BULL. AUSTRAL. MATH. SOC. 20B05, 20B10
VOL. 13 (1975), 211-240.

On the Sylow subgroups of a doubly transitive permutation group III

Cheryl E. Praeger

Let G be a 2-transitive permutation group of a set Ω of n points and let P be a Sylow p-subgroup of G where p is a prime dividing $|G|$. If we restrict the lengths of the orbits of P, can we correspondingly restrict the order of P? In the previous two papers of this series we were concerned with the case in which all P-orbits have length at most p; in the second paper we looked at Sylow p-subgroups of a two point stabiliser. We showed that either P had order p, or $G \geq A_n$, $G = \mathrm{PSL}(2, 5)$ with $p = 2$, or $G = M_{11}$ of degree 12 with $p = 3$. In this paper we assume that P has a subgroup Q of index p and all orbits of Q have length at most p. We conclude that either P has order at most p^2, or the groups are known; namely $\mathrm{PSL}(3, p) \leq G \leq \mathrm{PGL}(3, p)$, $\mathrm{ASL}(2, p) \leq G \leq \mathrm{AGL}(2, p)$, $G = \mathrm{P\Gamma L}(2, 8)$ with $p = 3$, $G = M_{12}$ with $p = 3$, $G = \mathrm{PGL}(2, 5)$ with $p = 2$, or $G \geq A_n$ with $3p \leq n < 2p^2$; all in their natural representations.

Let G be a doubly transitive permutation group on a set Ω of n points and let P be a Sylow p-subgroup of G where p is a prime dividing $|G|$. The previous two papers [9, 10] were concerned with the situation in which P has no orbit of length greater than p. We showed essentially that either G contains the alternating group or P has order p. The general problem is the following:

Received 21 May 1975.

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

If we impose certain restrictions on the orbit structure of P *, can we restrict the order of* P *?*

The results of [9, 10] deal with the simplest possible structure for P , and I was uncertain whether similar methods could be used to investigate groups whose Sylow subgroups P have a more complicated structure. However it seems that the results can be extended, and they yield an unusual characterisation of the 2-dimensional affine and projective linear groups. (The results are useful in the search for 2-transitive groups; for if G is 2-transitive of some fixed degree then the results give us information about the order and orbit structure of the Sylow subgroups of G .) We prove the following result.

THEOREM. *Let* G *be a doubly transitive permutation group on a set* Ω *of* n *points. Let* p *be a prime dividing* $|G|$ *and let* P *be a Sylow* p*-subgroup of* G *. Suppose that* P *has a subgroup* Q *of index* p *, all of whose orbits have length at most* p *. Then one of the following holds:*

(a) $|P| = p$;

(b) $|P| = p^2$ *, and* P *has an orbit of length* p^2 *unless*

(I) G *is* $\mathrm{PSL}(2, 5)$ *of degree* 6 *and* $p = 2$ *, or*

(II) G *is* M_{11} *in its* 3*-transitive representation of degree* 12 *, and* $p = 3$;

(c) $|P| = p^3$ *and* G *satisfies one of the following:*

(I) $\mathrm{PSL}(3, p) \le G \le \mathrm{PGL}(3, p)$ *, of degree* $1 + p + p^2$ *,*

(II) $\mathrm{ASL}(2, p) \le G \le \mathrm{AGL}(2, p)$ *, of degree* p^2 *,*

(III) $p = 3$ *and* G *is* $\mathrm{P\Gamma L}(2, 8)$ *of degree* 9 *or* G *is* M_{12} *of degree* 12 *,*

(IV) $p = 2$ *and* G *is* $\mathrm{PSL}(2, 5)$ *of degree* 6 ;

(d) $G \supseteq A_n$ *, where* $p \le n < 2p^2$.

Notation. (a) By A_n, S_n, M_n we mean the alternating, symmetric, or Mathieu group of degree n , respectively; $\mathrm{PSL}(m, q)$, $\mathrm{PGL}(m, q)$, $\mathrm{P\Gamma L}(m, q)$

denote respectively the group of projective special linear, general linear, and semilinear transformations of $(m-1)$-dimensional projective space over a field of q elements; similarly $\mathrm{ASL}(m, q)$, and so on, denote the groups of affine transformations.

(b) Most of the notation used for permutation groups is standard and the reader is referred to Wielandt's book [14]. By a long orbit we mean one containing more than one point. If a group G acts on a set Ω then we denote by $\mathrm{fix}_\Omega G$, and $\mathrm{supp}_\Omega G$ the subsets of Ω which are fixed by G , and permuted nontrivially by G , respectively. If the set in question is obvious then we shall often omit the subscript and write simply fix G, supp G .

The group generated by objects, say x, y (which may be elements or subgroups) is denoted by $\langle x, y\rangle$. If X is a group then X^p will denote $\langle x^p \mid x \in X\rangle$. X^p is a characteristic subgroup of X . We mean by $x \sim_G y$ that $x^g = y$ for some g in G , and if the group G is obvious from the context we may write just $x \sim y$. Finally, if x and y are integers then (x, y) denotes the greatest common divisor of x and y .

1.

Let G, P, Q satisfy the conditions of the theorem. If $|P| \geq p^2$ then P has an orbit of length p^2 unless $G \supseteq A_n$, G is $\mathrm{PSL}(2, 5)$ of degree 5 , or G is M_{11} of degree 12 . This follows from the result in [9], since the existence of the subgroup Q means that P has no orbits of length greater than p^2 ; in the second and third cases P has order 4 and 9 respectively. Thus the theorem is true if $|P| \leq p^2$, so we shall assume hereafter that P has order at least p^3 . Also we assume that $G \not\supseteq A_n$. Then P has at least one orbit of length p^2 .

The method of proof will depend both on $|\mathrm{fix}\ P|$ and on conjugation properties of Q . In this section we shall proceed as far as possible without splitting into subcases. In Sections 2 and 3 we consider the case when fix P is nonempty and this is divided into two subcases depending on the fusion of Q ; in Section 2 we characterise $\mathrm{PSL}(3, p)$. In the final Section, 4, we deal with the case $\mathrm{fix}\ P = \emptyset$.

REMARK 1.1. By [10] it follows that Q is not the Sylow p-subgroup of a stabiliser of two points. Hence if $|\mathrm{fix}\ P| \leq 1$, it follows that $\mathrm{fix}\ Q = \mathrm{fix}\ P$.

LEMMA 1.2. *Q is the only subgroup of P of index p such that all long Q-orbits have length p . In particular, Q is weakly closed in P with respect to G ; that is, if $g \in G$ and $Q^g \subset P$ then $Q^g = Q$.*

Proof. Suppose that Q_1, Q_2 are distinct subgroups of P with the property. Then $|P : Q_i| = p$, $|Q_i| \geq p^2$, and $Q_i \trianglelefteq P$. So $P = Q_1Q_2$ and $R = Q_1 \cap Q_2$ has index p^2 in P .

Let Γ be a P-orbit of length p^2 . Suppose that Q_1 has p orbits $\Gamma_1, \ldots, \Gamma_p$ of length p in Γ . Then Q_2 permutes these orbits nontrivially since $P = Q_1Q_2$ is transitive on Γ . It follows that R fixes Γ pointwise. Thus P acts regularly on each long P-orbit, and in particular, P is abelian. Now let Q be any subgroup of P containing R with $|P : Q| = p$. Then Q is not transitive on any P-orbit of length p^2 (since R fixes them all pointwise), and so Q has all long orbits of length p .

Now we shall show that R is weakly closed in P . Define

$$N^* = \langle Q^* \supset R \mid Q^* \text{ is conjugate to one of the groups } Q \text{ such that } R \subset Q \subset P \rangle .$$

Then $N^* \trianglelefteq N(R)$, and $P = \langle Q_1, Q_2 \rangle \subseteq N^*$. Also, since all of these generators Q^* of N^* have the same orbits as R has in $\mathrm{supp}\ R$, it follows that N^* acts on $\mathrm{supp}\ R$ as an elementary abelian p-group with all orbits of length p . Hence N^{*p} fixes $\mathrm{supp}\ R$ pointwise. Now let P^* be any Sylow p-subgroup of G containing R . Since P^* is abelian, $P^* \subseteq N(R)$ and hence $P^* \subseteq N^*$. Hence all P^*-orbits of length p^2 lie in $\mathrm{fix}\ R$ and it follows that R is the kernel of the action of P^* on the union of its orbits of length p^2 .

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

Now if $R^g \subseteq P$ for some g in G, then $R \subseteq P^{g^{-1}}$ and as above, R is the kernel of the action of $P^{g^{-1}}$ on its orbits of length p^2; thus R^g is the kernel of the action of P on its orbits of length p^2, that is, $R^g = R$. Hence R is weakly closed in P.

Hence $N(R)$ is 2-transitive on fix R (see [15], Satz 3). As $N^* \supset P$, N^* acts nontrivially and hence transitively on fix R. Also as N^{*p} is a characteristic subgroup of N^*, it is normal in $N(R)$. Suppose first that N^{*p} is trivial. Then N^* is a p-group containing P; so $N^* = P$. As N^* is transitive on fix R, and as P has an orbit, say Γ, of length p^2 in fix R, it follows that fix $R = \Gamma$ and fix P = fix $Q = \emptyset$ (see Remark 1.1). Since P has orbits of length p (that is, the long orbits of R), clearly p^2 does not divide n. Then for α in fix R, R is a subgroup of index p of a Sylow p-subgroup T of G_α, T is conjugate to some Q satisfying $R \subset Q \subset P$, and hence T has all long orbits of length p, a contradiction to [10].

