Can. J. Math., Vol. XXV, No. 1, 1973, pp. 1–13

FINITE p-GROUPS WITH ISOMORPHIC SUBGROUPS

JOHN J. CURRANO

1. Introduction. Throughout this paper, p will denote a prime and t an integer greater than 1. We consider those finite p-groups P, which satisfy the following conditions:

(1.1) *P has subgroups R and Q, both of index p, and there is an isomorphism φ of R onto Q which does not fix any non-identity subgroup of R setwise.*

Our main results will be the following theorems.

THEOREM 1. *Let P be a finite p-group of order p^t. Then the following two statements are equivalent.*

(a) *P satisfies* (1.1).

(b) *There are integers u, v, and k and elements $x_1, \ldots, x_t$ in P satisfying:*

(1.2) $2t/3 \leqq u \leqq t$, $v = t - u$, *and* $u + v/2 \leqq k \leqq t$;

(1.3) $P = \langle x_1, \ldots, x_t \rangle$;

(1.4) $x_i^p = 1$ *for* $1 \leqq i \leqq t$;

(1.5) $[x_1, x_i] = 1$ *for* $1 \leqq i \leqq u$;

(1.6) $[x_1, x_i] \in \langle x_{v+1}, \ldots, x_{i-v} \rangle$ *for* $u + 1 \leqq i \leqq k$;

(1.7) $[x_1, x_i] \in \langle x_{k-u+1}, \ldots, x_{u+i-k} \rangle$ *for* $k + 1 \leqq i \leqq t$; *and*

(1.8) *if* $0 \leqq j < t$ *and* $[x_1, x_{1+j}] = x_2^{a(2)} \ldots x_j^{a(j)}$ *with* $a(m) \in GF(p)$, *then for any i with* $1 \leqq i \leqq t - j$, $[x_i, x_{i+j}] = x_{i+1}^{a(2)} \ldots x_{i+j-1}^{a(j)}$.

Futhermore, if P satisfies (1.1), *we also have*

(1.9) $[x_1, x_i, x_m][x_i, x_m, x_1][x_m, x_1, x_i] = 1$ *for* $1 \leqq i, m \leqq t$; *and*

(1.10) *if* $p = 2$, *then* $[x_1, x_m, x_1] = [x_1, x_m, x_m] = 1$ *for* $1 \leqq m \leqq t$.

THEOREM 2. *Let u, v, and k be integers satisfying* (1.2). *There is a group P of order p^t which satisfies* (1.1) *and which is generated by elements $x_1, \ldots, x_t$, subject to the relations* (1.4) *and*

$$[x_i, x_j] = x_i^{e(j-i+1,1)} \ldots x_j^{e(j-i+1,j-i+1)}, \tag{1.11}$$

where $e(m, n)$, $1 \leqq n \leqq m \leqq t$, are any elements of $GF(p)$ which satisfy:

Received February 16, 1971.

(1.12)

(a) $e(m, n) = 0$ *for* $1 \leqq n \leqq m \leqq u$;
(b) $e(m, n) \neq 0$ *for* $u + 1 \leqq m \leqq k$ *only if* $v + 1 \leqq n \leqq m - v$;
(c) $e(m, n) \neq 0$ *for* $k + 1 \leqq m \leqq t$ *only if* $k - u + 1 \leqq n \leqq u + m - k$;
(d) $\sum_{j=u+1}^{u+m-k} e(j, n)e(m - i + 1, j - i + 1) - e(j - i + 1, n - i + 1) \times e(m, j) = 0$ *for* $k + 2 \leqq k + i \leqq m \leqq t$ *and* $v + 1 \leqq n \leqq u$;
(e) $\sum_{j=k-u-1}^{m-u} e(i - j + 1, n - j + 1)e(m, j) - e(m - j + 1, n - j + 1) \times e(i, j) = 0$ *for* $k + 1 \leqq i \leqq m \leqq t$ *and* $v + m - k < n \leqq u$;
(f) *if* $p = 2$, $\sum_{j=u+1}^{m+u-k} e(m, j)e(j, n) = 0$ *for* $k + 1 \leqq m \leqq t$ *and* $v \leqq n \leqq m + u - k - v$; *and*
(g) *if* $p = 2$, $\sum_{j=k-u+1}^{m-u} e(m, j)e(m - j + 1, n - j + 1) = 0$ *for* $k + 1 \leqq m \leqq t$ *and* $k - u + v + 1 \leqq n \leqq m - v$.

Conversely, if a group P of order p^t satisfies (1.1), *there are integers u, v, and k satisfying* (1.2) *such that P is generated by elements $x_1, \ldots, x_t$ of order p which satisfy* (1.11) *and* (1.12).

In the proof of Theorem 2, we shall see that conditions (a)-(g) are forced by (1.3)-(1.10). Moreover, (1.5)-(1.8) are statements about the commutator structure of P which we shall derive using only this structure, (1.9) is the "Jacobi identity," and only the derivation of (1.10) will require the use of the associative structure of P; in fact, (1.10) is forced on us by this structure. With this in mind, one can check that the proofs we give for Theorems 1 and 2, and those of the facts we use from [**2**], can be modified to prove the following results.

