TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 182, August 1973

SOME HIGHLY HOMOGENEOUS GROUPS

BY

LARRY DORNHOFF(1)

ABSTRACT. We study finite rank 4 permutation groups which are solvable and imprimitive, with a regular normal subgroup. This means determining those groups N with a solvable automorphism group A which has only three orbits on the nonidentity elements of N.

0. Introduction. The *rank* of a transitive permutation group G on a set Ω is the number of orbits on Ω of the subgroup G_α fixing a point $\alpha \in \Omega$. All groups discussed in this paper are finite. Solvable rank 2 groups (doubly transitive groups) were classified by Huppert [7] in 1957. Solvable primitive rank 3 groups were classified by Foulser [3] and independently by the present author (unpublished). Solvable imprimitive rank 3 groups with a regular normal subgroup were classified by the present author [2], and solvable primitive rank 4 groups were classified (with finitely many exceptions) by Foulser [3]. In this paper we study imprimitive rank 4 groups with regular normal subgroup. There are too many for a complete classification; we do get a complete classification in some cases, and some interesting examples and a general description of the groups in other cases.

If G is a solvable imprimitive rank m permutation group on the set Ω and N is a regular normal subgroup of G, let G_α be the subgroup fixing $\alpha \in \Omega$. Then $G_\alpha N = G$, $G_\alpha \cap N = 1$. By Theorem 11.2 of [12], G_α is an automorphism group of N acting with $m - 1$ orbits on $N^\# = N - \{1\}$. Conversely, if N is any group with a solvable automorphism group A having $m - 1$ orbits on $N^\#$, then the semidirect product $G = AN$ is a solvable rank m permutation group with regular normal subgroup N; G will be imprimitive if and only if A fixes some proper subgroup of N. Thus our problem in this paper is to classify those groups N with a solvable automorphism group A having only three orbits on $N^\#$ (all such N's will turn out to be solvable). The main results are stated in Theorems 1.1, 2.1, 3.1 and 4.1.

Because it is important for us in several places, we restate here the main theorem of [2].

Received by the editors October 20, 1972.

AMS (MOS) subject classifications (1970). Primary 20B05, 20B10, 20B25, 20D45.

Key words and phrases. Solvable permutation group, rank 4 permutation group, imprimitive permutation group, three-orbit automorphism group, Suzuki 2-group, regular normal subgroup.

(1) Research partially supported by NSF Contract GP 33137.

Theorem 0.1. *Let M be a finite group, B a solvable automorphism group of M acting with only two orbits on $M^{\#} = M - \{1\}$. Then we have one of the following:*

(i) *M is an elementary abelian p-group for some prime p.*

(ii) *For some prime p, M is a direct product of cyclic groups of order p^2.*

(iii) *For primes p and q, the polynomial $(X^q - 1)/(X - 1)$ is irreducible over $GF(p)$, and M is a Frobenius group of order $qp^{m(q-1)}$ (m an integer). Here M has an elementary abelian Frobenius kernel of order $p^{m(q-1)}$.*

(iv) *For some integer $n > 2$ which is not a power of 2, and some automorphism $\theta \neq 1$ of $GF(2^n)$ of odd order, $M = A(n, \theta) = \{(\alpha, \zeta) \in GF(2^n) \times GF(2^n) \mid (\alpha, \zeta)(\beta, \eta) = (\alpha + \beta, \zeta + \eta + \alpha\beta^{\theta})\}$. Thus $|M| = 2^{2n}$.*

(v) *For some integer $n \geq 1$, $M = B(n) = \{(\alpha, \zeta) \in GF(2^{2n}) \times GF(2^n) \mid (\alpha, \zeta)(\beta, \eta) = (\alpha + \beta, \zeta + \eta + \alpha\beta^{2^n}\mu + \alpha^{2^n}\beta\mu^{-1})\}$, where $\mu \in GF(2^{2n})$ has order $2^n + 1$. Here $|M| = 2^{3n}$, and M does not depend on μ.*

(vi) *For some odd prime p and integer $n \geq 1$, choose $\epsilon \in GF(p^{2n})$ such that $\epsilon + \epsilon^{p^n} = 0$. Then $M = C(p, n) = \{(\alpha, \zeta) \in GF(p^{2n}) \times GF(p^n) \mid (\alpha, \zeta)(\beta, \eta) = (\alpha + \beta, \zeta + \eta + \frac{1}{2}(\alpha\beta^{p^n} - \alpha^{p^n}\beta)\epsilon)\}$. Here $|M| = p^{3n}$, and M does not depend on ϵ.*

(vii) *M is an extra special 3-group of order 3^5 and exponent 3.*

(viii) *$M = P(\epsilon)$, where $|P(\epsilon)| = 2^9$, ϵ is a multiplicative generator in $GF(2^6)$, and $P(\epsilon) = \{(\alpha, \zeta) \in GF(2^6) \times GF(2^3) \mid (\alpha, \zeta)(\beta, \eta) = (\alpha + \beta, \zeta + \eta + \alpha\beta^2\epsilon + \alpha^8\beta^{16}\epsilon^8)\}$.*

Futhermore, all these groups except $|M| = 2$ have such solvable automorphism groups B; in case (i), *one orbit of B can be $H^{\#}$, any proper subgroup H of M.*

From now on throughout this paper, N is a fixed finite group and A a solvable automorphism group of N having three orbits on $N^{\#} = N - \{1\}$. For any p-group X, $\Omega_i(X) = \{x \in X \mid x^{p^i} = 1\}$, $\mho^i(X) = \{x^{p^i} \mid x \in X\}$, $\Phi(X) =$ Frattini subgroup of X.

1. The case when N is abelian.

Theorem 1.1. *Let N be a finite abelian group, A a solvable automorphism group of N with three orbits on $N^{\#}$. Then we have one of the following:*

(1) *$|N| = p$, p a prime with $p \equiv 1 \pmod 3$.*

(2) *N is elementary abelian of order $p^n \geq p^2$, for any prime p.*

(3) *N is a direct product of cyclic groups of order p^3, for any prime p.*

(4) *N has exponent p^2 and is not cyclic, for any prime p.*

(5) *N is cyclic of order 4.*

(6) *$N = P \times Q$, P an elementary abelian p-group, Q an elementary abelian q-group, $p \neq q$ primes.*

Moreover, all the groups in (1)–(6) *occur.*

Proof. Suppose first that N has exponent p. If N is elementary abelian of order $p^n \geq p^3$, let B, C, D be subgroups of N such that $N = B \times C \times D$, $B \neq 1$,

$C \neq 1$, $D \neq 1$. Let G_B, G_C, G_D be solvable matrix groups over $GF(p)$ which (as linear transformations) act transitively on $B^{\#}$, $C^{\#}$, $D^{\#}$, respectively. Then the group of all matrices with block form

$$\begin{pmatrix} x & * & * \\ 0 & y & * \\ 0 & 0 & z \end{pmatrix},$$

$x \in G_B$, $y \in G_C$, $z \in G_D$ is a solvable group acting transitively on the sets $B^{\#}$, $(B \times C) - B$ and $N - (B \times C)$; so N is such a group.

Suppose N has exponent p and order p^2. If $p = 2$, then $A = 1$ is an automorphism group with three orbits on $N^{\#}$. If $p > 2$, let $N = A \times B$, $|A| = |B| = p$, and let T be the multiplicative subgroup of $GF(p)^{\#} = GF(p) - \{0\}$ of index 2. Then the group of matrices of the form

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix},$$

$x \in GF(p)^{\#}$, $y \in GF(p)$, $z \in T$ is transitive on $A^{\#}$ and has two orbits on $N - A$, so N is a group of the theorem and all groups in (2) occur.

If $|N| = p$, a prime, then $|\mathrm{Aut}(N)| = p - 1$. If $p \equiv 1 \pmod 3$, then $\mathrm{Aut}(N)$ has a subgroup of index 3 with 3 orbits on $N^{\#}$, while if $p \not\equiv 1 \pmod 3$ no such subgroup is available. The groups of (1) and (2) are all the groups of exponent p.

If N is of exponent p^3 then $\Omega_1(N)^{\#} = \mho^2(N)^{\#}$ and $\Omega_2(N) - \Omega_1(N) = \mho^1(N) - \mho^2(N)$ are two orbits of A; N must be homocyclic (a group of type (3)). If N is homocyclic, say $|N| = p^{3m}$, let $T = \{\alpha \in \mathrm{Aut}(N) \mid \alpha \text{ is trivial on } N/\Phi(N)\}$. Easy counting arguments show that $|T| = p^{m^3}$ and $|\mathrm{Aut}(N)| = p^{m^3}|GL(m, p)|$. By Satz II.7.3 of [6], $GL(m, p) \cong \mathrm{Aut}(N/\Phi(N))$ contains an element ψ_0 of order $p^m - 1$, so $\mathrm{Aut}(N)$ also contains an element ψ of order $p^m - 1$. The solvable group $\langle\psi\rangle T$ is transitive on $N - \Omega_2(N)$, $\Omega_2(N) - \Omega_1(N)$ and $\Omega_1(N)^{\#}$, so the groups of (3) occur.

If N is of exponent p^2 and not homocyclic, say $N = B \times C$, $|B| = p^{2m}$, $|C| = p^n$, B homocyclic of exponent p^2, C elementary abelian, then we have $m > 0$, $n > 0$ so $1 < \mho^1(N) < \Omega_1(N) < N$ is a characteristic series of N. Let $T = \{\alpha \in \mathrm{Aut}(N) \mid \alpha \text{ is trivial on } N/\mho^1(N)\}$ and $U = \{\alpha \in \mathrm{Aut}(N) \mid \alpha \text{ is trivial on } \Omega_1(N)\}$. Then T and U are normal subgroups of $\mathrm{Aut}(N)$. Easy counting arguments show that $|T| = p^{m^2+mn} = |U|$ and $|T \cap U| = p^{m^2}$, so $|TU| = p^{m^2+2mn}$. Using Satz II.7.3 of [6], we can find automorphisms β, γ of N such that β and γ each fix groups B and C, and $\beta|_C = 1_C$, $\beta|_B$ has order $p^m - 1$, $\gamma|_B = 1_B$, $\gamma|_C$ has order $p^n - 1$, $\langle\beta\rangle$ transitive on $(B/\mho^1(N))^{\#}$, $\langle\gamma\rangle$ transitive on $C^{\#}$. Certainly β

and γ centralize each other, so $H = \langle\beta, \gamma\rangle TU$ is a solvable subgroup of $\mathrm{Aut}(N)$. $\langle\beta\rangle \leq H$ is transitive on $\mathfrak{V}^1(N)^\#$ since $\mathfrak{V}^1(N) \cong B/\mathfrak{V}^1(N)$ as $\langle\beta\rangle$-modules ($x \to x^p$ is a $\langle\beta\rangle$-isomorphism). If $x, y \in \Omega_1(N) - \mathfrak{V}^1(N)$, then there is a power γ^i of γ with $x^{\gamma^i} \equiv y \pmod{\mathfrak{V}^1(N)}$. Then there is $\tau \in T$ with $x^{\gamma^i\tau} = y$, so $\langle\gamma\rangle T \leq H$ is transitive on $\Omega_1(N) - \mathfrak{V}^1(N)$. Finally, if $x, y \in N - \Omega_1(N)$ then there is a power β^j of β with $x^{\beta^j} \equiv y \pmod{\Omega_1(N)}$ and a $\mu \in U$ with $x^{\beta^j\mu} = y$, so $\langle\beta\rangle U \leq H$ is transitive on $N - \Omega_1(N)$. Therefore H has only three orbits on $N^\#$, and the nonhomocyclic groups of (4) occur.

