Can. J. Math., Vol. XXIV, No. 1, 1972, pp. 17–28

CONJUGATE p-SUBGROUPS OF FINITE GROUPS

JOHN J. CURRANO

1. Introduction. Throughout this paper, let p be a prime, P be a p-group of order p^t, and φ be an isomorphism of a subgroup R of P of index p onto a subgroup Q which fixes no non-identity subgroup of P, setwise. In [**2**, Lemma 2.2], Glauberman shows that P can be embedded in a finite group G such that φ is effected by conjugation by some element g of G. We assume that P is thus embedded. Then $Q = P \cap P^g$. Let $H = \langle P, P^g\rangle$ and $V = [H, Z(Q)]$, so $Q \lhd H$ and $V \lhd H$.

Let $E(p)$ be the non-abelian group of order p^3 which is generated by two elements of order p. Then $E(p)$ is dihedral if $p = 2$ and has exponent p if p is odd. If p is odd, then $E^*(p)$ is defined in § 2 to be a particular group of order p^6 and nilpotence class three. Our main results are:

THEOREM 1. *Let G be a finite group, $g \in G$, and P be a p-subgroup of G of order p^t. Let $Q = P \cap P^g$, $H = \langle P, P^g\rangle$, and $V = [H, Z(Q)]$. Assume:*

(1.1) *P is non-abelian, $|P:Q| = p$, and g normalizes no non-identity subgroup of P;*

$$H = PO^p(H)C_H(Q/V) = P^gO^p(H)C_H(Q/V); \text{ and} \tag{1.2}$$

$$V \not\subseteq Z(H). \tag{1.3}$$

Also assume that the nilpotence class of P is two and that $|P'| = p^\nu$. Then $t \geqq 3\nu$ and P is the direct product of an elementary abelian subgroup of order $p^{t-3\nu}$ with the direct product of ν subgroups isomorphic to $E(p)$.

THEOREM 2. *Let G be a finite group, $g \in G$, and P be a p-subgroup of G of order p^t. Let $Q = P \cap P^g$ and $H = \langle P, P^g\rangle$. Assume* (1.1), *and*

$$H = P^gO^p(H)C_H(Q), \text{ and} \tag{1.4}$$

$$H = PO^p(H)C_H(Q). \tag{1.5}$$

Let $|P/Z(P)| = p^x$. Then x is even. Let $\nu = x/2$. Then:

(a) *If P has nilpotence class two, then $|P'| = p^\nu$, $t \geqq 3\nu$, and P is the direct product of an elementary abelian subgroup of order $p^{t-3\nu}$ with the direct product of ν subgroups isomorphic to $E(p)$.*

(*b*) *If P has nilpotence class three, then P is odd, $|P_3| = p^\nu$, ν is even, $t \geqq 3\nu$, and P is the direct product of an elementary abelian subgroup of order $p^{t-3\nu}$ with the direct product of $\nu/2$ subgroups isomorphic to $E^*(p)$.*

Received April 15, 1971, and in revised form, September 29, 1971.

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press

These theorems are related to the following type of question. Let S be a non-abelian Sylow p-subgroup of a finite group G, and let α be an automorphism of S. We may ask whether α fixes any non-identity normal subgroup of G contained in S. If not, and if there is an element h in G with $G = \langle S, S^h \rangle$ and $|S:S \cap S^h| = p$, we can determine the structure of S. To see this, let $\varphi:S \rightarrow S^h$ be given by $\varphi(x) = (x^\alpha)^h$. Then (1.1), (1.4), and (1.5) can be verified, so S has nilpotence class at most three (by Lemma 2.2) and has the structure indicated in Theorem 2.

Our results generalize part of [**2**, Theorem 2]. There, Glauberman assumes that P and P^g are conjugate in H and obtains the decompositions we obtain in Theorem 2. In [**2**, § 5], he shows that this assumption implies (1.4) and (1.5). He also shows that under hypothesis (1.1), P has nilpotence class two or three. Thus, Theorems 1 and 2 completely characterize P under the given conditions.

(1.1) alone is not sufficient to obtain the decompositions of Theorems 1 and 2, as we have shown in [**1**, Theorems 1 and 2]. Thus, we must make some additional assumptions about P. It appears that (1.2), (1.4), and (1.5) depend on the group G in which P is embedded, but in [**2**, § 4], Glauberman shows that (1.4) depends only on P and φ and not on G. (His proof also works for (1.2) and (1.5).) Thus, (1.2), (1.4), and (1.5) are really statements about the structure of P. Furthermore, they are natural ones to consider. Recall that $O^p(H)$ is the smallest normal subgroup K of H with H/K a p-group. (1.5) says that modulo $C_H(Q)$, H has no proper normal subgroup which contains P. We factor out $C_H(Q)$ for two reasons: (1) we shall look at the action of H on chains of subgroups of Q, and $C_H(Q)$ contributes nothing to this analysis; and (2) $C_P(Q) = Z(Q)$ (cf. Lemma 2.4(b)), and the rest of $C_H(Q)$ does not affect the structure of P. Similar remarks can be made about (1.4) and (1.2). Finally, it can be shown that neither (1.1) and (1.4) nor (1.1) and (1.5) suffice to prove Theorem 2. (Using [**1**, Theorem 2], a group can be constructed which satisfies (1.1) and (1.4), but violates (2.3).)