THEOREM 1′. *Let $\mathscr{L}$ be a nilpotent Lie algebra of dimension t over a field K. Then the following two statements are equivalent:*
(1.13) *$\mathscr{L}$ has subalgebras $\mathscr{M}$ and $\mathscr{N}$, both of codimension one, and there is an isomorphism, φ, of $\mathscr{M}$ onto $\mathscr{N}$ fixing no nonzero subalgebra of $\mathscr{M}$.*
(1.14) *There are integers u, v, and k satisfying* (1.2), *and elements $x_1, \ldots, x_t$ in $\mathscr{L}$ which span $\mathscr{L}$ as a vector space over K, such that*
(a) $[x_1x_i] = 0$ *for* $1 \leqq i \leqq u$, *where* $[\ ]$ *denotes multiplication in* $\mathscr{L}$;
(b) $[x_1x_i] \in \text{Span}\{x_{v+1}, \ldots, x_{i-v}\}$ *for* $u + 1 \leqq i \leqq k$, *where* $\text{Span}\{x_r, \ldots, x_s\}$ *denotes the vector subspace of $\mathscr{L}$ spanned by $x_r, \ldots, x_s$;*
(c) $[x_1x_i] \in \text{Span}\{x_{k-u+1}, \ldots, x_{u+i-k}\}$ *for* $k + 1 \leqq i \leqq t$; *and*
(d) *if* $0 \leqq j < t$ *and* $[x_1x_{1+j}] = a_2x_2 + \ldots + a_jx_j$ *with* $a_m \in K$, *then for any i with* $1 \leqq i \leqq t - j$,

$$[x_ix_{i+j}] = a_2x_{i+1} + \ldots + a_jx_{i+j-1}.$$

THEOREM 2′. *Let K be a field and let u, v, and k satisfy* (1.2). *Then there is a nilpotent Lie algebra $\mathscr{L}$ over K with generators $x_1, \ldots, x_t$ and Lie multiplication given by*

https://doi.org/10.4153/CJM-1973-001-2 Published online by Cambridge University Press

(1.15) $[x_i x_j] = e(j-i+1,1)x_i + \ldots + e(j-i+1, j-i+1)x_j$, *where* $e(m,n)$, $1 \leqq n \leqq m \leqq t$, *are any elements of* K *which satisfy* (1.12) (a)-(e).

Furthermore, $\dim_K \mathscr{L} = t$, $\mathscr{L}^4 = 0$, *and* $\mathscr{L}$ *satisfies* (1.13).

Conversely, if a nilpotent Lie algebra $\mathscr{L}$ *of dimension* t *over* K *satisfies* (1.13), *there are integers* u, v, *and* k *satisfying* (1.2), *and elements* $x_1, \ldots, x_t$ *of* $\mathscr{L}$ *such that* $\mathscr{L} = \mathrm{Span}\{x_1, \ldots, x_t\}$ *and* (1.15) *holds. Furthermore,* $\mathscr{L}^4 = 0$.

All groups considered in this paper are assumed to be finite. If G is a group and i a positive integer, we let G_i denote the ith term of the lower central series, defined inductively by $G_1 = G$ and $G_{i+1} = [G_i, G]$. We write $H \lhd G$ if H is a *normal subgroup* of G.

Most of the results in this paper constitute a portion of the author's doctoral dissertation. Free use is made of the work of Sims [**6**] and of Glauberman [**2**]. The author is especially indebted to Professor Glauberman for his many suggestions.

2. Preliminary results.

LEMMA 2.1 (Glauberman [**2**, Proposition 2.1]). *Let* P *be a* p*-group of order* p^t *satisfying* (1.1). *Then there are elements* $x_1, \ldots, x_t$ *in* P *such that:*

(2.1) (a) $R = \langle x_1, \ldots, x_{t-1}\rangle$ *and* $P = \langle R, x_t\rangle$;
(b) $|\langle x_1, \ldots, x_i\rangle| = p^i$ *for* $1 \leqq i \leqq t$; *and*
(c) $\varphi(x_i) = x_{i+1}$ *for* $1 \leqq i \leqq t-1$.

In the remainder of this section, let P be a p-group of order p^t satisfying (1.1). Choose $x_1, \ldots, x_t$ as in Lemma 2.1.

If $P_2 \neq 1$, *let* u *be a positive integer minimal subject to* $[x_j, x_{u+j}] \neq 1$ *for some* j. *If* $P_2 = 1$, *let* $u = t$. *Let* $v = t - u$.

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

By (2.1) and induction, every $x \in P$ can be expressed uniquely in the form $x = x_1^{a(1)} \ldots x_t^{a(t)}$, where $a(i) \in GF(p)$, for $1 \leqq i \leqq t$. Define elements $e(i,j) \in GF(p)$, for $1 \leqq i, j \leqq t$, by

$$[x_1, x_i] = x_1^{e(i,1)} x_2^{e(i,2)} \ldots x_t^{e(i,t)}. \tag{2.2}$$

LEMMA 2.2 (Glauberman-Sims [**2**; **6**]). *Let* P *be a* p*-group of order* p^t *satisfying* (1.1).

(a) $u \geqq 2t/3$ *and* $k \geqq u + v/2$.
(b) *If* $P_2 \neq 1$, $[x_i, x_{u+i}] \neq 1$ *for* $1 \leqq i \leqq v$.
(c) *If* $P_3 \neq 1$, $e(k+1, u+1) \neq 0$ *or* $e(k+1, k-u+1) \neq 0$, *and* $[x_i, x_{k+i}] \notin Z(P)$ *for* $1 \leqq i \leqq t-k$.
(d) $P_4 = 1$.
(e) *For* $1 \leqq i \leqq v$, $C_P(\langle x_1, \ldots, x_{u+i}\rangle) = \langle x_{i+1}, \ldots, x_u\rangle$ *and* $C_P(\langle x_i, \ldots, x_t\rangle) = \langle x_{v+1}, \ldots, x_{u+i-1}\rangle$.