If N is homocyclic but not cyclic of exponent p^2, let $N = B \times C$, B and C homocyclic of exponent p^2, say $|B| = p^{2b}$, $|C| = p^{2c}$, $b > 0$, $c > 0$. Let $\mathfrak{B}$ be a solvable group of automorphisms of $B/\Omega_1(B)$ transitive on $(B/\Omega_1(B))^\#$ and let $\mathfrak{C}$ be a solvable group of automorphisms of $C/\Omega_1(C)$ transitive on $(C/\Omega_1(C))^\#$. Then

$$N/\Omega_1(N) = B\Omega_1(N)/\Omega_1(N) \times C\Omega_1(N)/\Omega_1(N) \cong B/\Omega_1(B) \times C/\Omega_1(C).$$

Let $\mathfrak{G}$ be the group of all automorphisms τ of N such that the automorphism of $N/\Omega_1(N)$ induced by τ fixes $B\Omega_1(N)/\Omega_1(N)$ and has block matrix form

$$\begin{pmatrix} \beta & * \\ 0 & \gamma \end{pmatrix},$$

$\beta \in \mathfrak{B}$, $\gamma \in \mathfrak{C}$. In particular, $\mathfrak{G}$ contains $\mathfrak{T} = \{\tau \in \mathrm{Aut}(N) | \tau$ is trivial on $N/\Omega_1(N)\}$, a group of order $p^{(a+b)^2}$. We see that $\mathfrak{G}$ is transitive on $\Omega_1(N)^\#$, $B\Omega_1(N) - \Omega_1(N)$ and $N - B\Omega_1(N)$. Therefore the homocyclic groups of (4) occur.

Now let N be cyclic of order p^2; then $\mathrm{Aut}(N)$ is abelian of order $p(p-1)$. Suppose H is a subgroup of $\mathrm{Aut}(N)$ with three orbits. $x \to x^p$ is an H-isomorphism from $N/\Omega_1(N)$ to $\Omega_1(N)$, so H has the same number of orbits on $\Omega_1(N)^\#$ and $(N/\Omega_1(N))^\#$; H has only 3 orbits on $N^\#$, so this number must be 1. Since H is transitive on $\Omega_1(N)^\#$, $p-1$ divides $|H|$; hence $|H|$ is $p-1$ or $p(p-1)$. If $|H| = p(p-1)$, then $H = \mathrm{Aut}(N)$ has only two orbits on $N^\#$, a contradiction. If $|H| = p-1$, then H has $p+1$ orbits on $N^\#$; $p+1 = 3$ implies $p = 2$, $|N| = 4$, so the group of (5) is the only cyclic group of order p^2 occurring.

This completes the study of abelian p-groups. The only other abelian groups that can occur are those in (6), since $N^\#$ can only contain elements of three different orders. The groups of (6) do occur, for if $N = P \times Q$, $|P| = p^b$, $|Q| = q^c$, P and Q elementary abelian, let B be a solvable subgroup of $\mathrm{Aut}(P)$ transitive on $P^\#$ and C a solvable subgroup of $\mathrm{Aut}(Q)$ transitive on $Q^\#$. Then $A = B \times C$ acts naturally on N, with orbits $P^\#$, $Q^\#$ and $N - P - Q$ on $N^\#$, as desired. This completes the proof of Theorem 1.1.

2. **The case when two or more primes divide $|N|$, N nonabelian.** In this section, we prove

Theorem 2.1. *Let N be a finite nonabelian group with $|N|$ divisible by two or more distinct primes, A a solvable automorphism group of N acting with only three orbits on $N^{\#}$. Then we have one of the following:*

(1) *N is a Frobenius group with kernel a homocyclic abelian p-group of exponent p^2 and complement of order q, $p \neq q$ primes with $(X^q - 1)/(X - 1)$ irreducible over $GF(p)$.*

(2) *N is a Frobenius group with kernel an elementary abelian p-group and complement of order q, $p \neq q$ primes with $(X^q - 1)/(X - 1)$ irreducible over $GF(p)$.*

(3) *N is a Frobenius group with kernel a p-group occurring in Theorem* 0.1 (iv)–(viii) *and complement of order q, $p \neq q$ primes.*

(4) *N is a Frobenius group with kernel an elementary abelian p-group P and complement Q of order q, $p \neq q$ primes with $(X^q - 1)/(X - 1)$ a product of two irreducible factors of degree $\frac{1}{2}(q - 1)$ over $GF(p)$, all Q-submodules of P isomorphic.*

(5) *N is a Frobenius group with kernel an elementary abelian p-group and complement cyclic of order q^2, $p \neq q$ primes with $(X^{q^2} - 1)/(X^q - 1)$ irreducible over $GF(p)$.*

(6) *N is a Frobenius group with kernel elementary abelian of order 3^2, 5^2, 7^2, 11^2 or 23^2 and complement quaternion of order* 8.

Moreover, all groups in (1), (2) *and* (4)–(6) *occur, and infinitely many groups in* (3) *do occur.*

We first ask if $|N|$ can be divisible by three different primes p, q, r. If so and N is solvable, let P_0 be a minimal normal subgroup, say a p-subgroup. Since some p-elements are in a minimal normal subgroup, all must be; taking their product, N has a normal elementary abelian Sylow p-subgroup P. Nothing in $N - P$ centralizes anything in $P^{\#}$ (there are no pq- or pr-elements), so N is a Frobenius group with Frobenius kernel P (see p. 348 of [8]). If L is a Frobenius complement in N, then $L = QR$, Q and R Sylow q- and r-subgroups of N, respectively. Now QP and RP are Frobenius groups with Frobenius complements Q and R, and Theorem 13.3(3) of [1] implies $|Q| = q$, $|R| = r$, $|L| = qr$. Now the same theorem shows L is cyclic. Thus N has an element of order qr, a contradiction.

If N is not solvable, let N_0 be a minimal normal subgroup of N. By a theorem of Burnside (Theorem 6.3 in [1]), distinct primes p, q, r divide $|N_0|$. (N_0 solvable would force A to have at least four orbits on $N^{\#}$.) If A is a solvable subgroup of $\mathrm{Aut}(N)$ with only three orbits on $N^{\#}$ and M is the product of all A-conjugates of N_0, then N_0 and hence M are direct products of isomorphic simple groups. If $M = S \times S \times \cdots \times S$, S a simple group, then all three orbits of A

intersect M and hence are in M; $M = N$. If $N = S \times S \times \cdots$ has at least two factors then N has an element of composite order, a contradiction. Thus $N = S$ is simple. Results on p. 468 of [4] (groups of "Type A") show that $N = PSL(2, 2^n)$ for some $n \geq 2$, since in N the centralizers of 2-elements are 2-groups and the Sylow 2-subgroups are elementary abelian.(2)

If $q = 2^n$, then $|N| = q(q+1)(q-1)$. Theorem 38.2 of [1] shows that N contains an element a of order $q-1$ and an element b of order $q+1$. If $q+1$ is not a prime then some power (not 1) of b has order strictly dividing $q+1$ and N has elements of four different orders, a contradiction. So $q+1$ is a prime, and similarly $q-1$ is a prime; 3 must divide $q-1$ or $q+1$, so we must have $3 = q-1$, $4 = q$, $N = PSL(2, 4) = A_5$. Letting each Sylow 2-subgroup of A_5 correspond to the point it fixes, we see that an automorphism fixing all five Sylow 2-subgroups of A_5 fixes all five points permuted and must be trivial; this proves $\mathrm{Aut}(A_5) = S_5$. A_5 has 24 elements of order 5, 15 elements of order 2, and 20 elements of order 3. A is transitive on these sets, so 24, 15, and 20 divide $|A|$; this means 120 divides $|A|$, but $A \leq S_5$ so $A = S_5$, a contradiction since S_5 is not solvable. This completes the case when three primes divide $|N|$.

Lemma 2.2. *If A and N are as in Theorem 2.1, then N is not nilpotent. The Fitting subgroup $\mathrm{Fit}(N)$ of N is a p-group and $N/\mathrm{Fit}(N)$ is a q-group, for distinct primes p and q.*

Proof. We have just seen that N is a p, q-group. If N were nilpotent, say $N = P \times Q$, Q a q-group and P a nonabelian p-group, then $\mathrm{Aut}(N)$ fixes $(P')^{\#}$, $Q^{\#}$, $P - P'$ and $N - P - Q$, hence has more than three orbits on $N^{\#}$. Therefore N is not nilpotent. $\mathrm{Fit}(N)$ is nilpotent, so we see similarly that $\mathrm{Fit}(N)$ is not a p, q-group. We may therefore assume $P_0 = \mathrm{Fit}(N)$ is a p-group. Assuming $p \mid |N/P_0|$, we seek a contradiction. N/P_0 nilpotent would give N a normal p-subgroup larger than $\mathrm{Fit}(N)$, a contradiction. So we set $F/P_0 = \mathrm{Fit}(N/P_0)$ and get a characteristic series $1 < P_0 < F < N$. We must have F/P_0 a q-group and N/F a p-group, and A must be transitive on $P_0^{\#}$, $F - P_0$ and $N - F$. Since F has no elements of

(2) The referee has pointed out that this argument implicitly assumes the Feit-Thompson theorem on solvability of groups of odd order to show $|N|$ is even, and has contributed the following argument showing that Feit-Thompson is not necessary.

Let p_1, p_2, p_3 be the three prime divisors of $|N|$. If P_i is a Sylow p_i-subgroup and $1 \neq x_i \in Z_i = Z(P_i)$, then $P_i = C_N(x_i)$. Since all p_i-elements of N are conjugate, any p_i-element $x \neq 1$ is in the center of a unique Sylow p_i-subgroup. Since each Z_i is a T. I. set, we obtain a counting equation $|N| - 1 = \sum_{i=1}^{3} (|Z_i| - 1)\,|N : H_i|$ where $H_i = N_N(Z_i)$. If $|N| = n$, $|H_i| = h_i$, $|H_i : Z_i| = a_i$ we have $1 - n^{-1} = \sum_{i=1}^{3} (a_i^{-1} - h_i^{-1})$, or $1 - \sum_{i=1}^{3} a_i^{-1} = n^{-1} - \sum_{i=1}^{3} h_i^{-1} < 0$. If $a_1 \leq a_2 \leq a_3$ this forces $a_1 \leq 2$. $a_1 = 1$ would make N a Frobenius group with complement Z_1, a contradiction, so $a_1 = 2$ and $2 \mid |N|$.

order pq, F is a Frobenius group with kernel P_0, and Theorem 13.3(3) of [1] shows $|F/P_0| = q$.

Let Q be a Sylow q-subgroup of F. $N_N(Q) \cap P_0 = 1$, so $N_N(Q)$ is a complement to P_0 in N by a Frattini argument. Let P_1 be a Sylow p-subgroup of $N_N(Q)$, so $N_N(Q) = P_1Q$ and $P = P_0P_1$ is a Sylow p-subgroup of N. Choose $1 \neq x \in Z(P) \cap P_0$. P_1 normalizes Q, so P_1^x normalizes Q^x; but $P_1 = P_1^x$ while $Q^x \neq Q$. Therefore some elements of $N_N(Q)$ (those in P_1) normalize more than one Sylow q-subgroup.

Let $S = \bigcup_{n \in N} \{N_N(Q) - Q\}^n$. Since S is A-invariant we must have $S = N - F$. But $|N - F| = |F : P_0|(|N : F| - 1)|P_0|$. The number of groups Q^n, $n \in N$, is $|P_0|$, and $|N_N(Q) - Q| = |F : P_0|(|N : F| - 1)$, so $S = N - F$ forces S to be a disjoint union. This contradicts the conclusion of the previous paragraph.

Lemma 2.3. *Let A, N and $P = \mathrm{Fit}(N)$ be as in Lemma 2.2, with A transitive on $N - P$. If P is homocyclic of exponent p^2, then N is the group of Theorem 2.1(1). All such groups occur.*

Proof. Let Q be a Sylow q-subgroup of N. Then $N = PQ$. Elements of $N - P$ all have order q, so N has no elements of order pq and is a Frobenius group with kernel P and complement Q, $|Q| = q$. A must be transitive on $N - P$, $\Omega_1(P)^\#$ and $P - \Omega_1(P)$. We form AN (semidirect product). AN/P, being transitive on $(P/\Omega_1(P))^\#$, is a primitive linear group on $P/\Omega_1(P)$; $Q \cong QP/P \lhd AN/P$, so $P/\Omega_1(P)$ is a direct sum of some number m of isomorphic irreducible Q-modules. Since A is transitive on $N - P$, $N_A(Q)$ is transitive on $Q^\#$. Hilfssatz II.3.11 of [6] now implies that irreducible Q-submodules of $P/\Omega_1(P)$ have order p^{q-1}; hence $(X^q - 1)/(X - 1)$ is irreducible over $GF(p)$. By Lemma 2.1 of [11], $P = P_1 \times \cdots \times P_m$ where each P_i is Q-invariant, each $P_i/\Omega_1(P_i)$ Q-irreducible, each P_i homocyclic of order $p^{2(q-1)}$ and exponent p^2.