All groups considered in this paper are finite. We write $H \subseteq G$ if H is a subgroup of G; $H \subset G$ if $H \subseteq G$ and $H \neq G$; and $H \lhd G$ if H is a normal subgroup of G. Let G_i be the i-th member of the lower central series of G, defined inductively by $G_1 = G$ and $G_{i+1} = [G_i, G]$. For p a prime, let $O^p(G)$ be the subgroup of G generated by all the p'-elements of G and let GF(p) be the field of the integers modulo p. Finally, let $Z_2(G)$ be the inverse image in G of $Z(G/Z(G))$.

Acknowledgement. This work constitutes a portion of the author's doctoral dissertation. The author is indebted to his advisor, Professor George Glauberman, for his encouragement and many suggestions.

2. Preliminary results. We now state some facts which we shall need in the proofs of Theorems 1 and 2. We shall also fix some notation for the remainder of the paper.

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press

LEMMA 2.1 (Sims; [**1**, Lemma 2.1]). *If P satisfies* (1.1), *then:*

(2.1) *There are elements $x_1, \ldots, x_t$ in P which satisfy:*
(a) $|\langle x_1, \ldots, x_i\rangle| = p^i$ *for* $1 \leqq i \leqq t$; *and*
(b) $x_i^g = x_{i+1}$ *for* $1 \leqq i \leqq t-1$.

LEMMA 2.2 (Glauberman [**2**, Theorem 1]). *Assume that P satisfies* (1.1). *Then the nilpotence class of P is at most three if p is odd and at most two if* $p = 2$.

Throughout the paper, we assume that P satisfies (1.1). Choose $x_1, \ldots, x_t$ as in Lemma 2.1. Define $x_{t+1} = x_t^g$, so $P^g = \langle x_2, \ldots, x_{t+1}\rangle$.

Let u be a positive integer minimal subject to $[x_j, x_{u+j}] \neq 1$ for some j. (u exists by (1.1) and (2.1).) Let $v = t - u$.

If $P_3 \neq 1$, let k be a positive integer minimal subject to $[x_j, x_{k+j}] \notin Z(P)$ for some j. If $P_3 = 1$, let $k = t$. Let $r = t - k$.

Define $z_i = [x_i, x_{u+i}]$ for $1 \leqq i \leqq v+1$, and let $Z = \langle z_1, \ldots, z_v\rangle$. If $P_3 \neq 1$, define $w_i = [x_i, x_{k+i}]$ for $1 \leqq i \leqq r+1$.

The following *symmetry principle* will be useful:

LEMMA 2.3 (Glauberman [**2**, Lemma 3.3]). *Let n be a nonzero element of* GF(p). *Conditions* (1.1) *and* (2.1) *and the definitions of u, v, and k remain valid if we replace:*

(a) *P by P, Q by R, R by Q, g by g^{-1} (and thus φ by φ^{-1}), and x_i by $(x_{t+1-i})^n$ for $i = 1, \ldots, t$; or*

(b) *P by P^g, Q by Q, R by Q^g, g by g^{-1} (and thus φ by φ^{-1}), and x_i by $(x_{t+2-i})^n$ for $i = 1, \ldots, t$.*

LEMMA 2.4 (Glauberman-Sims; [**1**, Theorem 1 and Lemma 2.2]).

(a) $2t/3 \leqq u < u + v/2 \leqq k \leqq t$.

(b) $[x_i, x_{u+i}] \neq 1$ *for* $1 \leqq i \leqq v+1$.

(c) *If* $P_3 \neq 1$, *then* $[x_i, x_{k+i}] \notin Z(P)$ *for* $1 \leqq i \leqq r$.

(d) $Z(P) = \langle x_{v+1}, \ldots, x_u\rangle$, $Z(Q) = \langle x_{v+1}, \ldots, x_{u+1}\rangle$, *and* $P \cap Z(H) = P^g \cap Z(H) = \langle x_{v+2}, \ldots, x_u\rangle$. *Furthermore, these are elementary abelian groups.*

(e) $Z \subseteq Z(P)$.

We shall have use for the following three well-known lemmas:

LEMMA 2.5 [**3**, p. 179]. *Let S be a p-group and $T \subseteq$* Aut S. *Assume that T stabilizes some chain*

$$S = S_0 \supseteq S_1 \supseteq \ldots \supseteq S_n = 1$$

of normal subgroups of S; that is, T fixes each S_i and each coset of S_{i+1} in S_i. Then T is a p-group.

LEMMA 2.6 (P. Hall; [**3**, p. 19]). *Let G be any finite group.*

(a) $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$ *for all* $x, y, z \in G$.

(b) *If* class $G \leqq 3$, $[x, y, z][y, z, x][z, x, y] = 1$ *for all* $x, y, z \in G$.

(c) *Let A, B, and C be any subgroups of G. If* $[A, B, C] = [B, C, A] = 1$, *then* $[C, A, B] = 1$.