(f) $Z(P) = \langle x_{v+1}, \ldots, x_u \rangle$.
(g) $P' \subseteq \langle x_{k-u+1}, \ldots, x_k \rangle$, *which is elementary abelian.*

LEMMA 2.3 (P. Hall. [**3**, p. 19]). *Let G be any finite group. Then*
(a) $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$, *for any* $x, y, z \in G$; *and*
(b) *if* $G_4 = 1$, *then for any* $x, y, z \in G$, $[x, y, z][y, z, x][z, x, y] = 1$.

LEMMA 2.4 [**4**, p. 150]. *Let G be any finite group and* $x, y, z \in G$.
(a) $[xy, z] = [x, z][x, z, y][y, z]$.
(b) $[x, yz] = [x, z][x, y][x, y, z]$.

Lemma 2.4 is often used in calculations, even when it is not explicitly mentioned.

LEMMA 2.5 (von Dyck [**5**, Section 18]). *If a group G is given by a system of defining relations, and if a group H is given by these relations and some further relations in the same symbols, then H is isomorphic to a factor group of Q.*

3. Proof of Theorem 1. Let P be a p-group of order p^t. We first show that (a) implies (b). So assume that P satisfies (1.1). Let $x_1, \ldots, x_t$ be as in Lemma 2.1, so (1.3), (1.4), and (1.8) hold. Define u, v, and k as in Section 2, so (1.5) holds. By Lemma 2.2 and the definitions, we obtain (1.2).

Let $u + 1 \leqq i \leqq k$. Then $[x_1, x_i] \in Z(P)$ by the definition of k. If $[x_1, x_i] = 1$, (1.6) is clear. Otherwise, by Lemma 2.2(f),

$$[x_1, x_i] = {x_m}^{a(m)} \ldots {x_n}^{a(n)}, \tag{3.1}$$

where $v + 1 \leqq m \leqq n \leqq u$, $a(m) \neq 0$, and $a(n) \neq 0$. Now, $[x_{t-i+1}, x_t] \in Z(P)$ since $i \leqq k$. Also, by (3.1) and (2.1),

$$[x_{t-i+1}, x_t] = \varphi^{t-i}([x_1, x_i]) = {x_{t-i+m}}^{a(m)} \ldots {x_{t-i+n}}^{a(n)}.$$

As before, we obtain $t - i + n \leqq u$, so $n \leqq i - v$ and (1.6) holds. (1.7) is proved in a similar manner using Lemma 2.2(g). Thus (a) implies (b). Now Theorem 1 will follow from Theorem 2 and the following lemma.

LEMMA 3.1. *Let P be a p-group of order p^t satisfying* (1.2)-(1.8).
(1) *Each element $x \in P$ has a unique expression of the form $x = {x_1}^{a(1)} \ldots {x_t}^{a(t)}$ where $a(1), \ldots, a(t) \in GF(p)$.*
(2) *P satisfies* (1.9) *and* (1.10).
(3) *Define elements $e(i, j) \in GF(p)$ by*

$$[x_1, x_i] = {x_1}^{e(i,1)} \ldots {x_t}^{e(i,t)}, \quad \text{for} \quad 1 \leqq i \leqq t. \tag{3.2}$$

Then the elements $e(i, j)$, for $1 \leqq j \leqq i \leqq t$, satisfy (1.12) *and P satisfies* (1.11).
(4) *If Theorem 2 is true, P satisfies* (1.1).

We shall need the following corollary in Section 4.

https://doi.org/10.4153/CJM-1973-001-2 Published online by Cambridge University Press

COROLLARY 3.2. *Let P be a p-group of order p^t satisfying* (1.1), *let $x_1, \ldots, x_t$ be as in Lemma* 2.1, *and let u, v, and k be as in Section* 2. *Then P satisfies* (1.11) *and* (1.12).

Proof. By the portion of Theorem 1 which we have proved, P satisfies (1.2)-(1.8). The corollary follows from Lemma 3.1(3).

Proof of Lemma 3.1. (1) is clear from (1.2)-(1.8), as is

$$[x_i, x_j] \in \langle x_{k-u+1}, \ldots, x_k \rangle, \quad \text{for} \quad 1 \leqq i, j \leqq t. \tag{3.3}$$

Let $T = \langle x_{k-u+1}, \ldots, x_k \rangle$. Using (1.2), (1.6), and (1.8), we obtain

$$[x_i, x_j] \in \langle x_{v+1}, \ldots, x_u \rangle \quad \text{for} \quad 1 \leqq i \leqq t, x_j \in T. \tag{3.4}$$

Now, $S = \langle x_{v+1}, \ldots, x_u \rangle \subseteq Z(P)$ by (1.2) and (1.5), so it follows from (3.4) that

$$[P,T] \subseteq S \subseteq T \cap Z(P). \tag{3.5}$$

Therefore, $T \subseteq Z_2(P)$ and $T \lhd P$. By (3.3), $P' \subseteq T \subseteq Z_2(P)$, so $P_4 = 1$. Now (1.9) follows from Lemma 2.3(b).

Assume $p = 2$. By (1.4) and Lemma 2.4, we obtain

$$1 = [x_1^2, x_m] = [x_1, x_m][x_1, x_m, x_1][x_1, x_m], \text{ and}$$
$$1 = [x_1, x_m^2] = [x_1, x_m]^2[x_1, x_m, x_m].$$

But T is elementary abelian by (1.4), (1.5), and (1.8), so $[x_1, x_m]^2 = 1$ for $1 \leqq m \leqq t$. Furthermore, $P_3 \subseteq Z(P)$ since $P_4 = 1$. Now (1.10) follows. This completes the proof of (2).

