SOME PROBLEMS IN THE THEORY OF GROUPS

by

T.P. McDONOUGH

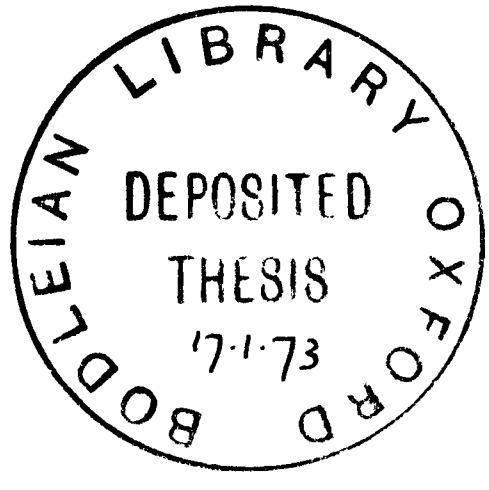
A Thesis submitted for

The Degree of Doctor of Philosophy

at

The University of Oxford

1972.



Abstract

This work is divided into three parts, all of which are concerned with the characterisation of certain families of classical groups as doubly transitive permutation groups satisfying certain extra hypotheses.

The first part is purely expository. It culminates in the characterisation - due to Marggraf - of the affine groups over GF(2).

The second part deals with a characterisation of certain collineation groups of projective spaces as Jordan groups which admit a Jordan set of prime power cardinality and which have extra restrictions on some Sylow subgroups.

The third part consists of results obtained while attempting to establish that insoluble groups of prime degree p (>7), whose Sylow p-subgroups have index 3 in their normalisers, are of the form PSL(3,q), for suitable prime powers q.

§1. Introduction.

This work is divided into three parts, all of which are concerned with the characterisation of certain families of classical groups.

The first part is an exposition of some theorems of Jordan [8] and Marggraf [10] concerning an arbitrary permutation group G on a set Ω, which satisfies the condition

(1.1) G has a subgroup H, which has exactly one non-trivial orbit Γ, where Γ is a proper subset of Ω. Jordan showed that a group satisfying (1.1), which is primitive on Ω, is 2-transitive on Ω; and further, that it is $(|\Omega - \Gamma| + 1)$-transitive on Ω if H is primitive on Γ. If G is a group satisfying (1.1) we say that G admits the Jordan set Γ; and if G is not $(|\Omega-\Gamma| + 1)$-transitive on Ω, we say that Γ is a non-trivial Jordan set - otherwise, the Jordan set Γ is trivial. A primitive permutation group which admits a non-trivial Jordan set will be called a Jordan group. Marggraf then asserts that if G is a Jordan group on Ω admitting a Jordan set Γ for which $|\Gamma| \leq \frac{1}{2}|\Omega|$, then $|\Omega| = 2|\Gamma|$, Ω has the structure of an affine space over GF(2) and G is the full collineation group.

The known Jordan groups are: (i) Subgroups of the full collineation groups of affine and projective spaces of dimension at least 2, which contain all elations, (the case of the affine plane over GF(2) is excluded); (ii) Alt(7) in its representation of degree 15; (iii) the Mathieu groups M_{22}, M_{23} and M_{24} in their usual representations; (iv) $\mathrm{Aut}(M_{22})$ in its representation of degree 22.

It is clear from the work of Jordan that every Jordan group is

a repeated transitive extension of a strictly 2-transitive group (i.e. 2-transitive but not 3-transitive). The second part is an attempt to characterise the subgroups of the collineation groups of projective spaces of dimension at least 2, which contain all elations, as the only strictly 2-transitive Jordan groups admitting a Jordan set of prime-power length. We prove this under certain extra restrictions.

The third part concerns insoluble groups G of prime degree p, in which a Sylow p-subgroup has index 3 in its normaliser. The known groups of this type are (i) Alt(7), and (ii) PSL(3,q), where $p=1+q+q^2$, acting on the points of the Desarguesian projective plane over GF(q). The main results of this part are: (i) If $\chi^{[p-2,1^2]}_G$ is an irreducible character of G, then p=7 and G=Alt(7); (ii) p=6q+1, where q is a prime, then G=Alt(7) or PSL(3,q), q=2,3 or 5; (iii) If $p=1+q+q^2$, where q is a prime and q^2 divides |G|, then G= Alt(7) or PSL(3,q).

The author is indebted to Professor G. Higman and Dr. P.M. Neumann for the many helpful suggestions they have made during the course of these researches.

The suggestion to include the classical theorems of Jordan and Marggraf, and many of the details of the proofs of these theorems are due to Professor Higman. A large part of the proof of Tsuzuku's result (14.1) (i) which is used is due to him also.

Dr. Neumann has pursued independently the problem considered in the third part, and has obtained many of the results of that part, including an elegant generalisation of (12.10). He has brought to the attention of the author, in connection with (12.9), that the work of A. Baker [15] implies that, for each integer k(≠0 or 1), the integral

solutions of the equation

(1.2) $(x-1)\{kx+1\}\{(k-1)x+3\} = y^2$

satisfy the inequality

(1.3) $\mathrm{Max}(|x|,|y|) < \exp\{(10^6\ell)^{10^6}\}$

where $\ell = \max\{|k(k-1)|,|k^2-5k+1|,4|k-1|,3\}$; and hence there are always only finitely many solutions of (1.2) in integers. He has also indicated that, in the notation of (17.2), $C_G(S_i) = S_i$ for $i=2,\ldots,q$. This sharpens the inequality (17.4) but does not significantly affect the subsequent calculations.

Finally, the author would like to thank Mrs. Valerie Peverett for her fine typing of this thesis.

§2. Notation and Definitions.

The notation used will be that of Wielandt [14] except where otherwise stated. Let G be a finite group and Ω a G-set. If $\Delta \subseteq \Omega$ and $\alpha \in \Omega$, then Δg and αg denote the images of Δ and α under the action of an element $g \in G$. $G_{(\Delta)}$ and $G_{\{\Delta\}}$ will denote the point- and set-stabilisers of Δ in G, respectively. For $S \subseteq G$ we put $fx_\Omega(S) = \{\alpha \in \Omega \mid \alpha s = \alpha \text{ for all } s \in S\}$ and $mv_\Omega(S) = \Omega - fx_\Omega(S)$. We will usually omit the subscript Ω where no confusion is likely to arise. Moreover, we will abbreviate $G_{(\alpha)}$ and $G_{(\alpha,\beta)}$ to G_α and $G_{\alpha,\beta}$. For $s \in S$ and $g \in G$ we let s^g denote the element $g^{-1}sg$, and put $S^g = \{s^g \mid s \in S\}$. We also put $N_G(S) = \{g \in G \mid S^g = S\}$ and $C_G(S) = \{g \in G \mid s^g = s \text{ for all } s \in S\}$.

An irreducible character of G is a mapping from G into $\mathbb{C}$ of the form trace ρ, where ρ is an irreducible representation of G. char (G) is the set of all linear combinations of irreducible characters of G with integral coefficients. An element of char (G) is called a generalised character. We define an inner product on char (G) by

$$(2.1) \qquad \langle \zeta, \eta \rangle = \frac{1}{|G|} \sum_{g \in G} \zeta(g)\overline{\eta(g)}.$$

A generalised irreducible character is an element $\zeta \in$ char (G) for which $\langle \zeta, \zeta \rangle = 1$. In this case, since $\zeta = \pm\chi$ for some irreducible character χ, a generalised irreducible character corresponding to χ will be denoted by $\tilde{\chi}$.

Let $H \leq G$, $\zeta \in$ char (G) and $\eta \in$ char (H). We define the restriction ζ_H of ζ to H by

(2.2) $\zeta_H(h) = \zeta(h)$ for all $h \in H$.

We construct a function $\dot{\eta} : G \to \mathbb{C}$ which satisfies

$$(2.3) \qquad \dot{\eta}(g) = \begin{cases} \eta(g) & \text{if } g \in H, \\ 0 & \text{if } g \in G - H. \end{cases}$$

The induced character η^G is then defined by

$$(2.4) \qquad \eta^G(g) = \frac{1}{|H|} \sum_{k \in G} \dot{\eta}(k^{-1}gk) \text{ for all } g \in G.$$

By a celebrated theorem of Frobenius (Curtis and Reiner [3] p. 271)

$$(2.5) \qquad \langle \zeta, \eta^G \rangle = \langle \zeta_H, \eta \rangle.$$

χ_0 will always denote the trivial character of the group G.

If $f : G \to \mathbb{C}$ is an arbitrary function we will abbreviate $\sum_{g \in G} f(g)$ to $\sum_G f$.

If g,h and k are three fixed elements of G, $*\{g'h' = k\}$ is defined to be the number of pairs (g_1, h_1) for which g_1 is conjugate in G to g, h_1 is conjugate in G to h, and $g_1 h_1 = k$. Then

$$(2.6) \qquad *\{g'h' = k\} = \frac{|G|}{|C_G(g)| \cdot |C_G(h)|} \sum_{\chi} \frac{\chi(g)\chi(h)\overline{\chi(k)}}{\chi(1)},$$

the summation being over all irreducible characters of G.

Since Ω is a G-set, G can be made to act naturally on (i) the set Ω^r of all ordered r-tuples from Ω, $(w_1, \ldots, w_r)g = (w_1 g, \ldots, w_r g)$; (ii) the set $\Omega^{\{r\}}$ of all subsets of r distinct elements of Ω, $\{w_1, \ldots, w_r\}g = \{w_1 g, \ldots, w_r g\}$; and (iii) cartesian products of sets of type (ii). The fact that

(2.7) The number of G-orbits in Ω is $\frac{1}{|G|} \sum_{G} fx_{\Omega}$

can be used to advantage on these composite sets when G acts multiply-transitively on Ω.

It has been shown by Frobenius [5] that there is a one-to-one correspondence between the irreducible characters of $\mathrm{Sym}(\Omega)$ - the symmetric group on Ω - and the partitions of $|\Omega|$. We let $\chi^{[\lambda]}$ denote the irreducible character corresponding to the partition $[\lambda] = [\lambda_1, \lambda_2, \ldots, \lambda_r]$, where $\lambda_1 \geq \ldots \geq \lambda_r > 0$ and $|\Omega| = \lambda_1 + \ldots + \lambda_r$. $\chi^{[\lambda]}$ is said to have dimension $|\Omega| - \lambda_1$.

An element $g \in \mathrm{Sym}(\Omega)$ has <u>type</u> $1^{\alpha_1(g)} 2^{\alpha_2(g)} 3^{\alpha_3(g)} \ldots$ if there are exactly $\alpha_i(g)$ i-cycles in its cycle decomposition.

We will have occasion to use the following characters of $\mathrm{Sym}(\Omega)$, where $|\Omega| = n$:

$$\chi^{[n]} = 1;$$

$$\chi^{[n-1,1]} = \alpha_1 - 1;$$

$$\chi^{[n-2,1^2]} = (\alpha_1 - 1)(\alpha_1 - 2)/2 - \alpha_2;$$

$$\chi^{[n-2,2]} = \alpha_1(\alpha_1 - 3)/2 + \alpha_2;$$

$$\chi^{[n-3,1^3]} = (\alpha_1 - 1)(\alpha_1 - 2)(\alpha_1 - 3)/6 - (\alpha_1 - 1)\alpha_2 + \alpha_3.$$

From Frobenius [6] we have the following important result

(2.8) Let $\chi^{[\lambda]}$ and $\chi^{[\mu]}$ be two irreducible characters of $\mathrm{Sym}(\Omega)$ of dimensions r and s, respectively, and let $G \leq \mathrm{Sym}(\Omega)$. Then, if G is $(r + s)$-transitive on Ω, we have $\langle \chi^{[\lambda]}{}_G, \chi^{[\mu]}{}_G \rangle = \begin{cases} 1 & \text{if } [\lambda] = [\mu]; \\ 0 & \text{if } [\lambda] \neq [\mu]. \end{cases}$

Sometimes we will find it convenient, if $|\Omega| = n$, to write

Sym(n) and Alt(n) for Sym(Ω) and Alt(Ω).

Although the term block will be used in both the permutation group sense and the geometric sense, it will generally be clear from the context which sense is intended. The definition of a design will be that of Kantor [9], namely a set of v points together with a set of b distinguished subsets, each having k points, so that any two points are contained in exactly λ such subsets. If r is the number of such subsets containing a given point, we have the equalities

(2.9) $vr = bk$ and $\lambda(v-1) = r(k-1)$.

(for a proof see Dembowski [4] p.5). If $\lambda = 1$, we call the design a partial plane, though for the remaining sections we add the condition $k \geq 3$. A subplane of a partial plane is a design consisting of a subset of the points and a subset of the lines, and which is itself a partial plane.

We use the definitions of projective plane and projective space given in Wagner [13]. Thus a projective plane is a partial plane with $b = v$. For a projective space of dimension at least 3 we have the following characterisation due to Veblen and Young [12]: It is a set of points together with a set of distinguished subsets, called lines, which satisfy the axioms

(2.10) There is one, and only one, line through every pair of points;

(2.11) Every line has at least three points,

(2.12) Every triple of non-collinear points is contained in a subplane of the partial plane of points and lines which is a projective plane;

(2.13) There are four points not all in the same projective subplane.

The following theorem, due to Witt, will be used throughout this work.

(2.14) Theorem: Let G be a k-transitive permutation group on a set Ω. Let $\Delta \subseteq \Omega$, $|\Delta| = k$. Suppose that $G_{(\Delta)}$ has a subgroup U which is conjugate in $G_{(\Delta)}$ to every subgroup of $G_{(\Delta)}$ to which it is conjugate in G. Then $N_G(U)$ is k-transitive on $fx(U)$.

The following corollaries are immediate.

(2.15) Corollary: If U is a Sylow subgroup of $G_{(\Delta)}$, then $N_G(U)$ is k-transitive on $fx(U)$.

(2.16) Corollary: $N_G(G_{(\Delta)})$ is k-transitive on $fx(G_{(\Delta)})$.

(2.17) Corollary: With the hypothesis of (2.14), if V is a subgroup of U, which is weakly closed in U with respect to G, then $N_G(V)$ is k-transitive on $fx(V)$.

Part I: Classical Theorems on Jordan Groups.

§3. Jordan Sets.

In this section, G will be a transitive permutation group on Ω. We recall that a Jordan set for G is a subset Γ of Ω such that $2 \leq |\Gamma| \leq |\Omega| - 1$ and $G_{(\Omega - \Gamma)}$ is transitive on Γ.

(3.1) Lemma: If Γ_1 and Γ_2 are Jordan subsets for G and $|\Gamma_1| \leq |\Gamma_2|$, then $\Gamma_1 g \leq \Gamma_2$ for some $g \in G$.

