FINITE PERMUTATION GROUPS

BY

Martin W. Liebeck

Thesis submitted for the degree of D.Phil. at the University of Oxford.

St. Peter's College,

Oxford.

June 1979.

To my parents.

ACKNOWLEDGMENTS.

It is a pleasure to thank my supervisor Dr. Peter Neumann for his great encouragement and guidance over the past three years. I am also grateful to the Science Research Council for their financial support.

ABSTRACT.

Finite permutation groups (D.Phil. Thesis, Trinity term, 1979).

by Martin W. Liebeck,

St. Peter's College, Oxford.

Two problems in the theory of finite permutation groups are considered in this thesis:

A. transitive groups of degree p, where $p = 4q+1$ and p,q are prime,

B. automorphism groups of 2-graphs and some related algebras.

Problem A should be seen in the following context: in 1963, N.Ito began a study of insoluble, transitive groups G of degree p on a set Ω, where $p = 2q+1$ and p,q are prime, showing among other things, that such a group G is 3-transitive. His methods involve the modular character theory of G for both the primes p and q (developed by R.Brauer). He uses this theory to prove facts about the permutation characters of G associated with $\Omega^{(2)}$ and $\Omega^{\{2\}}$, the sets of ordered and unordered pairs (respectively) of distinct elements of Ω. The first part of this thesis represents an attempt to extend these methods to the case $p = 4q+1$. The main result obtained is

Theorem. Let G be an insoluble, transitive permutation group of degree p, where $p = 4q+1$ and p,q are prime with $p > 13$. Then G is 3-transitive.

Also some progress is made towards a proof that the groups in Problem A are 4-transitive.

In the second part of this thesis (Problem B) certain algebras are defined from 2-graphs as follows: let (Ω, Δ) be a 2-graph, that is, Δ is a set of 3-subsets of a finite set Ω such that every 4-subset of Ω contains an even number of elements of Δ. Write $\Omega = \{e_1, \ldots, e_n\}$. Given any field F of characteristic 2, make $F\Omega$ into an algebra by defining

$$e_i e_j := \sum_{\{e_i, e_j, e_k\} \in \Delta} e_k .$$

It is shown that in many cases, this algebra is a Lie algebra. A study of the derived and lower central series is carried out and is used to show that if G is the automorphism group of one of a fairly large class of 2-graphs (including many regular 2-graphs) then $F\Omega$ has several nontrivial G-submodules. This result is perhaps of interest, since many of the known 2-transitive permutation groups are automorphism groups of regular 2-graphs.

Finally it is shown how to construct Lie algebras in any characteristic from certain graphs.

CONTENTS.

NOTATION.

In this thesis we consider only finite groups. If G is a group and H is a subgroup of G, the following notation is used:

$\lvert G\rvert$	order of G
$\lvert G:H\rvert$	index of H in G
$N_G(H)$	normaliser of H in G
$C_G(H)$	centraliser of H in G
$Z(G)$	centre of G
$H \lhd G$	H is a normal subgroup of G
$\langle g\rangle$	cyclic group generated by the element g of G
$\langle \chi,\psi\rangle_G$	inner product of the characters χ and ψ of G ; $\lVert\chi\rVert_G = \langle\chi,\chi\rangle_G$
$\chi \leq \psi$	$\psi - \chi$ is a character of G or zero (χ and ψ are characters of G)
χ_H, M_H	restriction to H of the character χ or FG-module M (F a field)
χ^G, M^G	induced character or FG-module from the character χ of H or the FH-module M
SG	group algebra of G over the ring S.

The following notation is also used:

$G \times H$	direct product of the groups G and H
$M \otimes N$	tensor product of the modules M and N
$M \oplus N$	direct sum of modules M and N
$\mathbb{C}$	field of complex numbers
$\mathbb{Q}$	field of rational numbers
Z_n	cyclic group of order n.

If G is a permutation group on a set Ω and Γ is a subset of Ω then we write $G_{(\Gamma)}$, $G_{\{\Gamma\}}$ respectively for the pointwise and setwise stabilisers of Γ in G. The group $G^{\Gamma}_{\{\Gamma\}}$ is the permutation group on Γ

induced by $G_{\{\Gamma\}}$. By $\Omega^{(k)}$, $\Omega^{\{k\}}$ we mean respectively the sets of ordered and unordered subsets of Ω of size k.

Reference is made in this thesis to the following well-known permutation groups:

(i) the symmetric and alternating groups S_n, A_n of degree n,

(ii) the affine group $AGL(d,p^r)$ acting with degree p^{rd} on a d-dimensional vector space $V = V(d,p^r)$ over $GF(p^r)$ (p a prime number); $AGL(d,p^r)$ consists of the permutations $\pi_{A,b} : v \rightarrow Av+b$ of V ($A \in GL(V)$, $b \in V$) and can be extended by field automorphisms to the group $A\Gamma L(d,p^r)$,

(iii) the Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$,

(iv) the projective groups $PSL(d,q)$, $PGL(d,q)$ acting on the projective space $PG(d-1,q)$ which consists of the 1-dimensional subspaces of the vector space $V(d,q)$ ($d > 1$, q a prime power); these can be extended by field automorphisms to the groups $P\Sigma L(d,q)$, $P\Gamma L(d,q)$.

"On Monday, when the sun is hot
I wonder to myself a lot:
'Now is it true or is it not,
'That what is which and which is what?'

On Tuesday, when it hails and snows,
The feeling on me grows and grows
That hardly anybody knows
If those are these or these are those.

On Wednesday, when the sky is blue,
And I have nothing else to do,
I sometimes wonder if it's true
That who is what and what is who.

On Thursday, when it starts to freeze
And hoar-frost twinkles on the trees,
How very readily one sees
That these are whose - but whose are these?"

A.A.Milne, 'Winnie-the-Pooh'.

INTRODUCTION.

This thesis is concerned with the following two areas in the theory of finite permutation groups:

A. transitive groups of degree p, where $p = 4q+1$ and p,q are prime numbers,

B. automorphism groups of 2-graphs and some related algebras.

These two subjects will be referred to as Problem A and Problem B; we introduce them separately.

INTRODUCTION TO PROBLEM A.

The search for transitive permutation groups of prime degree goes back as far as 1830, when Abel and Galois studied them in connection with the theory of polynomial equations. One of Galois' theorems says that if G is a soluble, transitive group of prime degree p, then G is a subgroup of the affine group AGL(1,p) acting on the field GF(p). Several nineteenth century mathematicians, notably Mathieu and Jordan, continued the work of Galois and provided the foundations for the rich material published since 1900. There are relatively few known transitive groups of prime degree; those groups G (of degree p) that are known are listed in the following table:

p	G	
p	$G \leqslant AGL(1,p)$	
p	A_p, S_p	
$\frac{q^d-1}{q-1}$	$PSL(d,q) \leqslant G \leqslant P\Gamma L(d,q)$ (q a prime power)	
11	$PSL(2,11)$	exceptional
11	M_{11}	exceptional
23	M_{23}	exceptional

Notice that the "exceptional" primes 11 and 23 are of the form 2q+1 where q is also prime. Indeed, it is on just such an arithmetic accident that Mathieu's discovery of M_{11} and M_{23} depends (see [25]). In 1963, N.Ito began a study of the insoluble transitive groups of degree p, where p = 2q+1 and p,q are prime; in [19] and [20] (see also [29]) it is shown that such groups are 3-transitive and that they are very nearly 4-transitive (the precise result is Theorem 1.15 of this thesis). The methods of Ito and Neumann involve the modular character theory of the groups for both the prime p and the prime q; the p-modular theory gives a certain description of the ordinary characters with respect to the prime p and the q-modular theory gives a description with respect to the prime q. These descriptions are combined with knowledge about characters of permutation groups to give the results mentioned above.

These methods seem to be applicable, more generally, to the study of primitive, insoluble groups of degree n, where the numbers n,n-1 are divisible by large primes p,q respectively. We have already mentioned the case n = p = 2q+1, while in [33] Neumann and Saxl show that if n = 2p = q+1 then, with the exceptions PSL(2,q) and PGL(2,q), the groups are 4-transitive. Note that in these two cases the ratio of n^2 to pq is roughly 2; as this ratio increases, the calculations with characters involved in the methods outlined above, grow very much more complicated. The first part of this thesis concerns the case n = p = 4q+1; here, the ratio of n^2 to pq is approximately 4. The main theorem proved is:

<u>THEOREM 3.1.</u> Let G be an insoluble, transitive permutation group of degree p, where p = 4q+1 and p,q are prime. Then either G is 3-transitive or q = 3, p = 13 and G is PSL(3,3) acting on the projective plane PG(2,3).

Chapter 3 of this thesis consists of a proof of this theorem and some results needed for this proof are given in Chapter 1. In Chapter 2 we prove some general facts about 2-transitive and 3-transitive groups; most of these involve deductions about the way a group G acts on a set Ω from information about the permutation characters ξ, η of G associated with $\Omega^{(2)}$, $\Omega^{\{2\}}$ respectively (where $\Omega^{(2)}$ and $\Omega^{\{2\}}$ are the sets of ordered and unordered pairs of distinct elements of Ω). The most important fact is:

PROPOSITION 2.2. Suppose that G is generously 2-transitive and 2-primitive of degree n on Ω, and let k be the rank of G_α on $\Omega \setminus \{\alpha\}$ (where $\alpha \in \Omega$). Then $\|\xi\| - \|\eta\| \geqslant k^2+k-2$; and if equality holds then either k = 2 or k = 3 and n is even.

This fact is used in the proof of Theorem 3.1. The results in Chapter 2 on 3-transitive groups are used in Chapter 4, where further study of transitive insoluble groups of degree p = 4q+1 is carried out.

INTRODUCTION TO PROBLEM B.

The second part of this thesis concerns algebras derived from certain combinatorial objects called 2-graphs, and the use of these algebras to deduce facts about the automorphism groups of the 2-graphs. Let us define our terms.

Let Ω be a finite set of size n and let $\Delta \subseteq \Omega^{\{3\}}$ (that is, Δ is a set of 3-subsets of Ω). Following G.Higman (see [36]), we say that (Ω, Δ) is a 2-graph if every 4-subset of Ω contains an even number of elements of Δ; it is trivial if Δ is $\emptyset$ or $\Omega^{\{3\}}$; its automorphism group is the set of permutations of Ω which preserve Δ. The 2-graph (Ω, Δ) is regular if every 2-subset of Ω is contained in the same number, a, of elements of Δ.

It can be shown that for a nontrivial regular 2-graph there are nonzero integers r, s such that $a = 2r$ and $n = 2+2r+2s$. Many of the known 2-transitive groups are automorphism groups of nontrivial regular 2-graphs.

Let G be a permutation group on Ω, p a prime number dividing n and F a field of characteristic p. Denote by $F\Omega$ the permutation module of G over F (that is, the vector space over F with basis Ω). Now $F\Omega$ has two obvious FG-submodules S, T, one of codimension 1 and the other of dimension 1, defined by

$$S = \left\{ \sum_{\omega\in\Omega} a_\omega \omega \,\middle|\, a_\omega \in F,\ \sum_{\omega\in\Omega} a_\omega = 0 \right\},$$
$$T = \left\{ \lambda \sum_{\omega\in\Omega} \omega \,\middle|\, \lambda \in F \right\}.$$

Since p divides n we have $T \subseteq S$. Following J.A.Green (see [26]) we call the FG-module $\frac{S}{T}$ the <u>heart</u> of G acting on Ω, over F. Recent results (see [24], [32]) have shown that knowledge of the structure of the heart can give much information about the action of G on Ω. One elementary fact is that if G is primitive on Ω and $n \geq 4$ and the heart is irreducible then G is 2-transitive.

Now let G be the automorphism group of a nontrivial regular 2-graph (Ω, Δ) with parameters r, s (where $a = 2r$, $n = 2+2r+2s$ as described above), and let F be a field of characteristic 2. Write $\Omega = \{e_1, \ldots, e_n\}$ and make $F\Omega$ into an algebra by defining

$$e_i e_j = \sum_{\{e_i, e_j, e_k\} \in \Delta} e_k \qquad (i, j \in \{1, \ldots, n\})$$

and extending products linearly. In Chapter 6 we show that in many cases the derived algebra is properly contained in the submodule S defined above, and use this to prove:

<u>THEOREM 6.3.</u> If r, s are not both odd then the heart of G acting on Ω, over F, is reducible (as an FG-module). In particular, if $n \equiv 0 \pmod 4$ the heart is reducible.

In Chapter 7 it is shown that the algebra $F\Omega$ defined as above from a nontrivial regular 2-graph over a field F of characteristic 2, is in fact a Lie algebra; we investigate its derived and lower central series. We conclude by showing how to define Lie algebras in other characteristics from certain types of graph.

"'Begin at the beginning,' the King said gravely,

'and go on till you come to the end: then stop.'"

Lewis Carroll, 'Alice in Wonderland'.

Chapter 1: RESULTS FROM THE LITERATURE FOR PROBLEM A.

In this chapter we outline the main results from the literature which we shall need in order to study transitive groups of degree p, where $p = 4q+1$ and p,q are prime. We begin with some of the modular character theory of groups whose order is divisible to the first power only by some prime, and give a sketch of the so-called Green correspondence for such groups. Next we outline some of the general character theory of permutation groups and state results of Neumann [30] relating this theory to certain "generosity" properties of permutation groups. Also several facts about characters of groups of prime degree are presented. After this we give a brief exposition of some graph theory related to permutation groups; this is followed by a result of Frame [12] and theorems of Cooper [8] and Rowlinson [35] on simply primitive groups of degree 4q, q being prime. Finally we state a few well-known theorems of Burnside, Jordan and others and present several more recent results.

1. GROUPS OF ORDER DIVISIBLE BY p TO THE FIRST POWER ONLY.

We present the results needed for Chapters 3 and 4; for an account of modular representation theory, see Curtis and Reiner [9].

Let G be a group whose order is divisible by a prime number p to the first power only. Let K be a p-adic number field which is a splitting field for G, let R be its local ring of integers with maximal ideal $\mathfrak{p}$ and let $\bar{K}$ denote the finite field $\frac{R}{\mathfrak{p}}$ of characteristic p. If M is any RG-module, put $\bar{M} = \frac{M}{\mathfrak{p}M}$ ($= \bar{K}\otimes M$), so that $\bar{M}$ is a $\bar{K}G$-module. Any ordinary irreducible character of G can be realised as the character of an RG-module ([9], p.496). If the regular representation module RG_{RG} is split as a direct sum of indecomposable RG-modules, known as <u>projective indecomposables</u>, then some of the summands afford irreducible characters of G whose degree is divisible by p. Each of the remaining projective indecomposables lies in some p-block of G of defect one. The full description is given in Theorem 1.1 below.

Generally, if X is a normal subgroup of a group Y and ψ_1, ψ_2 are ordinary characters of X, then we say that ψ_1 and ψ_2 are <u>Y-conjugate</u> if there exists $y \in Y$ such that $\psi_1(x) = \psi_2(y^{-1}xy)$ for all $x \in X$. For a character ψ of X we write

$$I_Y(\psi) = \{\, y \in Y \mid \psi(x) = \psi(y^{-1}xy) \text{ for all } x \in X \,\}.$$

Clearly $I_Y(\psi)$ is a subgroup of Y containing X; it is known as the <u>inertia subgroup</u> of ψ.

We may assume that K contains the cyclotomic field $\mathbb{Q}(\sqrt[e]{1})$ where e is the exponent of G. Write $e = pe_{p'}$ (so that $(p, e_{p'}) = 1$). Choose an automorphism γ of $\mathbb{Q}(\sqrt[e]{1})$ fixing the $e_{p'}$ th roots of unity and of largest possible order as a permutation on the set of pth roots of unity; extend γ to K. The characters χ_1 and χ_2 of G are said to be <u>p-conjugate</u> if there is an integer c such that $\chi_1(x) = \chi_2(x)^{\gamma^c}$ for all $x \in G$. A character is said to be <u>p-rational</u> if it is p-conjugate only to itself (that is, if its values lie in $\mathbb{Q}(\sqrt[e_{p'}]{1})$).

Now let P be a Sylow p-subgroup of G and put $C = C_G(P)$, $N = N_G(P)$. By Burnside's Transfer Theorem we may write $C = P \times X$ where $X = O_{p'}(C)$. Let $1 = \theta_1, \theta_2, \ldots, \theta_b$ be representatives of the N-conjugacy classes of ordinary irreducible characters of X, and for $m = 1, \ldots, b$ let Θ_m be the sum of the distinct N-conjugates of θ_m. If α, θ are characters of P,X respectively, denote by $\alpha.\theta$ the character of C defined by

$$\alpha.\theta\,(xy) = \alpha(x)\,\theta(y) \qquad (x \in P, y \in X).$$

For $m = 1, \ldots, b$ write $t_m = |I_N(\theta_m.1) : C|$, $s_m = \dfrac{p-1}{t_m}$.

THEOREM 1.1 (Brauer [4]).

(i) There is a 1-1 correspondence between the p-blocks of G of defect one and the characters $\{\Theta_m \mid m = 1,\ldots,b\}$. Let B_m denote the block corresponding to Θ_m.

(ii) The set of ordinary irreducible characters in B_m consists of t_m p-rational characters $\chi_0,\ldots,\chi_{t_m-1}$ and s_m characters, called the exceptional characters of B_m, which are all p-conjugate. We write χ_{t_m} for the sum of of the exceptional characters of B_m.

(iii) The block B_m contains precisely t_m projective indecomposables $U_0,\ldots,U_{t_m-1}$. If τ is the character of one of them, then $\tau = \chi_i + \chi_j$ for some i,j with $0 \leq i < j \leq t_m$.

(iv) For each χ_j $(0 \leq j \leq t_m)$ in the block B_m there is a number $\varepsilon_j \in \{-1,1\}$ such that

$$\chi_j(1) \equiv \varepsilon_j \Theta_m(1) \pmod{p}.$$

(v) If χ is one of the exceptional characters in the block B_m then

$$\chi(1) \equiv - \varepsilon_{t_m} t \Theta_m(1) \pmod{p}$$

where $t = |N:C|$. Moreover, if t_m is odd then χ is not real-valued, whereas if t_m is even then χ is real-valued.

Theorem 1.1 enables us to define a certain graph for each p-block B_m of defect one as follows: the t_m+1 nodes (vertices) are labelled with $\chi_0,\ldots,\chi_{t_m}$ and χ_i is joined to χ_j if and only if $\chi_i+\chi_j$ is the character of a projective indecomposable. This graph turns out to be a connected tree, called the Brauer tree of B_m. If χ_i and χ_j are joined in this Brauer tree, we say that χ_i is a mate of χ_j.

To each projective indecomposable U_k in the block B_m there corresponds an irreducible $\overline{K}G$-module F_k defined as $\overline{U}_k/(\mathrm{rad}\,\overline{U}_k)$ and $F_0,\ldots,F_{t_m-1}$ is a complete set of non-isomorphic irreducible $\overline{K}G$-modules in B_m. Let X_j be an RG-module affording the character χ_j (if $0 \leq j \leq t_m - 1$) or affording one of the exceptional characters in B_m (if $j = t_m$). Then $\chi_i + \chi_j$ is the character afforded by U_k if and only if $\overline{X}_i$ and $\overline{X}_j$ both have F_k as a composition factor. Thus we can label the edges of the Brauer tree of B_m with the modular irreducibles $F_0, \ldots, F_{t_m - 1}$, specifying that edge F_i is incident with vertex χ_j if and only if F_i is a composition factor of $\overline{X}_j$. The character χ_j is an end-node in the Brauer tree of B_m (that is, a node which lies on precisely one edge) if and only if $\overline{X}_j$ is irreducible.

The following result, taken from [34], gives information about the degrees of the modular irreducibles in B_m.

THEOREM 1.2. Let Γ_m be the Brauer tree of B_m and let F_i be any edge of Γ_m; write ϕ_i for the modular irreducible character afforded by F_i. If we delete the edge F_i from Γ_m, we disconnect Γ_m into two components; let Δ be the component which does not contain the "exceptional" node χ_{t_m}, and let χ_j be the vertex in Δ which is adjacent to F_i. Then if ε_j is the number in $\{-1, 1\}$ associated in Theorem 1.1 with χ_j, we have

$$\phi_i(1) \equiv \varepsilon_j c \pmod{p}$$

where c is the number of vertices in Δ.

We can say more about the Brauer tree of the principal block B_1:

THEOREM 1.3 (Tuan, [39]). The Brauer tree of the principal block B_1 has a subgraph Σ, called the real stem of Γ_1, with the following properties:

(i) the vertices in Σ are precisely the characters which are real-valued on p-regular elements; the "exceptional" node χ_{t_1} lies in Σ,

(ii) the subgraph Σ is an open polygon, that is, it is connected, exactly two of its vertices have valency one and the rest have valency two,

(iii) complex conjugation of characters induces an automorphism of Γ which fixes pointwise just Σ.

REMARK. If $C_G(P) = P$ then the characters in the real stem are precisely those which are real-valued on the whole of G.

Now suppose that $C_G(P) = P$, so that $X = 1$, $b = 1$ and the principal p-block B_1 is the only p-block of defect one; it contains t ($= |N_G(P):P|$) p-rational characters $\chi_0, \ldots, \chi_{t-1}$ ($\chi_0 = 1$) and $\frac{p-1}{t}$ exceptional characters with sum χ_t. Let $k = |G:G'|$. Then G has k distinct linear characters $\lambda_1, \ldots, \lambda_k$ ($\lambda_1 = 1$), which form a cyclic group Λ under multiplication. We have (see § 2 of [28]):

PROPOSITION 1.4. For each $i \in \{1, \ldots, k\}$ the map $\chi_j \to \chi_j \lambda_i$ ($j = 0, \ldots, t$) is an automorphism of the Brauer tree of B_1; in this way Λ acts on the Brauer tree as a group of automorphisms. The node χ_t is fixed by every element of Λ, while Λ acts semiregularly on the other vertices, that is, if $j \neq t$ and $i \neq 1$ then $\chi_j \lambda_i \neq \chi_j$.

From the theorem of Feit [11], we can deduce the following result, which is part of Lemma 2.1 of [28].

THEOREM 1.5. Suppose that G is insoluble and that G is not isomorphic to PSL(2,p) or to PGL(2,p). Let χ be an irreducible character of G. Then

(i) if χ has degree p-1 then either χ is an end-node or χ has valency two in the Brauer tree; in the latter case, one of the vertices joined to χ is a linear character,

(ii) if χ has degree $p+1$ then χ is an end-node in the Brauer tree.

---

2. THE GREEN CORRESPONDENCE.

We continue with the notation of Section 1 - G is a group whose order is divisible by p to the first power only and $P = \langle a \rangle$ is a Sylow p-subgroup of G with $C = C_G(P) = P \times X$, $N = N_G(P)$. If H is any subgroup of G containing N, the <u>Green correspondence</u> is the correspondence $W \leftrightarrow T_1$ between indecomposable $\bar{K}G$-modules and indecomposable $\bar{K}H$-modules given by the following theorem, which is taken from Theorem 2 of [13] (see also 4.1 and 4.2 of [14]).

<u>THEOREM 1.6</u> (Green [13]). Let W be an indecomposable $\bar{K}G$ - module such that $p \nmid \dim W$. Then

$$W_H = T_0 \oplus T_1$$
$$\text{and} \quad (T_1)^G = W \oplus T_2$$

where T_0 is a projective $\bar{K}H$-module, T_1 is an indecomposable $\bar{K}H$-module and T_2 is a projective $\bar{K}G$-module. Moreover, W lies in the principal p-block of G if and only if T_1 lies in the principal p-block of H.

<u>REMARK.</u> Theorem 1.6 remains unaltered if we replace $\bar{K}$ by the local ring R.

Finally we describe the indecomposable $\bar{K}C$- and $\bar{K}N$-modules; a fuller account can be found in [11]. For each $s \in \{1,\dots,p\}$ there is a unique indecomposable $\bar{K}P$-module V_s of dimension s on which we can take the generator a of P to have the Jordan form

$$\begin{pmatrix} 1 & & & & & \\ 1 & 1 & & & 0 & \\ & 1 & 1 & & & \\ & & \cdot & \cdot & & \\ & 0 & & \cdot & \cdot & \\ & & & & 1 & 1 \end{pmatrix}$$

Let $Y_1,\ldots,Y_c$ be a complete set of non-isomorphic irreducible RX-modules. Then there are precisely pc indecomposable $\overline{K}C$-modules - they are the modules

$$V_s\otimes\overline{Y}_i \quad (1\leq s\leq p,\ 1\leq i\leq c).$$

Let $W_1,\ldots,W_b$ be RX-modules affording the characters $\Theta_1,\ldots,\Theta_b$ of X described in Section 1. Then if W is any indecomposable $\overline{K}N$-module, we have

$$W_C\cong V_s\otimes\overline{W}_i$$

for some $s\leq p$, $i\leq b$. If W is in the principal block of N then

$$W_C\cong V_s\otimes\overline{W}_1$$

for some $s\leq p$.

---

3. CHARACTERS OF PERMUTATION GROUPS.

Let G be a permutation group on a set Ω of size n and denote by π the permutation character of G associated with Ω, that is, $\pi(g) = |\mathrm{fix}_\Omega(g)|$ for all $g\in G$. The inner product $\langle 1,\pi\rangle_G$ is $\#\mathrm{orb}(G,\Omega)$, the number of orbits of G on Ω. If G acts on Ω_1, Ω_2 with associated characters π_1, π_2, then $\pi_1\pi_2$ is the character associated with $\Omega_1\times\Omega_2$, so

$$\langle\pi_1,\pi_2\rangle_G = \langle 1,\pi_1\pi_2\rangle_G = \#\mathrm{orb}(G,\Omega_1\times\Omega_2).$$

If G is transitive on Ω_1 then $\langle\pi_1,\pi_2\rangle_G = \#\mathrm{orb}(G_\alpha,\Omega_2)$ for any $\alpha\in\Omega_1$.

Now consider the symmetric group S_n acting on Ω. Let π_0, η_0, ξ_0 denote the characters of S_n associated with Ω, $\Omega^{\{2\}}$, $\Omega^{(2)}$ respectively

($\Omega^{\{2\}}$, $\Omega^{(2)}$ are the sets of unordered and ordered pairs of distinct elements of Ω). We have

$$\langle 1 , \pi_0 \rangle_{S_n} = \# \mathrm{orb}(S_n, \Omega) = 1,$$

$$\langle \pi_0 , \pi_0 \rangle_{S_n} = \# \mathrm{orb}(S_n, \Omega \times \Omega) = 2.$$

Hence $\pi_0 = 1 + \chi_0^{(n-1,1)}$ for some irreducible character $\chi_0^{(n-1,1)}$ of S_n of degree n-1. Also

$$\langle 1 , \eta_0 \rangle_{S_n} = 1,$$

$$\langle \pi_0 , \eta_0 \rangle_{S_n} = \# \mathrm{orb}(S_n, \Omega \times \Omega^{\{2\}}) = 2,$$

$$\langle \eta_0 , \eta_0 \rangle_{S_n} = \# \mathrm{orb}(S_n, \Omega^{\{2\}} \times \Omega^{\{2\}}) = 3,$$

so $\eta_0 = 1 + \chi_0^{(n-1,1)} + \chi_0^{(n-2,2)}$ for some irreducible character $\chi_0^{(n-2,2)}$ of S_n.
Similarly, $\xi_0 = 1 + 2\chi_0^{(n-1,1)} + \chi_0^{(n-2,2)} + \chi_0^{(n-2,1^2)}$ where $\chi_0^{(n-2,1^2)}$ is irreducible.

We may restrict the characters π_0, η_0, ξ_0 to the characters π, η, ξ of G associated with Ω, $\Omega^{\{2\}}$, $\Omega^{(2)}$ respectively. Thus, denoting the restrictions of $\chi_0^{(n-1,1)}$, $\chi_0^{(n-2,2)}$, $\chi_0^{(n-2,1^2)}$ to G by $\chi^{(n-1,1)}$, $\chi^{(n-2,2)}$, $\chi^{(n-2,1^2)}$, we have

$$\pi = 1 + \chi^{(n-1,1)},$$

$$\eta = 1 + \chi^{(n-1,1)} + \chi^{(n-2,2)},$$

$$\xi = 1 + 2\chi^{(n-1,1)} + \chi^{(n-2,2)} + \chi^{(n-2,1^2)}.$$

Write $\zeta = \xi - \eta = \chi^{(n-1,1)} + \chi^{(n-2,1^2)}$. The group G is 2-transitive if and only if $\chi^{(n-1,1)}$ is irreducible.

If G is transitive on Ω and $\alpha \in \Omega$, then the induced character $(1_{G_\alpha})^G$ is equal to π. Also if G is 2-transitive and ν $(= (\chi^{(n-1,1)})_{G_\alpha})$ is the character of G_α associated with $\Omega \setminus \{\alpha\}$, then

$$\xi = (1_{G_{\alpha\beta}})^G = ((1_{G_{\alpha\beta}})^{G_\alpha})^G = \nu^G .$$

---

4. GENEROSITY IN PERMUTATION GROUPS.

In [30], Neumann defines certain "generosity" properties of permutation groups and relates them to the character theory described in the previous section. We state a few of the results.

Let G be a permutation group on a set Ω of size n and let k be an integer such that $1 \leq k < n$. Then G is said to be generously k-transitive if, for every $\Delta \in \Omega^{\{k+1\}}$, we have $S_{k+1} \leq G^{\Delta}_{\{\Delta\}}$; it is said to be almost generously k-transitive if, for every $\Delta \in \Omega^{\{k+1\}}$, we have $A_{k+1} \leq G^{\Delta}_{\{\Delta\}}$. Also G is a little generously 3-transitive if, for every $\Delta \in \Omega^{\{4\}}$, we have $V_4 \leq G^{\Delta}_{\{\Delta\}}$ (V_4 being the unique normal subgroup of A_4 of order 4). If G is generously or almost generously k-transitive then G is k-transitive; and if G is a little generously 3-transitive then it is 3-transitive (Lemmas 2.1, 2.2 and 2.3 of [30]). By the corollary to Proposition 3.2_0 of [30], G is generously k-transitive if and only if G is k-transitive and, given $\Delta = \{\alpha_1, \ldots, \alpha_{k-1}\} \in \Omega^{\{k-1\}}$ and $\alpha_k \in \Omega \setminus \Delta$, every orbit of $G_{\alpha_1 \ldots \alpha_k}$ is self-paired when considered as a suborbit of $G_{(\Delta)}$ acting transitively on $\Omega \setminus \Delta$ (see Section 6 for the definition of self-paired suborbits). Alternatively, G is generously k-transitive ($k \geq 2$) if and only if G is k-transitive and for any $\Delta \in \Omega^{\{k\}}$, the groups $G_{(\Delta)}$ and $G_{\{\Delta\}}$ have the same orbits on $\Omega \setminus \Delta$.

The following result is taken from Propositions 8.7 and 8.8 and the corollary to Proposition 8.9 of [30].

PROPOSITION 1.7. (i) If $n \geq 5$ then $\langle \chi^{(n-2,2)}, \chi^{(n-2,1^2)} \rangle_G = 0$ if and only if G is a little generously 3-transitive.

(ii) If $n \geq 5$ then $\chi^{(n-2,1^2)}$ is irreducible if and only if G is generously 3-transitive.

(iii) If $n \geq 10$ then $\chi^{(n-2,2)}$ is irreducible if and only if G is 4-transitive.

---

5. CHARACTERS OF GROUPS OF PRIME DEGREE.

Let G be an insoluble, transitive group of prime degree p on a set Ω. Suppose that $p > 11$, so that G is not isomorphic to PSL(2,p) or to PGL(2,p) by a theorem of Galois (see [18], p.214). Clearly p divides $|G|$ to the first power only and if P is a Sylow p-subgroup of G then $C_G(P) = P$. Consequently the results of Section 1 apply to G; by Theorem 1.1, the principal p-block is the only p-block of G of defect one. It contains t $(= |N_G(P):P|)$ p-rational characters $\chi_0, \ldots, \chi_{t-1}$ $(\chi_0 = 1)$ and $\frac{p-1}{t}$ exceptional characters (with sum χ_t). By Burnside's Theorem (1.25 in this chapter), G is 2-transitive, so $\chi^{(p-1,1)}$ is irreducible of degree p-1. We may choose our notation so that $\chi^{(p-1,1)} = \chi_1$. Recall that $\zeta = \xi - \eta$ $= \chi_1 + \chi^{(p-2,1^2)}$. The following proposition is proved in § 3 of [28].

PROPOSITION 1.8. (i) The character $\pi = 1 + \chi_1$ is the character of a projective indecomposable RG-module (where R is the ring defined in Section 1).

(ii) The characters ξ, η, ζ and $\chi^{(p-2,2)}$ are all characters of projective RG-modules (and hence are sums of characters of projective indecomposables).

The next two propositions are taken from Lemmas 3.2 and 3.3 and the proof of Lemma 3.4 of [28].

PROPOSITION 1.9. Let λ be a linear character of $N_G(P)$. Then

(i) if t is even, we have

$$\langle \lambda , \eta \rangle_{N_G(P)} \leqslant \frac{p-1}{t} \quad \text{and} \quad \langle \lambda , \xi \rangle_{N_G(P)} \leqslant \frac{p-1}{t} ,$$

(ii) if t is odd, we have

$$\langle \lambda , \eta \rangle_{N_G(P)} = \langle \lambda , \xi \rangle_{N_G(P)} = \frac{p-1}{2t} .$$

PROPOSITION 1.10. Let χ be an irreducible character of G. Then

(i) if $\chi(1) = kp+\varepsilon$ (where $\varepsilon \in \{0,-1,1\}$) we have $\langle \chi , 1 \rangle_P = k+\varepsilon$,

(ii) if $\chi(1) = kp-\varepsilon t$ (where $\varepsilon \in \{-1,1\}$) we have $\langle \chi , 1 \rangle_P = k$.

Now we state three results taken from the theorem of [27], Theorems 5.1 and 5.2 of [28], and [21].

THEOREM 1.11. If t is even then G is 3-transitive.

THEOREM 1.12. Suppose that t is odd and let $\alpha, \beta \in \Omega$. Then

(i) the exceptional characters do not appear as constituents of ξ ,

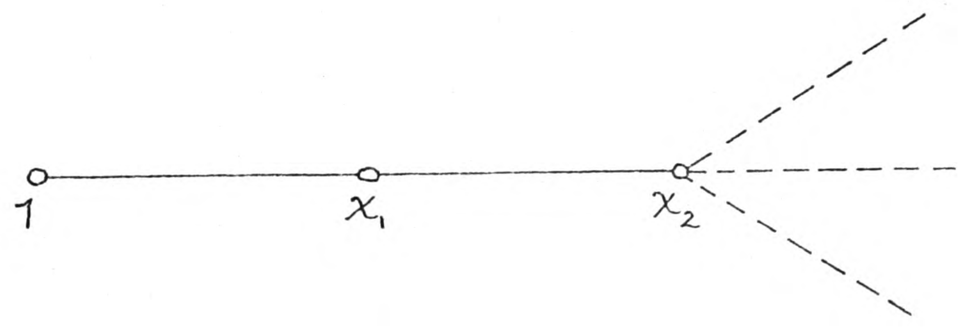
(ii) $G_{\alpha\beta}$ has at most $\frac{p-1}{t}$ orbits on $\Omega\backslash\{\alpha,\beta\}$,

(iii) $G_{\{\alpha\beta\}}$ has at most $1+ \frac{p-1}{2t}$ orbits on $\Omega\backslash\{\alpha,\beta\}$.

THEOREM 1.13. If $t = 2$ then G is $SL(2,2^r)$ where $p = 2^r+1$.

By Proposition 1.8, the principal character 1 is joined only to χ_1 in the Brauer tree of the principal p-block; and by Theorem 1.5(i), χ_1 is joined to precisely one nonprincipal character, say ψ , in the Brauer tree. Now ξ is a sum of characters of projective indecomposables by Proposition 1.8(ii) and $\chi_1 \subseteq \xi$, while $1 \nsubseteq \xi$. Hence $\chi_1 + \psi \subseteq \xi$ so by

Theorem 1.12(i), ψ is irreducible. We choose notation so that $\psi = \chi_2$. Thus we have the following fragment of the Brauer tree:



Since 1 and χ_1 are real-valued characters of G and χ_2 is the only other character adjacent to χ_1, it must be part of the real stem of the Brauer tree (Theorem 1.3).

Now suppose that q is a prime number dividing p-1 such that q divides $|G|$ to the first power only. Then the results of Section 1 apply with q replacing p. Let R_q be the local ring of integers in a q-adic splitting field K_q for G and write R_p, K_p for R,K of Section 1. We refer to characters of projective R_qG-modules as <u>q-projective</u> characters and to characters of projective R_pG-modules as <u>p-projective</u>. Similar notation is used to distinguish other concepts relative to the primes p and q; for instance we refer to p-projective indecomposables and q-projective indecomposables, to Brauer p-trees and Brauer q-trees, to p-exceptional characters and q-exceptional characters, to p-mates and q-mates, etc..

Notice that q divides $|G_\alpha|$ to the first power only, so the results of Section 1 apply to G_α. The next proposition follows from the proof of Lemma 3 of [27].

PROPOSITION 1.14. The characters ξ , η and ζ are all q-projective. Also the permutation character ν of G_α associated with $\Omega\setminus\{\alpha\}$ $(\alpha\in\Omega)$ is q-projective, that is, it is the character of a projective R_qG_α-module.

Finally we state the results, mentioned in the Introduction, of Ito and Neumann in [19], [20] and [29] for the case $p = 2q+1$.

THEOREM 1.15. Let G be an insoluble, transitive permutation group of degree p, where $p = 2q+1$ and p,q are prime with $p > 11$. Then G is 3-transitive; and if G is not 4-transitive then

$$\zeta = \chi_1 + \chi_2 \quad ,$$
$$\eta = 1 + \chi_1 + \psi_1 + \psi_2$$

where ψ_1, ψ_2 are the two q-exceptional characters (having degree $\frac{(q-1)}{2}p$) in the principal q-block. If $\alpha, \beta\in\Omega$ then $G_{\alpha\beta}$ has rank 3 on $\Omega\setminus\{\alpha,\beta\}$.

---

6. SOME GRAPH THEORY.

This section consists of a brief sketch of some of the theory of the edge-coloured complete graph associated with a permutation group; this will be used in Chapter 2. For a fuller treatment, see [31].

Let G be a transitive permutation group on a set Ω and let $\alpha\in\Omega$. There is a 1-1 correspondence between the orbits $\Delta_0,\ldots,\Delta_{r-1}$ of G on $\Omega\times\Omega$ (where $\Delta_0 = \{ (\omega,\omega) \mid \omega\in\Omega\}$) and the orbits $\Gamma_0(\alpha),\ldots,\Gamma_{r-1}(\alpha)$ of G_α on Ω (where $\Gamma_0(\alpha) = \{\alpha\}$). We may choose the labelling such that

$$\Gamma_i(\alpha) = \{ \gamma\in\Omega \mid (\alpha,\gamma) \in \Delta_i\} \quad .$$

The orbits $\Gamma_i(\alpha)$ are called <u>suborbits</u> of G ($\Gamma_0(\alpha)$ is the <u>trivial</u> suborbit), the suborbit sizes $n_i = |\Gamma_i(\alpha)|$ are called the <u>subdegrees</u> of G, and the number r is the <u>rank</u> of G. We often write just Γ_i instead of $\Gamma_i(\alpha)$ when this leads to no confusion.

For any orbit Δ_i put $\Delta_i^* = \{(\gamma,\beta) \mid (\beta,\gamma)\in\Delta_i\}$. Then Δ_i^* is an orbit of G on $\Omega\times\Omega$, say $\Delta_i^* = \Delta_{i^*}$. The corresponding suborbits $\Gamma_i(\alpha)$ and $\Gamma_{i^*}(\alpha)$ (also written $\Gamma_i^*(\alpha)$) are said to be <u>paired</u>. If $i = i^*$ then $\Gamma_i(\alpha)$ is <u>self-paired</u>.

We define the <u>edge-coloured complete graph</u> on Ω associated with G as follows: select r-1 colours $c_1,\dots,c_{r-1}$ and assign colour c_i to edge (β,γ) if and only if $(\beta,\gamma)\in\Delta_i$. The subgraph with edge set Δ_i is called the <u>c_i-monochrome</u> subgraph; if $i = i^*$ then we can regard it as an undirected graph.

The following result is taken from Lemmas 2 and 3 of [31].

