ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 12, Number 2, Spring 1982

A UNIVERSAL EXAMPLE OF A CORE-FREE PERMUTABLE SUBGROUP

FLETCHER GROSS AND T.R. BERGER

Introduction. Let H be a core-free permutable subgroup of the group G. This means that there is no non-identity normal subgroup of G contained in H and that $HK = KH$ for every subgroup K in G. (The term quasinormal has been used instead of permutable, but we feel that permutable, Stonehewer's word, is preferable since it is more descriptive.) In proving results about the structure of H, a reduction often is made to the special case when G is a finite p-group and $G = HC$ for some cyclic subgroup C. As examples of the sort of results obtainable in this way, we mention two: (1) H is residually finite nilpotent ([1] and [8]). (2) If n is any integer, then the set $\{x \in H | x^n = 1\}$ is a nilpotent subgroup of H and the class and derived length of this subgroup are bounded from above by functions of n ([2]; the best-possible bounds are given in [3]).

The study of the special case $G = HC$ with C cyclic and G a finite p-group has also led to the construction of counter-examples. Thus, although Itô and Szep [6] showed that H is nilpotent if G is finite, H need not be solvable if G is infinite. This follows from applying Theorem 3.3 of [1] to the finite groups constructed by Stonehewer in [9]. Stonehewer's groups all have the special structure referred to earlier. A study of Stonehewer's examples suggested that there might be a "universal" example. The main result of this paper then is the following.

THEOREM, *Let p be any prime and n a positive integer. Then there is a group* $G = H\langle x\rangle$ *such that*:

(i) *H is a core-free permutable subgroup of G and x has order p^n.*

(ii) *If $G^* = H^*\langle x^*\rangle$ where H^* is a core-free permutable subgroup of G^* and x^* has order p^n, then there is one and only one monomorphism ϕ of G^* into G such that $\phi(x^*) = x$ and $\phi(H^*) \leqq H$.*

The group G in this theorem is a finite p-group which will be constructed as a transitive permutation group with H being the stabilizer of a point. This procedure was suggested by Stonehewer's work although his groups are not the same as ours.

Originally, it was our intention to use the above theorem to try to prove

Received by the editors on May 8, 1978.

that, in general, a core-free permutable subgroup must be locally nilpotent or locally solvable. However by using an infinite analogue of our groups, one of the authors of this paper succeeded in constructing an example in which H is not locally solvable [**4**]. This example depends heavily on the properties proved in the present paper about the groups of the theorem. In particular, in the groups in the above theorem, H decomposes as a direct product in a nice way.

After some preliminary results in §2, we construct the groups in §3 and derive some of their properties. The "universal" property (part (ii) of the theorem) of these groups is proved in §4.

This work was done while the authors were attending a Group Theory Conference at the University of Warwick. We are deeply appreciative to Trevor Hawkes (who organized the conference) and to everyone else at the University of Warwick for their warm hospitality. We are particularly grateful to NATO and the Science Research Council for financial support during our stay at Warwick. We should also like to acknowledge some very useful discussions with Stewart Stonehewer.

2. Preliminaries. With a few exceptions, our notation is standard. If x and y are elements of a group G and m is a positive integer, then

$$[x, y; m] = [x, y, y, \ldots, y]$$

where y occurs m times. We also use this when x and y are subgroups of G. The lower central series $\{L_n(G)|n = 1, 2, \ldots\}$ is defined by $L_1(G) = G$ and $L_{n+1}(G) = [L_n(G), G]$. If G is nilpotent (solvable), then $\mathrm{c}(G)$ $(\mathrm{d}(G))$ denotes the class (derived length) of G. If H is a subgroup of G, then H_G, the core of H in G, is the intersection of all conjugates of H in G. The set of primes p such that G contains an element of order p is denoted by $\pi(G)$ $\mathbf{Z}$ is the additive group of integers while $Z(G)$ is the center of G.

We now prove some preliminary results. One of these, Corollary 2.3, surely is not new, but the authors have not found a reference in the literature. Thus, for the sake of completeness, we have included a proof.

LEMMA 2.1. *Let $G = HC$ where C is cyclic and H is a core-free permutable subgroup. Then G is nilpotent, H is finite, and $\pi(G) = \pi(C)$.*

PROOF. If $|C| = \infty$, then C normalizes H by either Theorem 4.1 of [**1**] or Lemma 2.1 of [**8**]. It follows from this that $H = 1$ and then the lemma certainly is true. Now suppose C has finite order. Since $H_G = 1$, $|G| \leqq |G\colon H|!$ and so G is finite. Then H is contained in the hypercenter $Z_\infty(G)$ [**7**]. Since $G/Z_\infty(G)$ then must be cyclic, we conclude that G is nilpotent. If q is any prime not dividing $|C|$, then H must contain a Sylow q-subgroup of G. The nilpotence of G and the fact that $H_G = 1$ now combine to imply that q does not divide $|G|$. Thus $\pi(G) = \pi(C)$.

LEMMA 2.2. *Let p be a prime, n a positive integer, $m = p^n$, and G a subgroup of the symmetric group S_m. Assume that G contains an m-cycle x and that $Z(G) \neq 1$. Let x_1 be an element of order p in $\langle x \rangle$, let $\Gamma_1, \ldots, \Gamma_r$ be all the orbits of $\langle x_1 \rangle$, and let $K = \{g \in G | \Gamma_i g = \Gamma_i \text{ for } 1 \leqq i \leqq r\}$. Then the following are true:*

(1) $x_1 \in Z(G) \leqq C_G(x) = \langle x \rangle$.

(2) *$r = p^{n-1}$, G transitively permutes $\Gamma_1, \ldots, \Gamma_r$ among themselves, and K is the kernel of this permutation representation.*

(3) *K is an elementary abelian p-group of order $\leqq p^r$.*

(4) *If G is a Sylow p-subgroup of S_m, then $|K| = p^r$ and G/K is a Sylow p-subgroup of S_r.*

(5) *If the stabilizer in G of a point is a permutable subgroup of G, then G is a p-group and $K = \Omega_1(G)$.*

PROOF. Since $\langle x \rangle$ is an abelian regular permutation group, $C_G(\langle x \rangle)$ must be $\langle x \rangle$. Then $Z(G) \leqq \langle x \rangle$. Since $\langle x \rangle$ is a cyclic p-group and since $Z(G) \neq 1$, this implies that $x_1 \in Z(G)$. Then $\langle x_1 \rangle \trianglelefteq G$ and so G must permute the orbits of $\langle x_1 \rangle$. Each orbit of $\langle x_1 \rangle$ has length p and so $r = p^{n-1}$. We now have proved (1) and (2).

Now suppose y and z are elements of K. Then Γ_i is fixed by x_1, y, and z and so x_1, y and z will induce permutations a_i, b_i, and c_i, respectively, on Γ_i. Now $\langle a_i \rangle$ is a regular, abelian, permutation group on Γ_i and a_i commutes with both b_i and c_i (since $x_1 \in Z(G)$). This forces b_i and c_i to belong to $\langle a_i \rangle$. Then $b_1^p = [b_i, c_i] = 1$ for all i. Therefore, $y^p = [y, z] = 1$ and so K is an elementary abelian p-group. There are at most p choices for each b_i and thus $|K| \leqq p^r$.

Now suppose G is a Sylow p-subgorup of S_m. Then $|G| = p^M$ where $M = (p^n - 1)/(p - 1)$. Since G/K is a subgroup of S_r, we see that $|G/K| \leqq p^N$ where $N = (p^{n-1} - 1)/(p - 1)$. But then

$$p^r \geqq |K| = |G|/|G/K| \geqq p^{M-N} = p^r.$$

This immediately implies that $|K| = p^r$ and that G/K is a Sylow p-subgroup of S_r. This proves (4).

Now assume that H, the stabilizer in G of a point, is a permutable subgroup of G. (We are no longer assuming that G is a Sylow p-subgroup of S_m.) Since $\langle x \rangle$ is transitive, we conclude that $G = H\langle x \rangle$ and that, since only the identity fixes everything, H is core-free in G. Lemma 2.1 now implies that G is a p-group. Now HK/K fixes a point (HK/K fixes the Γ_i which contains the point stabilized by H) and HK/K is core-free in G/K. This implies that $(HK)_G = K$. But $K \leqq \Omega_1(G)$ by (3) and obviously $\Omega_1(\langle x \rangle) = \langle x_1 \rangle \leqq K$. Hence, using **[2**, Lemma 3.1],

$$HK \geqq \Omega_1(H)\Omega_1(\langle x \rangle) = \Omega_1(G) \geqq K.$$

Since $(HK)_G = K$, we obtain $K = \Omega_1(G)$ and the lemma is proved.

COROLLARY 2.3. *Let x be an m-cycle in the symmetric group S_m where $m = p^n > 1$ and p is a prime. Then there is one and only one Sylow p-subgroup of S_m which contains x.*

PROOF. If $n = 1$, the result is obvious. Now assume $n > 1$ and use induction on n. Suppose P and Q are both Sylow p-subgroups of S_m containing x and let x_1 be an element of order p in $\langle x\rangle$. Let G be the centralizer of x_1 in S_m. Then G contains both P and Q by Lemma 2.2(1). The lemma also implies that G contains a normal elementary abelian p-subgroup K such that G/K is isomorphic to a subgroup of S_r where $r = p^{n-1}$. $K \leqq P \cap Q$ since K is a normal p-subgroup in G and P and Q are Sylow p-subgroups of G. Then P/K and Q/K are both Sylow p-subgroups of S_r. Since P/K and Q/K both contain the r-cycle Kx, we may use induction to obtain $P/K = Q/K$. Then $P = Q$ and the corollary is proved.