By (1.5)-(1.8), $[x_i, x_j] = x_i^{e(j-i+1,1)} \ldots x_j^{e(j-i+1,j-i+1)}$ and

$$e(m, n) = 0 \quad \text{for} \quad 1 \leqq m < n \leqq t. \tag{3.6}$$

We now show (*a*)-(*g*) of (1.12).

(a) follows from (1.5), (b) from (1.6), and (c) from (1.7). Let S be as in the proof of (2) and let $k + 2 \leqq m \leqq t$ and $2 \leqq i \leqq m - k$. Then $m - k < u$, so $[x_1, x_i] = 1$. Therefore, (1.9) implies that

$$[x_i, x_m, x_1] = [x_m, x_1, x_i]^{-1}.$$

Expanding this, using (3.2), (3.6), (1.5)-(1.8), and the fact that $S \subseteq Z(P)$, we obtain

$$\prod_{j=u+1}^{u+m-k} [x_1, x_j]^{e(m-i+1, j-i+1)} = \prod_{j=u+1}^{u+m-k} [x_i, x_j]^{e(m,j)}.$$

Expanding this and collecting factors, we obtain

$$\prod_{j=u+1}^{u+m-k} \prod_{n=v+1}^{j-v+1} x_n^{e(j,n)e(m-i+1, j-i+1) - e(j-i+1, n-i+1)e(m,j)} = 1.$$

(The order of the factors x_n is unimportant as $x_n \in S \subseteq Z(P)$.) By (1), the

https://doi.org/10.4153/CJM-1973-001-2 Published online by Cambridge University Press

exponents appearing for each x_n must sum to zero. This gives (1.12)(d). (e) follows in the same way from (1.9) with $k+1 \leqq i \leqq m \leqq t$.

If $p = 2$, (1.12)(f) and (g) are proved from (1.10) in a similar manner, using $[x_1, x_m, x_1] = 1$ for (f) and $[x_1, x_m, x_m] = 1$ for (g), with $k+1 \leqq m \leqq t$. This completes the proof of (3).

Now assume Theorem 2 is true. By (1.2), (1.4), and (3), P satisfies the hypotheses of Theorem 2. Thus P satisfies (1.1). This completes the proof of Lemma 3.1.

4. A reduction. The second half of Theorem 2 follows from Corollary 3.2. So suppose P is a p-group generated by elements $x_1, \ldots, x_t$ subject to relations (1.2), (1.4), and (1.11), as in Theorem 2. Let $T = \langle x_{k-u+1}, \ldots, x_k \rangle$. Then T is elementary abelian and $P' \subseteq T$ by (1.2), (1.11), and (1.12). Therefore, $|T| \leqq p^u$, and by (1.4), P/T is elementary abelian of order at most p^{t-u}. Thus $|P| \leqq p^t$.

So to prove Theorem 2, it suffices to construct a group H of order p^t satisfying (1.2), (1.4), and (1.11), and to show that H satisfies (1.1). For then H will be a homomorphic image of P by Lemma 2.5, so P will be isomorphic to H and therefore have order p^t and satisfy (1.1).

The remainder of the paper is devoted to the construction of a group H with the desired properties.

5. The Case $k = t$. We first construct H when $k = t$. This corresponds to those cases in Theorem 2 when $P_3 = 1$.

THEOREM 5.1. *Let $u = k = t$. Let H be an elementary abelian group of order p^t and let $\{x_1, \ldots, x_t\}$ be a basis of H. Then* (1.2), (1.4), *and* (1.11) *are satisfied. Define an automorphism φ of H by $\varphi(x_i) = x_{i+1}$ for $1 \leqq i \leqq t-1$, and $\varphi(x_t) = x_1$. Then H and $\varphi|\langle x_1, \ldots, x_{t-1} \rangle$ satisfy* (1.1).

Proof. This is immediate, since (1.12)(b)-(g) are vacuous.

In the remainder of this section assume that $k = t$ and $2t/3 \leqq u < t$. Then (1.12)(c)-(g) are vacuous. Assume that $e(i, j)$, for $1 \leqq i, j \leqq t$, are elements of $GF(p)$ which satisfy (1.12) if $j \leqq i$ and which are zero otherwise.

Define, for $1 \leqq i, j, m \leqq t$,

(5.1) $e(i, j, m) = e(j - i + 1, m - i + 1)$ for $1 \leqq i \leqq j, m \leqq t$, and
$e(i, j, m) = 0$ otherwise.

Let $H = \{(a_1, \ldots, a_t) | a_i \in GF(p)$ *for* $1 \leqq i \leqq t\}$, a set with $|H| = p^t$. Define a product on H by

$$(a_1, \ldots, a_t)(b_1, \ldots, b_t) = (c_1, \ldots, c_t),$$

where

$$c_m = a_m + b_m - \sum_{i=1}^{t-1} \sum_{j=i+1}^{t} e(i, j, m) a_j b_i, \quad \text{for} \quad 1 \leqq m \leqq t.$$

https://doi.org/10.4153/CJM-1973-001-2 Published online by Cambridge University Press

Define $x_i \in H$ by $x_i = (\delta_{i1}, \ldots, \delta_{it})$ for $1 \leqq i \leqq t$, where δ_{ij} is the Kronecker delta.

LEMMA 5.2 (a) *H is a group of order p^t.*
(b) $[x_i, x_j] = x_1^{e(i,j,1)} \ldots x_t^{e(i,j,t)}$, *for* $1 \leqq i \leqq j \leqq t$.
(c) $x_i^p = 1$, *for* $1 \leqq i \leqq t$.

Proof. Denote $(a_1, \ldots, a_t) \in H$ by (a_m).

