_P(x) \supseteq \langle x, Q\rangle = P$. Thus, $x \in Z(P)$ and $P = \langle Q, x\rangle$. In this case, $P_i = Q_i$, for all $i \geqq 2$, by induction. Therefore, for the remainder of the proof, we assume that $x \in Q$.

We have

$$xQ^* = x_r^{d(r)} \ldots x_s^{d(s)}, \tag{4.1}$$

for some $d(r), \ldots d(s) \in \mathbf{Z}_p$ and some r, s such that $d(r)$ and $d(s)$ are nonzero and $2 \leqq r \leqq s \leqq t$. Let $m = s - r + 1$ and $y = \phi^{-(r-1)}(x)$. Since

$$xQ^* \in Z(Q/Q^*),$$

Lemma 2.4 yields that $v + 1 \leqq r \leqq s \leqq u + 1$. Hence,

$$m \leqq t - 1 \text{ and } m \leqq u - v + 1. \tag{4.2}$$

As x centralizes Q, x centralizes $y_r, \ldots, y_s$. So

$$y \textit{ centralizes } y_1, \ldots, y_m. \tag{4.3}$$

Moreover,

$$yQ^* = x_1^{d(r)} \ldots x_m^{d(s)} \textit{ and } \langle y_1, \ldots, y_m, Q^*\rangle = \langle y, y_2, \ldots, y_m, Q^*\rangle. \tag{4.4}$$

Let $A = \langle y, \phi(y), \ldots, \phi^{t-m}(y)\rangle$. Since $x \in C_P(Q^*)$ and ϕ fixes Q^*, it follows that $y \in C_P(Q^*)$ and that

$$A \subseteq C_P(Q^*). \tag{4.5}$$

Suppose that $0 \leqq i \leqq t - m$. By (4.4),

$$\phi^i(y)Q^* = x_{i+1}^{d(r)} \ldots x_{i+m}^{d(s)}$$

and

$$\begin{aligned} P &= \langle y, \phi(y), \ldots, \phi^i(y), y_{i+1}, \ldots, y_{i+m-1}, \phi^{i+1}(y), \ldots, \phi^{t-m}(y), Q^*\rangle \\ &= \langle A, Q^*, y_{i+1}, \ldots, y_{i+m-1}\rangle, \textit{for } i = 0, 1, \ldots, t - m. \end{aligned} \tag{4.6}$$

By (4.3), $\phi^i(y)$ centralizes $y_{i+1}, \ldots, y_{i+m-1}$. So

$$P = \langle A, Q^*, C_P(\phi^i(y))\rangle, \textit{for } i = 0, 1, \ldots, t - m. \tag{4.7}$$

By (4.2), $v \leqq t - m$ and $v + m - 1 \leqq u$. Take $i = v$ in (4.6); we have

$$P = \langle AQ^*, y_{v+1}, \ldots, y_{v+m-1}\rangle \subseteq \langle AQ^*, y_{v+1}, \ldots, y_u\rangle.$$

By Lemma 2.4, $Z(P/Q^*) = \langle x_{v+1}, \ldots, x_u\rangle$. So $P/Q^* = (AQ^*/Q^*)Z(P/Q^*)$. Hence, $AQ^*/Q^* \trianglelefteq P/Q^*$ and $Q^*A = AQ^* \trianglelefteq P$.

https://doi.org/10.4153/CJM-1971-107-9 Published online by Cambridge University Press

Take any i such that $0 \leqq i \leqq t - m$. By (4.5) and (4.7),

$$P = C_P(\phi^i(y))Q^*A = C_P(\phi^i(y))A.$$

Consequently, for every $g \in P$ there exists $a \in A$ such that

$$(\phi^i(y))^g = (\phi^i(y))^a.$$

Since the elements $\phi^i(y)$ generate A, it follows that $A^g \subseteq A$ for every $g \in P$. Thus, $A \trianglelefteq P$. Hence, $A' \trianglelefteq P$. The above argument also shows that, for each i, the coset $\phi^i(y)A'$ lies in the center of P/A'. Therefore, $[A, Q] \subseteq [A, P] \subseteq A'$.