This group N does occur. For let P be homocyclic of exponent p^2, $|P| = p^{2m(q-1)}$, q a prime such that $(X^q - 1)/(X - 1)$ is irreducible over $GF(p)$. We saw in [2] that $GL(q - 1, p)$ has a solvable subgroup of order $(q - 1)(p^{q-1} - 1)$, the subgroup of semilinear transformations. We also saw by computing $|\mathrm{Aut}(P)|$ that every automorphism of $P/\Omega_1(P)$ can be realized from an automorphism of P. Hence there is a subgroup $\langle a, b\rangle$ of $\mathrm{Aut}(P)$ such that a has order $p^{m(q-1)} - 1$ on P. Also, if $c \in \langle a\rangle$ has order q, then $\langle b\rangle$, of order $q - 1$, transforms c to each of its nonidentity powers. Let $T = \{\alpha \in \mathrm{Aut}(P) | \alpha \text{ is trivial on } P/\Omega_1(P)\}$. $T \lhd \mathrm{Aut}(P)$ and $\langle a, b\rangle \leq N_{\mathrm{Aut}(P)}(\langle c\rangle)$ normalizes $C_T(\langle c\rangle)$, so $A = \langle a, b\rangle C_T(c)P$ acting by conjugation is a solvable automorphism group of $N = \langle c\rangle P$. We claim that A is transitive on $N - P$, $P - \Omega_1(P)$ and $\Omega_1(P)^\#$.

$C_P(c) = 1$, so P is transitive on each coset $c^iP \neq P$. $\langle b\rangle$ is transitive on

$\langle c\rangle^{\#}$, so $\langle b\rangle P \leq A$ is transitive on $N - P$. $\langle a\rangle \leq A$ has order $p^{m(q-1)} - 1 = |\Omega_1(P)^{\#}|$ on $\Omega_1(P)$ and is transitive on $\Omega_1(P)^{\#}$. Similarly, $\langle a\rangle$ is transitive on the set $\{x\Omega_1(P) | x \in P - \Omega_1(P)\}$ of cosets. We will show that $C_T(c)$ is transitive on any coset $x\Omega_1(P)$, $x \in P - \Omega_1(P)$; if $y \in \Omega_1(P)$ we will find $\alpha \in C_T(c)$ with $x^{\alpha} = xy$. Denote by P_1 the subgroup of P generated by $x, x^c, x^{c^2}, \cdots, x^{c^{q-2}}$; we have $x^{c^{q-1}} = x^{i_0}(x^c)^{i_1} \cdots (x^{c^{q-2}})^{i_{q-2}}$ and $P_1 = \langle x\rangle \times \langle x^c\rangle \times \cdots \times \langle x^{c^{q-2}}\rangle$ for some exponents $i_0, i_1, \cdots, i_{q-2} \in \mathbf{Z}$. We define $\alpha \in T$ by $x^{\alpha} = xy$, $(x^c)^{\alpha} = x^c y^c$, $\cdots$, $(x^{c^{q-2}})^{\alpha} = x^{c^{q-2}} y^{c^{q-2}}$, $\alpha = 1$ on a $\langle c\rangle$-invariant direct complement to P_1 in P. For $0 \leq j \leq q - 3$ we have

$$(x^{c^j})^{c\alpha} = (x^{c^{j+1}})^{\alpha} = x^{c^{j+1}} y^{c^{j+1}} = (x^{c^j} y^{c^j})^c = (x^{c^j})^{\alpha c},$$

so we have $\alpha c = c\alpha$ if and only if $(x^{c^{q-2}})^{\alpha c} = (x^{c^{q-2}})^{c\alpha}$.

$$(x^{c^{q-2}})^{\alpha c} = (x^{c^{q-2}} y^{c^{q-2}})^c = x^{c^{q-1}} y^{c^{q-1}}$$

and

$$\begin{aligned}(x^{c^{q-2}})^{c\alpha} &= (x^{c^{q-1}})^{\alpha} = x^{i_0} y^{i_0} \cdots (x^{c^{q-2}})^{i_{q-2}} (y^{c^{q-2}})^{i_{q-2}} \\ &= x^{c^{q-1}} y^{i_0} (y^c)^{i_1} \cdots (y^{c^{q-2}})^{i_{q-2}},\end{aligned}$$

so $\alpha c = c\alpha$ if and only if $y^{c^{q-1}} = y^{i_0}(y^c)^{i_1} \cdots (y^{c^{q-2}})^{i_{q-2}}$. This must be *true*, since $P/\Omega_1(P) \cong \Omega_1(P)$ as $\langle c\rangle$-modules via the isomorphism $z \to z^p$ so c must have the same minimal polynomial on $P/\Omega_1(P)$ and $\Omega_1(P)$.

Lemma 2.4. *Let A, N and $P = \mathrm{Fit}(N)$ be as in Lemma 2.2, with A transitive on $N - P$. If P is elementary abelian, then N is the group of Theorem 2.1(2). All such groups occur.*

Proof. Let Q be a Sylow q-subgroup of N, so $N = PQ$. Elements in $N - P$ all have order q, so N has no elements of order pq and is a Frobenius group with kernel P and complement Q, $|Q| = q$. We form the semidirect product AN.

First suppose AN/P is a primitive (not necessarily faithful) linear group on P. Then $Q \cong N/P \lhd AN/P$, so P is a direct sum of some number m of isomorphic irreducible Q-modules. Since A is transitive on $N - P$, also $N_A(Q)$ is transitive on $Q^{\#}$. It follows from Hilfssatz II.3.11 of [6] that irreducible Q-submodules of P must have order p^{q-1}; so $|P| = p^{m(q-1)}$ and $(X^q - 1)/(X - 1)$ is irreducible over $GF(p)$, N is the group of Theorem 2.1(2).

Second suppose AN/P is a reducible linear group on P. In this case, since AN/P has only two orbits on $P^{\#}$, there is a unique group P_0, $1 < P_0 < P$, fixed by AN/P. A is transitive on $P_0^{\#}$, $P - P_0$ and $N - P$. Since $P_0 \lhd AN$, $AN/C_{AN}(P_0)$ is a linear group on P_0. Being transitive on $P_0^{\#}$, $AN/C_{AN}(P_0)$ is a primitive linear group on P_0. $Q \cong QC_{AN}(P_0)/C_{AN}(P_0) \lhd AN/C_{AN}(P_0)$, so P_0 is a direct sum of isomorphic irreducible Q-modules. As in the previous paragraph, irreducible Q-submodules of P must have order p^{q-1}. Thus $(X^q - 1)/(X - 1)$ is irreducible over $GF(p)$. Since $N = PQ$ is a Frobenius group, *all* irreducible Q-submodules of P have order p^{q-1} and hence all are isomorphic. N is the group of Theorem 2.1(2).

Finally suppose AN/P is an irreducible but imprimitive linear group on P. Let $P = P_1 \oplus \cdots \oplus P_t$, the P_i spaces of imprimitivity, and let $T = \{g \in AN \mid g(P_1) = P_1\}$; T must be transitive on $P_1^{\#}$. Since $Q \cong N/P \lhd AN/P$ and AN/P is transitive on $\mathcal{S} = \{P_1, \cdots, P_t\}$, Q is half-transitive on $\mathcal{S}$; orbits of Q on $\mathcal{S}$ have length q or 1. If of length q, and $v_0 \in P_1^{\#}$, then the subgroup of P generated by $\{v_0^y \mid y \in Q\}$ has order p^q. However, if $Q = \langle x \rangle$ then the annihilator polynomial of x on v_0 divides $(X^q - 1)/(X - 1)$; hence this subgroup has order $\leq p^{q-1}$; we have proved that Q fixes all groups P_i. Hence $Q \cong N/P \lhd T/P$, where T/P is a primitive linear group on P_1. This means that P_1 is a direct sum of isomorphic irreducible Q-modules, and as in the previous two paragraphs we find that irreducible Q-submodules of P_1 must have order p^{q-1}. Again N is the group of Theorem 2.1(2).

If p is odd, this group $N = PQ$ does occur. For choose $\theta \in GF(p^{m(q-1)})$ of multiplicative order $\frac{1}{2}(p^{m(q-1)} - 1)$, $\lambda \in \langle \theta \rangle$ of order q, and define mappings $a: v \to \theta v$, $b: v \to v^p$, $c: v \to \lambda v$ for all $v \in GF(p^{m(q-1)})^+ = P$. $\langle a, b \rangle$ is a group of semilinear transformations of P, $c \in \langle a \rangle$ has order q, and $\langle a \rangle \lhd \langle a, b \rangle$. Let $Q = \langle c \rangle$; then $N = PQ$ is a Frobenius group of the desired type. $A = \langle a, b \rangle P$ acts by conjugation on $N \lhd A$. $GF(p)(\lambda) = GF(p^{q-1})$, so $\langle b \rangle$ is transitive on $Q^{\#}$. $C_P(Q) = 1$, so P is transitive on $c^i P$ for any coset $c^i P \neq P$. The last two facts mean that A is transitive on $N - P$. Let $S = \{\alpha \in P \mid \alpha^{\frac{1}{2}(p^{m(q-1)}-1)} = 1\}$, $T = P^{\#} - S$. Since b is an automorphism of $GF(p^{m(q-1)})$, we see that $\langle a, b \rangle$ fixes S and T; but $\langle a \rangle$ is transitive on each set, so A has exactly three orbits $N - P$, S and T on $N^{\#}$.

If $p = 2$, $N = PQ$ does also occur. For choose $\theta \in GF(2^{m(q-1)})$ of multiplicative order $(2^{m(q-1)} - 1)/3$, $\lambda \in GF(2^{m(q-1)})$ of multiplicative order q, and define $a: v \to \theta v$, $b: v \to v^2$, $c: v \to \lambda v$, all $v \in GF(2^{m(q-1)})^+ = P$. Then consider $A = \langle a, b \rangle P$ as an automorphism group acting by conjugation on $N = \langle c \rangle P$; $c^b = c^2$ and P acts transitively on any coset $c^i P \neq P$, so A is transitive on $N - P$. The orbits of a on $P^{\#}$ are $S = \{\alpha \in P \mid \alpha^{(2^{m(q-1)}-1)/3} = 1\}$ and its two cosets rS and

$\tau^2 S$, so $\langle a, b\rangle P$ has two orbits S and $\tau S \cup \tau^2 S$ on $P^{\#}$. This completes the proof of Lemma 2.4.

Lemma 2.5. *Let A, N and $P = \mathrm{Fit}(N)$ be as in Lemma 2.2, with A transitive on $N - P$. If P is nonabelian, then N is the group of Theorem 2.1(3). Infinitely many such groups occur.*

Proof. As in the proof of Lemma 2.4, $N = PQ$ is a Frobenius group with $|Q| = q$. A is an automorphism group of P with only two orbits on $P^{\#}$, so P must be one of the nonabelian p-groups of Theorem 0.1.

To see that infinitely many such groups occur, let $P = A(n, \theta)$ as in Theorem 0.1(iv). We know from [2] that if $\lambda \in GF(2^n)$ has order $2^n - 1$, then $\psi\colon (\alpha, \zeta) \to (\lambda\alpha, \lambda^{1+\theta}\zeta)$ is an automorphism transitive on $(P')^{\#}$ and $(P/P')^{\#}$, and if $T = \{\alpha \in \mathrm{Aut}(P) \mid \alpha \text{ is trivial on } P' \text{ and } P/P'\}$ then $\langle\psi\rangle T$ has only two orbits on $P^{\#}$. If $\sigma \in \mathrm{Aut}(GF(2^n))$, we easily see that $\Phi_\sigma\colon (\alpha, \zeta) \to (\alpha^\sigma, \zeta^\sigma)$ is an automorphism of P; if $\sigma\colon x \to x^{2^i}$, then $\Phi_\sigma^{-1}\psi\Phi_\sigma = \psi^{2^i}$, so each Φ_σ normalizes $\langle\psi\rangle$.

Now choose an odd prime q such that $(X^q - 1)/(X - 1)$ is irreducible over $GF(2)$, choose an integer $m > 0$, set $n = m(q - 1)$, and choose $\lambda_0 \in GF(2^n)$ of multiplicative order q. Define $\psi_0 \in \mathrm{Aut}(P)$ by $\psi_0\colon (\alpha, \zeta) \to (\lambda_0\alpha, \lambda_0^{1+\theta}\zeta)$; $N = \langle\psi_0\rangle P$ is a Frobenius group. Define $\sigma_0 \in GF(2^n)$ by $\sigma_0\colon x \to x^2$ and set $\Phi = \Phi_{\sigma_0}$. $\langle\Phi, \psi\rangle P$, acting as an automorphism group of N by conjugation, is transitive on $N - P$ and $(P')^{\#}$, since $\langle\Phi\rangle$ acts transitively on $\langle\psi_0\rangle^{\#}$. $\langle\psi\rangle$ is also transitive on $\{xP' \mid x \in P - P'\}$. As in the proof of Lemma 2.3 we find that $A = \langle\Phi, \psi\rangle C_T(\psi_0)P$ is transitive on $P - P'$, completing the proof.

