TRANSITIVE PERMUTATION GROUPS OF PRIME DEGREE, IV: A PROBLEM OF MATHIEU AND A THEOREM OF ITO

By PETER M. NEUMANN

[Received 1 February 1974]

1. Mathieu's problem

In this paper I shall apply the results of [**19**] to an insoluble transitive permutation group G of prime degree p in which a Sylow p-normaliser has order $\frac{1}{2}(p-1)p$, the largest order possible if G is not to contain odd permutations. Although these form a very special class of groups, interest in them goes back a hundred years to a very enjoyable paper of Émile Mathieu [**14**]. His main theme concerns groups of degree p where $p = 2q+1$ and q is also prime, especially groups of degrees 7, 11, and 23. In an earlier paper ([**13**], p. 311) he had shown that if G is insoluble and consists of even permutations then the Sylow p-normaliser (to which, of course, he does not refer in these terms) must have order qp, and at the end of [**14**] he asks generally what groups can occur if the Sylow p-normaliser has order $\frac{1}{2}(p-1)p$. He goes on to suggest that if p is 13, 17, or 19 then there is only the alternating group A_p. But here he is in error since the group $\Sigma L(2, 16)$, the extension of the group of unimodular 2 by 2 matrices over GF(16) by its group of field automorphisms, which is transitive of degree 17 on the projective line over GF(16), has Sylow 17-normaliser of order 8.17.

Even now, a century later, very few of these groups are known: only the alternating groups A_p, the group $\Sigma L(2, 16)$ of degree 17, and the 'exceptional' groups $PSL(2, 7)$, $PSL(2, 11)$, M_{11}, and M_{23} of degrees 7, 11, 11, and 23 respectively (see [**18**] for a fuller discussion). It is tempting to conjecture that there are no more, but this is only an optimistic guess for we have very little satisfactory evidence. My aim is to add a little to our general knowledge of the problem, and to show that in many cases G must be highly transitive.

Mathieu was also interested in groups X of degree $p+1$ such that $PSL(2, p) < X \leqslant A_{p+1}$. In § 2 I shall show that such a group must be 4-fold transitive if $p > 7$, and that in many cases $PSL(2, p)$ is a maximal proper subgroup of the alternating group A_{p+1}.

Throughout this paper G denotes an insoluble transitive group of prime degree p in which the Sylow p-normaliser has order $\frac{1}{2}(p-1)p$, and other

notation is continued from the preceding article [**19**]. The following theorem is a direct consequence of Theorems 4.1 and 5.1 of [**19**].

THEOREM 1.1. (i) *If* $p \equiv 1 \mod 4$ *then* G *is a little generously* 3-*transitive.*

(ii) *If* $p \equiv 3 \mod 4$ *then either* G *is* 3-*transitive or a two-point stabiliser* $G_{\alpha\beta}$ *has* 2 *orbits in* $\Omega \setminus \{\alpha, \beta\}$.

The next lemma brings us even closer to 3-transitivity and extends a result of Wielandt (see Ito [**7**]).

LEMMA 1.2. *If* $p > 7$ *then* G_α *is primitive on* $\Omega \setminus \{\alpha\}$.

Proof. If G is 3-transitive then G_α is 2-transitive and certainly primitive. Therefore we may assume that $G_{\alpha\beta}$ has two orbits Γ_1, Γ_2 in $\Omega \setminus \{\alpha, \beta\}$. Since $|\Gamma_1| + |\Gamma_2| = p - 2$ which is odd, $|\Gamma_1|$ and $|\Gamma_2|$ must be different. Therefore Γ_1 and Γ_2 are orbits for $G_{\{\alpha,\beta\}}$.

Suppose now that G_α is imprimitive on $\Omega \setminus \{\alpha\}$. A block of imprimitivity containing β is a union of $G_{\alpha\beta}$-orbits and we may therefore assume that it is $\{\beta\} \cup \Gamma_1$. Let $\Gamma := \{\alpha\} \cup \{\beta\} \cup \Gamma_1$. The group $G_{\{\Gamma\}}$ is 2-transitive (in fact 3-transitive) on Γ because, firstly, $G_{\alpha\{\Gamma\}}$ is transitive on the block of imprimitivity $\{\beta\} \cup \Gamma_1$, that is, on $\Gamma \setminus \{\alpha\}$, and secondly, $G_{\{\Gamma\}} \geqslant G_{\{\alpha,\beta\}}$ which puts α and β in the same $G_{\{\Gamma\}}$-orbit. It follows (see [**1**], p. 270, or [**17**], p. 464) that if $\mathscr{B} := \{\Gamma g \mid g \in G\}$ then $\mathscr{B}$ is the family of 'blocks' in a 2-design on Ω in which $\lambda = 1$: that is, any pair of points of Ω is contained in one and only one member of $\mathscr{B}$. If $k := |\Gamma|$ then a well-known counting argument shows that the number of blocks must be $p(p-1)/k(k-1)$.