Since $y \in P - Q$, $P = AQ$. By Lemma 2.3,

$$(4.8) \qquad P_i = A_iQ_i, \textit{for all } i \geqq 1.$$

Since P/Q^* has nilpotence class c, $A_{c+1} \subseteq P_{c+1} \subseteq Q^*$. For $i \geqq c + 2$,

$$A_i \subseteq A_{c+2} \subseteq [Q^*, A] = 1.$$

By (4.8), this proves (b).

We now consider (c). Suppose that $[P, Z(Q)] \not\subseteq Q^*$ or $[P, Z(R)] \not\subseteq Q^*$. Replacing ϕ by ϕ^{-1}, if necessary, we may assume that $[P, Z(Q)] \not\subseteq Q^*$. Then P/Q^* is not Abelian. So $c \geqq 2$, $u \leqq t - 1$, and $v \geqq 1$. We may assume that $[P, \langle x\rangle] \not\subseteq Q^*$. By (4.1) and Lemma 2.4, $s = u + 1$. Thus,

$$(4.9) \qquad s = u + 1, m = s - r + 1 = u + 2 - r, t - m = v + r - 2.$$

By Lemma 2.4, $Z(P/Q^*) = \langle x_{v+1}, \ldots, x_u\rangle$. Since $P_{c+1} \subseteq Q^*$,

$$(4.10) \qquad A_c \subseteq P_c \subseteq \langle y_{v+1}, \ldots, y_u, Q^*\rangle$$

Let i be an integer such that $0 \leqq i \leqq v - 1$. Then

$$(4.11) \qquad 2 + i \leqq v + 1 \leqq u \leqq u + i \leqq t.$$

Since x centralizes $y_2, \ldots, y_{u+1}, Q^*$, it follows that $\phi^i(x)$ centralizes $y_{2+i}, \ldots, y_{u+i+1}, Q^*$. By (4.10) and (4.11),

$$(4.12) \qquad \phi^i(x) \textit{ centralizes } A_c, \textit{ if } 0 \leqq i \leqq v - 1.$$

Now choose an integer i such that $1 \leqq i \leqq r - 1$. We obtain, similarly, that $1 \leqq r - i \leqq u + 1 - i \leqq t$, and that

$$(4.13) \qquad \phi^{-i}(x) \textit{ centralizes } \langle y_{r-i}, \ldots, y_{u+1-i}, Q^*\rangle.$$

Suppose that $1 \leqq j \leqq i - 1$. Then $2 - r \leqq j - (r - 1) \leqq j - i \leqq -1$. Since Q centralizes x, $\phi^{j-i}(x)$ centralizes x. So $\phi^{-i}(x)$ centralizes $\phi^{-j}(x)$. Thus,

$$(4.14) \qquad \phi^{-i}(x) \textit{ centralizes } \phi^{-(i-1)}(x), \ldots, \phi^{-1}(x).$$

By (4.9), $s = u + 1$. Hence, by (4.13), (4.14), and (4.1),

$$\begin{aligned} C_P(\phi^{-i}(x)) &\supseteq \langle y_{r-i}, \ldots, y_{u+1-i}, \phi^{-(i-1)}(x), \ldots, \phi^{-1}(x), Q^*\rangle \\ &= \langle y_{r-i}, \ldots, y_u, Q^*\rangle. \end{aligned}$$

Therefore,

(4.15) $\phi^{-i}(x)$ *centralizes* A_c, *if* $1 \leqq i \leqq r - 1$.

By (4.1) and (4.9), $x = \phi^{r-1}(y)$ and $t - m = (r - 1) + (v - 1)$. Consequently, (4.12) and (4.15) yield that

$$C_P(A_c) \supseteq \langle \phi^{-(r-1)}(x), \ldots, \phi^{-1}(x), x, \phi(x), \ldots, \phi^{v-1}(x) \rangle$$
$$= \langle y, \phi(y), \ldots, \phi^{t-m}(y) \rangle = A.$$

Thus, $A_{c+1} = [A_c, A] = 1$. By (4.8), $P_{c+1} = Q_{c+1}$. This completes the proof of (c) and of the theorem.

