

AUTOMORPHISM ORBITS OF FINITE GROUPS

THOMAS J. LAFFEY and DESMOND MacHALE

(Received 1 February 1984; revised 12 November 1984)

Communicated by D. E. Taylor

Abstract

Let G be a finite group and let $\text{Aut}(G)$ be its automorphism group. Then G is called a k -orbit group if G has k orbits (equivalence classes) under the action of $\text{Aut}(G)$. (For $g, h \in G$, we have $g \sim h$ if $g^\alpha = h$ for some $\alpha \in \text{Aut}(G)$.) It is shown that if G is a k -orbit group, then $k \leq |G|/p + 1$, where p is the least prime dividing the order of G . The 3-orbit groups which are not of prime-power order are classified. It is shown that A_5 is the only insoluble 4-orbit group, and a structure theorem is proved about soluble 4-orbit groups.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 20 F 28; secondary 20 E 36.

Let G be a finite group and let $\text{Aut}(G)$ be its automorphism group. Then G is partitioned into equivalence classes under the action of $\text{Aut}(G)$ —we say that g, h are equivalent if $g^\alpha = h$ for some $\alpha \in \text{Aut}(G)$. The equivalence classes are called *automorphism orbits*. We call G a k -orbit group if it has k automorphism orbits. The identity constitutes the only 1-orbit group, and it is easy to see that the (finite) 2-orbit groups are precisely the elementary abelian groups of prime-power order. In this paper, we prove that if G is a k -orbit group, then $k \leq 1 + |G|/p$ where p is the least prime divisor of $|G|$. We also completely classify the 3-orbit groups which are not of prime-power order and the insoluble 4-orbit groups. We also prove a structure theorem about 4-orbit groups which are not of prime-power order.

NOTATION. The notation is standard (compare Huppert [1]) with the following additions: $\pi(G)$ denotes the set of prime divisors of $|G|$, $\text{Syl}_p(G)$ denotes the set of Sylow p -subgroups of G , and $N \text{ char } G$ denotes that N is a characteristic subgroup of G .

We begin with

THEOREM 1. *Let G be a finite non-abelian group and let p be the least prime dividing $|G|$. Then G has at most $|G|/p$ automorphism orbits.*

PROOF. Let r be the number of conjugacy classes of G and k the number of automorphism orbits. Then $k \leq r$. Also G has r irreducible complex characters of which $|G/G'|$ are linear and the rest have degree at least p . Hence

$$|G| \geq |G/G'| + (r - |G/G'|)p^2$$

(since the squares of the degrees of the characters all equal $|G|$). Hence

$$r \leq \frac{1}{p^2} [|G| + (p^2 - 1)|G/G'|].$$

If $|G'| > p$, then $r \leq p^{-2}[|G| + (p - 1)|G|] = |G|/p$, which proves the result. Hence we may assume that $|G'| = p$. In particular, $G' \leq Z(G)$. If A is an abelian direct factor of G , say $G = A \times B$, then G has at most $|A|m$ automorphism orbits, where m is the number of automorphism orbits of B . Hence, by induction, we may assume that G has no abelian direct factors, and hence that G is indecomposable.

So we now have: G is an indecomposable p -group, and $|G'| = p$. Let G/G' have type (r_1, \dots, r_m) , i.e. let G/G' be a direct product of r_1 cyclic groups of order p , r_2 of order p^2, \dots, r_m of order p^m . Let $Z_i = \Omega_i(Z(G)) = \{z \in Z(G) \mid z^{p^i} = 1\}$. Theorem 1 of Sanders [2] states that the group $C(G)$ of central automorphisms of G has order $\prod_{i=1}^m |Z_i|^{r_i}$. Hence $|C(G)| \geq \prod_{i=1}^m |Z_i|^{r_i} = |Z_1|^d$, where $d = r_1 + \dots + r_m$ is the minimal number of generators of G/G' and hence of G .