Now put $L := N(P)_{\{\Gamma\}}$ and $l := |L|$. Certainly $L \cap P = 1$, and so L has one fixed point and $(p-1)/l$ orbits of length l in Ω. Since Γ is a union of L-orbits it follows that $k = |\Gamma| \geqslant l$. On the other hand, Γ has $|N(P) : L|$, that is, $p(p-1)/2l$ translates under $N(P)$. Therefore

$$|\mathscr{B}| = p(p-1)/k(k-1) \geqslant p(p-1)/2l \geqslant p(p-1)/2k.$$

It follows that $k \leqslant 3$ and therefore that our block design is a Steiner triple system. Furthermore, the fact that $G_{\alpha\beta}$ is transitive on $\Omega \setminus \Gamma$ means that G, as a group of automorphisms of the system, is transitive on triangles. By a theorem of M. Hall ([**5**], Theorem 4.3, or see Kantor [**12**]), G must be a subgroup of $\mathrm{GL}(n, 2)$ or of $\mathrm{AGL}(n, 3)$ for some n, acting on projective $(n-1)$-space over GF(2) or affine n-space over GF(3), respectively. Of these only subgroups of $\mathrm{GL}(n, 2)$ can have prime degree, and only for $n = 3$, $p = 7$ do we find that t (which is $|N(P) : P|$) can be $\frac{1}{2}(p-1)$. This completes the proof.

COROLLARY 1.3. *If $p = q+2$ where q is prime and $q > 5$ then G is 5-fold transitive.*

Proof. If $G_{\alpha\beta}$ is not transitive on $\Omega \setminus \{\alpha, \beta\}$ then its two orbits must have co-prime lengths. This is not possible in a primitive group such as G_α (see Wielandt [**24**], Theorem 17.5, or D. G. Higman [**6**], Lemma 5). Therefore G is 3-transitive, and since q is certainly not a Mersenne prime when $q+2$ is prime, it follows from Corollary 2 of [**15**] or Corollary 4.4 of [**19**] that G is 5-transitive, and even a little bit more.

In the case when $p = 2q+1 = 4r+3 > 23$, and q, r are also prime numbers we know ([**16**]) that G is the alternating group A_p. Corollary 1.3 yields results of a similar nature.

COROLLARY 1.4. *If*
(i) $p = q+2 = 2r+3 > 9$ *or if*
(ii) $p = q+2 = 3r+4 > 13$,
where r is prime, then $G = A_p$.

This corollary follows directly from Corollary 1.3 and theorems of Jordan ([**11**], or [**24**], Theorem 13.10). The primes of type (i) below 1000 are

$$13, \quad 61, \quad 109, \quad 181, \quad 229, \quad 349;$$

and those of type (ii) below 1000 are

$$19, \quad 43, \quad 61, \quad 73, \quad 181, \quad 241, \quad 271,$$
$$313, \quad 421, \quad 523, \quad 601, \quad 811, \quad 883.$$

2. On groups which contain PSL(2, p)

The results of § 1 can be applied to the problem of finding permutation groups X of degree $p+1$ such that $\mathrm{PSL}(2,p) \leqslant X \leqslant A_{p+1}$. Mathieu's original exercise ([**14**]) concerned such groups particularly. It has been pointed out to me that these groups are of some interest in algebraic coding theory (see [**20**], and references quoted there), and they also arise in a more introverted context (see [**18**], p. 531, for a little discussion). If $X > \mathrm{PSL}(2,p)$ then a stabiliser X_∞ is a group G which is insoluble of degree p and in which $N(P)$, since it contains a Sylow p-normaliser of $\mathrm{PSL}(2,p)$, has order $\frac{1}{2}(p-1)p$.