PROPOSITION 4.2. *Assume* (1.1) *and assume that* $\Omega_1(Z(P)) \neq \Omega_1(Z(Q))$ *and that* $C_P(Q) \nsubseteq Q^*$. *Then*:

(a) *There exists* $x \in C_P(Q) - Q^*$ *such that* $x^p = 1$.

(b) *For* $1 \leqq i \leqq p$, $P_i\mho^1(P) = P_i\mho^1(Q) = P_i\mho^1(R)$.

(c) *If* $p = 2$, *then* $P_3\mho^2(P) = P_3\mho^2(Q) = P_3\mho^2(R)$, *and*

$$P_4\mho^3(P) = P_4\mho^3(Q) = P_4\mho^3(R).$$

(d) *If* $p = 3$ *and* $1 \leqq i \leqq 5$, *then* $P_i\mho^2(P) = P_i\mho^2(Q) = P_i\mho^2(R)$.

Proof. Suppose that $\Omega_1(Z(Q)) \subseteq Q^*$. By Theorem 4.1(a), $P = QC_P(Q^*)$. Hence, $\Omega_1(Z(Q)) \subseteq Z(P)$, and the hypothesis yields that

$$\Omega_1(Z(Q)) \subset \Omega_1(Z(P)).$$

Since $\Omega_1(Z(P)) \cap Q \subseteq \Omega_1(Z(Q))$, there exists $x \in \Omega_1(Z(P)) - Q$, which proves (a) in this case. Since (a) is obvious when $\Omega_1(Z(Q)) \nsubseteq Q^*$, we obtain (a) in all cases.

Take x as in (a) and take $r \geqq 0$ maximal such that $\phi^{-r}(x)$ is defined. Then $\phi^{-r}(x)$ has order p and $P = \langle \phi^{-r}(x), Q \rangle$. Similarly, P is generated by R and $\phi^s(x)$, for some s. Now (b), (c), and (d) follow from Lemma 2.13.

Since $\phi(R_i\mho^j(R)) = Q_i\mho^j(Q)$, for all $i, j \geqq 1$, Theorem 4.1 and Proposition 4.2 yield the following result:

THEOREM 4.3. *Assume* (1.1) *and assume that* $\Omega_1(Z(P)) \neq \Omega_1(Z(Q))$ *and that* $C_P(Q) \nsubseteq Q^*$. *Let* $d = c + 1$, *if* $[P, Z(Q)] \nsubseteq Q^*$ *or* $[P, Z(R)] \nsubseteq Q^*$, *and let* $d = c + 2$, *otherwise. Suppose that* d, m, *and* n *satisfy* (3.1). *Then* $P_m\mho^n(P) = Q_m\mho^n(Q) = R_m\mho^n(R)$, *and* ϕ *fixes* $P_m\mho^n(P)$.

5. Case (iv). In this section, we consider the following hypotheses:

(5.1) (a) (1.1) *holds*;
(b) $Z(P) \subset Z(Q) \subseteq Q^*$.

(5.2) (a) (5.1) *holds*;
(b) $J(P) \neq J(Q)$.

We first require a general lemma.

LEMMA 5.1. *Suppose that p is a prime and that T is a subgroup of index p in a p-group S. Let $A \in \mathscr{A}(S)$. Assume that $Z(T) \not\subseteq Z(S)$ and that $A \not\subseteq T$. Then:*
(a) $Z(S) \cap T = Z(T) \cap A = C_{Z(T)}(A)$,
(b) $(A \cap T)Z(T) \in \mathscr{A}(S)$, *and*
(c) $|Z(T)/(Z(S) \cap T)| = p$.

Proof. Since $[S:T] = p$, $T \lhd S$ and $S = AT$. Therefore, $|A/(A \cap T)| = p$ and $Z(S) \cap T = Z(T) \cap C_S(A) = Z(T) \cap A$, by Lemma 2.1. Consequently, $Z(T) \not\subseteq A$, because $Z(T) \not\subseteq Z(S)$. Let $A^* = (A \cap T)Z(T)$. Then A^* is Abelian and

$$|A^*| \geqq p|A \cap T| = |A|.$$

Since $A \in \mathscr{A}(S)$, $A^* \in \mathscr{A}(S)$. So

$$\begin{aligned} p|A \cap T| = |A| = |A^*| &= |A \cap T|\,|Z(T)/(Z(T) \cap A)| \\ &= |A \cap T|\,|Z(T)/(Z(S) \cap T)|. \end{aligned}$$

Thus, $|Z(T)/(Z(S) \cap T)| = p$. This completes the proof of Lemma 5.1.

