Can. J. Math., Vol. XXIII, No. 6, 1971, pp. 983–1022

ISOMORPHIC SUBGROUPS OF FINITE p-GROUPS. I

GEORGE GLAUBERMAN

1. Introduction and Notation. Let p be a prime and P be a p-subgroup of a finite group G. Suppose that $g \in G$ and that $P \cap P^g$ has index p in P. In [**4**], we assumed that g normalizes no non-identity normal subgroup of P. We obtained some bounds on the order of P and some applications to the case in which $p = 2$ and P is a Sylow 2-subgroup of $\langle P, P^g \rangle$. In this paper, we examine this situation further by considering the isomorphism ϕ of $P \cap P^{g^{-1}}$ onto $P \cap P^g$ given by $\phi(x) = x^g$. We actually consider arbitrary isomorphisms ϕ between two subgroups of index p in P. However, an easy argument (Lemma 2.3) shows that every such ϕ can be obtained as above for some G and some g. We obtain some results concerning the nilpotence class rather than the order of P.

Let $E(p)$ be the non-Abelian group of order p^3 which is generated by two elements of order p. Thus, $E(p)$ is dihedral if $p = 2$, and $E(p)$ has exponent p if p is odd. If p is odd, then $E^*(p)$ is defined in § 5 to be a particular group of order p^6 and nilpotence class three. Our main results are:

THEOREM 1. *Suppose that p is a prime, that P is a finite p-group, that Q and R are subgroups of index p in P, and that ϕ is an isomorphism of R onto Q. Let N be the subgroup of P generated by all the subgroups of R that are fixed by ϕ. Then*

(a) *ϕ fixes N and $N \trianglelefteq P$,*

(b) *P/N has nilpotence class at most two if $p = 2$, and*

(c) *P/N has nilpotence class at most three if p is odd.*

THEOREM 2. *Let p be a prime and let P be a p-subgroup of a finite group Ht Assume that, for some $h \in H$, $\langle P, P^h \rangle = H$, and that $[P:P \cap P^h] = p$. Le. $P_1 = P$ and $P_{i+1} = [P_i, P]$, for $i = 1, 2, 3$.*

Suppose that α is an automorphism of P that fixes no non-identity normal subgroup of H contained in P. Let $|P/Z(P)| = p^x$ and let n be the smallest positive integer such that α^n fixes $P \cap P^h$. Then $P_4 = 1$, x is even, and, if $P_2 \neq 1$, $x/2$ divides n.

Furthermore, let $v = x/2$ and, if $P_2 \neq 1$, let $n = qv$. Then:

(a) *Suppose that $P_2 = 1$. Then P is an elementary Abelian group and $|P| \leqq p^n$.*

(b) *Suppose that $P_3 = 1$ and $P_2 \neq 1$. Then $|P_2| = p^v$; $q > 1$; $q = 2$, if $p = 2$; and q is a divisor of p, $p - 1$, or $p + 1$, if p is odd. Moreover, P is a*

Received March 12, 1971.

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

direct product of an elementary Abelian group with a direct product of v subgroups isomorphic to $E(p)$.

(c) *Suppose that $P_3 \neq 1$. Then p is odd, v is even, $|P_3| = p^v$, and $q = 1$. Moreover, P is a direct product of an elementary Abelian group with a direct product of $v/2$ subgroups isomorphic to $E^*(p)$.*

(d) *Let $Z = P \cap Z(H)$. Define t by $p^t = |P|$. If $t \geqq 2v + 2$, then $Z \cap Z^\alpha \cap \ldots \cap Z^{\alpha^{t-2v-2}} \neq 1$.*

(e) *If $P_3 \neq 1$ and P is a Sylow p-subgroup of H, then $p = 3$.*

Theorem 2 is related to a question about Sylow p-subgroups of finite groups. Let G be a finite group, p be a prime, S be a Sylow p-subgroup of G, and c be the nilpotence class of S. Suppose that G contains a normal p-subgroup T such that $C(T) \subseteq T$. Let α be an automorphism of S. We ask whether α fixes some non-identity normal p-subgroup U of G.

If p is odd and SL$(2, p)$ is not involved in G, then the answer is affirmative. By [**5**, Theorems 8.1.2 and 8.2.11], we can let $U = Z(J(S))$; here $J(S)$ is the Thompson subgroup of S, generated by the Abelian subgroups of S of maximal order. However, it is easy to construct examples in which the answer is negative, e.g., where $|T| = p^2$ and G/T is isomorphic to SL$(2, p)$. Thus, one might hope that the answer is affirmative if T or S is "large" in some sense. Let us consider the special case in which $|S/T| = p$ and

$$G = \langle S, S^h \rangle, \tag{1.1}$$

for some $h \in G$. Then Theorem 2 gives us an affirmative answer when $c > 2$ and $p \neq 3$, or when $c > 3$ and $p = 3$.

The relation between Theorem 2 and Theorem 1 is illustrated by the fact that Theorem 1 already gives an affirmative answer if $c > 3$. To see this, take h as in (1.1) and consider the mapping $\phi: T^{\alpha^{-1}} \rightarrow T$ given by $\phi(x) = (x^\alpha)^h$, $x \in T^{\alpha^{-1}}$. Assume that $c > 3$. Then we obtain $N \neq 1$ in Theorem 1. A short argument (using Lemma 2.4) shows that $N \trianglelefteq G$ and hence that α fixes N.

Theorem 1 is proved in § 3. The basic ideas of its proof stem from Sims' work (see Propositions 2.1 and 3.4). For Theorem 2, we are mainly interested in the case in which P is a Sylow p-subgroup of H. However, we make some use of weaker assumptions. Thus, throughout each of §§ 4, 5, and 7, we have a general hypothesis, stated at the beginning of the section, which is satisfied if P is a Sylow p-subgroup of H. An extension of Theorem 2 is given in § 8 (Theorem 8.1). Note that both Theorem 2 and Theorem 8.1 yield information if H is embedded in a larger group G and some element of $N_G(P)$ normalizes no non-identity normal subgroup of H contained in P.

Let P be an arbitrary group that satisfies Theorem 1 with $N = 1$. Comparing Theorems 1 and 2, one might suspect that P must always have a direct product decomposition as in part (a), (b), or (c) of Theorem 2. But this is not true. One may easily construct counterexamples (for example, see the note after Definition 5.8). In [**3**], J. Currano has characterized all such groups P by

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

generators and relations. Moreover, he has shown that P has a direct product decomposition under weaker assumptions than the hypothesis of Theorem 2 (see Remark 5.11).

All groups considered in this paper will be finite. Most of our notation is taken from [**5**]; we list some special cases and exceptions. Let G be a group. We write $H \subseteq G$ if H is a subgroup of G; $H \subset G$ if $H \subseteq G$ and $H \neq G$; $H \trianglelefteq G$ if H is a normal subgroup of G; and $H \triangleleft G$ if $H \trianglelefteq G$ and $H \neq G$. If $H \subseteq G$, let $[G:H]$ be the index of H in G. As in [**5**], let $[x, y, z] = [[x, y], z]$ and $[H, K, L] = [[H, K], L]$, for $x, y, z \in G$ and $H, K, L \subseteq G$.

Let p be a prime. For every group G, let $O^p(G)$ be the subgroup of G generated by all the p'-elements of G. Let $\mathbf{Z}_p$ be the field of the integers modulo p. In discussing a p-group, we will sometimes use "elementary" to mean "elementary Abelian".

For a vector space V, let $\mathrm{SL}(V)$ be the special linear group on V, i.e., the group of all linear transformations of determinant one on V.

Acknowledgement. We thank 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 part of this work during the Bowdoin Finite Groups Seminar in the summer of 1970.

2. Preliminary results. Let G be a group and let ϕ be an isomorphism from a subgroup H of G onto a subgroup K of G. We say that ϕ *fixes* an element or subgroup of H if it maps it to itself. Suppose that $L \subseteq G$. Define $\phi^0(L) = L \cap K$ and

$$\phi^{-(i+1)}(L) = \{\phi^{-1}(x) | x \in \phi^{-i}(L) \cap K\}, \quad i = 0, 1, 2, \ldots .$$

The following fundamental result is a restatement of some results of [**10**].

PROPOSITION 2.1 (Sims). *Suppose that P is a finite p-group of order p^t, that Q and R are subgroups of index p in P, and that ϕ is an isomorphism of R onto Q. Let N be the subgroup of P generated by all the subgroups of R that are fixed by ϕ. Then:*

(a) *ϕ fixes N;*

(b) *$N \trianglelefteq P$; and*

(c) *if $N = 1$, then there exists $x \in P$ such that $x \in \phi^{-(t-1)}(P)$, and such that $\langle x, \phi(x), \ldots, \phi^{i-1}(x)\rangle$ has order p^i, for $i = 1, 2, \ldots, t$.*

Proof. (a) This is obvious.

(b) If $Q = R$, then $N = Q$. Suppose that $Q \neq R$. Then ϕ maps $R \cap Q$ isomorphically into Q, and maps $\phi^{-1}(R \cap Q)$ isomorphically into R. Since $N \subseteq R \cap Q$ and $N \subseteq \phi^{-1}(R \cap Q)$, we may assume by induction that $N \trianglelefteq Q$ and that $N \trianglelefteq R$. Therefore, $N \trianglelefteq QR = P$.

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

(c) Let $R_0 = P$ and $R_1 = \phi^{-i}(P)$, for $i = 1, 2, 3, \ldots$. Then $R_1 = R$ and $R_{i+1} = R \cap \phi^{-1}(R_i) \subseteq R$, for all $i \geqq 0$. Since $N = 1$, we have $R_i \supset R_{i+1}$ whenever $R_i \neq 1$. However, for each i,

$$|R_{i+1}| = |R \cap \phi^{-1}(R_i)| = |\phi(R) \cap R_i| = |Q \cap R_i| \geqq |R_i|/p,$$

so $|R_i/R_{i+1}| \leqq p$. Thus, $|R_i/R_{i+1}| = p$, if $R_i \neq 1$. Consequently, $|R_{t-1}| = p$. Moreover, for $1 \leqq i \leqq t - 1$, we have $\phi(R_i) \neq R_i$ and $\phi(R_i) \subseteq R_{i-1}$; hence, $R_{i-1} = \langle R_i, \phi(R_i)\rangle$. By induction,

$$R_{t-1-i} = \langle R_{t-1}, \phi(R_{t-1}), \ldots, \phi^i(R_{t-1})\rangle, \quad \text{for} \quad i = 1, 2, \ldots, t-1.$$

Let x be a generator of R_{t-1}. We obtain (c).

Our next two lemmas are special cases of results of G. Higman, B. H. Neumann, and H. Neumann [**8**, Volume II, p. 53].

LEMMA 2.2. *Let H and K be subgroups of a finite group G. Let S be the symmetric group on G. Embed G in S by identifying each element g of G with the permutation $x \to xg (x \in G)$ of G.*

Suppose that there exists an isomorphism ϕ of H onto K. Then there exists $g \in S$ such that $g^{-1}Hg = K$ and $g^{-1}hg = \phi(h)$, for all $h \in H$.

Proof. Let $n = [G:H] = [G:K]$. Take $x_1, \ldots, x_n, y_1, \ldots, y_n \in G$ such that

$$G = \bigcup x_i H = \bigcup y_i K.$$

In this proof, we will write x^s to denote the image of an element x of G under an element s of S. Define $g \in S$ by

$$(x_i h)^g = y_i \phi(h), \quad \text{for} \quad 1 \leqq i \leqq n \text{ and } h \in H.$$

For $i = 1, \ldots, n$ and $h, z \in H$, we have

$$\begin{aligned}(y_i\phi(z))^{g^{-1}hg} &= (x_i z)^{hg} \\ &= (x_i zh)^g \\ &= y_i \phi(zh) \\ &= y_i \phi(z)\phi(h) \\ &= (y_i\phi(z))^{\phi(h)}.\end{aligned}$$

So $g^{-1}hg = \phi(h)$.

LEMMA 2.3. *Let H and K be subgroups of a finite group G. Let*

$$\Omega = \{(\alpha, r) | \alpha \in G; r = 1, 2\},$$

and let S be the symmetric group on Ω. Suppose that there exists an isomorphism ϕ of H into K. Then there exists an embedding of G into S and an element g of S such that $g^{-1}Hg = K = g^{-1}Gg \cap G$ and $g^{-1}hg = \phi(h)$, for all $h \in H$.

Proof. First assume that $H = 1$. Embed G in S by defining

$$(x, 1)^y = (xy, 1) \quad \text{and} \quad (x, 2)^y = (x, 2), \quad \text{for } x, y \in G.$$

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

Define g by

$$(x, 1)^g = (x, 2) \quad \text{and} \quad (x, 2)^g = (x, 1), \quad \text{for } x \in G.$$

Now assume that $H \neq 1$. Then $K \neq 1$. Take $k \neq 1$ in K. Define n and $x_1, \ldots, x_n, y_1, \ldots, y_n$ as in the proof of Lemma 2.2. We may assume that $x_1 = y_1 = 1$. Embed G in S by defining

$$(x, r)^y = (xy, r), \text{ for } x, y \in G \quad \text{and} \quad r = 1, 2.$$

Define g by

$$\begin{aligned}(x_ih, 1)^g &= (y_i\phi(h), 1), && \text{for } 1 \leqq i \leqq n \text{ and } h \in H;\\ (h, 2)^g &= (\phi(h), 2), && \text{for } h \in H; \text{ and}\\ (x_ih, 2)^g &= (y_ik\phi(h), 2), && \text{for } 2 \leqq i \leqq n \text{ and } h \in H.\end{aligned}$$

As in the proof of Lemma 2.2, we obtain $g^{-1}hg = \phi(h)$ for all $h \in H$.

We claim that $g^{-1}Gg \cap G = K = g^{-1}Hg$. Suppose that this is false. Take $x \in G - H$ such that $g^{-1}xg \in G$. Let $x = x_ih$, where $h \in H$. Then $i > 1$. Moreover,

$$g^{-1}x_ig = (g^{-1}xg)(g^{-1}hg)^{-1} \in G.$$

Since $x_1 = y_1 = 1$,

$$(g^{-1}x_ig, 1) = (1, 1)^{g^{-1}x_ig} = (1, 1)^{x_ig} = (x_i, 1)^g = (y_i, 1).$$

Thus, $g^{-1}x_ig = y_i$. So

$$(y_i, 2) = (1, 2)^{y_i} = (1, 2)^{g^{-1}x_ig} = (1, 2)^{x_ig} = (x_i, 2)^g = (y_ik, 2).$$

Since $k \neq 1$, this is a contradiction.

LEMMA 2.4. *Suppose that P is a finite p-subgroup of a group G. Let ψ be an isomorphism of P into G such that $P \cap \psi(P)$ has index p in P. Let $N(\psi)$ be the subgroup of P generated by all the subgroups of P that are fixed by ψ. Then:*

(a) *We have $N(\psi) \trianglelefteq \langle P, \psi(P)\rangle$.*

(b) *Suppose that $Q = P \cap \psi(P)$ and that ψ' is the restriction of ψ to $\psi^{-1}(Q)$. Then $N(\psi)$ is the subgroup of P generated by all the subgroups of $\psi^{-1}(Q)$ that are fixed by ψ'.*

Proof. Define Q and ψ' as in (b). Clearly, $N(\psi) = \psi^{-1}(N(\psi)) \subseteq \psi^{-1}(Q)$. This yields (b). By Sims' result (Proposition 2.1), $N(\psi) \trianglelefteq P$. Hence, $N(\psi) = \psi(N(\psi)) \trianglelefteq \psi(P)$.

Note. For any isomorphism ψ that satisfies the hypothesis of Lemma 2.4, we define $N(\psi)$ as in the lemma.

The next two lemmas are proved in [**5**, pp. 18–19]:

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

LEMMA 2.5. *Let G be a group in which $G' \subseteq Z(G)$. Let $x, y, z \in G$. Then*

$$[xy, z] = [x, z][y, z],$$
$$[x, yz] = [x, y][x, z], \text{ and}$$
$$[x^i, y^j] = [x, y]^{ij}, \text{ for all integers } i, j.$$

LEMMA 2.6 (Three Subgroups Lemma; P. Hall). *Let G be a group.*

(a) *For all $x, y, z \in G$,*

$$[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1.$$

(b) *If $H, K, L \subseteq G$ and $[H, K, L] = [K, L, H] = 1$, then $[L, H, K] = 1$.*

3. The general case. In this section we assume the hypothesis and notation of Proposition 2.1. We further assume that $N = 1$. Take x as in Proposition 2.1(c); let $x_i = \phi^{i-1}(x)$, for $i = 1, 2, \ldots, t$. Then we have

(3.1) (a) *$|P| = p^t$, p is a prime, and $t \geqq 1$;*

(b) *$|Q| = |R| = p^{t-1}$;*

(c) *ϕ is an isomorphism of R onto Q that fixes no non-identity subgroup of R;*

(d) *$x_1, \ldots, x_{t-1} \in R$ and $\phi(x_i) = x_{i+1}$, for $i = 1, \ldots, t-1$;*

and

(e) *$|\langle x_1, \ldots, x_i\rangle| = p^i$, for $i = 1, 2, \ldots, t$.*

We will not use subscripts to denote terms of the lower central series of a group, except that we define $P_2 = P'$; $P_3 = [P_2, P]$; and $P_4 = [P_3, P]$. We also define the parameters u, v, and k as follows. Let $u = t$ if P is Abelian. Otherwise, let u be the smallest positive integer such that $[x_i, x_{u+i}] \neq 1$ for some i. Let $v = t - u$. Let $k = t$ if $P_3 = 1$. Otherwise, let k be the smallest positive integer such that $[x_i, x_{k+i}] \notin Z(P)$ for some i (k must exist since $P/Z(P)$ is not Abelian).