LEMMA 2.4. *Let $G = H\langle x\rangle$ be a p-group with H being a core-free permutable subgroup. Then* $[G, \Omega_2(\langle x\rangle); p - 1] = 1$.

PROOF. Let $A = \Omega_2(\langle x\rangle)$ and let M denote the core of H in HA. By Lemma 3.1(c) of **[2]**, HA/M has class $\leqq p - 1$. Therefore, $[H, A; p - 1] \leqq M \leqq H$. Since $G = H\langle x\rangle$ and $[\langle x\rangle, A] = 1$, this implies that

$$[G, A; p - 1] = [H, A; p - 1] \leqq H.$$

Since x normalizes $[G, A; p - 1]$ and since $H_G = 1$, it follows from this that $[G, A; p - 1] = 1$.

3. Construction of the groups. We fix some notation for the rest of the paper. For the benefit of the reader a glossary is included at the end.

Let p be a prime. If $p > 2$, set $e = 1$ and $r = p - 1$. If $p = 2$, set $e = r = 2$. Let n be a positive integer and let Γ_n be the additive group $\mathbf{Z}/p^n\mathbf{Z}$. The permutation of Γ_n given by

$$p^n\mathbf{Z} + a \to p^n\mathbf{Z} + a + 1$$

is denoted by x_n. If $0 \leqq m \leqq n$, then

$$x_{n,m} = x_n^{p^{n-m}}.$$

Then $x_{n,m} \in \langle x_n\rangle$, $x_{n,n} = x_n$, $x_{n,0} = 1$, and $x_{n,m}$ has order p^m. Let $\Gamma_{n,m}$ be the set of elements in Γ_n of order dividing p^m and let $\Delta_{n,m}$ be the set of elements in Γ_n of order precisely p^m. Then, if $m \geqq 1$, $\Delta_{n,m}$ is the set-theoretic difference $\Gamma_{n,m} - \Gamma_{n,m-1}$ and $|\Delta_{n,m}| = p^m - p^{m-1}$.

Now suppose $0 \leqq m \leqq n - e$. Then $x_{n,m}$ fixes the set $\Delta_{n,m+e}$ and so $\Delta_{n,m+e}$ is the union of orbits $\{\theta_{n,m,i}\}$ under $\langle x_{n,m}\rangle$. The number of such orbits is

$$|\Delta_{n,m+e}|/|\langle x_{n,m}\rangle| = (p^{m+e} - p^{m+e-1})/p^m = r.$$

Next, if $1 \leqq i \leqq r$, let $\pi_{n,m,i}$ be the permutation on $\theta_{n,m,i}$ induced by $x_{n,m}$. Let $\pi_{n,m,i}$ act on all of Γ_n by having $\pi_{n,m,i}$ fix every element not in $\theta_{n,m,i}$. Then let

$$A_{n,m} = \left\{\prod_{i=1}^{r} \pi_{n,m,i}^{c_i} \,\middle|\, \sum_{i=1}^{r} c_i = 0\right\}.$$

It is easily verified that $A_{n,m}$ is an abelian group which fixes every element of $\Gamma_n - \Delta_{n\ m+e}$. Since $\pi_{n,m,i}$ is a p^m-cycle and since $r \geqq 2$, $A_{n,m}$ is the direct product of $(r-1)$ copies of a cyclic group of order p^m. Hence $A_{n,m}$ has order $p^{m(r-1)}$ and exponent p^m. In particular, $A_{n,0} = 1$. If $k \leqq m$, then $x_{n,k}$ fixes $\theta_{n,m,i}$ for $1 \leqq i \leqq r$. It follows from this that $[x_{n,k}, A_{n,m}] = 1$. Since $A_{n,m}$ is abelian and since $A_{n,m}$ and $A_{n,m'}$ move different points if $m \neq m'$, we conclude that $[A_{n,m'}, A_{n,m'}] = 1$. For future reference, we list these results as a lemma.

LEMMA 3.1. *Let* $0 \leqq m \leqq n - e$. *Then*

(1) $A_{n,m}$ *is homocyclic of order* $p^{m(r-1)}$ *and exponent* p^m.

(2) *If* $\alpha \in \Gamma_n$ *and* $\alpha \notin \Delta_{n,m+e}$, *then* α *is fixed by every element of* $A_{n,m}$.

(3) $A_{n,0} = 1$.

(4) *If* $0 \leqq k \leqq m$, *then* $[A_{n,m}, x_{n,k}] = 1$.

(5) *If* $0 \leqq m' \leqq n - e$, *then* $[A_{n,m}, A_{n,m'}] = 1$.

Now let $G_n = \langle x_n, A_{n,m} | 0 \leqq m \leqq n - e\rangle$ and let H_n be the stabilizer in G_n of the zero element of Γ_n. G_n and H_n will turn out to be the groups in the theorem in the introduction. First, we list some elementary properties of G_n.

LEMMA 3.2. (1) *If* $n \leqq e$, *then* $H_n = 1$ *and* $G_n = \langle x_n\rangle$.

(2) $G_n = H_n\langle x_n\rangle$ *for all* n.

(3) H_n *is core-free in* G_n.

(4) $x_{n,e} \in Z(G_n)$.

(5) $A_{n,m} \leqq H_n$ *if* $0 \leqq m \leqq n - e$.

PROOF. If $n \leqq e$, then $G_n = \langle x_n\rangle$ and (1) follows at once. Since $\langle x_n\rangle$ is transitive, both (2) and (3) are valid. Lemma 3.1 (2) implies that $A_{n,m} \leqq H_n$ if $0 \leqq m \leqq n - e$. Also from Lemma 3.1, we see that $[x_{n,e}, A_{n,m}] = 1$ if either $m \geqq e$ or $m = 0$. Thus (4) is proved if $p > 2$. Assume now that $p = 2$ and $n \geqq 3$. Let a, b, c, and d denote $2^n\mathbf{Z} + 2^{n-3}$, $2^n\mathbf{Z} + 3\cdot 2^{n-3}$, $2^n\mathbf{Z} + 5\cdot 2^{n-3}$, and $2^n\mathbf{Z} + 7\cdot 2^{n-3}$, respectively. Then $A_{n,1} = \langle (ac)(bd)\rangle$. Now $x_{n,2}$ fixes the set $\{a, b, c, d\}$ and, on this set, $x_{n,2} = (abcd)$. It is immediate that $[x_{n,2}, A_{n,1}] = 1$. Hence $[x_{n,e}, A_{n,m}] = 1$ for all m and the lemma is proved.

By Corollary 2.3, there is exactly one Sylow p-subgroup of the group of all permutations of Γ_n which contains x_n. Denote this Sylow p-subgroup by P_n and let the stabilizer in P_n of the zero element of Γ_n be denoted by Q_n. We now prove that $G_n \leqq P_n$ (so, in particular, G_n is a p-group) and there is a homomorphism of G_n onto G_{n-1}.

LEMMA 3.3. *The following are true.*

(1) $x_{n,1} \in Z(P_n)$.
(2) $G_n \leqq P_n$.
(3) *If* $n > 1$, *then there is a homomorphism* τ_n *of* P_n *onto* P_{n-1} *such that* $(P^{n-1}\mathbf{Z} + a)\tau_n(g) = p^{n-1}\mathbf{Z} + b$ *if* $(P^n\mathbf{Z} + a)g = P^n\mathbf{Z} + b$, *for all* $g \in P_n$ *and* a *and* $b \in \mathbf{Z}$.
(4) $\tau_n(x_{n,m}) = x_{n-1,m-1}$ *if* $n > 1$ *and* $m \geqq 1$.
(5) $\tau_n(A_{n,m}) = A_{n-1,m-1}$ *if* $1 \leqq m \leqq n - e$.
(6) $\tau_n(G_n) = G_{n-1}$ *if* $n > 1$.
(7) $\tau_n(Q_n) = Q_{n-1}$ *if* $n > 1$.
(8) $\tau_n(H_n) = H_{n-1}$ *if* $n > 1$.
(9) K_n, *the kernel of* τ_n, *is elementary abelian of order* $p^{p^{n-1}}$.
(10) $\langle x_{n,1}\rangle A_{n,1} \leqq K_n$ *if* $n \geqq e + 1$.
(11) $P_n = \langle x_n\rangle Q_n$ and $H_n = G_n \cap Q_n$.