THEOREM 2.1. *If $p > 7$ and $\mathrm{PSL}(2,p) < X \leqslant A_{p+1}$ then X is 4-transitive.*

Proof. Take the projective line over GF(p) to be $\Omega \cup \{\infty\}$. As observed above, if $G := X_\infty$ then G is a group of the kind treated in § 1. If

$p \equiv 1 \bmod 4$ then, by Theorem 1.1, that is, by Theorem 4.1 of [**19**], G is a little generously 3-transitive on Ω, and it follows easily that X is almost generously 4-transitive ([**17**]). Suppose then that $p \equiv 3 \bmod 4$. From Lemma 1.2 we know that G is primitive on $\Omega \setminus \{\alpha\}$ and so, since $G_\alpha \leqslant X_{\{\infty,\alpha\}}$, also $X_{\{\infty,\alpha\}}$ is primitive. Now $(\mathrm{PSL}(2,p))_{\{\infty,\alpha\}}$ is a dihedral group of order $p-1$ which, since $p \equiv 3 \bmod 4$, acts regularly on $\Omega \setminus \{\alpha\}$. By a theorem of Wielandt ([**22**], or [**24**], Theorem 25.6(i)), $X_{\{\infty,\alpha\}}$ is 2-transitive on $\Omega \setminus \{\alpha\}$. It follows immediately that $X_{\infty\alpha}$ is 2-transitive and so X is 4-transitive on the projective line $\Omega \cup \{\infty\}$.

COROLLARY 2.2. *If $p > 7$ and $p-2$ is prime, and if*

$$\mathrm{PSL}(2,p) < X \leqslant \mathrm{A}_{p+1}$$

then $X = \mathrm{A}_{p+1}$.

Proof (compare Corollary 1.3). If $q := p-2$ then since X is 4-transitive it contains a q-cycle with three fixed points, and Jordan's theorem ([**10**], or [**24**], Theorem 13.9) implies that $X = \mathrm{A}_{p+1}$.

3. A theorem of Ito

We turn now to the case where $p = 2q+1$ and q is prime.

THEOREM (N. Ito). *G is 4-fold transitive unless p is 5, 7, or 11 and G is $\mathrm{PSL}(2,p)$.*

Ito's proof ([**8**], [**9**]) of this remarkable theorem is long and intricate. The proof that I shall describe is perhaps no easier, but at least the proof of 3-transitivity is considerably shorter and it offers an excellent illustration of the power of modular representation theory in the service of permutation groups.

The Sylow p-normaliser $N(P)$ is of the form PQ where $Q = \langle b \rangle$ is a cyclic group of order q. For $p > 5$ we may clearly assume that $G < \mathrm{A}_p$ since the alternating group certainly is 4-transitive. It then follows from an old theorem of Jordan ([**10**], see [**24**], Theorem 13.9) that Q is a Sylow q-subgroup of G. Since $C_{\mathrm{A}_p}(Q)$ is elementary abelian of order q^2, we have that $C_G(Q) = Q$ and therefore that $N_G(Q) = QR$, where $R = \langle c \rangle$ is a non-trivial cyclic group whose order r divides $q-1$ (the non-triviality of R comes directly from Burnside's Transfer Theorem: but it was proved by Mathieu, in [**13**], pp. 317–19, by purely combinatorial arguments). If Q has α as its one fixed point, and Γ_1, Γ_2 as its two q-cycles, then R fixes α and either interchanges or fixes setwise Γ_1 and Γ_2. In the latter case the generator c would be a product of one transposition and $2(q-1)/r$ disjoint r-cycles, which is an odd permutation. This contradicts our hypothesis and shows that c fixes Γ_1 and Γ_2 setwise, it has one fixed point β in Γ_1,

one fixed point γ in Γ_2, and apart from the three fixed points it is a product of $(q-1)/r$ disjoint r-cycles in each of Γ_1 and Γ_2.

The remainder of the proof is given in §§ 6 and 7. The next section contains some character-theoretic preparations, and § 5 proves a necessary lemma about primitive groups of degree $2q$.