Thus N^{*p} is a nontrivial normal subgroup of $N(R)$ and so acts transitively on fix R (and N^{*p} fixes supp R pointwise). By a result of Bochert ([12], 52-54), we have $|\text{supp } R| \geq \frac{1}{4}(n-1)$. With this condition, it follows from work of Kantor [6] (and since $G \not\supseteq A_n$) that G satisfies one of the following list; where $c = |\text{supp } R|$:

List 1.3. (a) $\mathrm{PSL}(m, q) \leq G \leq \mathrm{P\Gamma L}(m, q)$ for $m \geq 3$, where $n = (q^m-1)/(q-1)$ and $c = (q^{m-1}-1)/(q-1)$.

(a^1) G is a subgroup of $\mathrm{GL}(4, 2)$ isomorphic to A_7, $n = 15$ and $c = 2^3 - 1 = 7$.

(b) $\mathrm{ASL}(m, q) \leq G \leq \mathrm{A\Gamma L}(m, q)$ for $m \geq 2$, where $n = q^m$, and either $c = q^{m-1}$, or $c = q^{m-2}$ and $q = 2$.

(b^1) G is a semi-direct product of the translation group of the 4-dimensional affine geometry over a field of 2 elements, and a subgroup

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

of GL(4, 2) isomorphic to A_7 ; in the case $n = 16$, $c = 4$.

(c) G is M_n where n is 22, 23 , or 24 , or G is $\mathrm{aut}(M_{22})$, and $c = n - 16$.

Suppose that $G \geq \mathrm{PSL}(m, q)$ (or $G \simeq A_7$). Then $|\mathrm{fix}\ R| = n - c = q^{m-1}$, so $|\mathrm{fix}\ R| - 1 = (q-1)|\mathrm{supp}\ R| \equiv 0 \pmod p$. Hence $n \equiv 1 \pmod p$ and by Remark 1.1, since G is 2-transitive, $|\mathrm{fix}\ P| = |\mathrm{fix}\ Q| = 1$ for all $R \subset Q \subset P$. As P has orbits of length p , then $n - 1$ is not divisible by p^2 . If $\alpha, \beta \in \mathrm{fix}\ R$ then R is a subgroup of index p of a Sylow p-subgroup T of $G_{\alpha\beta}$; T is conjugate to some Q such that $R \subset Q \subset P$ and hence all long orbits of T have length p , contradicting [10].

Next suppose that $G \geq \mathrm{ASL}(m, q)$. Then $|\mathrm{supp}\ R| = c$ is a power of q so p divides q . As P-orbits have length at most p^2 we must have $q = p$, $m = 2$. However a Sylow p-subgroup of ASL(2, p) is nonabelian; contradiction. We deal with case (b^1) similarly.

Finally suppose that $G \geq M_n$, and $c = 8, 7, 6$ as n is 24, 23, 22 respectively. As p divides c we see easily that n is congruent to 0 or 1 mod p . As above, we can show that a Sylow p-subgroup of a two point stabiliser has all orbits of length p , and order at least p^2 contradicting [10]. This completes the proof.

Now let Δ be a long Q-orbit and let R be the pointwise stabiliser of Δ in Q . Then $|Q : R| = p$ so R is normal in Q . We shall consider $N(R)$ and the subgroup N^* defined by

$$N^* = \langle Q^* \supset R \mid Q^* \sim_G Q \rangle .$$

Clearly $N^* \trianglelefteq N(R)$. Since each generator Q^* has the same orbits as R in supp R it is easy to show that N^* acts on supp R as an elementary abelian p-group with all orbits of length p . Then clearly N^{*p} fixes supp R pointwise.

LEMMA 1.4. *Q is a Sylow p-subgroup of N^* . (Hence all generators Q^* of N^* are conjugate in N^* .)*

Proof. If not, then a Sylow p-subgroup P of N^* is a Sylow

p-subgroup of G. Then all P-orbits in supp R have length p, so all P-orbits of length p^2 lie in fix R. Since $|P : R| = p^2$ it follows that R is the kernel of the action of P on the union of its orbits of length p^2, and hence that P is abelian. Therefore if P^* is any Sylow p-subgroup of G containing R, then $P^* \subseteq N(R)$, and hence $P^* \subseteq N^*$. Thus R is the kernel of the action of P^* on the union of its orbits of length p^2. It follows that R is weakly closed in P (for if $R^g \subseteq P$, then $R \subseteq P^* = P^{g^{-1}}$; so R is the kernel of the action of P^* on its orbits of length p^2; hence R^g is the kernel of the action of P on its orbits of length p^2, that is, $R^g = R$).

Thus $N(R)$ is 2-transitive on fix R ([15], Satz 3). First suppose that the group N^{*p} is trivial. Then N^* is a p-group containing P, so $N^* = P$. Since $N^* \trianglelefteq N(R)$, then N^* is transitive on fix R, and as P has an orbit of length p^2 in fix R, it follows that $|\text{fix } R| = p^2$, fix P is empty, and n is divisible by p. Since P has orbits of length p (in supp R), n is not divisible by p^2. However this means that, for α in fix R, R is a subgroup of index p in a Sylow p-subgroup T of G_α; then $T \subseteq N(R)$, and as $N(R)$ has a unique Sylow p-subgroup, $T \subset P$. Thus T is a subgroup of P of index p fixing a point α of the P-orbit fix R of length p^2, contradiction.

Hence N^{*p} is a nontrivial normal subgroup of $N(R)$, and hence is transitive on fix R. Also N^{*p} fixes supp R pointwise. Thus by [6], G satisfies one of (a)-(c) of List 1.3. In case (a) or (a^1) we find, as in the proof of Lemma 1.2, that $|\text{fix } P| = |\text{fix } Q| = 1$. As P has orbits of length p, then $n - 1$ is not divisible by p^2, so for α, β in fix R, R is a subgroup of index p of a Sylow p-subgroup T of $G_{\alpha\beta}$. As $|T| \geq p^2$ it follows from [10] that T has an orbit of length p^2. On the other hand, T is a p-group normalising R, so $T \subseteq N^*$, and hence all T-orbits of length p^2 lie in fix R. This is a contradiction

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

as $T^{\text{fix } R} \simeq T/R$ has order p .

In cases (b) and (b^1), we find as in Lemma 1.2 that $n = p^2$ and $G \geq \text{ASL}(2, p)$. Again we have a contradiction since the Sylow p-subgroups of $\text{ASL}(2, p)$ are nonabelian. Finally in case (c) we find that either n or $n - 1$ is divisible by p and this leads to a contradiction as in case (a) above.

COROLLARY 1.5. *Each long orbit of* N^* *contains a long* Q*-orbit.*

Proof. This is trivially true if fix Q is empty, so suppose that fix Q contains a point α . We shall show that either the N^*-orbit containing α contains a long Q-orbit or N^* fixes α .

If α is fixed by all conjugates Q^* of Q which contain R then α is fixed by N^* . Hence if α lies in a long N^*-orbit, there is some Q^* containing R such that α lies in a long Q^*-orbit. By Lemma 1.4, $Q^{*g} = Q$ for some g in N^* . Hence αg lies in a long Q-orbit and the N^*-orbit containing α contains this orbit.

LEMMA 1.6. *A Sylow* p*-subgroup of* $N(R)$ *is a Sylow* p*-subgroup of* G *unless either*

(I) $\text{ASL}(2, p) \leq G \leq \text{AGL}(2, p)$, $n = p^2$, *or*

(II) $G = \text{P}\Gamma\text{L}(2, 8)$, $n = 9$, *and* $p = 3$

(and these groups satisfy the conditions of the theorem).

Proof. Suppose that a Sylow p-subgroup of $N(R)$ has order less than $|P|$. Then $Q \subset N^*$ is a Sylow p-subgroup of $N(R)$. If P is a Sylow p-subgroup of G containing Q , then we deduce that P is nonabelian and R is the stabiliser of a point in a P-orbit Γ of length p^2 such that P^Γ is nonabelian. Then Q contains p distinct subgroups each of which is conjugate to R by an element of P .

First suppose that $|\text{fix } P| \leq 1$. Then for α, β in fix R , let T be a Sylow p-subgroup of $G_{\alpha\beta}$ containing R . Now $|T| < |P|$, and we suppose first that $T \neq R$. Then $|T : R| = p$, so $T \subseteq N(R)$, and as $|T| = |Q|$, T is conjugate to Q in $N(R)$. This is impossible as $|\text{fix } T| > |\text{fix } Q|$. Hence $T = R$ is a Sylow p-subgroup of $G_{\alpha\beta}$ with all

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

orbits of length p, and all long P-orbits have length p^2. It follows that

(I) $|R| = p$ (by [10]),

(II) for any γ in $\text{supp}\, Q$, Q_γ is conjugate to R,

(III) $N(R)$ is 2-transitive on $\text{fix}\, R$ ([15], Satz 3).

If N^{*p} is trivial then N^* is a p-group containing Q, so $N^* = Q$, and as N^* is transitive on $\text{fix}\, R$ (because $N^* \trianglelefteq N(R)$), $|\text{fix}\, R| = p$. Hence $\text{fix}\, P$ is empty and so p^2 divides n. Now $|Q| = p^2$ and so Q has $p + 1$ subgroups of order p. However, by (II), Q has n/p distinct subgroups of order p which fix points of Ω. It follows that $n = p^2$, and so by [11], either $\text{ASL}(2, p) \le G \le \text{AGL}(2, p)$, or $p = 3$ and G is $\text{P}\Gamma\text{L}(2, 8)$. Clearly these groups satisfy the hypotheses of the theorem, and it is not difficult to see that, for them, Q is a Sylow p-subgroup of $N(R)$.