Clearly $(0, 0, \ldots, 0)$ is an identity for H. If $(a_m) \in H$, let

$$(b_m) = \left(-a_m - \sum_{i=1}^{t-1} \sum_{j=i+1}^{t} e(i, j, m) a_i a_j\right) \tag{5.2}$$

and $(a_m)(b_m) = (c_m)$. Then a straightforward calculation shows that

$$c_m = \sum e(r, s, m) e(i, j, r) a_i a_j a_s, \tag{5.3}$$

where the sum is over all r, s, i, and j with $1 \leqq r < s \leqq t$ and $1 \leqq i < j \leqq t$. Now, if $e(r, s, m)e(i, j, r)$ is nonzero in some term, then by (5.1) $r \geqq v + i \geqq v + 1$ (otherwise $e(i, j, r) = 0$) and $s - r \geqq u$ (otherwise $e(r, s, m) = 0$); that is $s \geqq r + u \geqq v + 1 + u = t + 1$, which is impossible. Thus $(c_m) = (0, \ldots, 0)$, and (b_m) is a right inverse to (a_m).

Thus to show that H is a group under the given multiplication, it remains to verify the associative law. Let (a_m), (b_m), $(c_m) \in H$ and define $(d_m) = \{(a_m)(b_m)\}(c_m)$ and $(f_m) = (a_m)\{(b_m)(c_m)\}$. Then

$$d_m - f_m = \sum [e(r, s, n)e(i, j, s)a_j b_i c_r - e(r, s, n)e(i, j, r)a_s b_j c_i], \tag{5.4}$$

where the sum is as in (5.3). So it would suffice to show that each term of (5.4) is zero. Arguing as before, we see that $e(r, s, n)e(i, j, s) \neq 0$ in some term of (5.4) implies that $s \geqq r + u \geqq u + 1$ and that $s \leqq j - v$. Therefore, $t + 1 \leqq j$, which is a contradiction. We also obtain a contradiction if $e(r, s, n)e(i, j, r) \neq 0$, so each term in (5.4) is zero. Thus $(d_m) = (f_m)$ and H is a group.

Now we show (b). By (5.1), $[x_i, x_i] = 1 = x_1^{e(i,i,1)} \ldots x_t^{(i,i,t)}$, while for $1 \leqq i < j \leqq t$, a direct calculation leads to

$$[x_i, x_j] = x_i^{-1} x_j^{-1} x_i x_j = x_1^{e(i,j,1)} \ldots x_t^{e(i,j,t)}.$$

Finally, using induction we obtain $x_m^p = (0, \ldots, 0)$, and the lemma is proved.

By the preceding lemma and the definitions, H is a group of order p^t satisfying (1.2), (1.4), and (1.11). So to complete the proof of Theorem 2 in the case $k = t$, we must prove that H satisfies (1.1).

LEMMA 5.3. (a) $|\langle x_1, \ldots, x_i \rangle| = p^i$ *for* $1 \leqq i \leqq t$.
(b) *Each $x \in H$ has a unique expression of the form $x = x_1^{a(1)} \ldots x_t^{a(t)}$ for some elements $a(1), \ldots, a(t) \in GF(p)$.*

Proof. Let $H_i = \langle x_1, \ldots, x_i \rangle$ for $1 \leqq i \leqq t$. By Lemma 5.2(b) and (5.1),

https://doi.org/10.4153/CJM-1973-001-2 Published online by Cambridge University Press

$[x_j, x_{i+1}] \in H_i$ for $1 \leqq j \leqq i$. Thus, $H_i \lhd H_{i+1}$ and $H_{i+1} = H_i\langle x_{i+1}\rangle$, so by Lemma 5.2(c), $|H_1| = p$ and $|H_{i+1} : H_i| \leqq p$. Therefore, letting $H_0 = 1$,

$$p^t = |H| = \prod_{i=1}^{t} |H_i : H_{i-1}| \leqq p^t.$$

Therefore, $|H_i : H_{i-1}| = p$ for $1 \leqq i \leqq t$, so $|H_i| = p^i$. In particular, $x_i \notin H_{i-1}$. Now (b) follows by an easy induction.

LEMMA 5.4. *Let $R = \langle x_1, \ldots, x_{t-1}\rangle$ and $Q = \langle x_2, \ldots, x_t\rangle$. Then there is an isomorphism φ of R onto Q with $\varphi(x_i) = x_{i+1}$ for $1 \leqq i \leqq t-1$. In particular, H, R, Q, and φ satisfy* (1.1).

Proof. Let G be the group defined by generators $g_1, \ldots, g_{t-1}$ and relations:

$$(5.5) \qquad g_t^{\,p} = 1 \quad \text{for} \quad 1 \leqq i \leqq t-1; \text{ and}$$
$$[g_i, g_j] = g_1^{e(i,j,1)} \ldots g_{t-1}^{e(i,j,t-1)} \quad \text{for} \quad 1 \leqq i \leqq j \leqq t-1.$$

Then, since $e(i, j, m) = 0$ if $m \leqq i$ or $m \geqq j$, each element g of G has an expression of the form $g = g_1^{a(1)} \ldots g_{t-1}^{a(t-1)}$, with the $a(i) \in GF(p)$; so $|G| \leqq p^{t-1}$. By (5.5) and Lemmas 5.2 and 2.5, the mapping ψ given by $\psi(g_i) = x_i$ for $1 \leqq i \leqq t-1$, extends to a homomorphism, ψ, of G onto R. But $|R| = p^{t-1}$, so $|G| = p^{t-1}$ and ψ is an isomorphism. Similarly, the mapping θ given by $\theta(g_i) = x_{i+1}$ for $1 \leqq i \leqq t-1$, extends to an isomorphism, θ, of G onto Q, since

$$e(i+1, j+1, m+1) = e(m-i+1, m-j+1) = e(i, j, m).$$

Let $\varphi = \psi^{-1}\theta$. Then φ is the desired isomorphism. An easy calculation, using Lemma 5.3(b), shows the last statement.