For $1 \leqq i \leqq j \leqq t$, we write $\langle x_i, \ldots, x_j\rangle$ to denote the group $\langle x_r | i \leqq r \leqq j\rangle$. Similarly, we often denote an element of $\langle x_i, \ldots, x_j\rangle$ by $x_i^{e(i)} \ldots x_j^{e(j)}$ for some function e; here, it is understood that the subscripts on the x's increase from left to right in the actual product.

Throughout this section we assume (3.1).

From (d) and (e) we obtain easily:

LEMMA 3.1. *For every $x \in P$, there exist unique elements $e(1), \ldots, e(t) \in \mathbf{Z}_p$ such that $x = x_1^{e(1)} \ldots x_t^{e(t)}$.*

LEMMA 3.2. (a) *If $1 \leqq i < j \leqq t$, then*

$$[\langle x_i\rangle, \langle x_j\rangle] \subseteq \langle x_{i+1}, \ldots, x_{j-1}\rangle.$$

(b) *If $P' \neq 1$ and $1 \leqq i \leqq v$, then $[x_i, x_{u+i}] \neq 1$.*

Proof. (a) First, suppose that $j = i + 1$. Then $\langle x_i, x_j\rangle = \phi^{i-1}(\langle x_1, x_2\rangle)$. By (3.1) (e), $|\langle x_1, x_2\rangle| = p^2$. Hence, $\langle x_1, x_2\rangle$ and $\langle x_i, x_j\rangle$ are Abelian.

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

Now suppose that $j \geqq i + 2$. Similar calculations show that $\langle x_i, \dots, x_{j-1}\rangle$ and $\langle x_{i+1}, \dots, x_j\rangle$ have index p and are therefore normal in $\langle x_i, \dots, x_j\rangle$. Hence,

$$[\langle x_i\rangle, \langle x_j\rangle] \in \langle x_i, \dots, x_{j-1}\rangle \cap \langle x_{i+1}, \dots, x_j\rangle = \langle x_{i+1}, \dots, x_{j-1}\rangle.$$

This proves (a).

(b) By the definition of u, we have $[x_j, x_{u+j}] \neq 1$ for some j for which $1 \leqq j \leqq v$. Hence $[x_i, x_{u+i}] = \phi^{i-j}([x_j, x_{u+j}]) \neq 1$.

The following symmetry principle will be quite handy:

LEMMA 3.3. *Let n be a nonzero element of $\mathbf{Z}_p$. Condition* (3.1) *and the definitions of u, v, and k remain valid if we replace P by P, Q by R, R by Q, ϕ by ϕ^{-1}, and x_i by $(x_{t+1-i})^n$, for $i = 1, \dots, t$.*

Recall that $u = t$ if P is Abelian.

PROPOSITION 3.4 (Sims [**10**, Lemma 2.7]). *Assume that P is not Abelian. Then*

(a) $u \geqq \frac{2}{3}t$;

(b) $[x_1, x_{u+1}] \in \langle x_{v+1}, \dots, x_{u-v+1}\rangle$, *and*

(c) $[x_i, x_{u+i}] \in \Omega_1(Z(P))$, *for* $i = 1, \dots, v$.

Proof. Since P is not Abelian, $u < t$. Suppose that $1 \leqq i \leqq v$ and that $i \leqq u$. Then

$$[x_{u+1}^{-1}, x_{u+i}^{-1}, x_1] = [1, x_1] = 1,$$

and

$$[x_{u+i}, x_1^{-1}, x_{u+1}^{-1}] \in [\langle x_2, \dots, x_{u+i-1}\rangle, \langle x_{u+1}\rangle] = 1,$$

by Lemma 3.2 and the definition of u. By the Three Subgroups Lemma (Lemma 2.5)

$$[x_1, x_{u+1}, x_{u+i}] = 1. \tag{3.2}$$

By Lemma 3.2, $1 \neq [x_1, x_{u+1}] \in \langle x_2, \dots, x_u\rangle$. Let $[x_1, x_{u+1}] = x_m^{e(m)} \dots x_n^{e(n)}$, where $e(m)$, $e(n) \neq 0$. Then $m \leqq u$. Suppose that $m \leqq v$. Then $u + m \leqq t$, and x_{u+m} centralizes $x_{m+1}, \dots, x_n$ but not x_m (by Lemma 3.2). So

$$[x_1, x_{u+1}, x_{u+m}] = [x_m^{e(m)} \dots x_n^{e(n)}, x_{u+m}] \neq 1,$$

contrary to (3.2). Thus, $m \geqq v + 1$.

Let $y_i = x_{t+1-i}$, for $i = 1, 2, \dots, t$. Then

$$\begin{aligned}
[y_1, y_{u+1}] &= [x_t, x_v] \\
&= [x_v, x_t]^{-1} \\
&= \phi^{v-1}([x_1, x_{u+1}]^{-1}) \\
&= \phi^{v-1}(x_n^{-e(n)} \dots x_m^{-e(m)}) \\
&= \phi^{v-1}(y_{t+1-n}^{-e(n)} \dots y_{t+1-m}^{-e(m)}) \\
&= y_{u+2-n}^{-e(n)} \dots y_{u+2-m}^{-e(m)}.
\end{aligned}$$

By the above argument and by symmetry (see Lemma 3.3), we obtain $u + 2 - n \geqq v + 1$. Therefore,

$$v + 1 \leqq m \leqq n \leqq (u + 2) - (v + 1) = u - v + 1.$$

Since $v = t - u$, this proves (a) and (b).

Suppose that $1 \leqq i \leqq v$. Then

$$[x_i, x_{u+i}] = \phi^{i-1}([x_1, x_{u+1}]) \in \langle x_{v+i}, \ldots, x_{u-v+i}\rangle \subseteq \langle x_{v+1}, \ldots, x_u\rangle \subseteq Z(P),$$

by (b) and the definition of u. Since every x_j has order p, this proves (c) and completes the proof of Proposition 3.4.

LEMMA 3.5. (a) *For* $i = 1, \ldots, v$,

$$C_P(\langle x_i, \ldots, x_u\rangle) = \langle x_1, \ldots, x_{u+i-1}\rangle.$$

(b) *For* $i = u + 1, \ldots, t$,

$$C_P(\langle x_{v+1}, \ldots, x_i\rangle) = \langle x_{i-u+1}, \ldots, x_t\rangle.$$

(c) *Moreover*, $Z(P) = \langle x_{v+1}, \ldots, x_u\rangle$ *and* $Z(Q) = \langle x_{v+1}, \ldots, x_{u+1}\rangle$; *both are elementary Abelian.*

Proof. If P is Abelian, then $u = t$ and $v = 0$, and the lemma is obvious. Assume that P is not Abelian.

(a) Let $C = C_P(\langle x_i, \ldots, x_u\rangle)$. By the definition of u, C contains $\langle x_1, \ldots, x_{u+i-1}\rangle$. Suppose that it contains some further element x. Let $x = x_1^{e(1)} \ldots x_m^{e(m)}$, where $m \geqq u + i$ and $e(m) \neq 0$. Then $i \leqq m - u \leqq t - u \leqq u$, so $x \in C \subseteq C_p(x_{m-u})$ and x_{m-u} centralizes

$$x_1, x_2, \ldots, x_{m-u}, \ldots, x_{m-1}.$$

Hence, x_{m-u} centralizes $x_m^{e(m)}$, contrary to Lemma 3.2.

(b) Use (a) and symmetry.

(c) Take $i = 1$ in (a) and $i = t$ in (b). We obtain

$$Z(P) \subseteq \langle x_1, \ldots, x_u\rangle \cap \langle x_{v+1}, \ldots, x_t\rangle = \langle x_{v+1}, \ldots, x_u\rangle.$$

We obtain the reverse containment because $[x_i, x_j] = 1$ whenever $1 \leqq i \leqq t$ and $v + 1 \leqq j \leqq u$, by the definition of u and v. A similar argument yields that $Z(Q) = \langle x_{v+1}, \ldots, x_{u+1}\rangle$. Since every x_j has order p, $Z(P)$ and $Z(Q)$ are elementary Abelian.

Recall that $k = t$ if $P_3 = 1$.

PROPOSITION 3.6. *Suppose that* $P_3 \neq 1$. *Then*

$$k \geqq u + \tfrac{1}{2}v, \tag{3.3}$$

and

$$[x_1, x_{k+1}] = x_m^{e(m)} \ldots x_n^{e(n)}, \tag{3.4}$$

for some integers m, n and some $e(m), \ldots, e(n) \in \mathbf{Z}_p$ such that

(a) $1 \leqq m \leqq n \leqq t$,

(b) *both $e(m)$ and $e(n)$ are nonzero,*

(c) $m = k - u + 1$ *or* $n = u + 1$,

(d) $m = k - u + 1$ *or* $m \geqq v + 1$, *and*

(e) $n = u + 1$ *or* $n \leqq k + 1 - v$.

Proof. If $[x_1, x_{k+1}] = 1$, then $[x_i, x_{k+i}] = \phi^{i-1}([x_1, x_{k+1}]) = 1 \in Z(P)$, for $i = 1, \ldots, t - k$, contrary to the definition of k. Thus, $[x_1, x_{k+1}] \neq 1$. Take m, n and $e(m), \ldots, e(n)$ to satisfy (3.4), (a), and (b).

Suppose that $m \geqq v + 1$ and that $n \leqq k + 1 - v$. Then, for $1 \leqq i \leqq t - k$, we have $v + 1 \leqq m \leqq m + i - 1$ and $n + i - 1 \leqq u$; hence,

$$[x_i, x_{i+k}] = \phi^{i-1}([x_1, x_{k+1}]) = \phi^{i-1}(x_m{}^{e(m)} \ldots x_n{}^{e(n)})$$
$$= x_{m+i-1}{}^{e(m)} \ldots x_{n+i-1}{}^{e(n)} \in \langle x_{v+1}, \ldots, x_u\rangle \subseteq Z(P).$$

This contradicts the definition of k. So we have

$$m \leqq v \text{ or } n \geqq k + 2 - v. \tag{3.5}$$

We will assume for a while that $m \leqq v$. Let

$$N = \langle x_{v+1}, \ldots, x_k\rangle,$$

and let $C = C_P(N)$. Since $k \geqq u$, Lemma 3.5 yields that $N \supseteq Z(P)$ and that

$$C = \langle x_{k+1-u}, \ldots, x_t\rangle.$$

By our choice of k, we have $[\langle x_j\rangle, N] \subseteq Z(P)$, for $j = 1, \ldots, k - u$. Since $[C, N] = 1$, we have $[P, N] \subseteq Z(P) \subseteq N$. Therefore, $N \trianglelefteq P$ and $C \trianglelefteq P$. It follows that $[x_1, x_{k+1}] \in C$ and consequently that $m \geqq k + 1 - u$. We will show that $m = k + 1 - u$.

Let $Y = \langle [x_{k+1-u}, x_{k+1}]\rangle$. Then $Y \subseteq Z(P)$, by Proposition 3.4. Moreover, $[C, x_{k+1}] \subseteq Y$. Hence, the coset $x_{k+1}Y$ is in the centre of C/Y. Since $C \trianglelefteq P$, we have $C/Y \trianglelefteq P/Y$ and $Z(C/Y) \trianglelefteq P/Y$. Consequently,

$$[x_1, x_{k+1}]Y \in Z(C/Y). \tag{3.6}$$

Therefore,

$$[x_m{}^{e(m)} \ldots x_n{}^{e(n)}, x_{u+m}] = [x_1, x_{k+1}, x_{u+m}] \in Y = \langle [x_{k+1-u}, x_{k+1}]\rangle. \tag{3.7}$$

Let $Y_1 = \langle [x_m, x_{u+m}]\rangle$. Then $Y_1 \subseteq Z(P)$, and x_{u+m} centralizes $x_m, \ldots, x_n$ modulo Y_1. By (3.7),

$$1 \neq [x_m{}^{e(m)} \ldots x_n{}^{e(n)}, x_{u+m}] \in Y \cap Y_1 = Y \cap \phi^{m-(k+1-u)}(Y).$$

Since $|Y| = p$, $m - (k + 1 - u)$ is zero; that is, $m = k + 1 - u$.

Suppose that $k < u + \frac{1}{2}v$. Then $2k < 2u + v = u + t$, $2k + 1 \leqq u + t$, and $m + k = 2k + 1 - u \leqq t$. By (3.6) and the definition of C,

$$[x_m{}^{e(m)} \ldots x_n{}^{e(n)}, x_{m+k}] = [x_1, x_{k+1}, x_{m+k}] \in Y \subseteq Z(P).$$

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

Hence, x_{m+k} centralizes $x_m^{e(m)} \ldots x_n^{e(n)}$ modulo $Z(P)$. By the definition of k, x_{m+k} centralizes $x_{m+1}, \ldots, x_n$ modulo $Z(P)$. As $e(m) \neq 0$, x_{m+k} centralizes x_m modulo $Z(P)$. However,

$$\begin{aligned}[x_m, x_{m+k}] &= \phi^{m-1}([x_1, x_{k+1}]) \\ &= \phi^{m-1}(x_m{}^{e(m)} \ldots x_n{}^{e(n)}) \\ &= x_{2m-1}{}^{e(m)} \ldots x_{n+m-1}{}^{e(n)}.\end{aligned}$$

As $2m - 1 = 2(k + 1 - u) - 1 = 2k - 2u + 1 < v + 1$, this contradicts Lemma 3.5(c). Hence $k \geqq u + \frac{1}{2}v$.

We have now proved (3.3), (c), and (d) under the assumption that $m \leqq v$. Let $y_i = x_{t+1-i}$, for $i = 1, \ldots, t$. Then

$$\begin{aligned}[y_1, y_{k+1}] &= [x_t, x_{t-k}] \\ &= \phi^{t-k-1}([x_1, x_{k+1}]^{-1}) \\ &= \phi^{t-k-1}(y_{t+1-n}{}^{-e(n)} \ldots y_{t+1-m}{}^{-e(m)}) \\ &= y_{k+2-n}{}^{-e(n)} \ldots y_{k+2-m}{}^{-e(m)}.\end{aligned}$$

By symmetry (Lemma 3.3) and by the above argument, we obtain (3.3) and $k + 2 - n = k + 1 - u$ (that is, $n = u + 1$) if $k + 2 - n \leqq v$ (that is, if $n \geqq k + 2 - v$), regardless of m. Thus, we obtain (3.3), (c), and (e) if $n \geqq k + 2 - v$. By (3.5), $m \leqq v$ or $n \geqq k + 2 - v$. This proves (3.3) and (c) in all cases. Since (d) is trivial if $m > v$ and (e) is trivial if $n < k - v + 2$, this completes the proof of Proposition 3.6.

THEOREM 3.7. *If $p = 2$, then $P_3 = 1$. In all cases, $P_4 = 1$ and*

$$P' \subseteq \langle x_{t+1-k}, \ldots, x_k \rangle.$$

Proof. We assume that $P_3 \neq 1$ and use the notation and results of Proposition 3.6. By symmetry, we may assume that

$$m = k - u + 1. \tag{3.8}$$

Suppose that $p = 2$. Let $x = x_1$ and $y = x_{k+1}$. Then

$$x = x^{y^2} = (x[x, y])^y = x^y[x, y]^y = x[x, y]^2[x, y, y]. \tag{3.9}$$

Since $0 \leqq n - m \leqq (u + 1) - (k - u + 1) < u$ by Proposition 3.6, the group $\langle x_m, \ldots, x_n \rangle$ is elementary Abelian. Consequently,

$$[x, y]^2 = [x_1, x_{k+1}]^2 = 1,$$

and (3.9) yields

$$1 = [x, y, y] = [x_m{}^{e(m)} \ldots x_n{}^{e(n)}, x_{k+1}]. \tag{3.10}$$

By (3.8), $k + 1 = m + u$. Hence, x_{k+1} centralizes $x_{m+1}, \ldots, x_n$. Since $e(m) \neq 0$, (3.10) yields $[x_m, x_{k+1}] = 1$, which is a contradiction. Thus, $p \neq 2$.

Let

$$N_1 = \langle x_{v+1}, \ldots, x_k \rangle, \qquad N_2 = \langle x_{t+1-k}, \ldots, x_u \rangle,$$
$$C_1 = \langle x_{k+1-u}, \ldots, x_t \rangle, \text{ and } C_2 = \langle x_1, \ldots, x_{t+u-k} \rangle.$$

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

By the definition of k, we have $[N_i, P] \subseteq Z(P) \subseteq N_i$, for $i = 1, 2$. By Lemma 3.5, $C_i = C_P(N_i)$, for $i = 1, 2$. Thus, $N_1, N_2 \trianglelefteq P$. Hence, $C_1, C_2 \trianglelefteq P$.

Suppose that $1 \leqq i \leqq j \leqq t$ and that $[x_i, x_j] \neq 1$. Then $j - i \geqq u$, so $j \geqq u + 1 \geqq v + 1 \geqq k - u + 1$. Thus, $x_j \in C_1$ and $[x_i, x_j] \in C_1$. Similarly, $i \leqq u \leqq t + u - k$ and $[x_i, x_j] \in C_2$. Since $C_1 \cap C_2 \trianglelefteq P$, we obtain

$$P' \subseteq C_1 \cap C_2 = \langle x_{k+1-u}, \ldots, x_{t+u-k} \rangle. \tag{3.11}$$

Since $k \geqq u + \frac{1}{2}v$, $2k \geqq 2u + v = t + u$. Hence, $k + 1 - u \geqq t + 1 - k$ and $t + u - k \leqq k$. By (3.11),

$$P' \subseteq \langle x_{t+1-k}, \ldots, x_k \rangle. \tag{3.12}$$

By (3.12) and the definition of k, we have $P_3 = [P', P] \subseteq Z(P)$. Therefore, $P_4 = 1$.