<u>PROPOSITION 1.16.</u> The group G is primitive if and only if every monochrome subgraph is strongly connected (that is, for any $\beta,\gamma\in\Omega$ there is a directed path of c_i-edges from β to γ).

For $i,j\in\{1,\dots,r-1\}$, define

$$\Delta_i\circ\Delta_j = \{(\beta,\gamma) \mid \beta\neq\gamma \text{ and } \exists\,\delta\in\Omega \text{ such that } (\beta,\delta)\in\Delta_i,\ (\delta,\gamma)\in\Delta_j\}$$

Then $\Delta_i\circ\Delta_j$ is either empty (which occurs if and only if $j = i^*$ and $n_i = 1$), or it is a union of monochrome subgraphs. Write $(\Gamma_i\circ\Gamma_j)(\alpha)$ for the corresponding union of suborbits. The next result follows from the proof of Theorem 3 of [31].

<u>THEOREM 1.17.</u>

(i) For $i,j\in\{1,\dots,r-1\}$ let $k = \#\mathrm{orb}(G_\alpha, \Gamma_i(\alpha)\times\Gamma_j(\alpha))$. Then $(\Gamma_i^*\circ\Gamma_j)(\alpha)$ is a union of at most k suborbits.

(ii) Suppose, for some i,j, that G_α is transitive on $\Gamma_i(\alpha)\times\Gamma_j(\alpha)$. Then

$(\Gamma_i^* \circ \Gamma_j)(\alpha)$ is a single suborbit, $\Gamma_k(\alpha)$ say. If G is primitive and $n_i \geqslant n_j > 1$, then $n_k > n_i$.

Finally, suppose that G is 2-transitive on Ω and let $\alpha, \beta \in \Omega$. Denote the orbits of $G_{\alpha\beta}$ on $\Omega \setminus \{\alpha,\beta\}$ by $\Phi_1, \ldots, \Phi_s$ (so that these are the nontrivial suborbits of G_α acting on $\Omega \setminus \{\alpha\}$). Then for any $g \in G_{\{\alpha\beta\}} \setminus G_{\alpha\beta}$, the size of the set $\{i \mid \Phi_i g = \Phi_i\}$ is equal to the number of nontrivial self-paired suborbits Φ_i. If every suborbit Φ_i is self-paired then G is generously 2-transitive.

7. SOME RESULTS OF COOPER AND ROWLINSON.

In this section we state some results of Cooper [8] and Rowlinson [35] on simply primitive (that is, primitive but not 2-transitive) groups of degree 4q, q being a prime number greater than 13. These results are used in Chapter 3.

Let X be a simply primitive group on Ω of degree 4q where q is a prime number greater than 13. By a theorem of Jordan (Theorem 1.26), a Sylow q-subgroup Q of X is cyclic of order q. Our first result is Theorem 4.3 of [8]:

THEOREM 1.18. The subgroup Q is self-centralising in X.

The normaliser $N_X(Q)$ is of the form QR where $R = \langle c \rangle$ is a nontrivial cyclic group whose order r divides q-1. The next result is taken from Theorems 1.1 and 8.2 of [8].

THEOREM 1.19. If the rank of X on Ω is at least 4 then one of the following holds:

(i) X has rank 4, all its suborbits are self-paired and there is an integer a such that $q = 96a^2+80a+17$ and r divides either 32 or $4(2a+1)$,

(ii) X has rank 5, X has precisely one pair of non-self-paired suborbits and there is an integer a such that $q = 96a^2+80a+17$ and r divides either 8 or $2(2a+1)$; also the permutation character ν of X associated with Ω is of the form

$$\nu = 1+\phi_1+\phi_2+\overline{\phi_2}+\phi_3$$

where ϕ_1, ϕ_2, ϕ_3 are irreducible characters of X and $\phi_1(1) = q-1$, $\phi_2(1) = \phi_3(1) = q$,

(iii) X has rank 5 and all its suborbits are self-paired.

Finally, from Lemmas 6.4.1 and 6.4.2 of [35] we have:

<u>THEOREM 1.20.</u> If X has rank 3 then the permutation character ν of X associated with Ω is of the form $\nu = 1+\phi_1+\phi_2$ where ϕ_1, ϕ_2 are irreducible characters of X, and there is an integer a such that one of the following occurs:

(i) $\phi_1(1) = q-1$, $\phi_2(1) = 3q$, $q = 3a^2+3a+1$ and the subdegrees of X are 1, $n_1 = 3(2a+1)(a+1)$, $n_2 = 3a(2a+1)$,

(ii) $\phi_1(1) = 3q-1$, $\phi_2(1) = q$, $q = 36a^2+20a+3$ and the subdegrees of X are 1, $n_1 = (4a+1)(9a+2)$, $n_2 = 9(4a+1)(3a+1)$,

(iii) $\phi_1(1) = 3q-1$, $\phi_2(1) = q$, $q = 12a^2+6a+1$ and the subdegrees of X are 1, $n_1 = (4a+1)(6a+1)$, $n_2 = 2(4a+1)(3a+1)$.

8. A RESULT OF FRAME.

Let G be a permutation group acting transitively on a finite set Ω and let π be the associated permutation character of G. Partition the set of ordinary irreducible characters of G into three subsets as follows:

$\Lambda_1 = \{\chi \mid \chi$ is the character of a representation of G over $\mathbb{R}\}$,

$\Lambda_2 = \{\chi \mid \chi$ is not a real-valued character$\}$,

$\Lambda_3 = \{\chi \mid \chi$ is a real-valued character not afforded by any representation of G over $\mathbb{R}\}$.

For each irreducible character χ of G, let $d_\chi = \langle \pi, \chi \rangle_G$. The following theorem is a result of Frame [12] (it is also Lemma 1 of [5]).

THEOREM 1.21. The number of self-paired suborbits of G acting on Ω is

$$\sum_{\chi \in \Lambda_1} d_\chi \; - \; \sum_{\chi \in \Lambda_3} d_\chi \quad .$$

COROLLARY 1.22. Every suborbit of G is self-paired if and only if π is multiplicity-free (that is, $d_\chi \leq 1$ for every χ) and every constituent of π is real-valued.

---

9. SOME RESULTS ON LINEAR GROUPS.

We state two results on linear groups which we shall need in Chapter 4.

An ordinary irreducible representation ρ of a finite group G is said to be quasiprimitive if, for every normal subgroup H of G, the irreducible constituents of ρ_H are all equivalent.

THEOREM 1.23 (Huffman and Wales [17]). Let G be a finite group and suppose that G has faithful ordinary irreducible representation ρ which is quasiprimitive. Suppose also that for some involution x of G, $\rho(x)$ has precisely two eigenvalues equal to -1 and the rest equal to 1. Then G is a known group.

We shall use this theorem when G is a 2-transitive group, in which case the conclusion tells us that G is one of the groups in the table on page 103.

The following result, due to Brauer [4], will also be used in Chapter 4.

THEOREM 1.24. Let G be a finite group, p a prime number, and assume that G has a faithful ordinary irreducible representation whose degree is less than $\frac{p-1}{2}$. Then G has a normal Sylow p-subgroup.

10. SOME THEOREMS OF BURNSIDE, JORDAN AND OTHERS.

We state some theorems of Burnside, Jordan and Dickson and several more recent results on the groups which will interest us in Chapter 3.

THEOREM 1.25. (Burnside). If G is an insoluble, transitive permutation group of prime degree then G is 2-transitive.

THEOREM 1.26. (Jordan). Let G be a primitive group of degree mq+k where q is prime and m,k are positive integers. Suppose that G is neither the alternating nor the symmetric group and that G contains an element of order q and degree mq. Then

(i) $m = 1$, $q \geqslant 2$ imply $k \leqslant 2$,

(ii) $m = 2$, $q \geqslant 5$ imply $k \leqslant 2$,

(iii) $m = 3$, $q \geqslant 5$ imply $k \leqslant 3$.

PROPOSITION 1.27. (Dickson). If q is a prime number greater than 13, then PSL(2,q) has no maximal subgroup of index 4q (that is, PSL(2,q) has no primitive permutation representation of degree 4q).

These three results can be found in [18], p.609, Theorem 13.10 of [40] and Section 260 of [10].

We conclude this section with two results on the groups with which we are concerned in Problem A.

THEOREM 1.28. (Atkinson [2]). If G is an insoluble, transitive permutation group of degree p, where $p = 4q+1$ and p,q are prime with $p > 13$, then G is 2-primitive.

THEOREM 1.29. (Appel and Parker [1]). If G is an insoluble, transitive permutation group of degree p, where $p = 4q+1$, p,q are prime and $p > 13$, and G is neither the alternating nor the symmetric group then $q > 37$.

---

11. TWO ELEMENTARY FACTS.

We conclude this chapter with two elementary results.

PROPOSITION 1.30. If G is a sharply 2-transitive, 2-primitive permutation group on a set Ω, then G is $AGL(1,2^r)$ acting on $GF(2^r)$ for some r, where 2^r-1 is prime.

PROOF. The stabiliser G_α $(\alpha \in \Omega)$ must be regular of prime degree p, say, since it is primitive on $\Omega \setminus \{\alpha\}$; consequently by Theorems 5.1 and 11.3 of [40], G has a regular normal subgroup which is elementary abelian of order 2^r where $2^r-1 = p$. Now the action of G on this subgroup by conjugation identifies G with $AGL(1,2^r)$.

A Steiner system $\mathcal{S}(d,k,n)$ is a set Ω of size n together with a set of subsets of Ω of size k, called blocks, such that any d-subset of Ω is contained in precisely one block. Our final result is:

PROPOSITION 1.31. If G is an insoluble, transitive group of degree 13 which is not 3-transitive, then G is $PSL(3,3)$ acting on the projective plane $PG(2,3)$.

Proposition 1.31 goes back as far as Jordan ; a proof can also be found in [37]. Here is a sketch of an elementary proof: first note that if G acts as an automorphism group of a Steiner system $\mathcal{S}(2,m,13)$ for some m with

$3 < m < 13$ then $\frac{13.12}{2} = b\frac{m(m-1)}{2}$ where b is the number of blocks. Hence $m = 4$ and so, since $\mathcal{S}(2,4,13)$ is the projective plane PG(2,3), G must be PSL(3,3). If G_α were primitive on $\Omega\backslash\{\alpha\}$, it would be 2-transitive by the results of Section 3 of [31] (cf. the example on p.98 of [31]). Consequently G_α is imprimitive. If it has no blocks of imprimitivity of size 3 or 4 then G_α involves (that is, has as a factor group of a subgroup) a primitive, hence 2-transitive group of degree 6; but then G contains an element of order 5 fixing at least 3 points, contradicting Theorem 1.26. If G_α has blocks of size 4, then Lemmas 1 and 2 of [2] (or Lemmas A.1 and A.2 of the Appendix to this thesis) show that G acts on a Steiner system $\mathcal{S}(2,5,13)$, which is not so. Thus G_α has blocks of size 3; now Lemmas 1 and 2 of [2] show that G acts on the Steiner system $\mathcal{S}(2,4,13)$, so that G is PSL(3,3).

"Two things fill the mind with ever-increasing wonder and awe, the more often and the more intensely the mind of thought is drawn to them..."

Immanuel Kant, 'Critique of Practical Reason'.

Chapter 2: ON 2-TRANSITIVE AND 3-TRANSITIVE GROUPS.

The techniques used in Chapters 3 and 4 to study an insoluble, transitive group of degree p on a set Ω, where $p = 4q+1$ and p,q are prime, consist largely of the following two ingredients:

(a) analysis of the characters ξ, η of G associated with $\Omega^{(2)}$, $\Omega^{\{2\}}$, using the results of Sections 1-5 of Chapter 1,

(b) deductions about the way G acts on Ω from this character theory.

In this chapter we prove some facts relating to (b), about 2-transitive and 3-transitive groups. The first section consists of results on 2-transitive groups relating the rank of the stabiliser of a point to the difference $\|\xi\|_G - \|\eta\|_G$. In the second section we consider 3-transitive groups.

1. ON 2-TRANSITIVE GROUPS.

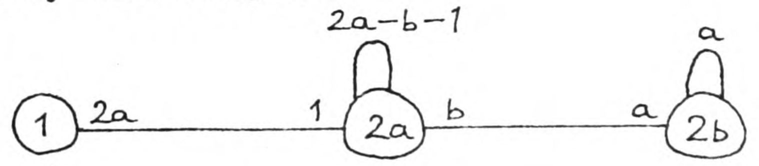
We begin with a definition. Let X be a transitive permutation group on a finite set Ω; then X has an associated edge-coloured complete graph as defined in Section 6 of Chapter 1. We say that the pair (X,Ω) (or just X, if the meaning is clear) is <u>of type (a,b)</u> if

(i) X is primitive of rank 3 on Ω,

(ii) both nontrivial suborbits Γ_1, Γ_2 of X are self-paired and $|\Gamma_1| = 2a$, $|\Gamma_2| = 2b$ for some integers a,b,

(iii) in the c_1-monochrome subgraph of X (undirected), every point of Γ_1 is joined to b points of Γ_2, and every point of Γ_2 is joined to a points of Γ_1.

If (X,Ω) is of type (a,b) then the c_1-monochrome subgraph of X can be illustrated by the diagram:



It is strongly regular of valency 2a; any two adjacent points are mutually joined to 2a-b-1 others, and any two non-adjacent points are mutually joined to a others.

Now let G be a 2-transitive but not 3-transitive group on a finite set Ω, and denote by k, the rank of G_α on $\Omega\setminus\{\alpha\}$ (where $\alpha\in\Omega$); then $k\geq 3$. Define the number d by

$$d = \# \operatorname{orb}(G,\Omega^{(2)}\times\Omega^{(2)}) - \# \operatorname{orb}(G,\Omega^{\{2\}}\times\Omega^{\{2\}}).$$

Then d is the difference between the rank of G on $\Omega^{(2)}$ and its rank on $\Omega^{\{2\}}$; alternatively, d is the difference $\|\xi\|_G - \|\eta\|_G$ where, as usual, ξ, η are the characters of G associated with $\Omega^{(2)}$, $\Omega^{\{2\}}$. The results which follow relate the numbers d and k. Recall that to say that G is generously 2-transitive is to say that the suborbits of G_α (acting transitively on $\Omega\setminus\{\alpha\}$) are all self-paired (see Section 4 of Chapter 1).

<u>PROPOSITION 2.1.</u> Suppose that G is generously 2-transitive on Ω. Then $d\geq k^2$.

<u>PROOF.</u> There is a natural G-morphism: $((\alpha,\beta),(\gamma,\delta)) \to (\{\alpha,\beta\},\{\gamma,\delta\})$ from $\Omega^{(2)}\times\Omega^{(2)} \to \Omega^{\{2\}}\times\Omega^{\{2\}}$. Under this G-morphism, an orbit of G on $\Omega^{\{2\}}\times\Omega^{\{2\}}$ corresponds to 1,2 or 4 orbits of G on $\Omega^{(2)}\times\Omega^{(2)}$; the orbit containing $(\{\alpha,\beta\},\{\gamma,\delta\})$ corresponds to 1,2 or 4 orbits on $\Omega^{(2)}\times\Omega^{(2)}$ according as $G^{D}_{\{D\}}$ (where $D=\{\alpha,\beta,\gamma,\delta\}$) contains 4,2 or 1 of the elements 1, $(\alpha\beta)$, $(\gamma\delta)$, $(\alpha\beta)(\gamma\delta)$.

Now let $\alpha,\beta\in\Omega$ and let $\Gamma_1,\ldots,\Gamma_{k-1}$ be the orbits of $G_{\alpha\beta}$ (and of $G_{\{\alpha\beta\}}$ since G is generously 2-transitive) on $\Omega\setminus\{\alpha,\beta\}$. We partition most of the orbits of G on $\Omega^{\{2\}}\times\Omega^{\{2\}}$ into sets X_{ij}, Y_{ij}, A_i, B_i, C_i as follows:

(a) X_{ij} $(1\leq i<j\leq k-1)$ consists of the orbits containing elements $(\{\alpha,\beta\},\{\gamma_i,\gamma_j\})$ $(\gamma_i\in\Gamma_i,\ \gamma_j\in\Gamma_j)$ which correspond to 4 orbits of G on $\Omega^{(2)}\times\Omega^{(2)}$; let $x_{ij}=|X_{ij}|$,

(b) Y_{ij} $(1\leq i<j\leq k-1)$ consists of the orbits containing elements $(\{\alpha,\beta\},\{\gamma_i,\gamma_j\})$ $(\gamma_i\in\Gamma_i,\ \gamma_j\in\Gamma_j)$ which correspond to 2 orbits of G on $\Omega^{(2)}\times\Omega^{(2)}$; let $y_{ij}=|Y_{ij}|$,

(c) A_i, B_i, C_i $(1 \leq i \leq k-1)$ consist of the orbits containing elements $(\{\alpha,\beta\},\{\gamma_i,\gamma_i'\})$ $(\gamma_i,\gamma_i' \in \Gamma_i)$, the orbits in A_i, B_i, C_i corresponding respectively to 4,2,1 orbits of G on $\Omega^{(2)} \times \Omega^{(2)}$; let $a_i = |A_i|$, $b_i = |B_i|$, $c_i = |C_i|$.

The rest are:

(d) the orbit containing $(\{\alpha,\beta\},\{\alpha,\beta\})$ which corresponds to 2 orbits (one containing $((\alpha,\beta),(\alpha,\beta))$, the other $((\alpha,\beta),(\beta,\alpha))$) of G on $\Omega^{(2)} \times \Omega^{(2)}$,

(e) the orbits containing elements $(\{\alpha,\beta\},\{\alpha,\gamma_i\})$ $(\gamma_i \in \Gamma_i)$, each of which corresponds to 4 orbits (containing $((\alpha,\beta),(\alpha,\gamma_i))$, $((\alpha,\beta),(\beta,\gamma_i))$, $((\alpha,\beta),(\gamma_i,\alpha))$ and $((\alpha,\beta),(\gamma_i,\beta))$) of G on $\Omega^{(2)} \times \Omega^{(2)}$.

The orbits described in (d) and (e) contribute $1+3(k-1)$ to the difference d. Let $\alpha,\beta,\gamma,\delta$ be distinct and let Δ be the orbit of G on $\Omega^{\{2\}} \times \Omega^{\{2\}}$ containing $(\{\alpha,\beta\},\{\gamma,\delta\})$. Write $D = \{\alpha,\beta,\gamma,\delta\}$. If $\Delta \in Y_{ij}$ for some i,j then $(\alpha\beta) \in G^D_{\{D\}}$ since $G_{\{\alpha\beta\}}$ fixes Γ_i and Γ_j setwise, and if $\Delta \in C_i$ for some i then $(\alpha\beta)$, $(\gamma\delta) \in G^D_{\{D\}}$.

Now if $\Delta \in \bigcup X_{ij} \cup \bigcup Y_{ij} \cup \bigcup A_i$ then $(\gamma\delta) \notin G^D_{\{D\}}$, so $\Delta^* \notin \bigcup Y_{ij} \cup \bigcup C_i$ (where Δ^* is the orbit containing $(\{\gamma,\delta\},\{\alpha,\beta\})$), that is, $\Delta^* \in \bigcup A_i \cup \bigcup B_i \cup \bigcup X_{ij}$.

Hence

$$\sum x_{ij} + \sum y_{ij} + \sum a_i \leq \sum a_i + \sum b_i + \sum x_{ij}$$

and so

$$\sum y_{ij} \leq \sum b_i . \tag{2.1.1}$$

We have

$$d = 1+3(k-1)+3\sum x_{ij} + \sum y_{ij} + 3\sum a_i + \sum b_i .$$

Clearly $\sum x_{ij} + \sum y_{ij} \geq \frac{1}{2}(k-1)(k-2)$ so, using (2.1.1), we have

$$d = 1+3(k-1)+3\sum x_{ij} + 2\sum y_{ij} + (\sum b_i - \sum y_{ij}) + 3\sum a_i \tag{2.1.2}$$
$$\geq 1+3(k-1)+(k-1)(k-2) = k^2 .$$

REMARKS. (a) If G is PSL(2,7) acting transitively with degree 7 (see [7]) then G is generously 2-transitive, G_α has rank $k = 3$ and $d = 9 = k^2$. Hence equality may occur in the conclusion of Proposition 2.1.

(b) If G is 3-transitive (which we are assuming not to be the case elsewhere in this chapter) then $k = 2$ and certainly $d \geq 4 = k^2$ since, as the proof of Proposition 2.1 shows, we always have $d \geq 1+3(k-1)$. Also it is easy to see that $d = 4$ if and only if G is generously 3-transitive.

If G is also 2-primitive, we can say more:

PROPOSITION 2.2. Suppose that G is generously 2-transitive and 2-primitive of degree n on Ω. Then $d \geq k^2+k-2$. Further, if equality holds then $k = 3$ and, for $\alpha \in \Omega$, the pair $(G_\alpha, \Omega\setminus\{\alpha\})$ is of type (a,b) for some a, b. In particular, n is even.

PROOF. We use the notation of the proof of Proposition 2.1. First note that $|\Gamma_i| > 1$ for $i = 1,\dots,k-1$; for suppose that $|\Gamma_i| = 1$. Then it is easy to see that G_α must be regular of prime degree on $\Omega\setminus\{\alpha\}$. Now G is generously 2-transitive so $G_{\alpha\beta}$ and $G_{\{\alpha\beta\}}$ have the same orbits on $\Omega\setminus\{\alpha,\beta\}$ (all of size 1); hence G contains the 2-cycle $(\alpha\beta)$. But then G contains all 2-cycles, so $G = S_n$. This forces $n = 2$ which is impossible.

Now take Γ_{k-1} to be the largest orbit of $G_{\alpha\beta}$. Then for any $i < k-1$, $G_{\alpha\beta}$ is not transitive on $\Gamma_i \times \Gamma_{k-1}$ by Theorem 1.17(ii), so we cannot have $x_{ik-1} = 0$, $y_{ik-1} = 1$. Consequently $3x_{ik-1} + y_{ik-1} \geq 2$ and so $3x_{ik-1}+2y_{ik-1} \geq 3$. Hence

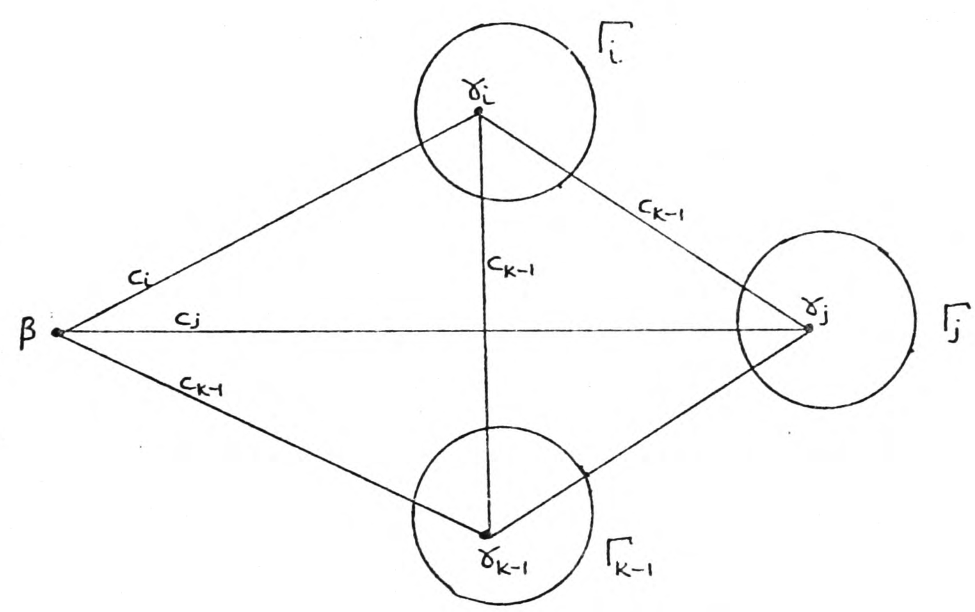
$$\begin{aligned} 3\sum x_{ij} + 2\sum y_{ij} &= \sum_{1\leq i<j\leq k-2} (3x_{ij}+2y_{ij}) + \sum_{i\leq k-2} (3x_{ik-1}+2y_{ik-1}) \\ &\geq (k-2)(k-3)+3(k-2) = k^2-2k. \end{aligned}$$

Therefore by (2.1.2), $d \geq 1+3(k-1)+k^2-2k = k^2+k-2$, as required.

Suppose now that equality holds. Then for each $i < k-1$, we must have $3x_{ik-1}+2y_{ik-1} = 3$, so that $x_{ik-1} = 1$, $y_{ik-1} = 0$; and from (2.1.2) we have $\sum a_i = 0$, $\sum b_i = \sum y_{ij}$ and $x_{ij} = 0$, $y_{ij} = 1$ for $1 \leq i < j \leq k-2$. Suppose that $k \geq 4$, and recall that each suborbit Γ_i of G_α is self-paired so that all the monochrome subgraphs of G_α are undirected. By Proposition 1.16 the c_{k-1}-monochrome subgraph is connected, so we may pick i with $1 \leqslant i < k-1$ such that $\gamma_{k-1} \in \Gamma_{k-1}(\gamma_i)$ for some $\gamma_{k-1} \in \Gamma_{k-1}$, $\gamma_i \in \Gamma_i$. Since $k \geqslant 4$ we may choose $j \notin \{i,k-1\}$ as follows: if Γ_i is the second largest suborbit, pick any $j \notin \{i,k-1\}$ with $j \geqslant 1$, and if Γ_i is not, take Γ_j to be the second largest suborbit (here, by the "second largest suborbit" we mean the largest suborbit distinct from Γ_{k-1} and of size $\leqslant |\Gamma_{k-1}|$). We have $x_{ij} = 0$, $y_{ij} = 1$ so $G_{\alpha\beta}$ is transitive on $\Gamma_i \times \Gamma_j$ and so by Theorem 1.17(ii), $\Gamma_i \circ \Gamma_j$ is a single suborbit of size greater than $|\Gamma_i|$ and $|\Gamma_j|$. By choice of j, then,

$$\Gamma_i \circ \Gamma_j = \Gamma_j \circ \Gamma_i = \Gamma_{k-1} .$$

Thus there are points $\gamma_i \in \Gamma_i$, $\gamma_{k-1} \in \Gamma_{k-1}$, $\gamma_j \in \Gamma_j$ such that the edges joining these points are coloured as in the diagram:

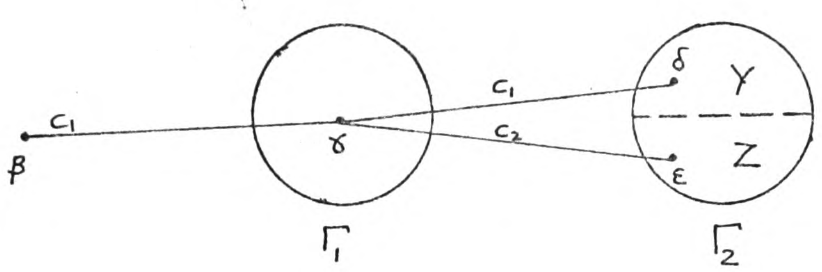


Now $x_{ik-1} = 1$, $y_{ik-1} = 0$ so $G_{\alpha\beta}$ has two orbits on $\Gamma_i \times \Gamma_{k-1}$; consequently, by Theorem 1.17(i), $\Gamma_{k-1} \circ \Gamma_i$ is a union of at most two, hence exactly two suborbits and so, from the diagram, we have $\Gamma_{k-1} \circ \Gamma_i = \Gamma_j \cup \Gamma_{k-1}$. Also $\Gamma_j \circ \Gamma_i = \Gamma_{k-1}$, so

$$(\Gamma_j \cup \Gamma_{k-1}) \circ \Gamma_i = \Gamma_j \cup \Gamma_{k-1} .$$

But this means that $\Gamma_j \cup \Gamma_{k-1}$ is a connected component in the c_i-monochrome subgraph of G_α, contradicting the primitivity of G_α (by Proposition 1.16).

Thus $k = 3$ and we have $x_{12} = 1$, $y_{12} = 0$, $a_i = b_i = 0$ for $i = 1,2$. Let $\gamma \in \Gamma_1$ and let $Y = \Gamma_1(\gamma) \cap \Gamma_2(\beta)$, $Z = \Gamma_2(\gamma) \cap \Gamma_2(\beta)$ so that $\Gamma_2 = Y \cup Z$:



We show that $|Y| = |Z|$. For since $G_{\alpha\beta}$ has two orbits on $\Gamma_1 \times \Gamma_2$, $G_{\alpha\beta\gamma}$ is transitive on Y and on Z. Pick $\delta \in Y$, $\varepsilon \in Z$ and choose $g \in G_{\{\alpha\beta\}}$ such that $\{\gamma,\delta\}g = \{\gamma,\varepsilon\}$ (we can do this since $x_{12} = 1$, $y_{12} = 0$). Then $\gamma g = \gamma$, $\delta g = \varepsilon$ since Γ_1, Γ_2 are orbits of $G_{\{\alpha\beta\}}$. Now choose any $\delta' \in Y$ and pick $h \in G_{\alpha\beta\gamma}$ such that $\delta h = \delta'$. We have $g^{-1}hg = h'$ for some $h' \in G_{\alpha\beta\gamma}$, so $\delta' g = \delta hg = \delta gh' = \varepsilon h'$ and so $\delta' g \in Z$. Thus $Yg \subseteq Z$. Similarly $Zg \subseteq Y$, so $|Y| = |Z|$. Repeating the argument with Γ_1 and Γ_2 interchanged, we see that $(G_\alpha, \Omega\backslash\{\alpha\})$ is of type (a,b) where $|\Gamma_1| = 2a$, $|\Gamma_2| = 2b$.

<u>REMARK.</u> If G is PSL(2,5) acting on PG(1,5) then G is generously 2-transitive and 2-primitive, $k = 3$ and $d = 10 = k^2+k-2$. Hence equality may hold in the conclusion of Proposition 2.2.

We consider further examples after the next proposition and its corollaries; in this proposition we drop the assumption that G is generously 2-transitive. In fact, Propositions 2.1 and 2.2 could have been deduced directly from Proposition 2.3, but their proofs have been included in order to make this chapter more readable.

<u>PROPOSITION 2.3.</u> Suppose that G is 2-transitive of degree n on Ω and write $k = k_1 + 2k_2 + 1$ where G_α $(\alpha \in \Omega)$ has k_1 self-paired suborbits and k_2 pairs of non-self-paired suborbits (acting on $\Omega\backslash\{\alpha\}$). Then

$$d \geq k_1^2 + 3k_2^2 + 3k_1k_2 + 2k_1 + 4k_2 + 1.$$

Further, if G also 2-primitive on Ω and is not $AGL(1,2^r)$ acting on $GF(2^r)$

where 2^r-1 is prime, then

$$d \geq k_1^2 + 3k_2^2 + 3k_1k_2 + 3k_1 + 7k_2$$

and if equality holds here, then $k_1 = 2$, $k_2 = 0$ and $(G_\alpha, \Omega\setminus\{\alpha\})$ is of type (a,b) for some a,b.

PROOF. Pick $\beta \in \Omega\setminus\{\alpha\}$ and let $\Gamma_1, \ldots, \Gamma_{k_1}, \Gamma_{k_1+1}, \ldots, \Gamma_{k_1+2k_2}$ be the orbits of $G_{\alpha\beta}$ on $\Omega\setminus\{\alpha\beta\}$, where if $g \in G_{\{\alpha\beta\}}\setminus G_{\alpha\beta}$ then $\Gamma_i g = \Gamma_i$ $(1 \leq i \leq k_1)$ and $\Gamma_{k_1+i} g = \Gamma_{k_1+k_2+i}$ $(1 \leq i \leq k_2)$ (we can do this by the remark on line 6 of p. 20). We partition most of the orbits of G on $\Omega^{\{2\}} \times \Omega^{\{2\}}$ into sets $X_{ij}, Y_{ij}, A_i, B_i, C_i, D_i, E_i$ as follows:

(a) X_{ij}, Y_{ij} $(1 \leq i < j \leq k_1)$ consist of the orbits containing elements $(\{\alpha,\beta\},\{\gamma_i,\gamma_j\})$ $(\gamma_i \in \Gamma_i, \gamma_j \in \Gamma_j)$ which correspond respectively to 4,2 orbits of G on $\Omega^{(2)} \times \Omega^{(2)}$,

(b) $X_{i\,k_1+j}$ $(1 \leq i \leq k_1,\ 1 \leq j \leq k_2)$ consists of the orbits containing elements $(\{\alpha,\beta\},\{\gamma_i,\gamma_{k_1+j}\})$; each of these corresponds to 4 orbits on $\Omega^{(2)} \times \Omega^{(2)}$,

(c) $X_{k_1+i\,k_1+j}$ $(1 \leq i < j \leq k_2)$ consists of the orbits containing elements $(\{\alpha,\beta\},\{\gamma_{k_1+i},\gamma_{k_1+j}\})$ and elements $(\{\alpha,\beta\},\{\gamma_{k_1+i},\gamma_{k_1+k_2+j}\})$; each corresponds to 4 orbits on $\Omega^{(2)} \times \Omega^{(2)}$ and if $x_{k_1+i\,k_1+j} = |X_{k_1+i\,k_1+j}|$ then $x_{k_1+i\,k_1+j} \geq 2$ for each i,j,

(d) A_i, B_i, C_i $(1 \leq i \leq k_1)$ consist of the orbits containing elements $(\{\alpha,\beta\},\{\gamma_i,\gamma_i'\})$ which correspond respectively to 4,2,1 orbits on $\Omega^{(2)} \times \Omega^{(2)}$,

(e) A_{k_1+i}, B_{k_1+i} $(1 \leq i \leq k_2)$ consist of the orbits containing elements $(\{\alpha,\beta\},\{\gamma_{k_1+i},\gamma_{k_1+i}'\})$ which correspond respectively to 4,2 orbits on $\Omega^{(2)} \times \Omega^{(2)}$,

(f) D_{k_1+i}, E_{k_1+i} $(1 \leq i \leq k_2)$ consist of the orbits containing elements $(\{\alpha,\beta\},\{\gamma_{k_1+i},\gamma_{k_1+k_2+i}\})$ which correspond respectively to 4,2 orbits on $\Omega^{(2)} \times \Omega^{(2)}$.

Let $x_{ij} = |X_{ij}|$, $y_{ij} = |Y_{ij}|$, $a_i = |A_i|, \ldots, e_i = |E_i|$ for each relevant i,j. As in the proof of Proposition 2.1, the orbits of G on $\Omega^{\{2\}} \times \Omega^{\{2\}}$ which are not in the above list contribute $1+3(k_1+2k_2)$ to the difference d.

Now let $\alpha,\beta,\gamma,\delta$ be distinct and let Δ be the orbit of G on $\Omega^{\{2\}} \times \Omega^{\{2\}}$ containing $(\{\alpha,\beta\},\{\gamma,\delta\})$; write $D = \{\alpha,\beta,\gamma,\delta\}$. Since every element of $G_{\{\alpha\beta\}} \setminus G_{\alpha\beta}$

interchanges Γ_{k_1+i} and $\Gamma_{k_1+k_2+i}$,

$\Delta \in Y_{ij}$ implies $(\alpha\beta) \in G^{D}_{\{D\}}$,

$\Delta \in C_i$ implies $(\alpha\beta)$, $(\gamma\delta) \in G^{D}_{\{D\}}$,

$\Delta \in B_{k_1+i}$ $(i \geq 1)$ implies $(\gamma\delta) \in G^{D}_{\{D\}}$,

$\Delta \in E_{k_1+i}$ $(i \geq 1)$ implies $(\alpha\beta)(\gamma\delta) \in G^{D}_{\{D\}}$.

Consequently, if $\Delta \in \bigcup Y_{ij}$ then $\Delta^* \in \bigcup_{1 \leq i \leq k_1+k_2} B_i$, so we have

$$\sum_{1 \leq i < j \leq k_1} y_{ij} \leq \sum_{1 \leq i \leq k_1+k_2} b_i . \tag{2.3.1}$$

Now

$$d = 1+3(k_1+2k_2)+\sum_{i,j \leq k_1}(3x_{ij}+y_{ij})+3\sum_{i \leq k_1, j \leq k_2} x_{i\,k_1+j}+3\sum_{i,j \leq k_2} x_{k_1+i\,k_1+j}$$
$$+\sum_{i \leq k_1}(3a_i+b_i)+\sum_{i \leq k_2}(3a_{k_1+i}+b_{k_1+i})+\sum_{i \leq k_2}(3d_{k_1+i}+e_{k_1+i}).$$

Also $\sum_{i,j \leq k_1}(x_{ij}+y_{ij}) \geq \frac{1}{2}k_1(k_1-1)$, $\sum_{i \leq k_1, j \leq k_2} x_{i\,k_1+j} \geq k_1 k_2$, $\sum_{i,j \leq k_2} x_{k_1+i\,k_1+j} \geq k_2(k_2-1)$ and $\sum_{i \leq k_2}(d_{k_1+i}+e_{k_1+i}) \geq k_2$. Hence, using (2.3.1),

$$d \geq 1+3(k_1+2k_2)+\sum_{i,j \leq k_1}(3x_{ij}+2y_{ij})+3\sum x_{i\,k_1+j}+3\sum x_{k_1+i\,k_1+j}$$
$$+3\sum_{i \leq k_1+k_2} a_i+\sum(3d_{k_1+i}+e_{k_1+i}) \tag{2.3.2}$$
$$\geq 1+3(k_1+2k_2)+k_1(k_1-1)+3k_1k_2+3k_2(k_2-1)+k_2$$
$$= k_1^2+3k_2^2+3k_1k_2+2k_1+4k_2+1.$$

Now suppose that G is also 2-primitive and is not $AGL(1,2^r)$ with 2^r-1 prime. Then $|\Gamma_i|>1$ for $i = 1,\dots,k_1+2k_2$; for if $|\Gamma_i| = 1$ then G_α is regular of prime degree, so G is sharply 2-transitive and hence by Proposition 1.30, G is $AGL(1,2^r)$ with 2^r-1 prime, which we have excluded.

Let $|\Gamma_{k_1}| = \max\{|\Gamma_i| : i \leq k_1\}$. If also $|\Gamma_{k_1}| = \max\{|\Gamma_i| : i \leq k_1+2k_2\}$, then by Theorem 1.17(ii), $G_{\alpha\beta}$ is not transitive on $\Gamma_i \times \Gamma_{k_1}$ for any $i<k_1$. Thus $3x_{ik_1}+y_{ik_1} \geq 2$, which gives $3x_{ik_1}+2y_{ik_1} \geq 3$, so

$$\sum_{i,j \leq k_1}(3x_{ij}+2y_{ij}) \geq k_1(k_1-1)+k_1-1 = k_1^2-1. \tag{2.3.3}$$

We now consider separately the two cases: 1. Γ_{k_1} is not the largest suborbit, 2. Γ_{k_1} is the largest suborbit.

<u>Case 1. Γ_{k_1} is not the largest suborbit.</u>

Let $\Gamma_{k_1+k_2}$ be the largest suborbit; then by Theorem 1.17(ii) we have

$x_{i\,k_1+k_2} \geq 2$ for $i \leq k_1$ and $x_{k_1+i\;k_1+k_2} \geq 4$ for $1 \leq i < k_2$ and $3d_{k_1+k_2} + e_{k_1+k_2} \geq 2$. Hence, from (2.3.2), we have

$$d \geq 1+3(k_1+2k_2)+ \quad k_1(k_1-1) \quad +3(k_1k_2+k_1)+3(k_2(k_2-1)+2(k_2-1))+(k_2+1)$$
$$= k_1^2+3k_2^2+3k_1k_2+5k_1+10k_2-4.$$

If $k_1 > 0$ then $2k_1+3k_2-4 \geq 1$, so $d \geq k_1^2+3k_2^2+3k_1k_2+3k_1+7k_2+1$, as required. If $k_1 = 0$ then, provided $k_2 \geq 2$, we have $3k_2-4 \geq 2$, so $d \geq k_1^2+3k_2^2+3k_1k_2+3k_1+7k_2+1$. Therefore we may assume that $k_1 = 0$, $k_2 = 1$. Now $G_{\alpha\beta}$ is not transitive on any of $\Gamma_1^{(2)}$, $\Gamma_2^{(2)}$ and $\Gamma_1 \times \Gamma_2$ (by Theorem 1.17(ii)), so $3a_1+b_1 \geq 2$, $3d_1+e_1 \geq 2$. It follows that

$$d = 1+6+3a_1+b_1+3d_1+e_1 \geq 11 = 3k_2^2+7k_2+1,$$

as required.

