J. Austral. Math. Soc. **22** (Series A) (1976), 221–233.

# $p$-GROUPS WITH AN ABELIAN MAXIMAL SUBGROUP AND CYCLIC CENTER

S. B. CONLON

(Received 22 April 1974; revised 11 April 1975)

**Abstract**

All such nonabelian finite $p$-groups are classified. They coincide with the class of nonabelian finite $p$-subgroups of $GL(p, F)$, where $F$ is a field, not of characteristic $p$, which contains all $p$ power roots of 1, or again with the class of all nonabelian finite subgroups of $\mathbf{Z}_{p^\infty} \, wr \, \mathbf{Z}_p$. Various automorphism groups associated to them and their representations are calculated. Two such subgroups of $GL(p, F)$ are conjugate as subgroups of $GL(p, F)$ iff they are isomorphic.

## Introduction

Let $G$ be a nonabelian finite $p$-group with an abelian maximal subgroup $M$ and cyclic center. As $G$ has cyclic center, it has faithful irreducible representations. As $G$ has an abelian maximal subgroup, these must have degree $p$. Hence $G$ is isomorphic to a subgroup of $GL(p, F)$, where $F$ is the complex numbers, for instance.

If now $G$ is any nonabelian finite $p$-subgroup of $GL(p, F)$, where $F$ is a field with all $p$ power roots of 1 and has characteristic not equal to $p$, this realization of $G$ is similar to a group of monomial matrices. Let $W(\approx \mathbf{Z}_{p^\infty})$ be the $p$-torsion subgroup of $F^\times(= F - \{0\})$. We identify $A = W \times \cdots^{(p)} \cdots \times W$ with the corresponding group of diagonal matrices in $GL(p, F)$. The permutational matrices corresponding to the monomial matrices of $G$ can be taken to be powers of

$$(0.1) \qquad x = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

Thus $(w_1, \cdots, w_p)^x = (w_2, \cdots, w_p, w_1)$ $(w_i \in W)$. Then $G$ is a subgroup of $P = \langle A, x \rangle \approx \mathbf{Z}_{p^\infty} \, wr \, \mathbf{Z}_p$.

Finally let $G$ be any nonabelian finite subgroup of $P$. Then $M = G \cap A$ is an abelian maximal subgroup of $G$. The center $Z = Z(P)$ of $P$ is the set of scalar elements in $A = W^{(p)}$, i.e. $Z \approx W \approx \mathbf{Z}_{p^\infty}$. As $G$ is nonabelian, its center is $G \cap Z$ and so is cyclic. This shows the equivalence of the three classes of $p$-groups mentioned in the abstract.

Various methods of attack exist. One can use Szekeres' classification (Szekeres (1949) and Nazarova, et al. (1972)) of all finite $p$-groups with an abelian maximal subgroup. However those with cyclic center can be found more directly. The author's original approach was to look for minimal nonabelian $p$-subgroups of $GL(p, F)$ and construct inductively all $p$-overgroups of those. The approach here will be to write down all nonabelian finite subgroups of $P(\approx \mathbf{Z}_{p^\infty} \, wr \, \mathbf{Z}_p)$. The author is grateful to the referee for pointing out that this approach is the more economical.

Szekeres' techniques will be used to advantage. His method is to study the structure of the abelian maximal subgroup $M$ of $G$ as a $\mathbf{Z}(G/M)$-module. This is carried out in section 1. The extension problem from $M$ to $G$ is resolved in section 2 and generators and relations given. Orbits of such $G$ under $Aut\, P$ are determined. In section 3 the isomorphism problem is resolved. In section 4, it is shown that the conjugacy classes in $GL(p, F)$ coincide with the isomorphism classes. Examples and further properties are given in section 5. Section 6 is devoted to $Aut\, G$ and in particular to the subgroup $SA(G)$, consisting of those automorphisms of $G$ realized as similarity transformations in $GL(p, F)$. It is found that $Aut\, G$ is the product $B \cdot SA$ of disjoint subgroups, where $B$ permutes faithfully (and transitively) the different faithful irreducible representations of $G$. In section 7 the representations of $G$ are discussed.

The notations of $W(\approx \mathbf{Z}_{p^\infty}) \leqq F^\times$ and of $Z = Z(P)$, $A = W^{(p)}$, $G$ and $M = G \cap A$ considered as subgroups of $P$, with this last in turn being embedded in $GL(p, F)$, will hold throughout.

An investigation has also been completed of $p$-subgroups of classical groups derived from linear groups of degree $p$ over any field $F$ (perhaps finite), not of characteristic $p$.

I wish to thank Dr. John Cannon and Miss Robyn Gallagher of Sydney University who checked the presentations of these groups on the computer and also Dr. Gordon Elkington for helpful discussions.

## 1. Normal subgroups of $P$ lying in $A$

An element $g \in G - M$ has form $g = x^n m$ $(0 < n < p,\ m \in M)$ and acts on $M$ just as $x^n$ does. Set $X = \langle x \rangle$. To obtain all possibilities for the abelian maximal subgroup $M = G \cap A$ of $G$, we look at finite $X$-modules ($\mathbf{Z}(X)$-modules) $M$ lying in $A$ or equivalently finite normal subgroups $M$ of $P$, contained in $A$.

We distinguish two $X$-submodules of $A$: $Z = Z(P)$ and $Y = \{(w_1, \cdots, w_p) \in A \mid \Pi w_i = 1\}$. Clearly $A = Y \curlyvee Z$, with the subgroup of $Z$ of order $p$ being amalgamated.

In the group algebra $\mathbf{Z}(X)$, write

$$\phi = x - 1 \quad \text{and} \quad \pi = 1 + x + \cdots + x^{p-1};$$

we regard $\phi$ and $\pi$ as abelian group endomorphisms of $A$. As $x^p = 1$, we have $\phi\pi = \pi\phi = 1$. From the corresponding polynomial identity in $x$ we have that

$$\pi = \binom{p}{1} + \binom{p}{2}\phi + \cdots + \binom{p}{p}\phi^{p-1}.$$

Thus for $a$ in $A$ we have:

$$\phi\colon a \mapsto [a, x] \tag{1.1}$$

$$\text{and} \quad \pi\colon a \mapsto a^{\binom{p}{1}}[a, x]^{\binom{p}{2}} \cdots [a, x, \cdot\cdot\overset{(p-1)}{\cdots}\cdot\cdot, x]^{\binom{p}{p}}.$$

LEMMA 1.2. *If $y \in Y$, then $\exists y' \in Y$ such that $y = y'^{\phi}$. Thus $Y = P'$. $Y$, $Z$ and $A = \langle Y, Z\rangle$ are characteristic in $P$ and any automorphism of $P$ sends an $X$-submodule $M$ of $A$ to another $X$-submodule of $A$.*

PROOF. Suppose $y = (w_1, \cdots, w_p) \in Y$ and so $\Pi w_i = 1$. Set $y' = (1, w_1, w_1 w_2, \cdots, w_1 \cdots w_{p-1})$ and then $y'^{\phi} = y$. The rest is immediate. Q.E.D.