PROOF. (1) follows from Lemma 2.2 (1). If $n = 1$, the lemma certainly is true. Now assume $n > 1$ and let C be the group generated by P_n and G_n. $Z(C)$ contains $x_{n,1}$ by Lemma 3.2 (4) and so C satisfies the hypothesis of Lemma 2.2. It follows from this that C has a normal subgroup K_n such that K_n is an elementary abelian p-group and C/K_n is faithfully represented as a permutation group on the set of all orbits of $\langle x_{n,1}\rangle$. These orbits are simply the cosets of $p^{n-1}\mathbf{Z}/p^n\mathbf{Z}$ in $\mathbf{Z}/p^n\mathbf{Z}$. Thus the orbits of $\langle x_{n,1}\rangle$ are in a natural one-to-one correspondence with the elements of $\mathbf{Z}/p^{n-1}\mathbf{Z}$. Thus, we obtain a homomorphism τ_n of C onto a permutation group on Γ_{n-1} such that the kernel of τ_n is K_n and, if a and b are integers, $g \in C$, and if

$$(p^n\mathbf{Z} + a)g = p^n\mathbf{Z} + b,$$

then

$$(p^{n-1}\mathbf{Z} + a)\tau_n(g) = p^{n-1}\mathbf{Z} + b.$$

An immediate consequence of this is that $\tau_n(x_n) = x_{n-1}$. It then follows that $\tau_n(A_{n,m}) = A_{n-1,m-1}$ if $1 \leqq m \leqq n - e$. This implies that $\tau_n(G_n) = G_{n-1}$. By induction, we may assume that G_{n-1} is a p-group. Since the kernel of τ_n is a p-group, this implies that G_n is a p-group. Since $x_n \in G_n$, Corollary 2.3 implies that $G_n \leqq P_n$. Then $C = P_n$. Lemma 2.2 (4) now implies that $\tau_n(P_n) = P_{n-1}$ and $|K_n| = p^{p^{n-1}}$. We now have proved parts (1), (2), (3), (4), (5), (6), and (9) of the Lemma. Part (10) follows from parts (4) and (5).

Since $\langle x_n\rangle$ is transitive, $P_n = \langle x_n\rangle Q_n$. Clearly $H_n = G_n \cap Q_n$ from the definitions of H_n and Q_n. From (3), $\tau_n(Q_n)$ fixes the zero element of Γ_{n-1}. Hence $\tau_n(Q_n) \leqq Q_{n-1}$ and $\tau_n(H_n) \leqq H_{n-1}$. Now suppose $g \in P_n$ and $\tau_n(g) \in Q_{n-1}$. Then g fixes all orbits of $\langle x_{n,1}\rangle$ and so g certainly fixes $\Gamma_{n,1}(\Gamma_{n,1}$ is the orbit of $p^n\mathbf{Z} + 0$ under $\langle x_{n,1}\rangle)$. Since $\langle x_{n,1}\rangle$ is transitive on $\Gamma_{n,1}$, we see that there is an integer k such that $gx_{n,1}^k$ fixes $p^n\mathbf{Z} + 0$. Hence $gx_{n,1}^k \in Q_n$. Since $x_{n,1} \in K_n$, we find that

$$\tau_n(g) = \tau_n(gx_{n,1}^k) \in \tau_n(Q_n).$$

Since $Q_{n-1} \leqq \tau_n(P_n)$, this implies that $Q_{n-1} = \tau_n(Q_n)$. If $g \in G_n$ and $\tau_n(g) \in H_{n-1}$, then as before, there is an integer k such that $gx_{n,1}^k \in H_n$. This implies that $\tau_n(g) \in \tau_n(H_n)$. Since $H_{n-1} \leqq \tau_n(G_n)$, we conclude that $H_{n-1} = \tau_n(H_n)$. This finishes the proof of the lemma.

Corollary 3.4. (1) *The exponent of* G_n is p^n.
(2) *The exponent of* H_n is $\mathrm{Max}\{1, p^{n-e}\}$.
(3) *If* $n \geqq 2$, *then* $G_n = C_{G_n}(x_{n,2})(G_n \cap K_n)$.

Proof. Since G_n is a p-subgroup of the symmetric group of degree p^n and since G contains an element of order p^n, part (1) is clear. If $n \leqq e$, then $H_n = 1$. Assume now that $n > e$. Then $H_{n-1} = \tau_n(H_n)$ has exponent p^{n-e-1} by induction. Since $A_{n,n-e}$ contains elements of order p^{n-e} and since the kernel of τ_n has exponent p, we see that H_n has exponent p^{n-e}.

Now suppose $n \geqq 2$. From Lemma 3.1 (4), we obtain

$$C_{G_n}(x_{n,2}) \geqq \langle x_n, A_{n,m} | 2 \leqq m \leqq n - e\rangle.$$

But $A_{n,1} \leqq G_n \cap K_n \trianglelefteq G_n$. This immediately implies (3).

Eventually, we will show that H_n is a permutable subgroup of G_n and that $K_n \cap G_n = \Omega_1(G_n)$. The proof of this will be by induction on n. To begin the induction, we need to know the structure of G_n when $n \leqq e + 1$. If $n \leqq e$, then $G_n = \langle x_n\rangle$ and $H_n = 1$. Thus, if $1 < n \leqq e$, then it follows from Lemma 3.3 (4, 9) that $K_n \cap G_n = \langle x_{n,1}\rangle$. This leaves G_3 when $p = 2$ and G_2 when $p > 2$. We consider these separately.

Lemma. 3.5. *Assume* $p = 2$. *Then* G_3 *has order 16, class 2, and exponent 8.* $H_3 = A_{3,1}$ *is a permutable subgroup of* G_3, $G_3 \cap K_3 = \Omega_1(G_3) = \langle x_{3,1}\rangle \times A_{3,1}$, $\Omega_1(G_3)$ *has order 4, and* $\mho^2(G_3) = \langle x_{3,1}\rangle$.

Proof. By direct computation, $x_3 = (0\ 1\ 2\ 3\ 4\ 5\ 6\ 7)$ and $A_{3,1} = \langle y\rangle$ where $y = (1\ 5)\ (3\ 7)$ where we have written i instead of $2^3\mathbf{Z} + \mathbf{i}$. Now $y^{-1}x_3y = x_3^5$ and so $G_3 = \langle x_3, y\rangle = \langle x_3\rangle\ \langle y\rangle$. Hence $H_3 = \langle y\rangle$. The permutability of H_3 follows from Lemma 4.1 of **[2]**. The rest of the lemma follows by a direct calculation and from Lemma 2.2 (5).

Lemma 3.6. *Assume* $p > 2$. *Then* G_2 *has order* p^p, *class* $p - 1$, *and exponent* p^2. $H_2 = A_{2,1}$ *is a permutable sungroup of* G_2,

$$G_2 \cap K_2 = \Omega_1(G_2) = \langle x_{2,1} \rangle \times A_{1,2},$$

$\Omega_1(G_2)$ has order p^{p-1}, and $\mho^1(G_2) = \langle x_{2,1} \rangle$.

PROOF. $G_2 = \langle x_2, A_{2,1} \rangle$. Let π_0 be the permutation induced by $x_{2,1}$ on $\Gamma_{2,1}$ and have π_0 fix all the elements of Γ_2 not in $\Gamma_{2,1}$. Then

$$x_{2,1} = \pi_0 \prod_{i=1}^{p-1} \pi_{2,1,i}.$$

Now $\pi_0^k = \pi_0^{(1-p)k}$ for any integer k and

$$(1 - p)k + \sum_{i=1}^{p-1} (c_i + k) = \sum_{i=1}^{p-1} c_i.$$

It follows from this, letting $\pi_i = \pi_{2,1,i}$ if $1 \leqq i \leqq p - 1$, that

$$\langle x_{2,1} \rangle A_{2,1} \leqq \left\{ \prod_{i=0}^{p-1} \pi_i^{c_i} \,\middle|\, \sum_{i=0}^{p-1} c_i = 0 \right\}.$$

The right-hand-side has order p^{p-1} since $|\pi_i| = p$ for all i. But $|A_{2,1}| = p^{p-2}$ from Lemma 3.1 and so the left-hand-side has order p^{p-1}. Thus

$$\langle x_{2,1} \rangle A_{2,1} = \left\{ \prod_{i=0}^{p-1} \pi_i^{c_i} \,\middle|\, \sum_{i=0}^{p-1} c_i = 0 \right\}.$$

Since conjugation by x_2 permutes $\pi_0, \ldots, \pi_{p-1}$ among themselves, this implies that $\langle x_{2,1} \rangle A_{2,1}$ is a normal subgroup of G_2. Then

$$G_2 = \langle x_2, A_{2,1} \rangle = \langle x_2 \rangle (\langle x_{2,1} \rangle A_{2,1}) = \langle x_2 \rangle A_{2,1}.$$

It follows from this that $H_2 = A_{2,1}$ and that $|G_2| = p^p$. Then $c(G_2) \leqq p - 1$ which implies that $\Omega_1(G_2)$ has exponent p. It follows from this that $\Omega_1(G_2) = \langle x_{2,1} \rangle A_{2,1}$. Since K_2 is elementary abelian and since $K_2 \geqq \langle x_{2,1} \rangle A_{2,1}$ from Lemma 3.3 (10), we obtain $G_2 \cap K_2 = \Omega_1(G_2)$. Now Lemma 2.2 (1) implies that

$$C_{G_2}(x_2) \cap \Omega_1(G_2) = \langle x_{2,1} \rangle.$$

Thus, the linear transformation induced by x_2 acting on $\Omega_1(G_2)$ written additively has a single Jordan block. Since $|\Omega_1(G_2)| = p^{p-1}$, it follows that

$$[\Omega_1(G_2), \langle x_2 \rangle; p - 2] \neq 1.$$

This implies that G_2 has class $p - 1$.