Proof: We choose $g \in G$ such that $|\Gamma_1 g \cup \Gamma_2|$ is minimal. By the transitivity of G on Ω, $\Gamma_1 g \cap \Gamma_2 \neq \emptyset$. So $G_{(\Omega - \Gamma_1 g \cup \Gamma_2)}$ is transitive on $\Gamma_1 g \cup \Gamma_2$. Suppose that $\Gamma_1 g \cup \Gamma_2 \neq \Gamma_2$. Then we can choose α and β in $\Gamma_1 g \cup \Gamma_2$ such that $\alpha \notin \Gamma_1 g$ and $\beta \notin \Gamma_2$. Moreover, we can find $h \in G_{(\Omega - \Gamma_1 g \cup \Gamma_2)}$ such that $\alpha h = \beta$. Thus $\Gamma_1 gh \cup \Gamma_2 \subseteq \Gamma_1 g \cup \Gamma_2$. But $\beta = \alpha h \notin \Gamma_1 gh$. Hence $\beta \in \Gamma_1 g \cup \Gamma_2 - \Gamma_1 gh \cup \Gamma_2$. This contradicts the minimal choice of g. Hence $\Gamma_1 g \cup \Gamma_2 = \Gamma_2$, as required.

(3.2) Corollary: If Γ is a Jordan subset for G, and $\Gamma \cap \Gamma g \neq \emptyset$, then $\Gamma gh = \Gamma$ for some $h \in G_{(\Omega - \Gamma \cup \Gamma g)}$.

Proof: If $|\Gamma \cup \Gamma g| = |\Gamma|$, the result is trivially true. Otherwise, both Γ and Γg are Jordan sets for $G_{(\Omega - \Gamma \cup \Gamma g)}$. The result follows from (3.1).

(3.3) Theorem: Let H be a subgroup of G with a non-empty fixed point set. Choose $g \in G - G_{\{\Gamma\}}$ such that $|\Gamma g \cup \Gamma|$ is minimal, where $\Gamma = mv(H)$. Then $\Gamma g \cup \Gamma - \Gamma$ is a block of $G_{\{\Gamma g \cup \Gamma\}}$.

Proof: Let $h \in G_{\{\Gamma g \cup \Gamma\}}$. Then $\Gamma h \subseteq \Gamma g \cup \Gamma$. By minimality, $\Gamma h = \Gamma$ or $\Gamma h \cup \Gamma = \Gamma g \cup \Gamma$. That is, $(\Gamma g \cup \Gamma - \Gamma)h = \Gamma g \cup \Gamma - \Gamma$ or $\emptyset = \Gamma g \cup \Gamma - \Gamma h \cup \Gamma =$

$(\Gamma g \cup \Gamma - \Gamma)h \cap (\Gamma g \cup \Gamma - \Gamma)$.

In (3.3), the transitivity of G on Ω was used to choose an element $g \in G$ which satisfied the hypothesis. If, in addition, G is primitive on Ω, then $\Gamma g \cap \Gamma \neq \emptyset$.

(3.4) Corollary: Let G be primitive on Ω, and let Γ be a Jordan set for G. Choose $g \in G - G_{\{\Gamma\}}$ such that $|\Gamma g \cup \Gamma|$ is minimal. Then $G_{(\Omega - \Gamma g \cup \Gamma)}$ is transitive on $\Gamma g \cup \Gamma$, and $|\Gamma g \cup \Gamma - \Gamma|$ divides $|\Gamma|$ properly.

Proof: Since $\Gamma g \cap \Gamma \neq \emptyset$, $G_{(\Omega - \Gamma g \cup \Gamma)}$ is transitive on $\Gamma g \cup \Gamma$. Hence $G_{\{\Gamma g \cup \Gamma\}}$ is transitive on $\Gamma g \cup \Gamma$. Since $\Gamma g \cup \Gamma - \Gamma$ is a block of $G_{\{\Gamma g \cup \Gamma\}}$ by (3.3), $\Gamma g \cup \Gamma$ is a union of disjoint images of $\Gamma g \cup \Gamma - \Gamma$. The result follows immediately.

A set D of subsets of Ω is said to be connected if it is not the union of two non-empty subsets D_1 and D_2 of D such that for all Γ_1 in D_1 and for all Γ_2 in D_2, $\Gamma_1 \cap \Gamma_2$ is empty.

(3.5) Theorem: Let G be primitive on Ω, and let Γ be a subset of Ω with $2 \leq |\Gamma| \leq |\Omega| - 1$. For any $\alpha \in \Omega$, $\Omega - \{\alpha\}$ is the union of a connected set of subsets of the form Γg, $g \in G$.

Proof: Let Δ be a proper subset of Ω which is a union of a connected set of sets $\Gamma g'$, and which is maximal subject to these conditions. By primitivity, $\Delta g \neq \Delta$ and $\Delta g \cap \Delta \neq \emptyset$ for some $g \in G$. Then $\Delta \cup \Delta g$ is the union of a connected set of sets $\Gamma g'$, and contains Δ properly. So $\Delta \cup \Delta g = \Omega$. Hence $|\Delta| > \frac{1}{2}|\Omega|$. If $|\Delta| \neq |\Omega| - 1$, we can find $h \in G$ such that $(\Omega - \Delta)h \neq \Omega - \Delta$ and $(\Omega - \Delta)h \cap (\Omega - \Delta) \neq \emptyset$. So $\Delta \cup \Delta h \neq \Omega$. But $\Delta \cap \Delta h \neq \emptyset$ since $|\Delta| > \frac{1}{2}|\Omega|$. This contradicts the maximal choice of Δ.

So $|\Delta| = |\Omega| - 1$. The result follows from the transitivity of G on Ω.

(3.6) Corollary: (Jordan [8]) If G is primitive on Ω and admits a Jordan set, then G is 2-transitive on Ω.

Proof: Let Γ be a Jordan set for G, and apply (3.5).

Let $\{\Omega, \mathcal{L}\}$ be a partial plane, as defined in §2. We recall that a subplane of Ω is a subset Ω_0 of Ω, together with a subset $\mathcal{L}_0$ of $\mathcal{L}$, such that (i) every block of $\mathcal{L}$ which contains at least two points of Ω_0 lies in $\mathcal{L}_0$, and (ii) if $\Psi \in \mathcal{L}_0$, then every point of Ψ is in Ω_0.

(3.7) Lemma: If Ω_0 is a proper subplane of Ω then $|\Omega_0| < \frac{1}{2}|\Omega|$.

Proof: Let $\alpha \in \Omega - \Omega_0$. If there are r lines through α, and k points on a line, then $|\Omega| = 1+r(k-1)$. But Ω_0 contains at most one point on each line through α. Thus $|\Omega_0| \leq r = (|\Omega|-1)/(k-1) < \frac{1}{2}|\Omega|$ since $k > 2$.

(3.8) Theorem: Let G be 2-transitive on Ω, and let Γ be a subset of Ω with $2 \leq |\Gamma| \leq |\Omega|-2$. Let $\alpha, \beta \in \Omega, \alpha \neq \beta$. Then there exists a unique set $\Phi(\alpha,\beta)$ such that (i) $\Phi(\alpha,\beta)$ is the union of a connected set of sets Γg not containing either α or β, and is maximal subject to this, and (ii) $|\Phi(\alpha,\beta)| > (|\Omega|-1)/2$. If $\Phi(\alpha,\beta) \neq \Omega - \{\alpha,\beta\}$, then Ω is a partial plane in which the lines are the subsets of the form $\Lambda(\gamma,\delta) = \Omega - \Phi(\gamma,\delta)$, $\gamma \neq \delta$, and G is a group of automorphisms of this plane. Lastly, $G_{\{\Lambda(\alpha,\beta)\}}$ is 2-transitive on $\Lambda(\alpha,\beta)$.

Proof: Let Φ be the union of a connected set of subsets $\Gamma g'$, with $|\Phi| \leq v-2$, where $v = |\Omega|$, and let Φ be maximal subject to these conditions. We can find $g \in G$ such that $\Phi g \cap \Phi \neq \emptyset$ and $\Phi g \neq \Phi$. Then $\Phi g \cup \Phi$ is the union of a connected set of subsets $\Gamma g'$, and it contains Φ properly. Hence $v-1 \leq |\Phi \cup \Phi g|$. So $|\Phi| > \frac{1}{2}(v-1)$. Since $|\Phi| \leq v-2$, we can find $h \in G$

such that Φh contains neither α nor β. So Φh satisfies conditions (i) and (ii) of the theorem. Now suppose that Ψ is a second set satisfying (i). Then $\Phi h \cap \Psi = \emptyset$, since otherwise $\Phi h \cup \Psi$ is the union of a connected set of subsets $\Gamma g'$ not containing α or β, but containing both Φh and Ψ properly. Hence Ψ cannot satisfy (ii). So Φh is uniquely determined by (i) and (ii). We denote Φh by $\Phi(\alpha,\beta)$.

Since $\Phi(\alpha,\beta)g$ satisfies (i) and (ii) with α and β replaced by αg and βg, we have $\Phi(\alpha,\beta)g = \Phi(\alpha g,\beta g)$. By 2-transitivity all $\Phi(\alpha,\beta)$ $(\alpha,\beta \in \Omega)$ have the same size and are permuted transitively by G. Let γ,δ be distinct elements of $\Lambda(\alpha,\beta) = \Omega - \Phi(\alpha,\beta)$. Then $\Phi(\alpha,\beta)$ satisfies (i) and (ii) with α,β replaced by γ,δ except, possibly, that it may not be maximal. So $\Phi(\alpha,\beta) \subseteq \Phi(\gamma,\delta)$. Since both sets have the same size, we get equality. Hence $\Lambda(\alpha,\beta) = \Lambda(\gamma,\delta)$. That is, each pair of points is contained in exactly one set of the form $\Lambda(\alpha,\beta)$. These "lines" $\Lambda(\alpha,\beta)$ satisfy all the requirements for a partial plane, provided that $|\Lambda(\alpha,\beta)| > 2$.

Finally, if $\Lambda(\alpha,\beta) = \Lambda(\gamma,\delta)$, choose $g \in G$ such that $\alpha g = \gamma$, $\beta g = \delta$. Then $\Lambda(\alpha,\beta) = \Lambda(\alpha g,\beta g) = \Lambda(\alpha,\beta)g$. So $g \in G_{\{\Lambda(\alpha,\beta)\}}$. This proves the last statement.

(3.9) Theorem: Let G be primitive on Ω, and suppose that G admits a Jordan set Γ, with $|\Gamma| < |\Omega| - 1$. Then either G is 3-transitive on Ω, or G is an automorphism group of a partial plane, and $\Omega - \Gamma$ is a subplane.

Proof: By (3.6), G is 2-transitive on Ω, so we may apply (3.8). If $\Phi(\alpha,\beta) = \Omega - \{\alpha,\beta\}$, then $G_{\alpha,\beta}$ is transitive on $\Phi(\alpha,\beta)$. So G is

3-transitive on Ω. In the remaining case, Ω is a partial plane in which the lines are $\Lambda(\alpha,\beta)$, $\alpha,\beta \in \Omega$.

Now suppose that α,β are distinct points of $\Omega - \Gamma$. Then if $\Gamma \not\subseteq \Phi(\alpha,\beta)$, we can choose $h \in G$ such that $\Gamma h \cap \Phi(\alpha,\beta) \neq \emptyset$, $\Gamma h \not\subseteq \Phi(\alpha,\beta)$ and $|\Phi(\alpha,\beta) \cup \Gamma h| \leq |\Omega| - 2$. Then $\Phi(\alpha,\beta) \cup \Gamma h$ is the union of a connected set of subsets $\Gamma g'$, and omits at least two distinct points, γ and δ say. Hence $\Phi(\alpha,\beta) \cup \Gamma h \subseteq \Phi(\gamma,\delta)$. This contradicts the fact that all sets of the form $\Phi(\alpha,\beta)$ have the same number of elements. Hence $\Gamma \subseteq \Phi(\alpha,\beta)$. So $\Lambda(\alpha,\beta) \subseteq \Omega - \Gamma$. Thus $\Omega - \Gamma$ is a partial plane.

The preceding argument can be readily modified, in this case, to show that $\Phi(\alpha,\beta)$ is the union of all $\Gamma g'$ which contain neither α nor β.

§4. Theorems of Marggraf and Jordan.

We consider now a permutation group G on Ω which admits a Jordan set Γ, and where further conditions are imposed either on $G_{(\Gamma)}$ or on the set Γ itself.

(4.1) Theorem: (Jordan [8]) Let G be primitive on Ω, and suppose that $G_{(\Omega - \Gamma)}$ is primitive on Γ. Then G is $(|\Omega| - |\Gamma| + 1)$ - transitive on Ω.

Proof: By (3.3), we can choose $g \in G$ such that $|\Gamma \cup \Gamma g| = |\Gamma| + 1$. So $G_{(\Omega - \Gamma \cup \Gamma g)}$ is 2-transitive on $\Gamma \cup \Gamma g$. If $|\Omega| - |\Gamma| = 1$, we are home. Suppose $|\Omega| - |\Gamma| > 1$, and use induction on $|\Omega| - |\Gamma|$. By induction, G is $(|\Omega| - |\Gamma \cup \Gamma g| + 1)$-transitive on Ω. Moreover, the stabiliser of the $|\Omega| - |\Gamma|$ points in $\Omega - \Gamma$ is transitive on the rest. Hence G is

$(|\Omega| - |\Gamma| + 1)$-transitive on Ω. So the theorem is true by induction.

In the case $|\Gamma| = 3$, it is readily shown that G contains the alternating group on Ω. This may be used to show that any group on Ω which is n-transitive, for $n > \frac{1}{3}|\Omega| + 1$, contains $\mathrm{Alt}(\Omega)$ - for a proof, see Burnside [2] p. 178.

(4.2) Corollary: If G is primitive on Ω, $|\Gamma| < 2|\Omega|/3$, and $G_{(\Omega - \Gamma)}$ is primitive on Γ, then G contains $\mathrm{Alt}(\Omega)$.

Proof: Since $|\Omega| - |\Gamma| + 1 > \frac{1}{3}|\Omega| + 1$, we get the result from (4.1) and the preceding remarks.

(4.3) Theorem (Marggraf [10]) If G is primitive on Ω and $|\Gamma| \leq \frac{1}{2}|\Omega|$, then G is 3-transitive on Ω.

Proof: This is an immediate consequence of (3.7) and (3.9).

Before characterising the groups mentioned in (4.3), we will relate the degree of transitivity of a permutation group G on Ω, which admits a Jordan subset Γ, to the degree of transitivity of $G_{\{\Gamma\}}$ on $\Omega - \Gamma$.

(4.4) Theorem: Let G be k-transitive on Ω, $k \geq 1$. Then $G_{\{\Gamma\}}$ is always (k-1)-transitive on $\Omega - \Gamma$, and it is k-transitive on $\Omega - \Gamma$ if $|\Gamma| > \frac{1}{2}(|\Omega| - k)$.

Proof: (i) Take $\alpha \in \Gamma$, and $\{\beta_1, \ldots, \beta_{k-1}\}$ and $\{\gamma_1, \ldots, \gamma_{k-1}\}$ to be two (k-1)-element subsets of $\Omega - \Gamma$. We can choose $g \in G$ such that $\alpha g = \alpha$, $\beta_i g = \gamma_i$, $i = 1, \ldots, k-1$. Since $\Gamma \cap \Gamma g \neq \emptyset$, we can choose $h \in G_{(\Omega - \Gamma \cup \Gamma g)}$ such that $\Gamma gh = \Gamma$, by (3.2). But then $\beta_i gh = \gamma_i$, $i = 1, \ldots, k-1$.