LEMMA 1.3. *$Z = ker\,\phi = im\,\pi$ and $Y = ker\,\pi = im\,\phi$.*

PROOF. The following inclusions are clear:

$$im\,\pi \leqq ker\,\phi \leqq Z \quad \text{and} \quad Y \leqq im\,\phi \leqq ker\,\pi.$$

As $Z\,(\approx \mathbf{Z}_{p^\infty})$ is divisible and $z^{\pi} = z^p$ for $z$ in $Z$, we have $Z \leqq im\,\pi$.

Take $a \in ker\,\pi$ and so $a \cdot a^x \cdots a^{x^{p-1}} = 1$. If $a = (w_1, \cdots, w_p)$, $x$ permutes cyclically the coordinates and so each coordinate of $a \cdot a^x \cdots a^{x^{p-1}}$ is $\Pi w_i$, i.e. $a \in Y$. Thus $ker\,\pi \leqq Y$. Q.E.D.

LEMMA 1.4. *If $a$ in $A$ has order $p^n$, then $a^{\phi^{n(p-1)+1}} = a^{\pi^{n+1}} = 1$.* (See Szekeres (1949), Theorem 1.)

PROOF. If $a \in A$, let $\langle a\rangle_X$ be the $X$-submodule of $A$ generated by $a$. Take $y$ in $Y$ and so $y^{\pi} = 1$. From 1.1, $y^{\phi^{p-1}} \in \langle y^p\rangle_X$. By induction on $l$, we get that $y^{\phi^{l(p-1)}} \in \langle y^{p^l}\rangle_X$. If $a$ in $A$ has order $p^n$, so $a^{\phi} \in Y$ and $a^{\phi^{n(p-1)+1}} \in \langle (a^{p^n})^{\phi}\rangle_X = (1)$. Also $a^{\pi} \in Z$ and $a^{\pi}$ has order at most $p^n$. Then $a^{\pi^{n+1}} = (a^{\pi})^{\pi^n} = (a^{\pi})^{p^n} = 1$. Q.E.D.

LEMMA 1.5. *For each $n \geqq 1$, $Y_n = Y \cap ker\,\phi^n$ $(Z_n = Z \cap ker\,\pi^n)$ is an $X$-submodule of $Y$ (of $Z$) and is generated as an $X$-module by any element $y \in Y\,(z \in Z)$ satisfying $y^{\phi^n} = 1$ and $y^{\phi^{n-1}} \neq 1$ $(z^{\pi^n} = 1$ and $z^{\pi^{n-1}} \neq 1)$. Also*

$|Y_n| = p^n$ ($|Z_n| = p^n$). *These are the only* $X$*-submodules of* $Y$ (*of* $Z$) *and are characteristic in* $P$.

PROOF. For $z$ in $Z$, we have $z^\pi = z^p$ and so the statements for $Z_n$ follow immediately.

Clearly $Y_n$ is an $X$-submodule. Take $y$ in $Y$ satisfying $y^{\phi^n} = 1$ and $y^{\phi^{n-1}} \neq 1$ and so $Y_n \geqq \langle y \rangle_X$. We proceed by induction on $n$. For $n = 1$, $Y_1$ coincides with the central subgroup of order $p$.

By induction we have $|Y_{n-1}| = p^{n-1}$ and $Y_{n-1} = \langle y^\phi \rangle_X$. Take $y'$ in $Y_n$. Then $y'^\phi = (y^\phi)^{m_1} \cdots (y^{\phi^{n-1}})^{m_{n-1}}$ for some integers $m_i$ satisfying $0 \leqq m_i < p$. Set $y'' = y^{m_1} \cdots (y^{\phi^{n-2}})^{m_{n-1}}(y')^{-1}$ and we have that $y'' \in Y_1 = Y \cap \ker \phi \leqq \langle y \rangle_X$. Thus $y' \in \langle y \rangle_X$. Thus $Y_n = \langle y \rangle_X$. Now $y^\pi = 1$, $y^\phi \in Y_{n-1}$ and $y^p \in Y_{n-1}$ by 1.1. Hence $|Y_n| = p^n$. This rest is immediate. Q.E.D.

LEMMA 1.6. *Suppose* $n = r(p-1) + s$, *where* $r \geqq 0$ *and* $1 \leqq s \leqq p-1$. *If* $y \in Y_n - Y_{n-1}$, *then* $y$ *has order* $p^{r+1}$. *As an abelian group,* $Y_n$ *has at most* $p-1$ *generators, viz.* $Y_n = \langle y, y^\phi, \cdots, y^{\phi^{p-2}} \rangle$, *and is of type* $(p^{r+1}, \cdot\cdot\overset{(s)}{\cdots}\cdot\cdot, p^{r+1}, p^r, \cdot\cdot\overset{(p-1-s)}{\cdots}\cdot\cdot, p^r)$.

PROOF. Take $y$ in $Y_n - Y_{n-1}$ and so $y^\pi = 1$. From the second relation in 1.1, using induction on $n$, we have that $y^{-p} \equiv y^{\phi^{p-1}} \not\equiv 0 \mod Y_{n-p}$, i.e. $y^p \in Y_{n-p+1} - Y_{n-p}$ and so $y$ has order $p^{r+1}$. Also $Y_n$ is generated by $y, y^\phi, \cdots, y^{\phi^{p-2}}$.