LEMMA 5.2. *Assume* (5.2). *Then there exists $A \in \mathscr{A}(P)$ such that $A \not\subseteq Q$ and*

$$|A/(A \cap Q^*)| = |Z(Q^*)/C_{Z(Q^*)}(A)| = p.$$

Moreover, for every such A and every $x \in A - Q^*$, $|Z(Q^*)/C_{Z(Q^*)}(x)| = p$.

Proof. By Lemma 2.1, $J(P) \not\subseteq Q$. So $J(P) \not\subseteq Q^*$. Take $A \in \mathscr{A}(P)$ such that $|A \cap Q^*|$ is maximal subject to the condition that $A \not\subseteq Q^*$. Take $r \geqq 0$ maximal such that every element of A lies in the image of ϕ^r. Then $\phi^{-r}(A) \not\subseteq Q$, by the maximal choice of r. Since ϕ fixes Q^*, $|\phi^{-r}(A) \cap Q^*| = |\phi^{-r}(A \cap Q^*)| = |A \cap Q^*|$. Therefore, we may assume that $A \not\subseteq Q$.

Let $A^* = (A \cap Q)Z(Q)$. By Lemma 5.1, $A^* \in \mathscr{A}(P)$. Moreover,

$$|A^* \cap Q^*| \geqq |(A \cap Q^*)Z(Q)| > |A \cap Q^*|.$$

By the maximal choice of A, $A^* \subseteq Q^*$. Thus, $A \cap Q = A \cap Q^*$, and

$$|A \cap Q^*| = |A \cap Q| = |A|/p.$$

Let $X = Z(Q^*)$ and $S = AQ^*$. By (5.1), $X \supseteq Z(Q)$ and $X \not\subseteq A$. Since $Z(S) \subseteq C_S(A) = A$, $X \not\subseteq Z(S)$. By Lemma 5.1,

$$|X/C_X(A)| = |X/(A \cap X)| = p.$$

For every $x \in A - Q^*$, we have $A = \langle A \cap Q^*, x\rangle$ and, hence,

$$C_X(A) = C_X(x).$$

This completes the proof of Lemma 5.2.

LEMMA 5.3. *Assume* (5.1). *Then* $C_P(Z(Q^*)) = Q^*$.

Proof. Let $S = C_P(Z(Q^*))$. Then $S \subseteq C_P(Z(Q)) = Q$, by (5.1). So $|\phi^{-1}(S)| = |S|$. Since ϕ fixes Q^*, $\phi^{-1}(S) \subseteq S$. Hence, ϕ fixes S, and $S \subseteq Q^*$. Obviously, $Q^* \subseteq S$.

PROPOSITION 5.4. *Assume* (5.1). *Suppose that there exists* $x \in P$ *such that*

$$|Z(Q^*)/C_{Z(Q^*)}(x)| = p. \tag{5.3}$$

Then P/Q^* *is Abelian.*

Proof. Assume P/Q^* is not Abelian. Let $Z = Z(Q^*)$. Take x to satisfy (5.3). Then $x \in P - Q^*$. Let r be the maximum integer such that $\phi^{-r}(x)$ is defined. Then $\phi^{-r}(x)$ does not belong to Q; let $x' = \phi^{-r}(x)$. Then $P = \langle Q, x'\rangle$. By (5.1),

$$x' \textit{ does not centralize } Z(Q). \tag{5.4}$$

Define t, u, and $x_1, \ldots, x_t \in P/Q^*$ as in Lemma 2.4. Let y be an element of the coset x_{u+1}. Define $x'' = (x')^y = y^{-1}x'y$ and $z = (x')^{-1}x'' = [x', y]$. By Lemma 2.4, the coset zQ^* generates $\langle [x_1, x_{u+1}]\rangle$. Now, $\langle x', x''\rangle = \langle x', z\rangle$ and

$$|Z/C_Z(z)| \leqq |Z/C_Z(\langle x', x''\rangle)| \leqq |Z/C_Z(x')|\, |Z/C_Z(x'')| = p^2.$$