This completes the construction of H in the case $k = t$.

6. The Case $k < t$. Now we construct H when $k < t$, using an inductive argument. Let u, v, and k be any integers satisfying (1.2) with $k < t$. This corresponds to those cases in Theorem 2 when class $P = 3$. (By Lemma 2.2, class $P \leqq 3$.)

Let $e(i, j)$, for $1 \leqq i, j \leqq t$, be elements of $GF(p)$ which satisfy (1.12) if $j \leqq i$ and which are zero otherwise. Define elements $e(i, j, m)$ of $GF(p)$, for $1 \leqq i, j, m \leqq t$, as in (5.1).

Let $H = \{(a_1, \ldots, a_t) | a_i \in GF(p)\}$, a set with p^t elements. For $1 \leqq m \leqq t$, let $H^{(m)}$ be the subset $\{(a_1, \ldots, a_t) | a_{m+1} = \ldots = a_t = 0\}$ of H, so that $|H^{(m)}| = p^m$. Let φ be the map of $H^{(t-1)}$ into H given by $\varphi(a_1, \ldots, a_{t-1}, 0) = (0, a_1, \ldots, a_{t-1})$. For $1 \leqq i \leqq t$, let $x_i = (\delta_{i1}, \ldots, \delta_{it}) \in H$.

Define multiplication in $H^{(k)}$ by

$$(6.1) \quad (a_1, \ldots, a_k, 0, \ldots, 0)(b_1, \ldots, b_k, 0, \ldots, 0) = (c_1, \ldots, c_k, 0, \ldots, 0)$$

where

$$c_m = a_m + b_m - \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} e(i, j, m) a_j b_i, \quad \text{for} \quad 1 \leqslant m \leqslant k.$$

https://doi.org/10.4153/CJM-1973-001-2 Published online by Cambridge University Press

We now proceed to define inductively a multiplication on $H^{(m)}$, $k+1 \leqq m \leqq t$, and to show that $H^{(m)}$ satisfies (1.1).

So let $k+1 \leqq m \leqq t$. By induction, we may assume that

(6.2) (a) $H^{(i)}$ is a group of order p^i, $1 \leqq i \leqq m-1$;
(b) $x_1^{a(1)} \dots x_{m-1}^{a(m-1)} = (a(1), \dots, a(m-1), 0, \dots, 0)$;
(c) $\varphi | H^{(m-2)}$ is an isomorphism of $H^{(m-2)}$ into $H^{(m-1)}$ with $\varphi(x_i) = x_{i+1}$ for $1 \leqq i \leqq m-2$;
(d) $[x_i, x_j] = x_1^{e(i,j,1)} \dots x_{m-1}^{e(i,j,m-1)}$ for $1 \leqq i \leqq j \leqq m-1$;
(e) $Z(H^{(m-1)}) \supseteq \langle x_{m-u+1}, \dots, x_u \rangle \supseteq \langle x_{v+1}, \dots, x_u \rangle$; and
(f) $(H^{(m-1)})' \subseteq \langle x_{k-u+1}, \dots, x_{u+(m-1)-k+1} \rangle \subseteq \langle x_{k-u+1}, \dots, x_k \rangle$.

(Note that for $m = k+1$, (6.2) follows from (6.1), (5.1), and Lemmas 5.2, 5.3, and 5.4.)

Let $F = H^{(m)}$, $R = H^{(m-1)}$, and $Q = \varphi(R)$. Define a multiplication on Q by

$$\varphi(a)\varphi(b) = \varphi(ab) \text{ for } a, b \in R. \tag{6.4}$$

This makes Q a group and φ an isomorphism of R with Q. Also, by (6.2)(c), if $\varphi(a)$ and $\varphi(b)$ lie in $R \cap Q$, then multiplication in Q and in R agree.

If $2 \leqq i \leqq m$, we see, using (5.1), that

$$[x_i, x_m] = \varphi([x_{i-1}, x_{m-1}]) = x_1^{e(i,m,1)} \dots x_m^{e(i,m,m)}.$$

Therefore, combining this with (6.2)(d), we obtain

$$[x_i, x_j] = x_1^{e(i,j,1)} \dots x_m^{e(i,j,m)} \quad \text{for} \quad 1 \leqq i \leqq j \leqq m-1 \text{ or } 2 \leqq i \leqq j \leqq m. \tag{6.5}$$

Let $S = R \cap Q$, so that $S \lhd R$ and $S \lhd Q$. We inductively make the following definitions:

(6.6) (a) $\{x_1, x_m\} = x_1^{e(1,m,1)} \dots x_m^{e(1,m,m)}$;
(b) $\{x_1^{a+1}, x_m\} = \{x_1^a, x_m\}[\{x_1^a, x_m\}, x_1]\{x_1, x_m\}$, for $1 \leqq a \leqq p-2$;
(c) $\{x_1^a, x_m^{c+1}\} = \{x_1^a, x_m\}\{x_1^a, x_m^c\}[\{x_1^a, x_m^c\}, x_m]$, for a fixed a, $1 \leqq a \leqq p-1$, and for $1 \leqq c \leqq p-2$;
(d) $\{x_m^c, x_1^a\} = \{x_1^a, x_m^c\}^{-1}$ for $1 \leqq a, c \leqq p-1$; and
(e) $\{x_1^a, x_m^c\} = 1$ if $ac \equiv 0 \pmod{p}$.

All the elements defined in (6.6) lie in S.