We call an element $g \in G$ *small* if

$$|\{g^\sigma \mid \sigma \in C(G)\}| < |Z_1|,$$

and we call g *nearly small* if

$$|\{g^\sigma \mid \sigma \in C(G)\}| \leq |Z_1|.$$

Let S be the subgroup generated by the small elements. Suppose first that $S = G$. Let $\{s_1, \dots, s_d\}$ be a set of small elements which generate G . Let b be the d -tuple (s_1, \dots, s_d) and, for $\sigma \in C(G)$, let $b^\sigma = (s_1^\sigma, \dots, s_d^\sigma)$. Note that for $\sigma, \tau \in C(G)$, we have $b^\sigma = b^\tau$ if and only if $\sigma\tau^{-1}$ fixes each one of s_1, \dots, s_d , and thus if and only if $\sigma = \tau$, since $\{s_1, \dots, s_d\}$ generates G . Hence $|\{b^\sigma \mid \sigma \in C(G)\}| = |C(G)|$. However, since s_i is small, $|\{s_i^\sigma \mid \sigma \in C(G)\}| < |Z_1|$, and hence $|\{b^\sigma \mid \sigma \in C(G)\}| < |Z_1|^d$. This contradicts Sanders' Theorem 1 [2]. Hence $S \neq G$.

Suppose that $|Z_1| \geq p^2$. Then we have

$$\begin{aligned} k &\leq |Z(G)| + \frac{1}{p}|S - Z(G)| + \frac{1}{p^2}|G - S| \\ &\leq |G| \left[\frac{1}{p^2} + \frac{1}{p} \cdot \frac{p-1}{p^2} + \frac{p-1}{p^3} \right] \\ &= |G| \left[\frac{3p-2}{p^3} \right] \\ &\leq |G|/p. \end{aligned}$$

Hence we may assume that $|Z_1| = p$, and thus that $Z(G)$ is cyclic.

Suppose next that G/G' is not elementary abelian. Let T be the subgroup generated by the nearly small elements of G . Arguing as above, we find that $|C(G)| \leq |Z_1|^d$, and this contradicts Sanders' theorem unless $Z(G) = Z_1$. Hence $|Z(G)| > p$ implies that $T \neq G$, and then we obtain as above, that

$$k \leq |Z(G)| + \frac{1}{p}|T - Z(G)| + \frac{1}{p^2}|G - T| \leq |G|/p.$$

Hence we may assume that $|Z(G)| = p$. But $|G'| = p$ implies that $[x, y]^p = 1$ for all $x, y \in G$, and thus that $[x, y^p] = 1$, whence $y^p \in Z(G)$. Hence $\Phi(G) \leq Z(G) = G'$, and G/G' is elementary abelian.

So the proof is reduced to a consideration of the following situation: G/G' is elementary abelian and $Z(G)$ is cyclic. Suppose that M is a maximal subgroup of G and that $G = MZ(G)$. Let $\sigma \in \text{Aut}(M)$ and let $\sigma_0 \in \text{Aut}(Z(G))$ be such that $\sigma_0|_{Z(G) \cap M} = \sigma|_{Z(G) \cap M}$. Extend σ_0 to G by setting $\sigma_0(m) = \sigma(m)$ for all $m \in M$, and by making σ_0 multiplicative. Then $\sigma_0 \in \text{Aut}(G)$, and so the theorem holds for G if it holds for M . Hence we may assume that $M = G$, and thus that $Z(G) = \Phi(G)$ has order p . But then G is an extraspecial p -group. So $\text{Aut}(G)$ is known (Winter [4]). Suppose $|G| = p^{2n+1}$. Then $Z(G)$ is composed of two automorphism orbits (by the Theorem of [4]), and each $g \in G \setminus Z(G)$ is conjugate to gz for all $z \in Z(G)$. Hence the number of automorphism orbits of G is at most $2 + p^{-1}(p^{2n+1} - p) = p^{2n} + 1$ with equality if and only if elements in distinct cosets of $Z(G)$ belong to distinct automorphism orbits. However, by [4, (3c), page 161], the automorphisms of G which act trivially on $G/Z(G)$ are precisely the group of inner automorphisms. Since G has an outer automorphism we conclude that there exist $g_1, g_2 \in G$ such that $g_1Z(G) \neq g_2Z(G)$, but such that g_1, g_2 lie in the same automorphism orbit. (We remark here that $\text{Aut}(G)$ does not transitively permute the non-trivial elements of $G/Z(G)$ in the case where G has exponent p^2 ($p > 2$) by the Theorem of [4].) Hence G has at most $p^{2n} = |G|/p$ automorphism orbits, and the proof is complete.