If $n \leqq p-1$, then $Y_n$ is elementary abelian of order $p^n$, generated by $y, y^\phi, \cdots, y^{\phi^{n-1}}$. If $n > p-1$, then we show that $y, \cdots, y^{\phi^{p-2}}$ are independent. For this it suffices to show that they are independent modulo $Y_{n-p+1}$. A nontrivial relation, modulo $Y_{n-p+1}$, would be transformed by $\phi^{n-p+1}$ to one in $Y_{p-1}$, which is impossible as this last is elementary abelian of order $p^{p-1}$ and is generated by the images $y^{\phi^{n-p+1}}, \cdots, y^{\phi^{n-1}}$. Q.E.D.

LEMMA 1.7. *If* $a = x^s y$ $(0 < s < p, y \in Y)$, *then* $\exists\, y' \in Y$ *such that* $a^{y'} = x^s$. *Also* $a$ *has order* $p$.

PROOF. Choose $r$ $(0 < r < p)$ such that $a^r = xy''$ $(y'' \in Y)$. If $y'' = y_k^{m_k} \cdots y_1^{m_1}$, set $y' = y_{k+1}^{m_k} \cdots y_2^{m_1}$ and then $(a^r)^{y'} = x$. Thus $a^{y'} = x^s$ and $a$ has order $p$, as $x$ has. Q.E.D.

We now have $X$-submodules $A_{kl} = \langle Y_k, Z_l \rangle$ $(k \geqq 1, l \geqq 1)$ of $A$ of order $p^{k+l-1}$ $(A_{k1} = Y_k,\ A_{1l} = Z_l)$ which are characteristic in $P$. Choose $1 \neq y_1 = z_1 \in Y_1 = Z_1$. For each $l \geqq 1$, choose $z_l$ in $Z_l - Z_{l-1}$ such that $z_l^p = z_{l-1}$. For each $k \geqq 1$, use 1.2 to choose $y_k$ in $Y_k - Y_{k-1}$ such that $y_k^\phi = y_{k-1}$. Write $y_k = z_l = 1$ if $k, l \leqq 0$.

PROPOSITION 1.8. *The only finite* $X$*-submodules of* $A$ *are the* $A_{kl}$ $(k \geqq 1, l \geqq 1)$ *and* $A_{klm} = \langle A_{k-1,l}, y_k^{(m)} \rangle$ $(0 < m < p,\ k \geqq 2,\ l \geqq 1)$, *where* $y_k^{(m)} = y_k z_{l+1}^m$.

PROOF. Let $M$ be a finite $X$-submodule of $A$ not equal to any $A_{kl}$. It is immediate that $M \geqq Y_1 = Z_1$. Choose integers $k$ and $l$ maximal such that $Y_{k-1} \leqq M$ and $Z_l \leqq M$. Suppose $m = y_r^{m_r} \cdots y_1^{m_1} \cdot z_s^{n_s} \cdots z_1^{n_1} \in M - Y - Z$, where $0 \leqq m_i, n_j < p$ and $m_r \neq 0 \neq n_s$. Then $m^{\pi} = z_{s-1}^{n_s} \cdots z_1^{n_2} \in Z_l$ and $m^{\phi} = y_{r-1}^{m_r} \cdots y_1^{m_2} \in Y_{k-1}$ and so $r \leqq k$ and $s \leqq l$. Modulo $A_{k-1,l}$ $(= \langle Y_{k-1}, Z_l \rangle)$, it suffices to look at elements $y_k^{(m)} = y_k z_{l+1}^m$ $(0 < m < p)$ in $M$. However both $y_k$ and $z_l \notin M$ and so $m$ is uniquely determined and $M = \langle y_k^{(m)}, A_{k,l} \rangle = A_{klm}$ of order $p^{k+l-1}$. Q.E.D.

$A_{klm}$ is annihilated by $\pi^{k-1} - m'\phi^l$ $(0 < m, m' < p)$ iff $m = m'$ and so $A_{kl}$. and the $A_{klm}$ $(0 < m < p)$ are not isomorphic as $X$-modules. Take $\psi = \psi(n)$ in $Aut\ X$ given by $x \mapsto x^n$ $(0 < n < p)$. An additive map $\theta$: $M \mapsto M'$ between $X$-modules is an *$\psi$-homomorphism* if $(m^x)^\theta = (m^\theta)^{x^\psi}$ $(m \in M)$.

LEMMA 1.9. *Take $\psi = \psi(n)$ in Aut X. (a) $A_{kl}$ is not $\psi$-isomorphic to any $A_{klm}$ $(0 < m < p)$. (b) If $A_{klm}$ is $\psi$-isomorphic to $A_{klm'}$, then $m' \equiv m\,n^{k-1} \bmod p$.*

PROOF. $\phi' = \phi^\psi = (x-1)^\psi = x^n - 1 = (x-1)(x^{n-1} + \cdots + 1) = \phi\chi$, say. By choosing $n'$ such that $nn' \equiv 1 \bmod p$, we see that $\phi = \phi'\chi'$. Also $\pi' = \pi^\psi = (1 + \cdots + x^{p-1})^\psi = 1 + \cdots + x^{p-1} = \pi$. Hence an $\psi$-isomorphism induces $\psi$-isomorphisms from $ker\,\phi$ to $ker\,\phi'$ and from $ker\,\pi$ to $ker\,\pi'$. For $A_{kl}$, we have $ker\,\phi = Z_l$ and $ker\,\pi = Y_k$. This proves (a), as $A_{klm} = \langle y_k^{(m)}, A_{k-1,l} \rangle$.

Now let $\theta$: $A_{klm} \to A_{klm'}$ be an $\psi$-isomorphism and so $\theta$ induces an $\psi$-isomorphism $A_{k-1,l} \to A_{k-1,l}$. Suppose $(y_k^{(m)})^\theta = (y_k^{(m')})^q \bmod A_{k-1,l}$. Then $y_1^\theta = [y_k^{(m)}, x, \cdots^{(k-1)} \cdots, x]^\theta = [(y_k^{(m')})^q, x^n, \cdots^{(k-1)} \cdots, x^n] = y_1^{qn^{k-1}}$. As $(y_k^{(m)})^{\pi^l} = (y_k z_{l+1}^m)^{\pi^l} = z_1^m = y_1^m$, so $(y_1^m)^\theta = ((y_k^{(m')})^q)^{\pi^l} = y_1^{m'q}$. As $y_1$ has order $p$, so $m' \equiv m\,n^{k-1} \bmod p$. Q.E.D.

Such $\psi$-isomorphisms between the $A_{klm}$ will be given in the next section.