(ii) If $\{\beta_1, \ldots, \beta_k\}$ and $\{\gamma_1, \ldots, \gamma_k\}$ are two k-element subsets

of $\Omega - \Gamma$, we can find $g \in G$ such that $\beta_i g = \gamma_i$, $i = 1, \ldots, k$. But if $|\Gamma| > \frac{1}{2}(|\Omega| - k)$, then $|\Gamma \cap \Gamma g| \neq 0$, since there are at least k elements in $\Omega - \Gamma \cup \Gamma g$. Again by (3.2), we can find $h \in G_{(\Omega - \Gamma \cup \Gamma g)}$ such that $\Gamma gh = \Gamma$. Then $\beta_i gh = \gamma_i$, $i = 1, \ldots, k$, as required.

(4.5) Theorem (Marggraf [10]). Let G be primitive on Ω, and $|\Gamma| \leq \frac{1}{2}|\Omega|$. Then, either (i) G contains $\mathrm{Alt}(\Omega)$, or (ii) $|\Omega| = 2^m$, $|\Gamma| = \frac{1}{2}|\Omega|$, G is the holomorph of an elementary abelian group V_2m of order 2^m, and Ω may be given the structure of an elementary abelian group via the regular normal subgroup V_2m of G in such a way that $\Omega - \Gamma$ is a subgroup.

Proof: The proof is by induction on $|\Omega|$. If $|\Omega| \leq 7$, then $|\Gamma| = 2$ or 3. So $G_{(\Omega - \Gamma)}$ is necessarily primitive on Γ. The result follows from (4.2).

Now suppose that $g \in G$ may be chosen such that $|\Gamma \cup \Gamma g| = |\Gamma| + 1$. Then $G_{(\Omega - \Gamma \cup \Gamma g)}$ is 2-transitive, and hence primitive, on $\Gamma \cup \Gamma g$. By (4.2), the result again follows, since $|\Gamma \cup \Gamma g| = |\Gamma| + 1 \leq \frac{1}{2}|\Omega| + 1 < 2|\Omega|/3$, so long as $|\Omega| > 6$.

Let g be chosen such that $\Gamma g \neq \Gamma$ and, subject to this, that $|\Gamma g \cup \Gamma|$ is minimal. Put $\Psi = \Gamma g \cup \Gamma - \Gamma$. We will assume that $|\Psi| \geq 2$ in view of the preceding paragraph. Let $G^{\Omega - \Gamma}$ be denoted by H. We will show that the hypotheses of the theorem are satisfied if G, Ω and Γ are replaced by H, $\Omega - \Gamma$ and Ψ, respectively. Indeed, G is 3-transitive by (4.3). So H is 2-transitive on $\Omega - \Gamma$ by (4.4). Hence H is primitive on $\Omega - \Gamma$. Since $\Gamma \cap \Gamma g \neq \emptyset$, $G_{(\Omega - \Gamma \cup \Gamma g)}$ is transitive on $\Gamma \cup \Gamma g$ and admits Γ as a Jordan set. Again by (4.4), $G_{\{\Gamma\}} \cap G_{(\Omega - \Gamma \cup \Gamma g)}$ is transitive

on Ψ, since $|\Gamma| > \frac{1}{2}|\Gamma \cup \Gamma g|$. Hence $H_{(\Omega - \Gamma \cup \Gamma g)}$ is transitive on Ψ. Finally, since $|\Psi|$ divides $|\Gamma|$ properly, by (3.4), we have $|\Psi| \leq \frac{1}{2}|\Gamma| \leq \frac{1}{2}|\Omega - \Gamma|$. So we may apply the inductive hypothesis to H, $\Omega - \Gamma$, Ψ.

We first consider the case: $\mathrm{Alt}(\Omega - \Gamma) \leq H$. We can write the elements of $G_{\{\Gamma\}}$ in the form (h_1, h_2) where $h_1 \in \mathrm{Sym}(\Gamma)$, $h_2 \in \mathrm{Sym}(\Omega - \Gamma)$. Let K_1 and K_2 be the images of the projection homomorphisms $(h_1, h_2) \to h_1$ and $(h_1, h_2) \to h_2$, respectively; and let L^*_2 and L^*_1 be their respective kernels. Let $L_1 = \{h \mid (h,1) \in L^*_1\}$, and define L_2 similarly. Then $L_1 \lhd K_1$, $L_2 \lhd K_2$ and $K_1/L_1 \cong K_2/L_2$. Since Γ is a Jordan set for G, L_1 is transitive on Γ. Hence $|L_1| \geq |\Gamma|$. But K_2 contains $\mathrm{Alt}(\Omega - \Gamma)$. So $|L_2| = |L_1| \cdot |K_2|/|K_1| \geq |\Gamma| \cdot \frac{1}{2} \cdot |\Omega - \Gamma|!/|\Gamma|! \geq \frac{1}{2}|\Gamma| > 1$. Thus L_2 is non-trivial. If $|\Omega - \Gamma| \geq 5$, L_2 must contain $\mathrm{Alt}(\Omega - \Gamma)$. So $\mathrm{Alt}(\Omega) \leq G$, by (4.1). If $|\Omega - \Gamma| \leq 4$, the restrictions $|\Gamma| \leq \frac{1}{2}|\Omega|$ and $|\Omega| \geq 8$ imply that $|\Omega| = 8$, $|\Gamma| = 4$. We exclude the possibility $H = \mathrm{Alt}(\Omega - \Gamma)$. Since G is 3-transitive on Ω and $|\Gamma| = 4 > \frac{1}{2}(8 - 3)$, we see that H is 3-transitive on $\Omega - \Gamma$. Hence $H = \mathrm{Sym}(\Omega - \Gamma) = \mathrm{Hol}\ V_4$. By assumption $|\Psi| \geq 2$. By 3-transitivity of G on Ω, we must have $|\Psi| \leq 2$. Hence $|\Psi| = 2$. So $\Omega - \Gamma \cup \Psi$ is a subgroup of order 2 of $\Omega - \Gamma$, if an element of $\Omega - \Gamma \cup \Psi$ is taken to be the identity of $\Omega - \Gamma$. So we are in the second case.

We now consider the case: Γ, $\Omega - \Gamma$ and Ψ satisfy the conditions (ii) of the theorem, with m replaced by $m-1$, and $m \geq 3$. From the inequalities $2^{m-2} = |\Psi| \leq \frac{1}{2}|\Gamma| \leq \frac{1}{2}|\Omega - \Gamma| = 2^{m-2}$, we find that $|\Gamma| = 2^{m-1}$ and $|\Omega| = 2^m$. Now, if $m > 3$, then H is not 4-transitive on $\Omega - \Gamma$, so G is not 4-transitive on Ω by (4.4). While for $m = 3$, a 4-transitive

group of degree 8 is easily seen to contain Alt(8) - and this case is already dealt with. So we have only to consider the case in which G is strictly 3-transitive on Ω, for $m \geq 3$. Hence, if α, β, γ are three distinct elements of Ω, then $\Omega - \{\alpha,\beta,\gamma\}$ is not the union of a connected set of sets $\Gamma g'$. But, since G is 3-transitive on Ω, we may assume that $\alpha,\beta,\gamma \in \Omega - \Gamma$. By our assumption about the action of H on $\Omega - \Gamma$, there is a unique element δ such that Ψh omits δ whenever it omits α, β and γ, for $h \in H$. Since $\Psi h = \Gamma_{\psi} \Gamma gh - \Gamma$, there is no point, other than δ, omitted by $\Gamma g'$, whenever $\Gamma g'$ omits α, β and γ. We call $\{\alpha,\beta,\gamma,\delta\}$, and similarly constructed sets in Ω, "quadruples". By 3-transitivity, G is transitive on quadruples. Let 0 be the identity of the group $\Omega - \Gamma$. We define addition on Ω by: $\alpha + \alpha = 0$, $\alpha + 0 = 0 + \alpha = \alpha$, and if $0,\alpha$ and $\beta$are distinct, let $\alpha + \beta$ be the element for which $\{0,\alpha,\beta,\alpha+\beta\}$ is a quadruple. For α, $\beta \in \Omega - \Gamma$, this addition agrees with the group addition in $\Omega - \Gamma$. We now want to show that, for all $\alpha,\beta,\gamma \in \Omega$, (a) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, and (b) $\{\alpha,\beta,\gamma, \alpha+\beta+\gamma\}$ is a quadruple. We first consider the case $m = 3$, and $0,\alpha,\beta, \alpha+\beta$ and γ distinct. Since distinct quadruples intersect in at most two points, the elements $0,\alpha, \beta,\gamma,\alpha+\beta,\beta+\gamma$ and $\gamma + \alpha$ are distinct and differ from the elements $\alpha + (\beta+\gamma)$, $(\alpha+\beta) + \gamma$ and the fourth element of the quadruple containing α, β and γ. (a) and (b) follow immediately. For $m > 3$, and the same restrictions on α, β and γ as before, we may assume that $\alpha,\beta, \gamma \in \Omega - \Gamma$ since G_0 is 2-transitive on $\Omega - \{0\}$ and $G_{(0,\alpha,\beta,\alpha+\beta)}$ is transitive on $\Omega - \{0,\alpha,\beta,\alpha+\beta\}$. But then (a) and (b) both hold by the inductive hypothesis. For $m \geq 3$, and $0,\alpha,\beta,\alpha+\beta$ and γ not all distinct, we may assume by 3-transitivity

that they all belong to $\Omega - \Gamma$. So (a) and (b) hold again by the inductive hypothesis. (a) guarantees that Ω is an elementary abelian group V_2m, in which $\Omega - \Gamma$ is a subgroup of index 2. By (b), G is a subgroup of $Hol(V_2m)$. Since G admits Jordan sets of sizes 2^m-2^i, i=0,1, ... ,m-1 - as can be seen by considering the corresponding property of $G_{\{\Gamma\}}$ on $\Omega - \Gamma$ - $|G|$ is divisible by $2^m(2^m-1)(2^m-2)$ ... $(2^m-2^{m-1}) = |Hol(V_2m)|$. Hence, $G = Hol(V_2m)$. This completes the proof of (4.5).

Part II: Jordan Sets of Prime Power Cardinality

§5. Statement of the Theorem.

In this section we begin the proof of the following theorem.

(5.1) Theorem: Let G be a strictly 2-transitive group on a set Ω, which admits a non-trivial Jordan set Γ of prime power cardinality p^r. Suppose that a Sylow p-subgroup of $G_{(\Lambda(\gamma,\delta))}$ is a Sylow p-subgroup of $G_{\gamma,\delta}$, for all $\gamma, \delta \in \Omega, \gamma \neq \delta$, where $\Lambda(\gamma,\delta)$ is defined as in (3.8). Then $\{\Omega,\mathcal{L}\}$ is the design of points and lines of projective space of dimension $d(\geq 2)$ over the field with $q = |\Lambda(\gamma,\delta)| - 1$ elements, where $\mathcal{L} = \{\Lambda(\gamma,\delta) | \gamma,\delta \in \Omega, \gamma \neq \delta\}$, and G contains the little projective group.

Throughout §5-8 $\{G,\Omega,\Gamma\}$ will denote a counter-example to (5.1) which is minimal with respect to $|\Omega|$. The points $\alpha,\beta \in \Omega - \Gamma$ will remain fixed, and H will denote a fixed Sylow p-subgroup of $G_{(\Omega-\Gamma)}$. Thus H is transitive on Γ. As $H \leq G_\alpha$, H is contained in some Sylow p-subgroup of G_α; we choose P to be one such subgroup. We abbreviate $\Lambda(\alpha,\beta)$ and $\Phi(\alpha,\beta)$ to Λ and Φ respectively. Note that because of 2-transitivity, the statement that a Sylow p-subgroup of $G_{(\Lambda(\gamma,\delta))}$ is a Sylow p-subgroup of $G_{\gamma,\delta}$ for all pairs γ,δ with $\gamma \neq \delta$, is equivalent to saying that a Sylow p-subgroup of $G_{(\Lambda)}$ is a Sylow p-subgroup of $G_{\alpha,\beta}$. Since Λ is fixed (as a set) by $G_{\alpha,\beta}$, this last statement implies (and so is equivalent to saying) that every Sylow p-subgroup of $G_{\alpha,\beta}$ is a Sylow p-subgroup of $G_{(\Lambda)}$.

It is immediate that the design $\{\Omega,\mathcal{L}\}$ satisfies axioms (2.10) and (2.11). In §6, we show that this design is more like a projective plane than a projective space of higher dimension. Some numerical

restrictions on the parameters are found in §7. These are used in the following section to limit the structure of a Sylow p-subgroup of G. The proof of (5.1) is then completed in §8.

6. The Impossibility of $\Phi \neq \Gamma$.

Suppose that $\Phi \neq \Gamma$. Let $\eta \in \Phi - \Gamma$. In view of (4.3) we have $|\Gamma| > \frac{1}{2}|\Omega| > \frac{1}{2}(|\Omega| - 2)$. So by (4.4), $G_{\{\Gamma\}}$ is 2-transitive on $\Omega - \Gamma$. Now G is an automorphism group of a partial plane, of which $\Omega - \Gamma$ is a subplane, by (3.9). As $\Omega - \Gamma$ contains triples of collinear points and triples of non-collinear points, e.g. $\{\alpha,\beta,\eta\}$, $G_{\{\Gamma\}}$ cannot act 3-transitively on $\Omega - \Gamma$. Hence $G^{\Omega-\Gamma}$ is strictly 2-transitive on $\Omega - \Gamma$.

If g is chosen as in (3.3), then $G^{\Omega-\Gamma}$ admits $\Gamma g \cup \Gamma - \Gamma$ as a non-trivial Jordan subset of prime power cardinality.

Let Q be a Sylow p-subgroup of $G_{\alpha,\beta}$ which contains H; and chose P to be a Sylow p-subgroup of G_α containing Q. Then $Q \leq P_\beta \leq G_{\alpha,\beta}$. Whence, by the choice of Q, $Q = P_\beta$. So, by hypothesis, $Q = P_{(\Lambda)}$. Clearly, $P \leq G_{\{\Gamma\}}$. So P and P_β map onto Sylow p-subgroups of $(G_\alpha)^{\Omega-\Gamma}$ and $(G_{\alpha,\beta})^{\Omega-\Gamma}$, respectively, under the natural homomorphism $G_{\{\Gamma\}} \to G^{\Omega-\Gamma}$. That is, $P_{(\Lambda)}{}^{\Omega-\Gamma}$ is a Sylow p-subgroup of $(G^{\Omega-\Gamma})_{\alpha,\beta}$.

Hence the hypotheses of (5.1) are satisfied by the triple $\{G^{\Omega-\Gamma}, \Omega-\Gamma, \Gamma g \cup \Gamma - \Gamma\}$. As $|\Omega-\Gamma| < |\Omega|$, this triple is not a counterexample. So $\Omega - \Gamma$ has the structure of a projective space of dimension $d(\geq 2)$, in which $\{\Lambda(\gamma,\delta) | \gamma,\delta \in \Omega-\Gamma, \gamma \neq \delta\}$ is the set of

* Γ is an orbit of H, $H \leq P$ and $|\Gamma| > \frac{1}{2}|\Omega|$; hence Γ is an

lines. In particular, the triple $\{\alpha,\beta,\eta\}$ is contained in a projective plane which is a subplane of $\{\Omega,\mathcal{L}\}$.