Write the element, $(a_1, \dots, a_m, 0, \dots, 0)$, of F as (a_1, x, a_m), where $x = (0, a_2, \dots, a_{m-1}, 0, \dots, 0) \in S$.

Define multiplication in F by

$$(a, x, b)(c, y, d) = (a + c, (x_1^{-c} x x_1^c)\{x_m^b, x_1^c\}[x_m^b, \{x_m^b, x_1^c\}] \times (x_m^b y x_m^{-b}), b + d). \tag{6.7}$$

(All the factors appearing in the middle expression on the right lie in Q, so we may associate anyway we please.)

https://doi.org/10.4153/CJM-1973-001-2 Published online by Cambridge University Press

LEMMA 6.1. *Under the multiplication defined in* (6.8), $(0, \ldots, 0) = (0, 1, 0)$ *is an identity for* F *and every element of the set* $R \cup Q$ *has an inverse in* F.

Proof. We observe that multiplication of elements of R (respectively Q) in F and in R (respectively Q) yield the same result. Now the lemma is obvious.

LEMMA 6.2. (a) $\{x_1{}^a, x_m{}^c\} = ((x_1{}^{-a}x_m{}^{-c})x_1{}^a)x_m{}^c = [x_1{}^a, x_m{}^c]$ *for all* $a, c \in GF(p)$.

(b) $[x_i, x_j] \in \langle x_{k-u+1}, \ldots, x_k \rangle$.

(c) $[x_i, x_j, x_n] \in \langle x_{v+1}, \ldots, x_u \rangle \subseteq Z(R) \cap Z(Q)$ *for* $1 \leqq i, j, n \leqq m$. *Thus,* $[[x_i, x_j, x_n], x] = 1$ *for all* $x \in F$.

(d) *If* $p = 2$, $[x_1, x_m, x_1] = [x_1, x_m, x_m] = 1$.

Proof. If $x, y \in R$ or $x, y \in Q$, let $\{x, y\} = [x, y]$. Then, if $1 \leqq i \leqq j \leqq m$, $\{x_i, x_j\} \in \langle x_{k-u+1}, \ldots, x_k \rangle$ by (6.2)(f), (6.4), and (1.12). These, together with (6.2)(e), yield

$$[\{x_i, x_j\}, x_n] \in \langle x_{v+1}, \ldots, x_u \rangle \subseteq Z(R) \cap Z(Q) \tag{6.8}$$

for $1 \leqq i, j, n \leqq m$, so (b) and (c) will follow from (a).

(d) will follow from (a) and

$$\text{if } p = 2, [\{x_1, x_m\}, x_1] = [\{x_1, x_m\}, x_m] = 1. \tag{6.9}$$

But, by (6.2) and (1.12),

$$\begin{aligned}[\{x_1, x_m\}, x_1] &= \prod_{j=u+1}^{m+u-k} [x_j, x_1]^{e(1,m,j)} \\ &= \prod_{j=u+1}^{m+u-k} \left(\prod_{n=v}^{j-v} x_n{}^{-e(1,j,n)\,e(1,m,j)} \right).\end{aligned} \tag{6.10}$$

The exponent appearing for x_n, $v \leqq n \leqq m + u - v - k \leqq k$, in (6.10) is

$$-\sum_{j=u+1}^{n+v} e(1, j, n)e(1, m, j) = -\sum_{j=u+1}^{n+v} e(j, n)e(m, j) = 0$$

by (1.12)(b) and (f). Thus $[\{x_1, x_m\}, x_1] = 1$.

A similar argument, using (1.12)(g) in place of (f), shows the rest of (6.9). Therefore, (d) will follow from (a).

We next prove that

$$[\{x_i{}^a, x_j{}^b\}{}^c, x_n{}^d] = [\{x_i, x_j\}, x_n]^{abcd} \tag{6.11}$$

for $1 \leqq i, j, n \leqq m$ and $0 \leqq a, b, c, d \leqq p - 1$. Let $1 \leqq i, j, n \leqq m$ and let $y = \{x_i, x_j\}$. Then, using (6.8) and induction, we obtain

$$[y^a, x_n] = [y, x_n]^a, [y, x_n{}^a] = [y, x_n]^a, \quad \text{and} \quad [x_i{}^a, x_j{}^b] \equiv y^{ab}$$

modulo $Z(R) \cap Z(Q)$, for $0 \leqq a, b \leqq p - 1$. These now yield (6.11).

Using (6.8)-(6.11) and Lemma 2.5, and calculating, we obtain

$$\begin{aligned}[x_1^a, x_m^c] &= \{x_1^a, x_m^{p-c}\}^{-1}[x_m^{p-c}, \{x_m^{p-c}, x_1^a\}] \\ &= \left(\prod_{i=1}^{p-c-1} (\{x_1^a, x_m\}[\{x_1^a, x_m^{p-c-i}\}, x_m])\{x_1^a, x_m\}\right)^{-1} [\{x_1, x_m\}, x_m]^{ac^2} \\ &= \{x_1^a, x_m\}^{-(p-c)}[\{x_1, x_m\}, x_m]^{-a(p-c)(p-c-1)/2+ac^2}.\end{aligned}$$

Then we obtain

$$[x_1^a, x_m^c] = \{x_1^a, x_m\}^c[\{x_1, x_m\}, x_m]^{(ac^2-ac)/2} \tag{6.12}$$

by calculation if $p > 2$ and by (6.9) if $p = 2$.

Finally, applying (6.6), (6.11), and induction to (6.12), we obtain (a). This completes the proof of the lemma.

We now summarize the facts we shall require about commutators.

LEMMA 6.3. (a) $[x_i, x_j] = x_1^{e(i,j,1)} \dots x_m^{e(i,j,m)}$ *for* $1 \leqq i, j \leqq m$.