COROLLARY. *Let $G \neq 1$ be a finite group. Then G has at most $1 + |G|/p$ automorphism orbits, where p is the least prime dividing $|G|$.*

PROOF. Using Theorem 1, we may assume that G is abelian. Thus G is the direct product of cyclic groups of prime power orders. Since the cyclic group $C(q^k)$ of prime power order q^k has exactly $k + 1$ automorphism orbits, and since the direct product of r copies of $C(q^k)$ also has exactly $k + 1$ automorphism orbits, the result follows immediately except in the case $G = \mathbf{Z}_2 \times \mathbf{Z}_4$. But in this case, G has only 4 automorphism orbits. This completes the proof.

REMARK. We note that the bound in Theorem 1 is attained by the dihedral group of order 8.

We now consider 3-orbit groups.

THEOREM 2. *Let G be a finite group which is not of prime-power order. The following are equivalent:*

- (1) G is a 3-orbit group;
- (2) $|G| = p^n q$, and G has a normal elementary abelian Sylow p -subgroup P , for some primes p, q , and for some integer $n \geq 1$. Furthermore, p is a primitive root mod q (i.e. $q - 1$ is the least natural number e with $p^e \equiv 1 \pmod{q}$). Let Q be a Sylow q -subgroup of G . Then P , regarded as a $\text{GF}(p)[Q]$ -module, is a direct sum of $t \geq 1$ copies of the (unique) irreducible $\text{GF}(p)[Q]$ -module of dimension $q - 1$. In particular $|P| = p^{t(q-1)}$.

PROOF. (1) Assume that G is a 3-orbit group and that G is not of prime-power order. Then $|G| = p^a q^b$ for some primes p, q and integers $a \geq 1, b \geq 1$. So G is soluble. We may thus assume that $O_p(G) \neq 1$. Since $O_p(G) \text{ char } G$, and since G is a 3-orbit group, we thus find that $P = O_p(G)$ is a Sylow p -subgroup of G . Also, since $\Omega_1(Z(P)) \text{ char } G$, P is elementary abelian. Let $Q \in \text{Syl}_q(G)$. Since G is a 3-orbit group, it has no element of order pq . Hence Q acts fixed-point-freely on P , so that Q is cyclic, or $q = 2$ and Q is (generalized) quaternion [1, V(8.15)]. Since Q must have exponent q , we thus obtain $|Q| = q$.

We now regard P as a $\text{GF}(p)[Q]$ -module. We write the operation in P as addition and the action of Q (by conjugation) as multiplication. By Maschke's theorem, $P = P_1 \oplus \cdots \oplus P_r$, where the P_i are irreducible $\text{GF}(p)[Q]$ -modules. Also by Huppert [1, II(3.10), page 166], $|P_i| = p^e$, where e is the order of $p \pmod{q}$ (i.e. e is the least natural number with $p^e \equiv 1 \pmod{q}$). If $Q = \langle \alpha \rangle$, we may choose a basis for P_i so that α is represented by the companion matrix of its

minimal polynomial $m_i(\lambda)$ on P_i . Hence P_i is determined up to $\text{GF}(p)[Q]$ -isomorphism by the minimal polynomial $m_i(\lambda)$ of α on P_i . We now claim that P_1, \dots, P_r are all isomorphic modules. For suppose that P_1 is not isomorphic to P_2 . Then $m_1(\lambda) \neq m_2(\lambda)$. Let $0 \neq u_i \in P_i$ ($i = 1, 2$). Since G is a 3-orbit group, there exists $\sigma \in \text{Aut}(G)$ with $u_1^\sigma = u_1 + u_2$. Now $\alpha^{\sigma^{-1}} = \alpha^k w$ for some $w \in P$, and for some $k \geq 1$ with $(k, q) = 1$. Let $g(\lambda)$ be the minimal polynomial of α^k on P_1 . Note that $\deg g = p^e$. Consider

$$\begin{aligned} u_1^\sigma g(\alpha) &= u_1^\sigma (g(\alpha^{\sigma^{-1}}))^\sigma \\ &= u_1^\sigma (g(\alpha^k))^\sigma && \text{(since } P \text{ is abelian)} \\ &= [u_1 g(\alpha^k)]^\sigma = 0. \end{aligned}$$

Hence $(u_1 + u_2)g(\alpha) = 0$. But the minimal polynomial of α on $u_1 + u_2$ is $m_1(\lambda)m_2(\lambda)$ (since $m_1 \neq m_2$ implies $(m_1, m_2) = 1$). Since $\deg g = \deg m_i$, we have a contradiction. So all the P_i are isomorphic $\text{GF}(p)[Q]$ -modules.

