PACIFIC JOURNAL OF MATHEMATICS
Vol. 53, No. 1, 1974

THE NON-MINIMALITY OF INDUCED CENTRAL REPRESENTATIONS

D. WRIGHT

Let G be a finite p-group and $\mathfrak{G}$ a minimal faithful permutation representation of G possessing the minimal number of generators of the centre of G transitive constituents. One surmises that the induced representation, $\mathfrak{G}'$, of the centre of G, is minimal. The conjecture is validated subject to either of the hypotheses $|G| \leqq p^5$ except $G = Q_8 \times Z_4$ or $Z(G) \cong n$ copies of the cyclic group of order p^m and is trivial when G is abelian. However, a group of order p^6 shows the conjecture to be false for p odd, also. The converse problem of extending minimal representations of $Z(G)$ to minimal representations of G is also, in general, not possible.

NOTATION. G a finite group, $Z(G)$ is the centre of G, $d(Z(G))$ is the minimal number of generators of $Z(G)$. When G is a p-group $\Omega_1(G) = \langle g \in G \mid g^p = e \rangle$. Zp^m is the cyclic group of order p^m. $\mu(G)$ is the least natural number n such that G can be embedded in the symmetric group of degree n.

Let $\mathfrak{G} = \{G_1, \cdots, G_n\}$ be a collection of subgroups of a finite group G and X_i be the set of distinct cosets of G_i in G. The transitive action of G on X_i defines a permutation representation of G on the set $X = \bigcup_{i=1}^n X_i$ with kernel core $(\bigcap_{i=1}^n G_i)$. A faithful representation is called minimal in case $|X| = \sum_{i=1}^n |G: G_i|$ is minimal over all faithful $\mathfrak{G}$. Suppose now that G is a p-group and $d = d(Z(G))$. Then by [1] Theorem 3 $n = d$ for $p \neq 2$ whilst when $p = 2$ $1/2d \leqq n \leqq d$, the upper bound being attained. It is assumed throughout that $n = d$ thereby imposing a restriction on $\mathfrak{G}$ only when $p = 2$.

The problem is approached by first classifying minimal representations $\mathfrak{G}$, say, of finite abelian p-groups (with a restriction on $\mathfrak{G}$ if $p = 2$) and then observing two elementary properties regarding the structure of $G_i \cap Z(G)$.

1. Minimal representations of abelian groups.

THEOREM 1. *Let G be a finite abelian p-group with $n \geqq 2$. Suppose $\mathfrak{G} = \{G_1, \cdots, G_n\}$ is a minimal faithful permutation representation of G and $K_i = \bigcap_{j=1, j \neq i}^n G_j$, then*

$$G = \bigtimes_{i=1}^n K_i \quad \text{and} \quad G_i = \prod_{\substack{j=1 \\ j \neq i}}^n K_j .$$

NOTE. Any $\mathfrak{G}$ of this form is a minimal representation of G, so this theorem characterizes minimal representations of abelian p-groups, $p \neq 2$.

Proof. If $G = Z_1 \times \cdots \times Z_n$ with Z_i cyclic then we know that the G_i can be reordered so that $G_i \cap Z_i = E$ (see [2], Lemma 2). Hence $|G: G_i| \geqq |Z_i|$. Suppose for some k, $|G: G_k| > |Z_k|$, then

$$\mu(G) = \sum_{i=1}^{n} |G: G_i| > \sum_{i=1}^{n} |Z_i| = \mu(G)$$

so that $|G: G_i| = |Z_i|$, for all $1 \leqq i \leqq n$. Now

$$|G: K_i| = \left|G: \bigcap_{\substack{j=1\\ j\neq i}}^{n} G_j\right| \leqq \prod_{\substack{j=1\\ j\neq i}}^{n} |G: G_j|, \text{ Pointcaré's theorem}$$