Lemma 2.6. *Let A, N and $P = \mathrm{Fit}(N)$ be as in Lemma 2.2, with A transitive on $P^{\#}$. Then N is a Frobenius group with complement Q a Sylow q-subgroup. Q is cyclic of order q, cyclic of order q^2, or quaternion of order 8.*

Proof. If N is not a Frobenius group, then N contains elements of order pq and since A has only three orbits on $N^{\#}$, P and Q are elementary abelian. If $x \in P^{\#}$, then $C_N(x) = PC_Q(x)$, $|C_Q(x)| = |C_N(x)|_q$. Since A is transitive on $P^{\#}$, $|C_Q(x)|$ is the same for every $x \in P^{\#}$. Since N is not Frobenius and not abelian, $1 < C_Q(x) < Q$. Write $P = P_1 \times \cdots \times P_k$, the P_i irreducible Q-modules.

If $k > 1$, choose $x_i \in P_i^{\#}$ for each i; then $C_Q(x_1 + \cdots + x_k) \subseteq C_Q(x_i)$ for every i, so we must have equality for every i. Fixing $x_1 \in P_1^{\#}$ and letting $x_2, \cdots, x_k$ vary throughout $P_2, \cdots, P_k$, and then fixing $x_2, \cdots, x_k$ and letting x_1 vary through P_1, etc., we eventually get $C_Q(x_1) = C_Q(x)$ for every $x \in P^{\#}$, $C_Q(x_1) = C_Q(P) = 1$, a contradiction.

Therefore $k = 1$, and Q acts irreducibly on P. Fix $y \in Q^{\#}$ and note that

$1 < C_P(y) < P$. If $y_1 \in Q$ and $x \in C_P(y)$, then $xy = yx$, $x^{y_1}y = yx^{y_1}$, $x^{y_1} \in C_P(y)$, Q fixes $C_P(y)$, contradicting Q-irreducibility of P.

Therefore N is a Frobenius group with complement Q. By Theorem 13.3(3) of [1], subgroups of Q of order q^2 are cyclic. A has only two orbits on $N - P$, so Q has exponent q or q^2. Q can have only one subgroup of order q, and Theorem 32.4 of [1] shows Q is cyclic or quaternion.

Lemma 2.7. *Let A, N, P and Q be as in Lemma 2.6, with Q cyclic of order q. Then N is a group of Theorem 2.1(2) or (4). All groups of type (4) occur.*

Proof. The semidirect product AN acts transitively on $P^{\#}$ and has at most two orbits on $N - P$. $Q \cong N/P \lhd AN/P$ and AN/P is a primitive linear group on P, so P is the direct sum of isomorphic irreducible Q-modules. $N_{AN}(Q)$ must have at most two orbits on $Q^{\#}$, so Hilfssatz II.3.11 of [6] implies that irreducible Q-submodules of P have order p^{q-1} or $p^{\frac{1}{2}(q-1)}$. If of order p^{q-1}, N is the group of Theorem 2.1(2).

We show that the case $p^{\frac{1}{2}(q-1)}$ also occurs. Assume primes p, q are related as in Theorem 2.1(4). Inside $GF(p^{\frac{1}{2}m(q-1)})$ for some $m > 0$, let μ be a multiplicative generator and λ an element of multiplicative order q; define $a: \alpha \to \mu\alpha$, $b: \alpha \to \alpha^p$, $c: \alpha \to \lambda\alpha$ for all $\alpha \in P = GF(p^{\frac{1}{2}m(q-1)})^+$. Conjugation by b has two orbits on $\langle c \rangle^{\#}$. Let $N = \langle c \rangle P$ and $A = \langle a, b \rangle P$, acting by conjugation on N. λ can be chosen to be a root of either of the two irreducible factors of $(X^q - 1)/(X - 1)$.

Lemma 2.8. *Let A, N, P and Q be as in Lemma 2.6, with Q cyclic of order q^2. Then N is a group of Theorem 2.1(5). All such groups occur.*

Proof. Here the semidirect product AN is by conjugation transitive on $P^{\#}$ and has two orbits, elements of order q and elements of order q^2, on $N - P$. $Q \cong N/P \lhd AN/P$ and AN/P is a primitive linear group on $P^{\#}$, so P is the direct sum of isomorphic irreducible Q-modules. $N_A(Q)$ must be transitive on $Q - \Omega_1(Q)$, so Hilfssatz II.3.11 of [6] implies that irreducible Q-submodules of P have order $p^{q(q-1)}$.

We must show this case does occur. So suppose p and q are primes such that $(X^{q^2} - 1)/(X^q - 1)$ is irreducible over $GF(p)$. Inside $GF(p^{mq(q-1)})$ for some $m > 0$, let μ be a multiplicative generator and λ an element of multiplicative order q^2; define $a: \alpha \to \mu\alpha$, $b: \alpha \to \alpha^p$, $c: \alpha \to \lambda\alpha$ for all $\alpha \in P = GF(p^{mq(q-1)})^+$. Conjugation by b sends c to all elements in $\langle c \rangle - \langle c^q \rangle$, and is also transitive on $\langle c^q \rangle^{\#}$. Let $N = \langle c \rangle P$ and $A = \langle a, b \rangle P$, acting by conjugation on N.

Lemma 2.9. *Let A, N, P and Q be as in Lemma 2.6, with Q quaternion of order 8. Then N is a group of Theorem 2.1(6). All such groups occur.*

Proof. Here AN is by conjugation transitive on $P^{\#}$ and has exactly two orbits, elements of order 2 and elements of order 4, on $N - P$. $Q \cong QP/P \lhd AN/P$, $Z(Q) \cong Z(Q)P/P \lhd AN/P$ and AN/P is a primitive linear group on P; this means that P is a direct sum of isomorphic irreducible Q-submodules and a direct sum of isomorphic irreducible $Z(Q)$-submodules. Therefore if $Z(Q) = \langle z \rangle$ then $x^z = x^{-1}$, all $x \in P$. For any odd prime p, all faithful irreducible $GF(p)Q$-modules have dimension 2 (and are isomorphic).

We first consider the possibility $|P| > p^2$; in that case $P = P_1 \oplus \cdots \oplus P_k$, $k > 1$, the P_i isomorphic faithful irreducible Q-modules, $|P_i| = p^2$ for all i. $Q \cong QC_{AN}(P)/C_{AN}(P) \lhd AN/C_{AN}(P)$, where $G = AN/C_{AN}(P)$ is transitive on $P^{\#}$ and isomorphic to a subgroup of $GL(2k, p)$. Since P_1 is an absolutely irreducible $GF(p)Q$-module, Theorem 25.9 of [1] applies and says that if V is a k-dimensional vector space over $GF(p)$, then there are projective representations $T: G \to GL(P_1)$, $U: G \to GL(V)$ such that $P \cong P_1 \otimes V$. Denote $G_1 = T(G)Z(GL(P_1))$, $G_2 = U(G)Z(GL(V))$; G_1 and G_2 are subgroups of $GL(P_1)$ and $GL(V)$, respectively, and $G_1 \times G_2$ acts naturally on $P_1 \otimes V$ by an action satisfying $(g_1, g_2)(u \otimes v) = g_1 u \otimes g_2 v$, all $g_i \in G_i$, $u \in P_1$, $v \in V$. If G is transitive on $P^{\#}$, then $G_1 \times G_2$ must be transitive on $(P_1 \otimes V)^{\#}$. But $S = \{u \otimes v \mid u \in P_1^{\#}, v \in V^{\#}\}$ is a proper subset of $(P_1 \otimes V)^{\#}$ fixed by $G_1 \times G_2$, so G cannot be transitive on $P^{\#}$.

We have proved that $|P| = p^2$. $AN/C_{AN}(P)$ is isomorphic to a subgroup of $GL(2, p) = \mathrm{Aut}(P)$. $Q \cong QC_{AN}(P)/C_{AN}(P) \lhd AN/C_{AN}(P)$, so there is a quaternion subgroup $\bar{Q}$ of $GL(2, p)$ acting on P, and AN can only be transitive on $P^{\#}$ if $N_{GL(2,p)}(\bar{Q})$ is transitive on $P^{\#}$. $|N_{GL(2,p)}(\bar{Q})|$ divides $|\mathrm{Aut}(\bar{Q})|\,|C_{GL(2,p)}(\bar{Q})| = 24(p-1)$ and $|P^{\#}| = (p+1)(p-1)$, so $N_{GL(2,p)}(\bar{Q})$ can only be transitive on $P^{\#}$ if $p + 1$ divides 24. This means $p \in \{3, 5, 7, 11, 23\}$.

These five groups all occur, and form case (6) of Theorem 2.1. To check this in case $p = 5$ is easy. Let λ be a multiplicative generator of $GF(5)^{\#}$. We see in the proof of Satz II.8.10 of [6] that

$$\bar{Q} = \left\langle \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$$

is a quaternion subgroup of $GL(2, p)$. Computation shows that

$$N_{GL(2,p)}(\bar{Q}) = \left\langle \bar{Q}, \begin{pmatrix} 1 & 1 \\ \lambda & \lambda^{-1} \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right\rangle$$

and that $N_{GL(2,p)}(\bar{Q})$ is transitive on $P^{\#}$.

The other four values of p satisfy $p \equiv 3 \pmod 4$, and we can use the methods

of §II.8 of [6], where the fact $SU(2, p^2) \cong SL(2, p)$ is proved. If $\lambda \in GF(p^2)$ has order 4, then

$$A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^p \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

generate a quaternion subgroup of $SU(2, p^2)$. (If V is a 2-dimensional vector space over $GF(p^2)$ with basis $\{w_1, w_2\}$, these matrices preserve the hermitian form $(\alpha_1 w_1 + \alpha_2 w_2, \beta_1 w_1 + \beta_2 w_2) = \alpha_1 \beta_1^p + \alpha_2 \beta_2^p$ on V.) Choose $a, c \in GF(p^2)$ satisfying $N(a) = aa^p = -1$ and $c^p = -c \neq 0$. Define a new basis for V by $u_1 = w_1 + aw_2$, $u_2 = cw_1 - caw_2$. If T_A and T_B are the linear transformations induced on V in the basis $\{w_1, w_2\}$ (so $T_B(w_1) = -w_2$, $T_B(w_2) = w_1$), then T_A and T_B have matrices in $SL(2, p)$ in the basis $\{u_1, u_2\}$. This must be true, since the proof of Satz II.8.8 of [6] shows that *all* linear transformations in $U(2, p^2)$ have matrices in $GL(2, p)$ with respect to the basis $\{u_1, u_2\}$. (Note that the u_1, u_2 here are preferable to the u_1, u_2 in [6], since the latter do not satisfy $(u_1, u_2) = -(u_2, u_1)$, needed in the proof.)

We also find by computation that the unitary matrices

$$C = \begin{pmatrix} \lambda & 1 \\ -1 & -\lambda \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} \gamma & \gamma \\ \gamma\lambda & -\gamma\lambda \end{pmatrix}$$

normalize $\langle A, B \rangle$, where $\gamma^p = -\gamma\lambda$, $\gamma \in GF(p^2)$. Let $f(X)$ be the irreducible polynomial for a over $GF(p)$. We find that the following values of c, λ, γ will suffice, and we list some matrices in $N_{GL(2,p)}(Q)$ obtained by writing T_A, T_B, T_C, T_D in the basis $\{u_1, u_2\}$:

p	$f(X)$	c	λ	γ	Q	$N_{GL(2,p)}(Q)$
3	$X^2 + X - 1$	a^2	a^2	a^3	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$	
7	$X^2 - 3X - 1$	a^2	a^2	a^2	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 5 & 4 \\ 5 & 2 \end{pmatrix}$
11	$X^2 - 5X - 1$	a^6	a^6	a^9	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 8 & -1 \\ -1 & 3 \end{pmatrix}$	$\begin{pmatrix} 7 & -1 \\ 2 & 1 \end{pmatrix}$
23	$X^2 + X - 1$	a^{12}	a^{12}	a^6	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 11 & -4 \\ -4 & 12 \end{pmatrix}$	$\begin{pmatrix} 11 & -3 \\ -5 & 12 \end{pmatrix}, \begin{pmatrix} 6 & 3 \\ 8 & 12 \end{pmatrix}$

For each value of p, it is easy to check that the matrices under Q give a quaternion subgroup of $GL(2, p)$, and all the matrices given in Q and $N_{GL(2,p)}(Q)$ generate a transitive group on the nonzero elements of a 2-dimensional $GF(p)$-vector space P. We also know $N_{GL(2,p)}(Q)$ is transitive on $Q - Z(Q)$, so if we

set $N = QP$, $A = N_{GL(2,p)}(Q)P$ acting on N by conjugation, then A has only three orbits on $N^{\#}$.