4. Some character theory

This section is a continuation of § 2 in [**19**]. If M is a projective indecomposable RG-module with character τ then the dual module $\mathrm{Hom}_R(M, R)$ is also projective indecomposable and its character is the complex conjugate $\bar{\tau}$. Therefore the map $\chi \mapsto \bar{\chi}$, $\tau \mapsto \bar{\tau}$, is an automorphism of the Brauer tree associated with $B_0(G)$. Its fixed point set consists, of course, of the real-valued characters in $B_0(G)$, and it is a theorem of Brauer and Tuan ([**2**], p. 958, and [**21**], pp. 124–25) that these form a connected subtree which is simply a chain: ×——○——×——···○——×. This chain is referred to as the real stem of the tree. The Brauer tree may be drawn so as to lie symmetrically above and below its real stem, and so that complex conjugation is represented by reflection in the line of the stem. If there are u pairs of complex conjugate characters and v real characters (including χ_t, the sum of the exceptional characters, which is to be counted as one only) then $2u+v = t+1$. Of course one end of the real stem is χ_0; if the sign associated with the other end is ε then $\varepsilon = (-1)^{v-1}$; consequently, if $\varepsilon = 1$ then t is even and if $\varepsilon = -1$ then t is odd, a useful observation which I owe to David Cooper.

In the case of our group G of degree p we know that χ_0 and χ_1 are real-valued, and as χ_2 is the only other character adjacent to χ_1 it too must be part of the real stem of $B_0(G)$.

In what follows I shall be using the modular theory both for the prime p and the prime q. Wherever necessary I shall use a prefix or a subscript to guard against ambiguity.

Now we return to our group G of degree $p = 2q+1$. Here is a useful technicality.

LEMMA 4.1. *If χ is an irreducible character of degree p then χ represents an end-node in the Brauer q-tree.*

Proof. Let X be an R_qG-module with character χ and consider its reduction $\bar{X}$ modulo q. Since PQ is a Frobenius group it has two faithful irreducible representations in any field of characteristic different from p, and they both have degree q. Since $\bar{X}$ represents G faithfully it is not hard to see that it has one linear composition factor and two non-linear composition factors as a $\bar{K}_qPQ$-module. It follows that if $\bar{X}$ is reducible as

a G-module then one of its composition factors has degree q or $2q$: but the degrees of the modular irreducibles in q-$B_0(G)$ are not divisible by q. Therefore $\overline{X}$ is irreducible, and χ is an end-node in the Brauer q-tree.

If $r < q-1$, so that the q-exceptional characters are easily distinguishable from other characters in the principal q-block of G, then I shall use $\psi_1, \ldots, \psi_{(q-1)/r}$ as names for these exceptional characters. Since they are certainly p-rational they must have degrees -1, 0, or 1 modulo p.

LEMMA 4.2. *Suppose that $r < q-1$ and that the q-exceptional characters are constituents of ξ. Then either $\psi_i(1) = (r-1)p+1$ or $\psi_i(1) = rp$.*

Proof. Suppose that $\psi_i(1) = kp+\varepsilon$ where $\varepsilon \in \{-1, 0, 1\}$. The proof of Lemma 3.4 of [**19**] shows that the restriction $(\psi_i)_{N(P)}$ has precisely $k+\varepsilon$ linear constituents (counting multiplicities) and it follows that

$$(\psi_i)_Q = 2k\rho_Q + \Lambda_i,$$

where ρ_Q denotes the character of the regular representation of Q and Λ_i is a sum of $k+\varepsilon$ linear characters of Q. If the ψ_i are constituents of $\chi^{(p-2,2)}$ or of $\chi^{(p-2,1^2)}$ then we know from Lemma 3.3 of [**19**] that $\sum_1^{(q-1)/r} \Lambda_i$ is multiplicity free. In particular Λ_i does not contain the principal character of Q and therefore $\psi_i(1) \equiv +r \bmod q$. Consequently $k+\varepsilon = r$. If now $\varepsilon = -1$ then the degree of $\sum \psi_i$ is

$$((r+1)p-1)\frac{(q-1)}{r} = p(q-1)+(p-1)\frac{(q-1)}{r} > pq,$$

which is impossible if $\sum \psi_i$ is to be contained in $\chi^{(p-2,2)}$ or in $\chi^{(p-2,1^2)}$. Therefore either $\varepsilon = 1$ and $\psi_i(1) = (r-1)p+1$ or $\varepsilon = 0$ and $\psi_i(1) = rp$.