Example 3.8. Let $P = E(p)$ and let a and b be two generators of P that have order p. Let

$$x_1 = a, \quad x_2 = [a, b], \quad \text{and} \quad x_3 = b.$$

Let $R = \langle x_1, x_2 \rangle$ and $Q = \langle x_2, x_3 \rangle$. Then Q and R are elementary Abelian groups of order p^2 and are isomorphic under a mapping ϕ that satisfies (3.1). Here P has nilpotence class two.

Example 3.9. Assume that p is odd. Take a and b as in Example 3.8, and let $c = [a, b]$. Let Q be the direct product of $\langle a, b \rangle$ and an elementary group $\langle d, e \rangle$ of order p^2. Then there exists a unique automorphism α of Q given by

$$a^\alpha = a, b^\alpha = a^{-1}bc, c^\alpha = c, d^\alpha = d, e^\alpha = d^{-1}e.$$

(Since p is odd, $(a^{-1}bc)^p = 1$.) Moreover, $\alpha^p = 1$.

Let P be the semi-direct product of Q by $\langle \alpha \rangle$. Let

$$x_1 = \alpha, \quad x_2 = a, \quad x_3 = d, \quad x_4 = c, \quad x_5 = e, \quad \text{and} \quad x_6 = b.$$

Let $R = \langle x_1, x_2, x_3, x_4, x_5 \rangle = \langle \alpha, e \rangle \times \langle a, c \rangle$. Then Q and R are isomorphic under a mapping ϕ that satisfies (3.1). Since $P' = \langle a, c, d \rangle$ and $P_3 = \langle c \rangle$, P has nilpotence class three.

Remark 3.10. It is easy to see that in (3.1), P is elementary Abelian if $v = 0$ and P is a direct product of $E(p)$ and a (possibly trivial) elementary Abelian group if $v = 1$. On the other hand, it is easy to construct examples for which $v = 0$ and t is an arbitrary positive integer, or for which $v = 1$ and t is an arbitrary integer greater than two. In [**3**], J. Currano has classified all groups P and isomorphisms ϕ that satisfy (3.1).

4. A restricted case. Suppose that P satisfies (3.1). In Lemma 2.2, we have shown that P can be embedded in some finite group G such that ϕ is effected by conjugation by some element g of G. Suppose that P is thus embedded;

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

let $H = \langle P, P^g \rangle$ and $x_{t+1} = x_t^g$. Since $[P^g : Q] = p$, Q is normal in P^g and therefore in H. Then $H = \langle Q, x_1, x_{t+1} \rangle$. In this section we investigate the structure of P when P and H satisfy the following restrictions:

$$(4.1) \qquad P \textit{ is not Abelian;}$$

$$(4.2) \qquad H = C_H(Q) O^p(H) P^g.$$

It is of interest to show that (4.2) depends only on P and ϕ, and does not depend on the group G in which P is embedded. Let ψ be the homomorphism of H into Aut Q that maps each $h \in H$ to the automorphism of Q given by $x \rightarrow x^h$. Let H^* be the image of ψ, and let P^* be the image of P^g under ψ. Then (4.2) is equivalent to the condition that $H^* = O^p(H^*)P^*$. However,

$$H^* = \langle \psi(x_i) | 1 \leqq i \leqq t + 1 \rangle \quad \textit{and} \quad P^* = \langle \psi(x_i) | 2 \leqq i \leqq t + 1 \rangle.$$

Now, $\psi(x_i)$ is determined by the structure of P, for $i = 1, \ldots, t$. Moreover, $\psi(x_{t+1})$ is determined by the condition

$$\begin{aligned} x_i^{\psi(x_{t+1})} &= x_i^{x_{t+1}} \\ &= (x_{i-1}^g)^{x_t g} \\ &= (x_{i-1}^{x_t})^g \\ &= \phi(x_{i-1}^{x_t}), \text{ for } i = 2, \ldots, t. \end{aligned}$$

Thus, (4.2) is determined solely by P and ϕ.

Throughout the remainder of this section we assume (3.1), (4.1), *and* (4.2).

By Proposition 3.4, $[x_1, x_{u+1}] \in \langle x_{v+1}, \ldots, x_{u-v+1} \rangle$. Define

$$c(v + 1), \ldots, c(u - v + 1) \in \mathbf{Z}_p$$

by

$$(4.3) \qquad [x_1, x_{u+1}] = x_{v+1}^{c(v+1)} \ldots x_{u-v+1}^{c(u-v+1)}.$$

If $P_3 \neq 1$, define $d(k - u + 1), \ldots, d(u + 1) \in \mathbf{Z}_p$ by

$$(4.4) \qquad [x_1, x_{k+1}] = x_{k-u+1}^{d(k-u+1)} \ldots x_{u+1}^{d(u+1)}.$$

By Proposition 3.6, these exponents exist.

Let us recall some notation from [**5**]. A series

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

in a group S is a *normal series* if $S_i \trianglelefteq S_{i-1}$, for $i = 1, 2, \ldots, n$. A subgroup K of Aut S *stabilizes* this series if it fixes $S_1, S_2, \ldots, S_n$ and fixes every coset of S_i in S_{i-1}, for $i = 1, 2, \ldots, n$.

LEMMA 4.1 (Maschke [**5**, p. 69]). *Suppose that S is an elementary Abelian p-group, that K is a p'-group of automorphisms of S, and that S_1 is a subgroup of S fixed by K. Then there exists a subgroup S_2 of S fixed by K such that $S = S_1 \times S_2$.*

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

LEMMA 4.2 ([**5**, pp. 178–179]). *Suppose that S is a p-group and that K is a group of automorphisms of S that stabilizes a normal series of S. Then K is a p-group.*

LEMMA 4.3. *Suppose that $Q_2 \subset Q_1 \subseteq Q$ and that $Q_1, Q_2 \trianglelefteq H$. Assume that $H/C_H(Q_1/Q_2)$ is a p-group. Then $H = C_H(Q_1/Q_2)P^g$.*

Proof. Clearly, $C_H(Q)O^p(H) \subseteq C_H(Q_1/Q_2)$. Apply (4.2).

LEMMA 4.4. *The group $H/C_H(Z(Q))$ is not a p-group.*

Proof. Suppose that this is false. By Lemma 4.3,

$$H = C_H(Z(Q))P^g \subseteq C_H(x_{u+1}),$$

contrary to $[x_1, x_{u+1}] \neq 1$.

PROPOSITION 4.5. *We have $c(v + 1) \neq 0$ and $c(u - v + 1) \neq 0$.*

Proof. Suppose that $c(u - v + 1) = 0$. Let $N_1 = Z(P) = \langle x_{v+1}, \ldots, x_u \rangle$ and let $N_2 = \langle x_{v+2}, \ldots, x_u \rangle$. Then $N_2 \subseteq Z(P) \cap Z(P^g) \subseteq Z(H)$. Since

$$\begin{aligned}[x_{v+1}, x_{t+1}] &= [x_1, x_{u+1}]^{g^v} \\ &= \phi^v({x_{v+1}}^{c(v+1)} \ldots {x_{u-v+1}}^{c(u-v+1)}) \\ &= {x_{2v+1}}^{c(v+1)} \ldots {x_u}^{c(u-v)} \in N_2,\end{aligned}$$

x_{t+1} centralizes N_1/N_2. So $N_1 \trianglelefteq H$ and $N_1/N_2 \subseteq Z(H/N_2)$. Moreover, $Z(Q) \trianglelefteq H$ and $Z(Q) = \langle N_1, x_{u+1} \rangle$, by Lemma 3.5. As $[x_1, x_{u+1}] \in N_1$ and $[x_{u+1}, x_{t+1}] = 1$, we have $Z(Q)/N_1 \subseteq Z(H/N_1)$. Let us regard $H/C_H(Z(Q))$ as a group of automorphisms of $Z(Q)$. Then it stabilizes the normal series

$$Z(Q) \supset N_1 \supset N_2 \supseteq 1$$

of $Z(Q)$. By Lemma 4.2, $H/C_H(Z(Q))$ is a p-group, contrary to Lemma 4.4. Hence, $c(u - v + 1) \neq 0$.

If $c(v + 1) = 0$, a symmetric argument (by Lemma 3.3) yields again that $H/C_H(Z(Q))$ is a p-group, contrary to Lemma 4.4.

Notation. Let $z_1 = [x_1, x_{u+1}]$. For $i = 2, \ldots, v + 1$, let $z_i = [x_i, x_{u+i}] = \phi^{i-1}(z_1)$. Let $Z = \langle z_1, \ldots, z_v \rangle$ and let $V = \langle z_1, z_{v+1} \rangle$.

LEMMA 4.6. *We have $Z(Q) = \langle Z(P), z_{v+1} \rangle$ and*

$$\langle Z, z_{v+1} \rangle \cap Z(P) = Z.$$

Proof. For $i = 1, \ldots, v$,

$$z_i = \phi^{i-1}(z_1) = {x_{v+i}}^{c(v+1)} \ldots {x_{u-v+i}}^{c(u-v+1)} \in \langle x_{v+1}, \ldots, x_u \rangle \subseteq Z(P),$$

by (4.3). Since $c(u - v + 1) \neq 0$, we obtain $z_{v+1} \notin Z(P)$ and $\langle Z(P), z_{v+1} \rangle = \langle Z(P), x_{u+1} \rangle = Z(Q)$, by a similar argument.

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

PROPOSITION 4.7. *We have $Z(Q) = V \times (Q \cap Z(H))$ and $V \trianglelefteq H$. Moreover, consider V to be a vector space over $\mathbf{Z}_p$; then the elements of H determine by conjugation the elements of* $\mathrm{SL}(V)$. *Thus, $H/C_H(V) \cong \mathrm{SL}(2, p)$.*

Proof. By parts (a) and (b) of Lemma 3.5, $Q \cap Z(H) = \langle x_{v+2}, \ldots, x_u \rangle$. Since $c(v + 1) \neq 0$ and $c(u - v + 1) \neq 0$, we obtain

$$Z(Q) = V(Q \cap Z(H)) \text{ and } V \cap (Q \cap Z(H)) = 1.$$

Thus, $Z(Q) = V \times (Q \cap Z(H))$.

Let $S = \langle Z(Q), x_1 \rangle = \langle Z(P), x_1, x_{u+1} \rangle$. Since $[x_1, x_{u+1}] \in Z(P)$, the group $S/Z(P)$ must be Abelian. So $S' \subseteq Z(P) \subseteq Z(S)$. By Lemma 2.5,

$$\begin{aligned}(z_{v+1})^{-1}(z_{v+1})^{x_1} &= [z_{v+1}, x_1] \\ &= [x_{2v+1}{}^{c(v+1)} \ldots x_{u+1}{}^{c(u-v+1)}, x_1] \\ &= [x_{u+1}{}^{c(u-v+1)}, x_1] \\ &= [x_{u+1}, x_1]^{c(u-v+1)} \\ &= z_1{}^{-c(u-v+1)}.\end{aligned}$$

So $(z_{v+1})^{x_1} = z_1{}^{-c(u-v+1)} z_{v+1}$. A similar argument shows that $z_1{}^{x_{t+1}} = z_1 z_{v+1}{}^{c(v+1)}$. Let us consider z_1 and z_{v+1} to form a basis of V as a vector space. Since $[x_1, z_1] = [x_{t+1}, z_{v+1}] = 1$ and since $V \subseteq Z(Q)$, we find that $V \trianglelefteq H$ and that

(4.5) *the automorphisms of V induced by conjugation by x_1 and x_{t+1} are represented by the matrices*

$$\begin{bmatrix} 1 & 0 \\ -c(u - v + 1) & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & c(v + 1) \\ 0 & 1 \end{bmatrix}, \text{ respectively.}$$

It is well known [**9**, pp. 115–118] that these matrices generate $\mathrm{SL}(2, p)$, since $c(u - v + 1)$ and $c(v + 1)$ are nonzero, by Proposition 4.5. As

$$H = Q\langle x_1, x_{t+1} \rangle = C_H(V)\langle x_1, x_{t+1} \rangle,$$

this completes the proof of the proposition.

Remark 4.8. In [**3**], J. Currano has obtained the conclusion of Proposition 4.7 by assuming (3.1), (4.1), and a weaker condition than (4.2).

LEMMA 4.9. *Let $N = \langle x_{t+2-k}, \ldots, x_k \rangle$. Then $[H, N] \subseteq Z(Q)$ and $[O^p(H), N] \subseteq V$.*

Proof. Since $u + 1 \leqq k \leqq t$, $Z(Q) \subseteq N \subseteq Q$. By the definition of k, we have $[P, N] \subseteq Z(P) \subseteq Z(Q)$. Similarly, $[P^g, N] \subseteq Z(Q)$. Hence,

$$N/Z(Q) \subseteq Z(H/Z(Q)),$$

which yields $[H, N] \subseteq Z(Q)$. By this calculation and by Proposition 4.7, the automorphisms of N/V induced by conjugation by elements of H stabilize the normal series

$$N/V \supseteq Z(Q)/V \supseteq V/V = 1$$

of N/V. By Lemma 4.2, $H/C_H(N/V)$ is a p-group. Hence, $O^p(H) \subseteq C_H(N/V)$.

We will say that a series of the form

$$1 = Q_0 \subset Q_1 \subset \ldots Q_n = Q \tag{4.6}$$

is an *H-composition series* of Q if $Q_i \trianglelefteq H$, for each i, and there is no normal subgroup S of H such that $Q_{i-1} \subset S \subset Q_i$ for some i, $1 \leqq i \leqq n$. We note that the Jordan-Hölder theorem applies to H-composition series [**6**, Theorem 8.4.3, p. 126].

PROPOSITION 4.10. *Assume that $P_3 = 1$. Suppose that* (4.6) *is an H-composition series of Q. Then precisely one of the factors Q_i/Q_{i-1} $(1 \leqq i \leqq n)$ has order p^2, and all of the other factors Q_i/Q_{i-1} have order p and are centralized by H.*

Proof. By the Jordan-Hölder Theorem, it is sufficient to find one H-composition series of Q that satisfies the conclusion of the lemma. Let $Q_1 = V$. By Proposition 4.7, V is a minimal normal subgroup of H and $Z(Q)/V$ is centralized by H. Since $P_3 = 1$, we have $k = t$. By Lemma 4.9, H centralizes $Q/Z(Q)$.

Consider the series

$$1 = Q_0 \subset Q_1 \subseteq Z(Q) \subseteq Q.$$

After deleting repeated terms, if any, we may refine this series to an H-composition series of Q that has the desired properties.

LEMMA 4.11. *For* $i = 1, \ldots, k - u$,

$$[P, \langle x_{u+i}\rangle] \subseteq \langle z_1, \ldots, z_i\rangle.$$

Proof. Use induction on i. Suppose that $1 \leqq r \leqq k - u$ and that the result is true whenever $1 \leqq i < r$. Let $M = \langle z_1, \ldots, z_r\rangle$ and $N = \langle M, z_{v+1}\rangle$. Then $M \subseteq Z(P)$ and $V \subseteq N \subseteq VZ(H)$. So $N \trianglelefteq H$.

We first show that $x_{u+r}N$ is in the centre of H/N; that is, that

$$[H, \langle x_{u+r}\rangle] \subseteq N. \tag{4.7}$$

By (4.2), $H = C_H(Q)O^p(H)P^g$. Certainly, $C_H(Q)$ centralizes the coset $x_{u+r}N$. By Lemma 4.9, $O^p(H)$ centralizes $x_{u+r}N$. Thus we must show that $[x_i, x_{u+r}] \in N$, for $i = 2, \ldots, t + 1$. For this, we may assume that $r \geqq 2$. Now,

$$\begin{aligned}[x_i, x_{u+r}] &= \phi([x_{i-1}, x_{u+r-1}]) \in \phi([P, \langle x_{u+r-1}\rangle]) \\ &\subseteq \phi(\langle z_1, \ldots, z_{r-1}\rangle) = \langle z_2, \ldots, z_r\rangle \subseteq M \subseteq N,\end{aligned}$$

by induction. This proves (4.7).

Since $u + r \leqq k$, we obtain $[P, \langle x_{u+r}\rangle] \subseteq N \cap Z(P) = M$, by (4.7) and Lemma 4.6.

LEMMA 4.12. *Suppose that* $1 \leqq i \leqq k - u$. *Then*

$$[P, \langle x_{t+i-k}\rangle] \subseteq \langle z_{t+i-k}, \ldots, z_v\rangle.$$

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

Proof. Let $Y = \langle z_{t+i-k}, \ldots , z_v\rangle$. Then $Y \subseteq Z(P)$. We must show that $[x_{t+i-k}, x_j] \in Y$, for $j = 1, 2, \ldots , t$. Now, $1 \leqq t + i - k \leqq v < u$. If $j \leqq u$, then $[x_{t+i-k}, x_j] = 1$. Assume that $j \geqq u + 1$. Let $r = j - (t + i - k - 1)$. Then

$$j > v \geqq t + i - k \quad \text{and} \quad 1 \leqq r \leqq t - (t + i - k - 1) \leqq k - i + 1 \leqq k.$$

Hence, by Lemma 4.11,

$$\begin{aligned}[x_{t+i-k}, x_j] &= \phi^{t+i-k-1}([x_1, x_r]) \in \phi^{t+i-k-1}(\langle z_1, \ldots , z_{r-u}\rangle) \\ &= \langle z_{t+i-k}, \ldots , z_{j-u}\rangle \subseteq Y,\end{aligned}$$

as desired.