This completes the proof of Lemma 2.9. Lemmas 2.2–2.9 together constitute the proof of Theorem 2.1.

3. The case when N is a p-group of class 3.

Theorem 3.1. *Let $N = P$ be a finite class 3 p-group, A a solvable automorphism group of P acting with only three orbits on $P^{\#}$. Then we have one of the following:*

(1) *P is a 2-group or a 3-group.*

(2) *$|P/P'| = p^2$ and $|P|$ is p^4 or p^5.*

(3) *P has exponent p.*

Moreover, some groups in (1) and (2) occur. If p is a prime ≥ 5, $n \geq 2$, $\epsilon \in GF(p^{2n})$ satisfies $\epsilon + \epsilon^{p^n} = 0$, and $g: GF(p^{2n}) \times GF(p^{2n}) \to GF(p^{2n})$ is a function satisfying $g(\alpha, 0) = g(0, \alpha) = g(\alpha, -\alpha) = 0$, $g(\lambda\alpha, \lambda\delta) = \lambda^{2+p^n} g(\alpha, \delta)$, and

$$g(\alpha, \delta) + g(\alpha + \delta, \mu) = g(\delta, \mu) + g(\alpha, \delta + \mu)$$

for all $\alpha, \delta, \mu, \lambda \in GF(p^{2n})$, then $P_g = \{(\alpha, \beta, \gamma) \in GF(p^{2n}) \times GF(p^n) \times GF(p^{2n}) \mid (\alpha, \beta, \gamma)(\delta, \epsilon, \phi) = (\alpha + \delta, \beta + \epsilon + \tfrac{1}{2}\epsilon(\alpha\delta^{p^n} - \alpha^{p^n}\delta), \gamma + \phi + \tfrac{1}{2}(\alpha\epsilon - \delta\beta) + \epsilon(\alpha^2\delta^{p^n} + \alpha^{p^n}\delta^2)/8 + g(\alpha, \delta))\}$ is a group in (3), at least when $p^n \equiv 2 \pmod 3$.

Remarks. The reader should have little difficulty verifying that some groups in (1) and (2) occur. We restrict our study to primes $p \geq 5$ here. The cases $p = 2$ and $p = 3$ are harder, for two reasons; the p-groups need not be regular, and more p-groups for these values of p occur in Theorem 0.1. (We will see that $P/[P, P']$ must be a group occurring in Theorem 0.1.) Groups occurring in (3) must be much like the groups P_g; same orders, same commutator maps $P/P' \times P/P' \to P'/[P, P']$ and $P/P' \times P'/[P, P'] \to [P, P']$, etc. But we have not been able to determine whether the groups P_g are the only groups in (3). We also do not know whether, for given p^n, the groups P_g are all isomorphic. (Note that for any $\tau \in GF(p^{2n})$,

$$g(\alpha, \delta) = \tau[2\alpha^{1+p^n}\delta + \alpha^{p^n}\delta^2 + \alpha^2\delta^{p^n} + 2\alpha\delta^{1+p^n}]$$

is an allowable function g.)

In this section we denote $P_2 = [P, P']$. We need the following

Lemma 3.2. *Let $G = \langle g \rangle$ be a cyclic group of order m, p a prime, $p \nmid m$. If d*

is the largest degree of an irreducible $GF(p)G$-module, then the degree of any irreducible $GF(p)G$-module divides d.

Proof. The semisimple ring $GF(p)G$ has form $GF(p)G \cong F_1 \oplus \cdots \oplus F_r$, the F_i finite fields which are the irreducible $GF(p)G$-modules. Each F_i must be generated over $GF(p)$ by the projection of g onto the ith summand; the latter must be a t_ith root of 1, some t_i dividing m. Therefore F_i is a splitting field of $X^{t_i} - 1$ over $GF(p)$ and is a subfield of $K = GF(p)(\zeta)$, ζ a primitive mth root of 1 over $GF(p)$. Therefore $d = \dim_{GF(p)} K = \dim_{F_i} K \cdot \dim_{GF(p)} F_i$, proving that $\dim F_i$ divides d.

Proof of Theorem 3.1. Since P has class 3, $P > P' > P_2 > 1$ and P has a solvable automorphism group A transitive on $P_2^{\#}$, $P' - P_2$ and $P - P'$. Necessarily $Z(P) = P_2$ and $\Phi(P) = P'$. By Satz VI.2.3 of [6], we can find a Hall p'-subgroup H of A and a Sylow p-subgroup Q of A such that $A = HQ = QH$. Let V be either P/P', P'/P_2 or P_2. $p \nmid |V^{\#}|$, so there is a $v \in V^{\#}$ such that $Q \subseteq A_v$. Then $A = HA_v$ must contain $|H| \cdot |A_v|/|H \cap A_v| = |H : H_v| \cdot |A_v|$ elements, and $|A : A_v| = |H : H_v|$. This means that H is transitive on $(P/P')^{\#}$, $(P'/P_2)^{\#}$ and $P_2^{\#}$. By Satz III.3.18 of [6] we also know that H is faithful on P/P'. Throughout the rest of this proof we shall assume $p \geq 5$, and prove that (2) or (3) holds.

If $|P/P'| \leq p^2$, then $|P/P'| = p^2$, say $P/P' = \langle aP' \rangle \times \langle bP' \rangle$. P'/P_2 must be generated by $[a, b]P_2$, and transitivity of H on $(P'/P_2)^{\#}$ shows $|P'/P_2| = p$. Finally, P_2 must be generated by $[a, [a, b]]$ and $[b, [a, b]]$. P_2 has exponent p by transitivity of H on $P_2^{\#}$, so $|P_2| \leq p^2$ and P is the group of (2).

Suppose now that $|P/P'| = p^m > p^2$. Set $|P'/P_2| = p^n$. By [7], H must act as a group of semilinear transformations on P/P'. Therefore there is $\xi \in H$, $\langle \xi \rangle \lhd H$, $|\langle \xi \rangle|$ divisible by $(p^m - 1)/(m, p^m - 1)$. As in [2], there must exist "conjugate bases" $u_0, u_1, \cdots, u_{m-1}$ and $v_0, v_1, \cdots, v_{n-1}$ of $P/P' \otimes GF(p^m)$ and $P'/P_2 \otimes GF(p^m)$, respectively, with $u_i\xi = \lambda^{p^i} u_i$ and $v_j\xi = \lambda^{p^j(1+p^n)} v_j$, where λ is an eigenvalue of ξ on P/P' and v_i is a scalar multiple of $[u_i, u_{n+i}]$ in $L \otimes GF(p^m)$, L the Lie ring of P. (Note we are in the case $n = r = \frac{1}{2}m$ of [2], since P/P_2 must be the group of Theorem 0.1(vi).)

We have $[u_i, v_j]\xi = \lambda^{p^i + p^j(1+p^n)}[u_i, v_j]$, so either $[u_i, v_j] = 0$ or $\lambda^{p^i + p^j(1+p^n)}$ is an eigenvalue of ξ on $P_2 \otimes GF(p^m)$. H is a primitive linear group on P_2 and $\langle \xi \rangle \lhd H$, so P_2 is a direct sum of isomorphic irreducible (not necessarily faithful) $\langle \xi \rangle$-modules.

Suppose that $0 \neq [u_i, v_j]$. Since v_j is a scalar multiple of $[u_j, u_{n+j}]$ this means $[u_i, [u_j, u_{n+j}]] \neq 0$, and the Jacobi identity then implies that either $[u_j, [u_{n+j}, u_i]] \neq 0$ or $[u_{n+j}, [u_i, u_j]] \neq 0$. In particular, $[u_{n+j}, u_i] \neq 0$ or $[u_i, u_j] \neq 0$

for values of i and j with $j < n$. The only nonzero $[u_s, u_t]$ are the terms $[u_k, u_{n+k}]$ or $[u_{n+k}, u_k]$ (by [2]), so the inequality $[u_{n+j}, u_i] \neq 0$ forces $i = j$ and the inequality $[u_i, u_j] \neq 0$ forces $i = n + j$. We conclude that the only terms $[u_i, v_j]$ which can be nonzero are the terms $[u_0, v_0], [u_1, v_1], \cdots, [u_{n-1}, v_{n-1}], [u_n, v_0], [u_{n+1}, v_1], \cdots, [u_{2n-1}, v_{n-1}]$. The $\{u_i\}$ and $\{v_j\}$ are conjugate bases; this means that if $\langle\sigma\rangle$ is the Galois group of $GF(p^m)$ over $GF(p)$, then $u_0^\sigma = u_1, \cdots, u_{2n-2}^\sigma = u_{2n-1}$, $u_{2n-1}^\sigma = u_0$, $v_0^\sigma = v_1, \cdots, v_{n-2}^\sigma = v_{n-1}$, $v_{n-1}^\sigma = v_0$. Applying σ to the list of terms $[u_0, v_0], \cdots, [u_{2n-1}, v_{n-1}]$ shows that any one of them is nonzero if and only if all of them are nonzero. Since P has class 3, some must be nonzero, so all are nonzero. Denote $w_0 = [u_0, v_0]$, $w_1 = [u_1, v_1], \cdots, w_{2n-1} = [u_{2n-1}, v_{n-1}]$. We have

$$w_0\xi = [u_0, v_0]\xi = [u_0\xi, v_0\xi] = [\lambda u_0, \lambda^{1+p^n} v_0] = \lambda^{2+p^n} w_0,$$

$w_1\xi = \lambda^{2p+p^{n+1}} w_1, \cdots$, and we find that the following numbers are eigenvalues of ξ on $P_2 \otimes GF(p^m)$:

$$(*) \qquad \begin{aligned} &\lambda^{2+p^n}, \lambda^{2p+p^{n+1}}, \cdots, \lambda^{2p^{n-1}+p^{2n-1}}, \\ &\lambda^{1+2p^n}, \lambda^{p+2p^{n+1}}, \cdots, \lambda^{p^{n-1}+2p^{2n-1}}. \end{aligned}$$

Denote $t = |\langle\xi\rangle|$, so t divides $p^{2n} - 1$ and is a multiple of $(p^{2n} - 1)/(2n, p^{2n} - 1)$. We wish to show the list (*) contains more than n distinct members; then Lemma 3.2, the fact that P_2 is a direct sum of isomorphic irreducible $\langle\xi\rangle$-modules, and the fact the w_i span $P_2 \otimes GF(p^m)$ together will imply that $|P_2| = p^{2n}$ and $\langle\xi\rangle$ acts irreducibly on P_2.

The exponents in the list (*) satisfy the inequality

$$(I) \qquad \begin{aligned} 2 + p^n < 1 + 2p^n < 2p + p^{n+1} < p + 2p^{n+1} \\ < \cdots < 2p^{n-1} + p^{2n-1} < p^{n-1} + 2p^{2n-1} \end{aligned}$$

and are therefore all different. Two eigenvalues can only be equal if the corresponding exponents are congruent modulo t.

If n is even, the $(n + 1)$th term in (I) is $2p^{n/2} + p^{n+(n/2)}$, the smallest term is $2 + p^n$, and we have

$$(2p^{n/2} + p^{n+(n/2)}) - (2 + p^n) < p^{n+(n/2)} < (p^{2n} - 1)/2n \leq t,$$

where only the next-to-last inequality requires proof. It is true for $p^n = 5^2$. For

other allowed values of p^n, we have $3n < p^{n/2}$, so $2n < p^{n/2} - 1/(p^{n+(n/2)})$, $2np^{n+(n/2)} < p^{2n} - 1$, and $p^{n+(n/2)} < (p^{2n} - 1)/2n$.