Since $G_2/\Omega_1(G_2)$ is abelian, we see that the p-th power of any commutator in G_2 is the identity. Since $c(G_2) < p$, Corollary 12.3.1 of [5] now implies that

$$\mho^1(G_2) = \mho^1(\langle x_2 \rangle \Omega_1(G_2)) = \mho^1(\langle x_2 \rangle) = \langle x_{2,1} \rangle.$$

It only remains to show that H_2 is a permutable subgroup of G_2. Let

T be any subgroup of G. If T has exponent $\leqq p$, then $T \leqq \Omega_1(G_2)$ and $TH_2 = H_2T$ since $H_2 \leqq \Omega_1(G_2)$ and $\Omega_1(G_2)$ is abelian. If T has exponent exceeding p, then $\mho^1(T) \neq 1$. This implies that $T \geqq \langle x_{2,1}\rangle$ and so

$$TH_2 = T\langle x_{2,1}\rangle H_2 = T\Omega_1(G_2) = G_2$$

(since $|G_2\colon \Omega_1(G_2)| = p$ and $T\Omega_1(G_2) \neq \Omega_1(G_2)$). Hence $TH_2 = H_2T$ in all cases and the lemma is proved.

To proceed further, we need another homomorphism ρ_n which will map $\langle x_{n,n-1}\rangle Q_n$ onto P_{n-1}.

LEMMA 3.7. *Assume $n > 1$. Then*

(1) *If $0 \leqq k \leqq n$, then $\langle x_{n,k}\rangle Q_n$ and $\langle x_{n,k}\rangle H_n$ are subgroups of P_n.*
(2) *$\langle x_{n,n-1}\rangle Q_n$ and $\langle x_{n,n-1}\rangle H_n$ are normal subgroups of P_n and G_n, respectively.*
(3) *There is a homomorphism ρ_n of $Q_n\langle x_{n,n-1}\rangle$ onto P_{n-1} such that for all $g \in \langle x_{n,n-1}\rangle Q_n$ and $a, b \in \mathbf{Z}$, $(p^{n-1}\mathbf{Z} + a)\rho_n(g) = p^{n-1}\mathbf{Z} + b$ if and only if $(p^n\mathbf{Z} + pa)g = p^n\mathbf{Z} + pb$.*
(4) *$\rho_n(x_{n,k}) = x_{n-1,k}$ if $0 \leqq k \leqq n-1$.*
(5) *$\rho_n(A_{n,m}) = A_{n-1,m}$ if $0 \leqq m \leqq n-e-1$.*
(6) *$\rho_n(A_{n,n-e}) = 1$.*
(7) *$\rho_n(Q_n) = Q_{n-1}$.*

PROOF. Since $P_n = \langle x_n\rangle Q_n$ is a p-group and $|P_n\colon Q_n| = p^n$, there must be a subgroup of P_n containing Q_n and of order $p^k|Q_n|$ for every k satisfying $0 \leqq k \leqq n$. But such a subgroup would have to be $\langle x_{n,k}\rangle Q_n$. $|P_n\colon \langle x_{n,n-1}\rangle Q_n| = p$ and so $\langle x_{n,n-1}\rangle Q_n$ is normal in P. Since $G_n \cap \langle x_{n,k}\rangle Q_n = \langle x_{n,k}\rangle H_n$, we have proved (1) and (2).

Now the orbit of $(p^n\mathbf{Z} + 0)$ under $Q_n\langle x_{n,n-1}\rangle$ is $\Gamma_{n,n-1}$. The mapping $p^{n-1}\mathbf{Z} + a \to p^n\mathbf{Z} + pa$ establishes a one-to-one correspondence between Γ_{n-1} and $\Gamma_{n,n-1}$. Thus, we obtain a representation ρ_n of $Q_n\langle x_{n,n-1}\rangle$ as a permutation group on Γ_{n-1} where

$$(p^{n-1}\mathbf{Z} + a)\rho_n(g) = p^{n-1}\mathbf{Z} + b$$

if and only if

$$(p^n\mathbf{Z} + pa)g = p^n\mathbf{Z} + pb$$

for all $g \in Q_n\langle x_{n,n-1}\rangle$ and $a, b \in \mathbf{Z}$. This certainly implies that $\rho_n(x_{n,n-1}) = x_{n-1}$. Since $\rho_n(Q_n\langle x_{n,n-1}\rangle)$ must be a p-group and since P_{n-1} is the only Sylow p-subgroup of the symmetric group of degree p^{n-1} which contains x_{n-1}, we find that $\rho_n(Q_n\langle x_{n,n-1}\rangle) \leqq P_{n-1}$.

Now let T be the kernel of ρ_n. Then T fixes every element of $\Gamma_{n,n-1}$. Since $|\Gamma_n - \Gamma_{n,n-1}| = p^n - p^{n-1}$ and since T is a p-group, we conclude that $|T| \leqq p^{N-1}$ where $N = p^{n-1}$.

But

$$|P_{n-1}| \geqq \rho_n(Q_n\langle x_{n,n-1}\rangle)| = |P_n|/p|T| \geqq |P_n|/p^N.$$

However, $|P_{n-1}| = |P_n|/p^N$ and so ρ_n must map $Q_n\langle x_{n,n-1}\rangle$ onto P_n. We now have proved (3) and the rest of the lemma follows by direct computation.

From parts (4), (5), and (6) of the previous lemma, we immediately conclude that $G_{n-1} \leqq \rho_n(H_n\langle x_{n,n-1}\rangle)$. To assert that this inclusion is an equality, we need to know generators for $H_n\langle x_{n,n-1}\rangle$. This is done in the next lemma. If $n > 1$, let R_n be the intersection of $H_n\langle x_{n,n-1}\rangle$ and the kernel of ρ_n.

LEMMA 3.8. *Assume $n \geqq e$. Then the following are true:*

(1) *R_n is the core of H_n in $H_n\langle x_{n,n-1}\rangle$.*

(2) *$x_n^{-i}A_{n,m}x_n^i \leqq \langle x_{n,n-1}, A_{n,\ell}|0 \leqq \ell \leqq n-e-1\rangle R_n$ for all integers i and $0 \leqq m \leqq n-e$.*

(3) *$H_n\langle x_{n,n-1}\rangle = \langle x_{n,n-1}, A_{n,\ell}|0 \leqq \ell \leqq n-e-1\rangle R_n$.*

(4) *$\rho_n(H_n\langle x_{n,n-1}\rangle) = G_{n-1}$.*

(5) *$\rho_n(H_n) = H_{n-1}$.*

PROOF. R_n consists of those elements of $H_n\langle x_{n,n-1}\rangle$ which fix every element of $\Gamma_{n,n-1}$. But $H_n\langle x_{n,n-1}\rangle$ is transitive on $\Gamma_{n,n-1}$ and H_n is the stabilizer of a point. Hence, R_n is the core of H_n in $H_n\langle x_{n,n-1}\rangle$.

Now let

$$L = \langle x_{n,n-1}, A_{n,\ell}|0 \leqq \ell \leqq n-e-1\rangle R_n$$

and

$$M = \langle x_{n,n-1}, x_n^{-i}A_{n,m}x_n^i|0 \leqq m \leqq n-e, \text{ all } i\}.$$

Then M and L are both contained in $H_n\langle x_{n,n-1}\rangle$. Since M is normalized by x_n and $\langle x_n, M\rangle = G_n$, we conclude that $M \lhd G_n = M\langle x_n\rangle$. Since $x_n^p \in M$ and since $|G_n\colon H_n\langle x_{n,n-1}\rangle| = p$, we obtain $M = H_n\langle x_{n,n-1}\rangle$. Assume now that (2) holds. Then $H_n\langle x_{n,n-1}\rangle \geqq L \geqq M$. Hence $L = H_n\langle x_{n,n-1}\rangle$. This together with Lemma 3.7 implies (4) and (5). Thus the lemma will be proved once we verify (2).

Now $A_{n,m} \leqq L$ for $0 \leqq m \leqq n-e$ (recall that $A_{n,n-e} \leqq R_n$ by Lemma 3.7 (6)) and $x_n^p \in L$. Hence it suffices to prove (2) when $1 \leqq i \leqq p-1$. We now consider 3 cases.

CASE 1. $0 \leqq m \leqq n-e-1$. Since $A_{n,m}$ fixes any element of Γ_n which does not have order p^{m+e} and since $p^{m+e} < p^n$, we see that $A_{n,m}$ fixes $p^n\mathbf{Z} + pa - i$. for all $a \in \mathbf{Z}$. (Recall that we are assuming $1 \leqq i \leqq p-1$.) This implies that

$$x_n^{-i}A_{n,m}x_n^i \leqq R_n \leqq L.$$

CASE 2. $m = n - e$ and $p > 2$. Then $A_{n,n-1} \leqq C_G(x_{n,n-1})$ by Lemma 3.1 (4). Then

$$x_n^{-i} A_{n,n-1} x_n^i \leqq C_{G_n}(x_{n,n-1}) \cap H_n\langle x_{n,n-1}\rangle = \langle x_{n,n-1}\rangle C_{H_n}(x_{n,n-1}).$$

But (1) implies that

$$R_n = \bigcap_i x_{n,n-1}^{-i} H_n x_{n,n-1}^i \geqq C_{H_n}(x_{n,n-1}).$$

It follows from this that

$$x_n^{-i} A_{n,n-1} x_n^i \leqq \langle x_{n,n-1}\rangle R_n \leqq L.$$

Case 3. $m = n - e$ and $p = 2$. In this case $e = 2$ and $i = 1$. If $1 \leqq k \leqq n - 2$, then define the permutation U_k on Γ_n by

$$(2^n\mathbf{Z} + a)\ U_k = \begin{cases} 2^n\mathbf{Z} + a + 2^{k+1} & \text{if } a \equiv 2^{k-1} \pmod{2^{k+1}} \\ 2^n\mathbf{Z} + a - 2^{k+1} & \text{if } a \equiv 2^{k-1} + 2^k \pmod{2^{k+1}} \\ 2^n\mathbf{Z} + \mathrm{a} & \text{otherwise.} \end{cases}$$