As $G_{(\Lambda)}$ is transitive on Φ, G is transitive on ordered triples of non-collinear points. Hence axiom (2.12) is satisfied. Axiom (2.13) follows from the fact that $\Omega - \Gamma$ contains a projective plane. So $\{\Omega,\mathcal{L}\}$ is the design of points and lines of a projective space of dimension $d(\geq 3)$, and $\Omega - \Gamma$ is a hyperplane. By Dembowski [4] (2.3.1), G is transitive on hyperplanes. Hence G contains all possible elations. Thus, G contains the little projective group, giving us a contradiction. So we get $\Phi = \Gamma$.

§7. Some Numerical Results for the case $\Phi = \Gamma$.

We recall that $\Phi = \Gamma$ is equivalent to $\Gamma g = \Gamma$ or $|\Omega - \Gamma g \cup \Gamma| \leq 1$, for each $g \in G$.

(7.1) Lemma: $|\Omega| = 1 + q + q^{2t}$, where $t \geq 1$ and $q^{2t} = p^r = |\Gamma|$.

Proof: Choose $g \in G$ as in (3.3). Then $|\Gamma g \cup \Gamma - \Gamma| = p^s$, where $s < r$. Since G is 2-transitive on Ω, $|\Omega - \Gamma g \cup \Gamma| \geq 1$. So $|\Omega - \Gamma g \cup \Gamma| = 1$. Thus $|\Omega| = 1 + p^s + p^r$. As $s = 0$ would imply that G was 3-transitive on Ω, we have $s \geq 1$. Put $q = p^s$.

The partial plane $\{\Omega,\mathcal{L}\}$ now has parameters $v = 1 + p^s + p^r$, $k = 1 + p^s$ and $\lambda = 1$. By (2.9) we have $b = (1 + p^s + p^r)(1 + p^{r-s})/(1 + p^s)$. Hence $(1 + p^{r-s})/(1 + p^s)$ is an integer. And this implies that $r - s$ is an odd multiple of s.

Let $\Delta_o = \Gamma g \cup \Gamma - \Gamma$, where g is as in (3.3) and also $\alpha g = \alpha$. Then Δ_o is a block of G_α. Let $\Delta_o, \Delta_1, \ldots, \Delta_n$ be the distinct images of

Δ_o under the action of G_α. Since G_α is transitive on $\Omega - \{\alpha\}$, we have $n = q^{2t-1}$.

(7.2) Lemma: G_α acts 2-transitively on the set $\{\Delta_i\}_{i=0}^{n}$ of blocks.

Proof: Since H fixes Δ_o and α, and is transitive on $\Gamma = \bigcup_{i=1}^{n} \Delta_i$, H must permute the blocks $\Delta_1,\ldots,\Delta_n$ transitively.

Let $P_i = P_{(\Delta_i)}$, $i = 0,\ldots n$; that is, the subgroup of P which fixes Δ_i pointwise, where P is a Sylow p-subgroup of G_α containing H.

(7.3) Lemma: $fx(P_i) = \{\alpha\} \cup \Delta_i$, for $i = 0, \ldots,n$.

Proof: The result is trivial for $i = 0$, since $H \leq P_o$ and $fx(H) = \Omega - \Gamma$. Put $H_1 = H_{\{\Delta_1\}}$. Since H is transitive on Γ and $\Delta_1 \subseteq \Gamma$ is a block of H, H_1 is transitive on Δ_1. Let $\{\Delta_i | i \in J\}$ be the set of blocks which are fixed (as sets) by H_1, and put $J^{\#} = J - \{0\}$. By (2.14) $N_H(H_1)$ is transitive on the set $\{\Delta_i | i \in J^{\#}\}$. So the groups $H_1^{\Delta_i}$, $i \in J^{\#}$, are similar as permutation groups. In particular, H_1 is transitive on each Δ_i, $i \in J$. Hence, $fx(H_1) = \{\alpha\} \cup \Delta_o$.

By (7.2) we can find an element $g_1 \in G_\alpha$ such that $\Delta_o g_1 = \Delta_1$ and $\Delta_1 g_1 = \Delta_o$. So $g_1^{-1} H_1 g_1$ is a p-subgroup of $G_\alpha \cap G_{\{\Delta_o\}}$. But P is a Sylow p-subgroup of $G_\alpha \cap G_{\{\Delta_o\}}$. So we can find an element $g_2 \in G_\alpha \cap G_{\{\Delta_o\}}$ such that $g_2^{-1} g_1^{-1} H_1 g_1 g_2 \leq P$. Put $g = g_1 g_2$. Then $fx(g^{-1} H_1 g) = \{\alpha\} \cup \Delta_o g = \{\alpha\} \cup \Delta_j$ for some $j \in \{1,\ldots,n\}$ as $g \in G_\alpha$. Since $g^{-1} H_1 g \leq P_j$, we see that $fx(P_j) = \{\alpha\} \cup \Delta_j$.

Now $\{P_1,\ldots,P_n\}$ is clearly a conjugacy class of subgroups of P. Hence $fx(P_i) = \{\alpha\} \cup \Delta_i$ for $i = 1,\ldots,n$.

Since P is transitive on Γ, we could have chosen g_2 in such a way that $j = 1$; that is, $g^{-1} H_1 g \leq P_1$, $\Delta_o g = \Delta_1$, $\Delta_1 g = \Delta_o$. But then

$g^{-1}P_1 g \leq G_{(\Omega-\Gamma)} \cap G_{\{\Delta_1\}}$. As H is a Sylow p-subgroup of $G_{(\Omega-\Gamma)}$, some conjugate of P_1 is contained in $H_{\{\Delta_i\}}$, for some $i \geq 1$. By comparing orders, we find that $|P_1| \leq |H_{\{\Delta_i\}}| = |H_1|$, so that $g^{-1}H_1 g = P_1$.

(7.4) Corollary: There is an element $g \in G_\alpha$ such that $\Delta_0 g = \Delta_1$, $\Delta_1 g = \Delta_0$ and $g^{-1}H_1 g = P_1$.

Let K denote the kernel of the representation of G_α on the set $\{\Delta_i | i=0,1,\ldots,n\}$. We show that K has a non-trivial Sylow p-subgroup M by showing that $Z(P) \leq K$; and determine, to a certain extent, the structure of M.

(7.5) Lemma: $C_P(H) \leq H$.

Proof: Suppose otherwise. Then $C_P(H)$ is non-trivial on Δ_0. Hence $C_G(H)$ is non-trivial on $\Omega - \Gamma$. Now if $g^{-1}Hg \leq G_{\alpha,\beta}$, then $\Gamma g \subseteq \Omega - \{\alpha,\beta\}$. Since $\Phi = \Gamma$, we have $\Gamma g = \Gamma$. So $g^{-1}Hg$ and H are conjugate in $G_{(\Omega-\Gamma)}$, and a fortiori in $G_{\alpha,\beta}$. Hence by (2.14), $N_G(H)$ is 2-transitive on $\Omega - \Gamma$. So $C_G(H)$ is transitive on $\Omega - \Gamma$. As $|\Omega - \Gamma| = 1 + q$, $C_G(H)$ has an element h of order prime to p, which is non-trivial on $\Omega - \Gamma$. By Wielandt [14] (4.5), $C_G(H)$ is semiregular on Γ. Hence h is trivial on Γ. The normal closure $\langle h \rangle^{N_G(H)}$ of h in $N_G(H)$ is thus transitive on $\Omega - \Gamma$ and trivial on Γ. So G is 3-transitive on Ω by (4.3). This is a contradiction.

An immediate corollary to (7.5) is

(7.6) Corollary: $Z(P) \leq H$, and $Z(P)$ is semiregular on Γ.

We get further information about $Z(P)$ by observing that $Z(P)$ normalises P_i for $i=0,\ldots,n$. If $g \in N_G(P_i)$, then $fx(P_i)g = fx(g^{-1}P_i g) = fx(P_i)$. So, if $g \in \bigcap_{i=0}^{n} N_G(P_i)$, then $\Delta_i g = \Delta_i$ for $i=0,\ldots,n$.

Hence $\bigcap_{i=0}^{n} N_G(P_i) \leq K$. In particular, $Z(P) \leq K$. So K has a non-trivial Sylow p-subgroup M, which we may assume to be contained in P.

(7.7) Lemma: The representations of M on the blocks Δ_i, $i=0,\ldots,n$, are similar as permutation groups. Also, $fx(M) = \{\alpha\}$.

Proof: By the Frattini argument, $G_\alpha = KN_{G_\alpha}(M)$. So $N_{G_\alpha}(M)$ is 2-transitive on the block set $\{\Delta_i | i = 0,\ldots,n\}$. Let $h_i \in N_{G_\alpha}(M)$ be chosen so that $\Delta_o h_i = \Delta_i$. Then the automorphism $m \mapsto h_i^{-1} m h_i$ of M induces the desired isomorphism $M^{\Delta_o} \cong M^{\Delta_i}$.

For the second part, $\{\alpha\} \subseteq fx(M) \subseteq fx(Z(P)) \cap fx(h_1^{-1} Z(P) h_1)$

$= \{\{\alpha\} \cup \Delta_o\} \cap \{\{\alpha\} \cup \Delta_1\} = \{\alpha\}$.

We continue with some general lemmas.

(7.8) Lemma: Let G be an arbitrary group of the form $G_o \times G_1$. Suppose that $G_2 \lhd G$ and $G_o \cap G_2 = G_1 \cap G_2 = 1$. Then $G_2 \leq Z(G)$.

Proof: $[G_i, G_2] \leq G_i \cap G_2 = 1$ for $i = 0,1$.

(7.9) Lemma: Let $G = G_o \times G_1$, and suppose that G has a set of subgroups $\{G_i | i = 0,\ldots,a\}$ such that $G = G_i \times G_j$ if $i \neq j$. Then $a \leq |G_o|$.

Proof: The theorem is trivially true for $a = 1$. If $a > 1$, the G_i's are isomorphic to one another. Also $G_i \cap G_j = 1$ if $i \neq j$. Let $S = \bigcup_{i=0}^{a} G_i$. Then $|S| = 1 + (a+1)(|G_o| - 1) \leq |G| = |G_o|^2$, from which the result follows.

We conclude this section with a numerical restriction on Ω which will imply that $\{\Omega, \mathcal{L}\}$ is a projective plane.

(7.10) Lemma: If $t = 1$ (i.e. $|\Omega| = 1 + q + q^2$) and $\mathcal{L} = \{\Lambda g | g \in G\}$, then $\{\Omega, \mathcal{L}\}$ is a projective plane.

Proof: The number of lines is $(1 + q + q^2)(q + q^2)/(1 + q)q$. Thus

$|\mathcal{L}| = |\Omega|$, so the plane is projective.

§8. Non-regularity Excluded.

In this section we show that H cannot act non-regularly on Γ. We assume the contrary. Take a point $\sigma \in \Gamma$ and write L for H_σ.

(8.1) Lemma: $fx(L)$ is a proper subplane of Ω.

Proof: Let $\gamma,\delta \in fx(L), \gamma \neq \delta$. Then $L \leq G_{\gamma,\delta}$. As L is a p-group we have $L \leq G_{(\Lambda(\gamma,\delta))}$ by the hypothesis of (5.1). Hence $\Lambda(\gamma,\delta) \subseteq fx(L)$. So $fx(L)$ is a subplane. Since $L \neq 1$, $fx(L) \neq \Omega$.

Now let Σ be the unique smallest subplane containing α,β and σ. Since G is transitive on triples of non-collinear points, $|\Sigma|$ is independent of the choice of α,β,σ. If α', β' are two points in Σ, choose σ' in Σ such that α', β', σ' is a non-collinear triple, and choose $g \in G$ such that $\alpha g = \alpha'$, $\beta g = \beta'$ and $\sigma g = \sigma'$. Then $\Sigma g = \Sigma(\alpha',\beta',\sigma') \subseteq \Sigma$. Hence G^Σ is strictly 2-transitive on Σ. If $\alpha' = \alpha$ and $\beta = \beta'$, we can choose g to be in H. So G^Σ admits $\Sigma - \Lambda$ as a Jordan set. Since $H_{\{\Sigma - \Lambda\}}$ acts transitively on $\Sigma - \Lambda$, this set has prime power cardinality. Finally, let R be a p-subgroup of $G_{\alpha,\beta}$ such that R^Σ is a Sylow p-subgroup of $G^\Sigma_{\alpha,\beta}$; and let S be a Sylow p-subgroup of $G_{\alpha,\beta}$ containing R. Then, if $R^\Sigma_{\{\Lambda\}}$ is non-trivial on Λ, we have $R_{\{\Lambda\}}$, and a fortiori $S_{\{\Lambda\}}$, non-trivial on Λ. But this contradicts the hypothesis of (5.1) which asserts that $S \leq G_{(\Lambda)}$. Hence we have

(8.2) Lemma: $\{G^\Sigma, \Sigma, \Sigma-\Lambda\}$ satisfies the hypothesis of (5.1).

(8.3) Theorem: H cannot act non-regularly on Γ.

Proof: Put $\mathcal{L}' = \{\Lambda g | g \in G_{\{\Sigma\}}\}$. Since $|\Sigma| < |\Omega|$ by (8.1), (8.2) implies

that $\{\Sigma,\mathcal{L}'\}$ has the structure of a projective space of dimension $d(\geq 2)$. So the non-collinear triple $\{\alpha,\beta,\sigma\}$ belongs to a projective plane which is a subplane of $\{\Omega,\mathcal{L}\}$. Hence axiom (2.12) is satisfied for $\{\Omega,\mathcal{L}\}$. As $\Sigma \neq \Omega$, axiom (2.13) is also satisfied for $\{\Omega,\mathcal{L}\}$. Thus $\{\Omega,\mathcal{L}\}$ is a projective space of dimension $d(\geq 3)$. In particular, $|\Omega| = 1 + q + \ldots + q^d$. But from (7.1), $|\Omega| = 1 + q + q^{2t}$. These two equalities imply $2t = d = 2$, contrary to $d \geq 3$. This establishes (8.3).

§9. The Regular Case.

At this stage our minimal counterexample to (5.1) is seen to satisfy: (a) G is strictly 2-transitive on Ω and admits Γ as a non-trivial Jordan set, (b) $\Phi = \Gamma$, (c) H acts regularly on Γ, and (d) a Sylow p-subgroup of $G_{\alpha,\beta}$ is a Sylow p-subgroup of $G_{(\Lambda)}$. Under these circumstances we show that $\{\Omega,\mathcal{L}\}$ is a projective plane.