## 2. Construction of groups $G$ and abstract presentations

We have determined the $X$-module structure of the maximal subgroup $M = G \cap A$ of $G$. Although the extension problem is easy to resolve, instead we put each $G$ into a standard form by elementary automorphisms of $P$.

(2.1) Regard $P = W wr X$ as embedded in $W wr\,\Sigma_p \leqq GL(p, F)$, with $\Sigma_p$ being realized by permutation matrices ($\Sigma_p$ is the symmetric group). The element $x$ is realized by the $p$-cycle permutation $(12 \cdots p)$ (see (0.1)). For $0 < n < p$, let $\kappa(n)$ be the permutation (matrix) leaving invariant the symbol 1 and satisfying $x^{\kappa(n)} = x^n$. Then $\langle x, \kappa(n) \rangle = N_{\Sigma_p}(\langle x \rangle)$ and this has order $p(p-1)$.

PROPOSITION 2.2 *Given a nonabelian finite subgroup $G$ of $P$, there exist an element $a$ in $A$ and an integer $n$ with $0 < n < p$ such that $(G^a)^{\kappa(n)}$ is one of the following groups:*

*$P_{klo} = \langle x, A_{kl}\rangle$, $P_{klm} = \langle x, A_{klm}\rangle$ or $P_{klp} = \langle x', A_{kl}\rangle$, where $k \geqq 2$, $l \geqq 1$, $0 < m < p$ and $x' = xz_{l+1}$. Each of these groups has order $p^{k+l}$. The automorphism $\kappa(n)$ of $P$ permutes the $P_{klm}$ $(0 < m < p)$, changing $P_{klm}$ to $P_{klm'}$ with $m' \equiv mn^{k-1} \bmod p$. Apart from this last, the orbit of $G$ under $\operatorname{Aut} P$ contains exactly one $P_{klm}$ $(0 \leqq m \leqq p)$.*

PROOF. Suppose first that $M = G \cap A = A_{kl}$. There exists $g$ in $G - A_{kl}$ of form $g = xyz$ $(y \in Y,\ z \in Z)$. By 1.7, $\exists y'$ in $Y$ such that $g' = g^{y'} = xz$. Let $z = z_q^{n_q} \cdots z_1^{n_1}$ $(0 \leqq n_i < p)$. Then $g'^p = z_{q-1}^{n_q} \cdots z_1^{n_2} \in A_{kl}$ and so $q \leqq l+1$. Modulo $A_{kl}$, one can assume that $g' = xz_{l+1}^{n}$ $(0 \leqq n < p)$. If $n = 0$, then $G' = G^{y'} = P_{kl0}$. If $n > 0$, then $(g')^{\kappa(n)} = (xz_{l+1})^n = (x')^n$ $(x' = xz_{l+1})$ and so $(G')^{\kappa(n)} = P_{klp}$. In this latter case, every element in $G - M$ has order $p^{l+1}$ by 1.7.

Suppose $G \cap A = A_{klm}$ $(0 < m < p)$. As above, the form of an element $g$ in $G - A_{klm}$ can be assumed to be $g = xz_{l+1}^{n}$ $(0 \leqq n < p)$. As $y_k^{(m)} = y_k z_{l+1}^{m} \in A_{klm}$, $g$ can be written $g = xy_k^{s} \pmod{A_{klm}}$ for some $s$. Then $g^{y_{k+1}^{s}} = x$ and $G^{y_{k+1}^{s}} = P_{klm}$. The remainder follows from 1.9. Q.E.D.

COROLLARY 2.3. *There exist elements of order $p$ in $P_{kl0} - A_{kl}$. Every element in $P_{klp} - A_{kl}$ has order $p^{l+1}$.*

PROPOSITION 2.4. *We have the following abstract presentations for $k \geqq 2$, $l \geqq 1$ and $0 < m < p$:*

$$P_{klo} = \langle x, y_1, \cdots, y_k, z_l \mid x^p = 1, z_l \text{ central}, z_l^{p^{l-1}} = y_1, \langle y_1, \cdots, y_k\rangle \text{ abelian},$$
$$[y_j, x] = y_{j-1} (2 \leqq j \leqq k), y_k^{\pi} = y_k^{(p)} \cdots y_{k-p+1}^{\binom{p}{p}} = 1\rangle.$$
$$P_{klm} = \langle x, y_1, \cdots, y_k^{(m)}, z_l \mid \text{as in } P_{klo} \text{ except that } y_k^{(m)\pi} =$$
$$(y_k^{(m)})^{(p)} y_{k-1}^{\binom{p}{2}} \cdots y_{k-p+1}^{\binom{p}{p}} = z_l^{m}\rangle.$$
$$P_{klp} = \langle x', y_1, \cdots, y_k, z_l \mid \text{as in } P_{klo}, \text{ except that } x'^p = z_l\rangle.$$

PROOF. The necessity of these relations follows from their realizations in $P$. The sufficiency follows if the order of these groups is $p^{k+l}$. This is shown by induction on $k$ for $P_{k10}$ and follows for $P_{kl0}$, as $P_{kl0} \approx P_{k10} \curlyvee \mathbf{Z}_{p^l}$. In $P_{klm}$ and $P_{klp}$, the element $z_l$ is central and so by adding a central element $z_{l+1}$ such that $z_{l+1}^{p} = z_l$ the order is increased by $p$. The extended groups are readily seen to be isomorphic to $P_{k,l+1,0}$ of order $p^{k+l+1}$. Q.E.D.

COROLLARY 2.5 $P_{klm} \curlyvee \mathbf{Z}_{p^{l+1}} \approx P_{k,l+1,0}$ $(0 \leqq m \leqq p)$.

In the above presentations the last relation may be replaced by $(y_k x^{-1})^p = 1$ in $P_{klo}$, by $(y_k^{(m)} x^{-1})^p = z_l^{m}$ in $P_{klm}$ and by $(y_k (x')^{-1})^p = z_l^{-1}$ in $P_{klp}$.

When necessary, the relevant prime $p$ will be included as a fourth suffix: $P_{klmp}$.

https://doi.org/10.1017/S1446788700015330 Published online by Cambridge University Press

## 3. Isomorphic classes

(3.1) $P_{21o}$ ($\neq P_{2102}$) has the following automorphism:

$$p > 2 \quad : \quad \omega : x \mapsto y_2,\ y_2 \mapsto x^{-1},\ z_l \mapsto z_l.$$

$$p = 2,\ l \geqq 2 : \quad \omega : x \mapsto y_2 z_l^{2^{l-2}},\ y_2 \mapsto x z_l^{2^{l-2}},\ z_l \mapsto z_l.$$

Also the element $y_3$ acts by conjugation.