$$= \prod_{\substack{j=1\\ j\neq i}}^{n} |Z_j| = |G: Z_i| .$$

It follows that $|K_i| \geqq |Z_i|$ and $|\times_{i=1}^{n} K_i| \geqq \prod_{i=1}^{n} |Z_i| = |G|$ so that $G = \times_{i=1}^{n} K_i$ and $|K_i| = |Z_i|$ (see [3], Lemma 0). Also, $G_i \supseteqq \prod_{\substack{j=1\\ j\neq i}}^{n} K_j$ but $|G: \prod_{\substack{j=1\\ j\neq i}}^{n} K_j| = |K_i| = |Z_i| = |G: G_i|$ and the lemma is now clear.

From the proof of [1], Proposition 2 we conclude that whenever G and H have coprime orders any stabilizer in a minimal representation of $G \times H$ has the form $G_1 \times H$ or $G \times H_1$, $G_1 \leqq G$, $H_1 \leqq H$. By decomposing an abelian group A into the direct product of its Sylow p-subgroups we easily generalize Theorem 1 to classify minimal representations of abelian groups (of odd order).

2. Induced central representation. Throughout this section whenever $\mathfrak{G} = \{G_1, \cdots, G_n\}$, $n = d(Z(G))$.

LEMMA 2. *No generator of $G_i \cap Z(G)$ is a p-power of any element in $Z(G)$ provided $\mathfrak{G}$ is minimal.*

Proof. Let $H_i = (\bigcap_{\substack{j=1\\ j\neq i}}^{n} G_j) \cap Z(G)$. Since $G_i \supseteqq H_1 \times \cdots \times H_{i-1} \times H_{i+1} \times \cdots \times H_n$, see [3] lemma, it follows that $d(G_i \cap Z(G)) = n - 1$. Suppose $G_i \cap Z(G) = \langle x_k \mid k \in I\rangle$ and $x_j = y^p$, for some j. Then $|I| \geqq n - 1$. Define $Y = \langle x_k, y \mid k \in I\backslash\{j\}\rangle \supseteqq G_i \cap Z(G)$. Clearly, $\Omega_1(Y) = \Omega_1(G_i \cap Z(G))$ and $YG_i \cap Z(G) = Y$. Thus, the representation $\{G_1, \cdots, G_{i-1}, YG_i, G_{i+1}, \cdots, G_n\}$ is faithful. The minimality of $\mathfrak{G}$ yields $YG_i = G_i$ so that $Y = G_i \cap Z(G)$. It follows that $x_j \in \langle x_k \mid k \in I\backslash\{j\}\rangle$, contradicting that x_i is a generator of G.

The next lemma is easy to verify.

LEMMA 3. *Let* $A = \times_{i=1}^{n} \langle a_i \rangle$ *be an abelian p-group with* $d(A) = n$. *If* $B \leqq A$ *with* $d(B) = n - 1$ *such that no generator of* B *is a p-power of any element of* A *then*

(i) $B = \langle a_j \mid j \in N \backslash \{s\}$, *some* $s \rangle$, *where* $N = \{k \mid 1 \leqq k \leqq n\}$

or

(ii) $B = \langle a_r a_s^{\gamma_r}, a_k \mid r \in J, k \in K, J \cup K = N\backslash\{s\}$, *some* s, $J \cap K = \Phi \rangle$.

COROLLARY. *If* $Z(G) = Z_1 \times \cdots \times Z_n$ *with* $Z_i = \langle z_i \rangle$ *cyclic then*

$$G_i \cap Z(G) = \langle z_j \mid j \in N\backslash\{s\}\rangle$$

or

$$G_i \cap Z(G) = \langle z_r z_s^{\gamma_r}, z_k \mid r \in J, k \in K, J \cup K = N\backslash\{s\}, J \cap K = \Phi \rangle .$$

Proof. By Lemma 2 $G_i \cap Z(G)$ and $Z(G)$ satisfy the conditions of Lemma 3.