Recall that we may choose P - a Sylow p-subgroup of G_α - to contain H and M, where M is a Sylow p-subgroup of the kernel of the action of G_α on $\{\Delta_i | i=0,\ldots,n\}$. Since $|G_\alpha : G_{\alpha,\beta}| = q + q^{2t}$ and $|P:P_\beta| = q$, P_β is a Sylow p-subgroup of $G_{\alpha,\beta}$. Hence $P_\beta \leq G_{(\Lambda)}$. As $H \leq P_\beta$, we have $H = P_\beta$. Hence, $M_\beta \leq H$. By the regularity of H on Γ, M_β must be semiregular on each Δ_i, $1 \leq i \leq n$. Furthermore, $M_{\beta,\gamma} = 1$ for all $\gamma \in \Gamma$. So $|M_\beta| = p^{r'} \leq q$. That is, $|M_{(\Delta_o)}| = p^{r'}$. Also $|M_{(\Delta_o \cup \Delta_i)}| = 1$, for $i \geq 1$. Since P acts regularly on Δ_o, we have $|M:M_{(\Delta_o)}| = p^{r''} \leq q$.

From (7.2), $N_G(M)$ is 2-transitive on the set $\{\Delta_i | i=0,\ldots,n\}$. Hence we have $|M_{(\Delta_i)}| = p^{r'}$ and $|M_{(\Delta_i \cup \Delta_j)}| = 1$ for $i,j=0,\ldots,n$ and $i \neq j$.

So the number of elements in the set $\bigcup_{i=0}^{n} M_{(\Delta_i)}$ is $1 + (q^{2t-1} + 1)(p^{r'} - 1) \leq |M| = p^{r'+r''}$. This inequality implies that $t = 1$. So $\{\Omega,\mathcal{L}\}$ is a projective plane by (7.10).

As this plane clearly admits all possible elations it is a Moufang plane, so that it can be co-ordinatised by a finite alternative division ring (Hall [7] Theorem (20.5.3)). By the Artin-Zorn Theorem ([7] (20.6.2)), such a ring is a field. Hence the plane is Desarguesian and so $PSL(3,q) \leq G$. So G is not, after all, a counterexample. This completes the proof of (5.1).

§10. A Variation.

It is possible to prove the following variation on (5.1) in a similar manner.

(10.1) Theorem: Let G be a strictly 2-transitive permutation group on a set Ω, which admits a non-trivial Jordan set Γ of prime power cardinality p^r. Suppose that a Sylow p-subgroup of $G_{(\Omega-\Gamma)}$ contains an abelian subgroup which is transitive on Γ. Then $\{\Omega,\mathcal{L}\}$ is the design of points and lines of projective space of dimension $d(\geq 2)$ over the field of $q = |\Lambda|-1$ elements, where $\mathcal{L} = \{\Lambda(\gamma,\delta) | \gamma,\delta\in\Omega,\gamma\neq\delta\}$ and $PSL(d+1,q) \leq G$.

Proceeding as for (5.1) we find that a minimal counterexample $\{G,\Omega,\Gamma\}$ to (10.1) satisfies $\Phi = \Gamma$. We will show that H acts regularly on Γ. Let $\gamma \in \Gamma$ and put $L = H_\gamma$.

(10.2) Lemma: $N_G(L)^\Lambda$ is 2-transitive on Λ.

Proof: Let H' be a conjugate of H which lies in $G_{\alpha,\beta}$. Since $\Phi = \Gamma$, $fx(H') = fx(H) = \Lambda$. So H' is also a Sylow p-subgroup of $G_{(\Lambda)}$. Hence H' is conjugate in $G_{\alpha,\beta}$ to H. By (2.14) $N_G(H)$ is 2-transitive on $fx(H)$. Let α',β' be any two distinct elements of Λ. Choose $g \in N_G(H)$ such that $\alpha g = \alpha'$, $\beta g = \beta'$. Then $g^{-1}Lg \leq H_{\gamma g}$. So $g^{-1}Lg = H_{\gamma g}$. Since H is transitive on Γ and $\gamma g \in \Gamma$, we can find $h \in H$ such that $\gamma gh = \gamma$. Then $h^{-1}g^{-1}Lgh = L$. So $gh \in N_G(L)$, $\Lambda gh = \Lambda$, $\alpha gh = \alpha'$ and $\beta gh = \beta'$.

We now study the fixed point set of L. We recall that, in the notation of §7, $\Delta_o = \Lambda - \{\alpha\}$, and that $\Delta_o,\Delta_1,\ldots,\Delta_n$ are the distinct images of Δ_o under the action of G_α. We index these sets so that $fx(L) \cap \Delta_i \neq \emptyset$ for $0 \leq i \leq a$, and $fx(L) \cap \Delta_i = \emptyset$ for $a < i \leq n$. Moreover, Δ_1 will be the set which contains γ.

(10.3) Lemma: $fx(L) = \{\alpha\} \cup \Delta_o \cup \Delta_1 \cup \cdots \cup \Delta_a$.

Proof: Since H is transitive on Γ, $N_H(L)$ is transitive on $\Gamma \cap fx(L)$ by (12.7). So $N_H(L)$ is transitive on the set $\{\Delta_i | 1 \leq i \leq a\}$. Hence, a is a power of p.

Let $\Delta_{i(0)}, \Delta_{i(1)},\ldots, \Delta_{i(b)}$ be those Δ_i's which are fixed (as sets) by $P_1(=P_{(\Delta_1)})$, where $i(0) = 0$, $i(1) = 1$. Since $H_1(=H_{\{\Delta_1\}})$ acts transitively on each of the blocks which it fixes, with the exception of Δ_o, P_1 acts transitively on $\Delta_{i(j)}$ if $0 \leq j \leq b$ and $j \neq 1$, by (7.4). Suppose that $i' = i(j)$ for some i' and j satisfying $2 \leq i' \leq a$, $2 \leq j \leq b$. Let $\delta \in fx(L) \cap \Delta_{i'}$, and let δ' be any other point of $\Delta_{i'}$. Since $P_1 \leq P_\gamma$, $P_1 \leq N_P(L)$. Since P_1 is transitive on $\Delta_{i'}$, $\delta h = \delta'$ for some $h \in P_1$. But then $\delta' \in fx(h^{-1}Lh) \cap \Delta_{i'}h = fx(L) \cap \Delta_{i'}$. So $\Delta_{i'} \subseteq fx(L)$. Since $N_H(L)$ is transitive on the set $\{\Delta_i | 1 \leq i \leq a\}$, we get the result in

this case.

The alternative is that none of the blocks Δ_i, $2 \leq i \leq a$, are fixed by P_1. These sets are then permuted among themselves by P_1. Hence p divides a - 1. As a is a power of p, we must have a = 1. By (10.2), we may choose an element $g \in N_G(L)$ such that $\alpha g = \beta$ and $\Delta_1 g = \Delta_1$. But then $2 \leq |(\{\alpha\} \cup \Delta_1) \cap (\{\alpha g\} \cup \Delta_1 g)| < |\Lambda|$ contradicting $\Phi = \Gamma$.

(10.4) Lemma: $N_G(L)$ is 2-transitive on $fx(L)$.

Proof: From (10.2) and (10.3) we obtain that $N_G(L)_{\{\Lambda\}}$ is 2-transitive on Λ and transitive on $fx(L) - \Lambda$. Choose g as in (7.4). Then $g^{-1}Lg \leq G_{(\Lambda)}$. So $h^{-1}g^{-1}Lgh \leq H$ for some $h \in G_{(\Lambda)}$. As L has more than $|\Lambda|$ fixed points, $h^{-1}g^{-1}Lgh = kLk^{-1}$ for some $k \in H$. So $ghk \in N_G(L)$ and $\Delta_o ghk = \Delta_1 hk \subseteq fx(L) - \Lambda$.

If we put $\Psi = fx(L)$, it is immediate that $\{G^{\Psi}, \Psi, \Psi - \Lambda\}$ satisfies the hypotheses of (10.1). If $|\Psi| < |\Omega|$, we see that $\{G,\Omega,\Gamma\}$ is not a counterexample as in §8. If $\Psi = \Omega$, then H is abelian. So H_1 and P_1 fixes all blocks $\Delta_o,\ldots,\Delta_n$. Since $P_1 \leq N_G(H_1)$ and $[P_1,H_1] \leq H_{(\Delta_1)} = 1$, we have $T = \langle P_1,H_1\rangle = P_1 \times H_1$. Put $T_i = T_{(\Delta_i)}$, $i = 0,1,\ldots,n$. Then T_i belongs to some conjugate of H. So $fx(T_i) = \{\alpha\} \cup \Delta_i$. Hence $T_1,\ldots,T_n$ have pairwise trivial intersection. We apply (7.9) to conclude the proof of (10.1).

Part III: Groups of Prime Degree.

§11. Exceptional Character Theory.

In this section we derive some general formulae involving induced characters, and we apply them to groups which have a self-centralising p-cycle whose normaliser has order 3p, where p is a prime.

First, let G be an arbitrary group, and let S be a subset of G which contains 1. S is a T.I.-set (trivial intersection set) if $S \cap S^g = 1$ for all $g \in G - N_G(S)$. In this case, if $x \in S - 1$, $g \in G$ and $x^g \in S$, then $g \in N_G(S)$.

(11.1) Lemma: Let S be a T.I.-set in a group G, and let $H = N_G(S)$. Let ζ be a generalised character of H which vanishes on $\bigcup_{g \in G} (S^g \cap H) - S$. Then ζ^G and ζ take the same values on S - 1. If, in addition, η is a generalised character of H which vanishes on $(H - S) \cup \{1\}$, then $\langle \zeta^G, \eta^G \rangle = \langle \zeta, \eta \rangle$.

Proof: Let $x \in S - 1$. If $\dot{\zeta}$ is defined as in (2.3), then $\dot{\zeta}(k^{-1}xk) = 0$ unless $k^{-1}xk \in S$ (i.e. $k \in H$); in which case $\dot{\zeta}(k^{-1}xk) = \zeta(k^{-1}xk) = \zeta(x)$. Hence $\zeta^G(x) = \frac{1}{|H|} \sum_{k \in H} \zeta(k^{-1}xk) = \zeta(x)$.

For the second part, $\langle \zeta^G, \eta^G \rangle = \frac{1}{|G|} \sum_{g \in G} \zeta^G(g)\overline{\eta^G(g)}$

$= \frac{1}{|G|} \sum_{g \in \bigcup_{h \in G} S^h - 1} \zeta^G(g)\overline{\eta^G(g)}$, since η^G vanishes on classes which do not meet S - 1.

$= \frac{1}{|H|} \sum_{g \in S-1} \zeta^G(g)\overline{\eta^G(g)}$

$= \frac{1}{|H|} \sum_{g \in S-1} \zeta(g)\overline{\eta(g)}$, by the first part of the lemma;

$= \frac{1}{|H|}\sum_{g\in H} \zeta(g)\overline{\eta(g)} = \langle\zeta,\eta\rangle.$

(11.2) Corollary: If S is a Hall subgroup of G and ξ is an arbitrary generalised character of H, then $\langle\xi^G,\eta^G\rangle = \langle\xi,\eta\rangle$.

For the remainder of this section we assume that P is a subgroup of prime order p, which is a Sylow p-subgroup of G, and for which $|N_G(P):P| = 3$ and $C_G(P) = P$. The P is clearly a T.I.-set in G. We put $H = N_G(P)$. Then the character table of H is as follows:

	1	y	y^2	x	...	x^{j_s}	...	x^{j_t}
λ_{11}	1	1	1	1	...	1	...	1
λ_{12}	1	ε	ε^2	1	...	1	...	1
λ_{13}	1	ε^2	ε	1	...	1	...	1
λ_{21}	3	0	0	n_{11}		n_{1s}		n_{1t}
	.	.	.		.	.	.	
λ_{2r}	3	0	0	n_{r1}	...	n_{rs}	...	n_{rt}
	.	.	.		.	.	.	
λ_{2t}	3	0	0	n_{t1}	...	n_{ts}	...	n_{tt}

where y is an element of order 3 in H and represents one class of 3-elements, while y^2 represents the other. $\langle x\rangle = P$. ε and ω are primitive cube and p^{th} roots of unity in $\mathbb{C}$, respectively. i is a primitive cube root of unity mod p, and $\{j_1(=1),j_2,\ldots,j_t\}$ is a transversal of $\langle i\rangle$ in the multiplicative group of units mod p. So $t = (p-1)/3$. $\omega_{rs} = \omega^{j_r j_s}$ and $n_{rs} = \omega_{rs} + \omega_{rs}^{i} + \omega_{rs}^{i^2}$.

Since the subspace of characters which vanish on $(H - P) \cup \{1\}$ has codimension 3 in $\mathrm{char}(G)\otimes_{\mathbb{Z}}\mathbb{C}$ the set $\{\lambda_1,\ldots,\lambda_t\}$, where $\lambda_r = \lambda_{2r} - (\lambda_{11} + \lambda_{12} + \lambda_{13})$, $r=1,\ldots,t$, is a basis of this subspace.

Let $\theta_r = \lambda_r^G$. From (11.1) we see that θ_r coincides with λ_r on $P - 1$, and vanishes on the conjugacy classes which do not meet $P - 1$. Also, $\langle\theta_r,\theta_r\rangle = \langle\lambda_r,\lambda_r\rangle = 4$. By (2.5), $\langle\chi_0,\theta_r\rangle = \langle\lambda_{11},\lambda_r\rangle = -1$, for all r. Hence each θ_r is the sum of four distinct generalised irreducible characters of G, one of which is $-\chi_0$.

Again from (11.1), we get $\langle\theta_r,\theta_s\rangle = 3$ if $1 \leq r < s \leq t$. By choosing the notation appropriately we may assume that $\theta_i = -\chi_0 + \tilde{\chi}_1 + \tilde{\chi}_2 + \tilde{\phi}_i$, $i=1,2$, where χ_1, χ_2, ϕ_1 and ϕ_2 are distinct irreducible characters. Suppose that $t > 2$. Since p is a prime, this implies that $t \geq 4$. There are two possible forms for θ_3, namely $-\chi_0 + \tilde{\chi}_1 + \tilde{\chi}_2 + \tilde{\phi}_3$ or $-\chi_0 + \tilde{\chi}_1 + \tilde{\phi}_1 + \tilde{\phi}_2$, where ϕ_3 is an irreducible character distinct from $\chi_0,\chi_1,\chi_2,\phi_1$ and ϕ_2.

In the second case we put

$\theta_4 = -\chi_0 + m_1\tilde{\chi}_1 + m_2\tilde{\chi}_2 + m_3\tilde{\phi}_1 + m_4\tilde{\phi}_2 + \theta$, where m_1,m_2,m_3 and m_4 are integers and θ is an element of $\mathrm{char}(G)$ which does not involve $\chi_0,\chi_1,\chi_2,\phi_1$ or ϕ_2. We have the following equations

$$m_1^2 + m_2^2 + m_3^2 + m_4^2 + \langle\theta,\theta\rangle = 3$$

$$m_1 + m_2 + m_3 = 2$$

$$m_1 + m_2 + m_4 = 2$$

$$m_1 + m_3 + m_4 = 2.$$

So $m_2 = m_3 = m_4$. Hence $m_1^2 + 3m_2^2 + \langle\theta,\theta\rangle = 3$. $m_2 = 0$ implies $m_1 = 2$, and this is clearly impossible. Thus $m_2 = 1$, $m_1 = 0$ and $\theta = 0$. As

this argument determines θ_r for $4 \leq r \leq t$, we must have $t = 4$. Let a, b, c and d denote the integers $\tilde{\chi}_1(1)$, $\tilde{\chi}_2(1)$, $\tilde{\phi}_1(1)$ and $\tilde{\phi}_2(1)$. The equations $\theta_r(1) = 0$, $r = 1,2,3$ and 4 become

$$\begin{aligned} -1 + a + b + c &= 0 \\ -1 + a + b + d &= 0 \\ -1 + a + c + d &= 0 \\ -1 + b + c + d &= 0 \end{aligned}$$

But then $a = b = c = d = \frac{1}{3}$ - a contradiction.