5. Primitive groups of degree $2q$

In case our group G is not 3-transitive then we know that the stabiliser G_α is a primitive group (Lemma 1.2) of rank 3 (Theorem 1.1(ii)) on $\Omega \setminus \{\alpha\}$, and of course its degree is $2q$. Primitive groups of degree $2q$ which are not 2-transitive have been studied by Wielandt ([**23**], [**24**], pp. 93–103), and I shall call them Wielandt groups. They can exist only if $q = 2l^2+2l+1$ for some integer l; they always do have rank 3 and the orbit lengths of a stabiliser are 1, $l(2l+1)$, $(l+1)(2l+1)$. In a Wielandt group the Sylow q-subgroup Q is automatically cyclic of order q, self-centralising, and its normaliser $N(Q)$ is QR where R is a cyclic group whose order r divides $q-1$.

LEMMA 5.1. *Let X be a Wielandt group as described above and suppose that X contains no odd permutations. Then r divides l or r divides $l+1$.*

Proof. Let c be a generator for R. As on p. 55 one finds that c fixes two points β and γ, one in each Q-orbit, and is a product of $2(q-1)/r$ disjoint r-cycles. Let Γ_1, Γ_2 be the X_β-orbits of lengths $l(2l+1)$ and $(l+1)(2l+1)$ respectively. Since $c \in X_\beta$ it fixes Γ_1 and Γ_2 as sets: so if $\gamma \in \Gamma_2$ then

$$|\Gamma_1| = l(2l+1) \equiv 0 \mod r$$

and

$$|\Gamma_2| = (l+1)(2l+1) \equiv 1 \mod r.$$

The latter congruence tells us that r and $2l+1$ are co-prime, and so from the former we see that r divides l. A similar argument shows that if $\gamma \in \Gamma_1$ then r divides $l+1$.

6. The triple transitivity of G

We suppose throughout this section that our group G is not $\mathrm{PSL}(2,p)$ (for $p = 7$ or $p = 11$) and that G is not 3-transitive, and we shall seek a contradiction. Since G is not 3-transitive we know that $\chi_1 \subseteq \chi^{(p-2,2)}$ and therefore that $\tau_1 = \chi_1 + \chi_2 \subseteq \chi^{(p-2,2)}$. Recall that in [**19**], Theorem 5.1(i), I showed that χ_2 is not the sum of the p-exceptional characters. Therefore χ_2 is irreducible and $\chi_2(1) \equiv 1 \bmod p$. Now we distinguish two possibilities: either χ_2 is q-rational or it is not.

LEMMA 6.1. *If χ_2 is not q-rational then*

$$\chi^{(p-2,2)} = \psi_1 + \ldots + \psi_{(q-1)/r} + \varphi_1 + \ldots + \varphi_{(q-1)/r},$$

where the q-exceptional characters ψ_i have degree $(r-1)p+1$, and $\varphi_1, \ldots, \varphi_{(q-1)/r}$ are characters of degree $p-1$ such that $\sigma_i := \psi_i + \varphi_i$ is projective indecomposable relative to p. (Moreover, $\chi_2 = \psi_1$, $\chi_1 = \varphi_1$, and $\tau_1 = \sigma_1$.)

Proof. If χ_2 is ψ_1 then, since the q-exceptional characters are q-conjugate, while $\chi^{(p-2,2)}$ is rational-valued, all the ψ_i appear in $\chi^{(p-2,2)}$. Moreover, since $\chi_2(1) \equiv 1 \bmod p$ it follows that $\psi_i(1) \equiv 1 \bmod p$ and therefore, by Lemma 4.2, that $\psi_i(1) = (r-1)p+1$. Since $\chi^{(p-2,2)}$ is the character of a projective module there must exist p-projective indecomposables $\sigma_1, \ldots, \sigma_{(q-1)/r}$ such that $\sigma_i = \psi_i + \varphi_i$ for some $\varphi_i \in p\text{-}B_0(G)$ and

$$\sigma_1 + \ldots + \sigma_{(q-1)/r} \subseteq \chi^{(p-2,2)}.$$

If $\varphi_i(1) = k_i p - 1$ then

$$\sigma_1(1) + \ldots + \sigma_{(q-1)/r}(1) = \sum_1^{(q-1)/r} (r-1+k_i)p \leqslant (q-1)p = \chi^{(p-2,2)}(1).$$

This inequality gives that $\sum_1^{(q-1)/r} k_i \leqslant (q-1)/r$, and since $k_i \geqslant 1$ it follows that $k_i = 1$ for all i. Thus $\varphi_i(1) = p-1$.