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press

LEMMA 2.7 (von Dyck; [**4**, § 18]). *If a group G is given by a system of defining relations, and if a group H is given by these relations and some further relations in the same symbols, then H is isomorphic to a factor group of G.*

LEMMA 2.8 (Glauberman [**2**, Propositions 4.5, 4.7, and 4.15]).
(a) $V = \langle z_1, z_{v+1}\rangle$.
(b) *If P satisfies* (1.4), *then for* $1 \leqq i \leqq v + 1$,

$$z_i = x_i^{c(v+1)} \ldots x_{u-v+i}^{c(u-v+1)}, \tag{2.2}$$

where $c(v + 1) \neq 0$ *and* $c(u - v + 1) \neq 0$. *In particular,* $V \cap Z(H) = 1$, $V \not\subseteq Z(P)$, *and* $V \not\subseteq Z(P^g)$.
(c) *If* $P_3 \neq 1$ *and P satisfies* (1.4) *and* (1.5), *then* $v = 2r$ *and for* $1 \leqq i \leqq r + 1$,

$$w_i = x_{r+i}^{d(r+1)} \ldots x_{u+i}^{d(u+1)}, \tag{2.3}$$

where $d(r + 1) \neq 0$ *and* $d(u + 1) \neq 0$.

LEMMA 2.9. $V \not\subseteq Z(H)$ *if and only if*

$$z_1 = x_{v+1}^{c(v+1)} \ldots x_{u-v+1}^{c(u-v+1)}, \tag{2.4}$$

where $c(v + 1) \neq 0$ *or* $c(u - v + 1) \neq 0$.

Proof. By Lemma 2.4, $Z \subseteq Z(P) = \langle x_{v+1}, \ldots, x_u\rangle$. Using this, the fact that $z_v = \varphi^{v-1}(z_1)$, and (2.1), we obtain

$$z_1 = x_{v+1}^{c(v+1)} \ldots x_{u-v+1}^{c(u-v+1)}.$$

Then

$$z_{v+1} = \varphi^v(z_1) = x_{2v+1}^{c(v+1)} \ldots x_{u+1}^{c(u-v+1)}.$$

By Lemma 2.4, $P \cap Z(H) = \langle x_{v+2}, \ldots, x_u\rangle$, so $V = \langle z_1, z_{v+1}\rangle \subseteq Z(H)$ if and only if $c(v + 1) = c(u - v + 1) = 0$.

LEMMA 2.10. *Assume that* $P_3 = 1$.
(a) *If P satisfies* (1.4), *then* $H = P^g C_H(Q/V)$.
(b) *If P satisfies* (1.5), *then* $H = PC_H(Q/V)$.

Proof. (b) follows from (a) by symmetry. So assume that P satisfies (1.4). Let $N = C_H(Q/V)$. Then $N \lhd H$, since Q and V are normal subgroups of H. Since $[P, Q] \subseteq P' \subseteq Z(P) \subseteq Z(Q)$, H/N stabilizes the chain

$$Q/V \supseteq Z(Q)/V \supseteq 1,$$

so H/N is a p-group by Lemma 2.5. Therefore, $N \supseteq O^p(H)$. But clearly $C_H(Q) \subseteq N$, and the result follows from (1.4).

The following lemma is a generalization of part of [**2**, Proposition 4.13]. The proof is essentially the same as in [**2**].

LEMMA 2.11. *Assume that P satisfies* (1.2) *and* (1.3). *Then*
(a) $[P, x_{u+i}] \subseteq \langle z_1, \ldots, z_i\rangle$ *for* $1 \leqq i \leqq k - u$.
(b) *If* $P_3 = 1$, *then* $P' = Z$.

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press

Proof. By symmetry, we may assume that $z_{v+1} \notin Z(H)$, so $c(u - v + 1) \neq 0$ and $z_{v+1} \notin Z(P)$, by (2.4). Assume that $1 \leqq i \leqq k - u$, and that (a) is true for all j with $1 \leqq j < i$. Let $M = \langle z_1, \ldots, z_i, z_{v+1}\rangle$ and $N = \langle x_{v+1}, \ldots, x_{u+i}\rangle$. Then $M = V(M \cap Z(H))$ by Lemma 2.3 and (2.4), so $M \lhd H$.

Using the definition of k, we see that $Z_2(P) = \langle x_{r+1}, \ldots, x_k\rangle$ and $Z_2(P^g) = \langle x_{r+2}, \ldots, x_{k+1}\rangle$. Then

$$Z(P) \subseteq N \subseteq Z_2(P) \cap Z_2(P^g),$$

so $N \lhd H$.

Let $L = C_H(N/M)$, so $L \lhd H$. Since $V \subseteq M$, $C_H(Q/V) \subseteq L$. Also, $x_{v+1} \in Z(Q)$ and

$$\begin{aligned}(2.5) \qquad [P^g, \langle x_{v+2}, \ldots, x_{u+i}\rangle] &\subseteq \varphi[P, \langle x_{v+1}, \ldots, x_{u+i-1}\rangle] \\ &\subseteq \varphi\langle z_1, \ldots, z_{i-1}\rangle = \langle z_2, \ldots, z_i\rangle \subseteq M,\end{aligned}$$

by induction if $i > 1$ and by Lemma 2.4(d) if $i = 1$, so $Q \subseteq L$. Finally, $[x_{t+1}, x_{v+1}] = z_{v+1}{}^{-1}$, and, together with (2.5), this implies that $x_{t+1} \in L$. Therefore,

$$P^g C_H(Q/V) \subseteq L \lhd H = \langle P, P^g\rangle,$$

so H/L is a p-group. But then $O^p(H) \subseteq L$, so $H = P^g O^p(H) C_H(Q/V) \subseteq L$ and $L = H$. Thus, $P \subseteq L = C_H(N/M)$, so $[P, x_{u+i}] \subseteq [P, N] \subseteq M \cap Z(P) = \langle z_1, \ldots, z_i\rangle$.