By Lemma 5.3, $|Z/C_Z(z)| > 1$. If $|Z/C_Z(z)| = p^2$, then

$$C_Z(\langle x', x''\rangle) = C_Z(z) \supseteq Z(Q),$$

contrary to (5.4). Hence, $|Z/C_Z(z)| = p$. Thus, we may assume that our original element x satisfies

$$xQ^* \in \langle [x_1, x_{u+1}]\rangle \subseteq Z(P/Q^*). \tag{5.5}$$

Take r as above, and let $w = \phi^{-r}(x)$. Therefore $w \in P - Q$. By (5.5), $xQ^* \in Z(P/Q^*)$. Let s be the maximum integer such that $\phi^s(x)Q^* \in Z(P/Q^*)$. Then $\phi^{s+1}(x) = \phi^{r+s+1}(w)$ and, by Lemma 2.4,

$$\phi^{s+1}(x)Q^* = x_{v+1}{}^{e(v+1)} \ldots x_{u+1}{}^{e(u+1)},$$

for some $e(v + 1), \ldots, e(u + 1) \in \mathbf{Z}_p$ such that $e(u + 1) \neq 0$. By (5.5) and Lemma 2.4,

$$1 \neq [w, \phi^{r+s+1}(w)]Q^* \in \langle [x_1, x_{u+1}]\rangle = \langle \phi^r(w)Q^*\rangle. \tag{5.6}$$

Let $w_i = \phi^{i+1}(w)$, for $i = 1, 2, \ldots, r + s + 1$. Since

$$|Z/C_Z(w)| = p,\ |Z/C_Z(w_i)| = p,$$

for each i. Let

$$W(i) = \langle w_1, \ldots, w_i\rangle, \text{ for } i = 1, 2, \ldots, r + s + 1.$$

Then $|Z/C_Z(W(i))| \leqq p^i$, for each i.

We claim that $|Z/C_Z(W(i))| = p^i$, for each i. This is true for $i = 1$. Suppose that $1 \leqq i \leqq r + s$ and that the equality is true for i. Let $W = W(i)$ and $W^* = W(i + 1)$. Since

$$p^i = |Z/C_Z(W)| \leqq |Z/C_Z(W^*)| \leqq p^{i+1},$$

we have the equality for $i + 1$, unless $|Z/C_Z(W^*)| = p^i$. Assume that the latter occurs. Then $C_Z(W^*) = C_Z(W)$. Since $W^* = \langle W, \phi(W)\rangle$ and

$$|C_Z(\phi(W))| = |C_Z(W)|,$$

we obtain

$$C_Z(W) = C_Z(W^*) = C_Z(\phi(W)) = \phi(C_Z(W)).$$

In particular, $Z(Q) \subseteq C_Z(\phi(W)) = C_Z(W) \subseteq C_Z(w)$, which contradicts (5.1) because $P = \langle Q, w\rangle$. This contradiction proves our claim.

In particular, $|Z/C_Z(W(r+s+1))| = p^{r+s+1}$. By (5.6),

$$W(r+s+1) = \langle w_1, \ldots, w_{r+s+1}\rangle \subseteq \langle w_1, \ldots, w_r; w_{r+2}, \ldots, w_{r+s+1}, Q^*\rangle.$$

Hence, $|Z/C_Z(W(r+s+1))| \leqq p^{r+s}$, which is a contradiction. This completes the proof of Proposition 5.4.

Lemmas 5.2 and 5.3 and Proposition 5.4 yield the main result of this section:

THEOREM 5.5. *Assume* (5.2). *Then P/Q^* is Abelian and* $Q^* = C_P(Z(Q^*))$.

This yields case (iv) of Theorem 3.2 and thus completes the proof of Theorem 3.2.

6. Proof of Theorem 3.3. In this section, we prove Theorem 3.3 and, therefore, obtain Theorem 2. We will use the following sets of conditions.