Next, for any i with $(i, q) = 1$, there exists $\tau \in \text{Aut}(G)$ with $\alpha^\tau = \alpha^i$. Let $0 \neq u \in P$. Then the minimal polynomial $m(\alpha)$ such that $um(\alpha) = 0$ is also the minimal polynomial of α on P . But

$$0 = um(\alpha) = [um(\alpha)]^\tau = u^\tau m(\alpha^\tau) = u^\tau m(\alpha^i) \quad \text{(since } P \text{ is abelian).}$$

Hence $m(\alpha^i) = 0$, and thus $m(\lambda)$ divides $m(\lambda^i)$ ($i = 1, 2, \dots, q - 1$). Hence, if w is a root of $m(x)$ in the algebraic closure of $\text{GF}(p)$, so also is w^i . Therefore $m(\lambda)$ is divisible by the cyclotomic polynomial $\Phi_{q-1}(\lambda)$. Hence $e \geq q - 1$, so that $e = q - 1$, and the result follows.

(2) Assume that G satisfies (2). Then Q has no fixed point on P , so G has elements of order 1, p , q only. We first show that any two elements of order p are conjugate. Note that P is a homogeneous $\text{GF}(p)[Q]$ -module, so if $0 \neq u \in P$, then $P_0 = \{uf(\alpha) \mid f(x) \in \text{GF}(p)[x]\}$ is an irreducible $\text{GF}(p)[Q]$ -submodule of order p^{q-1} (using the same notation as above). Let $0 \neq v \in P$ and let $P_1 = \{vf(\alpha) \mid f(x) \in \text{GF}(p)[x]\}$. If $P_0 = P_1$, then we can write $P = P_0 \oplus P_2$ as $\text{GF}(p)[Q]$ -modules. But then a routine calculation shows that the map σ defined by $\alpha^\sigma = \alpha$, $u^\sigma = v$, and $w^\sigma = w$ ($w \in P_2$) extends to an automorphism of G .

If $P_0 \neq P_1$, then we may write $P = P_0 \oplus P_1 \oplus P_2$ as $\text{GF}(p)[Q]$ -modules. Again a routine calculation shows that the map τ defined by $\alpha^\tau = \alpha$, $u^\tau = v$, $v^\tau = u$, and $w^\tau = w$ ($w \in P_2$) extends to an automorphism τ of G .

We must now show that the elements of order q form a single orbit under $\text{Aut}(G)$. Since P transitively permutes the Sylow q -subgroups it suffices, by Sylow's theorem, to show that, for all i with $1 \leq i \leq q - 1$, there exists $\theta \in \text{Aut}(G)$ with $\alpha^\theta = \alpha^i$.

Let $P = P_1 \oplus \cdots \oplus P_t$ as irreducible $\text{GF}(p)[Q]$ -modules and let $0 \neq u_j \in P_j$. Then each $u \in P_j$ is uniquely expressible as $u_j f(\alpha)$ for some $f(\lambda) \in \text{GF}(p)[\lambda]$ with $\deg f < q - 1$. Define a map θ by $\alpha^\theta = \alpha^i$, $u_j^\theta = u_j$, and $(u_j f(\alpha))^\theta = u_j f(\alpha^i)$.

Note that if $0 \neq u \in P$ is such that $ug(\alpha) = 0$ for some $g(x) \in \text{GF}(p)[x]$, then $\Phi_{q-1}(\lambda)$ divides $g(\lambda)$, and hence it also divides $g(\lambda^i)$. So $ug(\alpha^i) = 0$. This proves that the natural extension of θ to P is well defined. Thus, by a routine calculation, we see that θ extends to an automorphism of G . This proves that G is a 3-orbit group, and so the proof of the theorem is complete.

We next consider 4-orbit groups.