LEMMA 2.12 (Glauberman [**2**, Theorem 3.7 and Proposition 4.15]). *Assume that $P_3 \neq 1$ and that P satisfies* (1.4) *and* (1.5). *Then $P_3 = Z$ and*

$$P' \subseteq \langle x_{r+1}, \ldots, x_k\rangle.$$

We now define the group $E^*(p)$ discussed in Theorem 2.

LEMMA 2.13 (Glauberman [**2**, Lemma 5.7]). *Assume that p is an odd prime. Then there exists a group S of order p^6 generated by elements a, b, c, d, e, f subject to the following restrictions:*

$$(2.6) \qquad a^p = b^p = c^p = d^p = e^p = f^p = 1;$$

$$(2.7) \qquad ab = ba, ac = ca, bc = cb;$$

$$(2.8) \qquad ad = da, bd = db, d^{-1}cd = cb;$$

$$(2.9) \qquad ae = ea, be = eb, ce = ec, e^{-1}de = db;$$

$$(2.10) \qquad af = fa, bf = fb, f^{-1}cf = ca, f^{-1}df = dc^{-1}, ef = fe.$$

Moreover, S is unique up to isomorphism and satisfies

$$(2.11) \qquad Z(S) = S_3 = \langle a, b\rangle.$$

Proof. To construct S, let D be the direct product of $E(p)$ and a group of order p. Then there exists a set $\{a, b, c, d\}$ of generators of D that satisfies

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press

(2.6) and (2.7). Also, there exist $e, f \in \operatorname{Aut} D$ for which

$$a^e = a^f = a,\ b^e = b^f = b,\ c^e = c,\ c^f = ca,\ d^e = db,\ d^f = dc^{-1}.$$

Note that $ef = fe$.

Since p is odd, D has exponent p, and e and f have order p. Let S be the semi-direct product of D by $\langle e, f\rangle$. Then we immediately obtain (2.6) – (2.10), and easy computations yield (2.11).

Now suppose that S^* is an arbitrary group generated by elements satisfying (2.6)–(2.10). Let $D^* = \langle a, b, c, d\rangle$. Then $D^* \lhd S^*$ and $S^* = \langle D^*, e, f\rangle$. Hence, $|D^*| \leqq p^4$ and $|S^*/D^*| \leqq p^2$. Assume that $|S^*| = p^6$. Then $D^* \cong D$ and $D^* \cap \langle e, f\rangle = 1$. Therefore, S^* is a semi-direct product of D^* by $\langle e, f\rangle$, and $S^* \cong S$.

Definition. If p is an odd prime, let $E^*(p)$ be the group S defined in Lemma 2.13.

3. The class two case. In this section, we prove Theorems 1 and 2(a).

Assume the hypothesis of Theorem 1. By Lemma 2.9, (2.4) holds, so by Lemma 2.11, $P' = Z = \langle z_1, \ldots, z_v\rangle$. Thus, $\nu = v$, so $t \geqq 3\nu$ by Lemma 2.4.

By (1.2) and (2.1), there are elements $a \in \langle x_2, \ldots, x_v\rangle$ and

$$b \in \langle x_{v+1}, \ldots, x_{t+1}\rangle$$

such that $x_1^{-1} \equiv ab$ (modulo $C_1 = C_H(Q/V)$). But $\langle x_{v+1}, \ldots, x_{t+1}\rangle$ is abelian modulo V, by (2.1) and the definitions of u and z_i, so, if $y \in \langle x_{v+2}, \ldots, x_t\rangle$,

$$1 \equiv [y, x_1ab] \equiv [y, x_1a][y, b]^{x_1a} \equiv [y, x_1a] \quad (\text{modulo V}).$$

Thus, $[x_1a, \langle x_{v+2}, \ldots, x_t\rangle] \subseteq V$. But $x_1a \in \langle x_1, \ldots, x_{v+1}\rangle$, which is abelian, so $[x_1a, Q] \subseteq V$. Thus, $x_1 \equiv a^{-1} \in Q$ (modulo C_1), so $x_1 \in QC_1$ and

$$H = PC_1 = QC_1. \tag{3.1}$$

Then, $P = Q(P \cap C_1) \supset Q$, so we may choose $x \in C_P(Q/V)$, $x \notin Q$.

Let $x = sy$ where $s = x_1^{a(1)} \ldots x_v^{a(v)}$ and $y \in \langle x_{v+1}, \ldots, x_t\rangle$. By (2.1) and Lemma 2.4 (a), $s^p = 1$ and

$$[s, Q] \subseteq [s, \langle x_{u+1}, \ldots, x_t\rangle] \subseteq [sy, \langle x_{u+1}, \ldots, x_t\rangle] \subseteq V \cap P' = \langle z_1\rangle. \tag{3.2}$$

(Note that $z_{v+1} \notin P' = Z$, by (1.1), since $\varphi(Z) = \langle z_2, \ldots, z_{v+1}\rangle$.) Also, since $x \notin Q$, $s \notin Q$ and therefore $a(1) \neq 0$.

By symmetry, there is $\tau = x_{u+2}^{b(1)} \ldots x_{t+1}^{b(v)}$ with $b(v) \neq 0$, $\tau^p = 1$, and $[\tau, Q] \subseteq \langle z_{v+1}\rangle$.