<u>Case 2. Γ_{k_1} is the largest suborbit.</u>

By Theorem 1.17(ii) we have $x_{k_1\,k_1+i} \geq 2$ for $1 \leq i \leq k_2$. Hence, from (2.3.2) and (2.3.3),

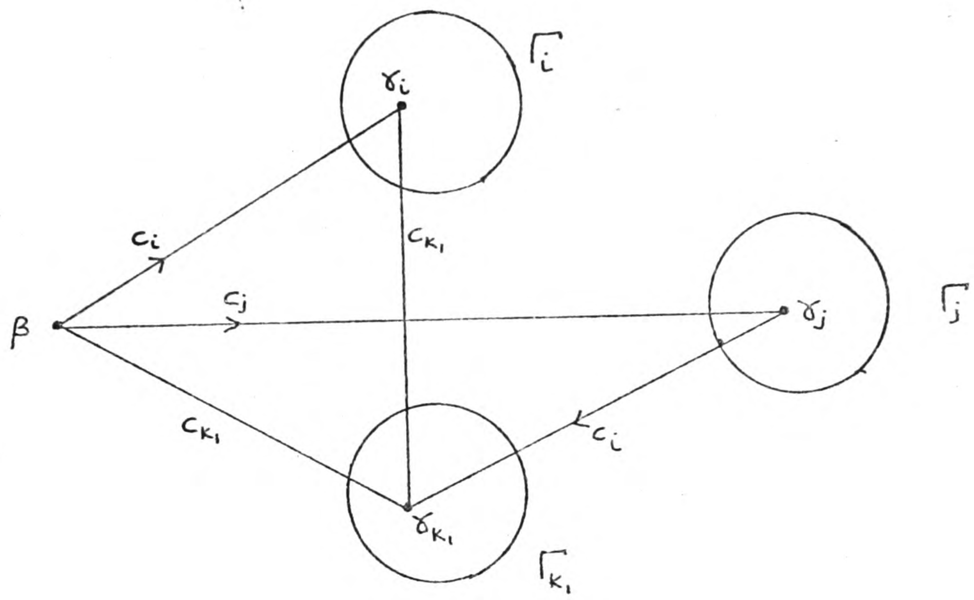
$$d \geq 1+3(k_1+2k_2)+(k_1^2-1)+3(k_1k_2+k_2)+3k_2(k_2-1)+k_2$$
$$= k_1^2+3k_2^2+3k_1k_2+3k_1+7k_2 \ .$$

If equality holds then $\sum_{i \leq k_1+k_2} a_i = \sum d_{k_1+i} = 0$ and $x_{ij} = 0$, $y_{ij} = 1$ for $1 \leq i < j < k_1$; for $i < k_1$ we have $x_{ik_1} = 1$, $y_{ik_1} = 0$ and $x_{i\,k_1+j} = 1$ for $1 \leq j \leq k_2$. Also $x_{k_1\,k_1+i} = 2$ for $1 \leq i \leq k_2$ and $x_{k_1+i\;k_1+j} = 2$ for $1 \leq i < j \leq k_2$; further, $d_{k_1+i} = 0$, $e_{k_1+i} = 1$ for $1 \leq i \leq k_2$. Consequently $G_{\alpha\beta}$ is transitive on $\Gamma_i \times \Gamma_j$ and has two orbits on $\Gamma_i \times \Gamma_{k_1}$ for any distinct i,j with $i \neq k_1$, $j \neq k_1$. Hence, if $k_1+2k_2 \geq 3$, then $|\Gamma_{k_1}| > |\Gamma_i|$ for $i \neq k_1$ and Γ_{k_1} is self-paired.

Suppose that $k_1+2k_2 \geq 3$ and pick $i \neq k_1$ such that $\gamma_{k_1} \in \Gamma_{k_1}(\gamma_i)$ for some $\gamma_{k_1} \in \Gamma_{k_1}$, $\gamma_i \in \Gamma_i$. If Γ_i is the second largest suborbit, choose any $j \notin \{i,k_1\}$ and if not, let Γ_j be the second largest suborbit. Then by Theorem 1.17(ii),

$$\Gamma_i \circ \Gamma_j = \Gamma_j \circ \Gamma_i = \Gamma_j \circ \Gamma_i^* = \Gamma_{k_1} \ .$$

Consequently there are points $\gamma_i \in \Gamma_i$, $\gamma_j \in \Gamma_j$, $\gamma_{k_1} \in \Gamma_{k_1}$ such that the (directed) edges between them are coloured as follows in the edge-coloured complete graph associated with G_α:



Now $G_{\alpha\beta}$ has two orbits on $\Gamma_i^* \times \Gamma_{k_1}$, so $\Gamma_{k_1} \circ \Gamma_i^*$ is a union of two suborbits (Theorem 1.17(i)). Hence, from the diagram, $\Gamma_{k_1} \circ \Gamma_i^* = \Gamma_{k_1} \cup \Gamma_j$. It follows that

$$(\Gamma_{k_1} \cup \Gamma_j) \circ \Gamma_i^* = \Gamma_{k_1} \cup \Gamma_j .$$

This means that the c_i^*-monochrome subgraph is not strongly connected, which contradicts the primitivity of G_α (by Proposition 1.16).

Thus $k_1 + 2k_2 \leqslant 2$, so $k_1 = 2$, $k_2 = 0$; now the result follows from Proposition 2.2.

REMARKS. (a) If G is $AGL(1,2^r)$ acting on $GF(2^r)$ where 2^r-1 is prime then $k_1 = 0$, $k_2 = 2^{r-1}-1$ and $d = 2^{r-2}(3.2^r-4) = 3k_2^2+4k_2+1$, as is shown in the examples considered after the following corollaries.

(b) The proof of Proposition 2.3 shows that if $k_1 = 0$ and G is 2-primitive then $d \geqslant 3k_2^2 + 10k_2 - 4$ (see Case 1 in this proof). Also if $k_1 = 0$, $k_2 = 1$ and G is 2-primitive then it is fairly easy to show that $d \geqslant 13$; and $PSL(2,7)$ acting on $PG(1,7)$ is 2-primitive with $k_1 = 0$, $k_2 = 1$ and $d = 13$.

We now deduce two corollaries concerning the characters $\chi^{(n-2,2)}$, $\chi^{(n-2,1^2)}$ of G introduced in Section 3 of Chapter 1.

<u>COROLLARY 2.4.</u> Suppose that G is 2-transitive of degree n on Ω with $k = 1+k_1+2k_2$ $(\geqslant 3)$ as in Proposition 2.3. Let $\|\chi^{(n-2,1^2)}\|_G = e$, $\langle \chi^{(n-2,1^2)}, \chi^{(n-2,2)}\rangle_G = f$. Then $e+2f \geqslant k_1^2+3k_2^2+3k_1k_2-2k_2$. If G is also 2-primitive and is not $AGL(1,2^r)$ acting on $GF(2^r)$ where 2^r-1 is prime, then

$$e+2f \geqslant k_1^2+3k_2^2+3k_1k_2+k_1+k_2-1,$$

equality here implying that $k_1 = 2$, $k_2 = 0$, n is even and $(G_\alpha, \Omega\setminus\{\alpha\})$ is of type (a,b) for some a,b.

<u>PROOF.</u> Pick $\alpha, \beta \in \Omega$. Now certainly $\langle 1, \chi^{(n-2,2)}+\chi^{(n-2,1^2)}\rangle_G = 0$. Also

$$k_1+2k_2 = \#\mathrm{orb}(G_{\alpha\beta}, \Omega\setminus\{\alpha,\beta\}) = \#\mathrm{orb}(G, \Omega\times\Omega^{(2)}) - 2 = \langle \pi, \xi\rangle_G - 2$$

and $$k_1+k_2 = \#\mathrm{orb}(G_{\{\alpha\beta\}}, \Omega\setminus\{\alpha,\beta\}) = \#\mathrm{orb}(G, \Omega\times\Omega^{\{2\}}) - 1 = \langle \pi, \eta\rangle_G - 1 .$$

Hence $k_2 = \langle \pi, \xi-\eta\rangle_G - 1 = \langle 1+\chi^{(n-1,1)}, \chi^{(n-1,1)}+\chi^{(n-2,1^2)}\rangle_G - 1 = \langle \chi^{(n-1,1)}, \chi^{(n-2,1^2)}\rangle_G$.

Also $\langle \chi^{(n-1,1)}, \chi^{(n-2,2)}\rangle_G = \langle \pi, \eta\rangle_G - 2 = k_1+k_2-1$. We may write

$$\eta = 1+(k_1+k_2)\chi^{(n-1,1)}+(\chi^{(n-2,2)}-(k_1+k_2-1)\chi^{(n-1,1)}),$$

$$\xi = 1+k\chi^{(n-1,1)}+(\chi^{(n-2,2)}-(k_1+k_2-1)\chi^{(n-1,1)})+(\chi^{(n-2,1^2)}-k_2\chi^{(n-1,1)}).$$

Therefore $d = \|\xi\|_G - \|\eta\|_G = k^2-(k_1+k_2)^2+(e-k_2^2)+2f-2k_2(k_1+k_2-1)$; consequently $d = e+2f+2k_1+6k_2+1$. By Proposition 2.3, then,

$$e+2f \geqslant k_1^2+3k_2^2+3k_1k_2-2k_2 ,$$

and if G is 2-primitive and is not $AGL(1,2^r)$ where 2^r-1 is prime, then

$$e+2f \geqslant k_1^2+3k_2^2+3k_1k_2+k_1+k_2-1$$

equality here implying that $k_1 = 2$, $k_2 = 0$ and $(G_\alpha, \Omega\setminus\{\alpha\})$ is of type (a,b) for some a,b.

<u>COROLLARY 2.5.</u> Suppose that G is generously 2-transitive of degree n on Ω, and let $\|\chi^{(n-2,1^2)}\|_G = e$, $\langle \chi^{(n-2,2)}, \chi^{(n-2,1^2)}\rangle_G = f$. Then $e+2f \geqslant (k-1)^2$. If G is also 2-primitive then $e+2f \geqslant k^2-k-1$, equality here implying that $k = 3$, n is even and G_α is of type (a,b) for some a,b.

SOME EXAMPLES.

We calculate the numbers d, k, k_1, k_2 for the affine groups $AGL(1,q)$ acting on $GF(q)$ and for the projective groups $PSL(2,q)$ acting on $PG(1,q)$ (q a prime power).

(a) Affine groups $AGL(1,q)$.

Let G be $AGL(1,q)$ acting on $GF(q)$ ($q>3$), so that

$$G = \{\pi_{a,b} \mid a \in GF(q)\setminus\{0\},\ b \in GF(q)\}$$

where $\pi_{a,b}$ is the permutation: $x \to ax+b$ of $\Omega = GF(q)$. The pointwise and setwise stabilisers of the subset $\{0,1\}$ of Ω are:

$$G_{01} = 1,\quad G_{\{01\}} = \{1, \pi_{-1,1}\}.$$

Now $\pi_{-1,1}$ is the permutation: $x \to -x+1$ of Ω; it has one fixed point, $\frac{q-1}{2}$ 2-cycles if q is odd, and it has no fixed points, $\frac{q}{2}$ 2-cycles if q is even. Thus G is 2-transitive but not generously 2-transitive; it is 2-primitive if and only if q is even and $q-1$ is prime. In the notation of Proposition 2.3, we have $k = q-1$ and

$$k_1 = \begin{cases} 1 \\ 0 \end{cases},\quad k_2 = \begin{cases} \frac{q-3}{2} & \text{if } q \text{ is odd.} \\ \frac{q-2}{2} & \text{if } q \text{ is even.} \end{cases}$$

Now we calculate the number d. Each orbit of $G_{\{01\}}$ on $\Omega^{\{2\}}$ has size 1 or 2; there are $\frac{q-1}{2}$ or $\frac{q}{2}$ orbits of size 1 according as q is odd or even. Therefore the number of orbits of size 2 is $\frac{1}{2}\left(\frac{q(q-1)}{2} - \frac{q-1}{2}\right) = \frac{1}{4}(q-1)^2$ if q is odd, and is $\frac{1}{2}\left(\frac{q(q-1)}{2} - \frac{q}{2}\right) = \frac{1}{4}q(q-2)$ if q is even. Hence

$$\#\operatorname{orb}(G, \Omega^{\{2\}} \times \Omega^{\{2\}}) = \#\operatorname{orb}(G_{\{01\}}, \Omega^{\{2\}}) = \begin{cases} \frac{1}{4}(q^2-1), & q \text{ odd.} \\ \frac{1}{4}(q^2), & q \text{ even.} \end{cases}$$

Also $\#\operatorname{orb}(G, \Omega^{(2)} \times \Omega^{(2)}) = \#\operatorname{orb}(G_{01}, \Omega^{(2)}) = |\Omega^{(2)}| = q^2 - q$. Thus

$$d = \begin{cases} \frac{1}{4}(3q^2-4q+1), & q \text{ odd.} \\ \frac{1}{4}(3q^2-4q), & q \text{ even.} \end{cases}$$

In both cases we find that $d = k_1^2 + 3k_2^2 + 3k_1k_2 + 2k_1 + 4k_2 + 1$, so that equality holds in the conclusion of Proposition 2.3.

(b) Projective groups PSL(2,q).

Let G be PSL(2,q) acting on PG(1,q). If q is even then G is 3-transitive, so we assume that q is odd. We may identify PG(1,q) with $\Omega = GF(q) \cup \{\infty\}$ in such a way that PSL(2,q) is the group

$$\left\{ x \to \frac{ax+b}{cx+d} \;\middle|\; a,b,c,d \in GF(q),\ ad-bc \text{ is a square in } GF(q)\setminus\{0\} \right\}$$

of permutations of Ω. Thus $G_{0\infty} = \{ x \to ax \mid a \text{ is a nonzero square}\}$ and $G_{\{0\infty\}} = \{ x \to ax,\ x \to \frac{-a}{x} \mid a \text{ is a nonzero square}\}$. Consequently $G_{0\infty}$ has two orbits $\Gamma_1 = \{x \mid x \text{ is a nonzero square}\}$ and $\Gamma_2 = \{x \mid x \text{ is a non-square}\}$ on $\Omega\setminus\{0,\infty\}$. Hence k = 3. Also $|G_{0\infty}| = \frac{q-1}{2}$, $|G_{\{0\infty\}}| = q-1$. We consider separately the cases $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$.

Case 1. $q \equiv 1 \pmod 4$.

In this case -1 is a square in GF(q) so $G_{\{0\infty\}}$ also has the two orbits Γ_1, Γ_2 on $\Omega\setminus\{0,\infty\}$ and G is generously 2-transitive and 2-primitive on Ω. We first calculate $\#\mathrm{orb}(G_{\{0\infty\}}, \Omega^{\{2\}})$. Suppose that $\{\alpha,\beta\}g = \{\alpha,\beta\}$ for some distinct $\alpha,\beta \in \Omega\setminus\{0,\infty\}$, $1 \neq g \in G_{\{0\infty\}}$. If g is the permutation $x \to ax$ then $a\alpha = \beta$, $a\beta = \alpha$, so a is -1 and $\beta = -\alpha$. If g is $x \to \frac{a}{x}$ then either $\frac{a}{\alpha} = \alpha$, $\frac{a}{\beta} = \beta$, whence $\beta = -\alpha$ and $a = \alpha^2$, or $\frac{a}{\alpha} = \beta$, $\frac{a}{\beta} = \alpha$, whence $a = \alpha\beta$. It follows that

$$|G_{\{0\infty\}} \cap G_{\{\alpha\beta\}}| = \begin{cases} 4, & \text{if } \beta = -\alpha \\ 2, & \text{if } \alpha\beta \text{ is a square and } \beta \neq -\alpha \\ 1, & \text{if } \alpha\beta \text{ is a non-square.} \end{cases}$$

Thus $G_{\{0\infty\}}$ has the following orbits on $\Omega^{\{2\}}$:

2 orbits of size $\frac{q-1}{4}$ on $\{\{\alpha,-\alpha\} \mid \alpha \in \Omega\setminus\{0,\infty\}\}$

$\frac{q-1}{2} - 2$ orbits of size $\frac{q-1}{2}$ on $\{\{\alpha,\beta\} \mid \alpha,\beta \in \Omega\setminus\{0,\infty\},\ \alpha\beta \text{ square},\ \beta \notin \{-\alpha,\alpha\}\}$

$\frac{q-1}{4}$ orbits of size q-1 on $\{\{\alpha,\beta\} \mid \alpha,\beta \in \Omega\setminus\{0,\infty\},\ \alpha\beta \text{ non-square}\}$

2 orbits of size q-1 on $\{\{\alpha,\beta\} \mid |\{\alpha,\beta\}\cap\{0,\infty\}| = 1\}$

1 orbit of size 1 on $\{\{0,\infty\}\}$.

Therefore $\#\mathrm{orb}(G, \Omega^{\{2\}}\times\Omega^{\{2\}}) = 2+\frac{q-1}{2}-2+\frac{q-1}{4}+2+1 = \frac{1}{4}(3q+9)$. Also every orbit of $G_{0\infty}$ apart from $\{(0,\infty)\}$ and $\{(\infty,0)\}$ on $\Omega^{(2)}$ has size $\frac{q-1}{2}$. Thus $\#\mathrm{orb}(G, \Omega^{(2)}\times\Omega^{(2)}) = 2+\frac{q(q+1)-2}{(q-1)/2} = 2(q+3)$. Hence $d = 2(q+3)-\frac{1}{4}(3q+9)$, so

$$d = \tfrac{1}{4}(5q+15).$$

Also G is 2-primitive and $k^2+k-2 = 10$, so PSL(2,q) ($q\equiv 1 \pmod 4$) gives equality in the conclusion of Proposition 2.2 only when $q = 5$.

Case 2. $q\equiv 3 \pmod 4$.

Here, -1 is a non-square in GF(q) so $G_{\{0\infty\}}$ is transitive on $\Omega\setminus\{0,\infty\}$ and G is not generously 2-transitive; we have $k_1 = 0$, $k_2 = 1$. A similar calculation to the one above gives

$$\#\mathrm{orb}(G, \Omega^{\{2\}}\times\Omega^{\{2\}}) = \tfrac{1}{4}(3q+7).$$

Hence $d = 2(q+3)-\frac{1}{4}(3q+7) = \frac{1}{4}(5q+17)$. Also G is 2-primitive; if $q = 3$ then $G = PSL(2,3) = AGL(1,4) = A_4$ (all of degree 4) and $d = 8 = 3k_2^2+4k_2+1$. If $q = 7$ then $d = 13$ (see Remark (b) on p.36).

---

2. ON 3-TRANSITIVE GROUPS.

Let G be a permutation group on a set Ω of size n, and partition the orbits of G on $\Omega^{\{2\}}\times\Omega^{\{2\}}$ into subsets X,Y,Z where the orbits in X,Y,Z correspond (via the natural G-morphism from $\Omega^{(2)}\times\Omega^{(2)}$ to $\Omega^{\{2\}}\times\Omega^{\{2\}}$) respectively to 4,2,1 orbits of G on $\Omega^{(2)}\times\Omega^{(2)}$. We have

$$\|\eta\|_G = x+y+z, \quad \|\xi\|_G = 4x+2y+z$$

where, as usual, η, ξ are the characters of G associated with $\Omega^{\{2\}}$, $\Omega^{(2)}$, and $x = |X|$, $y = |Y|$, $z = |Z|$. In this section we prove some results relating the way G acts on Ω with the numbers x,y,z, mainly when G is 3-transitive.

If Δ is an orbit of G on $\Omega^{\{2\}}\times\Omega^{\{2\}}$ containing $(\{\alpha,\beta\},\{\gamma,\delta\})$, denote by Δ^*, the orbit containing $(\{\gamma,\delta\},\{\alpha,\beta\})$; we say that Δ is <u>self-paired</u> if $\Delta^*=\Delta$ and use a similar notation for orbits of G on $\Omega^{(2)}\times\Omega^{(2)}$. If G is 3-transitive, denote by Δ_0 the orbit on $\Omega^{\{2\}}\times\Omega^{\{2\}}$ containing $(\{\alpha,\beta\},\{\alpha,\beta\})$ $(\alpha,\beta\in\Omega,\alpha\neq\beta)$, and denote by Δ_1 the orbit containing $(\{\alpha,\beta\},\{\alpha,\gamma\})$ $(\gamma\in\Omega\setminus\{\alpha,\beta\})$. Then $\Delta_0\in Y$, $\Delta_1\in X$ and $\Delta_0=\Delta_0^*$, $\Delta_1=\Delta_1^*$.

<u>PROPOSITION 2.6.</u> The group G is a little generously 3-transitive (see Section 4 of Chapter 1) if and only if every orbit in Y is self-paired and x = 1.

<u>PROOF.</u> Certainly if G is a little generously 3-transitive then x = 1 and every orbit of G on $\Omega^{\{2\}}\times\Omega^{\{2\}}$, hence every orbit in Y, is self-paired. Conversely, suppose that x = 1 and that every orbit in Y is self-paired, and let $D=\{\alpha,\beta,\gamma,\delta\}\in\Omega^{\{4\}}$. If $(\{\alpha,\beta\},\{\gamma,\delta\})\in\Delta\in Y$ then $(\alpha\beta)(\gamma\delta)\in G^D_{\{D\}}$ for if $(\alpha\beta)\in G^D_{\{D\}}$ then $(\gamma\delta)\in G^D_{\{D\}}$ also, since $(\{\gamma,\delta\},\{\alpha,\beta\})\in\Delta$ (Δ is self-paired). And if $(\{\alpha,\beta\},\{\gamma,\delta\})\in\Delta\in Z$ then certainly $(\alpha\beta)(\gamma\delta)\in G^D_{\{D\}}$. Hence $V_4\leq G^D_{\{D\}}$, so G is a little generously 3-transitive.

<u>PROPOSITION 2.7.</u> Suppose that G is 3-transitive and that every orbit in $X\cup Z$ is self-paired. Then $x\leq y$.

<u>PROOF.</u> If x = 1 then certainly $x\leq y$ (since $\Delta_0\in Y$), so suppose that $x>1$. Pick $\Delta\in X\setminus\{\Delta_1\}$, and let $(\{\alpha,\beta\},\{\gamma,\delta\})\in\Delta$. Then $(\alpha\beta)(\gamma\delta)\notin G^D_{\{D\}}$ (where $D=\{\alpha,\beta,\gamma,\delta\}$). By hypothesis, $\Delta=\Delta^*$, so we may suppose that $(\alpha\gamma)(\beta\delta)\in G^D_{\{D\}}$. If Ψ is the orbit of G on $\Omega^{\{2\}}\times\Omega^{\{2\}}$ containing $(\{\alpha,\gamma\},\{\beta,\delta\})$ then certainly $\Psi\notin X$; suppose that $\Psi\in Z$. Then $(\alpha\gamma)$, $(\beta\delta)\in G^D_{\{D\}}$. Also $\Psi=\Psi^*$ by hypothesis so, since $(\alpha\beta)(\gamma\delta)\notin G^D_{\{D\}}$, we must have $(\alpha\beta\gamma\delta)\in G^D_{\{D\}}$. But then

$$(\beta\delta)(\alpha\beta\gamma\delta)=(\alpha\beta)(\gamma\delta)\in G^D_{\{D\}}$$

which is not so. Hence $\Psi\in Y$. If Ψ is self-paired then $(\alpha\beta\gamma\delta)\in G^D_{\{D\}}$ and the elements $(\{a,b\},\{c,d\})$ of $\Omega^{\{2\}}\times\Omega^{\{2\}}$ with $\{a,b,c,d\} = D$ all fall into one of the two orbits Δ and Ψ ; so in this case Ψ is uniquely determined by Δ . If Ψ is not self-paired then the elements $(\{a,b\},\{c,d\})$ with $\{a,b,c,d\} = D$ all fall into one of the four orbits Ψ, Ψ^* , Δ and Δ' where $(\{\alpha,\delta\},\{\beta,\gamma\})\in\Delta'$, $\Delta'\in X$ and $\Delta\neq\Delta'$. Clearly then the map from $X\setminus\{\Delta_1\}$ to $Y\setminus\{\Delta_0\}$ taking $\Delta\to\Psi$ if $\Psi=\Psi^*$ and taking $\Delta\to\Psi$, $\Delta'\to\Psi^*$ if $\Psi\neq\Psi^*$, is one-to-one. Hence $x\leq y$.

COROLLARY 2.8. Suppose that G is 3-transitive and that every orbit in $X\cup Z$ is self-paired. Then $\#\mathrm{orb}(G,\Omega^{\{4\}})\leq y+z-1$.

PROOF. By the proof of Proposition 2.7 there is a one-to-one map $f: X\setminus\{\Delta_1\}\to Y\setminus\{\Delta_0\}$ such that, for any $\Delta\in X\setminus\{\Delta_1\}$, Δ and $f(\Delta)$ correspond to the same orbit of G on $\Omega^{\{4\}}$. It follows that $\#\mathrm{orb}(G,\Omega^{\{4\}})\leq y+z-1$.

COROLLARY 2.9. Suppose that G is 3-transitive and that every orbit of G on $\Omega^{\{2\}}\times\Omega^{\{2\}}$ is self-paired; suppose further that $\|\xi\|_G-\|\eta\|_G\leq 7$. Then G is a little generously 3-transitive. In particular, if $\|\chi^{(n-2,1^2)}\|\leq 2$ then the same conclusion holds.

PROOF. We have $3x+y = \|\xi\| - \|\eta\| \leq 7$ and $x\leq y$ by Proposition 2.7, so $x = 1$ and G is a little generously 3-transitive by Proposition 2.6. The last part follows since η is multiplicity-free by Corollary 1.22, and

$$\|\xi\| - \|\eta\| = 3 + \|\chi^{(n-2,1^2)}\| + 2\ \langle\chi^{(n-2,2)},\chi^{(n-2,1^2)}\rangle\ .$$

EXAMPLE. Let G be PSL(2,q) acting on PG(1,q) where q is a power of 2 and $q\geq 4$. Then G is a little generously 3-transitive (see Example 6.2 of [30]), so $x = 1$ by Proposition 2.6. Similar calculations to those performed in Section 1 of this chapter show that $\|\eta\|_G = \frac{1}{2}(q+2)$ and $\|\xi\|_G = q+4$. Thus $y+z = \frac{1}{2}q$, $2y+z = q$, so $y = \frac{1}{2}q$, $z = 0$, $x = 1$.

PROPOSITION 2.10. For any group G, let b be the number of self-paired orbits of G on $\Omega^{\{2\}}\times\Omega^{\{2\}}$. Then $b \geq z-x+3$ and also $b \geq \frac{z}{2}+2$.

PROOF. Let Z^* be the set of non-self-paired orbits in Z and let $|Z^*| = 2z^*$. Pick $\Delta \in Z^*$ and let $(\{\alpha,\beta\},\{\gamma,\delta\}) \in \Delta$. Then $(\alpha\gamma)(\beta\delta) \notin G^D_{\{D\}}$ (where $D = \{\alpha,\beta,\gamma,\delta\}$) and so $(\alpha\gamma)$, $(\beta\delta) \notin G^D_{\{D\}}$ since $(\alpha\beta)$, $(\gamma\delta) \in G^D_{\{D\}}$. Hence $(\{\alpha,\gamma\},\{\beta,\delta\}) \in \Psi \in X$. Further, $\Psi = \Psi^*$ and Ψ is uniquely determined by the pair (Δ,Δ^*) since any element $(\{a,b\},\{c,d\})$ with $\{a,b,c,d\} = D$ lies in one of Δ,Δ^* and Ψ. Thus the map $(\Delta,\Delta^*) \to \Psi$ is a one-to-one map from pairs in Z^* to self-paired orbits in X, so $z^* \leq x-1$. Now if b_X, b_Y, b_Z denote the numbers of self-paired orbits in X,Y,Z respectively, then

$$b_Z = z-2z^*, \quad b_X \geq z^*+1 \text{ and } b_Y \geq 1.$$

Therefore $b = b_X+b_Y+b_Z \geq z-2z^*+z^*+1+1 = z-z^*+2$. It follows that $b \geq \frac{z}{2}+2$ and also $b \geq z-x+3$ (since $z^* \leq x-1$).

We conclude this chapter with a result which shows that $y+z \geq 3$ for certain groups.

PROPOSITION 2.11. Let G be 3-transitive, n odd, and suppose that for $\alpha,\beta \in \Omega$ $G_{\{\alpha\beta\}}$ is imprimitive on $\Omega\setminus\{\alpha,\beta\}$ with blocks of odd size. Suppose also that for $\gamma \in \Omega\setminus\{\alpha,\beta\}$, $G_{\alpha\beta\gamma}$ has an orbit Γ of odd size on $\Omega\setminus(\{\alpha,\beta\} \cup \Delta_1)$ where Δ_1 is the block of imprimitivity containing γ. Then $y+z \geq 3$.

PROOF. Let $\Delta_1,\ldots,\Delta_k$ be the block system for $G_{\{\alpha\beta\}}$ with $|\Delta_i|$ odd. First we show that every orbit of $G_{\{\alpha\beta\}\gamma}$ on $\Omega\setminus\{\alpha,\beta,\gamma\}$ has even size; for suppose that $u = |G_{\{\alpha\beta\}\gamma}:G_{\{\alpha\beta\}\gamma\delta}|$ is odd for some $\delta \in \Omega\setminus\{\alpha,\beta,\gamma\}$. Then

$$|G:G_{\{\alpha\beta\}\gamma\delta}| = \tfrac{1}{2}n(n-1)(n-2)u,$$

so $|G_{\gamma\delta}:G_{\{\alpha\beta\}\gamma\delta}| = \frac{1}{2}(n-2)u$, which is certainly not possible (n is odd).

It follows that Γ is not an orbit of $G_{\{\alpha\beta\}\gamma}$, so $G_{\{\alpha\beta\}\gamma}$ pairs Γ with a different orbit Γ^* of $G_{\alpha\beta\gamma}$. Let T be a Sylow 2-subgroup of $G_{\{\alpha\beta\}\gamma}$; then T acts on $\Gamma \cup \Gamma^*$ without fixed points. Since $|\Gamma \cup \Gamma^*| \equiv 2 \pmod 4$, T has an orbit $\{\delta,\varepsilon\}$ of size 2 on $\Gamma \cup \Gamma^*$ and, say, $\delta \in \Gamma$, $\varepsilon \in \Gamma^*$. Suppose that $\delta, \varepsilon \in \Delta_i$ for some i (so that $i \geqslant 2$). Then T fixes Δ_i setwise and so, since $|\Delta_i|$ is odd, T fixes a point σ of Δ_i. However, this means that $\{\sigma\}$ is an orbit of T on $\Omega \setminus \{\alpha,\beta,\gamma\}$ of odd size, contradicting Theorem 3.4 of [40].

Consequently there exist distinct i,j such that $\delta \in \Delta_i$, $\varepsilon \in \Delta_j$. Clearly $(\alpha\beta)(\delta\varepsilon) \in G^D_{\{D\}}$ (where $D = \{\alpha,\beta,\delta,\varepsilon\}$), so $(\{\alpha,\beta\},\{\delta,\varepsilon\}) \in \Delta \in Y \cup Z$.

Now T fixes Δ_1 setwise and has orbits of even size on $\Delta_1 \setminus \{\gamma\}$, so we may pick an involution $t = (\rho\lambda)\ldots.$ of T with $\rho, \lambda \in \Delta_1 \setminus \{\gamma\}$. Then $(\{\alpha,\beta\},\{\rho,\lambda\}) \in \Psi \in Y \cup Z$. Clearly $\Psi \neq \Delta$ since $\Delta_1, \ldots, \Delta_k$ is a block system for $G_{\{\alpha\beta\}}$. Hence $Y \cup Z$ contains at least three orbits Δ_0, Δ and Ψ , so $y+z \geqslant 3$.

"This is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning."

Winston Churchill, Speech at the Mansion House, Nov. 1942.

Chapter 3: A THEOREM ON GROUPS OF PRIME DEGREE.

This chapter consists of a proof of the following theorem:

THEOREM 3.1. Let G be an insoluble, transitive permutation group of degree p, where $p = 4q+1$ and p,q are prime. Then either G is 3-transitive or $q = 3$, $p = 13$ and G is PSL(3,3) acting on the projective plane PG(2,3).

The theorem has the following corollary, a proof of which is given in the Appendix.

COROLLARY 3.2. If G is an insoluble, transitive group of degree p, where $p = 4q+1 = 3r+2 = 2s+3$ and p,q,r,s are all prime, then G contains the alternating group A_p.

The two smallest sets of primes p,q,r,s to which Corollary 3.2 applies are:

$$p = 1229,\ q = 307,\ r = 409,\ s = 613,$$

and $$p = 2309,\ q = 577,\ r = 769,\ s = 1153.$$

PROOF OF THEOREM 3.1.

Let G be an insoluble, transitive permutation group on Ω of degree p, where $p = 4q+1$ and p,q are prime, and suppose that G is not 3-transitive. Now G is 2-transitive by Theorem 1.25; also if $p = 13$ then by Proposition 1.31 G is PSL(3,3) acting on PG(2,3), so we suppose that p is not 13. By Theorem 1.29 we may assume that $q > 37$. Let π, ξ, η, ζ, $\chi^{(p-1,1)} = \chi_1$, χ_2, $\chi^{(p-2,2)}$ and $\chi^{(p-2,1^2)}$ be the characters of G defined in Sections 3 and 5 of Chapter 1.

Let P be a Sylow p-subgroup of G; then P is cyclic of order p and $C_G(P) = P$. Let $t = |N_G(P):P|$. By Theorem 1.11, t is odd; also t divides $p-1$, so t is 1 or q. If $t = 1$ an easy counting argument shows that $G = P$, so $t = q$. Hence $N_G(P) = PQ$ where Q is a cyclic group of order q fixing just one point, say α, of Ω. It follows from Theorem 1.26 that Q is a Sylow q-subgroup of G. Now G is 2-primitive by Theorem 1.28, so G_α is primitive of degree $4q$ on $\Omega\setminus\{\alpha\}$. Therefore $C_G(Q) = Q$ by Theorem 1.18. We also have $N_G(Q) = QR$ where $R = \langle c\rangle$ is a cyclic group whose order divides $q-1$; if $|R| = r$ then Burnside's Transfer Theorem shows that $r > 1$.

We have seen that $|P| = p$, $|Q| = q$ and $C_G(P) = P$, $C_G(Q) = Q$. In this situation Theorem 1.1 gives the following information about the ordinary irreducible characters of G:

(i) the principal p-block (q-block) is the only p-block (q-block) of defect one,

(ii) the principal p-block contains q p-rational irreducible characters whose degrees are congruent to 1 or -1 (mod p), and contains 4 p-exceptional characters (which do not appear in ξ, by Theorem 1.12(i)),

(iii) the principal q-block contains r q-rational irreducible characters whose degrees are congruent to 1 or -1 (mod q), and contains $\frac{q-1}{r}$ q-exceptional characters $\psi_1,\dots,\psi_{\frac{q-1}{r}}$ with $\psi_i(1)$ congruent to r or $-r$ (mod q).

The remainder of the proof is divided into eight steps. In the first we prove some preliminary lemmas and in the second we show that $q-1 > 5r$, that is, that there are at least six q-exceptional characters, a fact which is useful in the ensuing steps. Steps 3,4 and 5 are devoted to showing that the rank of G_α on $\Omega\setminus\{\alpha\}$ must be 3; this is done largely by consideration of the characters $\chi^{(p-2,2)}$ and $\chi^{(p-2,1^2)}$. Finally the proof of the theorem is completed in Steps 6,7 and 8, using the results of Chapter 2.

STEP 1. Some preliminary lemmas.

We first prove:

LEMMA 3.3. The group G is simple.

PROOF. Let H be a nontrivial normal subgroup of G. Then p divides $|H|$, so $P \leq H$ and by the Frattini argument, $G = HN_G(P)$. It follows that $\frac{G}{H} \cong \frac{N_G(P)}{N_H(P)}$. However, we know that $|N_G(P)| = pq$, so if $H < G$ then $N_H(P) = P$. This forces $H = P$ which means that $P \lhd G$; consequently G is soluble, which is not the case. Thus $H = G$ and G is simple.

As in Section 5 of Chapter 1 let K_p (K_q) be a p-adic (q-adic) splitting field for G with local ring of integers R_p (R_q). Recall (see Section 1 of Chapter 1) that the ordinary character χ in the Brauer p-tree of G is an end-node if and only if an R_pG-module X affording χ (or affording one of the exceptional characters if χ is the sum of these) remains irreducible when reduced modulo p, that is, if and only if the $\overline{K}_pG$-module $\overline{X} = \overline{K}_p \otimes X$ is irreducible; a similar condition holds for the Brauer q-tree. The next two lemmas are very similar to Lemmas 4.1 and 4.2 of [29].

LEMMA 3.4. If χ is an ordinary irreducible character of G of degree p or of degree 2p-1, then χ is an end-node in the Brauer q-tree of G.

PROOF. Let X be an R_qG-module affording χ and consider its reduction $\overline{X}$ modulo q. Since PQ is a Frobenius group, it has four faithful irreducible representations, all of degree q, in any field whose characteristic is not p. Now χ has degree p or 2p-1 so by Proposition 1.10, χ_{PQ} has precisely one linear constituent. Consequently, since $\overline{X}$ represents G faithfully, it has one linear, and 4 or 8 non-linear composition factors as a $\overline{K}_qPQ$-module, according as $\chi(1)$ is $p = 4q+1$ or $2p-1 = 8q+1$. It follows that if $\overline{X}$ is reducible as a $\overline{K}_q G$-module then one of its composition factors has degree divisible by q, which is not the case. Therefore $\overline{X}$ is irreducible and χ is an end-node in the Brauer q-tree.

<u>LEMMA 3.5.</u> Suppose that $q-1 > 2r$ and that the q-exceptional characters ψ_i appear in ξ. Then $\psi_i(1)$ is one of $(r-1)p+1$, rp and $(r+1)p-1$.

<u>PROOF.</u> Each ψ_i is certainly p-rational, so $\psi_i(1) = kp+\varepsilon$ where k is an integer and ε is $-1,0$ or 1. By Proposition 1.10 the restriction $(\psi_i)_{PQ}$ has $k+\varepsilon$ linear constituents (counting multiplicities) so we may write

$$(\psi_i)_{PQ} = \sum_{j=1}^{4k} \rho_{ij} + \Lambda_i$$

where each ρ_{ij} is an irreducible character of PQof degree q and Λ_i is a sum of $k+\varepsilon$ linear characters of PQ.

Now $\sum_{1}^{q-1/r} \psi_i$ is a constituent of either η or ξ, since the ψ_i are all q-conjugate and η, ξ are rational-valued. Also by Proposition 1.9(ii), if λ is a linear character of PQ then $\langle\lambda,\eta\rangle_{PQ} = \langle\lambda,\xi\rangle_{PQ} = 2$. Consequently $\sum_{1}^{q-1/r} \Lambda_i$ contains each linear character of PQ at most twice; it follows that each Λ_i does not contain the principal character 1_{PQ}, since the ψ_i are all q-conjugate and $\frac{q-1}{r} > 2$. Now PQ has $q-1$ distinct nonprincipal linear characters, so

$$(k+\varepsilon)\,\frac{q-1}{r} \leqslant 2(q-1)$$

which gives $k+\varepsilon \leqslant 2r$. We know that $\psi_i(1) \equiv k+\varepsilon \pmod q$. If $\psi_i(1) \equiv -r \pmod q$ then $k+\varepsilon \geqslant q-r$, so that $q-r \leqslant 2r$, contradicting the hypothesis that $\frac{q-1}{r} \geqslant 3$. Therefore $\psi_i(1) \equiv r \pmod q$ and $k+\varepsilon = r$. If ε is -1 then $\psi_i(1) = (r+1)p-1$, if ε is 0 then $\psi_i(1) = rp$ and if ε is 1 then $\psi_i(1) = (r-1)p+1$.

STEP 2. We have $q-1 > 5r$.

Recall that $\mathrm{fix}Q = \{\alpha\}$, that G_α is primitive of degree $4q$ on $\Omega\setminus\{\alpha\}$ and that $q > 37$. The results in Section 7 of Chapter 1 therefore apply to G_α. Theorem 1.19 gives information about the number r when the rank of G_α is at least 4; using the same method of proof (see Theorem 8.2 of [8]) when this rank is 3, we prove:

LEMMA 3.6. Suppose that G_α has rank 3 on $\Omega\setminus\{\alpha\}$. If case (i) of Theorem 1.20 occurs, then r divides one of $3a$, $3a+3$, $(2,a+1)$ and $(2,a)$. If case (ii) occurs then r divides one of $(6,a-2)$, $(2,a+1)$, $(14,a-4)$ and $(54, a-27)$. If case (iii) occurs then r divides one of $2a$, $2a+1$, $(3,2a-1)$ and $(6,2a+2)$.