(3.2) The $P_{2lm}$ $(0 < m < p)$ and $P_{2lp}$ lie in $P_{2,l+1,0}$. Choose $m'$ $(0 < m' < p)$ such that $mm' \equiv 1 \bmod p$. Then the composite automorphism $\omega \cdot y_3^m \cdot \omega \cdot y_3^{m'}$ of $P_{2,l+1,0}$ induces an isomorphism $P_{2lp} \to P_{2lm}$, except when $p = 2$ and $l = 1$. In this last case, the automorphism $\omega \cdot y_3 \cdot \omega$ of $P_{2202}$ induces an isomorphism $P_{2102} \to P_{2112}$.

The above isomorphisms arise as such a group $G$ has more than the one maximal abelian subgroup $M = G \cap A$. As $A$ is characteristic in $P$, these isomorphisms cannot be induced by elements of $Aut\,P$. (They will be realized as similarity transformations in $GL(p, F)$ in section 4.)

Proposition 3.3. *A nonabelian finite subgroup $G$ of $P(\approx \mathbf{Z}_{p^\infty}\, wr\, \mathbf{Z}_p)$ is isomorphic to one of the following groups:*

$$P_{klo},\ P_{klp}\ \ (k \geqq 2,\ l \geqq 1) \ \ or\ \ P_{klm}\ \ (k \geqq 3,\ l \geqq 1,\ 0 < m < p).$$

*These are nonisomorphic except that $P_{klm} \approx P_{klm'}$ $(0 < m, m' < p)$ whenever $m' \equiv mn^{k-1} \bmod p$, for some integer $n$. Thus the number of such groups of order $p^{k+l}$ and center of order $p^l$ is $(k-1, p-1) + 2$ if $k \geqq 3$ and $2$ if $k = 2$.*

Proof. From the isomorphisms of 3.2, there are at most two nonisomorphic groups amongst the $P_{2lm}$ $(0 \leqq m \leqq p)$. If $p$ is odd, then $P_{210}$ has exponent $p$ $(P_{2102} \approx D_8)$. As $P_{21o} \approx P_{210} \vee \mathbf{Z}_{p^l}$ (2.5), so $P_{21o}$ ($\neq P_{2102}$) has exponent $p^l$. On the other hand $P_{2lp}$ has exponent $p^{l+1}$ (2.3) $(P_{2122} \approx Q_8)$. Hence $P_{21o} \not\approx P_{2lp}$.

If $P_{klm}$ has two abelian maximal subgroups, their intersection is a central subgroup of index $p^2$. As the index of the center of $P_{klm}$ is $p^k$, we have that for $k \geqq 3$ each $P_{klm}$ has a unique abelian maximal subgroup ($A_{kl}$ or $A_{klm}$). An isomorphism between the $P_{klm}$ would induce a corresponding $\psi$-isomorphism between the $A_{kl}$ or $A_{klm}$. From 1.9, neither $P_{klo}$ or $P_{klp}$ is isomorphic to any $P_{klm}$ $(0 < m < p)$ and from 2.2 $P_{klm} \approx P_{klm'}$ iff $m' \equiv mn^{k-1} \bmod p$ for some integer $n$. By 2.3, $P_{klo} \not\approx P_{klp}$. Q.E.D.

Corollary 3.4 *The groups of 3.3 are the only nonabelian finite $p$-subgroups of $GL(p, F)$ and form a complete list of nonabelian $p$-groups with cyclic center and with an abelian maximal subgroup.*

## 4. Conjugacy classes in $GL(p, F)$

LEMMA 4.1. *The automorphism $\omega$ of $P_{2lo}$ ($\neq P_{2102}$), defined in 3.1, is realizable as a similarity transformation in $GL(p, F)$.*

PROOF. If $p > 2$, $\omega$ sends $x \mapsto y_2$, $y_2 \mapsto x^{-1}$, $z_l \mapsto z_l$. Suppose $y_1 = (w, \cdots, w)$ and $y_2 = (1, w, \cdots, w^{p-1})$, where $w$ in $W$ has order $p$. Write $t = t(w) = (w^{(i-1)(j-1)})$ for the $p \times p$ van der Monde matrix. Then $t^{-1} = (1/p) \cdot t(w^{-1})$, $txt^{-1} = y_2$, and $ty_2t^{-1} = x^{-1}$.

When $p = 2$, $l \geqq 2$, and $y_2 = (w, w^{-1})$ and $z_2 = (w, w)$, where $w$ is an element of order 4 in $W$, the automorphism $\omega$ of 3.1 is realized by $t = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ (*i.e.* $tgt^{-1} = g^{\omega}$ ($g \in P_{2lo}$)). Q.E.D.

PROPOSITION 4.2. *Two nonabelian finite $p$-subgroups of $GL(p, F)$ are conjugate iff they are isomorphic.*

PROOF. In 2.1, we had $P = W wr X \leqq W wr \Sigma_p \leqq GL(p, F)$. Thus $\kappa(n)$, action by elements of $Y$ and $\omega$ are similarity transformations. Composites of these realized the isomorphism relating the arbitrary $G$ to one of the groups listed in 3.3. Q.E.D.

COROLLARY 4.3. *Given two faithful (irreducible) representations, $\mu$ and $\mu'$, of $P_{klm}$ in $GL(p, F)$, there exists an automorphism $\theta$ of $P_{klm}$ such that $\mu^{\theta}$ is similar to $\mu'$.*

## 5. Properties and examples

(5.1) For $p > 2$, $P_{210}$ has order $p^3$ and exponent $p$, while $P_{21p}$ has order $p^3$ and exponent $p^2$. $P_{k102} \approx D_{2^{k+1}}$, $P_{k112} \approx SD_{2^{k+1}}$ (semidihedral) and $P_{k122} \approx Q_{2^{k+1}}$.

(5.2) As already noted, $P_{klo} \approx P_{k10} \curlyvee \mathbf{Z}_{p^l}$. Also $\mathbf{Z}_{p^r} wr \mathbf{Z}_p \approx P_{r(p-1)+1,r,m}$, where $m \equiv (-1)^{r-1} \bmod p$. $P_{2lp}$ is the $p$-group of order $p^{l+2}$ which has a cyclic maximal subgroup and center of index $p^2$.