LEMMA 6.2. *χ_2 must be q-rational.*

Proof. Suppose the lemma is not true, so that the decomposition of $\chi^{(p-2,2)}$ into irreducible constituents is as described above. Since χ_2 is part of the real stem of the Brauer p-tree, and since $\psi_1, \ldots, \psi_{(q-1)/r}$ are algebraic conjugates of χ_2, they too are all real-valued. Now the complex conjugate $\bar{\sigma}_i$ is a p-projective indecomposable, and it is contained in $\chi^{(p-2,2)}$; therefore

$$\bar{\sigma}_i = \bar{\psi}_i + \bar{\varphi}_i = \psi_i + \varphi_j$$

for some j. Then j must be i, else φ_j would be adjacent both to ψ_i and to ψ_j in the Brauer p-tree, which we know to be impossible (Lemma 2.1 of [**19**]). Thus $\varphi_1, \ldots, \varphi_{(q-1)/r}$ are also in the real stem of the Brauer p-tree. From Lemma 2.1 of [**19**] again, all except φ_1 (which is χ_1) must be end-nodes in the Brauer p-tree. But of course the real stem has only one end other than χ_0. Consequently $(q-1)/r = 2$ and φ_2 is the non-trivial end of the real stem. Now we apply Lemma 5.1:

$$l(l+1) = (q-1)/2 = r \leqslant l+1.$$

Hence $l = 1$, $q = 5$, $p = 11$, and in fact G would have to be PSL(2, 11) which we had excluded by assumption. Therefore χ_2 must be q-rational, as claimed.

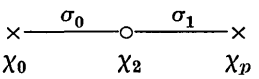
Since $\chi_2 \subseteq \chi^{(p-2,2)}$ and χ_2 is q-rational it follows that the restriction $(\chi_2)_{PQ}$ contains each non-principal linear character once and only once, and hence that $\chi_2(1) = (q-2)p+1$. Therefore

$$\chi^{(p-2,2)} = \chi_1 + \chi_2$$

and

$$\chi^{(p-2,1^2)} = \chi_2 + \chi_p,$$

where χ_p is an irreducible character of degree p. Now the modules $X_q := R_q\Omega^{(2)}$, $Y_q := R_q\Omega^{(2)}$, and Z_q where $X_q \cong Y_q \oplus Z_q$ are all q-projective (see [**15**], Lemma 3, and the argument which follows). Moreover, χ_1 has q-defect 0 since $\chi_1(1) = 2q$. It follows that $\sigma_0 := \chi_0 + \chi_2$ must be the q-projective indecomposable in η (the character afforded by Y_q) containing χ_0, and $\sigma_1 := \chi_2 + \chi_p$ must also be q-projective indecomposable. Thus



is part of the real stem of the Brauer q-tree. However, by Lemma 4.1, χ_p is an end-node of the Brauer q-tree, and so this is the whole real stem. Since one of the nodes of the real stem always corresponds to the exceptional characters, and since both χ_2 and χ_p are irreducible, it follows that $r = q-1$. Now, applying Lemma 5.1 once more, we get a manifest contradiction. This proves that if G is not PSL(2, 7) or PSL(2, 11) then G must be 3-fold transitive.

7. The 4-fold transitivity of G

LEMMA 7.1. *If χ is an irreducible constituent of $\chi^{(p-2,2)}$ or of $\chi^{(p-2,1^2)}$ then $\chi(1) > p$.*

Proof (cf. [9], Lemma 3). Let $H := G_\alpha$. Since H is now known to be 2-transitive of degree $2q$ it is not hard to see that the derived group H' is simple and, from Wielandt's theorem, that H' is 2-transitive on $\Omega\setminus\{\alpha\}$. The character afforded by the action of H on $(\Omega\setminus\{\alpha\})^{(2)}$ is just the restriction to H of $\chi_0+\chi^{(p-2,2)}+\chi^{(p-2,1^2)}$. Since H' is 2-transitive

$$\langle 1, \chi_0+\chi^{(p-2,2)}+\chi^{(p-2,1^2)}\rangle_{H'} = 1,$$

and therefore if λ is any linear character of H then

$$\langle \lambda, \chi^{(p-2,2)}+\chi^{(p-2,1^2)}\rangle_H = 0.$$

Let $\pi = 1+\pi_1$ be the permutation character of H on $\Omega\setminus\{\alpha\}$. Since H is 2-transitive π_1 is irreducible, and since ξ is the induced character π^G, while $\chi_0+\chi_1$ is 1_H^G, it follows that