(6.1) (a) *p is a prime;*
(b) *P is a p-subgroup of a finite group G;*
(c) *Q is a subgroup of index p in P;*
(d) $Q \trianglelefteq G$;
(e) $\hat{Q} = \bigcap_{\alpha \in \mathrm{Aut} P} Q^\alpha$;
(f) *$\mathscr{H}$ is a subset of G that generates G; and*
(g) *for every $h \in \mathscr{H}$, P is conjugate to P^h in $\langle P, P^h\rangle$.*

(6.2) (a) (6.1) *holds;*
(b) $h \in \mathscr{H}$;
(c) $H = \langle P, P^h\rangle$;
(d) *$k \in H$ and $P^k = P^h$.*

Suppose that (6.2) is satisfied. We will use the following notation. For every automorphism α of P, let ϕ_α be the isomorphism of $Q^{\alpha^{-1}}$ onto Q given by $\phi_\alpha(x) = (x^\alpha)^k$, for all $x \in Q^{\alpha^{-1}}$.

LEMMA 6.1. *Assume* (6.2). *Let $\alpha \in$ Aut P. Then $N(\phi_\alpha) \trianglelefteq H$, and α fixes $N(\phi_\alpha)$.*

Proof. Let $Q^* = N(\phi)$ and $H = \langle P, P^h\rangle$. Define $\psi: P \to P^h$ by $\psi(x) = (x^\alpha)^k$, for all $x \in P$. Clearly, ψ extends ϕ. By Lemma 2.5, we obtain $Q^* \trianglelefteq H$. Thus,

$$(Q^*)^\alpha = (((Q^*)^\alpha)^k)^{k^{-1}} = (\phi(Q^*))^{k^{-1}} = (Q^*)^{k^{-1}} = Q^*,$$

and α fixes Q^*.

LEMMA 6.2. *Assume* (6.2). *Suppose that* $\alpha \in \operatorname{Aut} P$ *and that* $P/N(\phi_\alpha)$ *is Abelian. Then*

(a) $[Q, k] \subseteq N(\phi_\alpha) \trianglelefteq H$, *and*

(b) $\hat{Q} \subseteq N(\phi_\alpha) \subseteq Q^\alpha$.

Proof. Let $Q^* = N(\phi_\alpha)$. By Lemma 6.1, $Q^* \trianglelefteq H$. Let $C = C_H(Q/Q^*)$. Then $C \trianglelefteq H$ and $C \supseteq P$. Hence, $C \supseteq \langle P, P^k \rangle = H$, which proves (a).

To obtain (b), let $S = \bigcap Q^{\alpha^i}$, where i ranges over the integers. Then α fixes S. Since $Q^* \subseteq Q$ and α fixes Q^*, $Q^* \subseteq S \subseteq Q$. By (a), $S \trianglelefteq H$. Thus, $S = (S^\alpha)^h = \phi(S)$, and $S \subseteq N(\phi) = Q^*$. Therefore, $S = Q^*$, which proves (b).

Lemma 6.3. *Assume* (6.2). *Suppose that* $P/N(\phi_\alpha)$ *is Abelian for all* $\alpha \in \operatorname{Aut} P$. *Then*

(a) $\hat{Q} \trianglelefteq H$,

(b) $Q/\hat{Q} \subseteq Z(H/\hat{Q})$, *and*

(c) h *normalizes* $\hat{Q}$.

Proof. By Lemma 6.2(b), the intersection of all the groups $N(\phi_\alpha)$ is equal to $\hat{Q}$. Therefore, $\hat{Q} \trianglelefteq H$ and $[Q, k] \subseteq \hat{Q}$. Since $P/\hat{Q}$ is Abelian,

$$C_H(Q/\hat{Q}) \supseteq \langle P, k \rangle = H.$$

As $hk^{-1} \in N_G(P)$ and $\hat{Q}$ is a characteristic subgroup of P, hk^{-1} and h normalize $\hat{Q}$.

We may now easily prove Theorem 3.3. Assume that p is a prime, that P is a p-group, and that Q is a subgroup of index p in P. Assume that p, P, and Q violate conditions (i), (ii), and (iii) of Theorem 3.3. Suppose that $\mathscr{H}$ and G satisfy (1.2) and, therefore, satisfy (6.1). By condition (iv) of Theorem 3.2 and by Lemma 6.3, every element of $\mathscr{H}$ normalizes $\hat{Q}$. Since $\mathscr{H}$ generates G, $\hat{Q} \trianglelefteq G$. This completes the proof of Theorem 3.3.