On the other hand, if N^{*p} is nontrivial then it is transitive on $\text{fix}\, R$; also N^{*p} fixes $\text{supp}\, R$ pointwise. So by [14], 13.5, $|\text{fix}\, R| \ge \frac{1}{2}n$. However we noted above that there are p distinct conjugates of R by elements of P which are contained in Q, and the fixed point sets of any pair of these overlap in precisely the set $\text{fix}\, P$, (and $|\text{fix}\, P| \le 1$). Hence $n \ge p(|\text{fix}\, R|-1) + 1 \ge p(\frac{1}{2}n-1) + 1$, and so $p = 2$ and $|\text{fix}\, R| = \frac{1}{2}(n+|\text{fix}\, P|)$ (since $|\text{fix}\, R|$ is an integer). By [6], G is one of the groups of List 1.3, where again $c = |\text{supp}\, R|$, and it is easy to check that G must be $\text{AGL}(m, 2)$, and $|\text{fix}\, P| = 0$. However since P has no orbit of length greater than p^2, then $m = 2$ and so $G \supseteq A_4$, contradiction.

Thus we may assume that $|\text{fix}\, P| \ge 2$. Then $p \ge 3$. We claim that all long N^*-orbits in $\text{fix}\, R$ contain at least two points of $\text{fix}\, Q$ and have length prime to p. Let Γ be a long N^*-orbit in $\text{fix}\, R$, and let α, β be two points of $\text{supp}\, Q$ in Γ (by Corollary 1.5). Let P' be a Sylow p-subgroup of $G_{\alpha\beta}$ containing R. Then R is a proper subgroup of $Q' = N(R) \cap P'$, and it follows that Q' is a Sylow p-subgroup of $N(R)$ and hence is conjugate to Q. Thus Q' lies in N^* and so

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

$Q'^g = Q$ for some g in N^*. Then α^g, β^g lie in fix Q and so $|\Gamma \cap \text{fix } Q| \geq 2$. Since $Q' \leq N(R)_\alpha$, it follows that $|\Gamma|$ is prime to p.

Thus by [14], 17.1, N^{*p} is transitive on each long N^*-orbit in fix R; and so N^{*p} is nontrivial. Since N^{*p} fixes supp R pointwise, $|\text{supp } N^{*p}| \leq |\text{fix } R| = f + rp$, where $|\text{fix } Q| = f$ and R fixes r long Q-orbits. On the other hand, as Q acts nontrivially on each long N^*-orbit in fix R, it follows from [8] that $|\text{supp } N^{*p}| < 2rp$. Finally by Bochert ([12], 52-54), $|\text{supp } N^{*p}| \geq \frac{1}{4}n$ (unless $n = 25$, and the minimal degree equals $|\text{supp } N^{*p}| = 6$. However each long N^{*p}-orbit has length at least $p + 2 \geq 5$ and has length prime to p, a contradiction). Thus, if Q has q long orbits we have

$$f + rp \geq \tfrac{1}{4}(f+qp) \text{ , and } 2rp > \tfrac{1}{4}(f+qp) \text{ .}$$

Eliminating f we find that $r > q/7$. Now Q contains p distinct conjugates of R by elements of P and the fixed point sets of any two overlap in precisely the set fix Q. Hence there are $pr > pq/7$ long Q-orbits which are fixed by one of these groups. As Q has just q long orbits it follows that p is 3 or 5.

Let $M = N(Q) \cap N(R)$ and let $l = |N(Q) : M|$; l is the number of conjugates of R in Q by elements of $N(Q)$. Since Q is a Sylow p-subgroup of M, it follows that l is divisible by p, and as $q \geq rl > ql/7$, then $l \leq 6$. Hence either $l = p = 3$ or 5, or $l = 2p = 6$. If either $f > l$, or $(f, l) = 1$, then M is transitive on fix Q (by [5], Hilfsatz 1, (though the result was known to Burnside) and [14], 17.1), and by our observations about the orbits of N^* it follows that $N(R)$ is transitive on fix R; hence N^{*p} is $\frac{1}{2}$-transitive on fix R, contradiction (see Lemma 1.2).

So suppose that M is transitive on fix Q. Then an orbit Γ of N^{*p} in fix R is a block of imprimitivity for $N(R)$, and it is easy to see that $\overline{\Gamma} = \Gamma \cap \text{fix } Q$ is a block of imprimitivity for M in fix Q. We showed above that $|\overline{\Gamma}| \geq 2$. Now for α in fix Q, $N(Q)_\alpha$ is

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

transitive on the $f - 1$ points of $\text{fix } Q - \{\alpha\}$, and $f - 1$ is not divisible by p . Hence as $|N(Q)_\alpha : M_\alpha| = l$ is p or $2p$, then $(f-1, l) \leq 2$ and it follows from [14], 17.1, that either M_α is transitive on $\text{fix } Q - \{\alpha\}$, or M_α has two orbits in $\text{fix } Q - \{\alpha\}$, each of length $\frac{1}{2}(f-1)$. In either case M is primitive on $\text{fix } Q$ and so $\overline{\Gamma} = \text{fix } Q$. Hence $\Gamma = \text{fix } R$ and N^{*p} is transitive on $\text{fix } R$. Thus by [6], G is one of the groups in List 1.3, where again $c = |\text{supp } R|$. However in each of the cases we showed that n or $n - 1$ is divisible by p , a contradiction since $f \geq 2$.

Thus M is not transitive on $\text{fix } Q$ and hence $(f, l) \neq 1$, so $l = 2p = 6$ and f is even. Since $p = 3$, we have $f \equiv 2 \pmod 3$. Then, since $f \leq l = 6$, we must have $f = 2$. It follows that N^{*p} is transitive on $\text{fix } R$, a contradiction as before.

Finally in this section we prove

LEMMA 1.7. *If a conjugate* Q^* *of* Q *normalises* R *then* Q^* *contains* R .

Proof. Suppose that $Q^* \subseteq N(R)$ but $Q^* \not\supseteq R$. Then $P^* = Q^*R$ is a Sylow p-subgroup of G contained in $N(R)$. We claim that P^* is abelian. If not then P^* has an orbit Γ of length p^2 such that $P^{*\Gamma}$ is nonabelian; $P^{*\Gamma}$ has a unique set of blocks of length p , namely the set of Q^*-orbits contained in Γ . Now as $R \trianglelefteq P^*$ and $|P^* : R| = p^2$, clearly R does not fix any points of Γ , and so R has p orbits of length p in Γ which are blocks of imprimitivity for P^* . Hence $Q^*R = P^*$ leave the unique set of blocks fixed setwise, contradiction. Hence P^* is abelian and so the Sylow p-subgroup P containing Q lies in $N(R)$. Therefore $P^g = P^*$ for some g in $N(R)$ and hence $R \subset Q^g = Q^*$, contradiction.

COROLLARY 1.8. *If there is a conjugate* R' *of* R *contained in* P *such that* $P = QR'$, *then* P *is nonabelian.*

Proof. If $P = QR'$ and P is abelian, then $Q \subseteq N(R')$ and so by Lemma 1.7, $Q \supset R'$, contradiction.

2. Characterisation of PSL(3, p)

Consider the following hypothesis:

A: *For each long* Q*-orbit* Δ *, the group* $R = Q_\Delta$ *has a conjugate* R' *contained in* P *such that* $P = QR'$.

In this section we shall prove the following proposition.

PROPOSITION 2.1. *If Hypothesis* A *is true and if* fix P *is nonempty, then*

$$n = 1 + p + p^2 \text{ and } \mathrm{PSL}(3, p) \le G \le \mathrm{PGL}(3, p) .$$

Clearly these groups satisfy the conditions of the theorem. Suppose that Hypothesis A is true. Then by Corollary 1.8, P is nonabelian. For a fixed $R = Q_\Delta$ let $T = Q \cap R'$, where R' is any group satisfying the conditions of Hypothesis A. If Γ is any P-orbit of length p^2 , then since $P = QR'$, R' permutes the Q-orbits in Γ transitively, and it follows that T fixes Γ pointwise. Since P is nonabelian, there is an orbit Γ of P of length p^2 such that $|P^\Gamma| \ge p^3$, and as $|P : T| = p^3$, it follows that T is the kernel of the action of P on the union of its orbits of length p^2 . Let Γ be a P-orbit of length p^2 such that $|P^\Gamma| = p^3$. Then $P^\Gamma \simeq P/T$ is nonabelian and so by [3], 1.3.4, its centre has order p . Let Z be the subgroup of P containing T such that $Z/T = Z(P/T)$. Then $Z \trianglelefteq P$ and so Z has p orbits of length p in Γ which are blocks of imprimitivity for P . Since P has a unique set of blocks of length p in Γ , namely the Q-orbits in Γ , we conclude that $Z \subseteq Q$. Now let $R_1, \ldots, R_p$ be the p distinct subgroups of P of index p^2 fixing points in Γ . Then $Q \supset R_i \supset T$ for $1 \le i \le p$. Since Q/T is an elementary abelian group of order p^2 , it follows that there are precisely $p + 1$ subgroups of Q of index p , containing T , and these are $R_1, \ldots, R_p, Z$.