$$\pi_1^G = \chi_1+\chi^{(p-2,2)}+\chi^{(p-2,1^2)}.$$

By Frobenius multiprocity, if χ is an irreducible constituent of $\chi^{(p-2,2)}$ or of $\chi^{(p-2,1^2)}$ then χ_H involves π_1. Consequently, if $\chi(1) = p-1$ then $\chi_H = \lambda+\pi_1$, where λ is a linear character of H. This is impossible as we have just seen. If $\chi(1) = p$ then $\chi_H = \mu+\pi_1$, where μ has degree 2. If μ were reducible then χ_H would have linear constituents, which is not the case. If μ were irreducible, then, since the only proper factor groups of H are cyclic (of order dividing $q-1$), it follows that μ would be faithful. But this is impossible because then H, being a group with trivial centre and with a faithful irreducible complex representation of degree 2, would have to be dihedral of order $2n$ where n is odd, which is certainly not the case. Thus there cannot be constituents of degree $p-1$ or p in $\chi^{(p-2,2)}$ or in $\chi^{(p-2,1^2)}$.

LEMMA 7.2. *If G is not 4-transitive then $\chi^{(p-2,1^2)}$ is irreducible and $\chi^{(p-2,2)} = \psi_1+\ldots+\psi_{(q-1)/r}$.*

Proof. Consider first the decomposition of $\chi^{(p-2,2)}$ as a sum of irreducible characters. By Lemma 7.1 it has no constituents of degree $p-1$ and therefore, by Lemma 4.2 and the argument of Lemma 6.1, either all its constituents are q-rational or $\chi^{(p-2,2)}$ is the sum $\psi_1+\ldots+\psi_{(q-1)/r}$. If every constituent is q-rational then, since we know that every constituent is also p-rational, it follows that either $\chi^{(p-2,2)} = \varphi_1+\varphi_2$, where $\varphi_1(1) = (q-2)p+1$ and $\varphi_2(1) = p-1$, or $\chi^{(p-2,2)}$ is irreducible. The former possibility is again excluded by Lemma 7.1. If $\chi^{(p-2,2)}$ is irreducible then G acts as a group

of rank 3 on $\Omega^{(2)}$ and it is easy to see then that G is 4-transitive on Ω (cf. [17]). Suppose therefore that G is not 4-transitive. Then $\chi^{(p-2,2)} = \psi_1 + \ldots + \psi_{(q-1)/r}$ and $\psi_i(1) = rp$. It follows that χ_2 is q-rational and therefore that either $\chi_2(1) = (q-2)p+1$ or $\chi_2(1) = (q-1)p+1$. In the former case we would have $\chi^{(p-2,1^2)} = \chi_2 + \varphi$ where $\varphi(1) = p$, and this is excluded by Lemma 7.1. Therefore $\chi_2(1) = (q-1)p+1 = \chi^{(p-2,1^2)}(1)$. Hence $\chi^{(p-2,1^2)}$ is χ_2 and is irreducible, which is what we wished to show.

The proof of 4-transitivity can now be completed as follows. Since $\chi^{(p-2,2)}$ is irreducible we know that G is generously 3-transitive ([17]), and certainly that every suborbit of G acting on $\Omega^{(2)}$ is self-paired. Since the character η corresponding to this permutation representation is multiplicity-free, every constituent of η is real-valued. (This is a special case of a well-known, more general theorem, similar to Theorem A of [3], for which I have been unable to find an appropriate reference. This special case may be proved quite simply as follows: since η is multiplicity-free the centraliser ring V of this permutation representation is commutative ([24], Theorem 29.3) and so there is a unitary matrix U such that $U^{-1}AU$ is a diagonal matrix for all $A \in V$. Moreover, V is spanned by symmetric matrices ([24], Theorem 28.9, and therefore U may be taken to have real coefficients; then $U^{-1}G^*U$ is completely reduced ([24], p. 85) and so the real field is a splitting field for η.) If G were not 4-transitive then the q-exceptional characters $\psi_1, \ldots, \psi_{(q-1)/r}$ would be constituents of η (Lemma 7.2), and hence would be real-valued. Therefore b would be conjugate to b^{-1}, that is, r would have to be even; and now the combinatorial computations of Fryer ([4]), as extended by Ito to complete his proof ([9], pp. 161–65), show that G must be A_p, which is a contradiction.