PROPOSITION 4.13. *Let* $Z^* = \langle Z, z_{v+1}\rangle = \langle z_1, \ldots , z_{v+1}\rangle$ *and let*

$$N = \langle x_{t+2-k}, \ldots , x_k\rangle.$$

Then:

(a) $Z^* \trianglelefteq H$;

(b) $N \trianglelefteq H$ *and* $[H, N] \subseteq Z^*$;

(c) *if* $P_3 = 1$, *then* $P' = Z$ *and* $[Q, H] = Z^*$; *and*

(d) *if* $P_3 \neq 1$, *then* $P_3 \subseteq Z \subseteq P'$.

Proof. Since $V \subseteq Z^* \subseteq Z(Q) \subseteq VZ(H)$, we obtain (a). Let

$$L = \langle x_{t+1-k}, N\rangle.$$

By Lemmas 4.11 and 4.12, we have

$$[P, N] \subseteq [P, L] \subseteq Z. \tag{4.8}$$

Hence, $[P^g, N] \subseteq [P^g, L^g] \subseteq Z^g \subseteq Z^* \subseteq N$. This yields (b).

Since $z_i = [x_i, x_{u+i}] \in P'$, for $i = 1, \ldots , v$, we have $Z \subseteq P'$.

Suppose that $P_3 = 1$. Then $k = t$ and $N = Q$. By Lemmas 4.11 and 4.12, $P' \subseteq Z$, so $P' = Z$. By (b), $[Q, H] \subseteq Z^*$. Thus,

$$Z^* = \langle Z, [x_{v+1}, x_{t+1}]\rangle \subseteq [Q, H] \subseteq Z^*,$$

which proves (c).

Finally, assume that $P_3 \neq 1$. By Theorem 3.7, $P' \subseteq L$. Hence, by (4.8), $P_3 \subseteq [L, P] \subseteq Z$. This yields (d) and completes the proof of Proposition 4.13.

PROPOSITION 4.14. *Assume that* $P_3 \neq 1$. *Take* m *and* n *as in Proposition* 3.6 *and* Z^* *and* N *as in Proposition* 4.13. *Let*

$$M = \langle x_{t+1-k}, \ldots , x_{k+1}\rangle = \langle N, x_{t+1-k}, x_{k+1}\rangle.$$

Then:

(a) $[Q, H] \subseteq M$, $[Q, M] \subseteq N$, *and* $M \trianglelefteq H$;

(b) *if* $M/N \subseteq Z(H/N)$, *then* $m \geqq v + 1$;

(c) *if* $M/N \not\subseteq Z(H/N)$, *then* $k = u + \frac{1}{2}v$; *and*

(d) $n = u + 1$.

Proof. (a) By Theorem 3.7, $P' \subseteq \langle x_{t+1-k}, \dots, x_k\rangle \subseteq M$. Hence, $M \trianglelefteq P$. Similarly,

$$(P^g)' = \phi(P') \subseteq \langle x_{t+2-k}, \dots, x_{k+1}\rangle \subseteq M,$$

and $M \trianglelefteq P^g$. So $M \trianglelefteq H$. Moreover, $[Q, H] \subseteq M$ because

$$Q/M \subseteq Z(P/M) \cap Z(P^g/M) \subseteq Z(H/M).$$

By the definition of k, we have $[Q, M] \subseteq Z(P) \subseteq N$.

(b) Assume that $M/N \subseteq Z(H/N)$. By Proposition 4.13 (b), the elements of H determine by conjugation a group of automorphisms of M/Z^* that stabilizes the normal series

$$M/Z^* \supset N/Z^* \supset Z^*/Z^* = 1.$$

By Lemmas 4.2 and 4.3, $H/C_H(M/Z^*)$ is a p-group, and

$$H = C_H(M/Z^*)P^g. \tag{4.9}$$

By the definition of k,

$$[x_i, x_{k+1}] = [x_{i-1}, x_k]^g \in Z(P)^g = Z(P^g) \subseteq Z(Q),$$

for $i = 2, \dots, t + 1$. Hence, $x_{k+1}Z(Q) \in Z(P^g/Z(Q))$. Since $Z^* \subseteq Z(Q)$, (4.9) yields that $[H, \langle x_{k+1}\rangle] \subseteq Z(Q)$. In particular,

$$x_m{}^{e(m)} \dots x_n{}^{e(n)} = [x_1, x_{k+1}] \in Z(Q) = \langle x_{v+1}, \dots, x_{u+1}\rangle.$$

Since $k < t$, $k - u + 1 < v + 1 \leqq m$. By Proposition 3.6 (c), $n = u + 1$. This proves (b) and proves (d) when $M/N \subseteq Z(H/N)$.

(c) Assume that $M/N \not\subseteq Z(H/N)$. Let $C = C_H(M/N)$. By (a), $C \supseteq Q$. Suppose that $C \supseteq P^g$. Then $H = \langle P, P^g\rangle = PC$. Therefore, H/C is a p-group. By Lemma 4.3, $H = CP^g = C$, contrary to assumption. Thus, $C \not\supseteq P^g$. Since $C \supseteq Q$, we must have $x_{t+1} \notin C$. As $[x_{k+1}, x_{t+1}] = 1$, we obtain $[x_{t+1-k}, x_{t+1}] \not\equiv 1$, modulo N. Now,

$$\begin{aligned}[x_{t+1-k}, x_{t+1}] &= \phi^{t-k}([x_1, x_{k+1}]) \\ &= \phi^{t-k}(x_m{}^{e(m)} \dots x_n{}^{e(n)}) \\ &= x_{m+t-k}{}^{e(m)} \dots x_{n+t-k}{}^{e(n)}.\end{aligned}$$

Since

$$[x_{t+1-k}, x_{t+1}] \in \langle x_{t+2-k}, \dots, x_t\rangle \cap M = \langle N, x_{k+1}\rangle,$$

we obtain

$$n + t - k = k + 1. \tag{4.10}$$

Thus, $n = 2k - t + 1 > k + u - t + 1 = k - v + 1$. By Proposition 3.6 (e), $n = u + 1$. By (4.10), $2k = t + u = 2(u + \frac{1}{2}v)$. This proves (c) and completes the proof of (d) and of the proposition.

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

We now consider some consequences of assuming the following statement, symmetric to (4.2):

$$H = C_H(Q)O^p(H)P. \tag{4.11}$$

We continue to assume (3.1), (4.1), and (4.2). Recall that, if $P_3 \neq 1$, certain exponents $d(i)$ are defined by (4.4).

PROPOSITION 4.15. *Assume* (4.11). *Suppose that* $P_3 \neq 1$. *Then:*

(a) *v is even, $m = 1 + \frac{1}{2}v$, and $k = u + \frac{1}{2}v$,*

(b) *both $d(k - u + 1)$ and $d(u + 1)$ are nonzero, and*

(c) *$P_3 = Z$.*

Proof. Take m and n as in Propositions 3.6 (and 4.14). By Proposition 4.14 (d), $n = u + 1$. Since (4.11) is symmetric to (4.2), Proposition 4.14 (d) yields the symmetric result that $m = k - u + 1$ (see Lemma 3.3 and Proposition 3.6). Hence, $m < t - u + 1 = v + 1$. By Proposition 4.14, $k = u + \frac{1}{2}v$. Thus, we obtain (a) and (b).

By Proposition 4.13, $P_3 \subseteq Z$. Now, $z_1 \in Z$. Let $d = d(u + 1)$. Then $d \neq 0$. By Lemma 2.5,

$$\begin{aligned}[x_1, x_{k+1}, x_1] &= [x_m{}^{d(m)} \ldots x_{u+1}{}^{d(u+1)}, x_1] \\ &= [x_{u+1}{}^d, x_1] \\ &= [x_1, x_{u+1}]^{-d} \\ &= z_1{}^{-d} \neq 1.\end{aligned}$$

Therefore, $z_1 \in P_3$. For $i = 1, 2, \ldots, v/2$, we have $k + i \leqq t$ and

$$[x_i, x_{k+i}, x_i] = \phi^{i-1}([x_1, x_{k+1}, x_1]) = \phi^{i-1}(z_1{}^{-d}) = z_i{}^{-d};$$

thus, $z_i \in P_3$. Let $w = v/2$. For the same values of i, similar calculations yield that

$$z_{w+i}{}^{d(k-u+1)} = [x_i, x_{k+i}, x_{k+i}] \in P_3.$$

This proves (c).

PROPOSITION 4.16. *Assume* (4.11). *Suppose that* $P_3 \neq 1$. *Let* $w = v/2$. *Define*

$$M = \langle x_{w+1}, \ldots, x_{u+w+1} \rangle \quad \text{and} \quad N = \langle x_{w+2}, \ldots, x_{u+w} \rangle.$$

Then:

(a) *$[Q, H] \subseteq M$ and $[Q, M] \subseteq N$;*

(b) *$M, N \trianglelefteq H$ and $H/C_H(M/N) \cong \mathrm{SL}(2, p)$; and*

(c) *for any H-composition series*

$$1 = Q_0 \subset Q_1 \subset \ldots \subset Q_n = Q$$

of Q, precisely two of the factors Q_i/Q_{i-1} $(1 \leqq i \leqq n)$ have order p^2, while all the other factors Q_i/Q_{i-1} have order p and are centralized by H.

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

Proof. Since $w = k - u$, M and N have the same definitions as in Propositions 4.13 and 4.14. This proves (a) and yields that $M, N \trianglelefteq H$.

By Proposition 4.15, $d(w + 1)$ and $d(u + 1)$ are both nonzero. We may complete the proof of Proposition 4.16 by arguing as in Propositions 4.7 and 4.10 and using (4.4) instead of (4.3).

Remark 4.17. Suppose that $p = 2$ or $p = 3$. Then $\mathrm{SL}(2, p)$ has a normal p-complement. Using Proposition 4.7, we can obtain (4.11) from (3.1), (4.1), and (4.2). If $p = 2$, then $\langle x_1, x_{t+1}\rangle$ is a dihedral group, and (4.2) yields a stronger result: $PC_H(Q)/C_H(Q)$ and $P^gC_H(Q)/C_H(Q)$ are Sylow p-subgroups of $H/C_H(Q)$.

5. The conjugate case. Suppose that P satisfies (3.1). As in § 4, we may and will assume that P is contained in a group G possessing an element g for which $\phi(x) = x^g$ $(x \in R)$. In this section, we extend ϕ to an isomorphism of P into G by defining $\phi(x)$ to be x^g for *all* $x \in P$. Let $H = \langle P, \phi(P)\rangle$. We assume that

$$\text{(5.1)} \qquad P \textit{ is not Abelian, and}$$

$$\text{(5.2)} \qquad \phi(P) \textit{ is conjugate to } P \textit{ in } H.$$

We will determine the structure of P (Theorem 5.10), and other information (Corollary 5.14) that will be applied in the proof of Theorem 2.

Let $w = v$ if $P_3 = 1$ and $w = v/2$ if $P_3 \neq 1$. Since ϕ has been extended, there is no further need for the element g given above; we will therefore use the letter "g" to denote an arbitrary element of H.

Throughout this section we assume (3.1), (5.1), *and* (5.2), *and use the letters "g" and "w" as in the previous paragraph.*

LEMMA 5.1. *We have*

$$\text{(5.3)} \qquad H = O^p(H)P = O^p(H)\phi(P),$$

and, for some $h' \in O^p(H)$, $P^{h'} = \phi(P)$. Moreover,

$$\text{(5.4)} \qquad P \cap \phi(P) = Q.$$

Proof. Clearly, $O^p(H)$ is a normal subgroup of H and $H/O^p(H)$ is a p-group. Suppose that $PO^p(H) \neq H$. Then $PO^p(H)$ is contained in a maximal subgroup H^* of H. Since $H/O^p(H)$ is a p-group, $H^*/O^p(H)$ is a normal subgroup of $H/O^p(H)$. Hence, $H^* \triangleleft H$. By (5.2),

$$H = \langle P, \phi(P)\rangle \subseteq H^* \subset H,$$

which is a contradiction. Thus, $H = PO^p(H)$. Similarly, $H = O^p(H)\phi(P)$.

Take $g \in H$ such that $P^g = \phi(P)$. Take $k' \in P$ and $h' \in O^p(H)$ such that $k'h' = g$. Then $P^{h'} = P^g = \phi(P)$.

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

Obviously, $Q \subseteq P \cap \phi(P) \subseteq P$. Suppose that $P \cap \phi(P) \neq Q$. Then $P \cap \phi(P) = P$. Since P is finite, $\phi(P) = P$. Therefore, $\phi(P') = P'$. By (3.1), $P' = 1$, contrary to (5.1). Thus, $P \cap \phi(P) = Q$.

By Lemma 5.1, H satisfies (4.2) and (4.11) (for some $g \in G$). *Therefore, all the results of* § 4 *are valid in this section. In particular, if* $P_3 \neq 1$ *then* v *is even and* $k = u + w$.

Because of (5.4), we will use Lemma 2.4 to discuss various isomorphisms ψ of P onto $\phi(P)$.

Take $h \in H$ such that $P^h = \phi(P)$. Define $\alpha : P \rightarrow P$ by

$$x^\alpha = (\phi(x))^{h^{-1}}, \tag{5.5}$$

for all $x \in P$. Then α is an automorphism of P and $\phi(x) = (x^\alpha)^h$, for all $x \in P$.

Henceforth, we will assume that h and α *are fixed elements of H and* Aut P *that satisfy* (5.5).

Lemma 5.2. *For* $i = 1, 2, \ldots, v - 1$, $z_i^\alpha = z_{i+1}$ *and* $z_{i+1} \in Z(H)$; *also*, $\langle z_v \rangle^\alpha = \langle z_1 \rangle$. *Therefore, v divides the order of* α.

Proof. Let $g = h^{-1}$. By Lemma 4.6, $Z = \langle z_1, \ldots, z_v \rangle \subseteq Z(P)$. Therefore,

$$\langle z_2, \ldots, z_v \rangle \subseteq Z(P) \cap \phi(Z(P)) = Z(P) \cap Z(\phi(P)) \subseteq Z(H).$$

For $i = 1, 2, \ldots, v - 1$, $z_i^\alpha = (\phi(z_i))^g = (z_{i+1})^g = z_{i+1}$.

By Lemma 4.6 and Proposition 4.7, $V = \langle z_1, z_{v+1} \rangle \lhd H$ and $V \cap Z(P) = \langle z_1 \rangle$. Since $z_v \in Z(P)$,

$$z_v^\alpha = (\phi(z_v))^g = (z_{v+1})^g \in V \cap Z(P) = \langle z_1 \rangle.$$

Hence, $\langle z_v \rangle^\alpha = \langle z_1 \rangle$. Since α permutes the subgroups $\langle z_1 \rangle, \ldots, \langle z_v \rangle$ cyclically, v divides the order of α.

Lemma 5.3. *Let* $z = z_{v+1}$ *and* $c = c(u - v + 1)$. *For* $i = 0, 1, \ldots, w$, *there exist* $y_i \in \langle x_{v+1}, \ldots, x_{u+i} \rangle$ *such that*

$$z^{\alpha^i} = y_i (x_{u+i+1})^c \quad (0 \leqq i \leqq w - 1), \tag{5.6}$$

and

$$(z^{\alpha^w})^h = y_w (x_{u+w+1})^c. \tag{5.7}$$

Furthermore, suppose that $P_3 \neq 1$. *Let* $z^* = (z^{\alpha^w})^h$. *For* $i = 0, 1, \ldots, w$, *there exist* $y_i^* \in \langle x_{w+1}, \ldots, x_{u+w+i} \rangle$ *such that*

$$(z^*)^{\alpha^i} = y_i^* (x_{u+w+i+1})^c \quad (0 \leqq i \leqq w - 1), \tag{5.8}$$

and

$$((z^*)^{\alpha^w})^h = y_w^* (x_{t+1})^c. \tag{5.9}$$

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

Proof. We prove (5.6) by induction on i. It is clear for $i = 0$ (e.g., see the proof of Lemma 4.6). Suppose that $0 \leqq i \leqq w - 2$ and that (5.6) holds for i. Let $g = h^{-1}$. Then

$$z^{\alpha^{i+1}} = (\phi(z^{\alpha^i}))^g = (\phi(y_i x_{u+i+1}{}^c))^g = \phi(y_i)^g (x_{u+i+2}{}^c)^g.$$

By Proposition 4.13,

$$[\langle x_{v+1}, \ldots, x_{u+w}\rangle, H] \subseteq \langle z_1, \ldots, z_{v+1}\rangle \subseteq Z(Q) = \langle x_{v+1}, \ldots, x_{u+1}\rangle.$$

Since $u + i + 2 \leqq u + w$,

$$\phi(y_i)^g (x_{u+i+2}{}^c)^g \equiv \phi(y_i) x_{u+i+2}{}^c, \quad \text{modulo } Z(Q).$$

Since $\phi(y_i) \in \langle x_{v+2}, \ldots, x_{u+i+1}\rangle$, we obtain (5.6) for $i + 1$. This completes the proof of (5.6).

Now let $i = w - 1$. Then

$$(z^{\alpha^w})^h = ((z^{\alpha^i})^\alpha)^h = \phi(z^{\alpha^i}) = \phi(y_i x_{u+w}{}^c) = \phi(y_i) x_{u+w+1}{}^c,$$

which yields (5.7).