PROOF. By Lemma 3.3, G is simple, so the element c (which generates R) is an even permutation. Hence there exist distinct elements $\beta,\gamma,\delta,\varepsilon \in \Omega\setminus\{\alpha\}$ such that $c \in G_{\alpha\{\beta\gamma\delta\varepsilon\}}$ and c acts on $\Omega\setminus\{\alpha,\beta,\gamma,\delta,\varepsilon\}$ as a product of $4\frac{q-1}{r}$ r-cycles, and on $\{\alpha,\beta,\gamma,\delta,\varepsilon\}$ as one of 1, $(\alpha)(\beta\gamma)(\delta\varepsilon)$ and $(\alpha)(\beta)(\gamma\delta\varepsilon)$. If c fixes α and β, let Γ_1, Γ_2 be the orbits of $G_{\alpha\beta}$ on $\Omega\setminus\{\alpha,\beta\}$; and if c acts on $\{\alpha,\beta,\gamma,\delta,\varepsilon\}$ as $(\alpha)(\beta\gamma)(\delta\varepsilon)$, let Γ_1,Γ_2 be the orbits of $G_{\beta\gamma}$ (and of $G_{\{\beta\gamma\}}$ since, because the subdegrees n_1, n_2 of G_α are different by Theorem 1.20, G is generously 2-transitive on Ω) on $\Omega\setminus\{\beta,\gamma\}$. Let $k = |\Gamma_1 \cap \{\gamma,\delta,\varepsilon\}|$ in the first case, $k = |\Gamma_1 \cap \{\alpha,\delta,\varepsilon\}|$ in the second. Then r divides n_1-k where $n_1 = |\Gamma_1|$, and consequently r divides $(q-1,n_1-k)$. The cases $k = 0,1,2,3$ give the values of $(q-1,n_1-k)$ listed in the lemma.

We now consider separately the case where G_α has rank at least 4, and the case where it has rank 3.

Case 1. G_α has rank 4 or more.

If case (i) of Theorem 1.19 occurs then $a \neq 0$ since $q > 37$, so $q \geq 193$

and $\frac{q-1}{32} \geqslant 6$. Also

$$\left| \frac{q-1}{4(2a+1)} \right| = \left| \frac{96a^2+80a+16}{4(2a+1)} \right| = |4(3a+1)| \geqslant 8.$$

Therefore $\frac{q-1}{r} \geqslant \min\left(\frac{q-1}{32}, \left|\frac{q-1}{4(2a+1)}\right| \right) > 5$. Similarly, if case (ii) of Theorem 1.19 occurs then $\frac{q-1}{r} > 5$.

In case (iii) of Theorem 1.19 the rank of G_α is 5 and all its suborbits are self-paired; it follows that, for $\beta \in \Omega\backslash\{\alpha\}$, $G_{\{\alpha\beta\}}$ has 4 orbits on $\Omega\backslash\{\alpha,\beta\}$, contradicting Theorem 1.12(iii).

Thus $q-1 > 5r$ in Case 1.

<u>Case 2. G_α has rank 3.</u>

If case (i) of Theorem 1.20 holds then by Lemma 3.6, $r \leqslant \max(|3a|, |3a+3|)$ so $\frac{q-1}{r} \geqslant \max(|a|, |a+1|) > 5$ since $q > 37$ and $4q+1$ is prime. Similarly $q-1 > 5r$ in cases (ii) and (iii) of Theorem 1.20.

Hence $q-1 > 5r$ in all cases.

<u>STEP 3. If G_α has rank 4 then χ_2 is q-rational.</u>

The character χ_2 was introduced in Section 5 of Chapter 1 as the only nonprincipal character of G which is adjacent to χ_1 in the Brauer p-tree; χ_2 is irreducible, it is part of the real stem of the p-tree and $\chi_2(1) \equiv 1 \pmod p$ since $\chi_1 + \chi_2$ is p-projective indecomposable and $\chi_1(1) = p-1$. Also $\chi^{(p-2,2)}$ is a p-projective character (Proposition 1.8(ii)). We can say much about $\chi^{(p-2,2)}$ when χ_2 is not q-rational (that is, χ_2 is q-exceptional) and the rank of G_α is at least 4; the following lemma is similar to Lemma 6.1 of [29].

<u>LEMMA 3.7.</u> If the rank of G_α is 4 or more and χ_2 is q-exceptional then one of the following occurs:

(i) $\chi^{(p-2,2)} = 2\sum_{1}^{q-1/r}\psi_i + 2\chi_1 + \delta_2 + \delta_2' + \sum_{3}^{q-1/r}(\delta_i + \bar{\delta}_i)$

(ii) $\chi^{(p-2,2)} = 2\sum_{1}^{q-1/r}\psi_i + 2\chi_1 + \delta_2 + \bar{\delta}_2 + \sum_{3}^{q-1/r}(\delta_i + \bar{\delta}_i) + \chi_p$

where in both cases, the q-exceptional characters ψ_i have degree $(r-1)p+1$ (and $\psi_1 = \chi_2$) and δ_i are distinct irreducible characters of G such that $\psi_i + \delta_i$ are p-projective indecomposable. In both cases δ_i has degree p-1 for $i \geq 2$, and is not real-valued for $i \geq 3$. In case (i), $\delta_2'(1) = 2p-1$, the character $\psi_2 + \delta_2'$ is p-projective indecomposable and δ_2, δ_2' are real-valued. In case (ii), χ_p is an irreducible character of degree p.

PROOF. If G_α has rank 4 then all its suborbits are self-paired by Theorem 1.19, so $\langle \xi, \pi \rangle_G = \# \mathrm{orb}(G_{\alpha\beta}, \Omega) = 5$ and $\langle \eta, \pi \rangle_G = \# \mathrm{orb}(G_{\{\alpha\beta\}}, \Omega) = 4$. If G_α has rank 5 then, since we have excluded case (iii) of Theorem 1.19 in the argument for Step 2, $\langle \xi, \pi \rangle_G = 6$ and $\langle \eta, \pi \rangle_G = 4$. In both cases $\langle \chi_1, \chi^{(p-2,2)} \rangle_G = 2$; consequently $2\chi_1 + 2\chi_2 \leq \chi^{(p-2,2)}$ since $\chi^{(p-2,2)}$ is p-projective and does not contain the principal character of G.

We may assume that χ_2 is ψ_1; then $2\sum_{1}^{q-1/r}\psi_i \leq \chi^{(p-2,2)}$, since the ψ_i are q-conjugate and $\chi^{(p-2,2)}$ is rational-valued. Now $\chi_2(1) \equiv 1 \pmod{p}$, so $\psi_i(1) = (r-1)p+1$ by Lemma 3.5 and Step 2. Because $\chi^{(p-2,2)}$ is p-projective, there exist p-projective indecomposables $\sigma_i = \psi_i + \delta_i$, $\sigma_i' = \psi_i + \delta_i'$ with δ_i, δ_i' in the principal p-block of G and $\sum_{1}^{q-1/r}(\sigma_i + \sigma_i') \leq \chi^{(p-2,2)}$; we can take $\delta_1 = \delta_1' = \chi_1$. Let $\delta_i(1) = k_i p - 1$, $\delta_i'(1) = k_i' p - 1$. Then

$$\sum_{1}^{q-1/r}(\sigma_i(1) + \sigma_i'(1)) = \sum_{1}^{q-1/r}(2(r-1) + k_i + k_i')p \leq \chi^{(p-2,2)}(1) = p(2q-1).$$

This inequality gives

$$\sum_{1}^{q-1/r}(k_i + k_i') \leq 2\left(\frac{q-1}{r}\right) + 1,$$

and it follows that either $k_i = k_i' = 1$ for all i, or $k_i = k_i' = 1$ for all but one value of i, say i = 2, and $k_2 = 1$, $k_2' = 2$. In the former case,

$$\chi^{(p-2,2)} = \sum_{1}^{q-1/r}(\sigma_i + \sigma_i') + \sigma$$

where σ is a p-projective character of degree p. Since G is simple (Lemma 3.3) $\chi^{(p-2,2)}$ contains no linear characters, so σ must be irreducible; write $\sigma = \chi_p$. Suppose now that $\delta_i = \delta_j$ for some $i \neq j$. Then δ_i is joined to ψ_i and to ψ_j in the

Brauer p-tree, contradicting Theorem 1.5. Hence the δ_i are all distinct. Also $\overline{\delta_i} \subseteq \chi^{(p-2,2)}$ for each i; if $\overline{\delta_i}$ is δ_j or δ_j' for some $j \neq i$ then $\overline{\delta_i}$ is joined to ψ_i (the ψ_i are all real-valued since χ_2 is) and to ψ_j in the p-tree, again contradicting Theorem 1.5. Consequently $\overline{\delta_i} = \delta_i'$ if δ_i is not real-valued. Finally if δ_j is real-valued for some $j \geqslant 2$ then by Theorem 1.5, δ_j is an end-node in the real stem of the p-tree; it follows that δ_i is real-valued for at most one value of $i \geqslant 2$ and case (ii) of the lemma holds.

If $k_i = k_i' = 1$ for $i \geqslant 3$ and $k_2 = 1$, $k_2' = 2$ then

$$\chi^{(p-2,2)} = \sum_{1}^{q-1/r} (\sigma_i + \sigma_i') .$$

Clearly δ_2' is real-valued, being the only character of degree 2p-1 contained in $\chi^{(p-2,2)}$; and if δ_2 is not real-valued then $\overline{\delta_2}$ is δ_i or δ_i' for some $i > 2$, so $\overline{\delta_2}$ is joined to ψ_2 and to ψ_i in the p-tree, contradicting Theorem 1.5. As before, for $i \geqslant 3$, $\overline{\delta_i} = \delta_i'$ and δ_i is not real-valued. Thus case (i) holds.

The character ς of G was defined in Section 3 of Chapter 1 by $\varsigma = \xi - \eta$, that is, $\varsigma = \chi_1 + \chi^{(p-2,1^2)}$. Both the characters η and ς are p-projective and q-projective (Propositions 1.8(ii) and 1.14). If G_α has rank 4 then, as noted at the beginning of the proof of Lemma 3.7, we have $\langle \xi, \pi \rangle_G = 5$, $\langle \eta, \pi \rangle_G = 4$; this means that $\langle \varsigma, \pi \rangle_G = 1$, that is, $\langle \varsigma, 1 + \chi_1 \rangle_G = 1$. Since $\langle \varsigma, 1 \rangle_G = 0$ it follows that $\langle \chi_1, \varsigma \rangle_G = 1$; and ς is p-projective, so $\chi_1 + \chi_2 \subseteq \varsigma$. Certainly then, either $\langle \chi_2, \varsigma \rangle_G = 1$ or $2\chi_2 \subseteq \varsigma$; we consider these two possibilities separately in the following three lemmas.

<u>LEMMA 3.8.</u> If $\langle \chi_1, \varsigma \rangle_G = 1$ (as is the case when G_α has rank 4), χ_2 is q-exceptional and $2\chi_2 \subseteq \varsigma$, then one of the following holds:

(i) $\varsigma = 2\chi_2 + \chi_1 + \chi_3 + 2\sum_{2}^{q-1/r} \psi_i + \sum_{2}^{q-1/r} (\varepsilon_i + \varepsilon_i')$

(ii) $\varsigma = 2\chi_2 + \chi_1 + \chi_3 + 2\sum_{2}^{q-1/r} \psi_i + \sum_{2}^{q-1/r} (\varepsilon_i + \varepsilon_i') + \chi_p'$

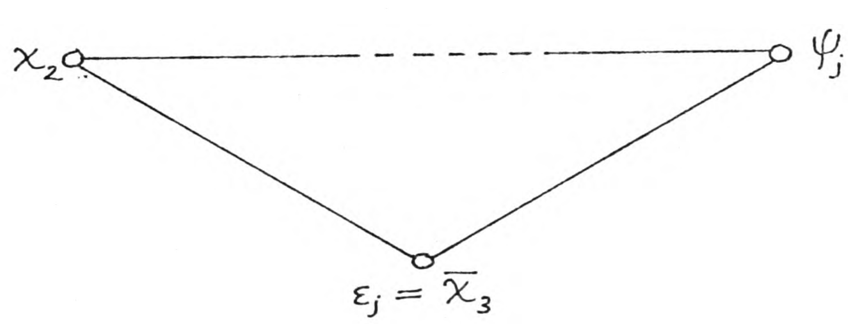
where in both cases, $\varepsilon_i, \varepsilon_i'$ are irreducible characters such that $\psi_i + \varepsilon_i$, $\psi_i + \varepsilon_i'$

are p-projective indecomposable and χ_3 is a real-valued irreducible character of degree 2p-1 such that $\chi_2+\chi_3$ is p-projective indecomposable. In case (i), $\varepsilon_i(1) = \varepsilon_i'(1) = p-1$ for all but one value of i, say i = j, and $\varepsilon_j(1) = p-1$, $\varepsilon_j'(1) = 2p-1$ and ε_j, ε_j' are real-valued. In case (ii), $\varepsilon_i(1) = \varepsilon_i'(1) = p-1$ for all i and χ_p' is a real-valued irreducible character of degree p.

PROOF. Now $2\chi_2 \subseteq \xi$ and $\langle \chi_1, \xi \rangle_G = 1$, so there exists an irreducible character χ_3, not equal to χ_1, such that $\chi_2+\chi_3$ is p-projective indecomposable and $\chi_3 \subseteq \xi$. Arguing as in the proof of Lemma 3.7, we find that $\chi_3(1)$ is p-1 or 2p-1. If it is p-1 then χ_3 is real-valued (for otherwise $\overline{\chi}_3$ would be joined to χ_2 and to some other nonlinear character of G in the p-tree, contradicting Theorem 1.5); also by Theorem 1.5, χ_3 is an end-node in the p-tree (note that G is simple and hence has no nontrivial linear characters). But then the real stem of the p-tree is just

contradicting the fact that the sum of the four p-exceptional characters appears in this real stem (Theorem 1.3).

Hence $\chi_3(1) = 2p-1$ and now similar arguments to those in the proof of Lemma 3.7 show that one of cases (i) and (ii) must hold. The only point to note is that $\overline{\chi}_3 \neq \varepsilon_j'$ in case (i), since equality here would give a circuit in the Brauer p-tree:



Consequently χ_3, ε_j' are real-valued.

LEMMA 3.9. If $\langle \chi_1, \xi \rangle_G = 1$ and $2\chi_2 \leq \xi$ then χ_2 is q-rational.

PROOF. Now ξ is q-projective, so if χ_2 is q-exceptional then by Lemmas 3.4 and 3.8, the whole real stem of the Brauer q-tree is

$$\overset{\circ}{\chi_3} \;\text{———}\; \overset{\circ}{\Sigma\psi_i} \;\text{———}\; \overset{\circ}{\varepsilon_j'}$$

in case (i) of Lemma 3.8, and it is

$$\overset{\circ}{\chi_3} \;\text{———}\; \overset{\circ}{\Sigma\psi_i} \;\text{———}\; \overset{\circ}{\chi_p'}$$

in case (ii) of Lemma 3.8. Both possibilities contradict the fact that the principal character χ_0 must appear in the real stem of the q-tree.

Before the next lemma we need a table of the numbers congruent to 0, 1 and −1 modulo p and q:

q \ p	0	1	−1
0	pq	(q−1)p+1	p−1
1	p	1	2p−1
−1	(q−1)p	(q−2)p+1	pq−1

The table lists the smallest positive number modulo pq.

LEMMA 3.10. If $\langle \chi_2, \xi \rangle_G = 1$ then χ_2 is q-rational (whatever the rank of G_α).

PROOF. Suppose that χ_2 is q-exceptional. By the arguments used in the proofs of Lemmas 3.7 and 3.8, we have

$$\xi = \sum_1^{\frac{q-1}{r}} \psi_i + \sum_1^{\frac{q-1}{r}} \delta_i + \sigma$$

where the q-exceptional characters ψ_i have degree $(r-1)p+1$ (and ψ_1 is χ_2), the δ_i are such that $\psi_i + \delta_i$ is p-projective indecomposable and σ is p-projective.

Let $\delta_i(1) = k_i p - 1$. Each δ_i is q-rational since $\langle \chi_2, \xi \rangle_G = \langle \psi_1, \xi \rangle_G = 1$, so each k_i is one of 1, 2, q, q+1 and q+2 (from the table). The table shows that either $\sigma(1) \geq (q-1)p$ or σ is a sum of irreducible characters of degree p, say $\sigma = \sum \phi_p$. In the former case, $\sum_1^{q-1/r} k_i \leq 2 + \frac{q-1}{r}$ so $k_i = 1$ for all but at most two values of i; thus $k_i = 1$ for at least 4 values of i since $q-1 > 5r$. But if $k_i = 1$ and $i > 1$ (that is, $\delta_i \neq \chi_1$) then δ_i is an end-node in the real stem of the Brauer p-tree by the usual argument using Theorem 1.5 (see the proof of Lemma 3.7). Consequently this real stem has at least 4 end-nodes (one of which is χ_0). This cannot be so; hence $\sigma = \sum \phi_p$, a sum of irreducible characters of degree p. If some k_i is q or more then $k_i = 1$ for all but at most 3 values of i and we obtain a contradiction as above. It follows that k_i is 1 or 2 for all i, and

$$\xi = \sum_1^{q-1/r} \psi_i + \sum_1^{q-1/r} \delta_i + \sum \phi_p$$

where $\sum \phi_p$ is a sum of at least $\frac{q-1}{r}$ (in fact, of $q - \sum k_i + \frac{q-1}{r} + 1$) characters of degree p. But $\delta_i(1)$ is congruent to 0 or 1 modulo q, $\phi_p(1) \equiv 1 (\mathrm{mod}\ q)$ and $\sum_1^{q-1/r} \psi_i$ is the sum of the q-exceptional characters, so ξ cannot be a sum of q-projective indecomposables. This contradicts the fact that ξ is q-projective. Hence χ_2 is q-rational.

Lemmas 3.8, 3.9 and 3.10 show that if G_α has rank 4 then χ_2 is q-rational, so Step 3 is complete.

STEP 4. If G_α has rank 5 then χ_2 is q-rational.

If G_α has rank 5 then $\langle \eta, \pi \rangle_G = 4$, $\langle \xi, \pi \rangle_G = 6$ and so

$$\langle \chi_1, \chi^{(p-2,2)} \rangle_G = \langle \chi_1, \xi \rangle_G = 2.$$

Since $\chi^{(p-2,2)}$ and ξ are p-projective, we have $2\chi_1 + 2\chi_2 \leq \chi^{(p-2,2)}$ and $2\chi_1 + 2\chi_2 \leq \xi$.
The usual arguments give:

LEMMA 3.11. If G_α has rank 5 and χ_2 is q-exceptional then one of the following occurs:

(i) $\quad \xi = 2\sum_{1}^{q-1/r} \psi_i + 2\chi_1 + \varepsilon_2 + \overline{\varepsilon}_2 + \sum_{3}^{q-1/r} (\varepsilon_i + \overline{\varepsilon}_i)$

(ii) $\quad \xi = 2\sum_{1}^{q-1/r} \psi_i + 2\chi_1 + \varepsilon_2 + \overline{\varepsilon}_2 + \sum_{3}^{q-1/r} (\varepsilon_i + \overline{\varepsilon}_i) + \phi_p + \overline{\phi}_p$

where $\psi_i + \varepsilon_i$ are p-projective indecomposable and for $i \geq 3$, ε_i has degree p-1 and is not real-valued. In case (ii), $\varepsilon_2(1) = p-1$ and ϕ_p is irreducible of degree p. In case (i), $\varepsilon_2(1) = 2p-1$.

Step 4 is completed by

LEMMA 3.12. If G_α has rank 5 then χ_2 is q-rational.

PROOF. Suppose that χ_2 is q-exceptional, so that Lemmas 3.7 and 3.11 hold. By Theorem 1.19, the permutation character ν of G_α associated with $\Omega\backslash\{\alpha\}$ is of the form

$$\nu = 1 + \phi_1 + \phi_2 + \overline{\phi}_2 + \phi_3$$

where ϕ_1, ϕ_2, ϕ_3 are irreducible characters of G_α and $\phi_1(1) = q-1$, $\phi_2(1) = \phi_3(1) = q$. Now ν is q-projective by Proposition 1.14, so the characters $1+\phi_1$, ϕ_2, $\overline{\phi}_2$, ϕ_3 are all q-projective, that is, they are characters afforded by projective R_qG_α-modules. They are also p-projective since p does not divide $|G_\alpha|$. It is easy to see that the characters $(1+\phi_1)^G$, ϕ_2^G, $\overline{\phi}_2^G$, ϕ_3^G of G must then be both p-projective and q-projective. Also we have (see Section 3 of Chapter 1)

$$\nu^G = (1+\phi_1)^G + \phi_2^G + \overline{\phi}_2^G + \phi_3^G = \zeta = \eta + \xi \ .$$

Suppose that case (i) of Lemma 3.7 and case (i) of Lemma 3.11 occur. Then

$$\eta = \chi_0 + 2\sum_{1}^{q-1/r} \psi_i + 3\chi_1 + \delta_2 + \delta_2' + \sum_{3}^{q-1/r} (\delta_i + \overline{\delta}_i),$$

$$\xi = 2\sum_{1}^{q-1/r} \psi_i + 2\chi_1 + \varepsilon_2 + \overline{\varepsilon}_2 + \sum_{3}^{q-1/r} (\varepsilon_i + \overline{\varepsilon}_i).$$

Now for j = 1,2,3 we have $\phi_j^G(1) \leq pq$, so $2\sum_{1}^{q-1/r} \psi_i \nleq \phi_j^G$; consequently

$\sum \psi_i \subseteq \phi_j^G$ for each j. The q-mates of $\sum \psi_i$ which appear in ξ (that is, the characters χ in ξ for which $\sum \psi_i + \chi$ is q-projective indecomposable) are χ_0, δ_2', ε_2 and $\bar{\varepsilon}_2$. Hence we have, say, $\delta_2' \subseteq \phi_3^G$, $\varepsilon_2 \subseteq \phi_2^G$, $\bar{\varepsilon}_2 \subseteq \bar{\phi}_2^G$. By Frobenius Reciprocity, $\langle \phi_3^G, \chi_1 \rangle_G = 1$. Also ϕ_3^G is real-valued, so if δ_i (or ε_i) appears in ϕ_3^G for some $i \geqslant 3$ then so does $\bar{\delta}_i$ (or $\bar{\varepsilon}_i$). All this shows that there exist sets $K, K' \subseteq \{3, \ldots, \frac{q-1}{r}\}$ with $K \cup K' \neq \emptyset$, such that

$$\phi_3^G = \sum_1^{q-k} \psi_i + \chi_1 + \delta_2' + \sum_{k \in K} (\delta_k + \bar{\delta}_k) + \sum_{k \in K'} (\varepsilon_k + \bar{\varepsilon}_k) + \sigma$$

where σ is either zero or δ_2. We can suppose that $K \neq \emptyset$; pick $k \in K$. Then, since ϕ_3^G is p-projective, there exists $j \neq k$ such that $\bar{\delta}_k + \psi_j$ is p-projective indecomposable. But then $\bar{\delta}_k$ is joined to both ψ_j and ψ_k in the Brauer p-tree of G, contradicting Theorem 1.5.

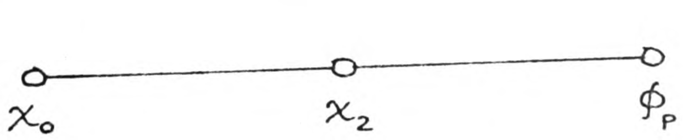
We obtain a contradiction in similar fashion in the other cases of Lemmas 3.7 and 3.11. Hence χ_2 is q-rational.

STEP 5. The rank of G_α is 3.

Suppose that the rank of G_α is 4 or more. Then χ_2 is q-rational by Steps 3 and 4; also $2\chi_1 + 2\chi_2 \subseteq \chi^{(p-2,2)}$. From the table on p.54 we see that either $\chi_2(1) \geqslant (q-1)p+1$ or $\chi_2(1) = (q-2)p+1$. The first possibility cannot occur since $2\chi_1 + 2\chi_2 \subseteq \chi^{(p-2,2)}$. Hence $\chi_2(1) = (q-2)p+1$ and

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

where ϕ_p is irreducible of degree p. It follows that $\eta = \chi_0 + 3\chi_1 + 2\chi_2 + \phi_p$ and so, since η is q-projective, $\chi_0 + \chi_2$ and $\chi_2 + \phi_p$ are q-projective indecomposable. Clearly ϕ_p is real-valued, so by Lemma 3.4 the whole real stem of the Brauer q-tree is



which contradicts the fact that the sum of the q-exceptional characters must appear in this real stem (Theorem 1.3).

Thus G_α has rank 3 and Step 5 is complete.

STEP 6. Some lemmas on the character χ_2.

LEMMA 3.13. The character χ_2 is q-rational and $\chi_2(1) \geqslant (q-2)p+1$.

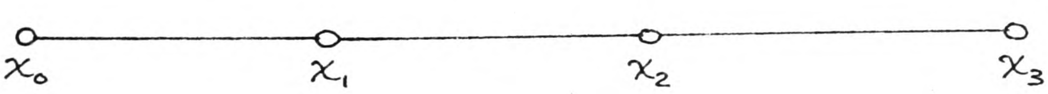
PROOF. Now G_α has rank 3 and G is generously 2-transitive since the subdegrees of G_α are different by Theorem 1.20. Hence $\langle \eta, \pi \rangle_G = 3$, $\langle \xi, \pi \rangle_G = 4$ and so $\langle \chi_1, \xi \rangle_G = 1$. Suppose that χ_2 is q-exceptional. Then by Lemma 3.10, we have $2\chi_2 \subseteq \xi$; but this cannot be so by Lemma 3.9. Consequently χ_2 is q-rational. From the table on p. 54 we see that $\chi_2(1) \geqslant (q-2)p+1$.

LEMMA 3.14. We have $\langle \eta, \chi_2 \rangle_G = \langle \xi, \chi_2 \rangle_G = 1$.

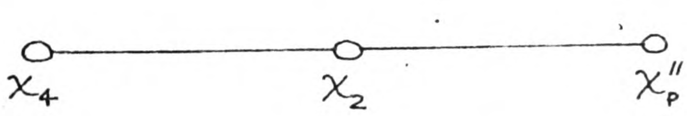
PROOF. Now $\langle \chi_1, \eta \rangle_G = 2$, $\langle \chi_1, \xi \rangle_G = 1$ so certainly $\chi_2 \subseteq \eta$ and $\chi_2 \subseteq \xi$. Suppose that $2\chi_2 \subseteq \xi$. Then $\chi_1 + 2\chi_2 \subseteq \xi$; and by Lemma 3.13,

$$\chi_1(1) + 2\chi_2(1) \geqslant (2q-3)p+1.$$

Hence $\chi_2(1)$ is either $(q-2)p+1$ or $(q-1)p+1$. If $\chi_2(1) = (q-2)p+1$ then $\xi = \chi_1 + 2\chi_2 + \sigma$ where either $\sigma = \chi_3 + \chi_p + \chi_p'$ (with $\chi_3(1) = p-1$, $\chi_p(1) = \chi_p'(1) = p$) or $\sigma = \chi_4 + \chi_p''$ (with $\chi_4(1) = 2p-1$, $\chi_p''(1) = p$). In the first case the Brauer p-tree of G has real stem



which is not so, since the sum of the p-exceptional characters appears in this real stem; in the second case the Brauer q-tree of G has real stem



which again is not so. Thus $\chi_2(1) = (q-1)p+1$ so $\xi = \chi_1 + 2\chi_2 + \chi_3$ where $\chi_3(1) = p-1$

and $\chi_3 \neq \chi_1$. But then $\chi_2+\chi_3$ is p-projective indecomposable, so the real stem of the p-tree is just

$$\underset{\chi_0}{\circ}\!\!-\!\!-\!\!-\!\!-\!\!-\!\!\underset{\chi_1}{\circ}\!\!-\!\!-\!\!-\!\!-\!\!-\!\!\underset{\chi_2}{\circ}\!\!-\!\!-\!\!-\!\!-\!\!-\!\!\underset{\chi_3}{\circ}$$

which again is not the case.

Hence $\langle \chi_2, \xi \rangle_G = 1$. Similar arguments show that $\langle \chi_2, \eta \rangle_G = 1$.

<u>LEMMA 3.15.</u> The degree of χ_2 is one of $(q-2)p+1$, $(q-1)p+1$ and $qp+1$.

<u>PROOF.</u> Suppose that this is false. Now $\chi_0+2\chi_1+\chi_2 \subseteq \eta$, so from the table on p. 54 we have $\chi_2(1) = (2q-2)p+1$. But then $\eta = \chi_0+2\chi_1+\chi_2$ and $\xi = \chi_1+\chi_2+\chi_p$ where $\chi_p(1) = p$, so the real stem of the q-tree is

$$\underset{\chi_0}{\circ}\!\!-\!\!-\!\!-\!\!-\!\!-\!\!\underset{\chi_2}{\circ}\!\!-\!\!-\!\!-\!\!-\!\!-\!\!\underset{\chi_p}{\circ}$$

which is not so.

By Theorem 1.20, the permutation character ν of G_α associated with $\Omega\backslash\{\alpha\}$ is of the form $\nu = 1+\phi_1+\phi_2$ where ϕ_1, ϕ_2 are irreducible and either $\phi_1(1) = q-1$, $\phi_2(1) = 3q$ or $\phi_1(1) = 3q-1$, $\phi_2(1) = q$. We consider these two possibilities separately in the final steps.

<u>STEP 7.</u> <u>We cannot have $\phi_1(1) = q-1$, $\phi_2(1) = 3q$.</u>

Now $\eta = \chi_0+2\chi_1+\chi_2+\sigma$, $\xi = \chi_1+\chi_2+\rho$ where σ and ρ are characters of G which are p-projective. Also $(1+\phi_1)^G$ and ϕ_2^G are both p-projective and q-projective. We know that $(1_{G_\alpha})^G = \chi_0+\chi_1$ and by Frobenius Reciprocity, $\langle \chi_1, \phi_1^G \rangle_G = 1$, so $\chi_0+2\chi_1 \subseteq (1+\phi_1)^G$. Hence $\chi_0+2\chi_1+\chi_2 \subseteq (1+\phi_1)^G$ and so by Lemma 3.15, $\chi_2(1) = (q-2)p+1$ and

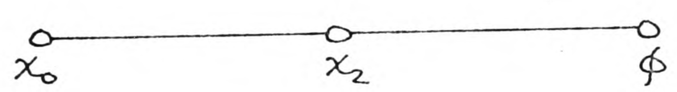
$$(1+\phi_1)^G = \chi_0 + 2\chi_1 + \chi_2 \,,$$

$$\phi_2^G = \chi_1 + \chi_2 + \rho + \sigma \quad .$$

It follows that $\chi_0+\chi_2$ is q-projective indecomposable and that σ is both p-projective and q-projective of degree pq. Also $\rho(1) = p(q+1)$.

Since ξ is q-projective there exists $\phi \subseteq \rho$ such that $\chi_2+\phi$ is q-projective indecomposable. We have $\phi(1) \equiv 1 (\mathrm{mod}\ q)$ and ϕ is irreducible, for if ϕ were $\Sigma\psi_i$ then by Lemma 3.5, $\phi(1)$ would be congruent to $-1(\mathrm{mod}\ q)$. By Theorem 1.9(i), ϕ is p-rational, so $\phi(1)$ is one of p, 2p-1, pq+1 and p(q+1). If ϕ is not real-valued then, since $\bar{\phi} \subseteq \rho$, we must have $\phi(1) = p$ or $\phi(1) = 2p-1$; also there exists $\chi_3 \subseteq \rho$ such that $\chi_3+\bar{\phi}$ is q-projective indecomposable. But then $\bar{\phi}$ is joined to χ_2 and to χ_3 in the Brauer q-tree, contradicting the fact that, by Lemma 3.4, $\bar{\phi}$ must be an end-node in the q-tree.

Thus ϕ is real-valued. If $\phi(1)$ is p or 2p-1 then the real stem of the Brauer q-tree is just



which is not so, since this real stem must contain the sum of the q-exceptional characters. Consequently $\phi(1)$ is either pq+1 or p(q+1).

Suppose that $\phi(1) = pq+1$. Then $\rho = \phi + \psi$ where ψ is irreducible of degree p-1. Hence $\phi_2^G = \chi_1+\chi_2+\phi+\psi+\sigma$ and so $\psi_{G_\alpha} = \phi_2 + \delta$ where δ is a character of G_α of degree q. By Frobenius Reciprocity, $\psi \subseteq \delta^G$; and δ^G is p-projective since p does not divide $|G_\alpha|$. But ψ is an end-node in the Brauer p-tree of G, joined only to ϕ (Theorem 1.5), so $\psi+\phi \subseteq \delta^G$. However, $\delta^G(1) = pq$ while $\psi(1)+\phi(1) = p(q+1)$, which is a contradiction.

The only remaining case is $\phi(1) = p(q+1)$, whence $\rho = \phi$. We have

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

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

from which, using Lemma 3.14, it follows that $\|\chi^{(p-2,1^2)}\|_G = 2$ and $\langle \chi^{(p-2,1^2)}, \chi^{(p-2,2)} \rangle_G = 1$. This is a contradiction by Corollary 2.5.

STEP 8. Completion of the proof.

are p-projective.

s Reciprocity,

that $\chi_2(1)$ is

ere χ_p is

able. Now $\chi_o + \chi_2$

'eal stem of the

s q-projective

$) \equiv 1 (\mathrm{mod}\ q)$,

r 2p-1. But

follows that

ective. Also

ory of Section 1

phic to PSL(2,q)

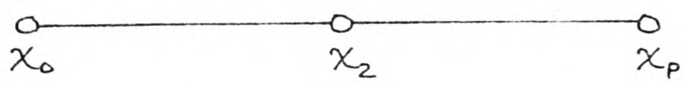
to G_α.

STEP 8. Completion of the proof.

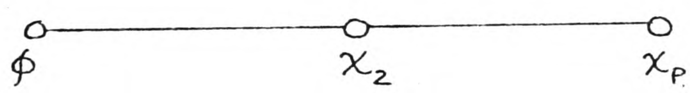
By Step 7, we have $\phi_1(1) = 3q-1$, $\phi_2(1) = q$.

Again $\eta = \chi_0 + 2\chi_1 + \chi_2 + \sigma$ and $\xi = \chi_1 + \chi_2 + \rho$ where σ, ρ are p-projective. Now ϕ_2^G is both p-projective and q-projective and by Frobenius Reciprocity, $\langle \chi_1, \phi_2^G \rangle_G = 1$, so $\chi_1 + \chi_2 \subseteq \phi_2^G$. It follows from Lemma 3.15 that $\chi_2(1)$ is either $(q-2)p+1$ or $(q-1)p+1$.

Suppose that $\chi_2(1) = (q-2)p+1$. Then $\phi_2^G = \chi_1 + \chi_2 + \chi_p$ where χ_p is irreducible of degree p and $\chi_2 + \chi_p$ is q-projective indecomposable. Now $\chi_0 + \chi_2$ cannot be q-projective indecomposable, for if it were, the real stem of the q-tree of G would be just



which is not so. Hence there exists $\phi \subseteq \sigma$ such that $\chi_2 + \phi$ is q-projective indecomposable. The arguments used in Step 7 show that $\phi(1) \equiv 1 (\mathrm{mod}\ q)$, ϕ is irreducible, p-rational, real-valued and $\phi(1)$ is p or 2p-1. But then by Lemma 3.4, the real stem of the q-tree is just



which is not the case.

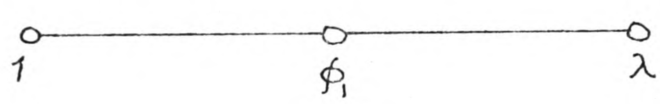
Thus $\chi_2(1) = (q-1)p+1$ (which is divisible by q). It follows that $\phi_2^G = \chi_1 + \chi_2$, $\phi_1^G = \chi_1 + \chi_2 + \sigma + \rho$ and ρ, $\chi_0 + \sigma$ are q-projective. Also $\rho(1) = pq$, $\sigma(1) = p(q-1)$.

In the proof of the following lemma, we use the theory of Section 1 of Chapter 1 for the group G_α. Note that G_α is not isomorphic to PSL(2,q) or to PGL(2,q) by Proposition 1.27, so Theorem 1.5 applies to G_α.

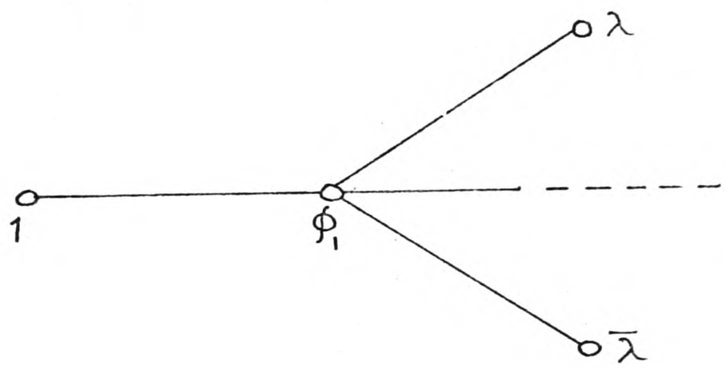
LEMMA 3.16. If ψ is a real-valued irreducible constituent of $\sigma+\rho$ then $\psi(1)\geqslant p$.

PROOF. Suppose that ψ is a real-valued irreducible constituent of $\sigma+\rho$ with $\psi(1)< p$. Then $\psi(1)= p-1$. Since $\psi\subseteq \phi_1^{G}$ we have $\psi_{G_{\alpha}} = \phi_1+\delta$, where δ is a character of G_α of degree q+1 and $\phi_1+\delta$ is q-projective. Let λ be a constituent of δ such that $\phi_1+\lambda$ is q-projective indecomposable. Then either λ is linear or $\lambda = \delta$.

Suppose that λ is linear. If λ is real-valued then the real stem of the Brauer q-tree of G_α is just

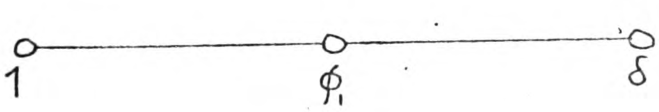


which contradicts the fact that the sum of the $\frac{q-1}{r}$ q-exceptional characters of G_α must appear in this real stem. Consequently λ is not real-valued and the diagram below shows part of the q-tree of G_α:



Now multiplication by λ gives an automorphism of the q-tree of G_α, fixing only the sum of the q-exceptional characters of G_α (Proposition 1.4). However, ϕ_1 is the only character joined to λ in the q-tree, so multiplication by λ must fix ϕ_1 , which is a contradiction.

Hence $\lambda=\delta$ and δ is irreducible. But then the real stem of the q-tree of G_α is just



since δ is an end-node by Theorem 1.5(ii). This contradicts Theorem 1.3.

LEMMA 3.17. One of the following holds:

(A) $\sigma = \sum_{1}^{\frac{q-1}{2}} \psi_i$, where $\psi_i(1) = rp$,

(B) $\sigma = \sum_{1}^{\frac{q-1}{2}} (\psi_i + \delta_i)$, where $\psi_i(1) = (r-1)p+1$, $\delta_i(1) = p-1$ for all i,

(C) σ is irreducible.

Also, one of the following holds:

(a) $\rho = \sum_{1}^{\frac{q-1}{2}} \psi_i + \chi_p$, where χ_p is irreducible of degree p and $\psi_i(1) = rp$,

(b) $\rho = \sum_{1}^{\frac{q-1}{2}} (\psi_i + \varepsilon_i) + \chi_p$, where $\psi_i(1) = (r-1)p+1$, $\varepsilon_i(1) = p-1$ for all i and χ_p is irreducible of degree p,

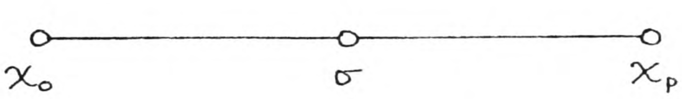
(c) $\rho = \chi_{p(q-1)} + \chi_p$, a sum of two irreducible characters of degrees p(q-1) and p,

(d) $\rho = \chi_{(q-2)p+1} + \chi_{2p-1}$, a sum of two irreducible characters of degrees (q-2)p+1 and 2p-1,

(e) ρ is irreducible.