Then, as may be verified by a straight-forward calculation, $\langle U_k\rangle = A_{n,n-1-k}$. Thus it suffices to prove that $x_n^{-1} U_1 x_n \in L$.
Define v_k by

$$v_k = x_n^{(2^{k-1}-2)} U_k x_n^{-(2^{k-1}-2)}.$$

Then $v_1 = x_n^{-1} U_1 x_n$ and, by case 1, $v_k \in L$ if $2 \leqq k \leqq n - 2$. For $1 \leqq k \leqq n - 2$, we have

$$(2^n\mathbf{Z} + a)v_k = \begin{cases} 2^n\mathbf{Z} + a + 2^{k+1} & \text{if } a \equiv 2 \pmod{2^{k+1}} \\ 2^n\mathbf{Z} + a - 2^{k+1} & \text{if } a \equiv 2 + 2^k \pmod{2^{k+1}} \\ 2^n\mathbf{Z} + a & \text{otherwise.} \end{cases}$$

Now

$$(2^n\mathbf{Z} + a)x_n^4 v_1 = \begin{cases} 2^n\mathbf{Z} + a + 8 & \text{if } a \equiv 2 \pmod 4 \\ 2^n\mathbf{Z} + a + 4 & \text{if } a \text{ is odd} \\ 2^n\mathbf{Z} + a & \text{otherwise} \end{cases}$$

It is now an easy induction to verify that, if $1 \leqq \ell \leqq n - 2$, then

$$(2^n\mathbf{Z} + a)x_n^4 v_1 v_2 \cdots v_\ell = \begin{cases} 2^n\mathbf{Z} + a + 2^{\ell+2} & \text{if } a \equiv 2 \pmod{2^{\ell+1}} \\ 2^n\mathbf{Z} + a + 4 & \text{if } a \text{ is odd} \\ 2^n\mathbf{Z} + a & \text{otherwise} \end{cases}$$

Since x_n^4 and v_k belong to $H_n\langle x_{n,n-1}\rangle$ for all k, this implies that

$$x_n^4 v_1 v_2 \cdots v_{n-2} \in R_n \leqq L.$$

Since x_n^4 and $v_2, \ldots, x_{n-2}$ all belong to L, we conclude that $v_1 \in L$ and the lemma is proved.

COROLLARY 3.9. *If* $n > 1$, *then* $\langle x_{n,n-1}\rangle H_n$ is a subdirect product of p copies of G_{n-1}.

PROOF. If $n \leqq e$, then $H_n = 1$ and this is trivial. Now suppose $n > e$. Then, for all i,

$$\langle x_{n,n-1}\rangle H_n/(x_n^{-i}R_n x_n^i) \cong \langle x_{n,n-1}\rangle H_n/R_n \cong G_{n-1}.$$

Now $R_n \leqq H_n$ and $H_n\langle x_n^p\rangle$ normalizes R_n. Hence

$$1 = (H_n)_{G_n} = (R_n)_{G_n} = \bigcap_{i=0}^{p-1} x_n^{-i}R_n x_n^i.$$

The corollary now follows.

Before proving that H_n is a permutable subgroup of G_n, we first need to show that $\Omega_1(G_n) = K_n \bigcap G_n$ and that $\mho^{n-1}(G_n) = \langle x_{n,1}\rangle$. This is done in the next two lemmas.

LEMMA. 3.10. $\Omega_1(G_n) = \Omega_1(\langle x_n\rangle)\Omega_1(H_n) = K_n \cap G_n$. *In particular,* $\Omega_1(G_n)$ *is elementary abelian.*

PROOF. If $n \leqq e + 1$, this follows from previous results. Now assume $n > e + 1$ and let g be an element of order p in G_n. Then $\tau_n(g) \in \Omega_1(G_{n-1})$. By induction, $\Omega_1(G_{n-1}) \leqq K_{n-1}$. This implies that $\tau_n(g)$ fixes all the orbits of $\langle x_{n-1,1}\rangle = \langle \tau_n(x_{n,2})\rangle$. Since an orbit of $\langle x_{n,2}\rangle$ is the union of orbits of $\langle x_{n,1}\rangle$, this implies that g fixes all the orbits of $\langle x_{n,2}\rangle$. In particular, g fixes $\Gamma_{n,2}$. Then there is an integer k such that $gx_{n,2}^k \in H_n$. It follows from this that $g \in H_n\langle x_{n,2}\rangle \leqq H_n\langle x_{n,n-1}\rangle$ since $n - 1 \geqq e + 1 \geqq 2$.

From the above argument, we see that $\Omega_1(G_n) \leqq H_n\langle x_n^p\rangle$. Hence $\Omega_1(G_n) = \Omega_1(H_n\langle x_n^p\rangle)$. By induction, $\Omega_1(G_{n-1})$ is elementary abelian. Corollary 3.9 now implies that $\Omega_1(H_n\langle x_n^p\rangle)$ is elementary abelian. Hence $\Omega_1(G_n)$ is elementary abelian.

Clearly, $\rho_n(\Omega_1(G_n)) \leqq \Omega_1(G_{n-1})$ and, by induction,

$$\Omega_1(G_{n-1}) = \langle x_{n-1,1}\rangle\Omega_1(H_{n-1}) \leqq \rho_n(\langle x_{n,1}\rangle H_n).$$

Since $R_n \leqq H_n$, this implies that $\Omega_1(G_n) \leqq \langle x_{n,1}\rangle H_n$. From the fact that $x_{n,1} \in Z(G_n)$, we conclude that

$$\Omega_1(G_n) = \Omega_1(\langle x_{n,1}\rangle H_n) = \langle x_{n,1}\rangle \times \Omega_1(H_n).$$

Now $\langle x_{n,1}\rangle \leqq K_n \cap G_n \leqq \Omega_1(G_n) = \langle x_{n,1}\rangle\Omega_1(H_n)$. Hence $H_n(K_n \cap G_n) \geqq \Omega_1(G_n) \geqq (K_n \cap G_n)$. But $H_{n-1} = \tau_n(H_n)$ is core-free in $G_{n-1} = \tau_n(G_n)$ and K_n is the kernel of τ_n. This implies that $H_n(K_n \cap G_n)/(K_n \cap G_n)$

is core-free in $G_n/(K_n \cap G_n)$. It follows from this that $\Omega_n(G_n) = K_n \cap G_n$ and the lemma is proved.

COROLLARY 3.11. If $0 \leqq k \leqq n$, then $\Omega_k(G_n)$ has exponent p^k and $\Omega_k(G_n) = \Omega_k(\langle x_n \rangle)\Omega_k(H_n)$.

PROOF. If $k \leqq 1$, this has been done. Now $G_n \cap K_n$ has exponent p. Hence $\tau_n(\Omega_k(G_n)) = \Omega_{k-1}(G_{n-1})$. Similarly, $\tau_n(\Omega_k(H_n)) = \Omega_{k-1}(H_{n-1})$ and $\tau_n(\Omega_k(\langle x_n \rangle)) = \Omega_{k-1}(\langle x_{n-1} \rangle)$. The corollary now follows by induction on k.

LEMMA 3.12. (1) *If $n \geqq 2$, then $\langle x_{n,2} \rangle \Omega_1(G_n)$ has class $\leqq p-1$.*
(2) *If $n \geqq 1$, then $\mho^{n-1}(G_n) = \langle x_{n,1} \rangle$.*

PROOF. If $n \leqq e+1$, this follows from previous work. Assume now that $n > e+1$. Then $n \geqq e+2 \geqq 3$ and so both $\langle x_{n,2} \rangle$ and $\Omega_1(G_n)$ are contained in $\langle x_{n,n-1} \rangle H_n$. By induction, $c(\Omega_1(G_{n-1})\langle x_{n-1,2} \rangle) \leqq p-1$. Since $\rho_n(\Omega_1(G_n)) \leqq \Omega_1(G_{n-1})$, this implies that $L_p(\Omega_1(G_n)\langle x_{n,2} \rangle) \leqq R_n \leqq H_n$. But x_n normalizes $L_p(\Omega_1(G_n)\langle x_{n,2} \rangle)$ and

$$\bigcap_i x_n^{-i} H_n x_n^i = H_G = 1.$$

Hence $L_p(\Omega_1(G_n)\langle x_{n,2} \rangle) = 1$ and (1) is proved.

By, induction,

$$\mho^{n-2}(G_{n-1}) = \langle x_{n-1,1} \rangle.$$

This implies that

$$\mho^{n-2}(G_n) \leqq \langle x_{n,2} \rangle \Omega_1(G_n)$$

by taking inverse images under τ_n. It follows from this that

$$\mho^{n-1}(G_n) \leqq \mho^1(\langle x_{n,2} \rangle \Omega_1(G_n)).$$

Now $\langle x_{n,2} \rangle \Omega_1(G_n)$ has class $\leqq p-1$ and the commutator subgroup of $\langle x_{n,2} \rangle \Omega_1(G_n)$ is contained in the elementary abelian subgroup $\Omega_1(G_n)$. Corollary 12.3.1 of [5] now yields

$$\mho^{n\ 1}(G_n) \leqq \mho^1(x_{n,2} \rangle) = \langle x_{n,1} \rangle$$

and the lemma follows.