If $n \geq 3$ is odd, the $(n+1)$th term in (I) is $p^{(n-1)/2} + 2p^{n+(n-1)/2}$, the smallest term is $2 + p^n$, and we have

$$(p^{(n-1)/2} + 2p^{n+(n-1)/2}) - (2 + p^n) < 2p^{n+(n-1)/2} < (p^{2n} - 1)/2n \leq t,$$

where only the next-to-last inequality requires proof. For all allowed values of p^n we have $5n < p^{(n+1)/2}$, so $4n < p^{(n+1)/2} - 1/(p^{n+(n-1)/2})$, $4np^{n+(n-1)/2} < p^{2n} - 1$, and $2p^{n+(n-1)/2} < (p^{2n} - 1)/2n$.

We conclude in both cases that ξ has at least $n+1$ distinct eigenvalues on P_2, so P_2 is an irreducible $\langle\xi\rangle$-module, $|P_2| = p^{2n} = |P/P'|$.

Since P has class 3, any four-term commutator is 1 and P' is abelian. $xP_2 \to x^p$ is therefore a homomorphism from P'/P_2 to P_2. Its image, a characteristic subgroup of P, cannot be all of P_2 and hence must be trivial; P' has exponent p.

Since P/P_2 is a group of Theorem 0.1(vi), it also has exponent p. Since $p > 3$, Satz III.10.2(a) and Satz III.10.8(c) of [6] tell us that P is regular and for any $x, y \in P$ we have $(xy)^p = x^p y^p c^p = x^p y^p$, some $c \in P'$.

If the map $x \to x^p$ from P to P_2 is nontrivial, it will be a $\langle\xi\rangle$-isomorphism between P/P' and P_2 and ξ will have the same eigenvalues on $P/P' \otimes GF(p^m)$ and $P_2 \otimes GF(p^m)$. In particular, λ^{2+p^n} will equal λ^{p^i} for some $0 \leq i < 2n$, and we will have

$$2 + p^n \equiv p^i \pmod{t}.$$

We will show this last congruence is impossible, and hence that P has exponent p. Since $2 + p^n < t$, for the inequality to hold we must have $n < i \leq 2n - 1$, $2 + p^n < p^i$. Let $p^{2n} - 1 = td$, so $d \mid 2n$, $t \mid (p^i - p^n - 2)$. The facts $t \mid (p^i + p^n - 2)$ and $t \mid (2p^{2n} - 2)$ imply that $t \mid (2p^{2n} + p^n - p^i)$, so $t \mid p^n(2p^n + 1 - p^{i-n})$. Since $(t, p) = 1$, this means $2p^n + 1 \equiv p^{i-n} \pmod{t}$. $1 < p^{i-n} < p^n$, so this forces $t < 2p^n$. Thus $p^{2n} - 1 = td < 2p^n \cdot 2n$, $p^{2n} \leq 2p^n \cdot 2n$, $p^n \leq 4n$, the desired contradiction. P must have exponent p, and be a group of Theorem 3.1(3).

Now let P_g be as in the statement of Theorem 3.1. This family of groups was constructed with the methods of [5] and [2]. Knowledge of all the $[u_i, u_j]$ and $[u_i, v_j]$ enables one to construct the commutator maps $[\ ,\ ]: P/P' \times P/P' \to P'/P_2$ and $[\ ,\ ]: P/P' \times P'/P_2 \to P_2$. Elements of P are then represented as triples (α, β, γ), and multiplication of triples must satisfy the commutator laws computed, the definition of a group, and the requirement that if λ is a multiplicative generator of $GF(p^{2n})^\#$ then $\xi: (\alpha, \beta, \gamma) \to (\lambda\alpha, \lambda^{1+p^n}\beta, \lambda^{2+p^n}\gamma)$ must be an automorphism of P.

We discuss the verification that P_g is a group with the desired properties. We easily check that $(0, 0, 0)$ is an identity element in P_g, and that $(-\alpha, -\beta, -\gamma)$ is an inverse of (α, β, γ) with respect to this identity. Using the property $g(\delta, \mu) + g(\alpha, \delta + \mu) = g(\alpha, \delta) + g(\alpha + \delta, \mu)$ of g, we check the associative law; so P_g is a group. Next we verify that $\xi: (\alpha, \beta, \gamma) \to (\lambda\alpha, \lambda^{1+p^n}\beta, \lambda^{2+p^n}\gamma)$ is an automorphism of P_g, using the fact $g(\lambda\alpha, \lambda\delta) = \lambda^{2+p^n} g(\alpha, \delta)$.

Let I be the group of all automorphisms of P_g which are trivial on P_g/P_g'. For any $\sigma \in GF(p^{2n})$, we easily check that $\Phi_\sigma \in I$, where $\Phi_\sigma: (\alpha, \beta, \gamma) \to (\alpha, \beta, \gamma + \sigma\alpha)$. This means that for any $x \in P_g - P_g'$, $\{\Phi_\sigma \mid \sigma \in GF(p^{2n})\}$ is transitive on the coset $x(P_g)_2$. Computation shows that $(\delta, 0, 0)^{-1}(\alpha, 0, 0)(\delta, 0, 0) = (\alpha, \epsilon(\alpha\delta^{p^n} - \alpha^{p^n}\delta)$, something). If $\epsilon(\alpha\delta^{p^n} - \alpha^{p^n}\delta) = \epsilon(\alpha\delta_1^{p^n} - \alpha^{p^n}\delta_1)$ for some δ and δ_1, then $\alpha(\delta - \delta_1)^{p^n} = \alpha^{p^n}(\delta - \delta_1)$, so $(\delta - \delta_1)^{p^n - 1} = \alpha^{p^n - 1}$ or $\delta - \delta_1 = 0$. Therefore there are only p^n different values of δ giving the same value $\epsilon(\alpha\delta^{p^n} - \alpha^{p^n}\delta)$; p^{2n} possible δ's, so all p^n possible elements of $GF(p^n)$ appear as values $\epsilon(\alpha\delta^{p^n} - \alpha^{p^n}\delta)$. The inner automorphisms are certainly in I, so I is actually transitive on any coset xP_g', $x \in P_g - P_g'$.

Computation also shows that

$$(\alpha, 0, 0)^{-1}(0, \beta, 0)(\alpha, 0, 0) = (0, \beta, -\alpha\beta);$$

thus the group of inner automorphisms is transitive on cosets $y(P_g)_2$, $y \in (P_g)' - (P_g)_2$.

The automorphism ξ is transitive on $(P_g/P_g')^\#$ and $(P_g'/(P_g)_2)^\#$, since $|\langle\lambda\rangle| = p^{2n} - 1 = |(P_g/P_g')^\#|$ and $|\langle\lambda^{1+p^n}\rangle| = p^n - 1 = |(P_g'/(P_g)_2)^\#|$. *If* $p^n \equiv 2 \pmod 3$, then $3 \nmid (p^n - 1)$ so $(p^n - 1, p^n + 2) = 1$, $(p^{2n} - 1, p^n + 2) = 1$, $|\langle\lambda^{2+p^n}\rangle| = p^{2n} - 1 = |(P_g)_2^\#|$, and $\langle\xi\rangle$ is transitive on $(P_g)_2^\#$. So in every case $\langle\xi\rangle I$ is transitive on $P_g - P_g'$ and $P_g' - (P_g)_2$; if $p^n \equiv 2 \pmod 3$, $\langle\xi\rangle I$ is transitive on $(P_g)_2^\#$ and hence has only three orbits on $P_g^\#$.

4. The case when N is a p-group of class 2.

Theorem 4.1. *Let $N = P$ be a finite class 2 p-group, A a solvable automorphism group of P acting with only three orbits on $P^\#$. Then we have one of the following:*

(1) *$P = K \times L$, L an elementary abelian p-group, K a nonabelian p-group of Theorem* 0.1.

(2) *$\Phi(P) = P' = Z(P)$, so P is special. If p is odd, then P has exponent p, unless*

(3) *$|P| \leq p^6$ if $p > 3$ and $|P| \leq 3^{12}$ if $p = 3$.*

All groups in (1), *and some groups in* (2) *and* (3) *occur.*

The proof of Theorem 4.1 consists of Lemmas 4.2–4.7.

Lemma 4.2. *Let A and P be as in Theorem* 4.1, *with $P' < Z(P)$. Then P is a group of Theorem* 4.1(1).

Proof. The three orbits of A on $P^{\#}$ must be $P - Z(P)$, $Z(P) - P'$ and $(P')^{\#}$. We consider four cases, depending on whether $Z(P)$ has exponent p or p^2 and whether $\Phi(P)$ is P' or $Z(P)$.

If $\Phi(P) = Z(P)$ has exponent p^2, then P has exponent p^3. The main result of [10] tells us that we may assume $p = 2$. A Hall $2'$-subgroup of A will then be transitive on $(P')^{\#}$, the full set of elements of order 2 in P. The first paragraph on p. 15 of [9] shows that P is an S.I. group as defined in [9]. The main theorem of [9] then shows P is a Suzuki 2-group, a contradiction as all Suzuki 2-groups are shown in [5] to have exponent 4.

If $\Phi(P) = P'$ and $Z(P)$ has exponent p^2, we find a Hall p'-subgroup H of A transitive on $(P')^{\#}$, $(Z(P)/P')^{\#}$ and $(P/Z(P))^{\#}$. $Z(P)/P'$ is an H-invariant subspace of P/P', so $P/P' = Z(P)/P' \times K/P'$, K an H-invariant subgroup of P. K/P' must be H-isomorphic to $(P/P')/(Z(P)/P') \cong P/Z(P)$, so H is transitive on $(K/P')^{\#}$. $P = KZ(P)$ so $P' = K'$, and K must be a nonabelian p-group of Theorem 0.1. (This is true because the proof of [2] applies to any K with a p'-automorphism group transitive on $(K/K')^{\#}$ and $(K')^{\#}$.) Fix an $x \in K - K'$. If p is odd, then x has order p, but there is a $z \in Z(P)$ with xz of order p^2; A cannot be transitive on $P - Z(P)$, the desired contradiction. If $p = 2$, then x has order 4. But $\mho^1(Z(P)) = P' = \mho^1(K)$, so there is $z \in Z(P)$ with $z^2 = x^2$. Then $(xz^{-1})^2 = x^2z^{-2} = 1$ and xz^{-1} has order 2; A cannot be transitive on $P - Z(P)$, the desired contradiction.

Suppose $\Phi(P) = Z(P)$ has exponent p. Since P has class 2, the identity $(xy)^p = x^p y^p [y, x]^{p(p-1)/2}$ holds in P. If $p > 2$, this means $(xy)^p = x^p y^p$ and $L = \mho^1(P)$ is a subgroup of P such that $LP' = Z(P)$. If $L \cap P' \neq 1$, then $L^* = \{x \in P \mid x^p \in P'\}$ is a characteristic subgroup of P satisfying $Z(P) < L^* < P$, a contradiction; so $Z(P) = L \times P'$. Now $(P')^{\#}$, $L^{\#}$, $Z(P) - P' - L$ and $P - Z(P)$ are characteristic subsets of $P^{\#}$ and A cannot have only three orbits on $P^{\#}$, the desired contradiction. If $p = 2$, again denote $L^* = \{x \in P \mid x^2 \in P'\}$, a characteristic subgroup obviously satisfying $Z(P) \leq L^* < P$. A is transitive on $P - Z(P)$, forcing $L^* = Z(P)$. Transitivity of A on $P - Z(P)$, $Z(P) - P'$, and $(P')^{\#}$ now means that $(P')^{\#}$ contains no squares, all elements of $Z(P) - P'$ are squares, and all elements of $P - Z(P)$ have order 4. Denote $|P'| = 2^l$, $|Z(P)| = 2^{l+m}$, $|P| = 2^{l+m+n}$. Each element of $Z(P) - P'$ must be the square of k elements for the same fixed integer k. Since $(xz)^2 = x^2$ for all $x \in P$, $z \in Z(P)$, we have

$k = 2^{l+m}k_1$, some integer k_1. We must have $|P - Z(P)| = k \cdot |Z(P) - P'|$, so

$$2^{l+m+n} - 2^{l+m} = 2^{l+m}k_1(2^{l+m} - 2^l)$$

and $2^n - 1 = k_1(2^{l+m} - 2^l)$, a contradiction.