Define $s_i = \varphi^{i-1}(s)$, $t_i = \varphi^{i-(v+1)}(\tau)$, and $S_i = \langle s_i, t_i\rangle$ for $1 \leqq i \leqq v$. We first show that $S_i \cong E(p)$ and $[S_i, S_j] = 1$ if $1 \leqq i \neq j \leqq v$.

So let $1 \leqq i \neq j \leqq v$. Then

$$\begin{aligned}[s_i, t_j] &\in \varphi^{i-1}[s, \varphi^{1-i}(t_j)] \cap \varphi^{j-v-1}[\varphi^{v+1-j}(s_i), \tau] \\ &= \varphi^{i-1}\langle z_1\rangle \cap \varphi^{j-v-1}\langle z_{v+1}\rangle = \langle z_i\rangle \cap \langle z_j\rangle = 1.\end{aligned}$$

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press

Also,

$$\langle s_1, \ldots, s_v \rangle \subseteq \langle x_1, \ldots, x_{2v} \rangle \subseteq \langle x_1, \ldots, x_u \rangle,$$

which is elementary abelian. Thus, $[s_i, s_j] = 1$. By symmetry, $[t_i, t_j] = 1$. Therefore,

$$(3.3) \qquad [s_i, s_j] = 1 \quad \text{for } 1 \leqq i \neq j \leqq v.$$

From the definition of s_i, t_i, and u, we obtain

$$[s_i, t_i] = [x_1^{a(1)} \ldots x_v^{a(v)}, x_{u+2-i}^{b(1)} \ldots x_{u+i}^{b(v)}] = z_i^c,$$

where $c = a(1)\, b(v) \neq 0$. But $z_i \in Z(P) \cap S_i$, so $|S_i/\langle z_i\rangle| = p^2$ and $|S_i| = p^3$. Since $s_i^p = t_i^p = 1$ and S_i is non-abelian, $S_i \cong E(p)$.

Let Y be a complement to Z in $Z(P)$. Then $|Y| = p^{u-v}/p^v = p^{t-3v}$. So in light of (3.3), it suffices to show that $P = S_1 \ldots S_v Y$ and that

$$|P| = |S_1| \ldots |S_v||Y|$$

in order to complete the proof of Theorem 1. But

$$\begin{aligned} P &= \langle x_1, \ldots, x_t \rangle \\ &= Z(P)\langle x_1, \ldots, x_v, x_{u+1}, \ldots, x_t \rangle \\ &= Z(P)\langle s_1, \ldots, s_v, t_1, \ldots, t_v \rangle \\ &= YZS_1 \ldots S_v \\ &= YS_1 \ldots S_v \end{aligned}$$

and

$$p^t = |P| = |S_1 \ldots S_v Y| \leqq |S_1| \ldots |S_v||Y| = p^{3v} p^{t-3v} = p^t,$$

so equality holds everywhere. This completes the proof of Theorem 1.

Now assume the hypothesis of Theorem 2(a). By Lemma 2.4, $|P/Z(P)| = p^{2v}$ and, by the first paragraph of the proof of Theorem 1, $|P'| = p^v$. Now Theorem 2(a) follows from Theorem 1 and Lemmas 2.4, 2.8, and 2.10.

4. The class three case. We now prove Theorem 2(b). By Lemma 2.2, p is odd. By Lemmas 2.8 and 2.12, $P_3 = Z$, $|P_3| = p^v$, and $v = 2r$. Then Lemma 2.4 implies that $|P/Z(P)| = p^{2v}$, so $\nu = v$ and $t \geqq 3\nu$.

Recall that $V = [H, Z(Q)] = \langle z_1, z_{v+1} \rangle$. Using the definition of k, we see that

$$\begin{aligned} Z_2(P) &= \langle x_{r+1}, \ldots, x_k \rangle, \\ Z_2(P^g) &= \langle x_{r+2}, \ldots, x_{k+1} \rangle, \text{and} \\ Z_2(Q) &= \langle x_{r+1}, \ldots, x_{k+1} \rangle. \end{aligned}$$

Let

$$\begin{aligned} V_0 &= V\langle z_{r+1} \rangle = \langle z_1, z_{r+1}, z_{v+1} \rangle, \\ V_1 &= Z_2(P) \cap Z_2(P^g) = \langle x_{r+2}, \ldots, x_k \rangle, \text{ and} \\ M_1 &= [H, Z_2(Q)] = Z(Q)\langle w_1, w_{r+1} \rangle, \end{aligned}$$

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press

where for $1 \leqq i \leqq r + 1$, $w_i = [x_i, x_{k+i}]$. We complete the proof in a series of lemmas.