Finally, we prove part (1) of the theorem in the introduction.

THEOREM 3.13. *H_n is a permutable subgroup of G_n.*

PROOF. If $n \leqq e+1$, this has been done. Now assume $n > e+1$. By induction, H_{n-1} is a permutable subgroup of G_{n-1}. Taking inverse images under ρ_n and τ_n, we deduce that H_n and $H_n\Omega_1(G_n)$ are permutable subgroups of $H_n\langle x_{n,n-1} \rangle$ and G_n, respectively. Suppose now that T is a subgroup of G_n and $H_nT \neq TH_n$. Then T cannot be contained in $H_n\langle x_{n,n-1}\rangle$. But Corollary 3.11 and Corollary 3.4 imply that $H_n\langle x_{n,n-1}\rangle = \Omega_{n-1}(G_n)$. Hence $\mho^{n-1}(T) \neq 1$. Lemma 3.12 now implies that $\langle x_{n,1}\rangle \leqq T$. But then

$$H_nT = H_n\Omega_1(H_n)\langle x_{n,1}\rangle T = H_n\Omega_1(G_n)T.$$

Since $H_n\Omega_1(G_n)$ is a permutable subgroup of G_n, we see that H_nT is a subgroup contrary to $H_nT \neq TH_n$. Thus the theorem is proved.

We now have proved part (i) of the theorem in the introduction. In the next section, we will prove part (ii). Before doing this however, we wish to derive some additional properties of the groups G_n and H_n. Specifically, we will derive the order of G_n and show that H_n decomposes as a direct product: $H_n \cong H_{n-1} \times R_n$.

LEMMA 3.14.
(1) *If* $n \geqq e + 1$, *then*
$\Omega_1(G_n) = \langle x_n^{-i}A_{n,1}x_n^i \mid i = 0, 1, \ldots\rangle$
and $|\Omega_1(G_n)| = p^s$ *where* $s = p^{n-2}(p - 1)$.
(2) *If* $1 \leqq k \leqq n - e$, *then*
$\Omega_k(G_n) = \langle x_n^{-i}A_{n,k}x_n^i \mid i = 0, 1, \ldots\rangle\, \Omega_{k-1}(G_n)$.

PROOF. If (1) is valid, then an induction on k using the fact that $\Omega_{k-1}(G_{n-1}) = \tau_n(\Omega_k(G_n))$ will yield (2). Hence it suffices to prove (1). Now if $n = e + 1$, then $\Omega_1(G_n)$ has the right order and $|\Omega_1(G_n): A_{n,1}| = p$ by Lemmas 3.5 and 3.6. Since x_n does not normalize $A_{n,1}$ but does normalize $\Omega_1(G_n)$ we see that $\Omega_1(G_n)$ is generated by the conjugates of $A_{n,1}$ under $\langle x_n\rangle$. This proves (1) when $n = e + 1$.

Now assume $n > e + 1$. Then $A_{n,1}$ fixes each element of $\Delta_{n,n}$ by Lemma 3.1. Define B by

$$B = \langle x_{n,n-1}^{-i}A_{n,1}x_{n,n-1}^i \mid i = 0, 1, \ldots\rangle.$$

Then, since $\langle x_{n,n-1}\rangle$ fixes the set $\Delta_{n,n}$, B must fix every element of $\Delta_{n,n}$. If $0 \leqq k \leqq p - 1$, let $B_k = x_n^{-k}Bx_n^k$. Then, since $\Gamma_n - \Delta_{n,n} = \Gamma_{n,n-1}$, the points moved by B_k must belong to $\Gamma_{n,n-1}x_n^k$. But if $j \not\equiv k \pmod p$, then $\Gamma_{n,n-1}x_n^j$ and $\Gamma_{n,n-1}x_n^k$ are disjoint. It follows from this that $|\langle B_k \mid 0 \leqq k \leqq p - 1\rangle| = |B|^p$. Now, by induction and by Lemma 3.7,

$$|\rho_n(B)| = |\langle x_{n-1}^{-i}A_{n-1,1}x_{n-1}^i \mid i = 0. 1, \ldots\rangle| = p^t$$

where $t = p^{n-3}(p - 1)$. This implies that

$$|\langle x_n^{-i}A_{n,1}x_n^i \mid i = 0, 1, \ldots \rangle| \geqq p^{pt} = p^s.$$

Since $A_{n,1} \leqq \Omega_1(G_n)$ and since, by Lemma 3.1(*d*) of **[2]**, $|\Omega_1(G_n)| \leqq p^s$, the desired result now follows.

COROLLARY 3.15. $|G_n| = p^{(p^n-1)}$.

PROOF. This has been verified if $n \leqq e+1$. Now assume that $n > e+1$ and that

$$|G_{n-1}| = p^{(p^n-2)}.$$

Since $G_{n-1} = \tau_n(G_n) \cong G_n/\Omega_1(G_n)$, the corollary follows.

We now look at the relationship between H_n and R_n leading up to showing that R_n is a direct factor of H_n. First, let

$$W_n = \bigcap_{i=1}^{p-1} x_n^{-i} R_n x_n^i.$$

LEMMA 3.16. *Assume* $n > e$ *Then*

(1) $W_n = \{g \in H_n\langle x_{n,n-1}\rangle \mid \alpha g = \alpha$ *for all* $\alpha \in \Delta_{n,n}\}$.
(2) $W_n \trianglelefteq H_n\langle x_{n,n-1}\rangle$ *and* $W_n R_n = W_n \times R_n$.
(3) $\Omega_{n-e}(G_n) = H_n\langle x_{n,n-e}\rangle \geqq R_n \times W_n \geqq H_n\langle x_{n,n-e-1}\rangle$.
(4) *If* $1 \leqq i \leqq p-1$, *then* $R_n(x_n^{-i}R_n x_n^i) = \Omega_{n-e}(G_n)$.

PROOF. It follows from the definition of R_n that

$$x_n^{-i} R_n x_n^i = \{g \in H_n\langle x_{n,n-1}\rangle \mid \alpha g = \alpha \text{ for all } \alpha \in \Gamma_{n,n-1}x_n^i\}.$$

Since

$$\bigcup_{i=1}^{p-1} \Gamma_{n,n-1} x_n^i = \Delta_{n,n},$$

(1) follows at once. Since $R_n \trianglelefteq H_n\langle x_{n,n-1}\rangle \trianglelefteq G_n$, we see that $W_n \trianglelefteq H_n\langle x_{n,n-1}\rangle$. Now $H_n\langle x_n^p\rangle$ normalizes R_n and so $R_n \cap W_n$ is the core of R_n in G_n. Since $R_n \leqq H_n$ and since H_n is core-free in G_n, $R_n \cap W_n = 1$. Hence (2) is proved.

Corollaries 3.11 and 3.4 imply that $\Omega_{n-e}(G_n) = H_n\langle x_{n,n-e}\rangle \geqq R_n$. Since $\Omega_{n-e}(G_n) \trianglelefteq G_n$, it follows that $\Omega_{n-e}(G_n)$ contains $x_n^{-i}R_n x_n^i$ for all i. But then $\Omega_{n-e}(G_n)$ certainly contains $R_n W_n$. To complete the proof of (3), we need to show that $R_n W_n \geqq H_n\langle x_{n,n-e}\rangle$.

Parts (1) and (2) of our lemma together with Lemma 3.1(2) imply that

$$W_n \geqq \langle x_{n,n-1}^{-k} A_{n,m} x_{n,n-1}^k \mid 0 \leqq m \leqq n-e-1, k \geqq 0\rangle.$$

Applying ρ_n to both sides of this and using Lemma 3.7 yields

$$\rho_n(W_n) \geqq \langle x_{n-1}^{-k} A_{n-1,m} x_{n-1}^k \mid 0 \leqq m \leqq n-1-e, k \geqq 0\rangle.$$

Using Lemma 3.14 and induction on m, we obtain $\rho_n(W_n) \geqq \Omega_{n-1-e}(G_{n-1})$. Using Corollaries 3.11 and 3.4(2) and Lemmas 3.8(5) and 3.7(4), we derive

$$\rho_n(W_n) \geqq \Omega_{n-1-e}(G_{n-1}) = H_{n-1}\langle x_{n-1,n-1-e}\rangle = \rho_n(H_n\langle x_{n,n-1-e}\rangle).$$

Taking inverse images yields $W_nR_n \geqq H_n\langle x_{n,n-e-1}\rangle$ and so (3) is proved.

Now suppose (4) is false for some i, $1 \leqq i \leqq p-1$. Then, since

$$\Omega_{n-e}(G_n) \geqq x_n^{-i}R_nx_n^i \geqq W_n$$

and since $|H_n\langle x_{n,n-e}\rangle : H_n\langle x_{n,n-e-1}\rangle| = p$, it follows from (3) that

$$\Omega_{n-e}(G_n) > R_n(x_n^{-i}R_nx_n^i) = R_nW_n = H_n\langle x_{n,n-e-1}\rangle.$$

Now

$$x_n^{-i}W_nx_n^i = \bigcap_{j=1}^{p-1} x_n^{-i-j}R_nx_n^{i+j} \leqq x_n^{-p}R_nx_n^p = R_n$$

where the last equality is because R_n is normal in $H_n\langle x_{n,n-1}\rangle$. We now see that

$$x_n^{-i}(R_nW_n)x_n^i \leqq (x_n^{-i}R_nx_n^i)R_n = R_nW_n.$$

It follows from this that x_n normalizes R_nW_n. But then, since $R_nW_n \geqq H_n \geqq A_{n,m}$ for $0 \leqq m \leqq n-e$, this implies that

$$R_nW_n \geqq \langle x_n^{-k}A_{n,m}x_n^k | 0 \leqq m \leqq n-e,\ k \geqq 0\rangle.$$

Using Lemma 3.14 and induction on m, we obtain $R_nW_n \geqq \Omega_{n-e}(G_n)$. This proves (4).