The following results can sometimes be used to improve upon the restrictions on nilpotence class and exponent given in condition (ii) of Theorem 3.3.

LEMMA 6.4. *Assume* (6.2). *Let* $\alpha \in \operatorname{Aut} P$ *and let* $Q^* = N(\phi_\alpha)$. *Suppose that* P/Q^* *is not Abelian, that* $C_P(Q) \nsubseteq Q^*$, *and that* $[P, Z(Q)] \subseteq Q^*$. *Then*

(a) $H = PC_H(Z(Q))$, *and*

(b) $h, k \in N_G(P)C_G(Z(Q)) \subseteq N_G(Z(P))$.

Proof. By Lemma 6.1, $Q^* \trianglelefteq H$. Let $C = C_H(Q^*)$ and $Y = Z(Q) \cap Q^*$. Then $C \trianglelefteq H$. By Theorem 4.1, $P = (C \cap P)Q \subseteq CQ$. Since $CQ \trianglelefteq H$, and $H = \langle P, P^k \rangle$, it follows that $H = CQ$. Thus,

$$Y = Z(Q) \cap Q^* \subseteq Z(H) \cap Q^* \subseteq Z(P). \tag{6.3}$$

Since $Z(Q) \trianglelefteq H$, the hypothesis yields that $[P, Z(Q)] \subseteq Y$. Hence,

$$Z(Q)/Y \subseteq Z(H/Y). \tag{6.4}$$

Suppose that $Z(P) \not\subseteq Q$. Then $P = Z(P)Q$. So $P' = Q'$. Let $R = Q^{\alpha^{-1}}$ and $\phi = \phi_\alpha$. Since $|R'| = |\phi(R')| = |Q'|$, $R' = P'$. Hence, ϕ fixes P' and $P' \subseteq N(\phi) = Q^*$, contrary to the assumption that P/Q^* is not Abelian. Consequently, $Z(P) \subseteq Q$ and

$$Z(P) \subseteq Z(Q). \tag{6.5}$$

By (6.3), (6.4), and Lemma 2.6, $H/C_H(Z(Q))$ is an Abelian group. Since $H = \langle P, P^h \rangle$,

$$H = PH' = PC_H(Z(Q)).$$

This yields (a). Now (b) follows by (6.5) and the fact that $hk^{-1} \in N_G(P)$.

THEOREM 6.5. *Suppose that p is a prime, that P is a finite p-group, and that Q is a subgroup of index p in P. Then P satisfies at least one of the following conditions*:

(i) $\Omega_1(Z(P)) = \Omega_1(Z(Q))$;

(ii) (a) $p = 2$ *and* $P_3\mho^2(P) = Q_3\mho^2(Q)$, *or*

(b) $p = 3$ *and* $P_4\mho^2(P) = Q_4\mho^2(Q)$, *or*

(c) $p \geqq 5$ *and* $P_4\mho^1(P) = Q_4\mho^1(Q)$;

(iii) $J(P) = J(Q)$;

(iv) *whenever* G, $\mathscr{H}$, *and* $\hat{Q}$ *satisfy* (6.1), *then* $G = C_G(Z(Q))N_G(\hat{Q})$, *and every element of* $\mathscr{H}$ *normalizes* $Z(P)$ *or* $\hat{Q}$.

Proof. Assume that (i), (ii), and (iii) are false. Assume (6.1). Let

$$G^* = C_G(Z(Q))N_G(\hat{Q}).$$

Take $h \in \mathscr{H}$. If h normalizes $\hat{Q}$, then $h \in G^*$. Suppose that h does not normalize $\hat{Q}$. Take k and H as in (6.2). By Lemma 6.3, there exists $\alpha \in \operatorname{Aut} P$ such that $P/N(\phi_\alpha)$ is not Abelian. Let $Q^* = N(\phi_\alpha)$. By Theorem 3.2, $C_P(Q) \not\subseteq Q^*$. Since (ii) is false, Theorem 4.3 yields that $[P, Z(Q)] \subseteq Q^*$. By Lemma 6.4, $h \in N_G(P)C_G(Z(Q)) \subseteq G^*$, and h normalizes $Z(P)$. Since h is an arbitrary element of $\mathscr{H}$ and $G = \langle \mathscr{H} \rangle$, we obtain (iv).