Suppose that $P_3 \neq 1$. Then $[Q, H] \subseteq \langle x_{w+1}, \ldots, x_{u+w+1}\rangle$, by Proposition 4.16. We obtain (5.8) and (5.9) by the arguments used to prove (5.6) and (5.7).

For our next results, recall the definition and properties of $N(\psi)$ for an isomorphism ψ (Lemma 2.4).

LEMMA 5.4. *Define an isomorphism ψ of P onto P^h by*

$$\psi(x) = (x^{\alpha^w})^h, \quad x \in P.$$

Let $Q^* = N(\psi)$. Then:

(a) *$Q^* \trianglelefteq H$ and α^w fixes Q^*;*

(b) *if $P_3 = 1$, then $Q^* \cap Z = \langle z_2, \ldots, z_v\rangle$; and*

(c) *if $P_3 \neq 1$, then $Q^* \cap Z = \langle z_2, \ldots, z_w; z_{w+2}, \ldots, z_v\rangle$.*

Proof. (a) By Lemma 2.4, $Q^* \trianglelefteq H$. Hence, $Q^* \subseteq P \cap P^h = Q$ and

$$Q^{*\alpha^w} = (\psi(Q^*))^{h^{-1}} = Q^{*h^{-1}} = Q^*.$$

(b) Suppose that $P_3 = 1$. By Lemma 5.2, each subgroup $\langle z_i\rangle$, $2 \leqq i \leqq v$, is fixed by α^v. Moreover, each such subgroup is contained in the centre of H. Therefore,

$$Q^* \cap Z \supseteq \langle z_2, \ldots, z_v\rangle.$$

Suppose that $Q^* \cap Z \supset \langle z_2, \ldots, z_v\rangle$. Then $Q^* \supseteq Z$. By Proposition 4.7, V is a minimal normal subgroup of H. Since $z_1 \in Q^* \cap V$, $V \subseteq Q^*$. So $z_{v+1} \in Q^*$. Therefore, $\psi(z_{v+1}) = (z_{v+1}{}^{\alpha^v})^h \in Q^*$, contrary to Lemma 5.3.

(c) Suppose that $P_3 \neq 1$. Let $Y = \langle z_2, \ldots, z_w;\ z_{w+2}, \ldots, z_v\rangle$. Using Lemma 5.2 as in (b), we obtain $Y \subseteq Q^* \cap Z$. Suppose that $Y \subset Q^* \cap Z$. Then there exists $x \in Q^* \cap Z$ and $i, j \in \mathbf{Z}_p$ such that $x = z_1{}^i z_{w+1}{}^j \neq 1$.

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

Since α^w fixes Q^* and interchanges $\langle z_1\rangle$ and $\langle z_{w+1}\rangle$, we may assume that $i \neq 0$. Then $x \notin Z(H)$ and, since $z_{w+1} \in Z(H)$,

$$1 \neq [\langle x\rangle, H] = [\langle z_1\rangle, H] \subseteq V.$$

Since $Q^* \trianglelefteq H$ and V is a minimal normal subgroup of H, $V \subseteq Q^*$. Hence, $\psi^2(z_{v+1}) \in Q^*$. Take z^* as in Lemma 5.3; then

$$\psi^2(z_{v+1}) = \psi((z_{v+1}{}^{\alpha^w})^h) = (z^{*\alpha^w})^h \notin Q^*,$$

which is a contradiction.

Lemma 5.5. *Define ψ and Q^* as in Lemma 5.4, and let $\bar{P} = P/Q^*$ and $\bar{H} = H/Q^*$. Let $\bar{P}_2 = \bar{P}'$ and $\bar{P}_3 = [\bar{P}_2, \bar{P}]$. Denote the coset hQ^* by $\bar{h}$. Define a mapping $\bar{\psi}$ of $\bar{P}$ into $\bar{H}$ by $\bar{\psi}(xQ^*) = \psi(x)Q^*$, for all $x \in P$. Then:*

(a) *$\bar{\psi}$ is an isomorphism of $\bar{P}$ onto $\bar{P}^{\bar{h}}$;*

(b) *$[\bar{P}: \bar{P} \cap \bar{P}^{\bar{h}}] = p$ and $N(\bar{\psi}) = 1$;*

(c) *if $P_3 = 1$, then $|\bar{P}_2| = p$ and $\bar{P}_3 = 1$; and*

(d) *if $P_3 \neq 1$, then $|\bar{P}_3| = p^2$.*

Proof. Since ψ is an isomorphism that fixes Q^*, $\bar{\psi}$ is well defined and satisfies (a). Likewise, (b) is easy. Clearly, $\bar{P}_i = P_iQ^*/Q^*$, for $i = 2, 3$. If $P_3 = 1$, then $\bar{P}_3 = 1$ and

$$|\bar{P}_2| = |P_2Q^*/Q^*| = |ZQ^*/Q^*| = |Z/(Z \cap Q^*)| = p,$$

by Proposition 4.13 (c) and Lemma 5.4 (b). This yields (c), and (d) follows similarly from Proposition 4.15 (c) and Lemma 5.4 (c).

Note that, by Lemma 5.5, $\bar{\psi}$ is an isomorphism of $\bar{P}$ into $\bar{H}$ that satisfies the assumptions of this section, i.e., (3.1), (5.1), and (5.2).

Lemma 5.6. *Define ψ and Q^* as in Lemma 5.4. Then $O^p(H)$ centralizes Q^*.*

Proof. Suppose that $P_3 = 1$. Let

$$1 = Q_0 \subset \ldots \subset Q_m = Q^* \subset \ldots \subset Q_n = Q$$

be an H-composition series of Q that contains Q^*; here, m may be zero. By Proposition 4.10, precisely one of the factors Q_i/Q_{i-1} has order p^2, while all the other factors have order p and are centralized by H. Because of Lemma 5.5, a similar statement is valid for the series

$$1 = Q^*/Q^* = Q_m/Q^* \subset \ldots \subset Q_n/Q^* = Q/Q^*.$$

Therefore, the factors Q_i/Q_{i-1}, $1 \leqq i \leqq m$, must have order p and must be centralized by H. By Lemma 4.2, $H/C_H(Q^*)$ is a p-group. Therefore, $O^p(H)$ centralizes Q^*.

The proof for the case in which $P_3 \neq 1$ is similar, but requires Proposition 4.16 (c) instead of Proposition 4.10.

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

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 relations:*

$$a^p = b^p = c^p = d^p = e^p = f^p = 1; \tag{5.10}$$

$$ab = ba, ac = ca, bc = cb; \tag{5.11}$$

$$ad = da, bd = db, d^{-1}cd = cb; \tag{5.12}$$

$$ae = ea, be = eb, ce = ec, e^{-1}de = db; \tag{5.13}$$

$$af = fa, bf = fb, f^{-1}cf = ca, f^{-1}df = dc^{-1}, ef = fe. \tag{5.14}$$

Moreover S is unique up to isomorphism and satisfies

$$Z(S) = [S, S, S] = \langle a, b\rangle. \tag{5.15}$$

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 (5.11) and (5.12). Also, there exist $e, f \in \operatorname{Aut} D$ for which

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

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 (5.10)–(5.14), and easy computations yield (5.15).

Now suppose that S^* is an arbitrary group generated by elements satisfying (5.10)–(5.14). Let $D^* = \langle a, b, c, d\rangle$. Then $D^* \trianglelefteq S^*$ 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 5.8. Suppose that p is an odd prime. Let $E^*(p)$ be the group defined in Lemma 5.7.

Note that, by (5.15), $E^*(p)$ is not isomorphic to the group of Example 3.9. We return to the isomorphism ϕ.

LEMMA 5.9. (a) *Suppose that $P_3 = 1$ and that $v = 1$. Then P is isomorphic to the direct product of $E(p)$ and an elementary group.*

(b) *Suppose that $P_3 \neq 1$ and that $v = 2$. Then p is odd and P is isomorphic to the direct product of $E^*(p)$ and an elementary group.*

Proof. (a) In this case, $|P| = p^{u+1}$ and $Z(P) = \langle x_2, \ldots, x_u\rangle$. By Proposition 4.13, $P' = Z = \langle z_1\rangle \subseteq Z(P)$. Let $S = \langle x_1, x_{u+1}\rangle$ and let Y be a complement of Z in $Z(P)$. Since $x_1{}^p = x_{u+1}{}^p = 1$, we have

$$S \cong E(p), S \cap Y = 1,$$

and

$$P = \langle x_1, Z(P), x_{u+1}\rangle = \langle S, Y\rangle = S \times Y.$$

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

(b) Here, $|P| = p^{u+2}$ and $Z(P) = \langle x_3, \ldots, x_u \rangle$. By Theorem 3.7, p is odd. Let

$$c = [x_1, x_{u+2}], \quad a = [c, x_1], \quad b = [c, x_{u+2}], \quad d = x_{u+2},$$
$$e = x_2^{-d(2)}, \quad f = x_1, \quad \text{and} \quad S = \langle a, b, c, d, e, f \rangle.$$

A few calculations suffice to verify (5.10) through (5.14) and to show that $S = \langle x_1, x_2, x_{u+2} \rangle$ and that $|S| = p^6$. Let Y be a complement to $Z = \langle z_1, z_2 \rangle$ in $Z(P)$. By Lemma 5.7 and Proposition 4.15,

$$S \cong E^*(p) \quad \text{and} \quad Z(S) = \langle a, b \rangle \subseteq P_3 = Z.$$

Thus, $Z(S) = Z$ and $S \cap Y = 1$. Since $c \in S$ and $d(u + 1) \neq 0$,

$$P = \langle x_1, \ldots, x_{u+2} \rangle = \langle S, x_3, \ldots, x_u \rangle = SZ(P) = S \times Y.$$

THEOREM 5.10. *If $P_3 = 1$, then P is a direct product of an elementary group of order p^{u-2v} with a direct product of v subgroups isomorphic to $E(p)$. If $P_3 \neq 1$, then p is odd, v is even, and P is a direct product of an elementary group of order p^{u-2v} with a direct product of $v/2$ subgroups isomorphic to $E^*(p)$.*

Proof. As before, let $w = v$ if $P_3 = 1$ and $w = v/2$ if $P_3 \neq 1$. Define Q^* as in Lemma 5.4. By Lemmas 5.5 and 5.9, P/Q^* is isomorphic to the direct product of $E(p)$ and an elementary group if $P_3 = 1$, and to the direct product of $E^*(p)$ and an elementary group if $P_3 \neq 1$; also, in the latter case p is odd and, by Proposition 4.15, v is even. Let $F_i = P/Q^{*\alpha^i}$, for $i = 0, 1, \ldots, w - 1$.

Let F be the direct product of the groups $F_0, F_1, \ldots, F_{w-1}$. Let

$$Q^{**} = \bigcap\nolimits_{0 \leqq i \leqq w-1} Q^{*\alpha^i}.$$

For each i, there is a natural map of P onto F_i; these maps yield a homomorphism θ of P into F. Clearly, Q^{**} is the kernel of θ.

By Lemma 5.4, α^w fixes Q^*. Therefore,

$$Q^{**\alpha} = \bigcap\nolimits_{1 \leqq i \leqq w} Q^{*\alpha^i} = Q^{*\alpha^w} \cap \left(\bigcap\nolimits_{1 \leqq i \leqq w-1} Q^{*\alpha^i}\right) = Q^{**}.$$

Since $Q^* \trianglelefteq P$, $Q^{*\alpha^i} \trianglelefteq P$, for each i. Hence, $Q^{**} \trianglelefteq P$. By Lemma 5.6, $O^p(H)$ centralizes Q^{**}. Since $H = O^p(H)P$, by Lemma 5.1, $Q^{**} \trianglelefteq H$ and

$$\phi(Q^{**}) = ((Q^{**})^\alpha)^h = (Q^{**})^h = Q^{**}.$$

Since ϕ fixes no non-identity subgroup of P, $Q^{**} = 1$. Consequently, θ is an isomorphism of P into F.

As α is an isomorphism, $F_i \cong F_0$, for $i = 1, 2, \ldots, w - 1$. Therefore, $F = F^* \times S$, where S is an elementary group and F^* is a direct product of v groups isomorphic to $E(p)$, or of w groups isomorphic to $E^*(p)$. For each i, the natural map of P onto F_i must map $Z(P)$ into $Z(F_i)$. Hence,

$$\theta(Z(P)) \subseteq Z(F) = Z(F^*) \times S. \tag{5.16}$$

Suppose that $P_3 = 1$. Then $|F^{*\prime}| = |E(p)'|^v = p^v = |P'|$. Since

$$\theta(P') \subseteq F' = F^{*\prime},$$

we have $\theta(P') = F^{*\prime} = Z(F^*)$. Thus,

$$Z(F^*) \subseteq \theta(Z(P)). \tag{5.17}$$

Suppose that $P_3 \neq 1$. By Lemma 5.7 and Proposition 4.15, we find similarly that $Z(F^*) = [F, F, F] = \theta(P_3)$. Thus, (5.17) is valid in this case as well.

Let $S_1 = \theta(Z(P)) \cap S$. By (5.16) and (5.17), $\theta(Z(P)) = Z(F^*) \times S_1$. Let S_2 be a complement of S_1 in S. Since $S_2 \subseteq Z(F)$,

$$\theta(P) \cap S_2 = \theta(Z(P)) \cap S_2 = 1.$$

Therefore, the mapping of P into F/S_2 given by $x \to \theta(x)S_2$ is an isomorphism into F/S_2. Since $|E(p)/Z(E(p))| = p^2$ and $|E^*(p)/Z(E^*(p))| = p^4$,

$$\begin{aligned} |F/S_2| &= |F/Z(F)||Z(F)/S_2| \\ &= |F^*/Z(F^*)||\theta(Z(P))| \\ &= p^{2v}|Z(P)| \\ &= p^{2v}p^{u-v} \\ &= p^t. \end{aligned}$$

Thus, $P \cong F/S_2 \cong F^* \times S_1$. This completes the proof of Theorem 5.10.

Remark 5.11. In [**3**, Theorems 2.3.2 and 2.4.1], J. Currano has proved Theorem 5.10 without assuming (5.2). He requires only the assumptions (3.1), (4.1), (4.2), and (4.11).

LEMMA 5.12. *Every automorphism of P that fixes Q also fixes $\langle z_1\rangle$.*

Proof. Since $Z(Q) = \langle x_{v+1}, \ldots, x_{u+1}\rangle$, we have $\langle z_1\rangle = [P, Z(Q)]$.

Recall that $R = \langle x_1, \ldots, x_{t-1}\rangle$ and that $Z(R) = \langle x_v, \ldots, x_u\rangle$.

LEMMA 5.13. *Suppose that $P_3 \neq 1$ and that $v = 2$. Then*
(a) *$Q' = \langle z_2\rangle$ and $R' = \langle z_1\rangle$, and*
(b) *every automorphism of P fixes or interchanges Q and R.*

Proof. Part (a) is obvious. Since $k = u + 1$,

$$(Q \cap R)/Z(P) = \langle x_2, \ldots, x_{u+1}\rangle/Z(P) = Z(P/Z(P)).$$

Thus, $Q \cap R$ is a characteristic subgroup of P.

Let S be an arbitrary subgroup of P that contains $Q \cap R$ as a subgroup of index p. If S is Q or R, then $|S'| = p$. Suppose that $S \neq R, Q$. Then there exist $y \in Q \cap R$ and $j \neq 0$ in $\mathbf{Z}_p$ such that $x_1 y x_{u+2}{}^j \in S$.

$$S' \supseteq [S, Q \cap R] \supseteq \langle z_1, z_2\rangle = Z.$$

Thus, $|S'| > p$. This yields (b).

COROLLARY 5.14. *Let n be the smallest positive integer for which α^n fixes Q. If $P_3 \neq 1$, then $n = v$. If $P_3 = 1$ and $p = 2$, then $n = 2v$. If $P_3 = 1$ and p is*

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

odd, then $n = qv$ for some $q > 1$, and q divides $p, p - 1$, or $p + 1$. Consequently, if α has odd order, then $P_3 = 1$ and p is odd.

Proof. We first reduce to the case in which $w = 1$. Assume that the result is true in this case, and consider the general case. By Lemmas 5.2 and 5.12, v divides n. So w divides n. Define Q^* as in Lemma 5.4. Let $n = n'w$; then n' is the smallest positive integer i for which $(\alpha^w)^i$ fixes Q (or, equivalently, fixes Q/Q^*). By Lemma 5.5 and our assumption, $n' = 2$ if $P_3 \neq 1$ or if $P_3 = 1$ and $p = 2$; while, otherwise, $n' > 1$ and n' divides $p, p - 1$, or $p + 1$. Hence, n satisfies the conclusion of the theorem.

Thus, we may assume that $w = 1$. Since $Q \trianglelefteq H$ and ϕ does not fix Q, α does not fix Q. So $n > 1$. Suppose first that $P_3 = 1$ and that p is odd. By Theorem 5.10, P is isomorphic to the direct product of $E(p)$ and an elementary group. Therefore, $|P/Z(P)| = p^2$. Now, $Z(P) \subset Z(Q) = Q$ and $|Q/Z(P)| = p$. We may consider $P/Z(P)$ to be a two-dimensional vector space over $\mathbf{Z}_p$. Thus, $\mathrm{Aut}(P/Z(P)) \cong \mathrm{GL}(2, p)$. Let $X = \mathrm{GL}(2, p)$. Then every element of $Z(X)$ fixes every one-dimensional subspace of the vector space. Therefore, n divides the order of an element of $X/Z(X)$. By considering eigenvalues, one sees that the order of every element of $X/Z(X)$ divides $p, p - 1$, or $p + 1$.