THEOREM 3.17. *Assume $n > 1$. For $1 \leqq k \leqq n$, define U_k by*

$$U_k = \{g \in H_n | \alpha g = \alpha \text{ for all } \alpha \notin \Delta_{n,k}\}.$$

Then

(1) *$U_n = R_n$.*
(2) *H_n is the direct sum $U_1 \times U_2 \times \cdots \times U_n$.*
(3) *If $1 \leqq k \leqq n$, then U_k as a permutation group acting on $\Delta_{n,k}$ is permutation isomorphic to R_k acting on $\Delta_{k,k}$.*
(4) *If $1 \leqq k \leqq n$, then $U_1U_2 \cdots U_k$ as a permutation group acting on $\Gamma_{n,k}$ is permutation isomorphic to H_k acting on Γ_k.*

PROOF. This is trivially true if $n \leqq e$. Now assume $n > e$. Since $R_n \leqq H_n$, the previous lemma implies that $H_n = R_n \times (H_n \cap W_n)$. Now R_n fixes every element of $\Gamma_{n,n-1}$ and so R_n is faithfully represented as a permutation group on $\Delta_{n,n}$. Similarly, $H_n \cap W_n$ is faithfully represented as a permutation group on $\Gamma_{n,n-1}$. This implies that $H_n \cap W_n$ acting on $\Gamma_{n,n-1}$ is permutation isomorphic to $\rho_n(H_n \cap W_n)$ acting on Γ_{n-1}. Since $\rho_n(R_n) = 1$. we see that $\rho_n(H_n \cap W_n) = \rho_n(H_n) = H_{n-1}$. The theorem now follows by an easy induction proof.

COROLLARY 3.18. *If $n > 2$, then $\tau_n(R_n) = R_{n-1}$.*

PROOF. R_n moves only points in $\Delta_{n,n}$. It follows that $\tau_n(R_n)$ moves only points in $\Delta_{n-1,\,n-1}$. Hence, $\tau_n(R_n) \leqq R_{n-1}$. Now $H_n \cong R_n \times H_{n-1}$. This implies both that $|R_n| = |H_n|/|H_{n-1}|$ and that $\Omega_1(H_n) \cong \Omega_1(R_n) \times \Omega_1(H_{n-1})$. But $\Omega_1(H_n)$ is the intersection of H_n with the kernel of τ_n. Hence,

$$\begin{aligned}|\tau_n(R_n)| &= |R_n/\Omega_1(R_n)| = |H_n/\Omega_1(H_n)|/|H_{n-1}/\Omega_1(H_{n-1})| \\ &= |\tau_n(H_n)|/|\tau_{n-1}(H_{n-1})| = |H_{n-1}|/|H_{n-2}| \\ &= |R_{n-1}|.\end{aligned}$$

This implies that $\tau_n(R_n) = R_{n-1}$.

The final result of this section exhibits a relationship between R_n and G_{n-e}. This will be of use in the next section in calculating the class and derived lengths of the groups G_n, H_n and R_n.

LEMMA 3.19. *Assume $n > e$. Then both $\Omega_{n-e}(G_n)$ and R_n are subdirect products of copies of G_{n-e}.*

PROOF. $R_n \trianglelefteq \Omega_{n-e}(G_n) \trianglelefteq G_n$ and so

$$\begin{aligned}\Omega_{n-e}(G_n)/x_n^{-i}R_nx_n^i &\cong \Omega_{n-e}(G_n)/R_n \cong H_n\langle x_{n,\,n-e}\rangle/R_n \\ &\cong \rho_n(H_n\langle x_{n,\,n-e}\rangle) = H_{n-1}\langle x_{n-1,\,n-e}\rangle.\end{aligned}$$

Since $\bigcap_{i=1}^{p} x_n^{-i}R_nx_n^i = 1$, this implies that $\Omega_{n-e}(G_n)$ is a subdirect product of copies of $H_{n-1}\langle x_{n-1,\,n-e}\rangle$.

Now suppose $1 \leqq i \leqq p-1$. Then Lemma 3.16(4) implies that $R_n(x_n^{-i}R_nx_n^i) = \Omega_{n-e}(G_n)$. Then we have

$$R_n/(R_n \cap x_n^{-i}R_nx_n^i) \cong \Omega_{n-e}(G_n)/x_n^{-i}R_nx_n^i \cong H_{n-1}\langle x_{n-1,\,n-e}\rangle.$$

Since $\bigcap_{p-1}^{i=1}(R_n \cap x_n^{-i}R_nx_n^i) = 1$, we see that R_n is also a subdirect product of copies of $H_{n-1}\langle x_{n-1,\,n-e}\rangle$. Thus the lemma will be proved once we show that $H_{n-1}\langle x_{n-1,\,n-e}\rangle$ is a subdirect product of copies of G_{n-e}. If $p \neq 2$, then

$$H_{n-1}\langle x_{n-1,\,n-e}\rangle = H_{n-1}\langle x_{n-1,\,n-1}\rangle = G_{n-1} = G_{n-e}.$$

If $p = 2$, then $e = 2$ and Corollary 3.9 implies that $H_{n-1}\langle x_{n-1,\,n-e}\rangle$ is a subdirect product of copies of G_{n-e}. Thus the lemma is proved.

COROLLARY. 3.20. *If $n > e$, then the three groups H_n, R_n and G_{n-e} have the same class, derived length, and exponent.*

PROOF. Since $R_n \leqq H_n \leqq \Omega_{n-e}(G_n)$, this follows from the lemma.

4. The universal property. The second half of the theorem in the introduction will follow from the following result.

THEOREM 4.1. *Suppose T is a subgroup of Q_n such that $T\langle x_n\rangle = \langle x_n\rangle T$ and that T is a permutable subgroup of $T\langle x_n\rangle$. Then $T \leqq H_n$.*

PROOF. T must be core-free in $T\langle x_n\rangle$ since $\langle x_n\rangle$ is transitive and T

stabilizes a point. Thus, by Theorem 5.1 of **[1]** and by Lemma 3.2 of **[3]**, T must have exponent $\leqq \text{Max}\{1, p^{n-e}\}$. If $n \leqq e$, then $T = 1$ and the theorem is true. Now assume that $n > e$. Lemma 2.2(5) implies that $\Omega_1(T\langle x_n\rangle)$ fixes all orbits of $\langle x_{n,1}\rangle$. Hence, $\Omega_1(T\langle x_n\rangle) \leqq K_n$. But $T\langle x_n\rangle$ must have class $\leqq p^{n-2}(p-1)$ [3, Theorem 3.4] and so

$$[\Omega_1(T\langle x_n\rangle), \langle x_n\rangle; p^{n-2}(p-1)] = 1.$$

Now define U by

$$U = \{u \in K_n | [u, x_n; p^{n-2}(p-1)] = 1\}.$$

Then U is a subgroup of K_n. Since

$$C_{K_n}(x_n) = \langle x_n\rangle \cap K_n = \langle x_{n,1}\rangle$$

by Lemma 2.2, we find that the linear transformation induced by x_n on K_n written additively, can have only one Jordan block. Now

$$|K_n| = p^{(p^n-1)}$$

by Lemma 3.3(9) and

$$p^{(p^n-1)} > p^s$$

with $s = p^{n-2}(p-1)$. It follows from all this that $|U| = p^s$. But $[\Omega_1(G_n), \langle x_n\rangle; s] = 1$ by Theorem 3.4 of **[3]**. This implies that U must contain both $\Omega_1(G_n)$ and $\Omega_1(T\langle x_n\rangle)$. Since $|\Omega_1(G_n)| = p^s$ by Lemma 3.14, we conclude that

$$\Omega_1(T\langle x_n\rangle) \leqq U = \Omega_1(G_n).$$

This implies that $\Omega_1(T) \leqq \Omega_1(G_n) \cap Q_n = \Omega_1(H_n)$.

Now $\tau_n(T) \leqq Q_{n-1}$ and $\tau_n(T)$ is a permutable subgroup of

$$\tau_n(T\langle x_n\rangle) = \tau_n(T)\langle x_{n-1}\rangle.$$

Induction now yields $\tau_n(T) \leqq H_{n-1} = \tau_n(H_n)$. Hence $T \leqq H_nK_n$. From Corollary 3.4(3) we deduce that

$$T \leqq C_{G_n}(x_{n,2})K_n.$$

Now let $g \in T$. Then $g = yz$ with $y \in C_{G_n}(x_{n,2})$ and $z \in K_n$. Then

$$[g, x_{n,2}] = [yz, x_{n,2}] = [z, x_{n,2}].$$

Thus $[g, x_{n,2}; p-1] = [z, x_{n,2}; p-1]$. But Lemma 2.4 then implies that $[z, x_{n,2}; p-1] = 1$. Since $z \in K_n$ and since

$$x_{n,2} = x_n^{(p^{n-2})},$$

it follows that

$$[z, x_n; p^{n-2}(p-1)] = 1.$$

Hence $z \in U = \Omega_1(G_n)$. But then $g = yz \in Q_n \cap G_n = H_n$ and the theorem is proved.