LEMMA 2.2. *If Hypothesis* A *is true then* $|P| = p^3$.

Proof. Suppose that Hypothesis A is true and that $|P| \ge p^4$. Then

$T \neq 1$. Let Δ be a long Q-orbit in supp T , and let $\hat{R}$ be a conjugate of Q_Δ contained in P such that $P = Q\hat{R}$.

Let Σ_1 be the union of P-orbits of length p^2 , and let $\Sigma_2 = \text{supp } Q - (\text{supp } T \cup \Sigma_1)$. Now as $P = Q\hat{R}$, clearly $\hat{R}$ permutes every Q-orbit in Σ_1 nontrivially. Also, as above, $Q \cap \hat{R}$ fixes Σ_1 pointwise, and since $|Q \cap \hat{R}| = |T|$, it follows that $T = Q \cap \hat{R} \subset \hat{R}$. Hence $\hat{R}$ fixes no point in supp T , and therefore $\text{fix } \hat{R} \subseteq \text{fix } Q \cup \Sigma_2$. Now since $|\text{fix } \hat{R}| = |\text{fix } Q_\Delta| > |\text{fix } Q|$, it follows that Σ_2 is nonempty.

We claim that Z fixes Σ_2 pointwise. Let Δ' be a long Q-orbit in Σ_2 (Δ' is an orbit of P). Then $T \subset Q_{\Delta'}$, and since $Q_{\Delta'}$ is normalised by $\langle P_{\Delta'}, Q \rangle = P$, then $Q_{\Delta'}$ does not fix any points in a P-orbit Γ of length p^2 such that P^Γ is nonabelian. (In future we shall refer to such an orbit as a "nonabelian P-orbit".) By our remarks above it follows that $Q_{\Delta'} = Z$. Thus we conclude that $\text{fix } Z \supseteq \Sigma_2 \cup \text{fix } Q$.

Now if Z' is a conjugate of Z contained in P such that $P = QZ'$ then

(I) Z' permutes all Q-orbits in Σ_1 nontrivially, and

(II) $Q \cap Z'$ fixes Σ_1 pointwise;

as above we conclude that $T = Q \cap Z' \subset Z'$ so that Z' fixes no points of supp T . Hence $\text{fix } Z' \subseteq \text{fix } Q \cup \Sigma_2 \subseteq \text{fix } Z$, and as $|\text{fix } Z'| = |\text{fix } Z|$, it follows that $\text{fix } Z = \text{fix } Z' = \text{fix } Q \cup \Sigma_2$. Now $Y = ZZ'$ is a subgroup of P such that $\text{fix } Y = \text{fix } Z \neq \text{fix } Q$; thus $|P : Y| = p$ and for any point α in Σ_2 , $Y = P_\alpha$. The group $\hat{R}$ defined above fixes some Q-orbit in Σ_2 , and so $\hat{R} \subset Y$ and $\text{fix } \hat{R} \supseteq \text{fix } Y = \text{fix } Z$. We shall show that $\hat{R}$ is conjugate to Z' in P .

First note that neither $\hat{R}$ nor Z' is normal in P (for if either were normal, then its orbits in the non-abelian P-orbit Γ would be

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

blocks of imprimitivity for P, whereas both $\hat{R}$ and Z' permute nontrivially the Q-orbits in Γ and these are the unique blocks of length p for P in Γ). Now Y has precisely $p+1$ subgroups of index p containing T, and three of them are Z, Z', and $\hat{R}$. Now as P normalises Y, T, and Z, it follows that P permutes transitively the p subgroups of Y of index p containing T, and different from Z. Hence $\hat{R}$ is conjugate to Z' in P.

It follows that Z is conjugate in G to Q_Δ, for any $\Delta \subseteq \text{supp}\, T$. Now both Z and Q_Δ are normal in P and so by a theorem of Burnside ([2], 154-155), Z is conjugate to Q_Δ in $N(P)$. This is impossible, since T is normal in $N(P)$ and $T \subset Z$, while $T \nsubseteq Q_\Delta$. Thus $|P| = p^3$.

Now we shall prove Proposition 2.1.

We have $|Q| = p^2$, and $\{R_1, \ldots, R_p, Z\}$ is the complete set of subgroups of Q of order p, and $R_1, \ldots, R_p$ are all conjugate in P. Let

$$N_i^* = \langle Q^* \supset R_i \mid Q^* \sim_G Q \rangle \quad \text{for} \quad 1 \le i \le p$$

and

$$N^* = \langle Q^* \supset Z \mid Q^* \sim_G Q \rangle .$$

Each R_i fixes p points of each nonabelian P-orbit of length p^2 and fixes no other points of $\text{supp}\, Q$. Let $|\text{supp}\, Q| = qp$, $|\text{fix}\, Q| = f$, and $|\text{fix}\, R_i| = rp + f$. Then $|\text{fix}\, Z| = f + (q-rp)p$, and $\text{supp}\, Z$ is the union of the nonabelian P-orbits of length p^2. If $\hat{R}$ is a conjugate of R_1 in P such that $P = Q\hat{R}$ then $\hat{R}$ must permute each Q-orbit in $\text{supp}\, Z$ nontrivially and hence $\text{fix}\, Z \supseteq \text{fix}\, \hat{R}$. Then since $|\text{fix}\, \hat{R}| > |\text{fix}\, Q|$ it follows that Z fixes points in $\text{supp}\, Q$. Hence, as in the proof of Lemma 2.2, there is a conjugate Z' of Z in P such that $P = QZ'$; we find as in Lemma 2.2 that $Y = Z'Z$ has index p in P, that $\text{fix}\, Y = \text{fix}\, Z' = \text{fix}\, Z$, and that $Y = P_\delta$ for any δ in $\text{supp}\, P - \text{supp}\, Z$. In particular this means that all P-orbits of length

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

p^2 lie in supp Z .

Further, since the group $\hat{R}$ defined above fixes a point of supp Q - supp Z , it follows that $\hat{R} \subseteq Y$, and we can show (by a proof analogous to that in Lemma 2.2), that $\hat{R}$ is conjugate to Z' . Thus it follows that $R_1, \ldots, R_p, Z$ are all conjugate in G , and so $n = f + rp(p+1)$.

It is easy to show that Y is weakly closed in P with respect to G (for if $Y' \subset P$ is conjugate to Y then Y' fixes a point δ of supp P ; and since $|P : Y'| = p$, clearly $\delta \in$ fix Y so $Y' = P_\delta = Y$). Thus, by [15], Satz 3, $N(Y)$ is 2-transitive on fix Y . Define $M = N(Y) \cap N(Z)$; and then since Y has $p + 1$ subgroups of order p , $l = |N(Y) : M| \le p + 1$. By [5], Hilfsatz 1, if $l < f + rp$, then M is transitive on fix Y = fix Z .

So suppose that $l < f + rp$. Then $N(Z)$ is transitive on fix Z and so N^* is $\frac{1}{2}$-transitive on fix Z . First of all, if N^{*p} is trivial then by Lemma 1.4, $N^* = Q$ which is $\frac{1}{2}$-transitive on fix Z . Hence $f = 0$, contradiction. Hence N^{*p} is nontrivial and so is $\frac{1}{2}$-transitive on fix Z . Since Q acts nontrivially on each N^*-orbit in fix Z , it follows from [8] that $|\text{supp } N^{*p}| = |\text{fix } Z| = rp + f < 2rp$. By Bochert ([12], 52-54), $|\text{supp } N^{*p}| \ge \frac{1}{4}n$ (unless $n = 25$ and the minimal degree is equal to $|\text{fix } Z| = 6$; but then $|\text{supp } Z| = 19$ which is impossible). Hence $2rp > \frac{1}{4}(qp+f)$, and $rp + f \ge \frac{1}{4}(qp+f)$, and eliminating f we find that $r > q/7 = r(p+1)/7$. Hence $p \le 5$. We claim now that $f \le r$. Suppose on the other hand that $f > r$. Let Δ be a long Q-orbit in fix Z . Then M permutes the long Q-orbits in fix Z in some way, so if L is the setwise stabiliser of Δ in M then $|M : L|$ r . Hence $|N(Y) : L| \le (p+1)r < rp + f$, so by [5], Hilfsatz 1, L is transitive on fix Z . However L fixes setwise the N^*-orbit containing Δ . Hence N^* is transitive on fix Z , and as $f \ne 0$, N^{*p} is also transitive on fix Z . Then, by [14], 13.5, $|\text{fix } Z| = rp + f \ge \frac{1}{2}n = \frac{1}{2}(rp(p+1)+f)$, that is $f \ge rp(p-1)$. This is impossible since $f < rp$ (by [8]). Hence $f \le r$.

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

Now as R_i is conjugate to Z, we know that N_i^{*P} is $\frac{1}{2}$-transitive on fix R_i for $i = 1, 2$. Consider the set $S = \left\{[g_1, g_2] \mid g_i \in N_i^{*P}\right\}$. If $S = \{1\}$ then N_1^{*P} is normal in $\left\langle N_1^{*P}, N_2^{*P}\right\rangle = L$, say. So N_1^{*P} is $\frac{1}{2}$-transitive (or trivial) on each L-orbit. It follows that N_1^{*P} fixes pointwise each orbit of L (and hence each orbit of N_2^{*P}) which contains a point of fix R_2 - fix Z. This means that N_1^{*P} fixes fix Q pointwise, a contradiction. Hence S contains a nontrivial element which, by [1], permutes at most $3f$ points. Hence $3f \geq \frac{1}{4}n$ (by [13], 52-54); that is, $rp(p+1) \leq 11f \leq 11r$. Hence $p = 2$, and as G is 2-transitive we must have $f = 1$. Thus G contains a non-identity element permuting at most 3 points. By [14], 13.3, $G \supseteq A_n$, contradiction.