THEOREM 3. *Let G be an insoluble 4-orbit group. Then $G \cong A_5$.*

PROOF. Since G is insoluble, it follows that $|\pi(G)| \geq 3$, and hence, since G is a 4-orbit group, that $|\pi(G)| = 3$. By the Feit-Thompson theorem, $|G|$ is even. So we may write $\pi(G) = \{2, p, r\}$. Since G is a 4-orbit group, the only possible orders for elements of G are 1, 2, p , r . In particular, G has an elementary abelian Sylow 2-subgroup. Let N be a minimal characteristic subgroup of G . Then N is the direct product of isomorphic simple groups. Also G/N is at most a 3-orbit group. Hence G/N is soluble, and thus N is not soluble. So N is a 4-orbit group. Since $N \text{ char } G$, and since G is a 4-orbit group, we must have $N = G$. Since all elements of $G - \{1\}$ have prime order, N is simple. Hence G is simple.

By Walter’s classification theorem [3], G is one of the following groups:

- (1) $\text{PSL}_2(q)$, $q \equiv \pm 3 \pmod 8$;
- (2) $\text{SL}_2(2^n)$, for some $n \geq 2$;
- (3) a group of Ree type;
- (4) the small Janko group J_1 . For q odd, $\text{PSL}_2(q)$ has cyclic subgroups of order $(q \pm 1)/2$, and thus, since $|\pi(G)| = 3$, we must have $(q \pm 1)/2 = 2$ in case (1). Thus $q = 5$ and $G \cong A_5$. Again $\text{SL}_2(2^n)$ has cyclic subgroups of order $2^n \pm 1$, and so again, since $2^{2n} - 1 \equiv 0 \pmod 3$, we have $2^n - 1 = 3$. This leads in case (2) to $n = 4$ and $G = \text{SL}_2(4) \cong A_5$. Groups which satisfy (3) or (4) have elements of nonprime order, and also their orders are divisible by more than three primes. So (3) and (4) are impossible for G . This proves the theorem.

We now consider the soluble case.

THEOREM 4. *Let G be a finite soluble 4-orbit group which is not of prime-power order. Then $|G| = p^a q^b$, and G has a normal Sylow p -subgroup P for some primes p, q . Let Q be a Sylow q -subgroup of G . Then one of the following holds:*

- (1) Q acts fixed-point-freely on P , $|Q| = q$, and P is a 2-orbit or 3-orbit group;
- (2) P is elementary abelian, and Q is cyclic of order q^2 or quaternion of order 8;
- (3) $G = P \times Q$, where P, Q are elementary abelian.

PROOF. Let $p \in \pi(G)$ be such that $O_p(G) \neq 1$. Suppose first that $|\pi(G)| = 3$. Let $\pi(G) = \{p, q, r\}$ and suppose that $O_q(G/O_p(G)) \neq 1$. Let $Q \in \text{Syl}_q(G)$, and let $R \in \text{Syl}_r(G)$. Let $1 \neq x \in R$ and let $N = QO_p(G)$. Since the only possible orders for elements of G are 1, p , q , r , and since $N \triangleleft G$, it follows that x acts fixed-point-freely on N . So, by Thompson's theorem on fixed-point-free automorphisms of prime order [1, V(8.14)], N is nilpotent. But then G has an element of order pq . This is a contradiction. Hence $|\pi(G)| = 2$.

Let $\pi(G) = \{p, q\}$, let $P \in \text{Syl}_p(G)$, and let $Q \in \text{Syl}_q(G)$. Suppose that P is not normal in G . Then since $\Omega_1(Z(O_p(G)))$ is characteristic in G , and since G is a 4-orbit group, $O_p(G)$ is elementary abelian. Furthermore, $QO_p(G)$ and $G/O_p(G)$ are 3-orbit groups. By Theorem 2, firstly Q is cyclic of order q , and secondly Q is elementary abelian of order $q^{t(p-1)}$ (for some $t \geq 1$) and $|P/O_p(G)| = p$. Hence $t = p - 1 = 1$, so that $p = 2$ and $G/O_p(G)$ is dihedral of order $2q$. The only possible orders for the elements in the four automorphism orbits of G are 1, 2, q , 2 or 1, 2, q , 4. The first possibility implies that P is abelian and hence that $P \leq C_G(O_p(G)) = O_p(G)$. Hence P has exponent 4, and each element of $P - O_p(G)$ has order 4. Now $QO_p(G)$ is characteristic in G , and by the Frattini argument, we have $G = O_p(G)N_G(Q)$. Hence $N_G(Q)$ contains a 2-element $\beta \notin O_2(G)$. Let $Q = \langle \alpha \rangle$. Then $[\alpha, \beta^2] \in Q$, and $1 \neq \beta^2 \in O_2(G)$. Hence $[\alpha, \beta^2] = 1$, and $\alpha\beta^2$ is an element of order $2q$. This is a contradiction. So P is normal in G , as required.