THEOREM 4.2. *Let $G = H\langle x \rangle$ where x has order p^n and H is a core-free permutable subgroup of G. Then there is one and only one monomorphism ψ of G into G_n such that $\psi(x) = x_n$ and $\psi(H) \leqq H_n$.*

PROOF. G must be a finite p-group by Lemma 2.1. Let Γ be the set of all cosets of H in G and define $f: \Gamma \to \Gamma_n$ by $f(Hx^i) = p^n\mathbf{Z} + i$. This is a one-to-one correspondence and so we obtain a faithful (since H is core-free) representation ψ of G as a permutation group of Γ_n where

$$(p^n\mathbf{Z} + i)\psi(g) = p^n\mathbf{Z} + j \text{ if and only if } Hx^ig = Hx^j.$$

Then, as is easily computed, $\psi(x) = x_n$. Since $\psi(G)$ must be a p-group and $\psi(G)$ contains x_n, Corollary 2.3 implies that $\psi(G) \leqq p_n$. Since $\psi(H)$ fixes $p^n\mathbf{Z} + 0$, $\psi(H) \leqq Q_n$. The previous theorem now is applicable with the result that $\psi(H) \leqq H_n$.

Now suppose that χ is any monomorphism of G into G_n such that $\chi(x) = x_n$ and $\chi(H) \leqq H_n$. Suppose $h \in H$ and i and j are integers such that

$$(p^n\mathbf{Z} + i)\chi(h) = p^n\mathbf{Z} + j.$$

Since $p^n\mathbf{Z} + i$ and $p^n\mathbf{Z} + j$ are the images of $p^n\mathbf{Z} + 0$ under x_n^i and x_n^j, respectively, we find that $\chi(x^ihx^{-j})$ fixes $(p^n\mathbf{Z} + 0)$. Hence, since $H_n \cap \chi(G) = H_n \cap \chi(H\langle x \rangle) = H_n \cap \chi(H)\langle x_n \rangle = \chi(H)$, $\chi(x^ihx^{-j}) \in \chi(H)$. This implies that $x^ihx^{-j} \in H$. From this follows that $Hx^ih = Hx^j$. An immediate consequence of this is $(p^n\mathbf{Z} + i)\psi(h) = p^n\mathbf{Z} + j$. We now see that $\chi = \psi$ and the theorem is proved.

As an application of this theorem, we will calculate the class and derived length of the groups G_n, H_n, and R_n. From Corollary 3.20, we need only do this for G_n.

THEOREM 4.3.
(1) $\mathrm{c}(G_n) = \mathrm{Max}\{1, p^{n-2}(p-1)\}$
(2) *If $p > 2$, then* $\mathrm{d}(G_n) = n$.
(3) *If $p = 2$, then* $\mathrm{d}(G_n) = [(n+1)/2]$.

PROOF. Theorem 3.4 of [3] and Lemma 3.2 of [2] imply that $\mathrm{c}(G_n)$ and $\mathrm{d}(G_n)$ are at most the values specified. Thus it suffices to verify that $\mathrm{c}(G_n)$ and $\mathrm{d}(G_n)$ are at least as big as soecified. If $n = 1$ then G_n is abelian and the theorem is true. We now assume that $n > 1$.

Since $C_{G_n}(x_n) = \langle x_n \rangle$ and since $\Omega_1(G_n)$ is elementary abelian of order $p^{(p^{n-2}(p-1))}$, we see that $[\Omega_1(G_n), \langle x_n \rangle; p^{n-2}(p-1) - 1] \neq 1$. This implies that $\mathrm{c}(G_n) \geqq p^{n-2}(p-1)$ and so (1) is proved.

Let $s = n$ if $p > 2$ and $s = [(n + 1)/2]$ if $p = 2$. Then in [9] if $p > 2$ and in [3] if $p = 2$, it is proved that there is a finite p-group G such that $G = \langle x \rangle H$ where x has order p^{n+e} and $\mathrm{d}(H) = s$. It follows from Theorem 4.2 that $\mathrm{d}(H_{n+e}) \geqq s$. Corollary 3.20 now yields $\mathrm{d}(G_n) \geqq s$ and the theorem is proved.

It should be noted that it is possible to give a direct proof of the value of $\mathrm{d}(G_n)$ without referring to the examples in [9] and [3]. More specifically, it is possible to explicitly find two elements (one of which is x_n) in G_n such that the subgroup generated by these two elements has derived length greater than or equal to n or $[(n + 1)/2]$ depending on whether $p > 2$ or $p = 2$, respectively. This proof, however, is longer and more complicated.

The final result to be presented is a technical result required in the study of infinite permutable subgroups in [4].

LEMMA 4.4. *There is an element $h \in H_n$ such that $(p^n\mathbf{Z} + a)h = p^n\mathbf{Z} + a(p^e + 1)$ for all $a \in \mathbf{Z}$.*

PROOF. If $n \leqq e$, simply choose $h = 1$. Now assume $n > e$ and let G be the group with generators x, y and relations

$$x^{p^n} = y^{p^{n-1}} = x^{-(p^e+1)}y^{-1}xy = 1.$$

Then $G = \langle x \rangle \langle y \rangle$ and $\langle y \rangle$ is a core-free permutable subgroup of G [2, Lemma 4.1]. It follows from Theorem 4.2 that there is an element $h \in H_n$ such that

$$h^{-1}x_nh = x_n^{(p^e+1)}.$$

Let g be the permutation of Γ_n given by $(p^n\mathbf{Z} + a)g = p^n\mathbf{Z} + a(p^e + 1)$. Then hg^{-1} centralizes $\langle x_n \rangle$. Since $\langle x_n \rangle$ is an abelian regular permutation group on Γ_n, we must have $hg^{-1} \in \langle x_n \rangle$. But hg^{-1} stabilizes the zero element of Γ_n. Hence $hg^{-1} = 1$ and the lemma follows.

GLOSSARY

p	a prime
e	$e = 1$ if $p > 2$, $e = 2$ if $p = 2$
r	$r = p - 1$ if $p > 2$, $r = 2$ if $p = 2$
n	a positive integer
Γ_n	$\mathbf{Z}/p^n\mathbf{Z}$
x_n	permutation $p^n\mathbf{Z} + a \to p^n\mathbf{Z} + a + 1$
$x_{n,m}$	$x_n^{p^{n-m}}$ if $0 \leqq m \leqq n$
$\Gamma_{n,m}$	$\Omega_m(\Gamma_n)$
$\Delta_{n,m}$	set of elements of order p^m in Γ_n
$\theta_{n,m,i}$	orbit of $\langle x_{n,m} \rangle$ contained in $\Delta_{n,m+e}$
$\pi_{n,m,i}$	permutation on $\theta_{n,m,i}$ induced by $x_{n,m}$

$A_{n,m}$	$\left\{\prod_{i=1}^{r} \pi_{n,m,i}^{c_i} \mid \sum_{i=1}^{r} c_i = 0\right\}$
G_n	$\langle x_n, A_{n,m} \mid 0 \leqq m \leqq n - e\rangle$
H_n	$\{g \in G_n \mid (p^n\mathbf{Z})g = p^n\mathbf{Z}\}$
P_n	Sylow p-subgroup of the symmetric group of degree p^n; P_n contains x_n
Q_n	$\{g \in P_n \mid (p^n\mathbf{Z})g = p^n\mathbf{Z}\}$
τ_n	a homomorphism of P_n onto P_{n-1} if $n > 1$.
K_n	the kernel of τ_n
ρ_n	a homomorphism of $Q_n\langle x_{n,n-1}\rangle$ onto P_{n-1} if $n > 1$
R_n	the intersection of kernel (ρ_n) and $H_n\langle x_{n,n-1}\rangle$
W_n	$\bigcap_{i=1}^{p-1} x_n^{-i} R_n x_n^i$

REFERENCES

1. R. Bradway, F. Gross, and W.R. Scott, *The nilpotence class of core-free quasinormal subgroups*, Rocky Mt. J. Math. **1** (1971), 375–382.

2. F. Gross, *p-subgroups of core-free quasinormal subgroups*, Rocky Mt. J. Math. **1** (1971), 541–550.

3. ———, *p-subgroups of core-free quasinormal subgroups II*, Rocky Mt. J. Math. **5** (1975), 349–359.

4. ———, *Infinite permutable subgroups*, Rocky Mtn. J. of Math., **12** (1982), 333–343.

5. M. Hall, Jr., *The theory of groups*, Macmillan, New York, 1959.

6. N. Itô and J. Szep, *Uber die Quasinormalteiler von endlichen Gruppen*, Acta Sci. Math. (Szeged) **23** (1962), 168–170.

7. R. Maier and P. Schmid, *The embedding of quasinormal subgroups in finite groups*, Math. Z. **131** (1973), 269–272.

8. S.E. Stonehewer, *Permutable subgroups of infinite groups*, Math. Z. **125** (1972), 1–16.

9. ———, *Permutable subgroups of some finite permutation groups*, Proc. London Math. Soc. (3) **28** (1974), 222–236.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF UTAH, SALT LAKE CITY, UT 84112
SCHOOL OF MATHEMATICS, UNIVERSITY OF MINNESOTA, MINNEAPOLIS, MN 55455