(b) $[x, y, z] \in Z(R) \cap Z(Q)$, $[[x^a, y^b]^c, z^d] = [x, y, z]^{abcd}$, *and* $[[x, y], [z, w]] = 1$, *for any* x, y, z, w *in the set* $T = S \cup \{x_1^e, x_m^e | e \in GF(p)\}$ *and any* $a, b, c, d \in GF(p)$.

(c) $[x_1^a, x_m^c] = [x_1, x_m]^{ac}[x_1, x_m, x_1]^{(ca^2-ca)/2}[x_1, x_m, x_m]^{(ac^2-ac)/2}$ *for any* $a, c \in GF(p)$.

Proof. (a) follows from (6.5) and (6.6).

The first part of (b) follows from Lemma 6.2. Then the second part is proved in the same way as (6.11). Finally, by Lemma 6.2(b) and induction, $[x, y]$ and $[z, w]$ lie in $\langle x_{k-u+1}, \dots, x_k \rangle$, which is an elementary abelian subgroup of R by (1.12) and the definitions. This completes the proof of (b).

(c) follows from (6.12) and a further argument similar to that preceding (6.12).

LEMMA 6.4. *The associative law holds in* F, *so* F *is a group under the multiplication defined in* (6.7).

COROLLARY 6.5. (6.2) *holds with* m *replaced by* $m + 1$.

Proof. By Lemma 6.4, $F = H^{(m)}$ is a group. (a)-(d) are clear from (6.2) in R, the definitions, and Lemma 6.3. (e) and (f) follow from the definitions, (1.12) and Lemma 6.3.

Before proving Lemma 6.4, we complete the proof of Theorem 2. By Lemma 6.4 and induction on m, $H = H^{(t)}$ is a group satisfying (6.2) with $m = t + 1$. Let $R = H^{(t-1)}$ and $Q = \varphi(R)$. Then, by (a), $|H:R| = |H:Q| = p$, and by (c), φ can fix no non-identity subgroup of R. Thus H, R, Q, and φ satisfy (1.1), which completes the proof of Theorem 2.

Proof of Lemma 6.4. We make repeated use of Lemma 6.3. If (a, x, b), (c, y, d), and (f, z, g) are in F, a direct calculation shows that

$$((a, x, b)(c, y, d))(f, z, g) = (a + c + f, X_1X_2, b + d + g) \text{ and}$$
$$(a, x, b)((c, y, d)(f, z, g)) = (a + c + f, Y_1Y_2, b + d + g),$$

where

$$X_1 = x[x, x_1^{c+f}][x_m^b, x_1^c][x_m^b, x_1^c, x_1^f][x_m^b, [x_m^b, x_1^c]]y[y, x_m^{-b}],$$
$$X_2 = [y[y, x_m^{-b}], x_1^f][x_m^{b+d}, x_1^f][x_m^{b+d}, [x_m^{b+d}, x_1^f]]z[z, x_m^{-b-d}],$$
$$Y_1 = x[x, x_1^{c+f}][x_m^b, x_1^{c+f}][x_m^b, x_1^{c+f}, x_m^b]^{-1}y[y, x_1^f][y[y, x_1^f], x_m^{-b}], \text{ and}$$
$$Y_2 = [x_m^d, x_1^f][x_m^d, x_1^f, x_m^{-b}][x_m^d, x_1^f, x_m^d]^{-1}z[z, x_m^{-b-d}].$$

Expanding these expressions, using Lemma 6.3, collecting commutators of length 3, and comparing the resulting expressions, we observe that it would suffice to show that $[y, x_m, x_1]^{-bf} = [x_1, x_m, y]^{-bf}[y, x_1, x_m]^{-bf}$, or

$$[x_m, y, x_1][x_1, x_m, y][y, x_1, x_m] = 1. \tag{6.13}$$

However, using Lemma 6.3, we obtain

$$[x_m, y_1y_2, x_1] = [x_m, y_1, x_1][x_m, y_2, x_1]$$

and similar statements about the other two triple commutators appearing, so it suffices to show (6.13) for $y = x_i$, $2 \leqq i < m$. So let $a = [x_m, x_i, x_1]$, $b = [x_1, x_m, x_i]$, and $c = [x_i, x_1, x_m]$. We consider three cases.

Case 1. If $2 \leqq i \leqq m - k$, $c \in [Z(F), x_m] = 1$ (here $Z(F)$ is the set of all elements of F which commute with every element of F) by Lemma 6.3(a), (6.1), and (1.12). Furthermore, using these and expanding, we also see that

$$ab = \prod_{n=v+1}^{u+m-k-v+i} x_n^{a(n)},$$

where
$$\begin{aligned} a(n) &= \sum_{j=u+1}^{u+m-k} e(1, j, n)e(i, m, j) - e(i, j, m)e(1, m, j) \\ &= \sum_{j=u+1}^{u+m-k} e(j, n)e(m - i + 1, j - i + 1) \\ &\qquad - e(j - i + 1, n - i + 1)e(m, j) \\ &= 0 \end{aligned}$$

by (1.12)(d). Thus $abc = 1$ in this case.

Case 2. If $m - k < i \leqq k$, then $a = b = c = 1$ by Lemma 6.3, (6.1), and (1.12).

Case 3. If $k < i < m$, then $a = 1$ and $bc = 1$ by arguments similar to those in Case 1, with the roles of a and c interchanged, and with (1.12)(d) replaced by (1.12)(e) in the last step.

This completes the proof of (6.13), the lemma, and Theorem 2.

References

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

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

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

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

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

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

Roosevelt University,
Chicago, Illinois