PROOF. This follows from Lemma 3.16 and the facts that ρ, σ are p-projective and ρ, $\chi_o + \sigma$ are q-projective.

We have $\chi^{(p-2,2)} = \chi_1 + \chi_2 + \sigma$, $\chi^{(p-2,1^2)} = \chi_2 + \rho$; hence $\|\chi^{(p-2,1^2)}\| \leq 3$ and $\langle \chi^{(p-2,2)}, \chi^{(p-2,1^2)} \rangle = 1$ in every case of Lemma 3.17 except cases (A)(a), (B)(b), (C)(a), (C)(b) and case (C)(c) when $\chi_{p(q-1)} = \sigma$ (we are using Lemma 3.14 here). However, if $\chi_{p(q-1)} = \sigma$ then the real stem of the Brauer q-tree of G is just



which is not so. Hence Corollary 2.5 rules out all cases in Lemma 3.17 except (A)(a), (B)(b), (C)(a) and (C)(b) (note that p is odd, so Corollary 2.5 gives that $e+2f \geqslant 6$). We deal with these remaining cases separately; the cases (A)(a) and (B)(b) yield to the same argument, as do (C)(a) and (C)(b), so we deal only with (A)(a) and (C)(a).

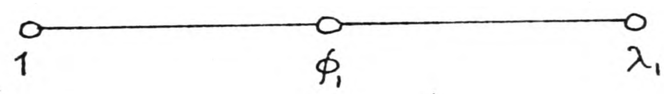
Case (A)(a). $\sigma = \sum \psi_i$, $\rho = \sum \psi_i + \chi_p$.

Recall that $\phi_1^G = \chi_1 + \chi_2 + \sigma + \rho$, so $\chi_p \subseteq \phi_1^G$ and we have

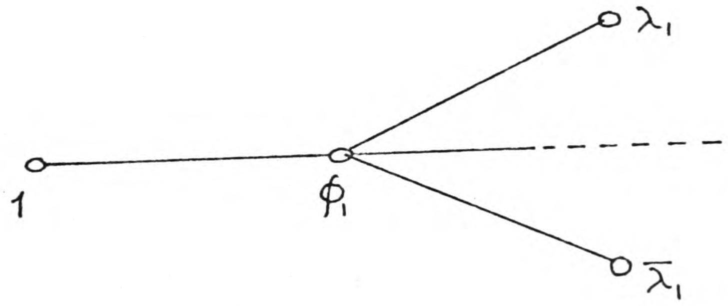
$$(\chi_p)_{G_\alpha} = \phi_1 + \psi$$

where ψ is a character of G_α of degree q+2. Certainly ψ is reducible, so ψ is one of $\delta + \lambda$ (where δ is irreducible of degree q+1 and λ is linear), $\delta + \lambda_1 + \lambda_2$ (where δ is irreducible of degree q and λ_i are linear), $\delta + \lambda_1 + \lambda_2 + \lambda_3$ (where δ is irreducible of degree q-1 and λ_i are linear) and $\sum \lambda_i$ (a sum of q+2 linear characters). If $\psi = \delta + \lambda$ then δ, λ are both real-valued (since ψ is), so both are end-nodes in the real stem of the Brauer q-tree of G_α by Theorem 1.5(ii). Consequently $\lambda = 1$, which is not so.

Suppose that $\psi = \delta + \lambda_1 + \lambda_2$. Now $(\chi_0 + \sum \psi_i)_{G_\alpha}$ is q-projective, so $\phi_1 \subseteq (\sum \psi_i)_{G_\alpha}$ and $(\sum \psi_i)_{G_\alpha} - \phi_1$ is q-projective. Also $(\sum \psi_i + \chi_p)_{G_\alpha}$ is q-projective; it follows that $(\sum \psi_i + \chi_p)_{G_\alpha} - (\sum \psi_i)_{G_\alpha} + \phi_1$ is q-projective, that is, $2\phi_1 + \delta + \lambda_1 + \lambda_2$ is q-projective. Thus $\phi_1 + \lambda_1$, $\phi_1 + \lambda_2$ are q-projective indecomposable. If λ_1 is real-valued then the real stem of the q-tree of G_α is just



which is not the case; and if λ_1 is not real-valued then $\overline{\lambda_1} = \lambda_2$ and the diagram below shows part of the q-tree of G_α:



This contradicts the fact that by Proposition 1.4, multiplication by λ_1 gives an automorphism of the q-tree of G_α fixing only the sum of the q-exceptional characters of G_α.

We obtain a similar contradiction if $\psi = \delta + \lambda_1 + \lambda_2 + \lambda_3$ or if $\psi = \Sigma \lambda_i$.

Case (C)(a). σ is irreducible, $\rho = \Sigma \psi_i + \chi_\rho$.

Here, $\# \operatorname{orb}(G, \Omega^{\{2\}} \times \Omega^{(2)}) = \langle \eta, \xi \rangle_G = 10$ and $\# \operatorname{orb}(G, \Omega^{(2)} \times \Omega^{(2)}) = \| \xi \|_G = 16 + \frac{q-1}{r}$. But each orbit of G on $\Omega^{\{2\}} \times \Omega^{(2)}$ corresponds to at most two orbits on $\Omega^{(2)} \times \Omega^{(2)}$. Hence $20 \geq 16 + \frac{q-1}{r}$, which contradicts Step 2.

All the cases of Lemma 3.17 have now been excluded, so the proof of the theorem is complete.

"I struck the board and cried 'No more!'"

George Herbert, 'The Collar'.

Chapter 4: MORE ON PROBLEM A.

In this chapter we carry out further investigation of insoluble, transitive groups of degree p, where $p = 4q+1$, p,q are prime and $p > 13$. We already know by Theorem 3.1 that such a group G is 3-transitive and we suppose that G is not 4-transitive. Our aim is to prove more facts about the action of G on Ω by restricting the possible decompositions of the characters η and ξ of G (see Section 3 of Chapter 1). This is done using the character theory described in Sections 1,2 and 5 of Chapter 1. In contrast with the situation in all the other problems of this type described in the Introduction (the cases "$n = p = 2q+1$" and "$n = 2p = q+1$"), a Sylow q-subgroup of G may not be self-centralising (Theorem 1.18 does not apply to 2-transitive groups of degree 4q), so G may have several q-blocks of defect one.

In the first section of this chapter we prove some results concerning modular representations of groups, which we use later to show that certain characters of relatively small degree do not appear as constituents of η or ξ. More elimination is carried out in the second section, and lists of about fifteen possibilities each are given for the degrees of the irreducible constituents of η and ξ. In the third and final section we use the results of Section 2 of Chapter 2 to make some deductions about the action of G on Ω from these lists.

1. SOME MODULAR REPRESENTATION THEORY.

Throughout this section we suppose only that G is a finite group with a Sylow p-subgroup of order p and that if V is a nontrivial normal subgroup of G then p divides $|V|$. We use the notation of Sections 1 and 2 of Chapter 1 - write $C = C_G(P) = P \times X$, $N = N_G(P)$. Using Theorem 1.6

and the description of the indecomposable $\overline{K}N$-modules given thereafter, we show that the existence of a $\overline{K}G$-module of relatively small dimension implies restrictions on the group X. Write $\overline{K}^*$ for the multiplicative group $\overline{K}\setminus\{0\}$.

<u>PROPOSITION 4.1.</u> Suppose that $X \neq 1$ and let W be an indecomposable $\overline{K}G$-module in the principal p-block of G. Then either dim W = 1 or dim $W \geqslant p$. In the latter case, W is faithful.

<u>PROOF.</u> By Theorem 1.6, we have

$$W_N = T_0 \oplus T_1$$

where T_0 is a projective, T_1 an indecomposable $\overline{K}N$-module. Also T_1 lies in the principal p-block of N, so in the notation of Section 2 of Chapter 1, we have $(T_1)_C \cong V_r \otimes \overline{W}_1$ for some $0 \leqslant r \leqslant p$ (where $V_0 = 0$).

Suppose that $T_0 = 0$. If $Y = \operatorname{Ker} W$ then $X \leqslant Y$ since X acts trivially on $\overline{W}_1$, and hence on W; consequently $Y \neq 1$, so $P \leqslant Y$ by our initial assumption on G (at the beginning of this section). Therefore $C_G(P) = P \times X \leqslant Y$. Now $G = YN_G(P)$ by the Frattini argument, so

$$\frac{G}{Y} \cong \frac{N_G(P)}{N_Y(P)} \cong \frac{N_G(P)/C_G(P)}{N_Y(P)/C_G(P)}$$

which is cyclic of order dividing p-1. Hence W, an indecomposable $\overline{K}(\frac{G}{Y})$-module, has dimension 1.

Now suppose that $T_0 \neq 0$. Then dim $W \geqslant p$ and $(T_0)_P$ is a faithful $\overline{K}P$-module, so $P \nleqslant \operatorname{Ker} W$. This forces Ker W = 1 by our initial assumption on G, so W is faithful.

Hence either dim W = 1 or dim $W \geqslant p$ and in the latter case, W is faithful.

PROPOSITION 4.2. Suppose that there is an indecomposable $\overline{K}G$-module W of dimension $p+c$ where $0 \leqslant c < p$, in the principal p-block of G. Then X is isomorphic to a subgroup of $\overline{K}^*$ and $X \leqslant Z(N)$.

PROOF. The result is trivial if $X = 1$; so suppose that $X \neq 1$. By Theorem 1.6,

$$W_N = T_0 \oplus T_1$$

where T_0 is projective and T_1 is an indecomposable in the principal p-block of N, so that $(T_1)_C \cong V_r \otimes \overline{W}_1$ for some $r \leqslant p$. By Proposition 4.1, W is faithful, so $T_0 \neq 0$; hence $r = c$ and $(T_0)_C \cong V_p \otimes \overline{W}_i$ for some nontrivial 1-dimensional $\overline{K}X$-module $\overline{W}_i$ which is N-conjugate only to itself. It follows that

$$W_C \cong (V_p \otimes \overline{W}_i) \oplus (V_c \otimes \overline{W}_1) .$$

Now X acts as scalars on $V_p \otimes \overline{W}_i$ and acts trivially on $V_c \otimes \overline{W}_1$, so X is isomorphic to a subgroup of $\overline{K}^*$ and $X \leqslant Z(N)$.

PROPOSITION 4.3. Suppose that there is an indecomposable $\overline{K}G$-module W of dimension $2p+c$ where $0 \leqslant c < p$, in the principal p-block of G. Then one of the following holds:

(i) X has a faithful ordinary irreducible representation of degree 2,

(ii) X is isomorphic to a subgroup of $\overline{K}^* \times \overline{K}^*$ and $X \leqslant Z(N)$,

(iii) X is isomorphic to a subgroup of $\overline{K}^* \times \overline{K}^*$ and $\left| \frac{N}{C_N(X)} \right| = 2$.

PROOF. If $X = 1$ then case(ii) holds; so suppose that $X \neq 1$. By Theorem 1.6,

$$W_N = T_0 \oplus T_1$$

where $(T_1)_C \cong V_c \otimes \overline{W}_1$ and $(T_0)_C$ is one of:

1. $V_p \otimes \overline{W}_i$ where $\overline{W}_i$ is an irreducible $\overline{K}X$-module of dimension 2 which is N-conjugate only to itself,

2. $V_p \otimes \overline{W}_i$ where $\overline{W}_i$ is a sum of two N-conjugate $\overline{K}X$-modules $\overline{W}_{i_1}$, $\overline{W}_{i_2}$

of dimension 1,

3. $(V_p \otimes \overline{W}_i) \oplus (V_p \otimes \overline{W}_j)$ where $\overline{W}_i, \overline{W}_j$ are $\overline{K}X$-modules of dimension 1, each N-conjugate only to itself.

In case 1, $\overline{W}_i$ is a faithful $\overline{K}X$-module since W_C is faithful and X acts trivially on T_1. Hence case (i) of the proposition holds.

In case 2, X acts as scalars on $\overline{W}_{i_1}$ and $\overline{W}_{i_2}$ so X is isomorphic to a subgroup of $\overline{K}^* \times \overline{K}^*$. Also, if θ_{i_1} is the character afforded by W_{i_1} (an RX-module), then $I_N(\theta_{i_1}.1) = C_N(X)$ and $|N:I_N(\theta_{i_1}.1)| = 2$ (see Section 1 of Chapter 1). Hence case(iii) holds.

Finally, in case 3, X acts on $\overline{W}_i$ and $\overline{W}_j$ as scalars, so again X is isomorphic to a subgroup of $\overline{K}^* \times \overline{K}^*$. Clearly $X \leq Z(N)$, so case (ii) holds.

---

2. SOME CHARACTER THEORY.

In this section we return to our insoluble, transitive group G of degree p on Ω, where $p = 4q+1$, $p > 13$ and p,q are prime. By Theorem 3.1 G is 3-transitive; from now on we assume that G consists only of even permutations and is not 4-transitive.

Let P be a Sylow p-subgroup of G and let $t = |N_G(P):P|$. Then t is one of 2,4,q,2q and 4q. It is not 2 by Theorem 1.13 and if it were 4 or 4q then G would contain odd permutations. Hence t is q or 2q. Let Q be a subgroup of order q contained in $N_G(P)$; then Q is a Sylow q-subgroup of G by Theorem 1.26 and $N_G(Q) = C_G(Q).R$ where $R = \langle c \rangle$ is a nontrivial cyclic group whose order r divides q-1. Write s for $\frac{q-1}{r}$. Also Q fixes just one point of Ω, say α. We write H for the subgroup G_α.

Let $\pi, \eta, \xi, \zeta, \chi^{(p-2,2)}, \chi^{(p-2,1^2)}, \chi_1$ and χ_2 be the characters of G defined in Sections 3 and 5 of Chapter 1. In what follows we use the theory of Sections 1 and 2 of Chapter 1 for both the primes p and q in the group G, and for the prime q in the group H ($= G_\alpha$). First we consider the various possibilities for $C_G(Q)$ and the corresponding q-blocks of G; then we eliminate some possible degrees for irreducible constituents of ξ. After this we reduce the list of possibilities for the degrees of the irreducible constituents of η and ξ to about fifteen each, considering the cases $t = q$ and $t = 2q$ separately.

a. Possibilities for $C_G(Q)$ and corresponding q-blocks.

We have $C = C_G(Q) = Q \times X$ where X is isomorphic to a subgroup of A_4 (acting on the four q-cycles of a generator of Q). Write $N = N_G(Q)$. Theorem 1.1 gives the following information about the q-blocks of G for each different possible subgroup X:

(i) $X = 1$.

Here there is precisely one q-block of defect one - the principal q-block B_1 - which contains r q-rational and s ($= \frac{q-1}{r}$) q-exceptional characters. We have

$$\chi_j(1) \equiv \varepsilon_j \pmod q, \qquad \chi(1) \equiv -\varepsilon r \pmod q$$

if χ_j is a q-rational and χ a q-exceptional character ($\varepsilon_j, \varepsilon$ are the numbers ± 1 described in Theorem 1.1).

(ii) $X \cong Z_2$ (cyclic of order 2).

Let $X = \langle x \rangle$. The character table of X is:

	1	x
θ_1	1	1
θ_2	1	-1

By Theorem 1.1 there are two q-blocks of defect one, B_1 and B_2. Each contains r q-rational and s q-exceptional characters and if χ_j is q-rational, χ q-exceptional then

$$\chi_j(1) \equiv \varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

(iii) <u>$X \cong Z_3$.</u>

Let $X = \langle y \rangle$. The character table of X is:

	1	y	y^2
θ_1	1	1	1
θ_2	1	ω	ω^2
θ_2'	1	ω^2	ω

$(\omega = e^{\frac{2\pi i}{3}})$

There are two possibilities:

1. <u>y is conjugate to y^2 in N.</u> Then $\left|\frac{N}{C_N(X)}\right| = 2$, $\Theta_1 = \theta_1$ and $\Theta_2 = \theta_2 + \theta_2'$, and $|I_N(\theta_2 . 1) : C| = \frac{r}{2}$. There are two q-blocks B_1, B_2 of defect one; B_1, the principal q-block, contains r q-rational and s q-exceptional characters and

$$\chi_j(1) \equiv \varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

And B_2 contains $\frac{r}{2}$ q-rational and 2s q-exceptional characters with

$$\chi_j(1) \equiv 2\varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

2. <u>y is not conjugate to y^2 in N.</u> Then $X \leq Z(N)$ and there are three q-blocks B_1, B_2, B_3 of defect one, each containing r q-rational and s q-exceptional characters, with

$$\chi_j(1) \equiv \varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

(iv) <u>$X \cong A_4$.</u>

The character table of X is:

	1	(12)(34)	(123)	(132)
θ_1	1	1	1	1
θ_2	3	-1	0	0
θ_3	1	1	ω	ω^2
θ_3'	1	1	ω^2	ω

$(\omega = e^{\frac{2\pi i}{3}})$

Again there are two possibilities:

1. <u>(123) is conjugate to (132) in N.</u> Then $\Theta_1 = \theta_1$, $\Theta_2 = \theta_2$, $\Theta_3 = \theta_3 + \theta_3'$ and $|I_N(\theta_3 . 1):C| = \frac{r}{2}$. There are three q-blocks B_1, B_2, B_3 of defect one; B_1 and B_2 contain r q-rational and s q-exceptional characters, B_3 contains $\frac{r}{2}$ q-rational and 2s q-exceptional characters. For B_1 we have

$$\chi_j(1) \equiv \varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

For B_2,

$$\chi_j(1) \equiv 3\varepsilon_j \pmod q, \quad \chi(1) \equiv -3\varepsilon r \pmod q.$$

For B_3,

$$\chi_j(1) \equiv 2\varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

2. <u>(123) is not conjugate to (132) in N.</u> Here there are four q-blocks B_1, B_2, B_3, B_4 of defect one; each contains r q-rational and s q-exceptional characters. For B_1, B_3, B_4,

$$\chi_j(1) \equiv \varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

For B_2,

$$\chi_j(1) \equiv 3\varepsilon_j \pmod q, \quad \chi(1) \equiv -3\varepsilon r \pmod q.$$

(v) <u>$X \cong V_4$.</u>

Let $X = \{1, x, y, z\}$. The character table of X is:

	1	x	y	z
θ_1	1	1	1	1
θ_2	1	-1	1	-1
θ_2'	1	-1	-1	1
θ_2''	1	1	-1	-1

There are three possibilities:

1. <u>3 divides $\left|\frac{N}{C_N(X)}\right|$ (that is, x,y,z are all N-conjugate).</u> Then $\Theta_1 = \theta_1$,

$\Theta_2 = \theta_2 + \theta_2' + \theta_2''$ and $|I_N(\theta_2 . 1) : C| = \frac{r}{3}$. There are two q-blocks B_1, B_2 of defect one; B_1 contains r q-rational, s q-exceptional characters, and B_2 contains $\frac{r}{3}$ q-rational, 3s q-exceptional characters. For B_1,

$$\chi_j(1) \equiv \varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

For B_2,

$$\chi_j(1) \equiv 3\varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

2. $\underline{\left|\frac{N}{C_N(X)}\right| = 2.}$ Then $\Theta_1 = \theta_1$, $\Theta_2 = \theta_2 + \theta_2'$ (say), $\Theta_3 = \theta_2''$ and $|I_N(\theta_2 . 1)| = \frac{r}{2}$. There are three q-blocks B_1, B_2, B_3 of defect one; B_1 and B_3 contain r q-rational, s q-exceptional characters and B_2 contains $\frac{r}{2}$ q-rational, 2s q-exceptional characters. For B_1 and B_3,

$$\chi_j(1) \equiv \varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

For B_2,

$$\chi_j(1) \equiv 2\varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

3. $\underline{X \leq Z(N).}$ There are four q-blocks of defect one, each containing r q-rational and s q-exceptional characters with

$$\chi_j(1) \equiv \varepsilon_j \pmod q, \quad \chi(1) \equiv -\varepsilon r \pmod q.$$

---

b. Constituents of ξ of small degree.

In order to eliminate some possibilities for constituents of ξ of relatively small degree, we first prove some facts about indecomposable $\bar{K}H$-modules (recall that $H = G_\alpha$).

LEMMA 4.4. If G has an irreducible character χ with $\chi(1) \equiv \pm 2 \pmod q$ then the dimension of any nonlinear indecomposable $\bar{K}H$-module in the principal q-block of H is at least 2q.

PROOF. The existence of such a character χ implies that one of the following holds: $X \cong Z_3$ and $X \nleq Z(N)$; $X \cong V_4$; $X \cong A_4$ (see Section a above). Let W be a nonlinear indecomposable $\overline{K}H$-module. By Proposition 4.1, dim $W \geq q$ (note that $1 \neq Y \triangleleft H$ implies that q divides $|Y|$, so the results of Section 1 of this chapter apply to H). If dim $W < 2q$ then Proposition 4.2 implies that X is cyclic and $X \leq Z(N)$, which is not possible.

LEMMA 4.5. If G has an irreducible character χ with $\chi(1) \equiv \pm 3 \pmod q$ then the dimension of any nonlinear indecomposable $\overline{K}H$-module in the principal q-block of H is at least 3q.

PROOF. By Section a above, either $X \cong V_4$ and 3 divides $\left|\frac{N}{C_N(X)}\right|$ or $X \cong A_4$. Let W be a nonlinear indecomposable $\overline{K}H$-module. By Propositions 4.1 and 4.2, dim $W \geq 2q$ and if dim $W < 3q$ then Proposition 4.3 yields a contradiction.

Next we need some further facts about H.

LEMMA 4.6. If L is a nontrivial normal subgroup of H then L is 2-transitive on $\Omega \setminus \{\alpha\}$.

PROOF. Certainly L is $\frac{3}{2}$-transitive on $\Omega \setminus \{\alpha\}$, so by Theorem 10.4 of [40], L is either primitive or a Frobenius group; if it is a Frobenius group it has a characteristic regular normal subgroup L_1 (Theorem 5.1 of [40]). Then by Theorem 11.3 of [40], L_1 is elementary abelian, so 4q is a prime power, which is not so.

It follows that L is primitive on $\Omega \setminus \{\alpha\}$. Hence by Theorem 1.1 of [8] one of the following holds:

(i) L is 2-transitive,

(ii) L has rank 3 or 5,

(iii) L has rank 4 and there is an integer a such that the subdegrees of L are 1, $8(2a+1)(12a+5)$, $4(3a+1)(8a+3)$ and $(12a+5)(8a+3)$. If L has rank 3 or 5 then since all the nontrivial suborbits of L have equal size m, say, we have $4q = 1+2m$ or $4q = 1+4m$, which is impossible. If L has rank 4 then the nontrivial subdegrees cannot be equal. Hence L is 2-transitive.

LEMMA 4.7. Any nonprincipal irreducible constituent of ξ_H is a faithful character of H. In particular, ξ_H has no nonprincipal irreducible constituent of degree 5 or less.

PROOF. Let ϕ be any nonprincipal irreducible character of H and suppose that ϕ is not faithful. Let $L = \mathrm{Ker}\,\phi$; then L is 2-transitive by Lemma 4.6, so

$$\langle 1_L, \xi_L \rangle_L = 1.$$

Thus $\langle (1_L)^H, \xi_H \rangle = 1$. But $(1_L)^H$ is the regular character of $\frac{H}{L}$, so $\phi \subseteq (1_L)^H$ and $1_H \subseteq (1_L)^H$. Consequently $\langle \phi, \xi_H \rangle_H = 0$ and so any nonprincipal irreducible constituent of ξ_H is faithful. In particular, ξ_H has no nonprincipal constituent of degree 5 or less, since the existence of such a constituent would mean that H had a normal Sylow q-subgroup by Theorem 1.24, which would imply that H was soluble and hence that 4q was a prime power.

Now we can eliminate some possibilities for the degrees of the irreducible constituents of ξ. We shall need to know the numbers congruent to $0, \pm 1 \pmod p$ and to $0, \pm 1, \pm 2, \pm 3 \pmod q$:

q \ p	0	1	-1
0	pq	$(q-1)p+1$	$p-1$
1	p	1	$2p-1$
-1	$(q-1)p$	$(q-2)p+1$	$pq-1$
2	$2p$	$p+1$	$3p-1$
-2	$(q-2)p$	$(q-3)p+1$	$(q-1)p-1$
3	$3p$	$2p+1$	$4p-1$
-3	$(q-3)p$	$(q-4)p+1$	$(q-2)p-1$

The table lists the smallest positive number modulo pq.

LEMMA 4.8. If χ is an irreducible constituent of $\chi^{(p-2,2)} + \chi^{(p-2,1^2)}$ then $\chi(1) > p+1$.

PROOF. Write $1+\pi_1$ for the permutation character of H associated with $\Omega\setminus\{\alpha\}$, so that π_1 is irreducible of degree 4q-1 and $1+\pi_1 = (\chi_1)_H$. Then $\xi = (1+\pi_1)^G$. Consequently if $\chi \subseteq \chi^{(p-2,2)} + \chi^{(p-2,1^2)}$ then $\chi \subseteq \pi_1{}^G$ and so $\pi_1 \subseteq \chi_H$. Also $\chi \neq \chi_1$, since the fact that G is 3-transitive means that $\langle \xi, \chi_1\rangle_G = 2$, which implies that $\langle \chi_1, \chi^{(p-2,2)} + \chi^{(p-2,1^2)}\rangle = 0$. Hence if $\chi(1) \leq p+1$ then

$$\chi_H = \pi_1 + \mu$$

where μ is a character of H of degree at most 3 and $\langle \mu, 1\rangle_H = 0$. This is not possible by Lemma 4.7. Thus $\chi(1) > p+1$.

LEMMA 4.9. If χ is an irreducible constituent of $\chi^{(p-2,2)} + \chi^{(p-2,1^2)}$ which is both p-rational and q-rational, and $\chi(1) \leq 4p-1$, then $\langle \xi, \chi\rangle_G = 1$.

PROOF. Let χ be an irreducible constituent of $\chi^{(p-2,2)} + \chi^{(p-2,1^2)}$ which is both p-rational and q-rational with $\chi(1) \leq 4p-1$; then $\chi(1) > p+1$ by Lemma 4.8 and from the table on the previous page we see that $\chi(1)$ is one of 2p-1, 2p, 2p+1, 3p-1, 3p and 4p-1. Suppose that $2\chi \subseteq \xi$; then $2\pi_1 \subseteq \chi_H$. If $\chi(1) \leq 2p+1$ then

$$\chi_H = 2\pi_1 + \mu$$

where μ has degree at most 5. This is not possible by Lemma 4.7.

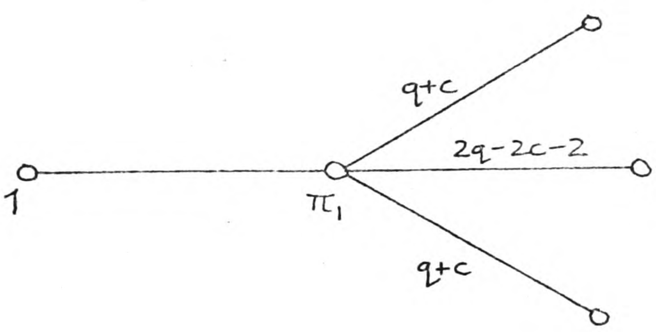
Consequently $\chi(1)$ is 3p-1, 3p or 4p-1. Now $H \geq N_G(Q)$ and if $g \in G\setminus H$ then $Q^g \cap H = 1$, so Theorem 1.6 tells us that

$$\chi_H = \varsigma_1 + \varsigma_2$$

where ξ_1 is a q-projective, ξ_2 a q-indecomposable character of H; also ξ_2 does not lie in the principal q-block of H since χ is not in the principal q-block of G. Hence $2\pi_1 \subseteq \xi_1$, so ξ_1 contains $\phi_{bq+1} + \phi_{dq+1}$ where ϕ_{bq+1}, ϕ_{dq+1} are both nonprincipal q-mates of π_1. Thus

$$\chi_H = 2\pi_1 + \phi_{bq+1} + \phi_{dq+1} + \phi_{cq} + \phi_{aq+\delta}$$

where ϕ_m denotes a character of H of degree m; ϕ_{cq} is q-projective, $\phi_{aq+\delta}$ (δ is 2 or 3) is q-indecomposable and a+b+c+d is either 4 (if $\chi(1)$ is 3p-1 or 3p) or 8 (if $\chi(1) = 4p-1$). By Lemma 4.7, $a \geq 1$, so either b or d is 3 or less. It follows that the Brauer tree of the principal q-block of H has the following fragment:



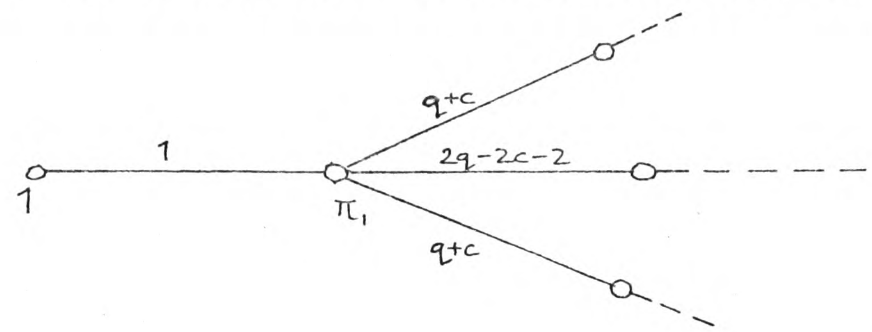
where $0 < c < q$ by Proposition 4.1 (note that q+c cannot be 1 by the argument on p.62 which uses Prop. 1.4); we have labelled the edges with the degrees of the corresponding modular irreducibles. Hence there is an irreducible $\bar{K}H$-module of dimension q+c in the principal q-block of H, contradicting Lemmas 4.4 and 4.5.

LEMMA 4.10. If χ is an irreducible character of G of degree 2p or 2p+1 then $\chi \notin \xi$.

PROOF. Suppose that χ is an irreducible character of G of degree 2p or 2p+1 and that $\chi \subseteq \xi$. By Theorem 1.6,

$$\chi_H = \pi_1 + \phi_{bq+1} + \phi_{cq} + \phi_{aq+\delta}$$

where $\pi_1 + \phi_{bq+1}$ is q-projective indecomposable, ϕ_{cq} is q-projective, $\phi_{aq+\delta}$ (δ is 2 or 3) is q-indecomposable and $a+b+c = 4$. By Lemma 4.7, $a \geq 1$, so $b \leq 3$ and the Brauer tree of the principal q-block of H is



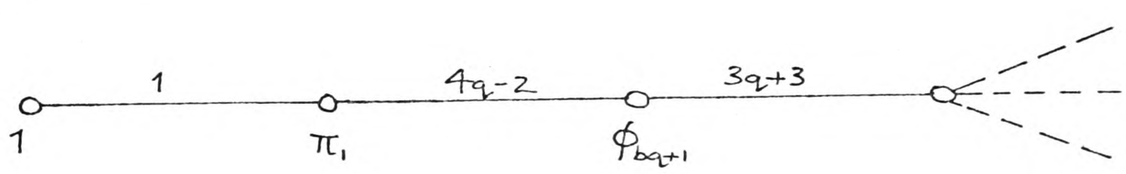
where $0 < c < q$. Hence there is an irreducible $\bar{K}H$-module of dimension $q+c$ in the principal q-block of H, contradicting Lemmas 4.4 and 4.5.

LEMMA 4.11. If χ is an irreducible character of G of degree 3p then $\chi \notin \xi$.

PROOF. As usual, we have

$$\chi_H = \pi_1 + \phi_{bq+1} + \phi_{cq} + \phi_{aq+3}$$

where $\pi_1 + \phi_{bq+1}$ is q-projective indecomposable, ϕ_{cq} is q-projective, ϕ_{aq+3} is q-indecomposable and $a+b+c = 8$. By Lemma 4.5, any nonlinear irreducible $\bar{K}H$-module in the principal q-block of H has dimension at least 3q; it follows that $a = 1$, $b = 7$, $c = 0$ and the Brauer q-tree of the principal q-block of H is



Let V be an $R_q H$-module affording ϕ_{q+3} and let $W = \bar{V}$, so that W is indecomposable. By Theorem 1.6,

$$W_N = T_0 \oplus T_1$$

where T_0 is a q-projective, T_1 a q-indecomposable $\bar{K}N$-module. We have $(T_1)_C \cong V_u \otimes \bar{W}_i$ for some u,i. Now either $X \cong A_4$ or $X \cong V_4$ and 3 divides $\left|\frac{N}{C_N(X)}\right|$.

Since W is faithful (Proposition 4.1) it follows that $\dim \overline{W}_i = 3$. Consequently $u = 1$ and $(T_0)_C \cong V_q \otimes \overline{W}_j$ for some 1-dimensional $\overline{K}X$-module $\overline{W}_j$. Thus

$$W_C \cong (V_q \otimes \overline{W}_j) \oplus (V_1 \otimes \overline{W}_i) .$$

Now X acts on $\overline{W}_j$ as scalars and $X \geqslant V_4$, so X must contain an involution x which acts trivially on $\overline{W}_j$. In its action on W, then, x has precisely two eigenvalues equal to -1 and the rest equal to 1.

We now seek to apply Theorem 1.23 by showing that V affords a quasiprimitive representation of H. Let L be any nontrivial normal subgroup of H. By Clifford's Theorem we may write

$$V_L = \bigoplus X_i$$

where each X_i is an irreducible $\mathbb{C}L$-module and all the X_i have the same dimension. However, we know that $Q \leqslant L$ and

$$\overline{V}_Q \cong V_q \oplus V_1 \oplus V_1 \oplus V_1 .$$

It follows that V_L itself is irreducible, and hence that the representation of H afforded by V is quasiprimitive. By Theorem 1.23 then, H is a known group; since H is 2-transitive, it is one of the groups in the table on p. 103. Hence H contains one of PSL(d,a), PSU(3,a) and Re(a) where a is a prime power and in the respective cases, $4q = a^{d-1}+a^{d-2}+\ldots+a+1$, $4q = a^3+1$ and $4q = a^3+1$. Since $a+1 \mid a^3+1$, the first case must hold. It is easy to see that d must be prime, and hence that $d = 2$. So $PSL(2,a) \leqslant H \leqslant P\Sigma L(2,a)$.

However, in each of these cases we do not have either $C_H(Q) \cong Q \times V_4$ or $C_H(Q) \cong Q \times A_4$ (see [6]), which gives a contradiction.

Lemmas 4.8 - 4.11 show that if χ is a p-rational, q-rational irreducible constituent of $\chi^{(p-2,2)} + \chi^{(p-2,1^2)}$ and $\chi(1) \leqslant 4p-1$ then $\chi(1)$ is one of $2p-1, 3p-1$ and $4p-1$ and $\langle \chi, \xi \rangle_G = 1$.

c. Further facts about ξ.

Recall (see Section a) that $C = C_G(Q) = Q \times X$ where X is isomorphic to a subgroup of A_4, and that $\Theta_1, \dots, \Theta_b$ are characters of X which are sums of N-conjugacy classes of irreducible characters of X.

LEMMA 4.12. If $\Theta_m(1) > 1$ and $s \geqslant 5$ (where $s = \frac{q-1}{r}$) then the q-exceptional characters in the q-block B_m of G do not appear in ξ.

PROOF. It is clear from the results of Section a that we only need to consider the three possibilities: 1. B_m contains 2s q-exceptional characters $\psi_1, \dots, \psi_{2s}$ and $\psi_i(1) \equiv -\varepsilon r \pmod q$, 2. B_m contains s q-exceptional characters $\psi_1, \dots, \psi_s$ and $\psi_i(1) \equiv -3\varepsilon r \pmod q$, and 3. B_m contains 3s q-exceptional characters $\psi_1, \dots, \psi_{3s}$ and $\psi_i(1) \equiv -\varepsilon r \pmod q$.

Case 1. The proof of Lemma 3.5 shows that $\psi_i(1)$ is one of $(r-1)p+1$, rp and $(r+1)p-1$; in the first case $\sum_1^{2s} \psi_i(1) = 2pq-2p-2s(p-1)$, in the second, $\sum_1^{2s} \psi_i(1) = 2pq-2p$, and in the third $\sum_1^{2s} \psi_i(1) = 2pq-2p+2s(p-1)$ (we are supposing here that $\sum \psi_i \subseteq \xi$). Now certainly either $\sum \psi_i \subseteq \chi^{(p-2,2)}$ or $\sum \psi_i \subseteq \chi^{(p-2,1^2)}$. If $\sum \psi_i \subseteq \chi^{(p-2,2)}$ then, since $\chi^{(p-2,2)}(1) = 2pq-p$, we have $\psi_i(1) = (r-1)p+1$ ($\psi_i(1)$ is not rp since this would force $\chi^{(p-2,2)}$ to have a constituent of degree at most p, contradicting Lemma 4.8). But then $\chi^{(p-2,2)}$, a p-projective character, must contain a p-mate for each ψ_i and each of these p-mates has degree at least $2p-1$ by Lemma 4.8. Consequently

$$\chi^{(p-2,2)}(1) = 2pq-p \geqslant 2s((r-1)p+1+2p-1) = 2pq-2p+2sp$$

which is impossible. We obtain a similar contradiction if $\sum \psi_i \subseteq \chi^{(p-2,1^2)}$.

Case 2. Suppose that $\sum \psi_i \subseteq \xi$. If $\psi_i(1) = kp+\varepsilon$ where $\varepsilon \in \{0,1,-1\}$ then the proof of Lemma 3.5 shows that $k+\varepsilon \leqslant 2r$. However, $\psi_i(1) \equiv -3\varepsilon r \pmod q$ so $k+\varepsilon \equiv -3\varepsilon r \pmod q$. This is impossible since $s = \frac{q-1}{r} \geqslant 5$.

Case 3. Suppose that $\sum \psi_i \subseteq \xi$; again the proof of Lemma 3.5 shows that $\psi_i(1)$ is one of $(r-1)p+1$, rp and $(r+1)p-1$. We rule out these possibilities as in Case 1. The lemma is now proved.

LEMMA 4.13. If $t = q$ and $s \geq 5$ then χ_2 is q-rational.

PROOF. Suppose that χ_2 is q-exceptional. Now $\chi_2 \subseteq \chi^{(p-2,1^2)}$ since $\xi = \chi_1 + \chi^{(p-2,1^2)}$ is p-projective, so by Lemma 4.12 the q-block B_m containing χ_2 has $\Theta_m(1) = 1$. Thus $\chi_2(1) \equiv \pm r \pmod q$ and so $\chi_2(1) = (r-1)p+1$ by the proof of Lemma 3.5. We have

$$\xi = \chi_1 + \chi_2 + \sum_2^s (\psi_i + \delta_i) + \sigma$$

where the q-exceptional characters in B_m are $\psi_1 = \chi_2, \psi_2, \ldots, \psi_s$ and $\psi_i + \delta_i$ are p-projective indecomposable characters, σ is p-projective and $\delta_i(1) \equiv -1 \pmod p$. Now $\sum_1^s \psi_i$ has a q-mate in ξ ; if it is one of the δ_i, say it is δ_2. Each δ_i $(i \geq 3)$ has a q-mate σ_i (possibly zero) in σ and each σ_i is p-rational by Theorem 1.12(i). From the table on p.75 we see that $\delta_i(1) + \sigma_i(1) \geq (q-2)p+2$ for $i \geq 3$. Hence, since $s \geq 5$,

$$\xi(1) = 2pq \geq \chi_1(1) + \sum \psi_i(1) + \delta_2(1) + \sum_3^s (\delta_i(1) + \sigma_i(1)) \geq p-1+3(q-2)p+6$$

which is certainly not so.

---

d. Possibilities for $\chi^{(p-2,2)}$ and $\chi^{(p-2,1^2)}$ when $t = q$ and $s \geq 5$.

We suppose that $t = q$ and $s \geq 5$; then by Theorem 1.12(i) the p-exceptional characters do not appear in ξ . If the q-exceptional characters in the block B_m appear in ξ then Lemma 4.12 shows that $\Theta_m(1) = 1$. Hence by Theorem 1.1, B_m contains s q-exceptional characters $\psi_1, \ldots, \psi_s$ and $\psi_i(1) \equiv -\varepsilon r \pmod q$. By the proof of Lemma 3.5, $\psi_i(1)$ is one of $(r-1)p+1$, rp and $(r+1)p-1$, and $\sum_1^s \varphi_i(1) \equiv -1 \pmod q$.

Possibilities for $\chi^{(p-2,1^2)}$.