Write $\mathfrak{G}' = \{G_1 \cap Z(G), \cdots, G_n \cap Z(G)\}$ then:

LEMMA 4. $\mathfrak{G}'$ *is minimal whenever* $Z(G) \cong n$ *copies of* Z_p^m.

Proof. $n = 1$ is trivial. For $n \neq 1$, by the corollary to Lemma 3 we deduce $|Z: G_i \cap Z(G)| = p^m$, $1 \leqq i \leqq n$, yielding $\deg \mathfrak{G}' = np^m$ and $\mathfrak{G}'$ is minimal.

THEOREM 5. *If* $|G| \leqq p^5$ *then* $\mathfrak{G}'$ *is minimal, except for the case* $p = 2$, $G = Q_8 \times Z_4$, *the direct product of the quaternionic group of order* 8 *and the cyclic group of order* 4.

Proof. We already have the result if G is abelian or $Z(G)$ is isomorphic to n copies of Z_p^m. This leaves the case: $|G| = p^5$, $Z(G) = \langle z_1 \rangle \times \langle z_2 \rangle \cong Z_{p^2} \times Z_p$. If $G = H \times K$ and is non-abelian then $K \cong Z_p$ or $K \cong Z_{p^2}$. Let $\mathfrak{G} = \{G_1, G_2\}$ be a minimal faithful representation of G. By [3], $\mu(G) = \mu(H) + \mu(K)$. When $K \cong Z_p$, $|G: G_1| = p$, say, and $G_1 \cap Z(H) \neq E$. By the corollary to Lemma 3, $G_1 \supseteqq Z(H)$, so that $\mathfrak{G}'$ is minimal. If $K \cong Z_{p^2}$, then except for the case $p = 2$ and $H \cong Q_8$, $\mu(H) = p^2$. Therefore, $\mu(G) = p^2 + p^2$ and $|G_1| = |G_2| = p^3$. As above, $\mathfrak{G}'$ not minimal implies $G_1 \cap Z(H) = E = G_2 \cap Z(H)$. It follows that $G = G_1Z(H) = G_2Z(H)$ and G_1, G_2 are normal subgroups of G. Hence, $G_1 \cap G_2$ is a nontrivial normal subgroup of G, contradicting the faithfulness of $\mathfrak{G}$. When $G = Q_8 \times Z_4$, suppose $Q_8 = \langle x, y \mid x^2 = y^2, x^y = x^{-1}\rangle$, $Z_4 = \langle z \mid z^4 = e\rangle$. Then $\mathfrak{G} = \{Q_8, \langle xz \rangle\}$ is minimal but $\mathfrak{G}' = \{\langle x^2 \rangle, \langle x^2 z^2 \rangle\}$ is not. Under the hypothesis $G \not\cong Q_8 \times Z_4$, (a) any counterexample is not a nontrivial direct product. We also have, (b) g^p is central for all $g \in G$, since $G/Z \cong Z_p \times Z_p$. By Lemma 2, since $|G_1 \cap Z(G)| = p = |G_2 \cap Z(G)|$, we may assume without loss of generality that $G_1 \cap Z(G) = \langle z_2 \rangle$, $G_2 \cap Z(G) = \langle z_1^{pr} z_2 \rangle$ where $(r, p) = 1$ because $G_i \supseteqq \langle z_1^p \rangle$ implies $G_i \supseteqq \langle z_1 \rangle$. Also, if $|G_i| = p^3$ then $G_i \cap Z_{p^2} = E$ yields $G = G_i Z_{p^2}$: Let $g \in G_i$, $h \in G$ then $h = g_1 z$, $g_1 \in G_i$, $z \in Z_{p^2}$ hence $g^h = g^{g_1 z} = g^{g_2} \in G_i$ so G_i is normal in G and $G = G_i \times Z_{p^2}$, contradicting (a). We deduce, (c) $|G_i| \leqq p^2$, $i = 1, 2$ and $\mu(G) \geqq 2p^3$.