Thus we conclude that $p + 1 \geq l \geq f + rp$, and so $r = f = 1$. By [11] it follows that $\mathrm{PSL}(3, p) \leq G \leq \mathrm{PGL}(3, p)$ and the proof is complete.

3. Completion of the proof when fix $P \neq \emptyset$

We shall assume now that fix P is nonempty and that Hypothesis A is not true. Then for some δ in supp Q, $R = Q_\delta$ satisfies the hypothesis:

B: *If P' is any Sylow p-subgroup of G containing R then R is a subgroup of Q', the unique conjugate of Q lying in P'.*

We now proceed to obtain a contradiction. We shall consider $N(R)$ and $N^* = \langle Q^* \supset R \mid Q^* \sim_G Q \rangle$.

LEMMA 3.1. *(a) Each long N^*-orbit Σ in fix R contains a long Q-orbit and at least $d = \min(2, |\text{fix } P|)$ points of fix Q. Further, $|\Sigma|$ is prime to p, and hence N^{*P} is transitive on Σ.*

(b) If $\alpha \in$ fix Q and if $f = |\text{fix } Q| \geq 2$, then each long N_α^*-orbit contains a long Q-orbit and a point of fix Q.

Proof. Let Σ be a long N^*-orbit in fix R and let Δ be a set of

$d = \min(2, f)$ points in $\Sigma \cap \text{supp } Q$ (by Corollary 1.5). Let P' be a Sylow p-subgroup of G_Δ containing R, and then by Hypothesis B, $R \subseteq Q'$, the unique conjugate of Q in P'. Then $Q' \subseteq N^*$ and so, by Lemma 1.4, $Q'^g = Q$ for some g in N^*. Then $\Delta^g \subseteq \text{fix } Q \cap \Sigma$. By Lemma 1.4, since $Q \subseteq N^*_\Delta$, Σ has length prime to p. Part *(b)* can be proved analogously.

It follows from Lemma 3.1 that N^{*P} is transitive on each N^*-orbit in fix R, and in particular that N^{*P} is nontrivial. By Bochert ([12], 52-54), $|\text{supp } N^{*P}| \geq \frac{1}{4}n$ (unless $n = 25$ and the minimal degree is equal to $|\text{supp } N^{*P}| = 6$, by Lemma 3.1, then $p \leq 5$, and since p does not divide n, then p is 2 or 3. Since each long N^*-orbit has length prime to p and length at least $p + 1$, it follows that $p = 2$ and hence $|\text{fix } P| = 1$. By Lemma 3.1, N^{*P} is transitive on fix R, a contradiction to [14], 13.5). By [8] we have $2rp > |\text{supp } N^{*P}| \geq \frac{1}{4}(qp+f)$, and also $rp + f \geq |\text{supp } N^{*P}| \geq \frac{1}{4}(qp+f)$, where, as usual, $|\text{fix } Q| = f$, $|\text{supp } Q| = qp$, and $|\text{fix } R| = rp + f$. Hence, eliminating f, we find that $r > q/7$. So there are at most six distinct conjugates of R in Q.

Now we show that N^{*P} is not transitive on fix R. If it is transitive then, by [6], G is one of the groups in List 1.3. In case (a), $G \geq \text{PSL}(m, s)$ for some $m \geq 3$, and prime power s. We found that $f = 1$. Since $|\text{supp } R| = (s^{m-1}-1)/(s-1) \geq \frac{1}{4}(n-1)$ (by [12], 52-54), it follows that $s \leq 4$, while if $s = 4$ then $|\text{supp } R| < \frac{1}{4}n$ which contradicts [12], 52-54 (since $n \neq 25$). Hence s is 2 or 3. Now if $p \geq s$ then fix R is a subspace (for if $\alpha, \beta \in \text{fix } R$, the line through α and β contains $s - 1 < p$ points distinct from α and β and so is fixed pointwise by R). Then $|\text{fix } R| = (s^t-1)/(s-1)$ for some $t > 1$, which is impossible. Hence $p < s$ and so $p = 2$ and $s = 3$. However for any $m \geq 3$, the Sylow 2-subgroups of $\text{PSL}(m, 3)$ have an orbit of length greater than 4, so none of these groups are satisfactory. In case (b) and (b^1) we found that $f = 0$ so the case does not arise either.

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

Finally, in case (c), we found that, since p^3 divides $|G|$, p is 2 or 3 . Then as $|\text{supp } R| = n - 16$ is divisible by p , $n \neq 23$, and as $f \neq 0$, we must have $p = 3$ and $n = 22$. However 3^3 does not divide $|\text{Aut } M_{22}|$. Hence N^{*p} is not transitive on fix R . Then, by Lemma 3.1, it follows that $f = |\text{fix } Q| \geq 3$.

Now $N(Q)$ is 2-transitive on fix Q (by Lemma 1.2 and [15], Satz 3). If $N(Q)$ has a subgroup of index x where either $x < f$ or $(x, f) = 1$, then that subgroup is transitive on fix Q (by [5], Hilfsatz 1, and [14], 17.1).

Let $M = N(Q) \cap N(R)$ and let $l = |N(Q) : M|$, the number of distinct conjugates of R in Q by elements of $N(Q)$, $l \leq 6$. Suppose first that M is transitive on fix Q . Then by Lemma 3.1, $N(R)$ is transitive on fix R , and so N^{*p} is $\frac{1}{2}$-transitive on fix R . An N^{*p}-orbit Σ in fix R is then a block of imprimitivity for $N(R)$ and it is easy to see that $\overline{\Sigma} = \Sigma \cap \text{fix } Q$ is a block of imprimitivity for M in fix Q . By Lemma 3.1, it follows that $2 \leq |\overline{\Sigma}| < f$, so $\overline{\Sigma}$ is a nontrivial block. Let $\alpha \in \overline{\Sigma}$; then $\overline{\Sigma}$ is a union of M_α-orbits in fix Q , and by [14], 17.1, each long M_α-orbit in fix Q has length a multiple of $(f-1)/(f-1, l)$. Hence $b = |\overline{\Sigma}| = 1 + a(f-1)/(f-1, l)$, for some integer a , $1 \leq a < (f-1, l)$ and b divides f . Checking for $l \leq 6$ we find that the only possibilities are the following:

List 3.2

l	3	6	5	5	4	5	6
f	4	4	6	6	9	16	25
b	2	2	2	3	3	4	5
$f/b = d$	2	2	3	2	3	4	5

If on the other hand M is not transitive on fix Q , then by our remarks above it follows that $3 \leq f \leq l \leq 6$, and that $(f, l) \neq 1$. Hence

(3.3) either $3 \leq f = l \leq 6$, or $l = 6$ and f is 3 or 4 .

We note that in all cases $f \leq rl$; this is trivially true if $f \leq l$,

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

while in the cases of List 3.2, N^* has f/b orbits and each contains a long Q-orbit, and we check that $f \le lf/b \le rl$.

Now since $l > 1$, let R' be a conjugate of R contained in Q , $R' \ne R$, and let N'^*, N'^{*p} be the analogues of N^*, N^{*p} for R' . Consider the set $S = \{[g, g'] \mid g \in N^{*p}, g' \in N'^{*p}\}$. If $S = \{1\}$ then N^{*p} is normal in $L = \langle N^{*p}, N'^{*p} \rangle$ and hence N^{*p} acts $\frac{1}{2}$-transitively (or trivially) on every L-orbit. Hence N^{*p} fixes pointwise every orbit of L (and hence every orbit of N'^{*p}) which contains a point of fix R' - fix Q . Thus, by Lemma 3.1, N^{*p} fixes $\Pi' = \text{supp } N'^* \cap \text{fix } Q$ pointwise.

In the cases of List 3.2, N^{*p} fixes no points of fix Q whereas by Lemma 3.1, $|\Pi'| \ge 2$. So we have cases (3.3) to consider. If N'^* has at least two orbits in fix R' then $|\Pi'| \ge 4$, and similarly (since $R \sim R'$), $\Pi = \text{supp } N^* \cap \text{fix } Q$ contains at least four points and is fixed by N'^{*p} . Hence $\Pi \cap \Pi' = \emptyset$ and so $f \ge |\Pi \cup \Pi'| \ge 8 > l$, contradiction. So N'^{*p} has just one long orbit which contains at most $|\text{fix } Q - \Pi| \le f - 2$ points of fix Q , and so, by [14], 13.5, $rp + f - 2 \ge |\text{supp } N'^{*p}| \ge \frac{1}{2}(qp+f) \ge \frac{1}{2}(rlp+f)$; that is, $1 \ge \frac{1}{2}f - 2 \ge \frac{1}{2}rp(l-2) \ge \frac{1}{2}p$. However, since $f \ge 3$, we have $p \ge 3$, contradiction.

Hence S contains a non-identity element which, by [1], permutes at most $3f$ points. By [14], 15.1, $3f \ge \frac{1}{3}n(1-\alpha)$, where $\alpha = 2/\sqrt{n}$. If $p \ge 11$, then $9f \ge (1-\alpha)(qp+f)$, so $(8-\alpha)f \ge (1-\alpha)qp \ge 11(1-\alpha)rl$, and since $f \le rl$ we have $\alpha \ge 3/10$; that is $n < 45$. However since p^3 divides $|G|$, this means that there is a p-element of degree at most $2p$ with many fixed points, a contradiction by [14], 13.10.