Acknowledgements. I thank B. N. Cooperstein, J. E. McLaughlin, and Richard Rasala, whose interest and encouragement helped me considerably to decrease the length while increasing the scope of § 2 of this paper. It is a pleasure also to be able to acknowledge gratefully the generosity and charming hospitality of the Mathematics Department of the University of Michigan at Ann Arbor, where I was given the opportunity to complete this work and to write these two papers.

REFERENCES

1. M. D. Atkinson, 'Two theorems on doubly transitive permutation groups' *J. London Math. Soc.* (2) 6 (1973) 269–74.
2. Richard Brauer, 'Investigations on group characters', *Ann. of Math.* 42 (1941) 936–58.
3. J. S. Frame, 'The double cosets of a finite group', *Bull. Amer. Math. Soc.* 47 (1941) 458–67.

4. K. D. Fryer, 'A class of permutation groups of prime degree', *Canad. J. Math.* 7 (1955) 24–34.
5. Marshall Hall, Jr, 'Group theory and block designs', *Proceedings international conference on theory of groups, Canberra* 1965, edited by L. G. Kovács and B. H. Neumann (Gordon and Breach, New York, 1967), 115–44.
6. Donald G. Higman, 'Finite permutation groups of rank 3', *Math. Z.* 86 (1964) 145–56.
7. Noboru Ito, 'A note on transitive permutation groups of degree p', *Osaka Math. J.* 14 (1962) 213–18.
8. —— 'Transitive permutation groups of degree $p = 2q+1$, p and q being prime numbers, II', *Trans. Amer. Math. Soc.* 113 (1964) 454–87.
9. —— 'Transitive permutation groups of degree $p = 2q+1$, p and q being prime numbers, III', ibid. 116 (1965) 151–66.
10. Camille Jordan, 'Sur la limite de transitivité des groupes non alternés', *Bull. Soc. Math. France* 1 (1872–73) 40–71; *Œuvres, I*, edited by J. Dieudonné (Gauthier-Villars, Paris, 1961), 365–96.
11. —— 'Mémoire sur les groupes primitifs', *Bull. Soc. Math. France* 1 (1872–73) 175–221; *Œuvres, I*, edited by J. Dieudonné (Gauthier-Villars, Paris, 1961) 397–443.
12. William M. Kantor, 'On 2-transitive groups in which the stabilizer of two points fixes additional points', *J. London Math. Soc.* (2) 5 (1972) 114–22.
13. Émile Mathieu, 'Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables', *J. Math. Pures Appl. (Liouville)* (2e *série*) 6 (1861) 241–323.
14. —— 'Sur la fonction cinq fois transitive de 24 quantités', ibid. 18 (1873) 24–46.
15. Peter M. Neumann, 'Transitive permutation groups of prime degree', *J. London Math. Soc.* (2) 5 (1972) 202–8.
16. —— 'Transitive permutation groups of prime degree, II: a problem of Noboru Ito', *Bull. London Math. Soc.* 4 (1972) 337–39.
17. —— 'Generosity and characters of multiply transitive permutation groups', *Proc. London Math. Soc.* (3) 31 (1975) 457–81.
18. —— 'Transitive permutation groups of prime degree', *Proceedings international conference on theory of groups, Canberra* 1973, Lecture Notes in Mathematics 372 (Springer-Verlag, Berlin, 1974), 520–35.
19. —— 'Transitive permutation groups of prime degree, III: character-theoretic observations', *Proc. London Math. Soc.* (3) 31 (1975) 482–94.
20. Edward P. Shaughnessy, 'Codes with simple automorphism groups', *Arch. Math. (Basel)* 22 (1971) 459–66.
21. Hsio-Fu Tuan, 'On groups whose orders contain a prime number to the first power', *Ann. of Math.* 45 (1944) 110–40.
22. Helmut Wielandt, 'Zur Theorie der einfach transitiven Permutationsgruppen. II', *Math. Z.* 52 (1949) 384–93.
23. —— 'Primitive Permutationsgruppen vom Grad $2p$', ibid. 63 (1956) 478–85.
24. —— *Finite permutation groups* (Academic Press, New York, 1964).

Queen's College
Oxford OX1 4AW
and
University of Michigan
Ann Arbor, Michigan 48104