(5.3) The descending central series of $P_{klm}$ is:

$$P_{klm} > P'_{klm} = \langle y_1, \cdots, y_{k-1} \rangle > \cdots > \langle y_1, y_2 \rangle > \langle y_1 \rangle > (1),$$

and so $P_{klm}$ has class $k$.

(5.4) $P_{klm}$ has maximal class ($k$) iff $l = 1$. The groups $P_{k1m}$ of maximal class were classified by Wiman (1946).

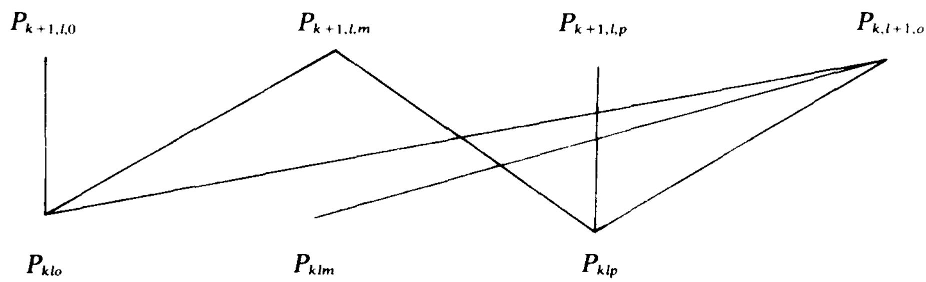
(5.5) The homomorphism $P_{klm} \to P_{k-1,1,0}$ ($k \geqq 3$), $x$ (or $x'$) $\mapsto x$, $y_k$ (or $y_k^{(m)}$) $\mapsto y_{k-1}$, $z_l \mapsto 1$, induces an isomorphism $P_{klm}/Z(P_{klm}) \approx P_{k-1,1,0}$. As $P'_{klm} = \langle y_1, \cdots, y_{k-1} \rangle$, we see that for a fixed $k$ ($l$ and $m$ varying), the $P_{klm}$ are isoclinic (to $P_{k10}$, say).

(5.6) The Frattini subgroups are as follows:

$$\Phi(P_{kl0}) = A_{k-1,l-1}\ (l \geqq 2) \text{ and } \Phi(P_{k10}) = A_{k-1,1} = Y_{k-1}.$$

For $0 < m \leqq p$, $\Phi(P_{klm}) = A_{k-1,l}$.

(5.7) From an analysis of the maximal subgroups of the $P_{klm}$ we obtain the following diagram of inclusions to within isomorphism.




where $k \geqq 2$, $l \geqq 1$ and $0 < m < p$ ($k \geqq 3$ in $P_{klm}$). These inclusions provide an alternative method for showing that $P_{klo}$, $P_{klm}$ $(0 < m < p)$ and $P_{klp}$ are nonisomorphic.

## 6. Automorphism groups

We have the following automorphisms of $P$:

$\kappa(n)$ $(0 < n < p)$,

$y$ $(\in Y)$, *acting as an inner automorphism*,

$x^m$ $(0 \leqq m < p)$, *acting as an inner automorphism*,

$\lambda(n)$: $x \mapsto x$, $y_k \mapsto y_k^n$, $z_l \mapsto z_l^n$ $(0 < n < p)$,

$\eta = \eta(\alpha_2, \alpha_3, \cdots)$: $x \mapsto x$, $y_k \mapsto y_k \cdot y_{k-2}^{\alpha_2} \cdots y_1^{\alpha_{k-1}}$, $z_l \mapsto z_l$ $(0 \leqq \alpha_i < p)$,

$\zeta = \zeta(\beta_1, \beta_2, \cdots)$: $x \mapsto x$, $y_k \mapsto y_k$, $z_l \mapsto z_l \cdot z_{l-1}^{\beta_1} \cdots z_1^{\beta_{l-1}}$ $(0 \leqq \beta_i < p)$.

The arbitrary element $\theta$ of $Aut P$ can be expressed as the composite $\zeta \cdot \eta \cdot \lambda(n) \cdot x^m \cdot y \cdot \kappa(n')$. Here $y$ is only determined modulo $Y_1 = \langle y_1 \rangle \leqq Z(P)$. This is shown by composing $\theta$ with $\kappa(n)$ and $y$ to obtain identical action on $x$, with $x^m$, $\lambda(n)$ and $\eta$ to obtain identical action on $Y$ and finally with $\zeta$ to obtain the identity automorphism.

The same method is used for the $P_{klm}$. Use is made of the characteristic subgroup $\Phi(P_{klm}) \cdot Z(P_{klm})$ of index $p^2$ and of the abelian maximal subgroup whenever it is characteristic. For $P_{klo}$ $(k>2)$ and $P_{2102}$ we simply use restrictions of the above automorphisms. For $P_{klm}$ $(0<m<p)$, $\kappa(n)$ gives an automorphism iff $n^{k-1}\equiv 1 \bmod p$ and so these $\kappa(n)$ generate a group of automorphisms which involves a cyclic group of order $(k-1, p-1)$.

If $G$ is equal to $P_{2lo}$ $(\neq P_{2102})$ or $P_{2122}$, an automorphism $\theta$ may permute the maximal (abelian) subgroups of $G$ and induces a linear transformation of $G/(\Phi(G)\cdot Z(G))$. If

$$\theta\colon x\mapsto x^a y_2^b,\ y_2\mapsto x^c y_2^d \bmod \Phi(G)\cdot Z(G),$$

then $\begin{pmatrix} a & b\\ c & d\end{pmatrix}$ $(\in GL(2,\mathbf{F}_p))$ is called the *matrix* of $\theta$. Thus $y_3$ has matrix $\begin{pmatrix} 1 & -1\\ 0 & 1\end{pmatrix}$ and $\omega$ (see 3.1) has matrix $\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}$. Thus $y_3$ and $\omega$ generate a group of automorphisms involving $SL(2,\mathbf{F}_p)$ which has order $p(p^2-1)$. If $\omega_1,\cdots,\omega_{p(p^2-1)}$ denote automorphisms in $\langle \omega, y_2\rangle$ whose matrices are the distinct elements of $SL(2,\mathbf{F}_p)$, then the arbitrary automorphism $\theta$ can be expressed as above with the $\omega_i$ replacing the $\kappa(n)$.