Remark 6.6. Assume that (6.1) is satisfied. Suppose that $Z(P) \subseteq Q$, that $\Omega_1(Z(P))$ is not normal in G, and that $J(P) \neq J(Q)$. Let $Z = \Omega_1(Z(Q))$. A slight extension of a result mentioned in the introduction shows that $\mathrm{SL}(2, p)$ is involved in G. Actually, a stronger result is true.

Lemma 5.1 shows that some element x of P acts as a *transvection* on Z; i.e., that $|Z/C_Z(x)| = p$ and $[Z, x] \subseteq C_Z(x)$. Let N be the normal subgroup of G generated by all the conjugates of P in G. Let L be the largest normal p-subgroup of $N/C_N(Z)$ and let $M = (N/C_N(Z))/L$. By two theorems of McLaughlin [**5**; **6**], M is a direct product of classical linear groups over $\mathbf{Z}_p$, if p is odd, and is a direct product of known groups, if $p = 2$. Note that $M \cong H/K$ for some $H, K \trianglelefteq G$ such that $K \subset H$.

7. Proof of Theorem 3.4. We may now derive Theorem 3.4. Suppose that p, P, Q, and $\hat{Q}$ satisfy the hypothesis of Theorem 3.4 and violate conditions (i), (ii), (iii) of Theorem 3.4. Let G be a group that satisfies (3.2). By Lemma 2.7, P is conjugate to P^h in $\langle P, P^h \rangle$, for every $h \in G$. Thus, G satisfies (6.1) with $\mathscr{H} = G$.

Assume that $\hat{Q}$ is not normal in G. Let $h \in G - N_G(\hat{Q})$. Take k and H as in (6.2). By Lemma 6.3, there exists $\alpha \in \operatorname{Aut} P$ such that $P/N(\phi_\alpha)$ is not Abelian. Let $Q^* = N(\phi_\alpha)$. By Theorem 3.2, $C_P(Q) \not\subseteq Q^*$ and $\Omega_1(Z(P)) \neq \Omega_1(Z(Q))$. By Lemma 2.7, P/Q^* is weakly closed in some Sylow p-subgroup of H/Q^* with respect to H/Q^*. Therefore, by Theorem 7.11 of I, $c \leqq 2$, if $p \neq 3$. Since condition (ii) of Theorem 3.4 is false, Theorem 4.2 yields that $[P, Z(P)] \subseteq Q^*$. By Lemma 6.4, h normalizes $Z(P)$.

Thus, $N_G(Z(P))$ contains $G - N_G(\hat{Q})$. Take $h \in G - N_G(\hat{Q})$. For every $g \in N_G(\hat{Q})$, gh belongs to $G - N_G(Q)$, and, therefore, gh and g normalize $Z(P)$. Hence, $N_G(Z(P)) = G$. This completes the proof of Theorem 3.4.

Remark 7.1. Assume the situation of Remark 6.6, and suppose further that P is weakly closed in some Sylow p-subgroup of G. By McLaughlin's work and some additional arguments, there exist W, $Y \trianglelefteq G$ such that W is an elementary Abelian group of order p^2, $Y \subseteq Z(N)$, $Z = W \times Y$, and

$$N/C_N(W) \cong \mathrm{SL}(2, p).$$

REFERENCES

1. G. Glauberman, *Weakly closed elements of Sylow subgroups*, Math. Z. *107* (1968), 1–20.
2. ——— *Isomorphic subgroups of finite p-groups*. I, Can J. Math *23* (1971), 983–1020.
3. D. Gorenstein, *Finite groups* (Harper and Row, New York, 1968).
4. B. Huppert, *Endliche Gruppen*. I (Springer-Verlag, Berlin, 1967).
5. J. McLaughlin, *Some groups generated by transvections*, Archiv. der Math. *18* (1967), 364–368.
6. ——— *Some subgroups of $SL_n(F_2)$*, Illinois J. Math. *13* (1969), 108–115.

Department of Mathematics,
The University of Chicago,
Chicago, Illinois