LEMMA 4.1. *There are elements* $a(1), \ldots, a(v)$ *and* $b(1), \ldots, b(v)$ *in* $\mathrm{GF}(p)$ *such that* $a(1) = b(v) = 1$ *and such that, if* $s = x_1^{a(1)} \ldots x_v^{a(v)}$ *and* $t = x_{u+2}^{b(1)} \ldots x_{t+1}^{b(v)}$, *then*

$$[V_1, s] \subseteq \langle z_1 \rangle, \tag{4.1}$$

$$[Q, s] \subseteq Z(Q)\langle w_1 \rangle, \tag{4.2}$$

$$[Q, t] \subseteq Z(Q)\langle w_{r+1} \rangle, \text{ and} \tag{4.3}$$

$$[V_1, t] \subseteq \langle z_{v+1} \rangle. \tag{4.4}$$

Proof. One easily verifies that H stabilizes the chains

$$V_1 \supseteq Z(Q) \supseteq V$$

and

$$Q \supseteq Z_2(Q) \supseteq M_1.$$

Let $C_2 = C_H(V_1/V) \cap C_H(Q/M_1)$. By Lemma 2.5, $H/C_H(V_1/V)$ and $H/C_H(Q/M_1)$ are p-groups, so $O^p(H) \subseteq C_H(V_1/V) \cap C_H(Q/M_1) = C_2$. Also $C_H(Q) \subseteq C_2$, so $H = PC_2 = P^g C_2$ by (1.4) and (1.5). Then $H = QC_2$ as in the proof of (3.1), so $P = Q(P \cap C_2) \supset Q$ and there is $x \in P \cap C_2$, $x \notin Q$. Let $x = sy$ with $s = x_1^{a(1)} \ldots x_v^{a(v)}$ and $y \in \langle x_{v+1}, \ldots, x_t \rangle$. Since $x \notin Q$, $s \notin Q$, so $a(1) \neq 0$.

Recalling that $V_1 \subseteq Z_2(P)$, we obtain

$$[V_1, s] \subseteq V \cap Z(P),$$

as in the proof of (3.2). But $z_{v+1} \notin Z(P)$ by Lemma 2.8, so (4.1) holds. In a similar manner we obtain

$$[Q, s] \subseteq M_1 \cap P'.$$

However, $P' \cap (w_{r+1}\langle Z(Q), w_1 \rangle) = \emptyset$ since $P' \subseteq \langle x_{r+1}, \ldots, x_k \rangle$ by Lemma 2.12, and $w_{r+1} = x_{2r+1}^{d(r+1)} \ldots x_{k+1}^{d(u+1)}$, where $d(u + 1) \neq 0$, by Lemma 2.8. Thus, (4.2) holds. By taking an appropriate power of s, we may assume that $a(1) = 1$. Now the rest of the lemma follows by symmetry.

Definitions. Let $y_1 = [s, \varphi^{-r}(t)]$, $y_2 = [\varphi^r(s), t]$, and $M = \langle z_1, z_{r+1}, z_{v+1}, y_1, y_2 \rangle$. Let Y be a complement to $Z \cap Z(H)$ in $P \cap Z(H)$.

Remark. $|Y| = p^{t-3v}$ and $Z(P) = YZ$ by Lemmas 2.4 and 2.8.

LEMMA 4.2. *M is a normal subgroup of H.*

Proof. $Y \subseteq Z(H)$, so Y centralizes M. Let $s_i = \varphi^{i-1}(s)$ for $1 \leqq i \leqq v$ and $t_j = \varphi^{j-(v+1)}(t)$ for $1 \leqq j \leqq v + 1$. Then $[s_i, t_i] = z_i$ for $1 \leqq i \leqq v$, so

$$P = Y\langle s_i, t_i | 1 \leqq i \leqq v \rangle. \tag{4.5}$$

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press

Also, a straightforward argument using the definition of k shows that

$$(4.6) \qquad y_1 = [s_1, t_{r+1}] = [x_1^{a(1)}, x_{k+1}^{b(v)}]z = w_1 z,$$

where $z \in Z(P)$.

Let $N_1 = \langle z_1, z_{r+1}, y_1\rangle$ and $N_2 = \langle z_{r+1}, z_{v+1}, y_2\rangle$. Assume that $1 \leqq i \leqq v$. Then, since s_i and $y_1 = w_1 z$ lie in $\langle x_1, \ldots, x_{u+1}\rangle$, we obtain

$$(4.7) \qquad [y_1, s_i] \in \langle z_1\rangle.$$

By the definition of u, $[t_{r+1}, t_i] = 1$. Also, $[t_i, s_1] = w_1^{\alpha} z'$ for $\alpha \in \mathrm{GF}(p)$ and $z' \in Z(Q)$ by (4.2). Therefore, using Lemma 2.6 and the definitions, we obtain

$$\begin{aligned} 1 &= [s_1, t_{r+1}, t_i][t_{r+1}, t_i, s_1][t_i, s_1, t_{r+1}] \\ &= [y_1, t_i][w_1^{\alpha} z', t_{r+1}] \\ &= [y_1, t_i][w_1^{\alpha}, t_{r+1}], \end{aligned}$$

so $[t_i, y_1] = [x_{r+1}^{\alpha d(r+1)}, x_{k+1}^{b(v)}] \in \langle z_{r+1}\rangle \subseteq N_1$. Together with (4.7) and (4.5), this shows that $[y_1, P] \subseteq N_1$. But $\langle z_1, z_{r+1}\rangle \subseteq Z(P)$, so $N_1 \lhd P$. By symmetry, $N_2 \lhd P^g$.