We know that $\chi_2 \leq \chi^{(p-2,1^2)}$, that $\chi_2(1) \equiv 1 \pmod p$ and that χ_2 is q-rational (Lemma 4.13). The table on p.75 and Lemmas 4.8 - 4.11 show that $\chi_2(1)$ is either $(q-k)p+1$ where k is one of 4,3,2,1,0,-1 and -2, or it is $(2q-1)p+1$. Now $\chi^{(p-2,1^2)}$ is q-projective so we may choose $\phi \leq \chi^{(p-2,1^2)}$ (ϕ possibly zero) such that $\chi_2+\phi$ is q-projective indecomposable. For $m>2$, we write χ_m and sometimes χ'_m to mean an irreducible character of G of degree m. We deal separately with the different possible degrees for χ_2:

$\chi_2(1) = (q-4)p+1.$

Here $\phi(1) \equiv 3 \pmod q$ so from the table on p.75 and Lemmas 4.10 and 4.11, we see that $\phi(1)$ is either $(q+3)p$ or $(q+2)p+1$. The second possibility forces $\chi^{(p-2,1^2)}$ to have a constituent of degree at most p-1, so it does not occur by Lemma 4.8. Hence $\chi^{(p-2,1^2)} = \chi_2 + \chi_{(q+3)p}$.

$\chi_2(1) = (q-3)p+1.$

In this case $\phi(1)$ is one of $3p-1$ and $(q+2)p$, so $\chi^{(p-2,1^2)}$ is either $\chi_2+\chi_{3p-1}+\sigma_{(q-1)p+1}$ where $\sigma_{(q-1)p+1}$ is q-projective of degree $(q-1)p+1$, or it is $\chi_2+\chi_{(q+2)p}$. Clearly every constituent of $\sigma_{(q-1)p+1}$ must be q-rational, so it is irreducible.

$\chi_2(1) = (q-2)p+1.$

Here $\phi(1) \equiv 1 \pmod q$ so ϕ is irreducible and $\phi(1)$ is one of $2p-1$, $pq+1$ and $p(q+1)$. It is not $pq+1$ by Lemma 4.8, so $\chi^{(p-2,1^2)}$ is either $\chi_2+\chi_{2p-1}+\chi_{(q-1)p+1}$ or $\chi_2+\chi_{p(q+1)}$.

$\chi_2(1) = (q-1)p+1.$

In this case $\chi^{(p-2,1^2)} = \chi_2+\sigma_{pq}$ where σ_{pq} is both p- and q-projective of degree pq. If σ_{pq} contains $\Sigma\varphi_i$ for some set $\{\varphi_i\}$ of q-exceptional characters then $\varphi_i(1)$ must be rp (otherwise σ_{pq} would have to contain a p-mate for each φ_i); but then $\Sigma\varphi_i(1) = (q-1)p$, so σ_{pq} has a constituent of degree p or less, contradicting Lemma 4.8. Hence every constituent of σ_{pq} is q-rational and the table on p.75 and Lemmas 4.8 - 4.11 show that σ_{pq} is one of $\chi_{2p-1}+\chi_{(q-2)(p)+1}$, $\chi_{3p-1}+\chi_{(q-3)p+1}$, $\chi_{4p-1}+\chi_{(q-4)p+1}$ and χ_{pq}.

$\chi_2(1)$ = qp+1.

Here $\phi(1) \equiv -1 \pmod q$, so either $\phi(1) = p(q-1)$ or ϕ contains $\Sigma\psi_i$, the sum of some q-exceptional characters. As usual, if $\Sigma\psi_i \subseteq \phi$ then $\psi_i(1) = rp$ and so $\Sigma\psi_i(1) = p(q-1)$. Hence either $\chi^{(p-2,1^2)} = \chi_2 + \chi_{p(q-1)}$ or $\chi^{(p-2,1^2)} = \chi_2 + \Sigma\psi_i$ (where $\psi_i(1) = rp$).

$\chi_2(1)$ = (q+1)p+1.

We have $\phi(1) \equiv -2 \pmod q$, so $\phi(1) = p(q-2)$ and $\chi^{(p-2,1^2)} = \chi_2 + \chi_{p(q-2)}$.

$\chi_2(1)$ = (q+2)p+1.

In this case $\chi^{(p-2,1^2)} = \chi_2 + \chi_{(q-3)p}$.

$\chi_2(1)$ = (2q-1)p+1.

Here $\chi^{(p-2,1^2)} = \chi_2$.

This completes the list of possibilities for $\chi^{(p-2,1^2)}$; they are summarised in a table on p.84.

Possibilities for $\chi^{(p-2,2)}$.

Now $\eta = 1 + \chi_1 + \chi^{(p-2,2)}$ is p-projective and q-projective, so there is a character $\phi \subseteq \chi^{(p-2,2)}$ such that $1+\phi$ is q-projective indecomposable.

Suppose first that ϕ is irreducible; now $\phi(1) \equiv -1 \pmod q$ so $\phi(1)$ is one of (q-2)p+1, (q-1)p, qp-1, (2q-2)p+1 and (2q-1)p. The last case is impossible since it means that $\chi^{(p-2,2)}$ is irreducible, which implies that G is 4-transitive by Proposition 1.7; and the fourth case does not occur by Lemma 4.8. Hence $\chi^{(p-2,2)}$ is one of $\chi_{(q-2)p+1} + \sigma_{(q+1)p-1}$, $\chi_{(q-1)p} + \sigma_{pq}$ and $\chi_{qp-1} + \chi_{(q-1)p+1}$ where $\sigma_{(q+1)p-1}$ is q-projective and σ_{pq} is p- and q-projective.

Now suppose that $\phi = \Sigma\psi_i$ for some q-exceptional characters $\{\psi_i\}$.

If $\psi_i(1)$ is congruent to 1 or -1 (mod p) then $\chi^{(p-2,2)} = \sum_1^s (\psi_i + \delta_i) + \sigma$ where $\psi_i + \delta_i$, σ are p-projective. Each δ_i has a q-mate σ_i (possibly zero) in σ, and for each i we see from the table on p.75 that $(\delta_i + \sigma_i)(1) \geq (q-2)p+2$. Hence

$$\chi^{(p-2,2)}(1) = p(2q-1) \geq s((q-2)p+2)$$

which is not the case, since $s \geq 5$. Consequently $\psi_i(1) = rp$ and $\chi^{(p-2,2)} = \sum_1^s \psi_i + \sigma_{pq}$.

We summarise the possibilities for $\chi^{(p-2,1^2)}$ and $\chi^{(p-2,2)}$ in two tables:

$\chi_2(1)$	Possible $\chi^{(p-2,1^2)}$	Group X
$(q-4)p+1$	$\chi_2 + \chi_{(q+3)p}$	V_4 or A_4
$(q-3)p+1$	$\chi_2 + \chi_{3p-1} + \chi_{(q-1)p+1}$ $\chi_2 + \chi_{(q+2)p}$	Z_3 or V_4 or A_4
$(q-2)p+1$	$\chi_2 + \chi_{2p-1} + \chi_{(q-1)p+1}$ $\chi_2 + \chi_{(q+1)p}$	any X
$(q-1)p+1$	$\chi_2 + \sigma_{pq}$	any X
$qp+1$	$\chi_2 + \sum_1^s \psi_i \quad (\psi_i(1) = rp)$ $\chi_2 + \chi_{p(q-1)}$	any X
$(q+1)p+1$	$\chi_2 + \chi_{(q-2)p}$	Z_3 or V_4 or A_4
$(q+2)p+1$	$\chi_2 + \chi_{(q-3)p}$	V_4 or A_4
$(2q-1)p+1$	χ_2	any X

where σ_{pq} is one of $\chi_{(q-2)p+1} + \chi_{2p-1}$, $\chi_{(q-3)p+1} + \chi_{3p-1}$, $\chi_{(q-4)p+1} + \chi_{4p-1}$ and χ_{pq}.

In the next table, $\sigma_{(q+1)p-1}$ is one of $\chi_{2p-1} + \sum_1^s \psi_i$ $(\psi_i(1) = rp)$, $\chi_{2p-1} + \chi_{(q-1)p}$, $\chi_{3p-1} + \chi_{(q-2)p}$, $\chi_{4p-1} + \chi_{(q-3)p}$ and $\chi_{(q+1)p-1}$.

Possible $\chi^{(p-2,2)}$
$\Sigma\psi_i + \sigma_{pq}\quad (\psi_i(1) = rp)$
$\chi_{(q-2)p+1} + \sigma_{(q+1)p-1}$
$\chi_{(q-1)p} + \sigma_{pq}$
$\chi_{qp-1} + \chi_{(q-1)p+1}$

REMARK. Note that if all constituents of ξ are q-rational then $\|\chi^{(p-2,2)}\| \leq 3$ and $\|\chi^{(p-2,1^2)}\| \leq 3$.

---

e. Possibilities for $\chi^{(p-2,2)}$ and $\chi^{(p-2,1^2)}$ when $t = 2q$ and $s \geq 5$.

Suppose that $t = 2q$ and $s \geq 5$. If the two p-exceptional characters θ_1, θ_2 do not appear in ξ then the arguments of the previous section show that $\chi^{(p-2,2)}$, $\chi^{(p-2,1^2)}$ are as in the tables above, so we assume that $\theta_1 + \theta_2 \subseteq \xi$. By Theorem 1.1 we know that $\theta_i(1) = kp - 2\varepsilon q$ for some integer k and $\varepsilon \in \{-1, 1\}$. Also each θ_i is q-rational, so $\theta_i(1)$ is congruent to one of $0, \pm 1, \pm 2$ and ± 3 modulo q. Hence k is one of $0, 1, 2, 3, q-3, q-2, q-1$ and q. Some possibilities are ruled out by:

LEMMA 4.14. If $\theta_1 + \theta_2 \subseteq \xi$ then $\theta_i(1) > 10q+3$ $(= 3p-2q)$.

PROOF. Suppose that $\theta_1 + \theta_2 \subseteq \xi$ and $\theta_i(1) \leq 10q+3$. Then k is 0, 1, 2 or 3 so $\theta_i(1)$ is one of $2q$, $6q+1$, $6q+2$, $10q+2$ and $10q+3$. If $1 + \pi_1$ is the permutation character of H $(=G_\alpha)$ associated with $\Omega \setminus \{\alpha\}$ then $\pi_1 \subseteq (\theta_1)_H$, so $\theta_1(1)$ is not $2q$; if it is $6q+1$ then

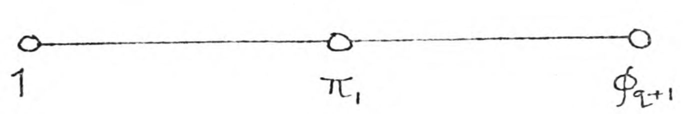
$$(\theta_1)_H = \pi_1 + \mu$$

where μ is a character of H of degree $2q+2$. By Theorem 1.6, $(\theta_1)_H = \zeta_1 + \zeta_2$

where ξ_1 is a q-projective and ξ_2 a q-indecomposable character of H. Now if θ_1, θ_2 were in the principal q-block B_1 of G then they would both be end-nodes in the Brauer tree of B_1 by the proof of Lemma 3.4 (note that $k = 1$, so $(\theta_1)_{N_G(P)}$ contains precisely one linear character by Proposition 1.10). However, t is even, so θ_1, θ_2 are real-valued (Theorem 1.1(v)) and it follows that the Brauer tree of B_1 has at least three real-valued end-nodes $1, \theta_1$ and θ_2, contradicting Theorem 1.3. Therefore θ_1, θ_2 are not in B_1 and so Theorem 1.6 tells us that the character ξ_2 is not in the principal q-block of H. Consequently $\pi_1 \leq \xi_1$, and it follows that ξ_1 contains a q-mate ϕ_{bq+1} for π_1. Thus

$$(\theta_1)_H = \pi_1 + \phi_{bq+1} + \phi_{cq} + \phi'_{aq+1}$$

where by ϕ_m or ϕ'_m we mean a character of H of degree m, and ϕ_{cq} is q-projective, ϕ'_{aq+1} a q-indecomposable character; also $a+b+c = 2$. By Lemma 4.7, $a \geq 1$ and $b \geq 1$, so $b = a = 1$. Also $\phi'_{q+1} \neq \phi_{q+1}$ since ϕ'_{q+1} is not in the principal q-block of H. Thus ϕ_{q+1} is a real-valued end-node in the Brauer tree of the principal q-block of H (Theorem 1.5(ii) applies when $C_G(Q) \neq Q$). This means that the whole real stem of this Brauer tree is just



which contradicts the fact that the sum of the s q-exceptional characters in the principal q-block of H must appear in this real stem (Theorem 1.3). Hence $\theta_1(1)$ cannot be $6q+1$.

If $\theta_1(1) = 6q+2$ then we have, as above

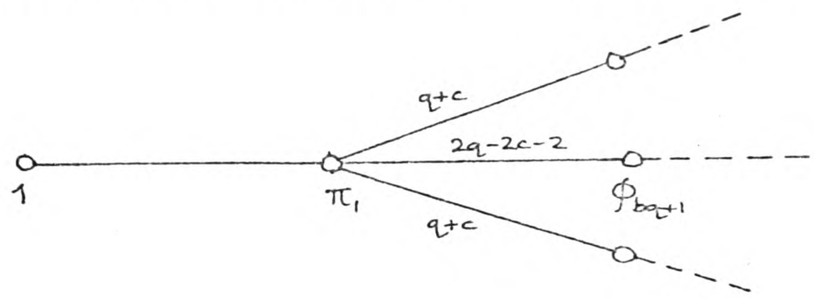
$$(\theta_1)_H = \pi_1 + \phi_{bq+1} + \phi_{cq} + \phi_{aq+2}$$

where $\pi_1 + \phi_{bq+1}$ is q-projective indecomposable, ϕ_{cq} is q-projective, ϕ_{aq+2} is q-indecomposable and $a+b+c = 2$. Again, b must be 1, yielding a contradiction as before.

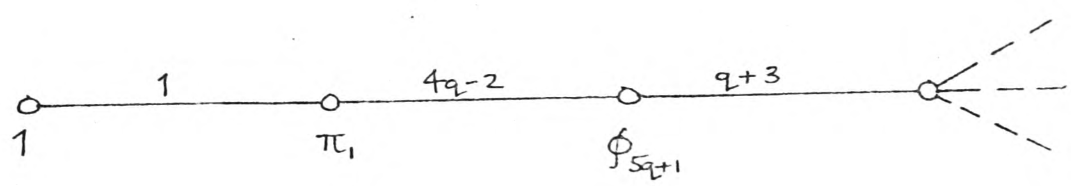
Finally, if $\theta_1(1)$ is $10q+2$ or $10q+3$ then again we have

$$(\theta_1)_H = \pi_1 + \phi_{bq+1} + \phi_{cq} + \phi_{aq+\delta}$$

where $a+b+c = 6$ and δ is 2 or 3. Also $a \geq 1$ by Lemma 4.7, so $b \leq 5$. If $b \leq 4$ then, labelling edges with the degrees of the corresponding modular irreducibles, the Brauer tree of the principal q-block of H is:



where $0 < c < q$ (Prop. 4.1); and if $b = 5$ this Brauer tree is either as above or it is:



Hence there is an irreducible $\overline{K}H$-module of dimension $q+c$ with $0 < c < q$, contradicting Lemmas 4.4 and 4.5. This completes the proof.

If $\theta_1 + \theta_2 \subseteq \eta$ (or ξ) let δ_1, δ_2 be constituents (possibly zero) of η (or ξ) such that $\theta_i + \delta_i$ are q-projective indecomposable ($i = 1,2$). We deal with the remaining possibilities for $\theta_i(1)$ separately:

1. <u>$k = 3$, $\theta_i(1) = 3p+2q = 14q+3$.</u>

Here $\delta_i(1) \equiv -3 \pmod q$ so $\delta_i(1) \geq (q-4)p+1$ for $i = 1,2$ and

$$(\theta_1+\theta_2+\delta_1+\delta_2)(1) \geq 7p-1+(2q-8)p+2 = (2q-1)p+1.$$

It follows that $\theta_1 + \theta_2 \nsubseteq \eta$ and that

$$\xi = \chi_1 + \theta_1 + \theta_2 + \chi_2 + \chi_{(q-4)p+1}$$

where $\chi_2(1) = (q-4)p+1$.

2. $k \geqslant q-3$.

Suppose that $k = q-3$ and $\Theta_i(1) = (q-3)p-2q$. Then $(\Theta_1+\Theta_2)(1) = (2q-7)p+1$ so $\delta_i(1) \equiv 3 \pmod q$ and $(\delta_1+\delta_2)(1) \leqslant 6p$. This forces $\delta_1(1) = \delta_2(1) = 3p$ and $\xi = \chi_1+\Theta_1+\Theta_2+\delta_1+\delta_2$ which means that $\chi_2 \notin \xi$, a contradiction. The remaining cases are ruled out in similar fashion.

We have proved:

LEMMA 4.15. Suppose that $t = 2q$ and $s \geqslant 5$. If the p-exceptional characters Θ_1, Θ_2 do not appear in ξ then $\chi^{(p-2,2)}$, $\chi^{(p-2,1^2)}$ are as in the tables on pp.84-85, and if $\Theta_1+\Theta_2 \subseteq \xi$ then $\Theta_1+\Theta_2 \notin \eta$, $\chi^{(p-2,2)}$ is as in the table on p.85 and

$$\chi^{(p-2,1^2)} = \chi_2 + \chi_{(q-4)p+1} + \Theta_1 + \Theta_2$$

where $\chi_2(1) = (q-4)p+1$ and $\Theta_i(1) = 3p+2q = 14q+3$.

REMARK. Note that if $t = 2q$ then certainly $C_G(Q) \neq Q$.

---

3. DEDUCTIONS FROM THE CHARACTER THEORY.

In this final section we deduce some facts about our insoluble, transitive (but not 4-transitive) group G of degree p, where $p = 4q+1$ and p,q are prime with $p > 13$, from the lists on pp.84 and 85 and Lemma 4.15. As before, we assume that $s \geqslant 5$. We consider separately the following (exhaustive) possibilities for the decomposition of the character ξ of G:

1. for some set $\{\psi_i \mid i = 1,\dots,s\}$ of q-exceptional characters of G, $2\sum_1^s \psi_i \subseteq \xi$,
2. for two different sets $\{\psi_i\}$ and $\{\psi_i'\}$ of q-exceptional characters, $\sum\psi_i + \sum\psi_i' \subseteq \xi$,
3. for precisely one set $\{\psi_i\}$ of q-exceptional characters, $\langle \xi, \psi_i \rangle_G = 1$,
4. every constituent of ξ is q-rational.

Case 1. $2\sum\psi_i \subseteq \xi$.

By Lemma 4.15 and the tables on pp.84 and 85,

$$\chi^{(p-2,2)} = \sum\psi_i + \sigma_{pq} ,$$
$$\chi^{(p-2,1^2)} = \chi_2 + \sum\psi_i$$

where $\chi_2(1) = pq+1$ and $\psi_i(1) = rp$. Recall that c is a generator for the group R, where $N_G(Q) = C_G(Q).R$ and $R \cap C_G(Q) = 1$.

LEMMA 4.16. If $2\sum\psi_i \subseteq \xi$ then r is odd, 3 divides r and $|fix_\Omega c| = 2$. Further, if $C_G(Q) = Q$ then σ_{pq} is irreducible.

PROOF. We have

$$\eta = 1 + \chi_1 + \sum\psi_i + \sigma_{pq} ,$$
$$\xi = 1 + 2\chi_1 + \chi_2 + 2\sum\psi_i + \sigma_{pq} .$$

If r is even then every ψ_i is the character of a real representation (Theorem 1.1 (v)) so by Theorem 1.21 every orbit of G on $\Omega^{\{2\}}\times\Omega^{\{2\}}$ is self-paired (in the sense of Section 2 of Chapter 2). Also, using the notation of Section 2 of Chapter 2,

$$x + y + z = \begin{cases} 3+s & \text{if } \sigma_{pq} \text{ is irreducible} \\ 4+s & \text{if not} \end{cases}$$

and

$$4x + 2y + z = \begin{cases} 7+4s & \text{if } \sigma_{pq} \text{ is irreducible} \\ 8+4s & \text{if not.} \end{cases}$$

Consequently if σ_{pq} is irreducible then $y = z = 1$, $x = 1+s$ and if not, then either $y = 4$, $z = 0$, $x = s$ or $y = 1$, $z = 2$, $x = 1+s$. All these possibilities contradict Proposition 2.7.

Hence r is odd. It follows that there exist $\alpha,\beta,\gamma,\delta,\varepsilon \in \Omega$ such that c acts on $\Omega\setminus\{\alpha,\beta,\gamma,\delta,\varepsilon\}$ as a product of 4s r-cycles, and on $\{\alpha,\beta,\gamma,\delta,\varepsilon\}$ as either 1 or $(\alpha)(\beta)(\gamma\delta\varepsilon)$; so $|fix_\Omega c|$ is 2 or 5. Suppose that it is 5; then $c \in G_{\alpha\beta\gamma\delta\varepsilon}$. Now σ_{pq} is either irreducible or it is the sum $\sigma_1 + \sigma_2$ of two irreducible characters. Suppose first that it is irreducible. Then $y = z = 1$, $x = 1+s$, as was shown above. Now $\#\mathrm{orb}(G_{\alpha\beta\gamma}, \Omega\setminus\{\alpha,\beta,\gamma\}) = \|\xi\| - 6 = 4s+1$, so the orbit lengths of $G_{\alpha\beta\gamma}$ on $\Omega\setminus\{\alpha,\beta,\gamma\}$ are $2,\underbrace{r,\ldots,r}_{4s}$ or $1,1,2r,\underbrace{r,\ldots,r}_{4s-2}$ or $1,r+1,\overbrace{r,\ldots,r}^{4s-1}$ (since $c \in G_{\alpha\beta\gamma}$). Also $\#\mathrm{orb}(G_{\{\alpha\beta\}\gamma}, \Omega\setminus\{\alpha,\beta,\gamma\}) = \langle \xi, \eta\rangle - 3 = 2s+1$, so the third possibility above does not occur and the orbit lengths of $G_{\{\alpha\beta\}\gamma}$ on $\Omega\setminus\{\alpha,\beta,\gamma\}$ are $2,\underbrace{2r,\ldots,2r}_{2s}$ where the orbit of size 2 is $\{\delta,\varepsilon\}$. Now the orbit lengths of $G_{\alpha\beta\gamma\delta}$ on $\Omega\setminus\{\alpha,\beta,\gamma,\delta\}$ are either $1,\underbrace{r,\ldots,r}_{4s}$ or $1,2r,\underbrace{r,\ldots,r}_{4s-2}$ (since $c \in G_{\alpha\beta\gamma\delta}$), so the unique orbit of $G_{\{\alpha\beta\}\delta}$ of size 2 is $\{\gamma,\varepsilon\}$. Hence $\{\gamma,\delta,\varepsilon\}$ is a block of imprimitivity for $G_{\{\alpha\beta\}}$ and so by Proposition 2.11 we have $y+z \geqslant 3$. But $y = z = 1$, which is a contradiction.

Now suppose that $\sigma_{pq} = \sigma_1 + \sigma_2$, a sum of two irreducible characters. Then $\#\mathrm{orb}(G_{\alpha\beta\gamma}, \Omega\setminus\{\alpha,\beta,\gamma\}) = \|\xi\| - 6 = 4s+2$, so the orbit lengths of $G_{\alpha\beta\gamma}$ on $\Omega\setminus\{\alpha,\beta,\gamma\}$ are $1,1,\underbrace{r,\ldots,r}_{4s}$. By the argument at the beginning of the proof of Proposition 2.11, every orbit of $G_{\{\alpha\beta\}\gamma}$ on $\Omega\setminus\{\alpha,\beta,\gamma\}$ has even size, so we must have $\#\mathrm{orb}(G_{\{\alpha\beta\}\gamma}, \Omega\setminus\{\alpha,\beta,\gamma\}) \leqslant 2s+1$. However, $\#\,\mathrm{orb}(G_{\{\alpha\beta\}\gamma}, \Omega\setminus\{\alpha,\beta,\gamma\}) = \langle \xi, \eta\rangle - 3 = 2s+2$, which is a contradiction. Thus we have $|\mathrm{fix}_{\Omega} c| = 2$, from which it follows that 3 divides r.

Finally, suppose that $C_G(Q) = Q$ and that $\sigma_{pq} = \sigma_1 + \sigma_2$. We can assume that $\sigma_1(1) = 2p-1$, so that σ_1 is an end-node in the real stem of the Brauer q-tree of G. Now the number of vertices in the Brauer q-tree is r+1, and by Theorem 1.3, this number is u+2v where u is the number of real-valued nodes, v the number of pairs of non-real-valued nodes. Since $\sigma_1(1) \equiv 1 \pmod q$ u must be odd, so r+1 is odd and r is even, which is not so. Consequently if $C_G(Q) = Q$ then σ_{pq} is irreducible.

Case 2. $\Sigma\psi_i + \Sigma\psi_i' \subseteq \xi$.

Here, the tables on pp.84 and 85 and Lemma 4.15 show that

$$\chi^{(p-2,2)} = \sum_1^s \psi_i + \sigma_{pq} ,$$
$$\chi^{(p-2,1^2)} = \chi_2 + \sum_1^s \psi_i'$$

where $\psi_i(1) = \psi_i'(1) = rp$ and $\chi_2(1) = pq+1$.

LEMMA 4.17. If $\Sigma\psi_i + \Sigma\psi_i' \subseteq \xi$ for distinct sets $\{\psi_i\}$, $\{\psi_i'\}$ of q-exceptional characters then r is even and G is a little generously 3-transitive.

PROOF. It is clear that $\langle\chi^{(p-2,2)}, \chi^{(p-2,1^2)}\rangle = 0$, so G is a little generously 3-transitive by Proposition 1.7(i). Consequently every orbit of G on $\Omega^{\{2\}} \times \Omega^{\{2\}}$ is self-paired (in the sense of Section 2 of Chapter 2), so by Theorem 1.21 each ψ_i is the character of a real representation of G. Hence r is even (Theorem 1.1(v)).

Case 3. $\langle \xi , \psi_i\rangle_G = 1$ for just one set $\{\psi_i\}$.

LEMMA 4.18. Suppose that $\langle \xi , \psi_i\rangle_G = 1$ for just one set $\{\psi_i\}$ of q-exceptional characters. Then

$$\chi^{(p-2,2)} = \sum_1^s \psi_i + \sigma_{pq} \quad \text{and} \quad \|\chi^{(p-2,1^2)}\| \leqslant 6.$$

PROOF. Suppose that $\Sigma\psi_i \subseteq \chi^{(p-2,1^2)}$. Then from the tables and Lemma 4.15 we have $\chi^{(p-2,1^2)} = \chi_2 + \Sigma\psi_i$ ($\chi_2(1) = pq+1$, $\psi_i(1) = rp$), $\|\chi^{(p-2,2)}\| \leqslant 3$ and $\langle\chi^{(p-2,2)}, \chi^{(p-2,1^2)}\rangle = 0$. In all cases then, $\langle \eta , \xi\rangle \leqslant 6$ and $\|\xi\| \geqslant 8+s > 12$, so $\|\xi\| > 2\langle \eta , \xi\rangle$. However $\langle \eta , \xi\rangle$ is the number of orbits of G on $\Omega^{\{2\}} \times \Omega^{(2)}$, each of which corresponds to at most two orbits of G on $\Omega^{(2)} \times \Omega^{(2)}$, so we must have $\|\xi\| \leqslant 2\langle \eta , \xi\rangle$, which is a contradiction.

It follows that $\Sigma\psi_i \subseteq \chi^{(p-2,2)}$, so $\chi^{(p-2,2)} = \Sigma\psi_i + \sigma_{pq}$ and $\|\chi^{(p-2,1^2)}\| \leqslant 6$.

We can say more if $C_G(Q) = Q$:

LEMMA 4.19. Suppose that $C_G(Q) = Q$ and that $\langle \xi, \psi_i \rangle_G = 1$ for the q-exceptional characters $\{\psi_i\}$. Then r is even and G is a little generously 3-transitive.

PROOF. By Lemma 4.18, $\chi^{(p-2,2)}$ is one of $\Sigma\psi_i + \chi_{pq}$ and $\Sigma\psi_i + \chi_{2p-1} + \chi_{(q-2)p+1}$. Suppose that G is not a little generously 3-transitive; then by Proposition 1.7 one of χ_{2p-1}, $\chi_{(q-2)p+1}$ and χ_{pq} appears in $\chi^{(p-2,1^2)}$. If $\chi_{2p-1} \subseteq \chi^{(p-2,1^2)}$ then $2\chi_{2p-1} \subseteq \xi$, contradicting Lemma 4.9. If $\chi_{pq} \subseteq \chi^{(p-2,1^2)}$ then

$$\eta = 1 + \chi_1 + \chi_{pq} + \sum_1^s \psi_i ,$$

$$\xi = 1 + 2\chi_1 + \chi_2 + 2\chi_{pq} + \sum_1^s \psi_i \quad (\chi_2(1) = (q-1)p+1),$$

so $x+y+z = 3+s$, $4x+2y+z = 10+s$ and $3x+y = 7$. Hence either $x = 1$, $y = 4$, $z = s-2$ or $x = 2$, $y = 1$, $z = s$; in the first case by Proposition 2.6 and in the second by Proposition 2.7, not every orbit of G on $\Omega^{\{2\}} \times \Omega^{\{2\}}$ is self-paired. It follows by Theorem 1.21 and Theorem 1.1(v) that r is odd and that G has precisely 3 self-paired orbits on $\Omega^{\{2\}} \times \Omega^{\{2\}}$. Then Proposition 2.10 tells us that

$$3 \geq z - x + 3$$

which forces $s \leq 3$, a contradiction.

Finally, if $\chi_{(q-2)p+1} \subseteq \chi^{(p-2,1^2)}$ then $\chi^{(p-2,1^2)}$ is one of $\chi_{(q-2)p+1} + \chi_{(q-1)p+1} + \chi'_{2p-1}$ and $\chi_{(q-2)p+1} + \chi_{(q+1)p}$. In the first case $\chi'_{2p-1} \neq \chi_{2p-1}$ by Lemma 4.9. But then 1, χ_{2p-1} and χ'_{2p-1} are all end-nodes in the real stem of the Brauer q-tree of G (recall that $C_G(Q) = Q$), which is impossible. In the second case we have $x+y+z = 4+s$, $4x+2y+z = 11+s$, so that $3x+y = 7$; we now obtain a contradiction using Proposition 2.10 as above.

Case 4. Every constituent of ξ is q-rational.

LEMMA 4.20. Suppose that every constituent of ξ is q-rational and that G is not a little generously 3-transitive. Then $\|\chi^{(p-2,2)}\| = 3$, $\langle \chi^{(p-2,2)}, \chi^{(p-2,1^2)} \rangle = 1$

and $\|\chi^{(p-2,1^2)}\|$ is 3 or 4.

PROOF. From the tables and Lemma 4.15 we have $\|\chi^{(p-2,2)}\| \leq 3$, $\|\chi^{(p-2,1^2)}\| \leq 6$. Suppose first that $\|\chi^{(p-2,2)}\| = 2$ under the hypotheses. Then $\langle \chi^{(p-2,2)}, \chi^{(p-2,1^2)} \rangle = 1$ by Proposition 1.7(i) and $\|\eta\| = 4$, $\|\xi\| = 5 + \|\chi^{(p-2,2)}\| + 2\langle \chi^{(p-2,2)}, \chi^{(p-2,1^2)} \rangle + \|\chi^{(p-2,1^2)}\|$. Now $\chi^{(p-2,1^2)}$ is reducible by Proposition 1.7(ii), so $\|\chi^{(p-2,1^2)}\|$ is 2, 3, 4 or 6. If it is 2 then we find that y = z = 1, x = 2, contradicting Proposition 2.7 (every orbit of G on $\Omega^{\{2\}} \times \Omega^{\{2\}}$ is self-paired by Theorem 1.21). If $\|\chi^{(p-2,1^2)}\|$ is 3 then y = x = 2, z = 0. By Corollary 2.8, G is 4-homogeneous and hence is 4-transitive by the results of [23]; this is not the case. If $\|\chi^{(p-2,1^2)}\|$ is 4 then y = 0, which is not so, and if it is 6 then $\|\xi\| > 2\langle \xi, \eta \rangle$.

Thus $\|\chi^{(p-2,2)}\| = 3$ and $\|\eta\| = 5$. We have

$$\|\xi\| = 8 + 2\langle \chi^{(p-2,2)}, \chi^{(p-2,1^2)} \rangle + \|\chi^{(p-2,1^2)}\|.$$

Suppose that $\langle \chi^{(p-2,2)}, \chi^{(p-2,1^2)} \rangle = 2$; then $\|\xi\|$ is 15 or 16. If it is 15 then y = z = 1, x = 3 and if it is 16 then y = 2, z = 0, x = 3; both these possibilities contradict Proposition 2.7.

Hence $\langle \chi^{(p-2,2)}, \chi^{(p-2,1^2)} \rangle = 1$. If $\|\chi^{(p-2,1^2)}\| = 2$ then $\|\xi\| = 12$, so either y = 1, x = z = 2 or y = 4, z = 0, x = 1; the first possibility contradicts Proposition 2.7, the second, Proposition 2.6. The lemma is now proved.

REMARK. In fact, if every constituent of ξ is q-rational then

$$3 \geq \|\chi^{(p-2,2)}\| \geq \|\chi^{(p-2,1^2)}\| .$$

For if this is not the case, it is easy to see that $\|\xi\| \geq 2\langle \xi, \eta \rangle$ which means that $|G_{\alpha\beta}|$ must be odd. This is impossible by the theorem of Bender in [3].

LEMMA 4.21. Suppose that $C_G(Q) = Q$ and that every constituent of ξ is q-rational. Then G is a little generously 3-transitive and $\|\chi^{(p-2,1^2)}\| \leq 2$.

PROOF. If G is not a little generously 3-transitive then by Lemma 4.20, $\|\chi^{(p-2,2)}\| = \|\chi^{(p-2,1^2)}\| = 3$ and from the tables on pp.84 and 85 we see that there are characters $\chi_{2p-1} \subseteq \chi^{(p-2,2)}$, $\chi'_{2p-1} \subseteq \chi^{(p-2,1^2)}$ with $\chi_{2p-1} \neq \chi'_{2p-1}$ by Lemma 4.9. But this means that 1, χ_{2p-1} and χ'_{2p-1} are distinct end-nodes in the real stem of the q-tree of G, which is a contradiction.

Consequently G is a little generously 3-transitive and $\|\chi^{(p-2,1^2)}\| \leq 2$.

To conclude, we summarise the results obtained in Lemmas 4.16 - 4.21 in a table:

Assumption on ξ	$C_G(Q)$	Result	$\chi^{(p-2,2)}$	$\chi^{(p-2,1^2)}$
$2\sum\psi_i \subseteq \xi$	any	r odd, $3 \mid r$, $\lvert \mathrm{fix}_\Omega c \rvert = 2$	$\sum\psi_i + \sigma_{pq}$	$\chi_2 + \sum\psi_i$
$\sum\psi_i + \sum\psi'_i \subseteq \xi$	any	G is l.g.3-tr., r is even	$\sum\psi_i + \sigma_{pq}$	$\chi_2 + \sum\psi'_i$
$\langle \xi, \psi_i \rangle = 1$ for one set $\{\psi_i\}$	any		$\sum\psi_i + \sigma_{pq}$	norm ≤ 6
$\langle \xi, \psi_i \rangle = 1$	Q	G is l.g.3-tr.	$\sum\psi_i + \sigma_{pq}$	norm ≤ 3
constituents of all q-rational	any	$3 \geq \|\chi^{(p-2,2)}\| \geq \|\chi^{(p-2,1^2)}\|$ and G not l.g.3-tr. $\Rightarrow \|\chi^{(p-2,2)}\| = \|\chi^{(p-2,1^2)}\| = 3$, $\langle \chi^{(p-2,2)}, \chi^{(p-2,1^2)} \rangle = 1$.		
constituents of all q-rational	Q	G is l.g.3-tr.	norm ≤ 3	norm ≤ 2

"Sometimes Eeyore thought sadly to himself, 'Why?' and sometimes he thought, 'Wherefore?' and sometimes he thought, 'Inasmuch as which?'"

A.A.Milne, 'Winnie-the-Pooh'.

Chapter 5: PRELIMINARIES FOR PROBLEM B.

As was stated in the Introduction, Problem B concerns certain algebras derived from 2-graphs and the use of these algebras to deduce facts about the automorphism groups of the 2-graphs. This chapter consists of some preliminaries for the problem; first we introduce 2-graphs and their correspondence with switching classes of graphs and give some examples of regular 2-graphs with 2-transitive automorphism groups. Then we state some results of Mortimer [26] on the hearts of the known 2-transitive groups (as defined in the Introduction). Finally we present a few definitions concerning Lie algebras, which we shall consider in Chapter 7.

1. SWITCHING CLASSES AND 2-GRAPHS.

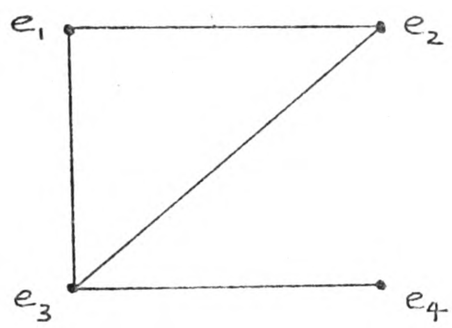
Let Ω be a finite set and let $\Delta \subseteq \Omega^{\{3\}}$. Recall (see the Introduction) that (Ω,Δ) is a 2-graph if every 4-subset of Ω contains an even number of elements of Δ; it is trivial if either $\Delta = \emptyset$ or $\Delta = \Omega^{\{3\}}$, and is nontrivial otherwise. It is regular if every 2-subset of Ω is contained in the same number a of elements of Δ. We say that (Ω,Δ) is an even 2-graph if $|\Omega|$ is even and every 2-subset of Ω is contained in an even number of elements of Δ.

Write $\Omega = \{e_1,\ldots,e_n\}$ and let Γ be a (simple, undirected) graph on Ω, Σ a subset of Ω. Define a new graph Γ_Σ as follows:

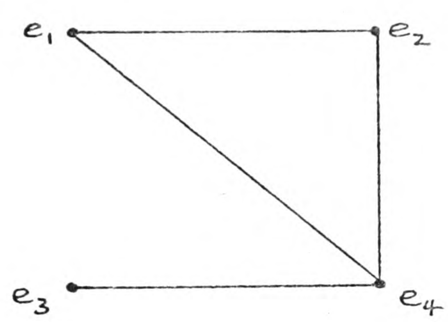
(i) if $e_i,e_j \in \Sigma$ or $e_i,e_j \in \Omega\backslash\Sigma$ then e_i,e_j are joined in Γ_Σ if and only if e_i,e_j are joined in Γ,

(ii) if $e_i \in \Sigma$, $e_j \in \Omega\backslash\Sigma$ then e_i,e_j are joined in Γ_Σ if and only if e_i,e_j are not joined in Γ.