Suppose that $P_3 = 1$ and that $p = 2$. Since $P/Z(P)$ is an elementary group of order four, P has precisely three subgroups of index two that contain $Z(P)$. These are Q, R, and $\langle Z(P), x_1x_t\rangle$. Clearly, Q and R are elementary. However,

$$(x_1x_t)^2 = x_1x_tx_1x_t = x_1^{-1}x_t^{-1}x_1x_t = [x_1, x_t] = [x_1, x_{u+1}] \neq 1.$$

Hence, α fixes $\langle Z(P), x_1x_t\rangle$. Since α does not fix Q, α interchanges Q and R. Thus, $n = 2$.

Suppose $P_3 \neq 1$. Then $v = 2$. By Lemmas 5.2 and 5.13, α interchanges Q and R. Thus, $n = 2$.

The following result is used in § 7.

LEMMA 5.15. *Suppose that $w = 1$. Let $\beta \in \mathrm{Aut}\, P$. Assume that*

(a) $P_3 = 1$ *and* $Q^\beta \neq Q$, *or*

(b) $P_3 \neq 1$ *and β interchanges* $\langle z_1\rangle$ *and* $\langle z_2\rangle$, *or*

(c) $P_3 \neq 1$ *and* $Q^\beta \neq Q$.

Define an isomorphism θ of P onto P^h by

$$\theta(x) = (x^\beta)^h, \quad x \in P.$$

Then $N(\theta) \cap Z = 1$.

Proof. Let $Q^* = N(\theta)$. By Lemma 2.4, $Q^* \trianglelefteq H$. Hence, $Q^* \subseteq P \cap P^h = Q$ and

$$Q^{*\beta} = (\theta(Q^*))^{h^{-1}} = Q^{*h^{-1}} = Q^*.$$

(a) Since $v = 1$, $Z(P) = \langle x_2, \ldots, x_u\rangle$ and $Z = \langle z_1\rangle$. Thus, $|Q/Z(P)| = p$. Since $Q^\beta \neq Q$, $Q \cap Q^\beta = Z(P)$. So $Q^* \subseteq Z(P)$. Now, $V = \langle z_1, z_2\rangle$. By Proposition 4.7, V is a minimal normal subgroup of H. Since $z_2 \notin Z(P)$, $z_2 \notin Q^*$. Hence $z_1 \notin Q^*$, as desired.

(b), (c) By Lemma 5.13, β interchanges Q and R. Hence,

$$Q^* = Q^{*\beta} \subseteq Q \cap R = \langle x_2, \ldots, x_{u+1}\rangle.$$

Define $M = \langle x_2, \ldots, x_{u+2}\rangle$ and $N = \langle x_3, \ldots, x_{u+1}\rangle = Z(Q)$, as in Proposition 4.16; then, by the proposition, M/N is a minimal normal subgroup of H/N. Since $NQ^* \subset M$, $Q^* \subseteq N$. Thus

$$Q^* = Q^{*\beta} \subseteq N \cap N^\beta = Z(Q) \cap Z(R) = Z(P).$$

Similarly,

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

Therefore,

$$Q^* \cap Z \subseteq Z(H) \cap Z = \langle z_2\rangle.$$

So $z_1 \notin Q^*$. Since $\langle z_2\rangle^\beta = \langle z_1\rangle$, $Q^* \cap Z = 1$.

6. Proof of Theorem 2(a), (b), (c), (d). Suppose that P, H, h, and α satisfy the hypothesis of Theorem 2. Define an isomorphism ϕ of P onto P^h by

$$\phi(x) = (x^\alpha)^h, \quad x \in P.$$

Let $Q = P \cap P^h$, $R = \phi^{-1}(Q)$, and $S = N(\phi)$ (see Lemma 2.4). Then $Q, R \subset P$ and $[P: Q] = [P: R] = p$. By Lemma 2.4, $S \trianglelefteq H$. Hence,

$$S^\alpha = ((S^\alpha)^h)^{h^{-1}} = (\phi(S))^{h^{-1}} = S^{h^{-1}} = S.$$

By the hypothesis of Theorem 2, $S = 1$. Consequently, the restriction of ϕ to R fixes no non-identity subgroup of R and satisfies (3.1).

Suppose that P is Abelian. Then P is elementary and $Q \subseteq P \cap P^h \subseteq Z(H)$. As in Theorem 2, let n be the smallest positive integer such that α^n fixes Q. Let

$$Q^* = Q \cap Q^\alpha \cap \ldots \cap Q^{\alpha^{n-1}}.$$

Then $Q^{*\alpha} = Q^*$ and $Q^* \subseteq Z(H)$. Hence, $\phi(Q^*) = (Q^{*\alpha})^h = Q^*$, and, therefore, $Q^* = 1$. Consequently,

$$|P| = [P:Q^*] \leqq [P:Q][P:Q^\alpha] \ldots [P:Q^{\alpha^{n-1}}] = p^n,$$

which yields part (a) of Theorem 2.

Suppose that P is not Abelian. Since $\phi(P) = (P^\alpha)^h = P^h$, ϕ and P satisfy (5.1), (5.2), and (5.5). Hence, parts (b) and (c) of Theorem 2 follow from Propositions 4.13 (c) and 4.15 (c), Theorem 5.10, and Corollary 5.14.

Suppose that $u \geqq v + 2$. By an argument similar to the proof of Lemma 5.2, $x_i^\alpha = x_{i+1}$, for $i = v + 1, v + 2, \ldots, u - 1$. Hence,

$$x_u = x_{u-1}{}^\alpha = x_{u-2}{}^{\alpha^2} = \ldots = x_{v+2}{}^{\alpha^{u-v-2}}.$$

Since $x_{v+2}, \ldots, x_u \in P \cap Z(H)$, this proves part (d) of Theorem 2.

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

7. The weakly closed case. In this section, we resume the hypothesis and notation of § 5. Suppose that S is a Sylow p-subgroup of H that contains P. Then P is said to be *weakly closed* in S with respect to H if, whenever $g \in H$ and $P^g \subseteq S$, then $P^g = P$. Throughout this section, we will assume the following condition:

(7.1) *P satisfies* (3.1), (5.1), *and* (5.2), *and P is weakly closed in some Sylow p-subgroup of H.*

We will show (Theorem 7.11) that if $P_3 \neq 1$, then $p = 3$. This immediately yields Theorem 2 (e). Another result (Theorem 7.6) will be used in § 8. Note that (7.1) is satisfied whenever P satisfies (3.1) and (5.1) and P is a Sylow p-subgroup of H.

Take $h \in H$ and $\alpha \in \operatorname{Aut} P$ as in § 5.

LEMMA 7.1. *Suppose that $g \in H$. Then P and P^g are conjugate in $\langle P, P^g\rangle$.*

Proof. Choose a Sylow p-subgroup S of H in which P is weakly closed. Let $K = \langle P, P^g\rangle$ and let T be a Sylow p-subgroup of K that contains P. Take $k \in K$ and $f \in H$ such that $(P^g)^k \subseteq T$ and $T^f \subseteq S$. Then $P^f \subseteq T^f \subseteq S$ and $P^{gkf} \subseteq T^f \subseteq S$. By the weak closure of P in S, $P = P^f = P^{gkf}$. Hence, f and gk normalize P, and $P^g = P^{k^{-1}}$.

LEMMA 7.2. *Let T be any p-subgroup of H that contains P. Then P is weakly closed in T with respect to H, and $P/Q \subseteq Z(T/Q)$.*

Proof. Suppose that $g \in H$ and $P^g \subseteq T$, but $P^g \neq P$. Let $T^* = \langle P, P^g\rangle$ and let M be a maximal subgroup of T^* that contains P. Since T^* is a p-group $M \lhd T^*$. By Lemma 7.1, P^g is conjugate to P in T^*. Hence, $T^* = \langle P, P^g\rangle \subseteq M$, which is a contradiction. Thus, P is weakly closed in T with respect to H. In particular, $P = P^g$ for all $g \in T$. So $P \trianglelefteq T$. Since T/Q is a p-group and contains P/Q as a normal subgroup of order p, $P/Q \subseteq Z(T/Q)$.

LEMMA 7.3. *Let i be a primitive $(p - 1)$th root of unity in $\mathbf{Z}_p$. Then $N(P)$ contains a p'-element k having the following properties:*

(a) $k^{-1}z_1k = z_1^{\,i}$;

(b) $k^{-1}z_{v+1}k = z_{v+1}^{\,i^{-1}}$;

(c) $k^{-1}xk \equiv x^{i^2}$, *modulo Q, for all $x \in P$; and*

(d) $k^{-1}x_{u+1}k \equiv x_{u+1}^{\,i^{-1}}$, *modulo $Z(P)$.*

Proof. Recall that $V = \langle z_1, z_{v+1}\rangle$. By Proposition 4.7, $Z(Q) = V \times (Q \cap Z(H))$, and $H/C(V)$ is isomorphic to $\mathrm{SL}(V)$ for V considered as a vector space over $\mathbf{Z}_p$. For every $g \in H$, let $\theta(g)$ be the matrix, with respect to the basis $\{z_1, z_{v+1}\}$, of the automorphism of V given by conjugation by g. Then $\theta(P)$ is the group of all matrices of the form

$$\begin{bmatrix} 1 & 0 \\ j & 1 \end{bmatrix}, \quad j \in \mathbf{Z}_p.$$

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

Since $\theta(H) = \mathrm{SL}(2, p)$, there exists $f \in H$ such that

$$\theta(f) = \begin{bmatrix} i & 0 \\ 0 & i^{-1} \end{bmatrix}.$$

Since $\theta(f)$ normalizes $\theta(P)$, f normalizes $PC(V)$.

Now, $\langle P, P^f \rangle \subseteq PC(V)$. By Lemma 7.1, there exist $e \in P$ and $c \in C(V)$ such that $P^{ec} = P^f$. Then $P^f = P^c$; fc^{-1} normalizes P. However, $\theta(fc^{-1}) = \theta(f)\theta(c^{-1}) = \theta(f)$. Let g be the p-part of fc^{-1} and k be the p'-part of fc^{-1}; i.e., let g be a p-element and k be a p'-element such that $gk = kg = fc^{-1}$. Since $\theta(fc^{-1})$ has order $p - 1$, $\theta(g) = 1$ and $\theta(k) = \theta(kg) = \theta(fc^{-1}) = \theta(f)$. Thus, k satisfies (a) and (b). A calculation shows that, for each $x \in P$, $\theta(k^{-1})\theta(x)\theta(k) = \theta(x)^{i^2}$; therefore, $\theta(k^{-1}xkx^{-i^2}) = 1$ and

$$k^{-1}xkx^{-i2} \in P \cap C(V) = Q.$$

This yields (c). Finally, (d) follows from (b) because

$$Z(P) = \langle x_{v+1}, \ldots, x_u \rangle,$$

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

and

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

LEMMA 7.4. *Suppose that p is odd, that $P_3 = 1$, and that $v = 1$. Define i and k as in Lemma 7.3. Then P contains a subgroup S with the following properties:*

(a) *$Z(P) \subset S$ and $S^k = S$;*

(b) *$P/Z(P) = S/Z(P) \times Q/Z(P)$;*

(c) *Q and S are the only subgroups of P that are normalized by k and contain $Z(P)$ as a subgroup of index p;*

(d) *$k^{-1}xk \equiv x^{i^2}$, modulo $Z(P)$, for all $x \in S$; and*

(e) *$k^{-1}xk \equiv x^{i^{-1}}$, modulo $Z(P)$, for all $x \in Q$.*

Proof. Since $v = 1$, $Z(P) = \langle x_2, \ldots, x_u \rangle$. Hence, $|P/Z(P)| = p^2$ and $P = \langle Z(P), x_1, x_{u+1} \rangle$. Let $F = P/Z(P)$. Consider F to be a vector space over $\mathbf{Z}_p$. By parts (c) and (d) of Lemma 7.3, conjugation by k induces a transformation on F having eigenvalues i^2 and i^{-1} and such that i^{-1} is an eigenvalue for the subspace $Q/Z(P)$. Thus, we obtain (e). Since p is odd and i has order $p - 1$, $i^2 \neq i^{-1}$. Hence, there exists a unique one-dimensional subspace $S/Z(P)$ for which i^2 is an eigenvalue. This gives (a), (b), (c), and (d).

Recall that $z_j = [x_j, x_{u+j}]$, for $j = 1, \ldots, v$, and that $Z = \langle z_1, \ldots, z_v \rangle$.

LEMMA 7.5. *Suppose that p is odd, that $P_3 = 1$, and that $v = 1$. Define k as in Lemma 7.3 and S as in Lemma 7.4. Let κ be the automorphism of P induced by conjugation by k. Let $\beta = \kappa^{-1}\alpha\kappa\alpha^{-1}$ and $\gamma = \kappa^{-1}\alpha^{-1}\kappa\alpha$. Then:*

(a) *β and γ fix z_1 and fix every element of $Z(P)/\langle z_1 \rangle$; and*

(b) *if $Q^\beta = Q^\gamma = Q$, then α interchanges Q and S.*

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

Proof. Since $v = 1$, $\langle z_1\rangle = Z = P'$. So $\langle z_1\rangle$ is a characteristic subgroup of P. As $\mathrm{Aut}\langle z_1\rangle$ is cyclic, β and γ fix z_1. By Proposition 4.7, k centralizes $Z(P)/\langle z_1\rangle$. Consequently, we obtain (a).

Suppose that $Q^\beta = Q$. Then $Q = Q^{\kappa^{-1}\alpha\kappa\alpha^{-1}} = Q^{\alpha\kappa\alpha^{-1}}$, and $Q^\alpha = (Q^\alpha)^\kappa$. By Lemma 7.4 (c), Q^α is Q or S. Since $Q^\alpha \neq Q$, $Q^\alpha = S$. Similarly, if $Q^\gamma = Q$, then $Q^{\alpha^{-1}} = S$ and $S^\alpha = Q$. This proves (b).

THEOREM 7.6. *Define k as in Lemma 7.3, and let κ be the automorphism of P induced by conjugation by k. Let $A = \langle\alpha, \kappa\rangle$. For every $\beta \in A$, define an isomorphism ϕ_β of P onto P^h by $\phi_\beta(x) = (x^\beta)^h$.*

Suppose that, for every $\beta \in A$, $N(\phi_\beta)$ is 1 or $N(\phi_\beta) \supseteq Z$. Then $w = 1$.

Assume further that p is odd. Then:

(a) *Suppose that $P_3 \neq 1$. Then $u = 2v = 4$ and $t = 6$.*

(b) *Suppose that $P_3 = 1$. Define S as in Lemma 7.4. Let A_Q be the set of all $\beta \in A$ that fix Q. Then either*

(i) *$u = 2v = 2$ and $t = 3$, or*

(ii) *$u = 3$, $t = 4$, A fixes S, and $[A{:}A_Q] = [A'{:}A' \cap A_Q] = p$.*

Proof. By Lemma 5.4, $w = 1$. Now assume that p is odd.

(a) Suppose that $P_3 \neq 1$. Then $v = 2$ and $Z = \langle z_1, z_2\rangle$. By Lemma 5.2, α interchanges $\langle z_1\rangle$ and $\langle z_2\rangle$. Since $z_2 \in Z(H)$, Lemma 7.3 (a) yields that κ fixes $\langle z_1\rangle$ and $\langle z_2\rangle$. Therefore, A has a normal subgroup B of index two in which every element fixes $\langle z_1\rangle$ and $\langle z_2\rangle$. Let λ be the 2-part of $\kappa^{(p-1)/2}$ and let A_2 be a Sylow 2-subgroup of A that contains λ. By Lemma 7.3 (a), $\kappa^{(p-1)/2}$ maps z_1 into z_1^{-1}. Hence, $z_1^\lambda = z_1^{-1}$. By Proposition 4.7,

$$Z(P) = \langle z_1\rangle \times (Z(P) \cap Z(H)).$$

Therefore, the fixed points of $Z(P)$ under λ are just the elements of $Z(P) \cap Z(H)$.

Since $|A/B| = 2$, $A_2 \not\subseteq B$. Take $\beta \in A_2 - B$, and let $C = \langle\lambda, \beta\rangle$. Then C is a 2-group and, by Lemma 5.15 (b), $N(\phi_\beta) \cap Z = 1$. Hence, $N(\phi_\beta) = 1$. Since λ fixes every element of $Z(P) \cap Z(H)$, λ fixes every element of $Z(P)/Z$. By Lemma 4.1, there exists $Y \subseteq Z(P)$ such that C fixes Y and $Z(P) = Y \times Z$. Then λ fixes every element of Y. Therefore, $Y \subseteq Z(P) \cap Z(H)$. Since $\beta \in C$, β fixes Y and $Y \subseteq N(\phi_\beta) = 1$.

(b) Suppose that $P_3 = 1$. Then $v = 1$ and $Z = \langle z_1\rangle$. Since $Z = P'$, A fixes Z. Assume α interchanges Q and S. Then A has a normal subgroup B of index two in which every element fixes Q and S. Define λ, A_2, β, and C as in the preceding argument. Then $Q^\beta = S$. By Lemma 5.15, $N(\phi_\beta) \cap Z = 1$. So $N(\phi_\beta) = 1$. Let Y be a complement of Z in $Z(P)$ that is fixed by C. As before, we obtain $Y \subseteq Z(P) \cap Z(H)$ and $Y \subseteq N(\phi_\beta) = 1$. Therefore, $Z(P) = Z$ and $u = 2 = 2v$. So (i) holds.

Assume that (i) does not hold; i.e., $u \geqq 3$. Then α does not interchange Q and S. By Lemma 7.5, there exists some element β in A' such that $Q^\beta \neq Q$, β fixes z_1, and β fixes every element of $Z(P)/\langle z_1\rangle$. As before, $N(\phi_\beta) = 1$.