The last three paragraphs have proved that $\Phi(P) = P'$ and $Z(P)$ has exponent p. We again find a Hall p'-subgroup H of A transitive on $(P/Z(P))^{\#}$, $(Z(P)/P')^{\#}$ and $(P')^{\#}$. Maschke's theorem shows $P/P' = Z(P)/P' \times K/P'$, K an H-invariant subgroup of P. $P = KZ(P)$, so $P' = K'$. $K/K' \cong P/Z(P)$ as H-modules, so H is transitive on $(K/K')^{\#}$ and $(K')^{\#}$. The proof of [2] shows that K is one of the nonabelian p-groups of Theorem 0.1. P' is an H-invariant subgroup of $Z(P)$, so $Z(P) = P' \times L$, L H-invariant. $L \cong Z(P)/P'$ as H-modules, so H is transitive on $L^{\#}$. $K \cap Z(P) = P'$, so $K \cap L = 1$ and $P = K \times L$. P is the group of Theorem 4.1(1).

We now must show all groups of Theorem 4.1(1) occur. Let $B = \{\alpha \in \mathrm{Aut}(P) | \alpha$ is trivial on $P/P'\}$; B is a normal p-subgroup of $\mathrm{Aut}(P)$. Also let $C = \{\alpha \in \mathrm{Aut}(P) | \alpha = 1$ on L and $\alpha(x) \in xL$ for all $x \in K\}$, and let D be a solvable automorphism group of K transitive on $K - K'$ and $(K')^{\#}$, E a solvable automorphism group of L transitive on $L^{\#}$. An easy counting argument shows that $|C| = |L|^t$ where $p^t = |K/K'|$, so C and BC are p-groups. $D \times E$ is naturally an automorphism group of $K \times L$; we claim that $D \times E$ normalizes C. Choose $\gamma \in C$, $(\delta, \epsilon) \in D \times E$, $x \in K$, $y \in L$. Then

$$(\delta, \epsilon)^{-1}\gamma(\delta, \epsilon) \cdot y = ((\delta^{-1}, \epsilon^{-1})\gamma)(\epsilon(y)) = (\delta^{-1}, \epsilon^{-1})(\gamma(\epsilon(y)))$$
$$= (\delta^{-1}, \epsilon^{-1})(\epsilon(y)) = \epsilon^{-1}(\epsilon(y)) = y$$

and

$$(\delta, \epsilon)^{-1}\gamma(\delta, \epsilon) \cdot x = ((\delta^{-1}, \epsilon^{-1})\gamma)(\delta(x)) = (\delta^{-1}, \epsilon^{-1})(\delta(x)l^*)$$
$$= \delta^{-1}(\delta(x)) \cdot \epsilon^{-1}(l^*) = x \cdot \epsilon^{-1}(l^*) \in xL$$

(where $l^* \in L$), proving the claim.

$A = BC(D \times E)$ is a solvable automorphism group of P. The orbits of $D \times E$ on $P^{\#}$ are obviously $1 \times L^{\#}$, $(K')^{\#} \times 1$, $(K')^{\#} \times L^{\#}$, $(K - K') \times 1$, $(K - K')^{\#} \times L^{\#}$. Using elements of B we see that $[(K')^{\#} \times L^{\#}] \cup [1 \times L^{\#}] = Z(P) - P'$ is a single orbit of A, and using elements of C we see that $[(K - K') \times L^{\#}] \cup [(K - K') \times 1] = P - Z(P)$ is a single orbit of A. This completes the proof of Lemma 4.2.

Lemma 4.3. *Let A and P be as in Theorem 4.1, with $P' = Z(P)$. Then P is special (i.e., $\Phi(P) = P' = Z(P)$).*

Proof. If the lemma is false then $1 < P' = Z(P) < \Phi(P) < P$, so there is a pth power in P which is not central, say $x, y \in P$ with $[x, y^p] \neq 1$. Since P has class 2, $[x, y^p] = [x, y]^p$, and we find that P' does not have exponent p. This contradicts the fact A is transitive on $(P')^{\#}$.

Lemma 4.4. *Let A and P be as in Theorem 4.1, with A transitive on $P - P'$, P special and p odd. Then P has exponent p.*

Proof. Suppose not. We can find a Hall p'-subgroup H of A transitive on P/P'. $\mho^1(P)$ is a group, since p is odd and P has class 2. If $\mho^1(P) = P'$, then the fact H is transitive on $(P/P')^{\#}$ implies H is also transitive on $(P')^{\#}$ (because $x^b = y$ implies $(x^p)^b = (y^p)^b$, all $x, y \in P$, $b \in H$). The proof of [2] shows P is a nonabelian p-group of Theorem 0.1. For p odd those are all of exponent p, so Lemma 4.4 holds in this case.

Therefore we may assume $\mho^1(P) < P'$. A must be transitive on $\mho^1(P)^{\#}$, $P - P'$ and $P' - \mho^1(P)$. We use a (rather awkward) counting argument to show P cannot exist. $x \to x^p$ is a homomorphism onto $\mho^1(P)$ with kernel $\Omega_1(P)$, so $P/\Omega_1(P) \cong \mho^1(P)$. $[x, y]^p = [x, y^p] = 1$ for any $x, y \in P$ since $\mho^1(P) \leq P'$; this implies P' has exponent p and $\Omega_1(P) = P'$.

Let $|P/P'| = p^a$, and $|P'/\mho^1(P)| = p^b$, so $|\mho^1(P)| = p^a$ and $|P| = p^{2a+b}$. Temporarily fix $x \in P - P'$, and denote $C_P^*(x) = \{y \in P \mid [x, y] \in \mho^1(P)\}$, $S_x = \{[x, y] \mid y \in C_P^*(x)\}$, $T_x = \{[x, y] \mid y \in P\}$, $|C_P^*(x) : C_P(x)| = p^{a_0} = |S_x|$, $|T_x| = p^t = |P : C_P(x)|$. Here $C_P^*(x)$, S_x and T_x are obviously all groups, and $y \to [x, y]$ is a homomorphism inducing isomorphisms $C_P^*(x)/C_P(x) \cong S_x$, $P/C_P(x) \cong T_x$. Note that for any $z \in P'$, $C_P(x) = C_P(xz)$, $C_P^*(x) = C_P^*(xz)$, $T_x = T_{xz}$, $S_x = S_{xz}$.

Since A is transitive on $P' - \mho^1(P)$, $P' - \mho^1(P)$ consists of commutators and we have $P' - \mho^1(P) = \bigcup_{x \in P - P'} (T_x - S_x)$. Assume $w \in P' - \mho^1(P)$ lies in $T_x - S_x$ for k different values of $x \in P - P'$; k is independent of the choice of w. Since $T_x - S_x = T_{xz} - S_{xz}$ for all $x \in P - P'$, $z \in P'$ we have $|P'| = p^{a+b}$ a divisor of k, say $k = p^{a+b} k_1$. The union shows that $k|P' - \mho^1(P)| = |P - P'| \cdot |T_x - S_x|$, so

$$p^{a+b} k_1 (p^{a+b} - p^a) = (p^{2a+b} - p^{a+b})(p^t - p^{a_0}),$$

implying that p^a divides $p^t - p^{a_0}$. This is impossible since

$$p^{a_0} < p^t = |P : C_P(x)| < |P : P'| = p^a.$$

Lemma 4.5. *Let A and P be as in Theorem 4.1, with A transitive on $(P')^{\#}$, P special and p odd. Then either P has exponent p, or $\mho^1(P) = P' < \Omega_1(P)$.*

Proof. $\Phi(P) = P'$, so $\mho^1(P) \leq P'$. If $\mho^1(P) \neq P'$, then transitivity of A on $(P')^{\#}$ implies $\mho^1(P) = 1$, P has exponent p. We may therefore assume $\mho^1(P) = P'$. $\Omega_1(P)$ is a characteristic subgroup with $P' \leq \Omega_1(P) < P$; $P' = \Omega_1(P)$ would contradict the main theorem of [10].

Lemma 4.6. *Let A and P be as in Lemma 4.5, with $\mho^1(P) = P' < \Omega_1(P)$. If $\Omega_1(P)$ is abelian, then P does not exist, except under the conditions of Theorem 4.1(3).*

Proof. Here the orbits of A on $P^{\#}$ are $P - \Omega_1(P)$, $\Omega_1(P) - P'$ and $(P')^{\#}$. We can find a Hall p'-subgroup H of A transitive on $(P/\Omega_1(P))^{\#}$, $(\Omega_1(P)/P')^{\#}$ and $(P')^{\#}$, and then an H-invariant subgroup K with $P/P' = \Omega_1(P)/P' \times K/P'$, H transitive on $(K/P')^{\#}$. The facts $K' \leq P'$ and H transitive on $(P')^{\#}$ imply that $K' = P'$ or $K' = 1$. $K' = P'$ would make K a nonabelian p-group of Theorem 0.1 with p odd and exponent p^2; no such groups exist, so $K' = 1$ and K is abelian. $P = K\Omega_1(P)$, so $\mho^1(K) = \mho^1(P) = P'$. Transitivity of H on $(K/\Omega_1(K))^{\#}$ and $\mho^1(K)^{\#}$ implies that K is homocyclic of exponent p^2.

Maschke's theorem also enables us to conclude that $\Omega_1(P) = P' \times L$, L H-invariant, H transitive on $L^{\#}$. We have $P = KL$, $K \lhd P$, $K \cap L = 1$. Suppose $h \in H$ acts trivially on K/P'. Then h is trivial on K, and for any $x \in K$, $y \in L$ we have

$$[x, y] = [x, y]^h = [x^h, y^h] = [x, y^h],$$

so

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

Thus $y^h y^{-1} \in C_L(K) \leq Z(P)$; but $L \cap Z(P) = 1$, so $y^h y^{-1} = 1$, $y^h = y$, $h = 1$. We conclude that H acts faithfully on K/P'. The map $x \longrightarrow x^p$ is an H-isomorphism between K/P' and P'.

Suppose first that H acts on K/P' as a group of semilinear transformations, and denote $|K| = p^{2m}$, $|L| = p^n$. Then there is $\langle \xi \rangle \lhd H$ with $|\langle \xi \rangle|$ dividing $p^m - 1$ and $(p^m - 1)/(m, p^m - 1)$ dividing $|\langle \xi \rangle|$. H is a primitive linear group on K/P', so K/P' is a direct sum of isomorphic irreducible $\langle \xi \rangle$-modules, say of order p^l. Then $|\langle \xi \rangle|$ divides $p^l - 1$. Lemma 1 of [2] implies that $l = m$, except possibly when $m = 2$; in that case $l = 1$ would mean $|H| \leq 2|\langle \xi \rangle| \leq 2(p-1) < p^2 - 1 = |(K/P')^{\#}|$, a contradiction. Therefore in all cases $l = m$ and $\langle \xi \rangle$ is irreducible on K/P'. If λ is one eigenvalue of ξ on K/P', then $|\langle \lambda \rangle| = |\langle \xi \rangle|$; we choose a

conjugate basis $u_0, u_1, \cdots, u_{m-1}$ for $(K/P') \otimes GF(p^m)$ and see that $\{\lambda, \lambda^p, \cdots, \lambda^{p^{m-1}}\}$ is the full set of eigenvalues of ξ on K/P', with $u_i\xi = \lambda^{p^i} u_i$. K/P' is $\langle\xi\rangle$-isomorphic to P', so ξ has the same set of eigenvalues on P'.

H is also a primitive linear group on L, so L is a direct sum of isomorphic irreducible $\langle\xi\rangle$-modules, say of order p^r. If μ is one of the eigenvalues of ξ on L, then $\mu, \mu^p, \cdots, \mu^{p^{r-1}}$ is the full set of eigenvalues of ξ on L. If $v_0, v_1, \cdots, v_{r-1}$ is a conjugate basis for ξ on an irreducible $\langle\xi\rangle$-submodule of L, then $v_i\xi = \mu^{p^i} v_i$. $\xi|_L$ has order $|\langle\mu\rangle|$, a divisor of $|\langle\xi\rangle|$, so $\mu = \lambda^t$ for some integer t. We have

$$[u_i, v_j]\xi = [\lambda^{p^i} u_i, \mu^{p^j} v_j] = \lambda^{p^i}\mu^{p^j}[u_i, v_j],$$

so either $[u_i, v_j] = 0$ or $\lambda^{p^i}\mu^{p^j} \in \{\lambda, \lambda^p, \cdots, \lambda^{p^{m-1}}\}$. $\lambda^{p^i}\mu^{p^j} = \lambda^{p^i + tp^j}$, so the latter condition forces

$$p^i + tp^j \equiv p^k \pmod{|\langle\xi\rangle|}$$

for some k.