Let M be a maximal subgroup of G containing $Z(G)$, then M is abelian and has one of the forms:

(i) $M = \langle a \rangle \times \langle b \rangle \times \langle c \rangle \cong Z_{p^2} \times Z_p \times Z_p$,

(ii) $M = \langle a \rangle \times \langle b \rangle \cong Z_{p^3} \times Z_p$,

(iii) $M = \langle a \rangle \times \langle b \rangle \cong Z_{p^2} \times Z_{p^2}$.

Case (i). We can choose a, b, c so that $Z(G) = \langle a \rangle \times \langle b \rangle$ and then $[\langle a, c \rangle \cap \langle b, c \rangle] \cap Z(G) = \langle c \rangle \cap Z(G) = E$ giving $\mu(G) \leqq p^2 + p^3 < 2p^3$, contradicting (c). Case (ii). $Z(G) = \langle a^p \rangle \times \langle b \rangle$. Suppose $G/M = \langle cM \rangle$. $c^p = e$ implies case (i) holds. $c^p \neq e$ then $c^p = a^{pr} b^s$ by (b). If $p \mid r$, let $c_1 = ca^{-r} \notin M$ then $c_1^p = b^s$ and $\{\langle a \rangle, \langle c_1, b \rangle\}$ is faithful of degree less than $2p^3$. Hence for all $c \in G \backslash M$ $\langle c \rangle \cap \langle a \rangle \neq E$. Let $\mathfrak{G} = \{G_1, G_2\}$ be minimal then by Lemma 2, $G_i \cap \langle a \rangle = E$ and it follows that $|G_i| = p$, contradicting the minimality of $\mathfrak{G}$. Case (iii). Without loss of generality we may assume $Z(G) = \langle a \rangle \times \langle b^p \rangle$. Suppose $G/M = \langle cM \rangle$. $c^p = e$ implies case (i) holds. If $c^{p^2} \neq e$ then $\langle c \rangle \cap \langle a \rangle = E$ or $\langle c \rangle \cap \langle b \rangle = E$ so that $|c| = p^3$ and $\{\langle c \rangle, \langle a \rangle\}$ or $\{\langle c \rangle, \langle b \rangle\}$ is faithful of degree less than $2p^3$. This leaves the case $c^{p^2} = e$. c^p is central, $c^p = a^{pr} b^{ps}$, say, but $(ca^{-r})^p = b^{ps}$ and $ca^{-r} \notin M$. As above, $b^{ps} = e$ reduces to case (i). We may now assume that

$$G = \langle a, b, c \mid a^{p^2} = b^{p^2} = c^{p^2} = e = [a, b] = [a, c], b^p = c^p, [b, c] = a^{pu} b^{pv} \rangle .$$

If $a^{pu} = e$ then G is a nontrivial direct product. If $b^{pv} \neq e$ we can choose a so that $[b, c] = (a^p b^p)^v$ then $[ab, ac] = [b, c] = (ab)^{pv}$ but $G = \langle a, ab, ac \rangle$ and we proceed as above. By suitable choice of a it remains to eliminate the case $[b, c] = a^p$. Since $(b^{-1}c)^p = [b, c]^{-1/2\, p(p+1)}$, when $p \neq 2$ $(b^{-1}c)^p = e$ and when $p = 2$ $(ab^{-1}c)^2 = e$. In either case G/M can be generated by an element of order p. This completes the argument.

While attacking groups of order p^6 by identical methods to Theorem 5, one obtains the following counterexample.