Thus, there are distinct irreducible characters $\chi_0, \chi_1, \chi_2, \phi_1, \ldots, \phi_t$ such that

$$\theta_r = -\chi_0 + \tilde{\chi}_1 + \tilde{\chi}_2 + \tilde{\phi}_r \text{ for } r = 1,2,\ldots,t$$

Evaluating these characters at x we get

$$n_{r1} - 3 = -1 + \tilde{\chi}_1(x) + \tilde{\chi}_2(x) + \tilde{\phi}_r(x), \quad r = 1,2,\ldots,t.$$

If we put $\tilde{\chi}_1(x) = -1 + \delta_1$ and $\tilde{\chi}_2(x) = -1 + \delta_2$, where $\delta_1, \delta_2 \in \mathbb{C}$, then $\tilde{\phi}_r(x) = n_{r1} - \delta_1 - \delta_2$. Let $\phi_{t+1}, \ldots, \phi_{t'}$ denote the remaining irreducible characters of G. Then $p = |C_G(x)| = 1 + (\delta_1 - 1)(\bar{\delta}_1 - 1) + (\delta_2 - 1)(\bar{\delta}_2 - 1) + \sum_{r=1}^{t} (n_{r1} - \delta_1 - \delta_2)(\bar{n}_{r1} - \bar{\delta}_1 - \bar{\delta}_2) + \sum_{r=t+1}^{t'} \phi_r(x)\overline{\phi_r(x)}$.

$$= p + \delta_1\bar{\delta}_1 + \delta_2\bar{\delta}_2 + t(\delta_1 + \delta_2)(\bar{\delta}_1 + \bar{\delta}_2) + \sum_{r=t+1}^{t'} \phi_r(x)\overline{\phi_r(x)}.$$

Hence $\delta_1 = \delta_2 = \phi_r(x) = 0$ for $r = t+1,\ldots,t'$; $\tilde{\chi}_1(x) = \tilde{\chi}_2(x) = -1$ and $\tilde{\phi}_r(x) = n_{r1}$ for $r=1,\ldots,t$. Similarly, we find

$$\left.\begin{aligned} \tilde{\chi}_1(x^{j_s}) &= \tilde{\chi}_2(x^{j_s}) = -1 \\ \tilde{\phi}_r(x^{j_s}) &= \begin{cases} n_{rs}, & 1 \leq r \leq t \\ 0, & t+1 \leq r \leq t' \end{cases} \end{aligned}\right\} \quad s = 1,\ldots,t.$$

Put $\tilde{\chi}_1(1) = -n_1$, $\tilde{\chi}_2(1) = -n_2$, $\tilde{\chi}_1(g) = -u(g)$ and $\tilde{\chi}_2(g) = -v(g)$ where g

is an arbitrary element of G which is not conjugate to an element of P. Then we have the following table of generalised irreducible characters, which for each irreducible character χ contains either $+\chi$ or $-\chi$, but not both.

	1	x	...	x^{j_t}	g
χ_0	1	1	...	1	1
$-\tilde{\chi}_1$	n_1	1	...	1	$u(g)$
$-\tilde{\chi}_2$	n_2	1	...	1	$v(g)$
$\tilde{\phi}_1$	$1+n_1+n_2$	n_{11}	...	n_{1t}	$1+u(g)+v(g)$
.	.	.	.	.	.
$\tilde{\phi}_t$	$1+n_1+n_2$	n_{t1}	...	n_{tt}	$1+u(g)+v(g)$
ϕ_{t+1}		0	...	0	
	.	.	.	.	.
$\phi_{t'}$		0	...	0	

(11.4) Lemma: $n_1 \equiv n_2 \equiv 1$ and $\phi_r(1) \equiv 0 \bmod p$, for $r = t+1,\ldots,t'$.

Proof: The inner product $\langle \chi_{0_P}, \zeta_P \rangle$ is an integer for any $\zeta \in \text{char } G$. Taking ζ to be $-\tilde{\chi}_1, -\tilde{\chi}_2$ and $\phi_r (t+1 \leq t \leq t')$, we find that $(n_1+p-1)/p$, $(n_2+p-1)/p$ and $\phi_r(1)/p$ are integers.

(11.5) Corollary: $1 + n_1 + n_2 \equiv 3 \bmod p$.

§12. Bounds for n_1 and n_2.

Throughout §12-13 and §15-17, G will denote a primitive insoluble permutation group on a set Ω, where $|\Omega| = p$ is a prime, and

a Sylow p-subgroup P of G has index 3 in its normaliser. Clearly $C_G(P) = P$. So the results of §11 apply, with $H = N_G(P)$.

(12.1) Theorem: G is a simple group which is 2-transitive on Ω.

Proof: For 2-transitivity we appeal to Burnside's prime degree Theorem. Now suppose that N is a proper normal subgroup of G. Then N is transitive on Ω. So $P \leq N$. By the Frattini argument, $G = N.N_G(P)$. As N is a proper subgroup, $N_G(P) \cap N$ is properly contained in $N_G(P)$ and contains P. Hence $N_G(P) = P$. By the Burnside p-complement Theorem, N has a normal p-complement K. Since K is characteristic in N, it is normal in G. But K is clearly not transitive. Thus, $K = 1$. This implies that $N = P$ and $G = N_G(P)$ - a soluble group. From this contradiction we see that G is simple.

From (2.8) we see that $\chi^{[p-1,1]}_G$ is an irreducible character of G of degree p-1. Comparing p-1 with the degrees in (11.3) and using the restrictions in (11.4) and (11.5), we may take $\chi^{[p-1,1]}_G$ to be χ_1, without loss of generality. Thus $\chi_1 = \tilde{\chi}_1$ and $n_1 = 1-p$. Moreover, for a p'-element $g \in G$, $u(g) = 1 - \alpha_1(g)$.

(12.2) Lemma: The integers n_2 and $1 + n_1 + n_2$ are positive.

Proof: Suppose that $n_2 < 0$. Then $n_2 = 1 - kp$, where $k > 0$ by (12.1) and (11.3). Let $\psi = \chi^{[p-2,1^2]}_{G_t}$. Then

$$\psi = a_1\chi_1 + a_2\tilde{\chi}_2 - a_3\Big(\sum_{r=1}^{t}\tilde{\phi}_r\Big) + \sum_{r=t+1}^{t'} b_r\phi_r, \tag{12.3}$$

for some non-negative integers $a_1, a_2, a_3, b_{t+1}, \ldots, b_{t'}$, since $\langle\psi, \chi_0\rangle = 0$ by (2.8). Evaluating (12.3) at x, we get $-a_1 - a_2 + a_3 = 1$. Thus $a_3 = 1 + a_1 + a_2$. Now evaluating (12.3) at 1, we get

$$a_1(p-1) + a_2(kp-1) + (a_1+a_2+1)((k+1)p-3)(p-1)/3 \leq (p-1)(p-2)/2.$$

This implies that $a_1 = a_2 = 0$. So $(k+1)p-3 \leq 3p/2-3$. Hence $k = 0$, contrary to our assumption.

So $n_2 = kp + 1$ for some positive integer k. But then $1 + n_1 + n_2 = (k-1)p+3 > 0$.

In our character table (11.3), we now have $\chi_2 = \tilde{\chi}_2$ and $\phi_r = \tilde{\phi}_r$ for $r = 1,2,\ldots,t$.

(12.4) Lemma: $-n_1n_2(1 + n_1 + n_2)$ is a perfect square.

Proof: Let g be an involution. Write $u(g) = n_1 - \ell_1$ and $v(g) = n_2 - \ell_2$. From (2.6) we see that

$$\#(g^{\cdot}g^{\cdot} = x) = \frac{|G|}{|C_G(g)|^2}\{1+\frac{(n_1-\ell_1)^2}{n_1}+\frac{(n_2-\ell_2)^2}{n_2}-\frac{(1+n_1+n_2-\ell_1-\ell_2)^2}{1+n_1+n_2}\}$$

$$= \frac{|G|}{|C_G(g)|^2}\{\frac{\ell_1^2}{n_1}+\frac{\ell_2^2}{n_2}-\frac{(\ell_1+\ell_2)^2}{1+n_1+n_2}\} = \frac{|G|}{|C_G(g)|^2}\cdot\frac{\ell_1^2n_2(1+n_2)-2\ell_1\ell_2n_1n_2+\ell_2^2n_1(1+n_1)}{n_1n_2(1+n_1+n_2)}$$

Now if g_1, g_2 are two conjugates of g for which $g_1g_2 = x$, then $g_2g_1 = x^{-1}$. So $g_1 \in N_G(P)$. Since $N_G(P)$ has odd order, we must have $\#(g^{\cdot}g^{\cdot}=x)=0$. Thus,

(12.5) $$\ell_1^2n_2(1+n_2) - 2\ell_1\ell_2n_1n_2 + \ell_2^2n_1(1+n_1) = 0.$$

By (12.1), g is not in the kernel of χ_1 or χ_2. Hence ℓ_1 and ℓ_2 are non-zero. An inspection of (11.3) shows that no other irreducible characters are algebraically conjugate to χ_1 or χ_2. Hence χ_1 and χ_2 are integer-valued. So ℓ_1 and ℓ_2 are non-zero integral solutions of (12.5). We conclude that the discriminant $n_1^2n_2^2 - n_1n_2(1+n_1)(1+n_2)$ is a perfect square.

In view of (12.2) we write

$$(12.6)\qquad \Psi = a_1\chi_1 + a_2\chi_2 + a_3\Big(\sum_{r=1}^{t}\phi_r\Big) + \sum_{r=t+1}^{t'} b_r\phi_r,$$

where $a_1, a_2, a_3, b_{t+1}, \ldots, b_{t'}$ are non-negative integers. Evaluating (12.6) at x, we get

$$(12.7)\qquad a_2 = 1 + a_1 + a_3$$

Since $a_2 \geq 1$, the degree of χ_2 is not greater than the degree of ψ, which is $(p-1)(p-2)/2$. We find, therefore,

(12.8) Lemma: $k \leq (p-3)/2$.

We shall find it convenient at a later stage to have considered the possibilities k=1 and k=2.

(12.9) Lemma: (i) If k=1, then p=7.

(ii) If k=2, then p=7 or 13.

Proof: For k=1, G is a simple group with an irreducible character ϕ_1 of degree 3. So the primes dividing $|G|$ must be ≤ 14 (see Blichfeldt [1]). Since p divides $|G|$ and 6 divides p-1, we have p=7 or 13. But for p=13, $(p-1)(p+1).3 = 36.14$, which is not a perfect square. Hence p=7.

For k=2, we have $-n_1 = p-1$, $n_2 = 2p+1$ and $1 + n_1 + n_2 = p + 3$. The highest common factor of n_1 and n_2 is $(n_1, n_2) = (p-1, 2p+1) = (p-1, 3) = 3$. Similarly, $(n_1, 1+n_1+n_2) = (p-1, 4) = 2$ or 4, and $(n_2, 1+n_1+n_2) = (-5, p+3) = 1$ or 5. From (12.4) we have the following possibilities:

	(i)	(ii)	(iii)	(iv)
p-1	$3A^2$	$6A^2$	$3A^2$	$6A^2$
2p+1	$3B^2$	$3B^2$	$15B^2$	$15B^2$
p+3	C^2	$2C^2$	$5C^2$	$10C^2$

where A, B and C are relatively prime in pairs, except in cases (i) and

(iii), when (A,C) = 2. Since $p \equiv 1 \bmod 3$, cases (ii) and (iii) imply that $C^2 \equiv 2 \bmod 3$. Since 2 is not a square mod 3, cases (ii) and (iii) cannot occur.

In case (i), $5p = 9B^2 - C^2$. So 3B+C = 5p or p and 3B-C=1 or 5. Hence C = (5p-1)/2 or (p-5)/2. Substituting in $p+3 = C^2$, the first value gives p = 1 or $-\frac{11}{25}$ and the second p = 1 or 13. So in case (i) we have p = 13, A = 2, B = 3 and C = 4.

In case (iv) we have $5C^2 - 3A^2 = 2$, $4C^2 - 3B^2 = 1$ and $p = 2A^2 + 5B^2$. Taking equivalences modulo 7 we find that the possible solutions of the first equation are

C	0	±1
A	±2	±1

and of the second equation

C	0	±1	±3
B	±3	±1	0

. If $A \equiv \pm 1$ and $B \equiv \pm 1 \bmod 7$, then $p \equiv 0 \bmod 7$. So p = 7. It remains to show that the case $C \equiv 0 \bmod 7$ cannot occur. Suppose it does, and write C = 7D. Then $(14D)^2 - 3B^2 = 1$.

The integral solutions of $X^2 - 3Y^2 = 1$ are the pairs of integers x,y for which $x + y\sqrt{3} = \pm(2 + \sqrt{3})^n$, for some $n \in \mathbb{Z}$, since $2 - \sqrt{3} = (2+ \sqrt{3})^{-1}$. Thus, $[x,y] = [1,0]\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}^n$, $n \in \mathbb{Z}$. Taking congruences modulo 14, we find that $[x,y] \equiv [1,0],[2,1],[7,4],[12,1],[13,0],[12,13],[7,10]$ or $[2,13]$. So there is no integral solution x,y of $X^2 - 3Y^2 = 1$ in which $x \equiv 0 \bmod 14$. Hence $(14D)^2 - 3B^2 = 1$ has no integral solution.

(12.10) Lemma: In the decomposition (12.6) of ψ, $a_3 = 0$.

Proof: Evaluating (12.6) at 1, we get

$$(12.11)\quad a_1(p-1) + a_2(kp+1) + a_3((k-1)p+3)(p-1)/3 + \sum_{r=t+1}^{t'} b_r\phi_r(1) = (p-1)(p-2)/2.$$

If $a_3 \geq 2$, then $4((k-1)p+3) \leq 3(p-2)$. So k=1. By (12.9), p=7. But

then $15 \geq 6a_1 + 8a_2 + 6a_3$. This is impossible, since $a_2 = 1 + a_1 + a_3 \geq 3$.

If $a_3 = 1$ we may rearrange (12.11) to obtain

$$(12.12) \quad a_1 p(k+1) + 2(kp+1) + \sum_{r=t+1}^{t'} b_r \phi_r(1)$$

$$= (p-1)((5-2k)p-12)/6.$$

As the left-hand side of (12.12) is a positive integer, we must have $k \leq 2$. $k=1$ implies $p=7$, as before. Substituting in (12.12), we get $14a_1 + 16 \leq 9$. $k=2$ implies $p=7$ or 13, by (12.9). In this case, $p=7$ makes the right-hand side of (12.12) negative, while $p=13$ yields the inequality $54 \leq 2$. This concludes the proof of (12.10).