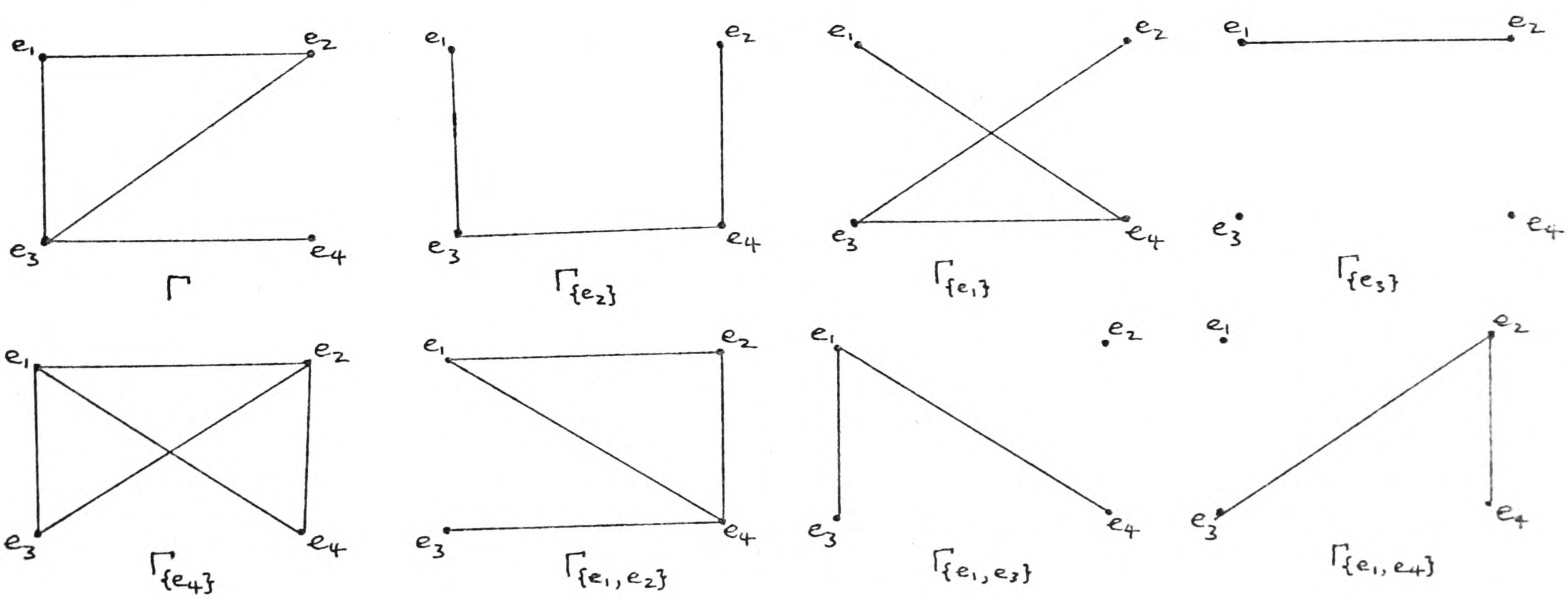
The graph Γ_Σ is said to be the graph obtained from Γ by switching with respect to the vertices Σ. Thus if Γ is the graph:



then the graph $\Gamma_{\{e_1,e_2\}}$ obtained from Γ by switching with respect to $\{e_1, e_2\}$ is:



Two graphs Γ, Γ' on Ω are <u>switching equivalent</u> if $\Gamma' = \Gamma_\Sigma$ for some subset Σ of Ω; this is an equivalence relation on the graphs on Ω, and the equivalence classes are called <u>switching classes</u>. Any graph Γ on Ω belongs to a switching class consisting of 2^{n-1} distinct graphs (some of which may be isomorphic to each other). The switching class to which the above graphs on 4 vertices belong consists of the following 8 graphs:



It is clear that, for any vertex of any graph, there is precisely one graph in the switching class to which the graph belongs in which this vertex is isolated.

Again let Γ be a graph on Ω and define $\Delta \subseteq \Omega^{\{3\}}$ by

$\Delta = \{\{e_i, e_j, e_k\} \mid e_i, e_j, e_k$ have an odd number of edges in Γ between them$\}$.

Then (Ω, Δ) is a 2-graph; two graphs Γ_1, Γ_2 on Ω give rise to the same 2-graph in this way if and only if they are switching equivalent. This gives a 1-1 correspondence between 2-graphs and switching classes of graphs (Theorem 4.2 of [36]).

The graphs in a switching class corresponding to an even 2-graph are easily characterised:

PROPOSITION 5.1. Let Γ be a graph on a set Ω of n vertices, where n is even. Then the corresponding 2-graph (Ω, Δ) is even if and only if either every vertex of Γ has even valency or every vertex of Γ has odd valency.

PROOF. For any $e_i \in \Omega$ let V_i denote the set of vertices joined to e_i in Γ. If e_i, e_j are non-adjacent points in Γ then $\{e_i, e_j, e_k\} \in \Delta$ if and only if $e_k \in (V_i \cup V_j) \setminus (V_i \cap V_j)$, so the number of elements of Δ containing $\{e_i, e_j\}$ is

$$|V_i \cup V_j| - |V_i \cap V_j| = |V_i| + |V_j| - 2|V_i \cap V_j| .$$

If e_i, e_j are joined in Γ, the number of elements of Δ containing $\{e_i, e_j\}$ is

$$n - |V_i| - |V_j| + 2|V_i \cap V_j| .$$

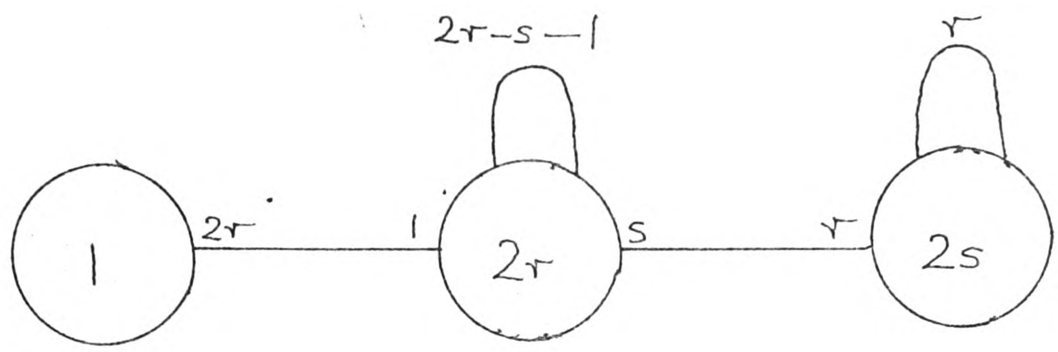
The result follows.

Finally, let (Ω, Δ) be a nontrivial regular 2-graph in which every 2-subset is contained in a elements of Δ. Define a graph Γ on Ω by

(i) e_1 is an isolated vertex in Γ,

(ii) e_i is joined to e_j in Γ if and only if $\{e_1, e_i, e_j\} \in \Delta$.

Then Γ is in the switching class corresponding to (Ω, Δ). It is easy to see that the subgraph of Γ on $\{e_2, \ldots, e_n\}$ is strongly regular with parameters given by the diagram:



where r,s are nonzero integers and 2r = a (also n = 2+2r+2s); that is, this subgraph is regular of valency 2r, any two joined points have 2r-s-1 mutual adjacencies and any two non-joined points have r mutual adjacencies. Note that this means that a and n are even, so that a nontrivial regular 2-graph is even.

For a fuller introduction to switching classes of graphs, see [15].

---

2. EXAMPLES OF REGULAR 2-GRAPHS.

Regular 2-graphs were introduced by G.Higman in [16] in order to provide a combinatorial setting for 2-transitive representations of certain groups. In this section we give examples of regular 2-graphs with 2-transitive automorphism groups; our main references are [36] and Chapter 4 of [38].

(a) Symplectic 2-graphs.

Let $V = V(2m,2)$ be a vector space of dimension $2m$ $(m \geq 2)$ over $GF(2)$, and let $B: V \times V \to GF(2)$ be a non-degenerate, alternating, bilinear form on V. The symplectic 2-graph $\Sigma(2m,2)$ consists of the vectors of V and the set of 3-subsets $\{u,v,w\}$ of V satisfying

$$B(u,v)+B(v,w)+B(w,u) = 0 .$$

The 2-graph $\Sigma(2m,2)$ is regular and its parameters (as described in the previous section) are

$$n = 2^{2m}, \quad r = 2^{2m-2}-1, \quad s = 2^{2m-2},$$

(see 2.4 of [38]). The group of linear transformations of V which leave B invariant is the symplectic group $Sp(2m,2)$; if $T(V)$ is the group of translations of V (that is, the set of permutations $t : v \to v+a$ $(a \in V)$ of V), then the automorphism group of $\Sigma(2m,2)$ is $T(V).Sp(2m,2)$ (Theorem 2.5 of [38]). Note that this is a subgroup of $AGL(2m,2)$.

(b) <u>Quadratic forms over GF(2).</u>

We continue the above notation. Denote by $\mathcal{S}$, the set of quadratic forms $Q:V \to GF(2)$ satisfying

$$Q(x+y)+Q(x)+Q(y) = B(x,y) \quad \text{for all } x,y \in V .$$

The group $Sp(2m,2)$, acting in the natural way, has two orbits on $\mathcal{S}$: the orbit $\mathcal{S}^+$ of forms of index m and the orbit $\mathcal{S}^-$ of forms of index m-1. Denote the actions of $Sp(2m,2)$ on $\mathcal{S}^+$, $\mathcal{S}^-$ by $Sp(2m,2)^+$, $Sp(2m,2)^-$ respectively; both these actions are 2-transitive. Fix $Q_0 \in \mathcal{S}$. For each $Q \in \mathcal{S}$ there is a unique $a \in V$ such that

$$Q(x) = Q_0(x) + B(a,x)^2 \quad \text{for all } x \in V.$$

Write $Q = Q_a$. We define sets of 3-subsets Δ^+ (Δ^-) of $\mathcal{S}^+$ $(\mathcal{S}^-)$ by taking $\{Q_a,Q_b,Q_c\}$ to be an element of Δ^+ (Δ^-) if $Q_a,Q_b,Q_c \in \mathcal{S}^+$ $(\mathcal{S}^-)$ and

$$B(a,b)+B(b,c)+B(c,a) = 0.$$

Then $\Omega^+(2m,2) = (\mathcal{S}^+, \Delta^+)$ and $\Omega^-(2m,2) = (\mathcal{S}^-, \Delta^-)$ are regular 2-graphs with parameters (Theorem 3.18 of [38]):

$$\underline{\Omega^+(2m,2)}: \; n = 2^{m-1}(2^m+1), \quad r = 2^{2m-3}+2^{m-2}-1, \quad s = 2^{2m-3},$$

$$\underline{\Omega^-(2m,2)}: \; n = 2^{m-1}(2^m-1), \quad r = 2^{2m-3}-2^{m-2}-1, \quad s = 2^{2m-3}.$$

The automorphism groups of $\Omega^+(2m,2)$, $\Omega^-(2m,2)$ are $Sp(2m,2)^+$, $Sp(2m,2)^-$ respectively (Theorem 3.37 of [38]).

(c) Payley 2-graphs.

Let q be a prime power with $q \equiv 1 \pmod 4$. Identify $PG(1,q)$ with the set $\Omega = \{\infty\} \cup GF(q)$ on which $P\Sigma L(2,q)$ acts as the group

$$\left\{ x \to \frac{ax^{\sigma}+b}{cx^{\sigma}+d} \;\middle|\; ad-bc \text{ a nonzero square in } GF(q),\ \sigma \text{ a field automorphism} \right\}$$

and define the set Δ of 3-subsets of Ω as follows:

(i) for $x,y \in GF(q)$, $\{\infty,x,y\} \in \Delta \iff x-y$ is a nonzero square

(ii) for $x,y,z \in GF(q)$, $\{x,y,z\} \in \Delta \iff (x-y)(y-z)(z-x)$ is a nonzero square.

Then (Ω,Δ) is a regular 2-graph, called the Payley 2-graph $P(q)$. It has parameters

$$n = q+1, \quad r = s = \tfrac{1}{4}(q-1)$$

and its automorphism group is $P\Sigma L(2,q)$, which is 2-transitive on Ω (Theorem 3.2 of [38]).

(d) Unitary 2-graphs.

Let V be a 3-dimensional vector space over $GF(q^2)$ where q is a power of an odd prime, and let $PG(2,q^2)$ be the associated projective plane. Let $H: V \times V \to GF(q^2)$ be a non-degenerate Hermitean form on V, so that $H(x,y) = \overline{H(y,x)}$ for all $x,y \in V$, and let

$$\Omega = \{\langle x\rangle \in PG(2,q^2) \mid H(x,x) = 0\} .$$

Define the set Δ of 3-subsets of Ω as follows:

(i) if $q \equiv 3 \pmod 4$ then $\{\langle x\rangle, \langle y\rangle, \langle z\rangle\} \in \Delta \iff H(x,y)H(y,z)H(z,x)$ is a nonzero square,

(ii) if $q \equiv 1 \pmod 4$ then $\{\langle x\rangle, \langle y\rangle, \langle z\rangle\} \in \Delta \iff H(x,y)H(y,z)H(z,x)$ is not a square.

Then (Ω,Δ) is a regular 2-graph, called the unitary 2-graph $U(q)$, on which

$P\Gamma U(3,q^2)$ acts 2-transitively. Its parameters are

$$n = q^3+1, \quad r = \tfrac{1}{4}(q-1)(q^2+1), \quad s = \tfrac{1}{4}(q+1)(q^2-1)$$

(Theorem 4.11 of [38]).

(e) 2-graphs of Ree type.

It is explained on pp. 110 - 112 of [38] how the existence of the Ree groups $Re(q)$ (or ${}^2G_2(q)$), where q is an odd power of 3, implies the existence of a family $R(q)$ of regular 2-graphs having the same parameters as $U(q)$.

(f) The groups HS and Co_3.

The regular 2-graphs $H(176)$ and $C(276)$ on 176 and 276 points respectively, having the Higman-Sims group HS and the Conway group Co_3 as their automorphism groups (acting 2-transitively), are constructed on pp. 112-121 of [38]. The parameters are

$\underline{H(176)}$: $n = 176$, $r = 36$, $s = 51$,

$\underline{C(276)}$: $n = 276$, $r = 56$, $s = 81$.

We conclude this section with a theorem of Taylor (taken from pp. 121 - 123 of [38]).

THEOREM 5.2. Let G be a known 2-transitive group of degree n (so that G belongs to the list of groups given in the table on p.103) and suppose that G acts on a nontrivial regular 2-graph (Ω, Δ) on n points. Then either $G \leqslant AGL(d,2)$ and G contains the translations of $V(d,2) = \Omega$, or (Ω, Δ) is one of the regular 2-graphs listed above under (a),(b),(c),(d),(e) and (f) and G is a subgroup of the relevant known 2-transitive group.

3. THE HEART OF A PERMUTATION GROUP.

Let G be a permutation group of degree n on a set Ω and let p be a prime number dividing n, F a field of characteristic p. Recall that in the Introduction, we defined the FG-submodules S, T of the permutation module $F\Omega$ and called the FG-module $\frac{S}{T}$ the heart of G acting on Ω, over F. The methods of [24] and Chapters 5 and 6 of [32] illustrate how knowledge of the structure of the heart can give information about the action of G on Ω. An elementary example of this is the fact that if G is primitive, $n \geq 4$ and the heart is an irreducible FG-submodule (for some prime number p dividing n) then G is 2-transitive on Ω. The converse is not true - the heart need not be irreducible when G is 2-transitive; the affine groups AGL(d,p) acting on V(d,p) ($p \geq 5$) give the easiest counterexamples (for these groups $F\Omega$ has a d-dimensional submodule

$$\left\{ \sum_{\omega \in \Omega} f(\omega)\omega \;\middle|\; f \text{ a linear function on } V(d,p) \right\}).$$

Mortimer has studied the hearts in all characteristics of the known 2-transitive groups in [26]; his results are summarised in the table on the following page.

Group G	Degree n	Conditions under which the heart of G over F (of char. p dividing n) is reducible
S_n, A_n $(n \geq 5)$	n	always irreducible
$G \leq A\Gamma L(d,p^r)$ containing the translations	p^{rd}	reducible
$PSL(d,q) \leq G \leq P\Gamma L(d,q), d \geq 3$	$\frac{q^d-1}{q-1}$	always irreducible
$Sp(2m,2)^+$, $m \geq 2$	$2^{m-1}(2^m+1)$	$p = 2$
$Sp(2m,2)^-$, $m \geq 3$	$2^{m-1}(2^m-1)$	$p = 2$
G a 3-transitive subgroup of $P\Gamma L(2,q)$	$q+1$	always irreducible
$PSL(2,q) \leq G \leq P\Sigma L(2,q)$	$q+1$	$F \geq GF(2)$ if $q \equiv \pm 1 \pmod 8$ $F \geq GF(4)$ if $q \equiv \pm 3 \pmod 8$
$Sz(q) \leq G \leq Aut(Sz(q))$	q^2+1	$p \mid (q+1+2^{k+1})$ where $q = 2^{2k+1}$
$PSU(3,q^2) \leq G \leq P\Gamma U(3,q^2)$	q^3+1	$p \mid q+1$
$Re(q) \leq G \leq Aut(Re(q))$	q^3+1	$p \mid (q+1)(q+1+3^{k+1})$ where $q=3^{2k+1}$
M_{24}	24	$p = 2$
M_{23}	23	irreducible
M_{22}	22	$p = 2$
M_{12}	12	irreducible
M_{11}	11	irreducible
M_{11}	12	$p = 3$
$PSL(2,11)$	11	irreducible
HS	176	$p = 2$ or $p = 3$
Co_3	276	no result obtained
A_7	15	irreducible

4. LIE ALGEBRAS.

Let $\mathcal{L}$ be a finite dimensional algebra over a field F (that is, a finite dimensional vector space over F in which a bilinear product is defined). We say that $\mathcal{L}$ is a Lie algebra if, for every $x,y,z \in \mathcal{L}$,

$$x^2 = 0 \quad \text{and} \quad (xy)z+(yz)x+(zx)y = 0.$$

The latter equation is called the Jacobi identity.

For any two subspaces $\mathcal{U}, \mathcal{V}$ of $\mathcal{L}$, we define

$$[\mathcal{U}\mathcal{V}] = \langle uv \mid u \in \mathcal{U}, v \in \mathcal{V} \rangle ,$$

that is, $[\mathcal{U}\mathcal{V}]$ is the subspace of $\mathcal{L}$ over F spanned by all products uv. Define

$$\mathcal{L}' = [\mathcal{L}\mathcal{L}] \quad , \mathcal{L}'' = [\mathcal{L}'\mathcal{L}'] \quad ,\ldots, \quad \mathcal{L}^{(k)} = [\mathcal{L}^{(k-1)}\mathcal{L}^{(k-1)}] ,\ldots.$$

Then the series $\mathcal{L} \geq \mathcal{L}' \geq \mathcal{L}'' \geq \ldots \geq \mathcal{L}^{(k)} \geq \ldots$ is called the derived series of $\mathcal{L}$. If $\mathcal{L}^{(k)} = 0$ for some k then $\mathcal{L}$ is said to be solvable; the smallest integer k for which $\mathcal{L}^{(k)} = 0$ is called the derived length of $\mathcal{L}$.

Now define

$$\mathcal{L}^2 = [\mathcal{L}\mathcal{L}] \quad (= \mathcal{L}'), \ \mathcal{L}^3 = [\mathcal{L}^2\mathcal{L}] \quad ,\ldots, \quad \mathcal{L}^{k+1} = [\mathcal{L}^k\mathcal{L}] \quad ,\ldots.$$

The series $\mathcal{L} \geq \mathcal{L}^2 \geq \mathcal{L}^3 \geq \ldots \geq \mathcal{L}^k \geq \mathcal{L}^{k+1} \geq \ldots$ is called the lower central series of $\mathcal{L}$; if $\mathcal{L}^{k+1} = 0$ for some k then $\mathcal{L}$ is nilpotent, and the smallest such integer k is the class of $\mathcal{L}$.

The centre $\mathcal{C}$ of $\mathcal{L}$ is the subspace defined by

$$\mathcal{C} = \{ u \in \mathcal{L} \mid uv = 0 \text{ for all } v \in \mathcal{L} \} .$$

Let K be a field containing F and consider the tensor product $\mathcal{L}_K = K \otimes \mathcal{L}$ as an algebra over K (with $\alpha(\sum \alpha_i \otimes x_i) = \sum \alpha\alpha_i \otimes x_i$ for $\alpha, \alpha_i \in K$, $x_i \in \mathcal{L}$). This is a Lie algebra over K, and if $\{e_i \mid i \in I\}$ is a basis for $\mathcal{L}$ over F then $\{1 \otimes e_i \mid i \in I\}$ is a basis for $\mathcal{L}_K$ over K. Further, $\mathcal{L}$ is nilpotent (solvable) if and only if $\mathcal{L}_K$ is nilpotent (solvable).

For a comprehensive treatment of Lie algebras, see [22].

"The heart has its reasons which reason knows nothing of."

Blaise Pascal, 'Pensées'.

Chapter 6: A RESULT ON THE HEART.

In this chapter we consider even 2-graphs (Ω, Δ) (that is, 2-graphs for which $|\Omega|$ is even and every 2-subset of Ω is contained in an even number of elements of Δ) and the permutation modules in characteristic 2 of their automorphism groups. The main result proved is Theorem 6.3.

Let (Ω, Δ) be a nontrivial even 2-graph with $\Omega = \{e_1, \ldots, e_n\}$ (n even) and let G be its automorphism group. Let F be any field of charactersistic 2 and define products on the permutation module $F\Omega = \mathcal{L}$ by

$$e_i e_j = \sum_{\{e_i, e_j, e_k\} \in \Delta} e_k \qquad (i,j \in \{1,\ldots,n\}),$$

extending linearly. This makes $\mathcal{L}$ into an algebra; $\mathcal{L}$ is commutative, $e_i e_i = 0$ for all i, and G acts on $\mathcal{L}$ by algebra automorphisms. Clearly the derived algebra $\mathcal{L}'$ is an FG-submodule of $\mathcal{L}$, and if S is the submodule of codimension 1 defined (as in the Introduction) by

$$S = \{\ \Sigma \lambda_i e_i \mid \Sigma \lambda_i = 0\}$$

then $\mathcal{L}' \subseteq S$ since (Ω, Δ) is an even 2-graph. We shall study the algebra $\mathcal{L}$ in some detail in Chapter 7, but for our present purposes we only need the following result.

PROPOSITION 6.1. There is a subset J of $\{e_2, \ldots, e_n\}$ such that

$$\{e_1 e_j \mid e_j \in J\} \cup \{\textstyle\sum_1^n e_k\}$$

is a basis for $\mathcal{L}'$. Further, let Γ be the graph in the switching class corresponding to (Ω, Δ) in which the point e_1 is isolated (see Section 1 of Chapter 5). Then $\mathcal{L}' \subset S$ if and only if there is a proper nonempty subset K of $\{e_2, \ldots, e_n\}$ such that every point of Ω is joined in Γ to an even number of points of K.

PROOF. Let $i,j \in \{2,\ldots,n\}$. If e_i is not joined to e_j in Γ then $e_i e_j$ is the sum of those e_k which are joined in Γ to precisely one of e_i and e_j;

therefore

$$e_i e_j = e_1 e_i + e_1 e_j \ .$$

If e_i is joined to e_j in Γ then $e_i e_j$ is the sum of those e_k which are joined to both or neither of e_i, e_j, so

$$e_i e_j = e_1 e_i + e_1 e_j + \sum_1^n e_k \ .$$

Hence $\mathcal{L}'$ is contained in the subspace spanned by $\{e_1 e_j \mid j = 2,\dots,n\} \cup \{\sum_1^n e_k\}$. Since (Ω, Δ) is nontrivial there is a 3-subset, say $\{e_a, e_b, e_c\}$ in Δ. It is easy to see that

$$e_a e_b + e_b e_c + e_c e_a = \sum_1^n e_k$$

so that $\sum_1^n e_k \in \mathcal{L}'$ and so $\mathcal{L}' = \langle \{e_1 e_j \mid j = 2,\dots,n\} \cup \{\sum_1^n e_k\} \rangle$.
Now $\sum_1^n e_k$ involves e_1 and hence is linearly independent of $\{e_1 e_j \mid j = 2,\dots,n\}$. Consequently there is a subset J of $\{e_2,\dots,e_n\}$ such that

$$\{e_1 e_j \mid e_j \in J\} \cup \{\sum_1^n e_k\}$$

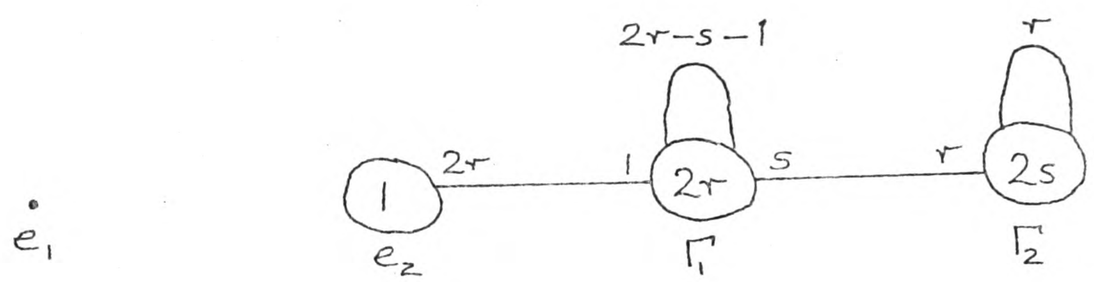
is basis for $\mathcal{L}'$, and the first part of the proposition is proved.

Since S has dimension n-1, $\mathcal{L}' \subset S$ if and only if there is a proper subset K (nonempty) of $\{e_2,\dots,e_n\}$ such that $\sum_{k \in K} e_1 e_k = 0$, that is, if and only if every point of Ω is joined in Γ to an even number of points of K (recall that F has characteristic 2).

Now we apply this result to regular 2-graphs; recall that a nontrivial regular 2-graph is even (see Section 1 of Chapter 5).

PROPOSITION 6.2. Let (Ω, Δ) be a nontrivial regular 2-graph and let Γ be the graph in the corresponding switching class in which the point e_1 is isolated. Let r, s be the parameters associated with the subgraph of Γ on $\{e_2,\dots,e_n\}$ as described in Section 1 of Chapter 5. Then $\mathcal{L}' \subset S$ if r is even.

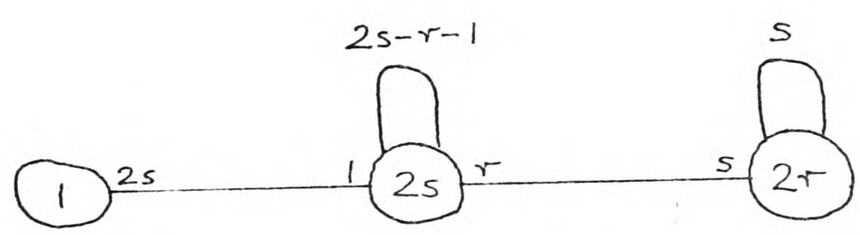
PROOF. Let Γ_1 be the set of points joined to e_2 in Γ and let $\Gamma_2 = \{e_2,\dots,e_n\} \setminus \Gamma_1$. We can represent Γ by the diagram:



If r is even and s is odd, then Γ_1 satisfies the conditions for the set K in Proposition 6.1 (that is, every point of Ω is joined to an even number of points of Γ_1), and if r and s are even then Γ_2 satisfies the conditions. Hence $\mathcal{L}' \subset S$ in both cases by Proposition 6.1.

THEOREM 6.3. Let G be the automorphism group of a nontrivial regular 2-graph (Ω, Δ) and suppose that the parameters r,s (as in Proposition 6.2) are not both odd. Then the heart of G acting on Ω, in characteristic 2, is reducible. In particular, if $n \equiv 0 \pmod 4$ then the heart is reducible.

PROOF. Now the complement $(\Omega, \Omega^{\{3\}} \setminus \Delta)$ is also a nontrivial regular 2-graph and a graph in the corresponding switching class with a point isolated is represented by the diagram:



Hence if r and s are not both odd then by Proposition 6.2, we have $\mathcal{L}' \subset S$ for either (Ω, Δ) or its complement $(\Omega, \Omega^{\{3\}} \setminus \Delta)$; and certainly $T \subset \mathcal{L}'$ for both these 2-graphs. The result follows (note that G is the automorphism group of both (Ω, Δ) and its complement).

REMARK. As is shown by Theorem 5.2 and the table on p.103, the known 2-transitive groups which act on a nontrivial regular 2-graph and have a reducible heart over GF(2) are listed in the following table:

Group G	Degree n	Regular 2-graph	r	s
some subgroups of $AGL(d,2)$ $(d \geq 2)$, eg. $G = T(V).Sp(2m,2)$	2^d	eg. $\Sigma(2m,2)$		
$Sp(2m,2)^+$ $(m \geq 2)$	$2^{m-1}(2^m+1)$	$\Omega^+(2m,2)$	$2^{2m-3}+2^{m-2}-1$	2^{2m-3}
$Sp(2m,2)^-$ $(m \geq 3)$	$2^{m-1}(2^m-1)$	$\Omega^-(2m,2)$	$2^{2m-3}-2^{m-2}-1$	2^{2m-3}
$P\Gamma L(2,q), q \equiv 1(8)$	$q+1$	$P(q)$	$\frac{1}{4}(q-1)$	$\frac{1}{4}(q-1)$
$P\Gamma U(3,q^2)$, q odd	q^3+1	$U(q)$	$\frac{1}{4}(q-1)(q^2+1)$	$\frac{1}{4}(q+1)(q^2-1)$
$Re(q), q = 3^{2k+1}$	q^3+1	$R(q)$	$\frac{1}{4}(q-1)(q^2+1)$	$\frac{1}{4}(q+1)(q^2-1)$
HS	176	H(176)	36	51
Co_3	276	C(276)	56	81

(in fact the reducibility of the heart over GF(2) for Co_3 was not proved by Mortimer).

Theorem 6.3 does indeed show the reducibility of the heart for all the groups in the above table.

"The eternal silence of these infinite spaces
terrifies me."

Blaise Pascal, 'Pensées'.

Chapter 7: LIE ALGEBRAS FROM 2-GRAPHS AND GRAPHS.

Let (Ω, Δ) be a nontrivial even 2-graph with $\Omega = \{e_1, \ldots, e_n\}$ (n even), F a field of characteristic 2 and $\mathcal{L} = F\Omega$ the algebra defined at the beginning of Chapter 6. In the first two sections of this chapter we consider the structure of the algebra $\mathcal{L}$ in greater detail. First we show that it is in fact a Lie algebra which is solvable of derived length at most 3. After this we examine the lower central series of $\mathcal{L}$ and consider this series for regular 2-graphs and other examples. In the final section we show how Lie algebras in other characteristics may be constructed from certain graphs.

1. SOME FACTS ABOUT $\mathcal{L}$.

THEOREM 7.1. Let $\mathcal{L}$ be as above. Then $\mathcal{L}$ is a Lie algebra.

PROOF. For each $i,j,k \in \{1,\ldots,n\}$ define a_{ijk} by

$$a_{ijk} = \begin{cases} 1 & \text{if } \{e_i, e_j, e_k\} \in \Delta \\ 0 & \text{otherwise} \end{cases}$$

Then $e_i e_j = \sum_{k=1}^{n} a_{ijk} e_k$, and

$$(e_i e_j) e_k + (e_j e_k) e_i + (e_k e_i) e_j = \sum_{m=1}^{n} \sum_{\ell=1}^{n} b_{ijk\ell m} e_m,$$

where $b_{ijk\ell m} = a_{ij\ell} a_{\ell km} + a_{jk\ell} a_{\ell im} + a_{ki\ell} a_{\ell jm}$; the result will follow if we show that $\sum_{\ell=1}^{n} b_{ijk\ell m}$ is even for every i,j,k,m.

Pick $i,j,k,m \in \{1,\ldots,n\}$. If i,j,k,m are not all distinct then it is easy to see that $b_{ijk\ell m}$ is even for all ℓ ; so suppose that i,j,k,m are distinct. Now (Ω, Δ) is a 2-graph, so $\{e_i, e_j, e_k, e_m\}$ contains 0,2 or 4 elements of Δ . We consider these possibilities separately.

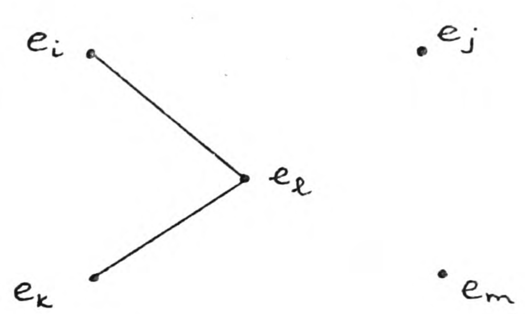
Case 1. $\{e_i, e_j, e_k, e_m\}$ contains no elements of Δ .

Recall (see Section 1 of Chapter 5) that the switching class of graphs corresponding to the 2-graph (Ω, Δ) consists of those graphs Γ on Ω for which

$$\Delta = \{ \{e_a, e_b, e_c\} \mid e_a, e_b, e_c \text{ have an odd number of edges between them in } \Gamma \}.$$

Thus in this case, the switching class corresponding to (Ω, Δ) contains a graph Γ whose subgraph on $\{e_i, e_j, e_k, e_m\}$ is:

For any $\ell \in \Omega$, it is easy to see that $b_{ijk\ell m}$ is 0 or 2. For instance, if the subgraph of Γ on $\{e_i, e_j, e_k, e_\ell, e_m\}$ is:

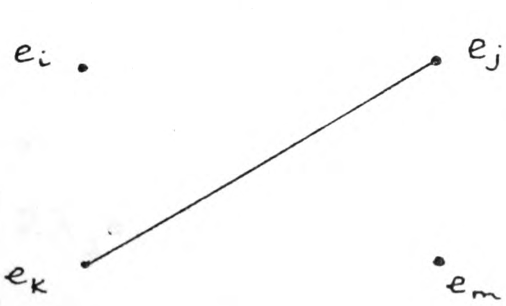


then $a_{ij\ell} = a_{im\ell} = a_{jk\ell} = a_{km\ell} = 1$, $a_{ki\ell} = a_{jm\ell} = 0$, so $b_{ijk\ell m} = 2$.

Hence $\sum_{\ell=1}^{n} b_{ijk\ell m}$ is even in case 1.

<u>Case 2. $\{e_i, e_j, e_k, e_m\}$ contains 2 elements of Δ.</u>

We can suppose that these elements of Δ are either $\{e_i, e_j, e_k\}$ and $\{e_j, e_k, e_m\}$ or $\{e_i, e_j, e_m\}$ and $\{e_j, e_k, e_m\}$. Suppose that they are $\{e_i, e_j, e_k\}$ and $\{e_j, e_k, e_m\}$; then the switching class corresponding to (Ω, Δ) contains a graph Γ whose subgraph on $\{e_i, e_j, e_k, e_m\}$ is:



For any $\ell \in \{1,\ldots,n\}$ it is easy to verify that $b_{ijk\ell m}$ is odd if and only if e_ℓ is joined in Γ to precisely one of e_i and e_m, that is, if and only if $\{e_i, e_m, e_\ell\} \in \Delta$. It follows that

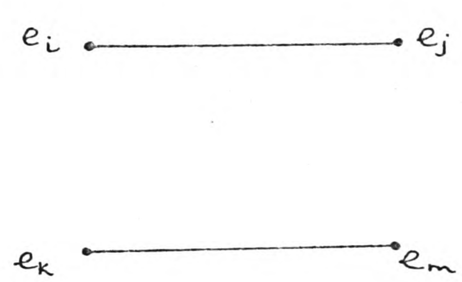
$$\sum_{\ell=1}^{n} b_{ijk\ell m} = \sum_{\ell=1}^{n} a_{im\ell}$$

which is even, since (Ω, Δ) is an even 2-graph.

Similar reasoning deals with the case when the elements of Δ contained in $\{e_i, e_j, e_k, e_m\}$ are $\{e_i, e_j, e_m\}$ and $\{e_j, e_k, e_m\}$.

<u>Case 3. $\{e_i, e_j, e_k, e_m\}$ contains 4 elements of Δ.</u>

The switching class corresponding to (Ω, Δ) contains a graph Γ whose subgraph on $\{e_i, e_j, e_k, e_m\}$ is:



Again, it is easy to show that $b_{ijk\ell m}$ is odd if and only if e_ℓ is joined in Γ to an even number of points of $\{e_i, e_j, e_k, e_m\}$, that is, if and only if both or neither of $\{e_j, e_k, e_\ell\}$ and $\{e_i, e_m, e_\ell\}$ are elements of Δ. Hence, if Φ_{jk}, Φ_{im} are the sets of elements of Δ containing $\{e_j, e_k\}$, $\{e_i, e_m\}$ respectively, then

$$\sum_{\ell=1}^{n} b_{ijk\ell m} \equiv n-4- |\Phi_{jk} \cup \Phi_{im}| + |\Phi_{jk} \cap \Phi_{im}| \pmod 2$$

$$\equiv n-4- |\Phi_{jk}| - |\Phi_{im}| + 2\,|\Phi_{jk} \cap \Phi_{im}| \pmod 2$$

which is congruent to $0 \pmod 2$ since (Ω, Δ) is an even 2-graph.

Hence $\sum_{\ell=1}^{n} b_{ijk\ell m}$ is even in every case, and the proof is complete.

As before, we define the subspaces S, T of $\mathcal{L}$ by

$$S = \{\Sigma\lambda_i e_i \mid \Sigma\lambda_i = 0\}, \quad T = \langle \sum_{1}^{n} e_i \rangle .$$

The derived series of the Lie algebra $\mathcal{L}$ has a simple form:

PROPOSITION 7.2. Let $\mathcal{L}$ be as above. Then $\mathcal{L}' \subseteq S$, $\mathcal{L}'' \subseteq T \subseteq \mathcal{C}$ (where $\mathcal{C}$ is the centre of $\mathcal{L}$) and $\mathcal{L}''' = 0$ (so $\mathcal{L}$ is solvable of derived length at most 3).

PROOF. It is clear that $\mathcal{L}' \subseteq S$ and that $T \subseteq \mathcal{C}$, so we have only to show that $\mathcal{L}'' \subseteq T$. Let $\{i,j,k,\ell\} \subseteq \{1,\ldots,n\}$ with $|\{i,j,k,\ell\}| \geq 3$ and consider the product $(e_i e_j)(e_k e_\ell)$. Now

$$(e_i e_j)(e_k e_\ell) = (\sum_{r=1}^{n} a_{ijr} e_r)(\sum_{s=1}^{n} a_{k\ell s} e_s)$$

$$= \sum_{r=1}^{n} a_{ijr} (\sum_{s,t=1}^{n} a_{k\ell s} a_{rst} e_t) .$$

Let x,y be the coefficients of e_1, e_2 respectively, in $(e_i e_j)(e_k e_\ell)$. Then if $V_{ij} = \{ m \mid \{e_i, e_j, e_m\} \in \Delta \}$, we have

$$x = \sum_{r \in V_{ij}} \sum_{s=1}^{n} a_{k\ell s} a_{1rs} = \sum_{r \in V_{ij}} \sum_{s \in V_{k\ell}} a_{1rs} ,$$

$$y = \sum_{r \in V_{ij}} \sum_{s \in V_{k\ell}} a_{2rs} .$$

Let Γ be a graph in the switching class corresponding to (Ω, Δ) and for $a = 1,2$, define

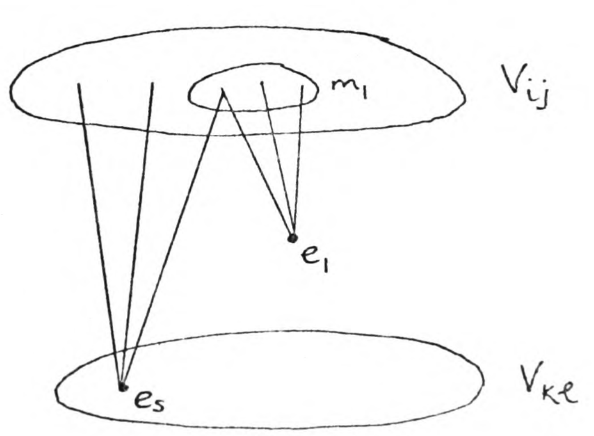
$$m_a = |\{ m \in V_{ij} \mid e_m \text{ joined to } e_a \text{ in } \Gamma \}| .$$

Also, let

$$R_1 = \{ m \in V_{k\ell} \mid e_m \text{ joined in } \Gamma \text{ to an even number of elements of } V_{ij} \} ,$$

$$R_2 = \{ m \in V_{k\ell} \mid e_m \text{ joined in } \Gamma \text{ to an odd number of elements of } V_{ij} \} .$$

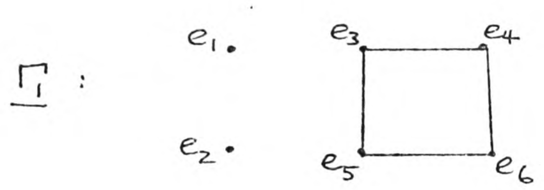
Now suppose that m_1 is odd and let $s \in V_{k\ell}$:

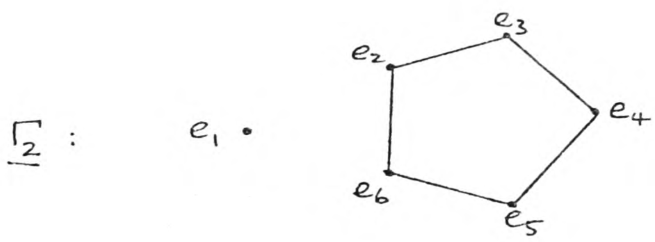


It is quite easy to see that $\sum_{r \in V_{ij}} a_{1rs}$ is odd if and only if $s \in R_1$. Hence $x = |R_1|$.