THEOREM 6. *Let* $G = \langle a, b, c \mid a^{p^3} = b^{p^2} = c^p = 1 = [a, b] = [a, c], [c, b] = a^{p^2} \rangle$ *then*

(i) $|G| = p^6$ *and* $Z(G) = \langle a \rangle \times \langle b^p \rangle \cong Z_{p^3} \times Z_p$,

(ii) *G is not a nontrivial direct product,*

(iii) $\mu(G) = p^2 + p^4$,

(iv) $\mathfrak{G} = \{\langle ab, c\rangle, \langle b\rangle\}$ *is a minimal representation of* G, *but* $\mathfrak{G}' = \{\langle ab, c\rangle \cap Z(G), \langle b\rangle \cap Z(G)\}$ *is not minimal.*

Proof. (i) For $1 \leqq i \leqq p^2$ define α_i, β_i, γ_i by

$$\alpha_i\colon (r, i, s) \mapsto (r, i, s+1)$$

$$\beta_i\colon (r, i, s) \mapsto (r+s, i, s+2)$$

$$\gamma_i\colon (r, i, s) \mapsto (r+1, i, s)$$

$1 \leqq r$, $s \leqq p$, mod p in the first and third components [i.e., $\alpha_1 = ((1, 1, 1)(1, 1, 2) \cdots (1, 1, p))((2, 1, 1)(2, 1, 2) \cdots (2, 1, p)) \cdots ((p, 1, 1) \cdots (p, 1, p))$]. α_i, β_i, γ_i each have order p and $[\alpha_i, \beta_i] = \gamma_i$. Define λ, μ, ν as follows

$$\lambda\colon (r, i, s) \mapsto \begin{cases} (r, i+1, s), \ 1 \leqq i \leqq p^2 \\ (r+1, 1, s), \ i = p^2 \end{cases}$$

$$\mu = (12 \cdots p^2) \prod_{i=1}^{p^2} \beta_i$$

$$\nu = \prod_{i=1}^{p^2} \alpha_i \,.$$

λ, μ, ν satisfy $\lambda^{p^3} = \mu^{p^2} = \nu^p = 1 = [\lambda, \mu] = [\lambda, \nu]$, $[\nu, \mu] = \lambda^{p^2}$. Clearly any element of G has the form $a^i b^j c^k$, $0 \leqq i < p^3$, $0 \leqq j < p^2$, $0 \leqq k < p$ and the representation shows that these are distinct and (i) follows.

(ii) Suppose $G = H \times K$, then $Z(G) = Z(H) \times Z(K)$. We may assume $Z(H) \cong Z_p$ and $Z(K) = \langle ab^{ps}\rangle \cong Z_{p^3}$. $K \cap \langle b\rangle = E$ implies $|K| \leqq p^4$. If $|K| = p^4$ K and H are abelian and consequently G is abelian. It follows that $|K| = |H| = p^3$. Therefore, there exist $h \in H$ and r, $0 \leqq r < p^3$ such that $c = (ab^{ps})^r h$ then $[h, b] = [(ab^{ps})^r h, b]$ (since $(ab^{ps})^r$ is central) $= [c, b] = a^{p^2}$. But H is normal in G and so $a^{p^2} = [h, b] \in H \cap K$, a contradiction.

(iii) Let $\mathfrak{G} = \{G_1, G_2\}$ be a minimal faithful representation of G. This always exists by [1], Theorem 3. If $|G\colon G_i| = p$ then G_i is normal in G and G is a nontrivial direct product. Therefore, $|G\colon G_i| \geqq p^2$, $i = 1, 2$. For some i, $G_i \cap \langle a\rangle = E$, since $\mathfrak{G}$ is faithful suppose, say, $G_1 \cap \langle a\rangle = E$. If $|G_1| = p^3$, $G = G_1 \times \langle a\rangle$ since a is central. Hence $\mu(G) \geqq p^2 + p^4$ but (i) exhibits a faithful representation of degree $p^2 + p^4$. The final part of the theorem is now easy.

The converse problem: Given $\mathfrak{G}' = \{Z_1, \cdots, Z_n\}$, $n = d(Z(G))$ a minimal representation of $Z(G)$, does there exist a minimal representation $\mathfrak{G} = \{G_1, \cdots, G_n\}$ of G such that $G_i \cap Z(G) = Z_i$? The answer to this question is quickly found to be negative.