§13. $k=(p-3)/2$.

In this case $n_2 = p(p-3)/2 + 1 = (p-1)(p-2)/2$. From (12.7) we see that $\psi = \chi_2$. Moreover, for $1 \leq r \leq t$, ϕ_r has degree $(p-2)(p-3)/2$.

(13.1) Lemma: $p-3 = m^2$, for some integer m.

Proof: By (12.4), $(p-1).\{(p-1)(p-2)/2\}.\{(p-2)(p-3)/2\}$ is a perfect square. The result follows.

(13.2) Lemma: The functions ϕ_r and $(\alpha_1 - 2)(\alpha_1 - 3)/2 - \alpha_2$ coincide on p'-elements of G, for $1 \leq r \leq t$.

Proof: We already know that $u(g) = 1 - \alpha_1(g)$ for any p'-element g. Since $\chi_2 = \psi$, $v(g) = (\alpha_1(g)-1)(\alpha_1(g)-2)/2 - \alpha_2(g)$. Hence $\phi_r(g) = 1 + u(g) + v(g) = (\alpha_1(g) - 2)(\alpha_1(g) - 3)/2 - \alpha_2(g)$.

Put $\xi = \chi_G^{[p-2,2]}$.

(13.3) Lemma: $\langle \chi_2, \xi \rangle = \langle \phi_r, \xi \rangle = 0$, for $1 \leq r \leq t$.

Proof: Since χ_2 is irreducible and has degree greater than $p(p-3)/2$, which is the degree of ξ, $\langle \chi_2, \xi \rangle = 0$. Since ξ is a rational character,

$\langle\phi_r,\xi\rangle \neq 0$ for some r satisfying $1 \leq r \leq t$ implies that $\langle\phi_r,\xi\rangle \neq 0$ for all such r, since $\phi_1,\ldots,\phi_t$ are algebraically conjugate. If this is so, then

$(p-1)(p-2)(p-3)/6 \leq p(p-3)/2$. So $p \leq 5$. Since this is impossible, we have $\langle\phi_r,\xi\rangle = 0$ for $r=1,\ldots,t$.

As G is 2-transitive on Ω, (2.8) implies that

(13.4) Lemma: $\langle\chi_0,\xi\rangle = 0$.

(13.5) Lemma: $\langle\chi_1,\xi\rangle = 0$.

Proof: From (13.3) and (13.4) we see that

$\xi = a\chi_1 + \sum_{r=t+1}^{t'} c_r\phi_r$, where $a,c_{t+1},\ldots,c_t$, are non-negative integers.

Thus $0 = \xi(x) = -a$. So $a = 0$.

(13.6) Theorem: G is 3-transitive on Ω.

Proof: Let G have r+4 orbits in its natural action on Ω^3. Since an element $g \in G$ has $\alpha_1(g)^3$ fixed points in Ω^3, we have $\sum_G \alpha_1^3 = (r+4)|G|$.

But $0 = \langle\chi_1,\chi_2+\xi\rangle.|G| = \sum_G(\alpha_1-1)(\alpha_1^2-3\alpha_1+1)$

$$= \sum_G\alpha_1^3 - 4\sum_G\alpha_1^2 + 4\sum_G\alpha_1 - \sum_G 1 = (r-1)|G|.$$

So r=1, and G has just one orbit on ordered triples of distinct elements from Ω.

Let α,β and γ be three distinct elements from Ω, and let $\Delta = \Omega - \{\alpha,\beta,\gamma\}$. Let ℓ,m and n be the number of orbits in Δ of the groups $G_{(\alpha,\beta,\gamma)}$, $G_{\{\alpha,\beta\}} \cap G_\gamma$ and $G_{\{\alpha,\beta,\gamma\}}$, respectively. By (13.6), ℓ,m and n are independent of the choice of α,β and γ.

(13.7) Lemma: (i) $\sum_G\alpha_1^4 = (\ell + 14).|G|$;

(ii) $\sum_G\alpha_1^2\{\alpha_1(\alpha_1-1)/2+\alpha_2\} = (m+5).|G|$;

(iii) $\sum_G\alpha_1\{\alpha_1(\alpha_1-1)(\alpha_1-2)/6+\alpha_1\alpha_2+\alpha_3\} = (n+1).|G|$.

Proof: (i) Consider the natural action of G on Ω^4. By (13.6) there are 14 orbits of quadruples, whose elements are not all distinct, obtained as follows

(a) One of type [4], with representative $(\alpha,\alpha,\alpha,\alpha)$;

(b) Four of type [3.1], typical representative $(\alpha,\alpha,\alpha,\beta)$;

(c) Three of type $[2^2]$, typical representative $(\alpha,\alpha,\beta,\beta)$;

(d) Six of type $[2.1^2]$, typical representative $(\alpha,\alpha,\beta,\gamma)$.

The map $\Delta' \mapsto \{(\alpha g,\beta g,\gamma g,\delta' g) | \delta' \in \Delta', g \in G\}$ establishes a bijection from the set of orbits of $G_{(\alpha,\beta,\gamma)}$ in Δ to the set of remaining orbits of G in Ω^4.

(ii) In this case we consider the action of G on $\Omega^2 \times \Omega^{\{2\}}$. There are 5 orbits with representatives $(\alpha,\alpha,\{\alpha,\beta\})$, $(\alpha,\beta,\{\alpha,\beta\})$, $(\alpha,\alpha,\{\beta,\gamma\})$, $(\alpha,\beta,\{\alpha,\gamma\})$ and $(\alpha,\beta,\{\beta,\gamma\})$. The quadruples in the remaining orbits are quadruples of four distinct points. The map $\Delta' \mapsto \{(\delta' g,\gamma g,\{\alpha g,\beta g\}) | \delta' \in \Delta', g \in G\}$ gives a bijection from the set of orbits of $G_{\{\alpha,\beta\}} \wedge G_\gamma$ in Δ to the set of remaining orbits of G in $\Omega^2 \times \Omega^{\{2\}}$.

(iii) Here we consider the action of G on $\Omega \times \Omega^{\{3\}}$. The map $\Delta' \mapsto \{(\delta' g,\{\alpha g,\beta g,\gamma g\}) | \delta' \in \Delta', g \in G\}$ gives a bijection from the set of orbits of $G_{\{\alpha,\beta,\gamma\}}$ in Δ to the set of orbits of G in $\Omega \times \Omega^{\{3\}}$, with the orbit containing $(\alpha,\{\alpha,\beta,\gamma\})$ excluded.

In its action on each of the three sets Ω^4, $\Omega^2 \times \Omega^{\{2\}}$ and $\Omega \times \Omega^{\{3\}}$, an element g has exactly $\alpha_1(g)^4$, $\alpha_1(g)^2\{\alpha_1(g)(\alpha_1(g)-1)/2 + \alpha_2(g)\}$ and $\alpha_1(g)\{\alpha_1(g)(\alpha_1(g)-1)(\alpha_1(g)-2)/6 + \alpha_1(g)\alpha_2(g) + \alpha_3(g)\}$ fixed points, respectively. The result then follows from (2.7).

(13.8) Lemma: $\ell = m$.

Proof: Since $\langle \chi_2, \phi_1 \rangle = 0$ and $\langle \chi_2, \xi \rangle = 0$, we have $0 = \langle \chi_2, \phi_1 + \xi \rangle . |G|$

$= \sum_G \{(\alpha_1 - 1)(\alpha_1 - 2)/2 - \alpha_2\}\{\alpha_1/2 + (\alpha_1 - 2)/2\}\{\alpha_1 - 3\} - |G|\{(p-1).3 - (-1).3\}/3p$

$= \sum_G \alpha_1^2\{(\alpha_1 - 1)(\alpha_1 - 2)/2 - \alpha_2\} - 4|G| . \langle \chi_1, \chi_2 \rangle - |G| . \langle \chi_0, \chi_2 \rangle - |G| .$

Thus

$$(13.9) \qquad \sum_G \alpha_1^2\{(\alpha_1 - 1)(\alpha_1 - 2)/2 - \alpha_2\} = |G| .$$

Adding this equation to the equation in (13.7) (ii) we get

$$\sum_G \alpha_1^2(\alpha_1 - 1)^2 = (m+6)|G| .$$

On the other hand, $\sum_G \alpha_1^2(\alpha_1 - 1)^2$

$= \sum_G \alpha_1^4 - 2\sum_G \alpha_1^3 + \sum_G \alpha_1^2 = (\ell + 14 - 10 + 2).|G| = (\ell + 6).|G| .$

Hence, $\ell = m$.

(13.10) Lemma: $\ell = n$.

Proof: As $G_{(\alpha,\beta,\gamma)} \leq G_{\{\alpha,\beta\}} \cap G_\gamma$, every orbit of $G_{\{\alpha,\beta\}} \cap G_\gamma$ in Δ is a union of orbits of $G_{(\alpha,\beta,\gamma)}$. Since $\ell = m$, every orbit of $G_{\{\alpha,\beta\}} \cap G_\gamma$ is an orbit of $G_{(\alpha,\beta,\gamma)}$. Similarly, each orbit of $G_{\{\alpha,\gamma\}} \cap G_\beta$ in Δ is an orbit of $G_{(\alpha,\beta,\gamma)}$. Because of 3-transitivity, $G_{\{\alpha,\beta,\gamma\}} = \langle G_{\{\alpha,\beta\}} \cap G_\gamma, G_{\{\alpha,\gamma\}} \cap G_\beta \rangle$. Hence every orbit of $G_{\{\alpha,\beta,\gamma\}}$ in Δ is an orbit of $G_{(\alpha,\beta,\gamma)}$. Thus, $\ell = n$.

(13.1) Lemma: $\langle \chi_1, \zeta \rangle = 0$ where $\zeta = \chi^{[p-3,1^3]}_G$.

Proof: $\langle \chi_1, \zeta \rangle . |G|$

$= \sum_G (\alpha_1 - 1)\{(\alpha_1 - 1)(\alpha_1 - 2)(\alpha_1 - 3)/6 - (\alpha_1 - 1)\alpha_2 + \alpha_3\}$

$= \sum_G (\alpha_1 - 1)\{\alpha_1(\alpha_1 - 1)(\alpha_1 - 2)/6 + \alpha_1\alpha_2 + \alpha_3 - (\alpha_1 - 1)(\alpha_1 - 2)/2 + \alpha_2 - 2\alpha_1\alpha_2\}$

$= n.|G| - \langle \chi_1, \chi_2 \rangle . |G| - 2\sum_G \alpha_1(\alpha_1 - 1)\alpha_2$, from (13.7) (iii),

$$= n.|G| + 2\sum_G \alpha_1(\alpha_1-1)\{(\alpha_1-1)(\alpha_1-2)/2-\alpha_2\} - \sum_G \alpha_1(\alpha_1-1)^2(\alpha_1-2),$$

$$= n.|G| + 2\sum_G \alpha_1^2\{(\alpha_1-1)(\alpha_1-2)/2-\alpha_2\} - 2\langle \chi_0+\chi_1, \chi_2\rangle |G|$$

$$- \sum_G \alpha_1^4 + 4\sum_G \alpha_1^3 - 5\sum_G \alpha_1^2 + 2\sum_G \alpha_1$$

9/ $= \{n + 2 - (\ell + 14) + 20-10+2\}.|G|$, from (13.6) and (13.7) (i)

$=(n-\ell)|G|=0$, by (13.10).

(13.12) Lemma: $\zeta = \sum_{r=1}^{t} \phi_r$.

Proof: $\langle \chi_0, \zeta\rangle = 0$ by 3-transitivity and (2.8). $\langle \chi_1, \zeta\rangle = 0$ by (13.11). So we may write $\zeta = a\chi_2 + a'(\sum_{r=1}^{t} \phi_r) + \sum_{r=t+1}^{t'} c_r\phi_r$, where $a, a', c_{t+1}, \ldots, c_{t'}$ are non-negative integers. Evaluating at the p-element x, we get $-1 = \zeta(x) = a - a'$. Hence $a' \geq 1$. Now evaluating at 1, we get

$$(p-1)(p-2)(p-3)/6 = a(p-1)(p-2)/2 + a'\{(p-2)(p-3)/2\}\{(p-1)/3\} + \sum_{r=t+1}^{t'} c_r\phi_r(1).$$

Thus, $a'=1$, $a=c_{t+1} = \ldots = c_{t'} = 0$.

If we evaluate ζ at a p'-element g, we get

$$(\alpha_1(g)-1)(\alpha_1(g)-2)(\alpha_1(g)-3)/6 - (\alpha_1(g)-1)\alpha_2(g) + \alpha_3(g)$$

$$= \{(p-1)/3\}\{(\alpha_1(g)-2)(\alpha_1(g)-3)/2 - \alpha_2(g)\}.$$

So we get the equation

(13.13) $(p-\alpha_1(g))(\alpha_1(g)-2)(\alpha_1(g)-3) = 2\alpha_2(g)(p-3\alpha_1(g)+2) + 6\alpha_3(g)$.

(13.14) Lemma: $p-1 = 2.3^u$, for some integer u.

Proof: Let q be a prime dividing p-1, and let g be an element of order q. Then $\alpha_1(g) \neq 0$ and q divides $p-\alpha_1(g)$. Hence q divides $\alpha_1(g)-1$. If $q > 3$, then $\alpha_1(g) = 1$ or $\alpha_1(g) > 4$. So the left-hand side of (13.13) is non-zero. But the right-hand side is clearly zero, if $q > 3$. Thus, only the primes 2 and 3 divide p-1.

Since p-3 is a perfect square, by (13.1), it is divisible by 4. So 4 does not divide p-1.

We now use (13.13) to find the possible cycle-structure of involutions, elements of order 3 and elements of order 6 in G. We recall that $p = m^2 + 3$.

(13.15) Lemma: Let g be an element of G. Then

(i) If g is an involution, $\alpha_1(g) = m+1$, $\alpha_2(g)=(m^2-m+2)/2$;

(ii) If g has order 3, $\alpha_1(g)=1$ or 4, $\alpha_3(g)=(p-1)/3$ or $(p-4)/3$;

(iii) If g has order 6, $\alpha_1(g)=0$, $\alpha_2(g)=2$, $\alpha_3(g)=1$, $\alpha_6(g)=0$ and $p=7$.

Proof: (i) If g is an involution, $\alpha_3(g)=0$ and $p=\alpha_1(g)+2\alpha_2(g)$. Thus $\alpha_1(g) \neq 0$ or p, and (13.13) yields

$$(\alpha_1(g)-2)(\alpha_1(g)-3) = p-3\alpha_1(g) + 2.$$

Hence,

$$\alpha_1(g)^2-2\alpha_1(g)-(p-4) = 0.$$

That is,

$$\{\alpha_1(g)+(m-1)\}\{\alpha_1(g)-(m+1)\} = 0.$$

So $\alpha_1(g) = m+1$, as required.

(ii) If g has order 3, then $\alpha_2(g) = 0$ and $p = \alpha_1(g)+3\alpha_3(g)$.