Hence p is 3, 5 , or 7 (since $f > 2$, then $p \ne 2$); $f \le rl$, and by [12], 52-54, $3f \ge \frac{1}{4}n$ (unless $n = 25$ and the minimal degree is equal to $3f = 6$, which is impossible since $f \ge 3$); that is $qp \le 11f$. Suppose first that M is transitive on fix Q . Then N^{*p} has $d = f/b$ orbits each containing say r' long Q-orbits, where $r = r'd$. Hence

$11f \geq qp \geq r'dlp = r'flp/b$. Then from List 3.2, $b/l \leq 5/6$, so $r'p \leq 9$. If $r' = 1$ then N^* has d orbits of length $p + b \geq p + 2$ with a p-element acting nontrivially on each. Clearly this constituent contains an insoluble factor with order divisible by p , and we deduce that N^{*P} contains a p-element of degree dp . If $p = 7$ then $d \leq 5$; if $p = 5$ then $f \neq 25$ so $d \leq 4$. Hence it follows from [14], 13.10, that $p = 3$. Also if $r' > 1$, then $p = 3$. However since $f > 2$, neither f nor $f - 1$ is divisible by 3 , and so none of the values of f in List 3.2 is suitable.

We conclude that $M^{\text{fix}Q}$ is intransitive and that the values of f and l satisfy (3.3). Then $11f \geq qp \geq rlp \geq rfp$; so $rp \leq 11$.

If N^{*P} has only one long orbit, it has length at most $rp + f - 1$, which is less than $\frac{1}{2}n$ (since $l \geq f$), which contradicts [14], 13.5. Hence N^{*P} has at least two long orbits and since $rp \leq 11$ and by Lemma 3.1, it follows that $f \geq 4$, $r \geq 2$, and p is 3 or 5 . If $p = 5$ then $r = 2$, $f = 4$ (since $f(f-1)$ is prime to p), and N^{*P} has two orbits of length 7 . Hence G contains a 7-element of degree 14 , a contradiction to [14], 13.10. If $p = 3$ then $f = l = 5$, and r is 2 or 3 . By Lemma 3.1, N^{*P} has exactly two long orbits, and since neither orbit length is divisible by 3 , each orbit contains exactly two points of fix Q . Hence at least one orbit has length $p + 2 = 5$, and so G contains a 5-element of degree at most 10 , a contradiction to [14], 13.10. This completes the proof that there are no groups satisfying Hypothesis B, with fix P nonempty.

4. The case fix $P = \emptyset$

This section will complete the proof of the theorem: we shall prove

PROPOSITION 4.1. *If P fixes no points then G satisfies one of the following*

(I) $\mathrm{ASL}(2, p) \leq G \leq \mathrm{AGL}(2, p)$, $n = p^2$;

(II) $G = \mathrm{P\Gamma L}(2, 8)$, $n = 9$, *and* $p = 3$;

(III) $G = M_{12}$, $n = 12$, *and* $p = 3$;

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

(IV) $G = \mathrm{PGL}(2, 5)$, $n = 6$, *and* $p = 2$.

By Remark 1.1, fix Q is empty. As in the previous sections we shall consider subgroups of Q , $R = Q_\alpha$, for α in Ω , and the subgroups N^* and N^{*p} of $N(R)$. First we show:

LEMMA 4.2. *If* p^2 *divides* n *then* G *satisfies* (I) *or* (II) *of Proposition* 4.1, *and those groups satisfy the conditions of the theorem.*

Proof. Suppose that p^2 divides n . Then $R = Q_\alpha$ is a Sylow p-subgroup of G_α . Hence, by [15], Satz 3, $N(R)$ is 2-transitive on fix R , and hence N^* is transitive on fix R . Now, by Lemma 1.6, the lemma is true unless a Sylow p-subgroup P' of $N(R)$ is a Sylow p-subgroup of G . However this means that, as $R \trianglelefteq P'$, fix R is a union of P'-orbits, and so $|\text{fix } R|$ is divisible by p^2 . Hence $|N^{*\text{fix}R}|$ is divisible by p^2 , a contradiction to Lemma 1.4. Thus the lemma is proved.

Hereafter we shall assume that n is divisible by p but not by p^2 , and that a Sylow p-subgroup of $N(R)$ has order $|P|$. Let S be a Sylow p-subgroup of G_α containing R . Then $|S| = |Q|$.

LEMMA 4.3. *Either*

(I) $|P| = p^3$, *or*

(II) $|P| \geq p^4$ *and* R *is the only subgroup of* S *of index* p *with all long orbits of length* p .

Hence R *is weakly closed in* S *with respect to* G .

Proof. Assume that $|P| \geq p^4$, that is $|R| \geq p^2$, and assume that R_1 and R_2 are distinct subgroups of S of order $|R|$ with all long orbits of length p . Since $|R_i| \geq p^2$, the group $T = R_1 \cap R_2$ is non-trivial and is normalised by $\langle R_1, R_2 \rangle = S$. If Γ is an S-orbit of length p^2 , then R_1 permutes the R_2-orbits in Γ , and it follows that

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

T fixes Γ pointwise. Thus S acts regularly on each of its orbits of length p^2, and in particular S is abelian. Also T is the kernel of the action of S on the union of its orbits of length p^2. Define

$$X = \langle S^* \supset T \mid S^* \sim_G S \rangle .$$

Then $X \trianglelefteq N(T)$. We claim that all these generators S^* of X are conjugate in X to S. Let $\alpha \in \text{fix } S$, $\beta \in \text{fix } S^*$, and let S' be a Sylow p-subgroup of $G_{\alpha\beta}$ containing T. Then as S^*, S' are both Sylow p-subgroups of X_β, $S^{*g} = S'$ for some g in X_β, and as S', S are both Sylow p-subgroups of X_α, $S^{*gh} = S'^h = S$ for some h in X_α.

Now let S^* be any conjugate of S containing T. Then $S^* = S^g$ for some g in X. As g fixes fix T setwise it follows that all S^*-orbits of length p^2 lie in fix T, and hence T is the kernel of the action of S^* on the union of its orbits of length p^2. From this it is easy to show that T is weakly closed in S with respect to G, and hence $N(T)$ is 2-transitive on fix T by [15], Satz 3. Further, since all S^*-orbits in supp T have length p, we deduce that X acts on supp T as an elementary abelian p-group with all orbits of length p, and hence that X^p fixes supp T pointwise. Now if X^p is nontrivial then X^p is transitive on fix T, and as $|\text{supp } T| \geq \frac{1}{4}(n-1)$ (by [12], 52-54), it follows from [6] that G is one of the groups in List 1.3, where $c = |\text{supp } T|$. Since p but not p^2 divides n, we can show (as in the proof of Lemma 1.2) that cases (a), (b), and (b^1) are not possible. In case (c), since p^4 divides $|G|$, $p = 2$; however a Sylow 2-subgroup of M_{22} has orbits of length 8 (see [4], 60) so none of these groups is suitable. Thus $X^p = 1$, and so X is a p-group containing S which is transitive on fix T. As fix $S \neq \emptyset$, X must be a Sylow p-subgroup of G, but then X has orbits of length both p and p^2 in fix T, contradiction. Thus the lemma is proved.

LEMMA 4.4. *If* $R = Q_\alpha$ *is weakly closed in a Sylow* p*-subgroup* S

of G_α *with respect to* G *(for some* α *in* Ω *), then* $Q \trianglelefteq N(R)$ *and* fix R *is an orbit of* Q *; that is,* $|\text{fix } R| = p$ *. Also if* $p \geq 5$ *, then* G *is not* 3*-transitive.*

Proof. Suppose that R is weakly closed in S. Then $N(R)$ is 2-transitive on fix R by [15], Satz 3, and so N^* is transitive on fix R. Suppose first that N^{*p} is nontrivial; then it is transitive and by [6], G is one of the groups of List 1.3. Since p but not p^2 divides n, we show as before that cases (a), (a^1), (b), (b^1) are not possible; in case (c) since p^3 divides $|G|$, p is 2 or 3, and as in Lemma 4.3, p is not 2. Hence $p = 3$ and so $n = 24$; however $|\text{supp } R| = 8$, contradiction. Hence we conclude that $N^{*p} = 1$ and therefore N^* is a p-group containing Q which is transitive on fix R. By Lemma 1.4 then $N^* = Q$ and fix R is an orbit of Q. Finally, since $N(R)^{\text{fix}R}$ is 2-transitive with the normal p-subgroup $Q^{\text{fix}R}$ it follows that $N(R)^{\text{fix}R} \cong \text{AGL}(1, p)$, which is not 3-transitive if $p \geq 5$; it follows from [15], Satz 3, that G is not 3-transitive if $p \geq 5$. This completes the proof.

LEMMA 4.5. *If* $|P| = p^3$ *then either*

(I) $G = M_{12}$, $n = 12$, *and* $p = 3$, *or*

(II) $G = \text{PGL}(2, 5)$, $n = 6$, *and* $p = 2$,

and these groups satisfy the conditions of the theorem.