Similarly $x = |R_2|$ if m_1 is even; and if m_2 is odd then $y = |R_1|$, if m_2 is even then $y = |R_2|$. However, $|R_1| + |R_2| = |V_{k\ell}|$, which is even since (Ω, Δ) is an even 2-graph, so $|R_1| \equiv |R_2| \pmod 2$ and the coefficients x,y are equal. It follows that the coefficients of all e_m in $(e_ie_j)(e_ke_\ell)$ are equal, that is, $(e_ie_j)(e_ke_\ell) \in T$. Consequently $\mathcal{L}'' \subseteq T$.

EXAMPLES. Let Γ_1, Γ_2 be the graphs on 6 vertices below:





Both Γ_1 and Γ_2 give rise to even 2-graphs (Proposition 5.1); let $\mathcal{L}_1, \mathcal{L}_2$ respectively, be the corresponding Lie algebras of characteristic 2. We have

$$\mathcal{L}_1' = \langle e_1+e_2,\ e_3+e_6, e_4+e_5 \rangle, \quad \mathcal{L}_1'' = 0$$

and $\quad \mathcal{L}_2' = S, \quad \mathcal{L}_2'' = T.$

---

2. THE LOWER CENTRAL SERIES OF $\mathcal{L}$.

As in the previous section, let $\mathcal{L}$ be a Lie algebra over a field F of characteristic 2 constructed from a nontrivial even 2-graph. We now describe the terms $\mathcal{L}^t$ $(t \geq 2)$ of the lower central series of $\mathcal{L}$ in terms of the graphs in the switching class corresponding to (Ω, Δ), and use this description to examine the lower central series for regular 2-graphs and some other examples.

First we need a definition: if Γ is a graph and α, β are vertices of Γ, t a positive integer, then a path of length t in Γ from α to β is a sequence

$(\alpha_0, \alpha_1, \ldots, \alpha_t)$ such that $\alpha_0 = \alpha$, $\alpha_t = \beta$ and α_i is joined to α_{i+1} for $i = 0, \ldots, t-1$.

PROPOSITION 7.3. Let $\mathcal{L}$ be as above and let Γ be the graph in the switching class corresponding to (Ω, Δ) in which the point e_1 is isolated. For each integer $t \geq 1$ and each $i, j \in \{1, \ldots, n\}$, let $m_{ij}^{(t)}$ be the number of paths of length t in Γ from e_i to e_j. If $m_{ij}^{(t)}$ is even for all i,j then the $(t+1)$th term in the lower central series, $\mathcal{L}^{t+1}$, is zero. If not, there is a subset J^t of $\{e_2, \ldots, e_n\}$ such that

$$\{ \underbrace{e_1(e_1 \ldots (e_1}_{t} e_j) \ldots) \mid e_j \in J^t \} \cup \{ \sum_1^n e_k \}$$

is a basis for $\mathcal{L}^{t+1}$. Further, $\mathcal{L}^{t+1} \subset S$ if and only if there is a proper nonempty subset K of $\{e_2, \ldots, e_n\}$ such that $\sum_{e_k \in K} m_{ik}^{(t)}$ is even for all $i \in \{1, \ldots, n\}$, and $\mathcal{L}^{t+1} \subset \mathcal{L}^t$ if and only if there is such a subset K for which $\sum_{e_k \in K} m_{k\ell}^{(t-1)}$ is odd for some $\ell \in \{1, \ldots, n\}$.

PROOF. We first prove by induction on t $(t \geq 2)$ that for $i, j \in \{1, \ldots, n\}$,

$$e_i(\underbrace{e_1(e_1 \ldots (e_1}_{t-1} e_j) \ldots) = \begin{cases} \sum\limits_{m_{j\ell}^{(t)} \text{ even}} e_\ell & \text{if } m_{ij}^{(t)} \text{ is odd.} \\ \sum\limits_{m_{j\ell}^{(t)} \text{ odd}} e_\ell & \text{if } m_{ij}^{(t)} \text{ is even.} \end{cases}$$

This is easily verified for $t = 2$. Suppose that it is true for $t-1$, so that

$$\underbrace{e_1(e_1 \ldots (e_1}_{t-1} e_j) \ldots) = \sum_{m_{j\ell}^{(t-1)} \text{ odd}} e_\ell$$

for any j. Now the total number of paths of length $t-1$ emanating from e_j is even, since every vertex of Γ has even valency (Proposition 5.1); therefore the set $L = \{ e_\ell \in \Omega \mid m_{j\ell}^{(t-1)} \text{ is odd} \}$ has even size. Suppose that $m_{ij}^{(t)}$ is odd; then e_i is joined to an odd number of points of L. Hence for any $e_k \in \Omega$, e_k is involved in $e_i \sum_{\ell \in L} e_\ell$ if and only if e_k is joined in Γ to an even number of points of L, that is, if and only if $m_{jk}^{(t)}$ is even. Thus

$$e_i(\underbrace{e_1(e_1 \ldots (e_1}_{t-1} e_j) \ldots) = \sum_{m_{kj}^{(t)} \text{ even}} e_k .$$

Similarly, if $m_{ij}^{(t)}$ is even then $e_i(\underbrace{e_1(e_1\ldots(e_1}_{t-1}e_j)\ldots) = \sum_{m_{kj}^{(t)}\text{ odd}} e_k$, so our original assertion is proved by induction.

Suppose now that $m_{ij}^{(t)}$ is odd for some i,j $(t\geq 2)$. Then

$$e_i(\underbrace{e_1\ldots(e_1}_{t-1}e_j)\ldots) + e_1(\underbrace{e_1\ldots(e_1}_{t-1}e_j)\ldots) = \sum_1^n e_k$$

so that $\sum_1^n e_k \in \mathcal{L}^{t+1}$. Also, for each k,ℓ, $e_k(\underbrace{e_1\ldots(e_1}_{t-1}e_\ell)\ldots)$ is either $e_1(e_1\ldots(e_1e_\ell)\ldots)$ or $e_1(e_1\ldots(e_1e_\ell)\ldots) + \sum_1^n e_k$. The existence of the subset J^t of $\{e_2,\ldots,e_n\}$ required by the proposition, follows by induction on t (the case $t=1$ follows from Proposition 6.1).

If $m_{ij}^{(t)}$ is even for all i,j $(t\geq 1)$ then $e_i(\underbrace{e_1\ldots(e_1}_{t-1}e_j)\ldots) = 0$ for all i,j, so $\mathcal{L}^{t+1} = 0$.

Finally, it is clear that $\mathcal{L}^{t+1}\subset S$ $(t\geq 2)$ if and only if there is a proper nonempty subset K of $\{e_2,\ldots,e_n\}$ such that $\sum_{e_k\in K} e_1(\underbrace{e_1\ldots(e_1}_{t-1}e_k)\ldots) = 0$, that is, if and only if $\sum_{e_k\in K}\ \sum_{m_{k\ell}^{(t)}\text{ odd}} e_\ell = 0$, that is, if and only if $\sum_{e_k\in K} m_{k\ell}^{(t)}$ is even for all $\ell\in\{1,\ldots,n\}$ (the case $t=1$ follows again from Proposition 5.1). And $\mathcal{L}^{t+1}\subset \mathcal{L}^t$ if and only if there is such a subset K with $\sum_{e_k\in K} e_1(\underbrace{e_1\ldots(e_1}_{t-1}e_k)\ldots) \neq 0$, that is, if and only if there is such a subset K and $\ell\in\{1,\ldots,n\}$ such that $\sum_{e_k\in K} m_{k\ell}^{(t-1)}$ is odd.

We can use Proposition 7.3 to examine the Lie algebra $\mathcal{L}$ for regular 2-graphs:

<u>PROPOSITION 7.4.</u> Let $\mathcal{L}$ be the Lie algebra obtained as above from a nontrivial regular 2-graph (Ω,Δ) with parameters r,s as described in Section 1 of Chapter 5. Then

(i) if r is even and s is odd then $\mathcal{L}^3 = 0$,

(ii) if s is even then $\mathcal{L}^2 = \mathcal{L}^3$ $(=\mathcal{L}^4 = \ldots)$,

(iii) if r and s are odd then $\mathcal{L}$ is not nilpotent.

<u>PROOF.</u> Let Γ be the graph in the switching class corresponding to (Ω,Δ) in

which the vertex e_1 is isolated, so that the subgraph of Γ on $\{e_2,\dots,e_n\}$ is strongly regular with parameters r,s as described in Section 1 of Chapter 5. For any i,j we have (in the notation of Proposition 7.3)

$$m_{ij}^{(2)} = \begin{cases} 2r-s-1 & \text{if } e_i, e_j \text{ are joined in } \Gamma \\ r & \text{if } e_i, e_j \text{ are not joined in } \Gamma \text{ and } i \neq j \\ 2r & \text{if } i = j. \end{cases}$$

Consequently if r is even and s is odd then $m_{ij}^{(2)}$ is even for all i,j and so $\mathcal{L}^3 = 0$ by Proposition 7.3. This proves (i).

Now suppose that s is even and that $\mathcal{L}^3 \subset \mathcal{L}^2$. Then by Proposition 7.3 there is a proper subset K of $\{e_2,\dots,e_n\}$ such that $\sum_{e_k \in K} m_{ik}^{(2)}$ is even for all i and such that there exists $e_a \in \Omega$ with $\sum_{e_k \in K} m_{ak}^{(1)}$ odd, that is, with e_a joined in Γ to an odd number, say x, of points of K. Let $y = |K| - x$. Then

$$\sum_{e_k \in K} m_{ak}^{(2)} = \begin{cases} x(2r-s-1)+yr, & \text{if } e_a \notin K \\ x(2r-s-1)+(y+1)r, & \text{if } e_a \in K. \end{cases}$$

If r is even then $\sum_{e_k \in K} m_{ak}^{(2)}$ is odd (since x and 2r-s-1 are both odd), which is a contradiction. Hence $\mathcal{L}^2 = \mathcal{L}^3$ if r,s are even. If r is odd then 2r-s-1 and r are both odd; for each i, let x_i be the number of points of K which are joined in Γ to e_i. Then

$$\sum_{e_k \in K} m_{ik}^{(2)} = \begin{cases} x_i(2r-s-1) + (|K|-x_i)r, & \text{if } e_i \notin K \\ x_i(2r-s-1) + (|K|-x_i+1)r, & \text{if } e_i \in K \end{cases}$$

$$\equiv \begin{cases} |K| \pmod 2, & \text{if } e_i \notin K \\ |K|+1 \pmod 2, & \text{if } e_i \in K \end{cases}$$

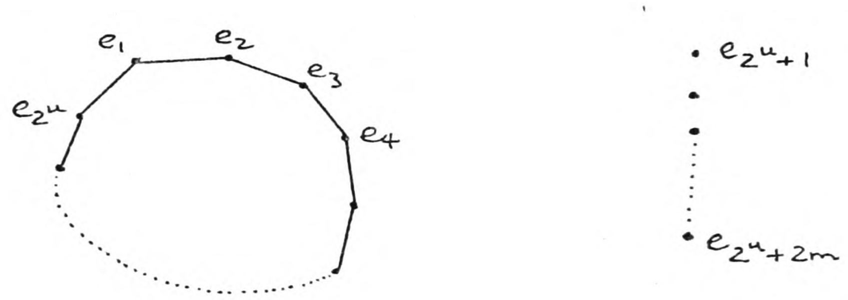
so that $\sum_{e_k \in K} m_{ik}^{(2)}$ is not even for all i, which is a contradiction. It follows that $\mathcal{L}^2 = \mathcal{L}^3$ if r is odd and s is even; hence $\mathcal{L}^2 = \mathcal{L}^3$ if s is even and (ii) is proved.

Finally, suppose that r,s are both odd and that $\mathcal{L}$ is nilpotent, so that there is an integer $t \geq 2$ with $\mathcal{L}^{t+1} = 0$. For each positive integer u, denote by $m_1^{(u)}$, $m_0^{(u)}$ the number of paths of length u in Γ between, respectively, two joined points, two distinct non-joined points in $\{e_2,\ldots,e_n\}$. Then

$$m_1^{(u+1)} = sm_0^{(u)} + (2r-s-1)m_1^{(u)} + m_{jj}^{(u)} \quad (\text{any } j \geq 2),$$
$$m_0^{(u+1)} = rm_0^{(u)} + rm_1^{(u)} \quad ,$$
$$m_{jj}^{(u+1)} = 2rm_1^{(u)} .$$

Consequently $m_1^{(u+1)} \equiv m_0^{(u)} \pmod 2$ and $m_0^{(u+1)} \equiv m_0^{(u)} + m_1^{(u)} \pmod 2$ and so by induction on u, one of $m_0^{(u)}$ and $m_1^{(u)}$ is odd for all $u \geq 1$ (for u = 1 this is obvious). But $\mathcal{L}^{t+1} = 0$, so $m_0^{(t)}$,$m_1^{(t)}$ are both even by Proposition 7.3, which is a contradiction. Hence $\mathcal{L}$ is not nilpotent if r,s are odd, and (iii) is proved.

We conclude this section with some examples of 2-graphs for which $\mathcal{L}$ is nilpotent. For each $m \geq 1$, $u \geq 2$ let $\Gamma_{m,u}$ be the graph on $2m+2^u$ vertices made up of 2m isolated points and a 2^u-gon:



If (Ω,Δ) is the corresponding 2-graph then (Ω,Δ) is nontrivial and even (Proposition 5.1). Denote the corresponding Lie algebra by $\mathcal{L}_{m,u}$.

<u>PROPOSITION 7.5.</u> We have $\mathcal{L}_{m,u}^{2^{u-1}} \neq 0$, $\mathcal{L}_{m,u}^{2^{u-1}+1} = 0$, that is, $\mathcal{L}_{m,u}$ is nilpotent of class 2^{u-1}.

<u>PROOF.</u> The proof goes by induction on u. The result is true for u = 2 by Proposition 7.3, since in the 4-gon $m_{ij}^{(2)}$ is even for all i,j. Suppose it is true for u-1, so that $\mathcal{L}_{m,u-1}^{2^{u-2}+1} = 0$, that is, $m_{yz}^{(2^{u-2})}$ is even for all e_y,e_z

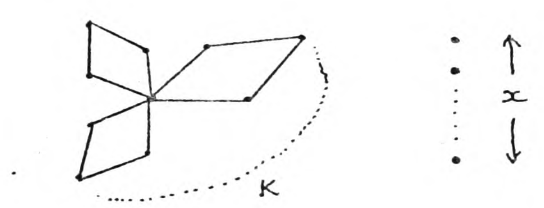
in $\Gamma_{m,u-1}$. It follows that $m_{yz}^{(2^{u-2})}$ is even for all e_y, e_z in $\Gamma_{m,u}$ unless $d(e_y, e_z) = 2^{u-2}$ (where $d(e_y, e_z)$ is the length of the shortest path in $\Gamma_{m,u}$ from e_y to e_z). Now pick $x \in \{1, 2, \ldots, 2^{u-1}+1\}$. Then in $\Gamma_{m,u}$,

$$m_{1x}^{(2^{u-1})} = \sum_{e_y \in \Gamma_{m,u}} m_{1y}^{(2^{u-2})} m_{yx}^{(2^{u-2})} .$$

For any $e_y \in \Gamma_{m,u}$, the product $m_{1y}^{(2^{u-2})} m_{yx}^{(2^{u-2})}$ is odd if and only if $d(e_1, e_y) = d(e_y, e_x) = 2^{u-2}$ which can occur if and only if x is 1 or $2^{u-1}+1$. However, it is clear that $m_{11}^{(2^{u-1})}$ and $m_{1\,2^{u-1}+1}^{(2^{u-1})}$ are both even, so we have shown that $m_{1x}^{(2^{u-1})}$ is even for all x. By Proposition 7.3 it follows that $\mathcal{L}_{m,u}^{2^{u-1}+1} = 0$. Also $m_{1\,2^{u-1}}^{(2^{u-1}-1)} = 1$, so $\mathcal{L}_{m,u}^{2^{u-1}} \neq 0$. The result is now proved by induction.

Examples of graphs which gives rise to even 2-graphs for which $\mathcal{L}^3 \neq 0$, $\mathcal{L}^4 = 0$ are:

(i)



(a graph on 3k+x+1 (even) points with x (≥ 1) isolated points and k quadrilaterals emanating from a single point)

(ii) graphs on m+x (m,x odd) points with x (≥ 1) isolated points and the rest forming a complete graph K_m.

---

3. LIE ALGEBRAS IN OTHER CHARACTERISTICS.

In this final section we show how to construct Lie algebras in all characteristics from certain graphs and investigate these algebras in similar fashion to Section 2 of this chapter.

PROPOSITION 7.6. Let Γ be a (simple, undirected) graph on a set $\Omega = \{e_1,\dots,e_n\}$ and for each i, let

$$V_i = \{e_j \mid e_j \text{ joined to } e_i \text{ in } \Gamma\}.$$

Suppose that F is a field in which $|V_i| = |V_j|$ for all i,j, and make $\mathcal{U} = F\Omega$ into an algebra by defining

$$e_ie_j = \sum_{e_k\in V_i} e_k - \sum_{e_m\in V_j} e_m$$

and extending linearly. Then $\mathcal{U}$ is a Lie algebra; further, $\mathcal{U}' \subseteq S$ and $\mathcal{U}'' = 0$.

PROOF. Certainly $e_i^2 = 0$ for all i, so we have only to verify the Jacobi identity. Let e_i, e_j, e_k be distinct points of Ω and let $e_m \in \Omega$. As before, denote by $m_{ij}^{(2)}$ the number of paths of length 2 in Γ from e_i to e_j. Then the coefficient of e_m in $(e_ie_j)e_k$ is

$$\begin{cases} |V_j| - m_{mj}^{(2)} - |V_i| + m_{mi}^{(2)}, & \text{if } e_m \text{ is joined to } e_k \\ m_{mi}^{(2)} - m_{mj}^{(2)}, & \text{if } e_m \text{ is not joined to } e_k. \end{cases}$$

Hence the coefficient of e_m in $(e_ie_j)e_k + (e_je_k)e_i + (e_ke_i)e_j$ is

$$\begin{cases} m_{mi}^{(2)} - m_{mj}^{(2)} + m_{mj}^{(2)} - m_{mk}^{(2)} + m_{mk}^{(2)} - m_{mi}^{(2)}, & \text{if } e_m \text{ is joined to none of } e_i, e_j, e_k \\ m_{mi}^{(2)} - m_{mj}^{(2)} + |V_k| - m_{mk}^{(2)} - |V_j| + m_{mj}^{(2)} + m_{mk}^{(2)} - m_{mi}^{(2)}, & \text{if } e_m \text{ is joined to } e_i, \text{ not } e_j \text{ or } e_k \\ m_{mi}^{(2)} - m_{mj}^{(2)} + |V_k| - m_{mk}^{(2)} - |V_j| + m_{mj}^{(2)} + |V_i| - m_{mi}^{(2)} - |V_k| + m_{mk}^{(2)}, & e_m \text{ joined to } e_i, e_j, \text{ not } e_k \\ |V_j| - m_{mj}^{(2)} - |V_i| + m_{mi}^{(2)} + |V_k| - m_{mk}^{(2)} - |V_j| + m_{mj}^{(2)} + |V_i| - m_{mi}^{(2)} - |V_k| + m_{mk}^{(2)}, & e_m \text{ joined to } e_i, e_j, e_k. \end{cases}$$

In every case this coefficient is zero in F, so $(e_ie_j)e_k + (e_je_k)e_i + (e_ke_i)e_j = 0$ and the Jacobi identity holds; hence $\mathcal{U}$ is a Lie algebra.

Clearly $\mathcal{U}' \subseteq S$. Let $i,j,k,\ell,m \in \{1,\dots,n\}$; the coefficient of e_m in the product $(e_ie_j)(e_ke_\ell)$ is

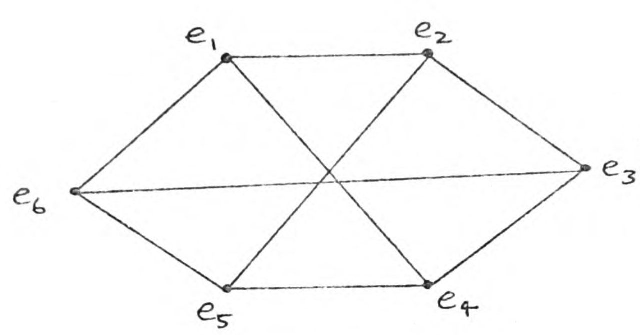
$$m_{mi}^{(2)}(|V_k| - m_{mk}^{(2)}) - m_{mi}^{(2)}(|V_\ell| - m_{m\ell}^{(2)}) + m_{mj}^{(2)}(|V_\ell| - m_{m\ell}^{(2)}) - m_{mj}^{(2)}(|V_k| - m_{mk}^{(2)})$$
$$+ m_{mk}^{(2)}(|V_j| - m_{mj}^{(2)}) - m_{mk}^{(2)}(|V_i| - m_{mi}^{(2)}) + m_{m\ell}^{(2)}(|V_i| - m_{mi}^{(2)}) - m_{m\ell}^{(2)}(|V_j| - m_{mj}^{(2)})$$

which is equal to

$$(m^{(2)}_{mi} - m^{(2)}_{mj})(|V_k| - m^{(2)}_{mk} - |V_\ell| + m^{(2)}_{m\ell}) + (m^{(2)}_{mk} - m^{(2)}_{m\ell})(|V_j| - m^{(2)}_{mj} - |V_i| + m^{(2)}_{mi})$$

which is zero in the field F. Hence $\mathcal{U}'' = 0$.

EXAMPLE. Let Γ be the graph on 6 vertices below:



Now Γ is regular of valency 3; let $\mathcal{U}$ be a Lie algebra (in any characteristic) obtained from Γ as in Proposition 7.6. Then $\mathcal{U}'$ is the 1-dimensional subspace of $\mathcal{U}$ spanned by $e_1+e_3+e_5-e_2-e_4-e_6$. The 2-graph (Ω, Δ) corresponding to Γ has $\Delta = \emptyset$, so its automorphism group is S_6; and $\mathcal{U}'$ is not an S_6-submodule of $\mathcal{U}$.

In general, therefore, if $\mathcal{U}$ is a Lie algebra obtained from a graph Γ as in Proposition 7.6, the characteristic subalgebras of $\mathcal{U}$ (for instance $\mathcal{U}'$, $\mathcal{U}^{(k)}$, $\mathcal{U}^k$) need not be G-submodules of $\mathcal{U}$, where G is the automorphism group of the corresponding 2-graph; also $\mathcal{U}$ itself need not be G-invariant as an algebra (that is, G need not act on $\mathcal{U}$ as algebra automorphisms). This is in contrast with the Lie algebra $\mathcal{L}$ in characteristic 2 defined from an even 2-graph as in Chapter 6.

The lower central series of a Lie algebra $\mathcal{U}$ obtained as in Proposition 7.6 can be analysed in similar fashion to Proposition 7.3:

PROPOSITION 7.7. Let $\mathcal{U}$ be a Lie algebra obtained from a graph Γ on $\Omega = \{e_1, \ldots, e_n\}$ as in Proposition 7.6. Then for each $t \geq 2$ and each i, j,

$$e_i(\underbrace{e_1(e_1\dots(e_1}_{t-1}e_j)\dots) = \sum_{k=1}^{n} (m_{kj}^{(t)} - m_{k1}^{(t)})(-1)^t e_k .$$

For $t \geq 2$, if $m_{kj}^{(t)} = m_{k1}^{(t)}$ in the field F for all j,k, then $\mathcal{U}^{t+1} = 0$. If not, there is a subset J_t of $\{e_2, \dots, e_n\}$ such that

$$\{ e_1(e_1\dots(e_1e_j)\dots) \mid e_j \in J_t \}$$

is a basis for $\mathcal{U}^{t+1}$.

PROOF. We first prove by induction on t (≥ 2) that

$$e_i(\underbrace{e_1\dots(e_1}_{t-1}e_j)\dots) = \sum_{k=1}^{n} (m_{kj}^{(t)} - m_{k1}^{(t)})(-1)^t e_k .$$

For t = 2, consider $e_i(e_1e_j)$; the coefficient of e_k in this is

$$\begin{cases} |V_1| - m_{k1}^{(2)} - |V_j| + m_{kj}^{(2)} , & \text{if } e_i \in V_k \\ m_{kj}^{(2)} - m_{k1}^{(2)} , & \text{if } e_i \notin V_k , \end{cases}$$

so that $e_i(e_1e_j) = \sum_{k=1}^{n} (m_{kj}^{(2)} - m_{k1}^{(2)})e_k$, as required. Now suppose that our assertion is true for t-1 ($t \geq 3$) and consider $e_i(\underbrace{e_1\dots(e_1}_{t-1}e_j)\dots)$; this is equal to $\sum_{e_k \in V_1} e_i(\underbrace{e_1\dots(e_1}_{t-2}e_k)\dots) - \sum_{e_\ell \in V_j} e_i(\underbrace{e_1\dots(e_1}_{t-2}e_\ell)\dots)$ which, by induction hypothesis, is

$$\sum_{e_k \in V_1} \sum_{k'=1}^{n} (-1)^{t-1}(m_{k'k}^{(t-1)} - m_{k'1}^{(t-1)})e_{k'} - \sum_{e_\ell \in V_j} \sum_{\ell'=1}^{n} (m_{\ell'\ell}^{(t-1)} - m_{\ell'1}^{(t-1)})(-1)^{t-1} e_{\ell'} .$$

The coefficient of $e_{k'}$ in this is

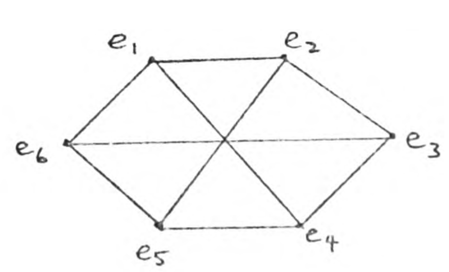
$$\sum_{e_k \in V_1} (-1)^{t-1}(m_{k'k}^{(t-1)} - m_{k'1}^{(t-1)}) - \sum_{e_\ell \in V_j} (-1)^{t-1}(m_{k'\ell}^{(t-1)} - m_{k'1}^{(t-1)})$$

which is equal to

$$(-1)^{t-1}(m_{k'1}^{(t-1)}(|V_j| - |V_1|) + m_{k'1}^{(t)} - m_{k'j}^{(t)}) = (-1)^t(m_{k'j}^{(t)} - m_{k'1}^{(t)}) .$$

Hence $e_i(\underbrace{e_1\dots(e_1}_{t-1}e_j)\dots) = \sum_{k=1}^{n} (m_{kj}^{(t)} - m_{k1}^{(t)})(-1)^t e_k$, as required, and our assertion is proved by induction. The rest of the proposition follows.

EXAMPLE. Let Γ be the graph



(as in the example on p.120), and let $\mathcal{U}$ be a Lie algebra in some characteristic obtained from Γ as in Proposition 7.6. If $\mathcal{C}$ is the centre of $\mathcal{U}$, we have

$$\mathcal{U}' = \langle e_1+e_3+e_5-e_2-e_4-e_6 \rangle,$$

$$\mathcal{C} = \langle e_1-e_3,\ e_1-e_5,\ e_2-e_4,\ e_2-e_6 \rangle .$$

If the characteristic is 3 then $\mathcal{U}^3 = 0$, whereas if it is not 3 then $\mathcal{U}^2 \neq 0$ and $\mathcal{U}^2 = \mathcal{U}^3 = \ldots$.

We conclude with a result on the Lie algebras in characteristic zero obtained from (regular) graphs as in Proposition 7.6. A graph is said to be <u>non-null</u> if it has at least one edge.

<u>PROPOSITION 7.8.</u> Let $\mathcal{U}$ be a Lie algebra in characteristic zero obtained from a non-null regular graph Γ as in Proposition 7.6. Then $\mathcal{U}$ is not nilpotent.

<u>PROOF.</u> We use the notation of Section 4 of Chapter 5. Now F certainly has a subfield isomorphic to $\mathbb{Q}$; denote by $\mathcal{U}_{\mathbb{Q}}$ the $\mathbb{Q}$-span of $\{e_1,\ldots,e_n\}$, so that $\mathcal{U}_{\mathbb{Q}}$ is certainly a Lie algebra (since $e_ie_j \in \mathcal{U}_{\mathbb{Q}}$). As in Section 4 of Chapter 5, let $\mathcal{U}_{\mathbb{C}} = \mathcal{U}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C}$; then $\mathcal{U}_{\mathbb{C}}$ is an n-dimensional Lie algebra over $\mathbb{C}$. Now $\mathcal{U}_{\mathbb{C}}$ has a natural inner product

$$\left(\sum_1^n \alpha_i e_i,\ \sum_1^n \beta_j e_j \right) = \sum_1^n \alpha_i \bar{\beta}_i .$$

Let $v = \sum_1^n e_i$. It is easy to see that, for any j,k,

$$(ve_j, e_k) = (e_j, ve_k) = \begin{cases} |V_k| , & \text{if } e_j \notin V_k \\ |V_k| - n , & \text{if } e_j \in V_k \end{cases}$$

since $|V_k| = |V_j|$. Hence the linear transformation $x \to vx$ $(x \in \mathcal{U}_{\mathbb{C}})$ is self-adjoint and so by the Spectral Theorem, there is a basis $\{x_1,\ldots,x_n\}$ of $\mathcal{U}_{\mathbb{C}}$ such that $vx_i = \lambda_i x_i$ for some $\lambda_i \in \mathbb{C}$ $(i = 1,\ldots,n)$. Since v is not in the centre of $\mathcal{U}$ (Γ is not the null graph) there exists i for which $\lambda_i \neq 0$.

Then

$$\underbrace{v(v\ldots(v}_{t}x_i)\ldots) = \lambda_i^t\, x_i$$

which is nonzero for all t. Hence $\mathcal{U}_{\mathbb{C}}$ is not nilpotent and so $\mathcal{U}$ itself is not nilpotent (see Section 4 of Chapter 5).

Appendix: THE PROOF OF COROLLARY 3.2.

In this appendix we prove

COROLLARY 3.2. Let G be an insoluble, transitive permutation group of degree p, where $p = 4q+1 = 3r+2 = 2s+3$ and p,q,r,s are all prime. Then G contains the alternating group A_p.

Two lemmas are required for the proof; the first is an easy generalisation of Lemma 1 of [2], and the second is the lemma on p.464 of [30].

LEMMA A.1. Let X be a k-transitive group on a set Ω of size n, let $\{\alpha_1,\ldots,\alpha_k\} \in \Omega^{\{k\}}$ and let K be a weakly closed subgroup of $X_{\alpha_1\ldots\alpha_k}$. Write $\Delta = \mathrm{fix}\,K$, $m = |\Delta|$ and let $\mathcal{B} = \{\Delta x \mid x \in X\}$. Then $\mathcal{B}$ is the set of blocks of a Steiner system $\mathcal{S}(k,m,n)$.

LEMMA A.2. Let X be a k-transitive group on a set Ω of size n and let Γ be a subset of Ω with $|\Gamma| = m$ and $k < m < n$. Let $\mathcal{B} = \{\Gamma x \mid x \in X\}$. Then $\mathcal{B}$ is the set of blocks of a Steiner system $\mathcal{S}(k,m,n)$ if and only if

(i) $X_{\{\Gamma\}}^{\Gamma}$ is k-transitive, and

(ii) for some Δ in $\Gamma^{\{k\}}$ we have $X_{(\Delta)} \leq X_{\{\Gamma\}}$.

We also need a result of Neumann (Theorem 10 of [31]).

THEOREM A.3. A simply primitive group of degree $3r$, where r is prime, can exist only if either

(i) $r = 192a^2 + 60a + 5$, or

(ii) $r = 3a^2 + 3a + 1$

for some integer a.

PROOF OF COROLLARY 3.2.

Let G be an insoluble, transitive group on Ω of degree p, where $p = 4q+1 = 3r+2 = 2s+3$ and p,q,r,s are prime. By Theorem 3.1, G is 3-transitive so for distinct $\alpha,\beta \in \Omega$, $G_{\alpha\beta}$ is transitive of degree $3r$ on $\Omega\setminus\{\alpha,\beta\}$. Also G is not sharply 3-transitive since it is not of degree t^a+1 for any prime number t (see 5.1 and 11.3 of [40]). We complete the proof in two steps:

STEP 1. $G_{\alpha\beta}$ is primitive on $\Omega\setminus\{\alpha,\beta\}$.

First we show that for any nontrivial weakly closed subgroup K of $G_{\alpha\beta\gamma}$ ($\gamma \in \Omega\setminus\{\alpha,\beta\}$), $|\mathrm{fix}\, K|$ is 3. For suppose that $|\mathrm{fix}\, K| = m > 3$. Then by Lemma A.1, we have a Steiner system $\mathcal{S}(3,m,p)$. If b is the number of blocks, then

$$bm(m-1)(m-2) = p(p-1)(p-2) = p(4q)(3r)$$

which is impossible since $p > m > 3$. Hence $|\mathrm{fix}\, K| = 3$. In particular $|\mathrm{fix}\, G_{\alpha\beta\gamma}| = 3$ since G is not sharply 3-transitive.

Now suppose that $G_{\alpha\beta}$ is imprimitive on $\Omega\setminus\{\alpha,\beta\}$. If it has 3 blocks of size r then the argument of Case 2 on p.274 of [2] (with the group G of [2] replaced by our G_α) gives a contradiction. Hence $G_{\alpha\beta}$ has r blocks of size 3. Let $\Delta_1 = \{\gamma,\delta,\varepsilon\}$ be a block. By the argument of Case 1 on p.274 of [2], we have $G_{\alpha\{\beta\gamma\}} = G_{\alpha\{\delta\varepsilon\}}$. Similarly $G_{\beta\{\alpha\gamma\}} = G_{\beta\{\delta\varepsilon\}}$. Thus if $\Gamma = \{\alpha,\beta,\gamma,\delta,\varepsilon\}$ then $G^{\Gamma}_{\{\Gamma\}}$ is transitive, hence 3-transitive; and clearly $G_{\alpha\beta\gamma} \leq G_{\{\Gamma\}}$, so by Lemma A.2 we have a Steiner system $\mathcal{S}(3,5,p)$. The above calculation shows that this cannot be so. Hence $G_{\alpha\beta}$ is primitive.

STEP 2. G is 4-transitive.

Now $G_{\alpha\beta}$ is primitive of degree $3r$, so if G is not 4-transitive then by Theorem A.3, there is an integer a such that either $r = 3a^2+3a+1$ or

$r = 192a^2 + 60a + 5$. If $r = 3a^2 + 3a + 1$ then $2s = 3r-1 = 9a^2 + 9a + 2 = (3a+1)(3a+2)$ which is not possible. If $r = 192a^2 + 60a + 5$ then $2s = 576a^2 + 180a + 14$, so $s = 288a^2 + 90a + 7 = (48a+7)(6a+1)$, which again cannot be so, unless $a = 0$ and $s = 7$. But then $q = 4$ which is not prime. Hence G is 4-transitive.

Now we can easily complete the proof; for G is 4-transitive and hence contains an element of order s. Theorem 1.26 now tells us that G must contain the alternating group A_p.

REFERENCES.

1. K.I.Appel and E.T.Parker, "On unsolvable groups of degree p = 4q+1, p and q primes", Can. J. Math. 19(1967), 583-589.
2. M.D.Atkinson, "Two theorems on doubly transitive permutation groups", J. London Math. Soc.(2), 6(1973), 269-274.
3. H.Bender, "Endliche zweifach transitive Permutationsgruppen, deren Involutionen keine Fixpunkte haben", Math. Z. 104(1968), 175-204.
4. R.Brauer, "On groups whose order contains a prime number to the first power, I and II", Amer. J. Math. 64(1942), 401-440.
5. P.J.Cameron, "Bounding the rank of certain permutation groups", Math. Z. 124(1972), 343-352.
6. R.W.Carter, 'Simple groups of Lie type', Wiley (Interscience), London, 1972.
7. J.H.Conway, "Three lectures on exceptional groups", Chapter VII of 'Finite Simple Groups', edited by M.B.Powell and G.Higman, Academic Press, 1971.
8. D.Cooper, "Primitive permutation groups of degree 4p", D.Phil. Thesis, Oxford, 1976.
9. C.W.Curtis and I.Reiner, 'Representation theory of finite groups and associative algebras', Wiley (Interscience), New York, 1962.
10. L.E.Dickson, 'Linear groups with an exposition of the Galois field theory', Dover, 1958.
11. W.Feit, "Groups with a cyclic Sylow subgroup", Nagoya Math. J. 27(1966), 571-584.
12. J.S.Frame, "The double cosets of a finite group", Bull. Amer. Math. Soc. 47(1941), 458-467.

13. J.A.Green, "A transfer theorem for modular representations", J. Algebra 1(1964), 73-84.

14. J.A.Green, "Walking around the Brauer tree", J. Austral. Math. Soc. 17(1974), 197-213.

15. D.Harries and H.Liebeck, "Isomorphisms in switching classes of graphs", J. Austral. Math. Soc. 26(1978), 475-487.

16. G.Higman, "On the simple group of D.G.Higman and C.C.Sims", Ill. J. Math. 13(1969), 74-84.

17. W.C.Huffman and D.B.Wales, "Linear groups containing an involution with two eigenvalues -1", J. Algebra 45(1977), 465-515.

18. B.Huppert, 'Endliche Gruppen I', Springer-Verlag, Berlin, 1967.

19. N.Ito, "Transitive permutation groups of degree p = 2q+1, p and q being prime numbers, II", Trans. Amer. Math. Soc. 113(1964), 454-487.

20. N.Ito, "Transitive permutation groups of degree p = 2q+1, p and q being prime numbers, III", Trans. Amer. Math. Soc. 116(1965), 151-166.

21. N.Ito, "Zur Theorie der Permutationsgruppen von Grad p", Math. Z. 74(1960), 299-301.

22. N.Jacobson, 'Lie algebras', Wiley (Interscience), New York, 1962.

23. W.M.Kantor, "k-homogeneous groups", Math. Z. 124(1972), 261-265.

24. M.Klemm, "Primitive Permutationsgruppen von Primzahlpotenzgrad", Comm. Alg. 5(1977), 193-205.

25. E.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) (2^{e} série), 6(1861), 241-323.

26. B.Mortimer, "The modular permutation representations of the known doubly transitive groups", to appear.

27. P.M.Neumann, "Transitive permutation groups of prime degree", J. London Math. Soc. (2), 5(1972), 202-208.

28. P.M.Neumann, "Transitive permutation groups of prime degree, III: character theoretic observations", Proc. London Math. Soc. (3), 31(1975), 482-494.

29. P.M.Neumann, "Transitive permutation groups of prime degree, IV: a problem of Mathieu and a theorem of Ito", Proc. London Math. Soc. (3), 32(1976), 52-62.

30. P.M.Neumann, "Generosity and characters of multiply transitive permutation groups", Proc. London Math. Soc. (3), 31(1975), 457-481.

31. P.M.Neumann, "Finite permutation groups, edge-coloured graphs and matrices", Chapter 5 of 'Topics in group theory and computation', London, Academic Press, 1977.

32. P.M.Neumann, 'Permutationsgruppen von Primzahlgrad und verwandte Themen', Lecture Notes, Mathematisches Institut, Giessen.

33. P.M.Neumann and J.Saxl, "The primitive permutation groups of some special degrees", Math. Z. 146(1976), 101-104.

34. B.Rothschild, "Degrees of irreducible modular characters of blocks with cyclic defect groups", Bull. Amer. Math. Soc. 73(1967), 102-104.

35. P.Rowlinson, "Some problems in the theory of finite groups", D.Phil. Thesis, Oxford, 1969.

36. J.J.Seidel, "A survey of two-graphs", in 'Colloquio internazionale sulle teorie combinatorie' (Roma, 1973).

37. C.C.Sims, "Computational methods in the study of permutation groups", pp.169-185 of 'Computational problems in abstract algebra', edited by J.Leech, Pergamon Press, 1970.

38. D.E.Taylor, "Some topics in the theory of finite groups", D.Phil. Thesis, Oxford, 1971.

39. H.F.Tuan, "On groups whose order contains a prime number to the first power", Ann. Math. (2), 45(1) (1944), 110-140.

40. H.Wielandt, 'Finite permutation groups', Academic Press, New York, 1964.

"We're home and dry."

Margaret Thatcher.