Next, if P is not elementary abelian, then P is a 3-orbit group. Hence every element outside P has order q and acts fixed-point-freely on P . Thus $|Q| = q$. Suppose then that P is elementary abelian. If the automorphism orbits of G are represented by elements of orders 1, p , p , q , then again conclusion (1) holds. Suppose these orders are 1, p , q , q or 1, p , q , q^2 . Then Q acts fixed-point-freely on P , so either Q is cyclic of order q or q^2 , or Q is a (generalized) quaternion group. Since Q has exponent at most q^2 , this implies that if Q is non-cyclic, then Q must be quaternion of order 8.

The only remaining possibility is that G has elements of orders 1, p , q , pq . Then Q is elementary abelian. For each maximal subgroup A of Q , let C_A be the centralizer in P of A . If $O_q(G) \neq 1$, then $O_p(G) \times O_q(G)$ is a characteristic 4-orbit subgroup of G . So it equals G , and (3) holds.

Suppose then that $O_q(G) = 1$, so that Q acts faithfully on P . By Maschke's theorem, P is the direct sum of irreducible $\text{GF}(p)[Q]$ -modules. Let $W \leq P$ be an irreducible $\text{GF}(p)[Q]$ -module. If K is the kernel of Q on W , then Q/K is cyclic, and thus K is a maximal subgroup of Q . Since the set of nonidentity elements of P forms one automorphism orbit, it follows that, for each $1 \neq x \in P$, $C_Q(x)$ has index q in Q . Also, the elements of order q form one automorphism orbit, so that $|C_P(y)| = p^c$ for all $1 \neq y \in Q$ (for some $c \geq 0$ independent of y). Let $|P| = p^a$,

and let $|Q| = q^b$. We now count the number of elements of G of order pq . Note that if $w \in G$ has order pq , then $w = xy$, where x has order p , y has order q , and $xy = yx$; moreover, this representation is unique. Now each $1 \neq y \in Q$ has $|P|/p^c$ conjugates (which belong to distinct Sylow q -subgroups), and y commutes with $p^c - 1$ elements of order p . Hence the number of elements of order pq is

$$(q^b - 1)p^a(p^c - 1)/p^c = p^{a-c}(p^c - 1)(q^b - 1).$$

On the other hand, each $1 \neq x \in P$ commutes with the $|Q|/q = q^{b-1}$ elements of Q . Each of these except for the identity has p^{a-c} conjugates (which belong to distinct Sylow q -subgroups). Hence the number of elements of order pq is

$$(p^a - 1)(q^{b-1} - 1)p^{a-c}.$$

A comparison of the two counts yields

$$(p^c - 1)(q^b - 1) = (p^a - 1)(q^{b-1} - 1).$$

If $b > 1$, we thus have

$$(p^a - 1)/(p^c - 1) = (q^b - 1)/(q^{b-1} - 1) = m, \text{ say.}$$

Now $q - 1 < m < q$, and $p^{a-c} - 1 < m < p^{a-c}$, so that $q - 1 < p^{a-c} < m + 1 < q + 1$. Thus $p^{a-c} = q$, which gives a contradiction. Hence $b = 1$, as asserted. The proof is complete.

References

- [1] B. Huppert, *Endliche Gruppen I* (Springer-Verlag, 1967).
- [2] P. R. Sanders, 'The central automorphisms of a finite group', *J. London Math. Soc.* **44** (1969), 225–228.
- [3] J. Walter, 'The characterization of finite groups with abelian Sylow 2-subgroups', *Ann. of Math.* **89** (1969), 405–514.
- [4] D. Winter, 'The automorphism group of an extraspecial p -group', *Rocky Mountain J. Math.* **2** (1972), 159–168.

Department of Mathematics
University College
Dublin
Ireland

Department of Mathematics
University College
Cork
Ireland