LEMMA 7. *Let $G = H \times K$ where $H = \langle a, b \mid a^p = b^p = [a, b]\rangle$ and $K = \langle c \mid c^p = e\rangle$ then $\mathfrak{G}' = \{\langle a^p c\rangle, \langle c\rangle\}$ is a minimal representation of $Z(G)$ which cannot be extended to a minimal representation of G.*

Proof. When $p \neq 2$ H is the non-abelian group of order p^3 containing an element of order p^2 and when $p = 2$ H is the quaternionic group of order 8. $Z(H) = \langle a^p\rangle$ and $\mathfrak{G}'$ is obviously minimal. Now

$$\begin{aligned}(a^i b^j)^p &= b^{jp}(b^{-jp}a^i b^{jp})(b^{-j(p-1)}a^i b^{j(p-1)}) \cdots (b^{-j}a^i b^j)\,, \qquad j \neq 0 \\ &= a^{(i+j)p+ijp(1+\cdots+p)}, \text{ since } a^b = a^{p+1},\ (a^i)^{b^m} = a^{i(mp+1)}\,.\end{aligned}$$

Case I. $p \neq 2$ then $p \mid (1 + \cdots + p) = 1/2\,p(p+1)$ and

$$(*) \qquad (a^i b^j c^k)^p = a^{(i+j)p} \text{ for all } i, j, k\,.$$

Every element of G has the form $a^i b^j c^k$, $0 \leqq i < p^2$, $0 \leqq j$, $k < p$. If $G_1 \supseteqq \langle a^p c\rangle$ then $a^i b^j c^k \in G_1$ implies that $i + j = 0 \pmod p$ i.e., $j = rp - i$ consequently for each choice of i there is only one choice for j. It follows that $|G_1| \leqq p^2$ and $|G: G_1| \geqq p^2$ since $G_1 \cap \langle c\rangle = E$. By $(*)$, $(ab^{p-1})^p = a^{p2} = e$, $\langle ab^{p-1}\rangle \cap Z(H) = E$ and trivially $\mu(H) = p^2$. By [3], $\mu(G) = \mu(H) + \mu(K) = p^2 + p$. $G_2 \supseteqq \langle c\rangle$ so $Z(H) \cap G_2 = E$ and $\{H, G_2\}$ is faithful. Therefore, $|G: H| + |G: G_2| \geqq \mu(G) = p^2 + p$ and $|G: G_2| \geqq p^2$. Hence $\deg\{G_1, G_2\} = |G: G_1| + |G: G_2| \geqq 2p^2 > \mu(G)$ proving $\{G_1, G_2\}$ is not minimal.

Case II. $p = 2$, $\mu(H) = 8$ and $\mu(G) = \mu(H) + \mu(K) = 10$, by [3]. $(*)$ becomes

$$(a^i b^j c^k)^2 = a^{(i+j)2+ij2} = \begin{cases} e, & i, j \text{ both even} \\ a^2, & \text{otherwise}\,. \end{cases}$$

One easily checks that $G_1 = \langle a^2 c\rangle$, $G_2 = \langle c\rangle$ and $\deg\{G_1, G_2\} = 16 > \mu(G)$ which proves the lemma.

REFERENCES

1. D. L. Johnson, *Minimal permutation representations of finite groups*, Amer. J. Math., **93** (1971), 857-866.

2. D. Wright, *Degrees of minimal permutation representations of covering groups of abelian groups*, Amer. J. Math., (to appear).

3. ———, *Degrees of minimal embeddings for some direct products*, Amer. J. Math., (to appear).

Received June 12, 1973. May I acknowledge the generous financial assistance of the Science Research Council and the first class advice of Dr. D. L. Johnson.

UNIVERSITY OF NOTTINGHAM

Present address: AUSTRALIAN NATIONAL UNIVERSITY