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

We claim that $u = 3$. Note that $x_3 \in Z(H)$. The hypothesis of the theorem is satisfied if ϕ is replaced by ϕ_β. Thus, to prove that $u = 3$, we may replace α by β; equivalently, we will assume in this paragraph alone that α fixes z_1 and every element of $Z(P)/\langle z_1\rangle$. (This permits us to retain our present notation.) In particular, $x_2 \equiv x_2^{\alpha} \equiv (\phi(x_2))^h \equiv (x_3)^{h-1} \equiv x_3$, modulo $\langle z_1\rangle$. So $x_2^{-1}x_3 \in \langle z_1\rangle$. Since $z_1 = x_2^{d(2)} \dots x_u^{d(u)}$ and $d(u) \neq 0$, we obtain $u = 3$.

We now have $Z(P) = \langle x_2, x_3\rangle = \langle z_1, x_3\rangle = \langle P', x_3\rangle$ and $P \cap Z(H) = \langle x_3\rangle$. Since A fixes P', A' must fix every element of P' and every element of $Z(P)/P'$. Since $\beta \in A'$ and $N(\phi_\beta) = 1$, β does not fix $\langle x_3\rangle$. By Lemma 4.2, A' induces a non-trivial p-group of automorphisms on $Z(P)$. Let A_0 be the subgroup of A' consisting of all the elements of A' that fix every element of $Z(P)$. Then $A_0 \lhd A$. Since $\operatorname{Aut} Z(P)$ has a Sylow p-subgroup of order p, $|A'/A_0| = p$.

Suppose that $\gamma \in A_0$. Then γ fixes x_3, which lies in the centre of H. Therefore, $x_3 \in N(\phi_\gamma)$. By hypothesis, $z_1 \in N(\phi_\gamma)$. Since $N(\phi_\gamma) \trianglelefteq H$,

$$V \subseteq N(\phi_\gamma) \subseteq Q.$$

As $\langle V, x_3\rangle = Q$, we obtain $N(\phi_\gamma) = Q$. So γ fixes Q. Since γ is arbitrary,

$$(7.2) \qquad A_0 \textit{ fixes } Q.$$

Let $\bar{A}$ be the group of automorphisms induced by A on $P/Z(P)$, and define $\bar{A}_0$ similarly. Suppose that $\bar{A}_0 \neq 1$. By (7.2), the subspace $Q/Z(P)$ of $P/Z(P)$ is invariant under $\bar{A}_0$. Since $A_0 \trianglelefteq A$, $Q^\alpha/Z(P)$ is also invariant under $\bar{A}_0$. Now, $Q^\alpha \neq Q$. Suppose that $Q/Z(P)$ and $Q^\alpha/Z(P)$ are the only invariant one-dimensional subspaces of $P/Z(P)$ under $\bar{A}_0$. Then they are permuted by A. Thus, $Q^{\alpha^2} = Q$. Moreover, since κ fixes $Q/Z(P)$, κ fixes $Q^\alpha/Z(P)$. By Lemma 7.4, $Q^\alpha = S$, contrary to our assumption that α does not interchange Q and S. Thus, $\bar{A}_0$ fixes at least three one-dimensional subspaces of $P/Z(P)$. Since $|P/Z(P)| = p^2$, $\bar{A}_0$ fixes all the one-dimensional subspaces of $P/Z(P)$, by a simple argument from linear algebra.

Since $\beta \in A'$ and $Q^\beta \neq Q$, $\beta \notin A_0$. Hence, $|\bar{A}'/\bar{A}_0| = p$ and the automorphism of $P/Z(P)$ induced by β has order divisible by p. It follows that β, and therefore A', fix a unique one-dimensional subspace $T/Z(P)$ of $P/Z(P)$. Since $A' \lhd A$, A fixes $T/Z(P)$. By Lemma 7.4, $T = S$.

Clearly, $[A':A' \cap A_Q] = p$. Since $P/Z(P)$ has only $p + 1$ one-dimensional subspaces and A fixes $S/Z(P)$, $[A:A_Q] = p$. This proves (ii) and completes the proof of Theorem 7.6.

Lemma 7.7 [7, p. 416]. *Suppose that T is an Abelian Sylow p-subgroup of a finite group K. Then $K' \cap Z(K) \cap T = 1$.*

Lemma 7.8. *Suppose that S is a Sylow p-subgroup of a finite group K. Assume that T and U are subgroups of S enjoying the following properties:*

(a) $|T| = p$;

(b) $U \trianglelefteq K$ *and* $T \not\subseteq U$;

(c) *$S = TU$;*

(d) *T is weakly closed in S with respect to K; and*

(e) *K is generated by some conjugates of T in K.*

Then $U = 1$.

Proof. The proof of Lemma 7.2 shows that $T \subseteq Z(S)$. Hence, $S = T \times U$. Let $C = C_K(U)$. Since $T \subseteq C$ and $C \trianglelefteq K$, (e) yields that $C = K$. Thus, $U \subseteq Z(K)$. Therefore, S is Abelian. By Lemma 7.7, $K' \cap U = 1$.

Suppose that K/U has a normal p-complement. Thus, $K'U/U$ is a p'-group. Since $K'U/U \cong K'/(K' \cap U) \cong K'$, K' is a p'-group. Since $TK' \trianglelefteq K$, $TK' = K$, by (e). So T is a Sylow p-subgroup ot K, and $U = 1$.

Suppose that K/U does not have a normal p-complement. By a theorem ot Burnside [**5**, p. 252], a Sylow p-subgroup of K/U is not contained in the centre of its normalizer. Hence,

$$S/U \not\subseteq Z(N_K(S)/U) \quad \text{and} \quad S \not\subseteq Z(N_K(S)).$$

Take $x \in N_K(S) - C_K(S)$. Since $S = T \times U$ and $U \subseteq Z(K)$, we obtain $[S, \langle x \rangle] = [T, \langle x \rangle] = T$, by (a) and (d). Thus, $T \subseteq K'$. By (e), $K = K'$. So $U = U \cap K' = 1$.

LEMMA 7.9. *Suppose that K is a finite group, that S is a Sylow p-subgroup of K, and that T is weakly closed in S with respect to K. Suppose that $N \trianglelefteq K$. Then TN/N is weakly closed in SN/N with respect to K/N.*

Proof. Suppose that $g \in K$ and that $(TN)^g \subseteq SN$. Then $T^g \subseteq SN = NS$. Since S is a Sylow p-subgroup of NS, there exists $k \in N$ and $s \in S$ such that $(T^g)^{ks} \subseteq S$. Then $T^{gk} \subseteq S$. By the weak closure of T, $T^{gk} = T \subseteq TN$. Hence, $T^g \subseteq (TN)^{k^{-1}} = TN$, and $(TN)^g = TN$.

PROPOSITION 7.10. *The subgroup $PC_H(Q)/QC_H(Q)$ is a Sylow p-subgroup of $H/QC_H(Q)$. Moreover, there exists an element g of H such that $gh^{-1} \in C_H(Q)$ and P is a Sylow p-subgroup of $\langle P, P^g \rangle$.*

Proof. Let T be a Sylow p-subgroup of H that contains P. Let $M_1 = C_H(V)$. By Proposition 4.7, $H/M_1 \cong \mathrm{SL}(2, p)$. If $P_3 = 1$, define $M_2 = M_1$. If $P_3 \neq 1$, define $M_2 = C_H(M/N)$, for M and N as in Proposition 4.14. Let $L = M_1 \cap M_2$. By Proposition 4.16, $H/M_2 \cong \mathrm{SL}(2, p)$ and $L \supseteq QC_H(Q)$; furthermore, L centralizes every factor Q_i/Q_{i-1} in an H-composition series

$$1 = Q_0 \subset Q_1 \subset \ldots \subset Q_n = Q$$

of Q. By Lemma 4.2, L induces a p-group of automorphisms on Q. Hence,

$$(7.3) \qquad L/C_H(Q) \text{ is a } p\text{-group.}$$

Suppose that $p = 2$ or $p = 3$. Then $\mathrm{SL}(2, p)$ has a normal p'-subgroup of index p. So $|H/H'M_1| = p$ and $H'M_1/M_1$ is a p'-group. Since P and P^h generate H,

$$H = H'P \quad \text{and} \quad P \cap H' \subseteq P \cap M_1 = Q, \quad \text{if } p < 5.$$

Thus, $|H/H'Q| = p$. Since $Q \subseteq L \subseteq M_1$ and $|H'Q| = |H'M_1|$,

(7.4) $$|H/H'Q| = p \quad \textit{and} \quad L \subseteq H'Q, \quad \textit{if } p < 5.$$

Moreover, $H'M_i/M_i$ is a p'-group, for $i = 1, 2$. Hence, $H'/(H' \cap M_i)$ is a p'-group, for $i = 1, 2$. Now,

$$(H' \cap M_1)/(H' \cap L) \cong (H' \cap M_1)/(H' \cap M_1 \cap M_2) \cong (H' \cap M_1)M_2/M_2 \subseteq H'M_2/M_2,$$

which is a p'-group. Thus,

(7.5) $$H'/(H' \cap L) \quad \textit{and} \quad H'L/L \textit{ are } p'\textit{-groups, if } p < 5.$$

Suppose that $p \geqq 5$. Then $Z(\mathrm{SL}(2, p))$ has order two, and

$$\mathrm{SL}(2, p)/Z(\mathrm{SL}(2, p))$$

is simple. Let $N_i/M_i = Z(H/M_i)$, for $i = 1, 2$. Then H/N_i is simple, for $i = 1, 2$. Let $K = N_1 \cap N_2$. We claim that $N_1 = N_2 = K$. Suppose otherwise. Since $N_1/K \cong N_1N_2/N_2 \trianglelefteq H/N_2$, it follows that N_1/K is simple and $H = N_1N_2$. So

$$H/K = N_1/K \times N_2/K \cong H/N_2 \times H/N_1.$$

Now, $T \cap N_i$ is a Sylow p-subgroup of N_i, for $i = 1, 2$, and

$$TK/K = (T \cap N_1)K/K \times (T \cap N_2)K/K.$$

Let $x \in P - Q$. Take $x_i \in T \cap N_i$ such that

$$x_1x_2 \equiv x, \quad \text{modulo } K.$$

Since $H = \langle P, P^h\rangle$, we have $P \nsubseteq N_1$. Therefore, $x_2 \notin K$. Likewise, $x_1 \notin K$.

We now obtain a contradiction. By the structure of $\mathrm{SL}(2, p)/Z(\mathrm{SL}(2, p))$, there exists $y \in N_1$ such that $y^{-1}x_1y \equiv x_1{}^j$, modulo K, for some $j \not\equiv 1$ in $\mathbf{Z}_p$. Then y normalizes $(T \cap N_1)K$ and centralizes $(T \cap N_2)K/K$. Hence, y normalizes TK. So there exists $z \in K$ such that $(T^y)^z = T$. Then, modulo K,

$$x_1{}^{yz} \equiv (x_1{}^j)^z \equiv x_1{}^j, \quad x_2{}^{yz} \equiv x_2, \quad \text{and} \quad x^{-1}x^{yz} \equiv x_1{}^{j-1} \not\equiv 1.$$

Since $P^{yz} \subseteq T$, $P^{yz} = P$, by the weak closure of P. Hence, P contains x, x^{yz}, and $x^{-1}x^{yz}$. Since $x^{-1}x^{yz} \notin K$, $x^{-1}x^{yz} \in P - Q$. Consequently,

$$P = \langle Q, x^{-1}x^{yz}\rangle \subseteq QN_1 = N_1,$$

and $H = \langle P, P^h\rangle \subseteq N_1$, which is a contradiction. Thus, $N_1 = N_2 = K$, as desired. Therefore,

(7.6) $$p^2 \textit{ does not divide } |H/K|, \textit{ if } p \geqq 5.$$

Also, since $|K/M_1| = |K/M_2| = 2$, $|K/L|$ is either two or four. By (7.6), p^2 does not divide $|H/L|$. By (7.4) and (7.5), we have a similar result if $p < 5$. Since $P \nsubseteq L$ for any p,

(7.7) $$PL/L \textit{ is a Sylow } p\textit{-subgroup of } H/L, \textit{ for any } p.$$

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

For every subgroup X of H, let $\bar{X} = XQC_H(Q)/QC_H(Q)$. By Lemma 7.9, $\bar{P}$ is weakly closed in $\bar{T}$ with respect to $\bar{H}$. By (7.3), $\bar{L}$ is a p-group. By the definition of L, L centralizes V. Thus, $P \not\subseteq LQC_H(Q)$. Since $|P/Q| = p$, $|\bar{P}| = p$. Now by (7.7) and Lemma 7.8, $\bar{L} = 1$. This proves the first part of the proposition.

Since $C_T(Q)$ is a Sylow p-subgroup of $C_H(Q)$, there exists $c \in C_H(Q)$ such that $C_T(Q)^c = C_T(Q)^h$. Let $g = hc^{-1}$. Then g normalizes $C_T(Q)$, and $gh^{-1} \equiv hc^{-1}h \equiv h^{-1}h \equiv 1$ (modulo $C_H(Q)$). Let $H^* = \langle T, T^g\rangle$ and $H^{**} = \langle P, P^g\rangle$. By Lemma 7.2, P is weakly closed in a Sylow p-subgroup of H^{**}. To prove the second part of the proposition, it suffices to prove that P is a Sylow p-subgroup of H^{**}. Let $K^* = QC_T(Q)$ and let $L^* = L \cap H^*$. Since T and g normalize $C_T(Q)$, $K^* \lhd H^*$. Since we proved that $L = QC_H(Q)$, L^*/K^* is a p'-group. Therefore,

(7.8) *$(K^* \cap H^{**})/Q$ is a normal p-subgroup of H^{**}/Q and $(L^* \cap H^{**})/(K^* \cap H^{**})$ is a p'-group.*

By (7.7), PK^*/K^* is a Sylow p-subgroup of H^*/K^*. By projecting H^{**} into H^*/K^*, we see that

(7.9) *$P(K^* \cap H^{**})/(K^* \cap H^{**})$ is a Sylow p-subgroup of $H^{**}/(K \cap H^{**})$.*

By (7.8), (7.9), and another application of Lemmas 7.8 and 7.9, $K^* \cap H^{**} = Q$.

By (7.9), this completes the proof of the proposition.

THEOREM 7.11. *Assume that $P_3 \neq 1$. Then $p = 3$.*

Proof. By Theorem 3.7, p is odd. Clearly, for every normal subgroup Q^* of H contained in Q, P/Q^* is weakly closed in some Sylow p-subgroup of H/Q^*. Moreover, if $Z \not\subseteq Q^*$, then P/Q^* has nilpotence class three. Hence, by Theorem 7.6, we may assume that $v = 2$, $u = 4$, and $t = 6$.

For g as in Proposition 7.10, g and h act in the same way on Q by conjugation. Hence, we may assume that P is a Sylow p-subgroup of H.

We will not use the elements i and k introduced in Lemma 7.3. Therefore, we will use the letters "i" and "k" for other purposes.

By Proposition 3.4, $[x_1, x_5] = x_3{}^i$, for some $i \in \mathbf{Z}_p$. Since $x_3 \in Z(P)$, the group $\langle x_1, x_5\rangle$ has nilpotence class two; hence,

$$[x_1{}^{i-1}, x_5{}^{i-1}] = (x_3{}^i)^{i-2} = x_3{}^{i-1}.$$

Since x_1 was chosen only under the condition that it satisfy Proposition 2.1 (c), we may replace x_1 by $x_1{}^{i-1}$ and then replace x_j by $x_j{}^{i-1}$, for $j = 2, \ldots, t+1$. Thus, we may assume that

$$[x_1, x_5] = x_3.$$

Take $i, j, k, m \in \mathbf{Z}_p$ such that

$$[x_1, x_6] = x_2{}^i x_3{}^j x_4{}^k x_5{}^m.$$

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

Then $[x_2, x_7] = x_3{}^i x_4{}^j x_5{}^k x_6{}^m$. By Proposition 4.15,

(7.10) *i and m are nonzero.*

Note that $Q' = \langle x_4 \rangle$. We obtain the following congruences modulo Q':

$$\begin{aligned} x_2{}^{x_1} &\equiv x_2, & x_2{}^{x_7} &\equiv x_2 x_3{}^i x_5{}^k x_6{}^m, \\ x_3{}^{x_1} &\equiv x_3, & x_3{}^{x_7} &\equiv x_3 x_5, \\ x_5{}^{x_1} &\equiv x_5[x_1, x_5]^{-1} \equiv x_3{}^{-1} x_5, & x_5{}^{x_7} &\equiv x_5, \\ x_6{}^{x_1} &\equiv x_2{}^{-i} x_3{}^{-j} x_5{}^{-m} x_6, & x_6{}^{x_7} &\equiv x_6. \end{aligned}$$

We consider Q/Q' to be a vector space over $\mathbf{Z}_p$ with the basis

$$\{x_2Q', x_6Q', x_3Q', x_5Q'\}.$$

For each $g \in H$, let $\theta(g)$ be the matrix corresponding to the transformation of Q/Q' induced by conjugation by g. Then

$$\theta(x_1) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -i & 1 & -j & -m \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}, \theta(x_7) = \begin{bmatrix} 1 & m & i & k \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

For each $g \in H$, let $\theta_1(g)$ and $\theta_2(g)$ be the upper left hand and lower right hand corner submatrices of degree two, respectively. Since $\langle x_3, x_5 \rangle \lhd H$, θ_1 and θ_2 are homomorphisms. By Propositions 4.7 and 4.16, $\theta_1(H) = \theta_2(H) = \mathrm{SL}(2, p)$. Denote by I_2 and I_4 the identity matrices of degrees two and four over $\mathbf{Z}_p$.