The groups $P_{klp}$ $(\neq P_{2122})$ do not admit the $\kappa(n)$ as automorphisms. Also the automorphism $\lambda(n)$ must be varied to $\lambda'(n)$: $x'\to(x')^n$, $y_k\to y_k^{n^{2-k}}$ $(0<n<p)$.

(6.1) The $\lambda(n)$ (or $\lambda'(n)$), $\eta$ and $\zeta$ generate a subgroup $B=B(P_{klm})$ of $Aut(P_{klm})$ of order $(p-1)p^{k+l-3}$. The $\kappa(n)$ (or $\omega_i$), $y_{k+1}$ and inner automorphisms generate a group $C(P_{klm})$ of similarity automorphisms. Also $Aut(P_{klm})=B(P_{klm})\cdot C(P_{klm})$ and the order of $Aut(P_{klm})$ can be calculated exactly. In particular $|Aut(P_{klm})\colon C(P_{klm})|=(p-1)p^{k+l-3}/|B\cap C|$.

PROPOSITION 6.2. *$P_{klm}$ has $(p-1)p^{k+l-3}$ faithful irreducible representations in $GL(p,F)$.*

PROOF. Any representation $\mu$ of $G=P_{klm}$ of degree $p$ may be written $\nu^G$, where $\nu$ is a linear representation of the abelian maximal subgroup $M$. Moreover $\mu$ is faithful iff the restriction of $\nu$ to $\langle y_1\rangle=\Omega_1(Z(G))$ $(\leqq M)$ is faithful. Now $M$ of order $p^{k+l-1}$ has $(p-1)p^{k+l-2}$ such linear "faithful" representations $\nu$. These fall into orbits of size $p$ under the action of $x$ in $G-M$ and so there are $(p-1)p^{k+l-1}$ distinct faithful irreducible representations $\mu$ of $G$. Q.E.D.

Given a faithful representation $\mu\colon G\to G^\mu\leqq GL(p,F)$, one can look at the subgroup $SA=SA_\mu(G)$ of $Aut\,G$ (*s*imilarity *a*utomorphism group), consisting of those automorphisms realizable by similarity transformations acting on $G^\mu$. By 4.3, $SA$ is determined up to conjugacy in $Aut$, as $\mu$ varies. $SA$ contains $IA$, the *i*nner *a*utomorphism group, and we call the quotient $SA/IA=OSA$, the *o*uter *s*imilarity *a*utomorphism group. Henceforth $SA$ and $OSA$ will be calculated from the natural embeddings $G=P_{klm}\leqq P\leqq GL(p,F)$.

Now the group $C(P_{klm})$ of 6.1 lies in $SA(P_{klm})$. Again by 4.3, $|Aut(P_{klm})\colon SA(P_{klm})|$ is the number of faithful irreducible representations of $P_{klm}$, i.e. $(p-1)p^{k+l-3}$, by 6.2. So from 6.1 we have:

$$(p-1)p^{k+l-3} = |Aut\colon SA| \leqq |Aut\colon C| = (p-1)p^{k+l-3}/|B \cap C|,$$

and so $B \cap C = (1)$ and $C = SA$. Summarizing we have:

Proposition 6.3. *$Aut(P_{klm}) = B(P_{klm}) \cdot SA(P_{klm})$ with $B(P_{klm}) \cap SA(P_{klm}) = (1)$. If $\mu$ is the representation of $P_{klm}$ afforded by its embedding in $GL(p, F)$, then the conjugates of $\mu$ by elements of $B(P_{klm})$ are the $(p-1)p^{k+l-3}$ faithful irreducible representations of $P_{klm}$.*

In general neither $B$ or $SA$ is a normal subgroup of $Aut$.

As $|IA| = p^k$, so $|SA| = |OSA| \cdot p^k$. Also $|Aut| = |SA| \cdot (p-1)p^{k+l-3}$. We list only the orders of the $OSA$.

| | Group | $\|OSA\|$ | $OSA$ |
|---|---|---|---|
| (6.4) | (1) $P_{klo}$ $(k \geqq 3)$ | $p(p-1)$ | metacyclic |
| | (2) $P_{klp}$ $(\neq P_{2122})$, $P_{2102}$ | $p$ | cyclic |
| | (3) $P_{klm}$ $(k \geqq 3, 0 < m < p)$ | $(k-1, p-1)$ | cyclic |
| | (4) $P_{2lo}$ $(\neq P_{2102})$, $P_{2122}$ | $p(p^2-1)$ | $SL(2, \mathbf{F}_p)$. |

In (1), the subgroup $Q$ of order $p$ is unique and $|C_{OSA}(Q)| = (k, p-1)p$.

A *$p$-overgroup* of $G$ in $GL(p, F)$ is defined to be any $p$-subgroup of $GL(p, F)$, in which $G$ is a maximal subgroup.

Proposition 6.5. (*a*) *$P_{klm}$ has one $p$-overgroup isomorphic to $P_{k,l+1,0}$, viz. $P_{k,l+1,0}$ itself. If $k \geqq 3$ and $0 < m < p$, this is the only $p$-overgroup of $P_{klm}$.*
(*b*) *The $p$-overgroups of $P_{klo}$ $(k \geqq 3)$ [of $P_{2102}$] are $P_{k,l+1,0}$ and $P_{k+1,l,m}$ $(0 \leqq m < p)$ [are $P_{2202}$, $P_{3102}$ and $P_{3113}$].*
(*c*) *The $p$-overgroups of $P_{klp}$ $(\neq P_{2122})$ are $P_{k,l+1,o}$, $P_{k+1,l,p}$ and $(P_{k+1,l,m})^{y^{m'}_{k+2}}$, where $0 < m$, $m' < p$ and $mm' \equiv 1 \bmod p$.*
(d) *If $k \geqq 3$, then $P_{klm}$ is contained in one subgroup of $GL(p, F)$ isomorphic $P_{k+1,l+1,0}$ viz. $P_{k+1,l+1,0}$ itself.*

Proof. (a) In enlarging the center of $P_{klm}$ one must add scalar matrices by Schur's lemma and this gives $P_{k,l+1,o}$. If $k \geqq 3$ and $0 < m < p$, this is the only possible extension by 6.4 (3).

https://doi.org/10.1017/S1446788700015330 Published online by Cambridge University Press

(b) and (c): By 6.4 (1) and (2), each of the groups in question has essentially one outer automorphism $\theta$ of order $p$ and this acts as $y_{k+1}$ does. By Schur's lemma, $\theta$ must have form $y_{k+1}z$ $(z \in Z)$. As $z^p \in Z(P_{klm})$ we can assume $\theta = y_{k+1}z_{l+1}^m$ $(0 \leqq m < p)$, which gives the possibilities listed above.