Proof. Consider $R = Q_\alpha$, for some α in Ω. By Lemmas 1.6 and 1.7 we may assume that R is normal in P. We claim that P has an orbit of length p in fix R (for if S' is a Sylow p-subgroup of $N(R)_\alpha$, and if P' is a Sylow p-subgroup of $N(R)$ containing S', then $S' = P'_\alpha$, so the P'-orbit containing α has length p, and P' is conjugate to P in $N(R)$). Thus we may assume that the P-orbit containing α has length p. Let $S = P_\alpha$. Suppose that R is not weakly closed in S. Then there is a conjugate R' of R, distinct from R, contained in S, and as $Q \cap S = R$, and $R' \not\trianglelefteq Q$, then $P = QR'$. Hence, by Corollary 1.8, P is nonabelian. Then we can show (as in §2)

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

that the subgroups of Q of order p are $R_1, \ldots, R_p$ (each of which fixes p points in each nonabelian P-orbit of length p^2, and no other points of Ω), and $Z(P)$ (which fixes the remaining points of Ω). The only group normal in P is $Z(P)$, so $R = Z(P)$, and $\text{supp } R$ is the union of the nonabelian P-orbits of length p^2. Now, by Lemmas 1.6 and 1.7, a Sylow p-subgroup P_i of $N(R_i)$ has order $|P|$ and R_i lies in its subgroup conjugate to Q. Since $R_i \trianglelefteq P_i$, it follows that $R = Z(P_i)$. Hence R is conjugate to $R_i = Z(P_i)$. Thus if $|\text{fix } R| = rp$ then $n = rp(p+1)$.

Again since $P = QR'$, R' permutes every Q-orbit in $\text{supp } R$, and since $|\text{supp } R| = |\text{supp } R'|$ and $S = RR'$, it follows that $\text{supp } R = \text{supp } R' = \text{supp } S$, and every long S-orbit has length p^2. Now $N(S)$ is 2-transitive on $\text{fix } S$ by [15], Satz 3.

Define $X = \langle P^* \supset S \mid P^* \sim_G P \rangle$.

Then every X-orbit Γ in $\text{supp } S$ has length p^2 and X^Γ has a transitive normal p-subgroup S^Γ. It is easy to show that either $X^\Gamma \le \text{AGL}(2, p)$ or $X^\Gamma \le \text{AGL}(1, p) \text{ wr } \text{AGL}(1, p)$, and hence the only possible nonabelian simple factor of $X^{\text{supp} S}$ with order divisible by p is $\text{PSL}(2, p)$. On the other hand $X^{\text{fix} S}$ is a nontrivial normal subgroup of $N(S)^{\text{fix} S}$ (which is 2-transitive). If we suppose that $|\text{fix } S| > p$, then $\text{fix } S$ is not a prime power and hence, by [14], 11.3, $N(S)^{\text{fix} S}$ does not have a regular normal subgroup. It follows (from [2], p. 202) that $X^{\text{fix} S}$ is a nonabelian simple group with order divisible by p. If $X^{\text{fix} S} \not\simeq \text{PSL}(2, p)$ then the kernel of X acting on $\text{supp } S$ is transitive on $\text{fix } S$, and hence $rp = |\text{fix } R| = |\text{fix } S| \ge \frac{1}{2}n = \frac{1}{2}rp(p+1)$ (by [14], 13.5), a contradiction. If $X^{\text{fix} S} \simeq \text{PSL}(2, p)$, then $N(S)^{\text{fix} S} \le \text{Aut}(\text{PSL}(2, p))$ is 2-transitive of degree $|\text{fix } S| \ge 2p$, which is impossible. Hence $|\text{fix } S| = |\text{fix } R| = p$.

If on the other hand R is weakly closed in S, then by Lemma 4.4,

$|\text{fix } R| \neq p$. Hence in any case, if $n = qp$ then Q has q distinct subgroups of order p fixing points of Ω . Therefore $q \le p+1$, and since P has orbits of length both p and p^2 , we have $n = p + p^2$. Thus S acts regularly on its unique long orbit which has length p^2 , and it follows from [7] that G is $(p+1)$-transitive. Hence, by [16, Satz 3], $N(S)^{\text{fix}S} \simeq S_p$. However $N(S)^{\text{supp}S}$ is a subgroup either of $\text{AGL}(2, p)$ or $\text{AGL}(1, p) \text{ wr } \text{AGL}(1, p)$.

Hence if $p \ge 7$ then $N(S)^{\text{supp}S}$ would contain a p-element of degree p , contradicting [14], 13.9. If $p = 5$, since G is 6-transitive, then G contains a 13-element of degree 26 , a contradiction to [15], 13.10. If p is 2 or 3 then we obtain the groups $\text{PGL}(2, 5)$ and M_{12} of degree 6 and 12 respectively by [13], and it is easy to check that they satisfy the conditions of the theorem.

Now we shall assume that $|P| \ge p^4$. Then, by Lemmas 4.3 and 4.4, all the subgroups $\{Q_\alpha \mid \alpha \in \Omega\}$ are conjugate in G and each fixes exactly p points. Let $R = Q_\alpha$, $R' = Q_\beta$, for some points α, β in Ω such that $R \ne R'$. Then $T = R \cap R'$ is nontrivial, $|P : T| = p^3$. Since each $|\text{fix } R| = p$, clearly P has no orbits of length p^2 on which it acts regularly. So in each P-orbit Γ of length p^2 , P has a unique set of blocks of length p , namely the Q-orbits in Γ . Thus if S is the stabiliser of a P-orbit of length p , it follows from $P = QS$, and $Q \cap S \ne 1$ that S is transitive on Γ . Suppose without loss of generality that $S = P_\alpha \supset R$, $Q \cap S = R$.

LEMMA 4.6. *There is a conjugate* T' *of* T *, distinct from* T *, contained in* S *such that* $S = RT'$ *.*

Proof. Suppose this is not true. Then if S' is a Sylow p-subgroup of G_α for some α in $\text{fix } T$, $S' \supset T$, then T lies in the unique subgroup R' of S' conjugate to R (see Lemma 4.3). Consider $N(T)$ and define

$$X = \langle Q^* \supset T \mid Q^* \sim_G Q \rangle .$$

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

Then $X \trianglelefteq N(T)$ and $X^{\mathrm{supp}T}$ is elementary abelian with all orbits of length p. We shall show that $X^{\mathrm{fix}T}$ is transitive. Let δ, γ be arbitrary points of fix T, and let S' be a Sylow p-subgroup of $G_{\delta\gamma}$ containing T. Then $T \subseteq R'$, the subgroup of S' conjugate to R. If P' is a Sylow p-subgroup of G containing S', then $T \subseteq R' \subseteq Q' \subseteq P'$, where $Q' \sim Q$, and $Q' \subseteq X$. By Lemma 4.4, fix S' is an orbit of Q', and it follows that γ, δ lie in the same X-orbit. Hence X is transitive on fix T.

Next we show that $X^{\mathrm{fix}T}$ is primitive. Assume to the contrary that B is a nontrivial block of imprimitivity for X in fix T. Suppose that B contains a point δ of a long Q-orbit Δ. Then $B \cap \Delta$ is a block for Q in Δ and so has length 1 or p. If $B \cap \Delta = \{\delta\}$ then Q_δ fixes B setwise, so B is a union of Q_δ-orbits. Since fix $Q_\delta = \Delta$, B contains a Q-orbit Δ'. Then $Q_{\Delta'}$ fixes B setwise, but is transitive on Δ, a contradiction. Hence B contains Δ and it follows that B is a union of Q-orbits. By the same argument, B is a union of Q^*-orbits for any conjugate Q^* of Q in X. Choose $\delta \in B$, $\gamma \in \mathrm{fix}\, T - B$ and, as above, choose $Q^* \supset T$ with δ and γ in the same Q^*-orbit. This is a contradiction. Hence $X^{\mathrm{fix}T}$ is primitive. Thus as $|\mathrm{fix}\, T| > p$, X is not a p-group and so X^p is a nontrivial normal subgroup of X. Hence X^p is transitive on fix T and fixes supp T pointwise. As $|\mathrm{supp}\, T| \geq \frac{1}{4}(n-1)$ by [12], it follows, from [6], that G is one of the groups of List 1.3, $c = |\mathrm{supp}\, T|$. We see, as in Lemma 4.4, that none of these groups is suitable. Thus the lemma is proved.

LEMMA 4.7. *If a conjugate S^* of S normalises T then T lies in the subgroup R^* of S^* conjugate to R.*

Proof. Suppose $T \trianglelefteq S^*$ but $T \nsubseteq R^*$. Then $S^* = TR^*$. We shall show that S^* is abelian. If not then there is a nonabelian S^*-orbit Γ of length p^2. S^* has a unique set of blocks of length p in Γ, namely the R^*-orbits in Γ. Since $T \trianglelefteq S^*$, the T-orbits in Γ are (possibly trivial) blocks of imprimitivity for S^*, and hence $TR^* = S^*$ fixes the R^*-orbits in Γ setwise, a contradiction. Thus S^* and hence

S is abelian; so $S \subseteq N(T)$. Let $\alpha \in \text{fix } S$, $\beta \in \text{fix } S^*$ and let S' be a Sylow p-subgroup of $N(T)_{\alpha\beta}$. Then S is conjugate to S' in $N(T)_\alpha$ and S' is conjugate to S^* in $N(T)_\beta$, and so $S^g = S^*$ for some g in $N(T)$. But then $T \subseteq R^g = R^*$, a contradiction.