Now $M = N_1 N_2$ and $V_0 = \langle z_1, z_{r+1}, z_{v+1}\rangle \lhd H$. Therefore, to show that $M \lhd H$, it suffices to show that $[y_1, t_{v+1}] \in M$ and $[y_2, s_1] \in M$. By symmetry, it suffices to show the former. Now, (4.4) and (4.6) imply, modulo $V = [H, Z(Q)]$, that

$$[y_1, t_{v+1}] \equiv [w_1 z, t_{v+1}] \equiv [x_{r+1}^{d(r+1)}, t_{v+1}] \equiv [s_{r+1}^{d(r+1)}, t_{v+1}].$$

But, modulo $V_0 \supseteq V$, $\langle x_{r+1}, \ldots, x_{t+1}\rangle$ has class at most two, so

$$[y_1, t_{v+1}] \equiv [s_{r+1}, t_{v+1}]^{d(r+1)} \equiv y_2^{d(r+1)}.$$

Therefore, $[y_1, t_{v+1}] \in M$, which completes the proof of the lemma.

LEMMA 4.3. *There are elements $m(1), \ldots, m(v)$ and $n(1), \ldots, n(v)$ in $\mathrm{GF}(p)$ such that $m(1) = n(v) = 1$ and such that, if $f = x_1^{m(1)} \ldots x_v^{m(v)}$ and $g = x_{u+2}^{n(1)} \ldots x_{t+1}^{n(v)}$, then*

$$(4.8) \qquad [f, \langle x_1, \ldots, x_k\rangle] \subseteq \langle z_1\rangle,$$

$$(4.9) \qquad [f, Q] \subseteq V_0\langle y_1\rangle,$$

$$(4.10) \qquad [g, Q] \subseteq V_0\langle y_2\rangle, \text{ and}$$

$$(4.11) \qquad [g, \langle x_{r+2}, \ldots, x_{t+1}\rangle] \subseteq \langle z_{v+1}\rangle.$$

Proof. By Lemma 4.1 and the definitions, H stabilizes the chain

$$Q \supseteq Z_2(Q) \supseteq MZ(Q) \supseteq M.$$

Then, $H/C_H(Q/M)$ is a p-group, by Lemma 2.5, so

$$O^p(H)C_H(Q) \subseteq C_2 \cap C_H(Q/M),$$

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press

where C_2 is as in the proof of Lemma 4.1. Then, $H = PC_3 = P^g C_3$, where $C_3 = C_2 \cap C_H(Q/M)$, by (1.4) and (1.5), and now the lemma is proved in the same manner as Lemma 4.1.

LEMMA 4.4. *For* $1 \leqq i \leqq v + 1$, *define*

$$f_i = \varphi^{i-1}(f) = x_i^{m(1)} \dots x_{v+i-1}^{m(v)}$$

and

$$g_i = \varphi^{i-(v+1)}(g) = x_{v+i+1}^{n(1)} \dots x_{u+i}^{n(v)}.$$

Then:

(4.12) $$[f_i, f_j] = [g_i, g_j] = 1, \text{ for } 1 \leqq i, j \leqq v.$$

(4.13) $$[f_i, g_i] = z_i, \text{ for } 1 \leqq i \leqq v.$$

(4.14) $$[f_i, g_j] = 1, \text{ for } 1 \leqq i, j \leqq v \text{ and } j \neq i, i + r.$$

Also, there are elements $h(r + 1), \dots, h(u + 1)$ *in* GF(p) *with* $h(r + 1) \neq 0$, $h(u + 1) \neq 0$, *and*

(4.15) $$[f_i, g_{r+i}] = x_{r+i}^{h(r+1)} \dots x_{u+i}^{h(u+1)}, \text{ for } 1 \leqq i \leqq r + 1.$$

Furthermore, we have

(4.16) $$[f_i, g_{r+i}, g_{r+i}] = z_{r+i}^{h(r+1)}, \text{ for } 1 \leqq i \leqq r + 1.$$

Proof. (4.12), (4.13), and (4.14) for $1 \leqq j \leqq i \leqq r$ follow from the definition of u.

Let $1 \leqq i \leqq r$ and $i < j < i +$ r. Then

$$[f_i, g_j] = \varphi^{i-1}[f, \varphi^{j-v-i}(g)] = \varphi^{j-(v+1)}[\varphi^{v+i-j}(f), g],$$

so, by (4.8) and (4.11),

$$[f_i, g_j] \in \varphi^{i-1}\langle z_1 \rangle \cap \varphi^{j-(v+1)}\langle z_{v+1} \rangle = \langle z_i \rangle \cap \langle z_j \rangle = 1.$$

Thus, (4.14) also holds for $1 \leqq i \leqq r$ and $i < j < i + r$.

Now let $r + 1 \leqq j \leqq v$. Using (4.6), Lemma 2.8, and symmetry, we obtain

(4.17) $$y_1 = x_{r+1}^{d(r+1)} x_{r+2}^{\alpha(r+2)} \dots x_u^{\alpha(u)} x_{u+1}^{d(u+1)} \text{ and } y_2 = \varphi^r(y_1),$$

where $d(r + 1) \neq 0$ and $d(u + 1) \neq 0$. Let

$$A = V_0\langle y_1 \rangle = \langle z_1, z_{r+1}, z_{v+1}, y_1 \rangle, \text{ and}$$
$$B = \varphi^{j-(v+1)}(V_0\langle y_2 \rangle) = \langle \varphi^{j-(v+1)}(z_1), z_{j-r}, z_j, \varphi^{j-(r+1)}(y_1) \rangle.$$

Then, using (4.9), (4.10), and a straightforward calculation of the type used in the previous case ($i < j < i + r$), we see that $[f_1, g_j] \in A \cap B$.