If $m \leq 2$, then $|H| \leq 2(p^2 - 1) < p^3 - 1$, so $|L| \leq p^2$ and $|P| \leq p^6$, one of the conditions of Theorem 4.1(3). If $m > 2$ and $r < m$, then by Lemma 1 of [2] there is a prime q, $q \mid (p^m - 1)$ and $q \nmid (p^s - 1)$ for $s < m$. Since $\lambda^{t(p^r-1)} = 1$ and $q \mid |\langle\lambda\rangle|$, we have $q \mid t$. The congruence $p^i + tp^j \equiv p^k \pmod{|\langle\xi\rangle|}$ then yields $p^i \equiv p^k \pmod{q}$ or $q \mid (p^{|k-i|} - 1)$, a contradiction.

So assume $m > 2$ and $r = m$; then $|H| \leq m(p^m - 1) < p^{2r} - 1$, so $\langle\xi\rangle$ is irreducible on L. Since some $[u_i, v_j] \neq 0$, we can choose i_0 with $[u_{i_0}, v_0] \neq 0$ (apply a Galois automorphism of $GF(p^m)$ to $[u_i, v_j] \neq 0$ repeatedly, using the fact the u_i's and v_j's are conjugate bases). Then our congruence becomes

$$p^{i_0} + t \equiv p^{k_0} \pmod{|\langle\xi\rangle|},$$

and $\mu = \lambda^t = \lambda^{p^{k_0} - p^{i_0}}$ is a power of λ^{p-1}. By Hilfssatz II.3.11 of [6], $H|_L$ is a group of semilinear transformations of L. Both the multiplications by powers of μ and the Galois automorphisms of $GF(p^m)$ fix the proper subset $S = \{\gamma \in GF(p^m) \mid \gamma^{(p^m-1)/(p-1)} = 1\}$ of $GF(p^m)^\#$, so H cannot be transitive on $L^\#$, the desired contradiction.

If H does not act on K/P' as a group of semilinear transformations, then [7] shows that $|K/P'| \in \{3^2, 5^2, 7^2, 11^2, 23^2, 3^4\}$; in fact [7] describes the possible

groups H. Since H must be transitive on $L^{\#}$, it is obvious that all possible groups $P = KL$ satisfy the conditions of Theorem 4.1(3).

Lemma 4.7. *Let A and P be as in Lemma 4.5, with $\mathfrak{V}^1(P) = P' < \Omega_1(P)$. If $\Omega_1(P)$ is nonabelian then P does not exist, except under the conditions of Theorem 4.1(3).*

Proof. The first paragraph of the proof of Lemma 4.6 also applies here, showing $P = K\Omega_1(P)$, K homocyclic abelian of exponent p^2 with $\mathfrak{V}^1(K) = P'$. $\Omega_1(P)$ must be one of the nonabelian p-groups of Theorem 0.1. If $\Omega_1(P)$ is the group of Theorem 0.1(vii) then $|P| = p^6$, satisfying Theorem 4.1(3). Otherwise, since p is odd P must be the group of Theorem 0.1(vi), and $|\Omega_1(P)| = p^{3n}$, $|P'| = p^n$, $|K| = p^{2n}$, $|P| = p^{4n}$. Since the conditions of Theorem 4.1(3) apply otherwise, we may assume $n \geq 2$ and if $p = 3$ then $n > 2$. A Hall subgroup H of A can be found fixing K and transitive on $(K/P')^{\#}$, $(\Omega_1(P)/P')^{\#}$ and $(P')^{\#}$. H must act on $\Omega_1(P)/P'$ as a group of semilinear transformations, so there is a cyclic group $\langle \xi \rangle \lhd H$; if we denote $l = |\langle \xi \rangle|$, then l divides $p^{2n} - 1$, $(p^{2n} - 1)/(2n, p^{2n} - 1)$ divides l, and there is $\lambda \in GF(p^{2n})$ with $|\langle \lambda \rangle| = l$. $\lambda, \lambda^p, \cdots, \lambda^{p^{2n-1}}$ are the distinct eigenvalues of ξ on $\Omega_1(P)/P'$, and the proof of [2] shows $\lambda^{1+p^n}, \lambda^{p(1+p^n)}, \cdots, \lambda^{p^{n-1}(1+p^n)}$ are the eigenvalues of ξ on P'. Since $x \to x^p$ induces a $\langle \xi \rangle$-isomorphism from K/P' to P', these are also the eigenvalues of $\langle \xi \rangle$ on K/P'.

We let $v_0, v_1, \cdots, v_{n-1}$ be a conjugate basis of $(K/P') \otimes GF(p^{2n})$ adapted to ξ and $u_0, u_1, \cdots, u_{2n-1}$ a conjugate basis of $(\Omega_1(P)/P') \otimes GF(p^{2n})$ adapted to ξ, so $v_i\xi = \lambda^{p^i(1+p^n)}v_i$ and $u_j\xi = \lambda^{p^j}u_j$. The commutator map $[\ ,\ ]: K/P' \times \Omega_1(P)/P' \to P'$ must satisfy

$$[v_i, u_j]\xi = [\lambda^{p^i(1+p^n)}v_i, \lambda^{p^j}u_j] = \lambda^{p^i(1+p^n)+p^j}[v_i, u_j].$$

The only eigenvalues of ξ on P' have form $\lambda^{p^k(1+p^n)}$ for some k. Since some $[v_i, u_j] \neq 0$, we must have $\lambda^{p^i(1+p^n)+p^j} = \lambda^{p^k(1+p^n)}$ and thus

$$(*) \qquad p^i + p^{i+n} + p^j \equiv p^k + p^{k+n} \pmod{l}.$$

We pause to prove a number-theoretic

Lemma 4.8. *There does not exist an odd prime p, positive integers n, a_1, a_2, a_3, a_4, and signs $e_2, e_3, e_4, e_5 \in \{\pm 1\}$ such that $2n > a_1 > a_2 > a_3 > a_4 > 0$ and $p^{2n} - 1$ divides $2n(p^{a_1} + e_2p^{a_2} + e_3p^{a_3} + e_4p^{a_4} + e_5)$.*

Proof. Denote $m = (2n, p^{2n} - 1)$; the hypothesis implies $n \geq 3$ and

$$m(p^{a_1} + e_2p^{a_2} + e_3p^{a_3} + e_4p^{a_4} + e_5) = t(p^{2n} - 1)$$

for some integer t, $0 < t < m$. Thus $t + e_5m \equiv 0 \pmod{p^{a_4}}$, forcing $p^{a_4} < 2m$. Denoting $t + e_5m = p^{a_4}t_1$ with $0 < |t_1| < m$, we get

$$-p^{a_4}t_1 \equiv m(p^{a_1} + e_2p^{a_2} + e_3p^{a_3} + e_4p^{a_4}) \pmod{p^{2n}}.$$

Dividing by p^{a_4}, this forces $t_1 + e_4m \equiv 0 \pmod{p^{a_3-a_4}}$, so $p^{a_3-a_4} < 2m$. Continuing this process shows $p^{a_2-a_3} < 2m$, $p^{a_1-a_2} < 2m$, $p^{2n-a_1} < 2m$. Therefore $p^{2n} < (2m)^5$.

In particular, $p^{2n} < (2 \cdot 2n)^5 = 2^{10}n^5$. This inequality alone implies

$$p^n \in \{3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 5^3, 5^4, 7^3\};$$

checking the inequality $p^{2n} < (2m)^5$ in these cases shows that actually $p^n \in \{3^3, 3^4, 5^3, 5^4, 7^3\}$. We complete the proof of the lemma in these cases by repeating the argument of the previous paragraph with specific values of p and n, finding that no values of the a_i and e_j ever work.

We now resume the proof of Lemma 4.7. Lemma 4.8 shows that the congruence (*) can never occur when the numbers i, $i + n$, j, k, $k + n$ are all different. If they are not all different, the facts $0 \le i < n$, $0 \le j < 2n$, $0 \le k < n$ imply that one of the following cases must hold.

Case I: $i = k$.

Case II: $j = k$.

Case III: $j = k + n$.

Case IV: $i = j$.

Case V: $i + n = j$.

We consider the congruence (*) in each of these five cases, using the facts $l \mid (p^{2n} - 1)$ and $(p^{2n} - 1) \mid 2nl$.

Case I. If $i = k$, then $i + n = k + n$ and (*) reduces to $p^j \equiv 0 \pmod{l}$, $l \mid p^j$, a contradiction.

We pause to prove a number-theoretic

Lemma 4.9. *There does not exist an odd prime p, positive integers n, a_1, a_2, and signs e_2, $e_3 \in \{\pm 1\}$ such that $2n > a_1 > a_2 > 0$ and $p^{2n} - 1$ divides $2n(p^{a_1} + e_2p^{a_2} + e_3)$.*

Proof. If $m = (2n, p^{2n} - 1)$, then we have $m(p^{a_1} + e_2p^{a_2} + e_3) = t(p^{2n} - 1)$ for some $0 < t < m$. As in the proof of Lemma 4.8, we get $p^{2n} < (2m)^3$. $n \ge 2$, so the only solutions of $p^{2n} < (2 \cdot 2n)^3$ are $p^n \in \{3^2, 3^3\}$; $p^n = 3^3$ does not satisfy

$p^{2n} < (2m)^3$, so $p^n = 3^2$. It is easy to check that no solution exists when $p^n = 3^2$.

We now complete the proof of Lemma 4.7.

Case II. Here (*) reduces to

$$p^i + p^{i+n} - p^{k+n} \equiv 0 \pmod{l},$$

impossible by Lemma 4.9 for i, $i+n$, $k+n$ all different. If they are not all different, $i+n = k+n$ and $l \mid p^i$, a contradiction.

Case III. Here (*) reduces to

$$p^i + p^{i+n} - p^k \equiv 0 \pmod{l},$$

impossible by Lemma 4.9 for i, $i+n$, k all different. If they are not all different, $i = k$ and $l \mid p^{i+n}$, a contradiction.

Case IV. Here (*) reduces to

$$2p^i + p^{i+n} - p^k - p^{k+n} \equiv 0 \pmod{l}.$$

We treat separately the cases $i = k$, $i < k$ and $i > k$. If $i = k$ then $l \mid p^i$, a contradiction. In the other two cases we get a contradiction by imitating the proof of Lemma 4.8.

Case V. Here (*) reduces to

$$p^i + 2p^{i+n} - p^k - p^{k+n} \equiv 0 \pmod{l}.$$

We get a contradiction in the same way as in Case IV.

BIBLIOGRAPHY

1. Larry Dornhoff, *Group representation theory. Part A*, Marcel Dekker, New York, 1971.

2. ———, *On imprimitive solvable rank 3 permutation groups*, Illinois J. Math. 14 (1970), 692–707. MR 42 #6090.

3. D. A. Foulser, *Solvable primitive permutation groups of low rank*, Trans. Amer. Math. Soc. 143 (1969), 1–54. MR 41 #1852.

4. Daniel Gorenstein, *Finite groups*, Harper and Row, New York, 1968. MR 38 #229.

5. Graham Higman, *Suzuki 2-groups*, Illinois J. Math. 7 (1963), 79–96. MR 26 #1365.

6. B. Huppert, *Endliche Gruppen*. I, Die Grundlehren der math. Wissenschaften, Band 134, Springer-Verlag, Berlin and New York, 1967. MR 37 #302.

7. ———, *Zweifach transitive, auflösbare Permutationsgruppen*, Math. Z. 68 (1957), 126–150. MR 20 #904.

8. W. R. Scott, *Group theory*, Prentice-Hall, Englewood Cliffs, N. J., 1964. MR 29 #4785.

9. David L. Shaw, *The Sylow 2-subgroups of finite, soluble groups with a single*

class of involutions, J. Algebra 16 (1970), 14–26. MR 42 #3179.

10. Ernest Shult, *The solution of Boen's problem*, Bull. Amer. Math. Soc. 74 (1968), 268–270. MR 37 #314.

11. D. R. Taunt, *On A-groups*, Proc. Cambridge Philos. Soc. 45 (1949), 24–42. MR 10, 351.

12. Helmut Wielandt, *Finite permutation groups*, Lectures, University of Tübingen, 1954/55; English transl., Academic Press, New York, 1964. MR 32 #1252.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS, URBANA, ILLINOIS 61801