COROLLARY 4.8. *With the notation of Lemma* 4.6, S *is nonabelian and* $U = T' \cap R$ *is the kernel of* S *acting on the union of its orbits of length* p^2 . *Hence* $U = T'' \cap R$ *where* T'' *is conjugate to any* R_β , $\beta \in \text{supp } R$, *in* S *such that* $S = RT''$.

Proof. Since $S = RT'$ it follows, from Lemma 4.7, that T' is not normal in S and hence S is nonabelian. Let Γ be an S-orbit of length p^2 . Then T' permutes the R-orbits in Γ and so $U = T' \cap R$ fixes Γ pointwise. As S is nonabelian we could choose Γ such that $|P^\Gamma| \geq p^3$, and the result follows since $|S : U| = p^3$.

Now let Γ be a nonabelian S-orbit of length p^2 . Then $S^\Gamma \simeq S/U$. Let $T_1, \ldots, T_p$ be the p distinct subgroups of S containing U , $|S : T_i| = p^2$, which fix points of Γ , and let Z be the subgroup of of index p^2 containing U such that $Z/U = Z(S/U)$. Clearly $T_1, \ldots, T_p$ fix setwise the unique set of blocks of length p of S in Γ , and so are subgroups of R . Also since $Z \trianglelefteq S$, the Z-orbits in Γ are blocks for S and so $Z \subseteq R$. Then $T_1, \ldots, T_p, Z$ are all the subgroups of R of index p containing U .

Since the T_i are not normal in S , each fixes exactly p points of every nonabelian S-orbit of length p^2 and no other points of $\text{supp } S = \text{supp } R$. Let Σ be the union of the nonabelian S-orbits of length p^2 . If $\Sigma' = \text{fix } U - (\Sigma \cup \text{fix } S)$ contains a point β then $U \subset R_\beta \subset R$, and hence $R_\beta = Z$, and $\Sigma' = \text{fix } Z - \text{fix } S$.

LEMMA 4.9. $\Sigma' = \text{fix } Z - \text{fix } R = \text{supp } S - (\Sigma \cup \text{supp } U)$ *is nonempty.*

Proof. Suppose first that $|P| = p^4$; that is, $U = 1$. If Σ' is

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

empty then $\operatorname{supp} S = \Sigma$ and each long S-orbit has length p^2. Now, by Lemma 4.6, $S = RT'$, for some $T' \sim T_1$, and hence T' permutes every point of $\Sigma = \operatorname{supp} R$, a contradiction as

$$|\operatorname{supp} T'| = |\operatorname{supp} T_1| < |\operatorname{supp} R| .$$

Now suppose that $|P| \geq p^5$, and let $\alpha \in \operatorname{supp} U$. Let T' be a conjugate of R_α in S such that $S = RT'$. Then, as before, $\operatorname{supp} T' \supset \Sigma$. Also $R \cap T' = U \subset T'$ so $\operatorname{supp} T' \supset \operatorname{supp} U$, and hence $\operatorname{fix} T' \subseteq \Sigma' \cup \operatorname{fix} R$. Since $|\operatorname{fix} T'| > |\operatorname{fix} R|$ it follows that $\Sigma' \neq \emptyset$.

Thus $Z = R_\beta$ for β in Σ', and, by Lemma 4.6, there is a conjugate Z' of Z in S such that $S = RZ'$. As in the proof of Lemma 4.9 we see that $\operatorname{fix} Z' \subseteq \Sigma' \cup \operatorname{fix} R = \operatorname{fix} Z$, and hence $\operatorname{fix} Z' = \operatorname{fix} Z$. Then $Y = ZZ'$ is the stabiliser in S of any point of Σ', and as Z' permutes nontrivially all the R-orbits in Σ, Y is transitive on each S-orbit in Σ. Now it follows, from Corollary 4.8, that $U \trianglelefteq N(S)$, and then also $Z \trianglelefteq N(S)$ (for if $g \in N(S)$ then $Z^g \supset U$, and $Z^g/U = Z(S/U) = Z/U$, so $Z^g = Z$).

Let $\alpha \in \operatorname{supp} S$. We claim that R_α is conjugate to Z. By Lemma 4.6 and Corollary 4.8 there is a conjugate T' of R_α such that $S = RT'$ and $U = R \cap T' \subset T'$. Then since $|\operatorname{fix} T'| > |\operatorname{fix} R|$, T' must fix a point of Σ' and so $T' \subseteq Y$. Now Y has exactly $p + 1$ subgroups of index p containing U, and Z, Z', T' are three of these. If $Z' \trianglelefteq S$ then, by [2], 154-155, Z is conjugate to Z' in $N(S) \cap G_\alpha$, a contradiction, since $Z \trianglelefteq N(S)$. Hence Z' is not normal in S. Now since Y, Z, U are all normal in S it follows that S permutes transitively the p subgroups of index p in Y which contain U and are different from Z. Hence $T' \sim_S Z'$, and so $R_\alpha \sim_G Z$.

Now if $|P| \geq p^5$ let $\alpha \in \operatorname{supp} U$. Then R_α is normal in $\langle S_\alpha, R \rangle = S$, and so, by [2], 154-155, R_α is conjugate to Z in $N(S)$, a contradiction since $Z \trianglelefteq N(S)$. Hence $|P| = p^4$, and $\{T_1, \ldots, T_p, Z\}$ is the complete set of subgroups of R of order p. Also Y is the

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

stabiliser in S of all S-orbits of length p, and so Y is weakly closed in S. Hence, by [15], Satz 3, $N(Y)^{\text{fix}Y}$ is 2-transitive. If P is any Sylow p-subgroup of G containing S then Y is normal in P (for if $\alpha \in \text{fix } Y - \text{fix } S$ then $Y \trianglelefteq \langle P_\alpha, S\rangle = P$). All p-orbits in $\text{fix } Y = \Sigma' \cup \text{fix } R$ have length p, and $|P^{\text{fix}Y}| = p^2$ (since S is transitive on all P-orbits of length p^2 and since $|S : Y| = p$). Thus, by [9], either

(I) $N(Y)^{\text{fix}Y} \supseteq \text{Alt}(\text{fix } Y)$ (the alternating group), and, since $|P^{\text{fix}Y}| = p^2$, $|\text{fix } Y| = 2p$; or

(II) $p = 2$, $|\text{fix } Y| = 6$, and $N(Y)^{\text{fix}Y} \simeq \text{PSL}(2, 5)$; or

(III) $p = 3$, $|\text{fix } Y| = 12$, and $N(Y)^{\text{fix}Y} \simeq M_{11}$.

Now define $X = \langle P^* \mid P^* \subseteq N(Y),\ P^* \sim_G P\rangle$.

Then $X \trianglelefteq N(Y)$ and every X-orbit Γ in $\text{supp } Y$ is a Y-orbit; X^Γ is transitive of degree p^2 with a transitive normal p-subgroup Y^Γ. It follows that the only possible nonabelian simple factor of $X^{\text{supp}Y}$ with order divisible by p is $\text{PSL}(2, p)$. However $X^{\text{fix}Y}$ contains an insoluble factor given by (I)-(III) above and hence the kernel of X on $\text{supp } Y$ is nontrivial and therefore is transitive on $\text{fix } Y$, a contradiction to [14], 13.5.

This completes the proof of the theorem.

References

[1] Alfred Bochert, "Ueber die Classe der transitiven Substitutionengruppen", *Math. Ann.* 40 (1892), 176-193.

[2] W. Burnside, *Theory of groups of finite order*, 2nd ed. (Cambridge University Press, Cambridge, 1911; reprinted Dover, New York, 1955).

[3] Daniel Gorenstein, *Finite groups* (Harper and Row, New York, Evanston, London, 1968).

https://doi.org/10.1017/S0004972700024424 Published online by Cambridge University Press

[4] Philip J. Greenberg, *Mathieu Groups* (Lecture Notes, Courant Institute of Mathematical Sciences, New York University, New York, 1973).

[5] Noboru Itô, "Über die Gruppen $PSL_n(q)$ die eine Untergruppe von Primzahlindex enthalten", *Acta Sci. Math.* 21 (1960), 206-217.

[6] William M. Kantor, "Jordan groups", *J. Algebra* 12 (1969), 471-493.

[7] William M. Kantor, "Primitive groups having transitive subgroups of smaller, prime power degree", *Israel J. Math.* (to appear).

[8] Cheryl E. Praeger, "Sylow subgroups of transitive permutation groups", *Math. Z.* 134 (1973), 179-180.

[9] Cheryl E. Praeger, "On the Sylow subgroups of a doubly transitive permutation group", *Math. Z.* 137 (1974), 155-171.

[10] Cheryl E. Praeger, "On the Sylow subgroups of a doubly transitive permutation group II", *Math. Z.* (to appear).

[11] Cheryl E. Praeger, "Primitive permutation groups containing a p-element of small degree, p a prime", *J. Algebra* 34 (1975), 540-546.

[12] J.-A. de Séguier, *Théorie des groupes finis* (Gauthier-Villars, Paris, 1912).

[13] Charles C. Sims, "Computational methods in the study of permutation groups", *Computational problems in abstract algebra*, 169-183 (Proc. Conf. Oxford, 1967. Pergamon, Oxford, London, Edinburgh, New York, Toronto, Sydney, Paris, Braunschweig, 1970).

[14] Helmut Wielandt, *Finite permutation groups* (translated by R. Bercov. Academic Press, New York, London, 1964).

[15] Ernst Witt, "Die 5-fach transitiven Gruppen von Mathieu", *Abh. Math. Sem. Univ. Hamburg* 12 (1938), 256-264.

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra, ACT.