First, assume that $r + 1 < j \leqq v$. Then $B \cap Z(P) = \langle z_{j-r}, z_j \rangle$. If $x \in B - Z(P)$, then x involves x_j or x_{v+r+j} to some non-zero power. (This can be seen by using (4.17) and Lemma 2.8 to expand the elements of B in terms of the x_i.) Similar calculations then show that $x \notin A$, so $B \cap A \subseteq Z(P)$. But

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press

$A \cap Z(P) = \langle z_1, z_{r+1} \rangle$, so $A \cap B = 1$. Thus, $[f_1, g_j] = 1$ for $r + 1 < j \leqq v$. Now, applications of φ establish (4.14) in the remaining cases.

Finally, let $j = r + 1$. Since

$$[f_1, g_{r+1}] \in A \cap B \subseteq \langle A, B \rangle \subseteq \langle \varphi^{-r}(z_1), z_1, z_{r+1}, z_{v+1}, y_1 \rangle,$$

we obtain (4.15) for $i = 1$ and for some elements $h(m) \in \mathrm{GF}(p)$. Applications of φ yield (4.15) for $1 \leqq i \leqq r + 1$.

Now, we must show that $h(r + 1) \neq 0$ and $h(u + 1) \neq 0$. But

$$[f_1, g_{r+1}] \equiv w_1 \not\equiv 1 \quad (\text{modulo } \langle x_{r+2}, \ldots, x_k \rangle), \tag{4.18}$$

by Lemma 2.8 and the definitions of f_1, g_{r+1}, and k, so $h(r + 1) \neq 0$. A similar argument using $[f_{r+1}, g_{v+1}]$ yields $h(u + 1) \neq 0$.

To establish (4.16), we observe that the congruences in (4.18) hold modulo $Z(P)$. Then $[f_1, g_{r+1}, g_{r+1}] = z_{r+1}{}^{h(r+1)}$, by the definitions of w_1, g_{r+1}, and u. Finally, applications of φ yield (4.16). This completes the proof of the lemma.

Recall that $Y \subseteq Z(H)$ and $Z(P) = YZ$.

LEMMA 4.5. *Let $S_i = \langle f_i, g_i, g_{r+i} \rangle$ for $1 \leqq i \leqq r$. Then $[S_i, S_j] = 1$ if $i \neq j$ and $P = S_1 \ldots S_r Y$.*

Proof. This follows directly from the definitions and (4.12)–(4.16), using arguments similar to those in the class two case.

LEMMA 4.6. *For $1 \leqq i \leqq r$, $S_i \cong E^*(p)$ and $P = S_1 \times \ldots \times S_r \times Y$.*

Proof. Fix i with $1 \leqq i \leqq r$. We keep the notation of the previous lemmas. Let $m = h(r + 1)$ and $n = h(u + 1)$, so $m \neq 0$ and $n \neq 0$. Define

$$a = z_{r+i}{}^{-m}, b = z_i{}^{-n}, c = [g_{r+i}{}^{-1}, f_i], d = f_i, e = g_i{}^{-n}, f = g_{r+i}{}^{-1}.$$

Then $S_i = \langle a, b, c, d, e, f \rangle$, so, by Lemma 2.13, to show that $S_i \cong E^*(p)$, it suffices to show that $|S_i| = p^6$ and that (2.6)–(2.10) hold for the elements a, b, c, d, e, and f defined above.

(2.6) follows from the definitions and Lemmas 2.1 and 4.4. (2.7) and the first two statements in each of (2.8) and (2.9) follow since $\langle a, b \rangle \subseteq Z(P)$.

By (4.15), Lemma 2.6, and the definitions of f_i, g_i, and u,

$$[c, d] = [g_{r+i}{}^{-1}, f_i, f_i] = [f_i, g_{r+i}, f_i] = [x_{u+i}{}^n, x_i] = z_i{}^{-n} = b.$$

A similar argument shows that $[c, e] = 1$. By (4.13) and the definitions, $[d, e] = b$. Thus, (2.8) and (2.9) hold. Finally, $[d, f] = c^{-1}$ by definition, and $[c, f] = a$ by (4.16) and Lemma 2.6, so (2.10) holds. Thus, by Lemma 2.7 and the proof of Lemma 2.13, S_i is a homomorphic image of $E^*(p)$. In particular, $|S_i| \leqq p^6$.

Now we can finish the proof of the lemma. $P = S_1 \ldots S_r Y$, so we have

$$p^t = |P| \leqq |Y| \cdot \prod_{i=1}^{r} |S_i| \leqq p^{t-6r} p^{6r} = p^t. \tag{4.19}$$

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press

Therefore, equality holds everywhere in (4.19). In particular, this means that $|P| = |Y| . \prod |S_i|$, so $P = S_1 \times \ldots \times S_r \times Y$. Also, (4.19) implies that $|S_i| = p^6$, so $S_i \cong E^*(p)$ by Lemma 2.13. This completes the proof of Theorem 2.

References

1. J. Currano, *Finite p-groups with isomorphic subgroups* (to appear).

2. G. Glauberman, *Isomorphic subgroups of p-groups*. I, Can. J. Math. *23* (1971), 983–1022.

3. D. Gorenstein, *Finite groups* (Harper and Row, New York, 1968).

4. A. G. Kurosh, *The theory of groups*, second English edition, translated by K. A. Hirsh (Chelsea, New York, 1960).

Roosevelt University,
Chicago, Illinois

https://doi.org/10.4153/CJM-1972-003-x Published online by Cambridge University Press