Let N be the subgroup of H consisting of all $g \in G$ for which $\theta_2(g)$ is I_2 or $-I_2$. Since $Q \subseteq N$ and $P \not\subseteq N$, $P \cap N = Q$. Since P is a Sylow p-subgroup of H, Q is a Sylow p-subgroup of N. Therefore, N/Q is a p'-group. Since $Q \subseteq \operatorname{Ker} \theta$,

(7.11) *$\theta(N)$ is a normal p'-subgroup of $\theta(H)$, and $\theta_1(N)$ is a normal p'-subgroup of $\theta_1(H)$* (i.e., *of* $\mathrm{SL}(2, p)$).

Let $g = x_1{}^2 x_7$. Then

$$\theta_1(g) = \begin{bmatrix} 1 & m \\ -2i & 1 - 2im \end{bmatrix}, \theta_2(g) = \begin{bmatrix} 1 & 1 \\ -2 & -1 \end{bmatrix},$$

and

$$\theta_1(g^2) = \begin{bmatrix} 1 - 2im & 2m - 2im^2 \\ 4i^2m - 4i & 1 - 6im + 4i^2m^2 \end{bmatrix} \tag{7.12}$$

Thus, $\theta_2(g^2) = -I_2$. So $g^2 \in N$. By (7.11), $\theta_1(g^2) = \pm I_2$ if $p > 3$. If $p = 3$, then $\mathrm{SL}(2, p)$ has a normal quaternion subgroup of order eight and index three. In this case, $\theta_1(g^2)$ is a 2-element, by (7.11); hence, $\theta_1(g)$ is a 2-element and $\theta_1(g^2) = \theta_1(g)^2 = \pm I_2$. Thus, $\theta_1(g^2) = \pm I_2$, regardless of p. Conse-

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

quently, $4i^2m - 4i = 0$. By (7.10), $i \neq 0$. Since p is odd, $4i \neq 0$. Therefore,

$$im = 1. \tag{7.13}$$

Now, calculation yields

$$\theta(g) = \theta(x_1{}^2x_7) = \begin{bmatrix} 1 & m & i & k \\ -2i & -1 & m - 2j - 2i^2 & -2ik - m - 2j \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -2 & -1 \end{bmatrix},$$

$$\theta(g^4) = \begin{bmatrix} 1 & 0 & -2(m^2 - 2jm - 2k) & -2(i - m^2 - 2k - 2jm) \\ 0 & 1 & -2(4ik + 2m + 4j - 2i^2) & -2(3m - 2i^2 + 2ik + 2j) \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Hence, $g^4 \in N$ and $\theta(g^4)^p = I_4$. By (7.11), $\theta(g^4) = I_4$. Therefore,

$$0 = i - m^2 - 2k - 2jm = 3m - 2i^2 + 2ik + 2j.$$

By (7.13), this yields

$$0 = i - m^2 - 2k - 2jm = (-m)(3m - 2i^2 + 2ik + 2j) = \\ -3m^2 + 2i - 2k - 2jm.$$

So $i - m^2 = 2k + 2jm = -3m^2 + 2i$, which yields $i = 2m^2 = 2i^{-2}$. Thus,

$$i^3 = 2. \tag{7.14}$$

We now apply the symmetry between ϕ and ϕ^{-1} (see Lemma 3.3). Let $y_n = (x_{8-n})^{-1}$, for $n = 1, 2, \ldots, 7$. Then

$$\phi(P) = \langle y_1, \ldots, y_7 \rangle, \quad Q = \langle y_2, \ldots, y_6 \rangle,$$

and ϕ^{-1} maps $\phi(P)$ onto P. Just as we had $[x_1, x_5] = x_3$, we have

$$[y_1, y_5] = [x_7{}^{-1}, x_3{}^{-1}] = [x_3{}^{-1}, x_7{}^{-1}]^{-1} = x_5{}^{-1} = y_3.$$

Define $[y_1, y_6] = y_2{}^{i'}y_3{}^{j'}y_4{}^{k'}y_5{}^{m'}$. The proof of (7.14) applies to give

$$i'^3 = 2. \tag{7.15}$$

However, $\langle x_4, x_5 \rangle = \langle y_3, y_4 \rangle = Z(\phi(P))$. Modulo $Z(\phi(P))$,

$$x_6{}^{-i'}x_3{}^{-m'} \equiv y_2{}^{i'}y_5{}^{m'} \equiv [y_1, y_6] \equiv [x_7{}^{-1}, x_2{}^{-1}] \equiv [x_2, x_7]^{-1} \equiv x_6{}^{-m}x_3{}^{-i}.$$

Thus, $i' = m = i^{-1}$. By (7.14) and (7.15), $4 = i^3i'^3 = i^3i^{-3} = 1$ in $\mathbf{Z}_p$. Thus, $p = 3$.

8. A further result.

Let C_p denote a cyclic group of order p.

THEOREM 8.1. *Suppose that H is a finite group and that P is a weakly closed subgroup of some Sylow subgroup of H with respect to H. Assume that, for some $h \in H$,*

$$\langle P, P^h \rangle = H \quad \textit{and} \quad [P: P \cap P^h] = p.$$

Let A be a subgroup of Aut P *that contains the automorphisms induced by conjugation by the elements of $N_H(P)$. Suppose that some element of A does not fix Q.*

Take $Q^* \subset Q$ maximal such that $Q^* \trianglelefteq H$ and such that there exists an element of A that fixes Q^* but not Q. Take $\alpha \in A$ such that α fixes Q^* but not Q. Let n be the smallest positive integer such that α^n fixes Q. Let $\bar{P} = \bar{P}_1 = P/Q^*$ and $\bar{P}_{i+1} = [\bar{P}_i, \bar{P}]$, for $i = 1, 2, 3$. Then $\bar{P}_4 = 1$. Furthermore:

(a) *Suppose that $\bar{P}_2 = 1$. Then $|\bar{P}| \leqq p^n$.*

(b) *Suppose that $\bar{P}_2 \neq 1$, that $\bar{P}_3 = 1$, and that $p = 2$. Then $\bar{P}$ is the direct product of $E(p)$ and an elementary group, and $n = 2$.*

(c) *Suppose that $\bar{P}_2 \neq 1$, that $\bar{P}_3 = 1$, and that p is odd. Then n is a divisor of p, $p - 1$, or $p + 1$, and either $\bar{P} \cong E(p)$ or $\bar{P} \cong E(p) \times C_p$. In the latter case, there exists $\alpha \in A'$ such that α^p fixes Q and α does not fix Q.*

(d) *Suppose that $\bar{P}_3 \neq 1$. Then $p = 3$, $\bar{P} \cong E^*(3)$, and $n = 2$.*

Proof. The proof of (a) is similar to the proof of Theorem 2 (a). The other parts of Theorem 8.1 follow from Theorems 7.6 and 7.11 and Corollary 5.14.

Note that Theorem 8.1 can be applied when H is embedded in a group G and A is the group of automorphisms of P induced by a subgroup of $N_G(P)$ that contains $N_H(P)$.

9. Some examples. In this section, let p be an arbitrary odd prime. We will construct groups P and H such that P and H satisfy the conditions of § 5 and $P \cong E^*(p)$. If $p = 3$, P will be a Sylow p-subgroup of H.

Let Q be a group of order p^5 and exponent p isomorphic to $E(p) \times C_p \times C_p$. Take $x_2, x_3, x_4, x_5, x_6 \in Q$ such that

$$Q = \langle x_2, x_6 \rangle \times \langle x_3, x_5 \rangle \quad \textit{and} \quad [x_2, x_6] = x_4 \neq 1.$$

Let B be the subgroup of all automorphisms α of Q such that α is trivial on $\langle x_3, x_5 \rangle$ and on $Q/\langle x_3, x_5 \rangle$. Then B is in one-to-one correspondence with the set of all homomorphisms η of $\langle x_2, x_6 \rangle$ into $\langle x_3, x_4 \rangle$; here, η corresponds to α if

$$x^\eta = x^\alpha x^{-1}, \quad \text{for all } x \in Q.$$

Thus, $|B| = p^4$ and B acts faithfully on Q/Q'.

Take $c \in \mathbf{Z}_p$ such that $2c = 1$. There exist unique automorphisms α_1, α_7 of Q such that

$$\begin{array}{ll} {x_2}^{\alpha_1} = x_2, & {x_2}^{\alpha_7} = x_2 {x_4}^c {x_6}^{-1}, \\ {x_6}^{\alpha_1} = x_2 {x_4}^{c-1} x_6, & {x_6}^{\alpha_7} = x_6, \\ {x_3}^{\alpha_1} = x_3,\ {x_5}^{\alpha_1} = {x_3}^{-1} x_5 & {x_3}^{\alpha_7} = x_3 x_5,\ {x_5}^{\alpha_7} = x_5. \end{array}$$

Let $S = \langle \alpha_1, \alpha_7 \rangle$. Since α_1 and α_7 fix $\langle x_3, x_5 \rangle$, S normalizes B.

Now, for every $x \in Q$, let $x^{\frac{1}{2}}$ be the unique element of Q such that $(x^{\frac{1}{2}})^2 = x$. (Then $x^{\frac{1}{2}} = x^c$.) For every $x, y \in Q$, let $x \circ y = x^{\frac{1}{2}} y x^{\frac{1}{2}}$.

LEMMA 9.1. *Under the operation* $\circ$, Q *forms an elementary Abelian group.*

Proof. We first prove that Q is an Abelian group; this result is well known [**1**, § VII.5, Example 2, p. 128]. Let $x, y \in Q$. By Lemma 2.5,

$$[x^{\frac{1}{2}}, y]^2 = [x, y] = [x, y^{\frac{1}{2}}]^2.$$

Thus, $[x, y]^{\frac{1}{2}} = [x^{\frac{1}{2}}, y] = [x, y^{\frac{1}{2}}]$. Now,

$$\begin{aligned} x \circ y &= x^{\frac{1}{2}} y x^{\frac{1}{2}} = xy[y, x^{\frac{1}{2}}] = xy[y, x]^{\frac{1}{2}} \\ &= yx[x, y][y, x]^{\frac{1}{2}} = yx[x, y]^{\frac{1}{2}} = y \circ x. \end{aligned}$$

For $z \in Q$,

$$x \circ (y \circ z) = x(y \circ z)[y \circ z, x]^{\frac{1}{2}} = x(y \circ z)[yz, x]^{\frac{1}{2}} = xyz[z, y]^{\frac{1}{2}}[y, x]^{\frac{1}{2}}[z, x]^{\frac{1}{2}},$$

and

$$(x \circ y) \circ z = (x \circ y)z[z, x \circ y]^{\frac{1}{2}} = xy[y, x]^{\frac{1}{2}}z[z, x]^{\frac{1}{2}}[z, y]^{\frac{1}{2}}.$$

Thus, Q is an Abelian group. Since $x^i \circ x = x^{i+1}$ for all $i \geqq 1$, every element of Q has order p under $\circ$.

LEMMA 9.2. *The group* S *is isomorphic to* $\mathrm{SL}(2, p)$, *and* $S \cap B = 1$. *Furthermore,* SB *acts faithfully on* Q/Q'.

Proof. We may consider S to be a group of automorphisms of Q under $\circ$. Now,

$$x_2 \circ x_6 = x_2x_6[x_6, x_2]^{\frac{1}{2}} = x_2{x_4}^{c-1}x_6 = {x_6}^{\alpha_1}$$

and

$$x_2 \circ {x_6}^{-1} = x_2{x_6}^{-1} = [{x_6}^{-1}, x_2]^{\frac{1}{2}} = x_2{x_4}^{c}{x_6}^{-1} = {x_2}^{\alpha_7}.$$

Consider Q (under $\circ$) to be a vector space over $\mathbf{Z}_p$ with basis $\{x_2, x_6, x_3, x_5, x_4\}$. Then α_1 and α_7 are represented by the matrices

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

respectively. Let D be the matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Then S is a subgroup of the group of all matrices of the form

$$\begin{bmatrix} M & 0 & 0 \\ 0 & D^{-1}MD & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

for $M \in \mathrm{SL}(2, p)$. Clearly, the latter group is isomorphic to $\mathrm{SL}(2, p)$. Moreover, it is generated by the matrices for α_1 and α_7 (see the proof of Proposition

https://doi.org/10.4153/CJM-1971-106-0 Published online by Cambridge University Press

4.7). Hence, $S \cong \mathrm{SL}(2, p)$. In addition, $S \cap B = 1$ because no non-identity element of S is trivial on x_3 and x_5. Since B acts faithfully on Q/Q', SB acts faithfully on Q/Q'. This completes the proof of Lemma 9.2.

We will have no further need for the operation $\circ$ on Q. Define $x_1, x_7 \in \operatorname{Aut} Q$ by

$$\begin{aligned} x_2^{x_1} &= x_2, & x_2^{x_7} &= x_2 x_3^{-1} x_4^{c} x_5^{-c} x_6^{-1}, \\ x_3^{x_1} &= x_3, & x_3^{x_7} &= x_3 x_5, \\ x_5^{x_1} &= x_3^{-1} x_5, & x_5^{x_7} &= x_5, \\ x_6^{x_1} &= x_2 x_3^{-c} x_4^{c-1} x_5 x_6, & x_6^{x_7} &= x_6. \end{aligned}$$

Then $x_1\alpha_1^{-1}$, $x_7\alpha_7^{-1} \in B$, so $x_1, x_7 \in SB$. Note that $x_1^p = x_7^p = 1$, since $p > 2$. Let K be the semi-direct product of Q by SB. Let $P = \langle Q, x_1\rangle$ and $H = \langle P, x_7\rangle$. Then calculations yield:

LEMMA 9.3. *There is a unique isomorphism ϕ of P onto $\langle Q, x_7\rangle$ such that $\phi(x_i) = x_{i+1}$, for $i = 1, 2, \ldots, 6$.*

Note that P has nilpotence class three. The proof of Lemma 5.9 can be adapted to show that P is isomorphic to $E^*(p)$. However, this will follow from Lemmas 5.9 and 9.5.

LEMMA 9.4. *We have $x_1x_7x_1 = x_7x_1x_7$. If $p = 3$, then $(x_1x_7^{-1})^2$ is an element of order two in the centre of $\langle x_1, x_7\rangle$.*

Proof. Consider Q/Q' to be a vector space over $\mathbf{Z}_p$ with basis x_2Q', x_6Q', x_3Q', x_5Q'. Then x_1 and x_7 induce automorphisms of Q/Q' represented by the matrices

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & -c & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & -1 & -1 & -c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

respectively. Hence, $x_1x_7x_1$ and $x_7x_1x_7$ are both represented by the matrix

$$\begin{bmatrix} 0 & -1 & 0 & -1-c \\ 1 & 0 & -1-c & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$$

Thus, $(x_1x_7x_1)\ (x_7x_1x_7)^{-1}$ is an element of SB that acts trivially on Q/Q'. By Lemma 9.2, $x_1x_7x_1 = x_7x_1x_7$.

Suppose that $p = 3$. Then $(x_1x_7^{-1})^2$ is represented by the diagonal matrix with every entry being -1. Apply Lemma 9.2 to the elements $(x_1x_7^{-1})^4$ and $[(x_1x_7^{-1})^2, y]$ for every $y \in SB$.

LEMMA 9.5. *For all p, x_1 is conjugate to x_7.*

Proof. By Lemma 9.4,

$$x_1 = x_7^{-1}x_1^{-1}(x_1x_7x_1) = x_7^{-1}x_1^{-1}x_7x_1x_7 = x_7^{x_1x_7}.$$

LEMMA 9.6. *Suppose that $p = 3$. Then $\langle x_1, x_7\rangle \cong$ SL(2, 3), and P is a Sylow p-subgroup of H.*

Proof. Let $L = \langle x_1, x_7\rangle$. Since $LB/B = \langle\alpha_1, \alpha_7, B\rangle/B = SB/B \cong S$, it follows that L has a homomorphic image isomorphic to SL(2, 3). Let $z = (x_1^{-1}x_7)^2$, $x = x_1z$, and $y = x_7^{-1}z$. Then, by Lemma 9.4,

$$x_1 = x^4, x_7 = y^2, \quad xy = x_1x_7^{-1}z^2 = x_1x_7^{-1}.$$

So $\langle x, y\rangle = L$ and $x^3 = y^3 = (xy)^2 = z \neq 1$. By [**2**, pp. 68–69], L is a homomorphic image of SL(2, 3). Thus, $L \cong$ SL(2, 3). Since $H = LQ$ and $|P/Q| = p$, P is a Sylow p-subgroup of H.

REFERENCES

1. R. H. Bruck, *A survey of binary systems* (Springer, Berlin, 1958).

2. H. S. M. Coxeter and W. O. J. Moser, *Generators and relations for discrete groups* (Springer, Berlin, 1957).

3. J. Currano, *Conjugate p-subgroups with maximal intersection*, Ph.D. Thesis, University of Chicago, 1970.

4. G. Glauberman, *Normalizers of p-subgroups in finite groups*, Pacific J. Math. *29* (1969), 137–144.

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

6. M. Hall, *The theory of groups* (Macmillan, New York, 1959).

7. B. Huppert, *Endliche Gruppen*. I (Springer, Berlin, 1967).

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

9. D. S. Passman, *Permutation groups* (Benjamin, New York, 1968).

10. C. C. Sims, *Graphs and finite permutation groups*, Math. Z. *95* (1967), 76–86.

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