(d): If $k \geqq 3$, each $p$-overgroup of $P_{klm}$ is contained in $P_{k+1,l+1,o}$. Q.E.D.

Proposition 6.5 shows why the inductive method of construction the $P_{klm}$ within $GL(p, F)$, as mentioned in the introduction, is feasible. One obtains the diagram 5.7 of $p$-overgroups.

(6.6) Note that $N_{GL}(P_{klm})/(C_{GL}(P_{klm}) \cdot P_{klm}) \approx OSA(P_{klm})$.

## 7. Irreducible representations of the $P_{klm}$

(7.1) The following construction sets up a one to one correspondence between the nonequivalent irreducible representations $\mu$ of $P_{klo}$ of degree $p$ over $F$ and those of $P_{klm}$ $(0 < m \leqq p)$, which preserves faithfulness. Choose a primitive $p^{l+1}$th root $w$ of 1 in $F^\times$. Suppose $(z_l)^\mu = w^{np}I$, where $I$ is the unit matrix and $0 \leqq n < p^l$. Write $(z_{l+1})^\mu = w^n I$ to get a representation $\mu$ of $P_{k,l+1,o}$. The corresponding representation of $P_{klm}$ is given by restriction.

As $P_{klo} \approx P_{k10} \curlyvee \mathbf{Z}_{p^l}$ (see 2.5) the problem of degree $p$ representations is reduced to that of $P_{k10}$. For $1 \leqq i \leqq k-1$, there is only one normal subgroup $\langle y_1, \cdots, y_i \rangle$ of $P_{k10}$ of order $p^i$ and $P_{k10}/\langle y_1, \cdots, y_i \rangle \approx P_{k-i,1,0}$ $(0 \leqq i < k-1)$ $(P_{k10}/\langle y_1, \cdots, y_{k-1} \rangle \approx \mathbf{Z}_p \times \mathbf{Z}_p)$. Thus we need only look at faithful irreducible representations of $P_{k10}$.

Suppose $k = r(p-1) + s$, with $r \geqq 0$ and $1 \leqq s \leqq p-1$. The maximal subgroup $Y_k$ of $P_{k10}$ is generated as an abelian group by elements $y_k, \cdots, y_{k-p+2}$ (see 1.6). Let $\nu$: $y_k \mapsto \nu_1, \cdots, y_{k-p+2} \mapsto \nu_{p-1}$ be a linear representation of $Y_k$. As $(y_{r(p-1)+1})^{p^r} = y_1^{(-1)^r}$, we see that $\mu = \nu^{P_{k10}}$ is faithful iff $\nu_s$ is a primitive $p^{r+1}$th root of 1. The image $\nu_p$ of $y_{k-p+1}$ is given by

$$(7.2) \quad \nu_1^{\binom{p}{1}} \cdots \nu_{p-1}^{\binom{p}{p-1}} \nu_p^{\binom{p}{p}} = 1.$$

Instead of looking at the orbit of $\nu$ under the action of $x$, we look directly at the matrices $x^\mu$ and $(y_k)^\mu$. We can assume that $x^\mu$ has form 0.1 and that $(y_k)^\mu = \mathit{diag}(\alpha_1, \cdots, \alpha_p)$. Then we have that

$$(7.3) \quad \alpha_n = \nu_1^{\binom{n-1}{0}} \cdots \nu_n^{\binom{n-1}{n-1}} (1 \leqq n \leqq p)$$

and $\Pi \alpha_n = 1$. If $\mu$ is faithful, then at least one of the $\alpha_n$ is a primitive $p^{r+1}$th root of 1. We regard two $p$-tuples $(\alpha_1, \cdots, \alpha_p)$ equivalent if they are the same under cyclic permutation (action of $x$).

Conversely, if $\alpha_1, \cdots, \alpha_p$ are $p^{r+1}$th roots of 1, at least one of which is primitive and with product 1, then the matrices $(y_k)^\mu = \mathit{diag}(\alpha_1, \cdots, \alpha_p)$ and $x$

generate a subgroup of $GL(p, F)$ isomorphic to $P_{k10}$, where $k = r(p-1)+s$ and $1 \leqq s \leqq p-1$. To find the precise value of $s$, form

$$(7.4) \quad \nu_r = \alpha_r^{\binom{r-1}{0}} \alpha_{r-1}^{-\binom{r-1}{1}} \cdots \alpha_1^{(-1)^{r-1}\binom{r-1}{r-1}} \quad (1 \leqq r \leqq p).$$

Suppose $\nu_s$ is the last primitive $p^{r+1}$th root of 1 in the sequence $\nu_1, \cdots, \nu_p$. Then $s < p$ and $s$ is the value sought above.

For instance if $w$ is a primitive $p^{r+1}$th root of 1, then $x$ and $\operatorname{diag}(w, \cdots, w, w^{1-p})$ generate $P_{r(p-1)+1,1,0}$ in $GL(p, F)$

$$(\nu_1 = w, \nu_2 = \cdots = \nu_{p-1} = 1, \nu_p = w^{-p}).$$

## References

L. A. Nazarova, A. V. Roĭter, V. V. Sergeitčuk, V. M. Bondarenko (1972), 'Applications of the theory of modules over dyads to the classification of finite $p$-groups with an abelian subgroup of index $p$, and to the classification of pairs of annihilating operators', *Sem. Math. V. A. Steklov Math. Inst. Leningrad.* **28,** 69–92.

G. Szekeres (1949), 'Determination of a certain family of finite metabelian groups', *Trans. Amer. Math. Soc.* **66,** 1–43.

A. Wiman (1946), 'Über mit Diedergruppen verwandte $p$-Gruppen', *Ark. Mat. Astr. Fys.* **33A,** no. 6.

Department of Pure Mathematics
The University of Sydney
Sydney, N. S. W. 2006, Australia