From (13.13) we get

$$(\alpha_1(g)-2)(\alpha_1(g)-3) = 2.$$

That is,

$$(\alpha_1(g)-1)(\alpha_1(g)-4) = 0.$$

So $\alpha_1(g) = 1$ or 4.

(iii) Let g be an element of order 6. Then $\alpha_1(g)+3\alpha_3(g) = \alpha_1(g^3) = m+1$ and $\alpha_1(g)+2\alpha_2(g) = \alpha_1(g^2) = 1$ or 4. If $\alpha_2(g) = 0$, then $\alpha_1(g) \equiv 1 \mod 3$. So $m \equiv 0 \mod 3$, and $p=m^2+3 \equiv 0 \mod 3$. This is not possible.

If $\alpha_2(g) = 1$, then $\alpha_1(g) = 2$. So $2(p-4) + 6\alpha_3(g) = 0$ by (13.13). But $\alpha_3(g) \geq 0$. So $p-4 \leq 0$. Hence $p \leq 4$, which is absurd. The only remaining case is $\alpha_2(g) = 2$. Then $\alpha_1(g) = 0$. So $6p = 4(p+2) + 6\alpha_3(g)$ and $3\alpha_3(g) = m+1$. Hence $m^2 - m - 2 = 0$. From this we get $m = 2$ and $p = 7$.

(13.16) Lemma: If $p > 7$, there are no elements of order 3 in G with 4 fixed points.

Proof: Suppose that there are such elements in G. Let Q be a Sylow 3-subgroup of the stabiliser of three points in Ω. Then Q has exactly four fixed points, and $N_G(Q)$ acts 3-transitively on this four-point set. Hence $N_G(Q)$ involves Alt(4). So the Sylow 2-subgroup of $N_G(Q)$ contains a subgroup V of order 4.

From (13.15) (ii), Q acts semiregularly on $\Omega - fx_\Omega(Q)$. Thus, $|Q|$ divides $p-4$. If $|Q| > 3$, then 9 does not divide $p-1$. From (13.14) we get $p=7$, contrary to hypothesis. Hence $|Q| = 3$. Since $|Aut_G(Q)| \leq 2$, $V \cap C_G(Q) \neq 1$. So we get an element of order 6. By (13.15) (iii), $p=7$. This contradiction completes the proof of (13.16).

(13.17) Lemma: If $p > 7$, all elements of order 3 are conjugate.

Proof: Let g and h be two elements of order 3 in G. Let $\{\alpha,\beta,\gamma\}$ be a non-trivial orbit of g, with $\alpha g=\beta$, $\beta g=\gamma$. Similarly, let $\{\alpha',\beta',\gamma'\}$ be a non-trivial orbit of h, with $\alpha' h = \beta'$, $\beta' h = \gamma'$. Choose an element g_1 such that $\alpha' g_1 = \alpha$, $\beta' g_1 = \beta$ and $\gamma' g_1 = \gamma$. Put $h_1 = g_1^{-1} h g_1$. Then $\langle g,h_1\rangle$ has an orbit of length 3. By (13.16), $\langle g\rangle$ and $\langle h_1\rangle$ are Sylow 3-subgroups of $\langle g,h_1\rangle$. So $\langle g\rangle$ is conjugate to $\langle h_1\rangle$ by an element of $\langle g,h_1\rangle$. Since the constituent of $\langle g,h_1\rangle$ on $\{\alpha,\beta,\gamma\}$ is cyclic of order 3, g must be conjugate to h_1. Hence, g is conjugate to h.

(13.18) Theorem: The case $k = (p-3)/2$ is possible only if $p=7$.

Proof: We assume that it occurs for some prime $p > 7$. Let g be an element of order 3 in the centre $Z(R)$ of a Sylow 3-subgroup R of G. By (13.17), g is conjugate to g^{-1}. By Burnside's Theorem, g is conjugate to g^{-1} by an element of $N_G(R)$. Hence $|N_G(R)|$ is even.

From (13.16) R has one fixed point, and acts semiregularly on $\Omega - fx_\Omega(R)$. Since $p-1 = 2.3^u$, $|R| = 3^u$ and R has two non-trivial orbits in Ω. Let h be an involution in $N_G(R)$. If h interchanges the two orbits of R, then $\alpha_1(h) = 1$. This is impossible, since it implies that $m = 0$. As $C_G(h) \cap R = 1$ by (13.15) (iii), the only other possibility is that h should have one fixed point in each orbit of R. Thus $\alpha_1(h) = 3$; so $m=2$ and $p=7$ - contrary to assumption. This establishes the theorem.

§14. Groups of degree $1 + q + q^2$, where q is a prime.

The main result of this section is due to Tsuzuku [11], although the proofs differ slightly to allow for an extended result, which will be useful in the sequel.

(14.1) Theorem: Let G be a 2-transitive group on a set Ω, where $|\Omega| = 1 + q + q^2$ and q is a prime. Then

(i) If q^3 divides $|G|$, $Alt(\Omega) \leq G$ or $PSL(3,q) \leq G \leq PGL(3,q)$;

(ii) If q^2 divides $|G|$ exactly, then the Sylow q-subgroups are elementary abelian and have orbits of lengths 1, q and q^2.

Proof: We will use the following notation throughout the proof: α is the unique fixed point of a given Sylow q-subgroup Q; when points β and γ are chosen R and S will denote Q_β and Q_γ, respectively; and Δ, Γ will denote

$fx(R)$, $fx(S)$ respectively. We will suppose that $Alt(\Omega) \not\leq G$, but that q^2 divides $|G|$.

We first show that Q has orbits of lengths 1, q and q^2. Suppose otherwise. Then Q must have q+1 orbits of length q, and 1 of length 1. Let $\Omega_0, \Omega_1, \ldots \Omega_q$ be the non-trivial orbits of Q. Then $Q^{\Omega_i} = \langle g_i \rangle$, where g_i is a q-cycle, for i=0,1,...,q.

We define a relation $\sim$ on {0,1,...,q} by: $i \sim j$ if $g_0^{n_0} g_1^{n_1} \ldots g_q^{n_q} \in Q$ with $n_i = 0$ implies $n_j = 0$. This is clearly a reflexive and transitive relation. By 2-transitivity, one sees that each i is related to $(|fx(Q_\omega)|-1)/q = r$ elements, for any $\omega \in \Omega - \{\alpha\}$. Hence, $\sim$ is an equivalence relation in which all the equivalence classes have the same size r. As q^2 divides $|G|$, $r \neq q + 1$. Choose Ω_i and Ω_j so that i is not equivalent to j. Choose $\beta \in \Omega_i$ and $\gamma \in \Omega_j$. Then R and S are Sylow q-subgroups of $G_{\alpha,\beta}$ and $G_{\alpha,\gamma}$ respectively. Also $|\Gamma| = |\Delta| = rq+1$ and $|\Gamma \cap \Delta| = 1$. Now, $N_G(R)$ is 2-transitive on Δ by (2.15). So the normal subgroup U of $N_G(R)$, which centralises R and fixes each non-trivial orbit of R, acts transitively on Δ, since it contains Q. Thus U^q - the subgroup of U generated by all q^{th} powers of elements of U - is transitive on Δ (being normal in $N_G(R)$) and trivial on $\Omega - \Delta$. Similarly, we get a subgroup V^q which is transitive on Γ and trivial on $\Omega - \Gamma$. So $\langle U^q, V^q \rangle$ contains a 3-cycle. By (4.2), $Alt(\Omega) \leq G$, contrary to assumption.

Now suppose that q^3 divides $|G|$. Let β be chosen in the orbit of Q of length q. We show that R has exactly one non-trivial orbit, and this has length q^2. The alternative is that R has q non-trivial orbits, each of length q. Let $\Omega_1, \ldots, \Omega_q$ be these orbits. Then

$R^{\Omega_i} = \langle g_i \rangle$ for some q-cycle g_i, i=1,...,q. We define a relation on {1,...,q} by: $i \sim j$ if $g_1^{n_1}...g_q^{n_q} \in R$ and $n_i=0$ implies $n_j=0$. As $Q \leq N_G(R)$, $N_G(R)$ is transitive on the set $\{\Omega_1,...,\Omega_q\}$. Hence, each i is related to the same number of elements. This together with transitivity and reflexivity (which are obvious) implies that the relation is an equivalence relation. Since q is a prime, the relation is trivial. {1,...,q} cannot be an equivalence class; for, if it were, we would have $|R| = q$ and $|Q| = q^2$. So, for each $i \geq 2$, there are elements $g_1^{n_1}...g_q^{n_q} \in R$ with $n_1=0$ and $n_i \neq 0$. Choose $\gamma \in \Omega_1$. Let W be a Sylow q-subgroup of $G_{\alpha,\gamma}$ which contains R_γ. Then for some set $\Omega'_1 \subseteq \Omega_1 \cup \Delta - \{\alpha,\gamma\}$, $|\Omega'_1| = q$, and some q-cycle g' on Ω_1, we have $W \leq \langle g', g_2,...,g_q \rangle$. If $\Omega_1 \cap \Omega'_1 = \emptyset$, then $\langle W,R \rangle$ is a Sylow q-subgroup of G with q+1 orbits of length q. Hence $\Omega_1 \cap \Omega'_1 \neq \emptyset$. So $\langle W,R \rangle$ is transitive on $\Omega_1 \cup \Omega'_1$. As $|\Omega_1 \cup \Omega'_1|$ is relatively prime to q, $\langle W,R \rangle^q$ acts non-trivially on $\Omega_1 \cup \Omega'_1$ and trivially on $\Omega - \Omega_1 \cup \Omega'_1$. But $\langle W,R \rangle$ is at least 2-transitive on $\Omega_1 \cup \Omega'_1$. Hence $\langle W,R \rangle^q$ is transitive on $\Omega_1 \cup \Omega'_1$. Since $|\Omega_1 \cup \Omega'_1| < 2q$, we have $|\Omega_1 \cup \Omega'_1| < \frac{1}{2}|\Omega|$. Applying (4.5), we obtain the contradiction $Alt(\Omega) \leq G$.

We continue with the case: q^3 divides $|G|$. Let β be an element in the orbit of Q of length q. Put $\mathcal{L} = \{\Delta g | g \in G\}$. We show that $\{\Omega,\mathcal{L}\}$ is a projective plane. As before, we find that no element of $N_G(R)$ can act non-trivially on Δ and trivially on $\Omega - \Delta$. Hence $C_G(R)$ acts trivially on Δ. Now choose h so that $|(\Omega - \Delta) \cup (\Omega - \Delta h)|$ is minimal, subject to being greater than $|\Omega - \Delta|$. By (3.3), $\Delta h - \Delta \cap \Delta h$ is a block of R. If this block is trivial, G is (q+2)-transitive on Ω by (4.1). Hence $N_G(R)/C_G(R)$ involves Sym(q+1). Thus R is not regular on

$\Omega - \Delta$. Let $\Delta^* = \Delta - \{\alpha\}$, $\Omega^* = \Omega - \Delta^*$. Then $G_{(\Delta^*)}$ is 2-transitive on Ω^*. By considering two Sylow q-subgroups of $G_{(\Delta^*)}$, which contain R_γ for some $\gamma \in \Omega^* - \{\alpha\}$, and which have different fixed points in Ω^*, we find that $\mathrm{Alt}(\Omega^*) \leq G_{(\Delta^*)}$ as in the previous paragraph. Hence $\mathrm{Alt}(\Omega) \leq G$, contrary to assumption. So $\Delta h - \Delta \cap \Delta h$ is a non-trivial block of R. Hence, q divides $|\Delta h - \Delta \cap \Delta h|$. Thus $|\Delta \cap \Delta h| = 1$. So, for $g \in G$, either $\Delta g = \Delta$ or $|\Delta g \cap \Delta| \leq 1$. Together with 2-transitivity, this implies that there is exactly one set Δg containing a given pair of points. Hence there are $q^2 + q + 1$ such sets. A simple counting argument now yields that for $g \in G$, $\Delta g = \Delta$ or $|\Delta g \cap \Delta| = 1$. Moreover, there are four points, no three of which belong to the same Δg. Thus $\{\Omega, \mathcal{L}\}$ is indeed a projective plane, and G is a collineation group containing all elations. That is, $\mathrm{PSL}(3,q) \leq G \leq \mathrm{PGL}(3,q)$.

We now consider the case in which q^2 divides $|G|$ exactly. We have already shown that a Sylow q-subgroup Q of G has orbits of lengths 1, q and q^2. Suppose that Q is cyclic. Let $R = Q^q$. Then Q is a Sylow subgroup of $C_G(R)$. By a theorem of P. Hall, $N_G(Q) \cap C_G(R) = C_G(Q) \cap C_G(R)$. By Burnside's theorem, $C_G(R)$ has a normal q-complement, T (say). Now $C_G(R)$ has two orbits - one of length q+1 on which it acts 2-transitively and one of length q^2 on which it acts transitively. On the first, T must act transitively, and on the second, trivially. Since $1 + q < q^2$, (4.5) implies that $\mathrm{Alt}(\Omega) \leq G$. So Q cannot be cyclic.

We now deal with the special cases which occurred in (12.9) and (13.18). We use the notation and hypotheses leading to these results.

(14.2) Theorem: (i) If $(k,p) = (1,7)$ or $(2,13)$, then $G = \mathrm{PSL}(3,q)$;

(ii) If $(k,p) = (2,7)$, then $G = \mathrm{Alt}(7)$.

Proof: If $k=1$ and $p=7$, then G has irreducible characters of degrees 1,6,8,3 and 3; the degrees of the remaining irreducible characters are divisible by 7. As $\mathrm{Alt}(7)$ and $\mathrm{Sym}(7)$ both have an irreducible character of degree 10, $\mathrm{Alt}(7) \not\leq G$. Since $7 = 1 + 2 + 2^2$ and 2^3 divides $|G|$, $\mathrm{PSL}(3,2) \leq G \leq \mathrm{PGL}(3,2)$ by (14.1). Since $\mathrm{SL}(3,2) = \mathrm{GL}(3,2)$, we have concluded this case.

If $k=2$ and $p=13$, then the irreducible characters whose degrees are not divisible by 13 have degrees 1,12,27,16,16 and 16. Thus $\mathrm{Alt}(13) \not\leq G$, as $\mathrm{Alt}(13)$ and $\mathrm{Sym}(13)$ have irreducible characters of degree 66. As before, $\mathrm{PSL}(3,3) \leq G \leq \mathrm{PGL}(3,3)$. Since G is simple, we have $G = \mathrm{PSL}(3,3)$.

For part (ii), we observe that the irreducible characters of G, whose degrees are not divisible by 7, have degrees 1,6,15,10 and 10. So there are integers $n_1,\ldots,n_s$ such that $|G| = 1 + 36 + 225 + 2.100 + 49 \sum_{i=1}^{s} n_i^2$, $|G|$ divides $7!$ and 6 divides $|G|$. The only possible value for $|G|$ is $7.5.3^2.2^3$, i.e. $(7!)/2$. Hence $G = \mathrm{Alt}(7)$.

(14.3) Theorem: If G satisfies the hypothesis of §1, and $|\Omega| = 7$, 13, or 19, then $G = \mathrm{Alt}(7)$ or $\mathrm{PSL}(2,q)$, $q = 2$ or 3.

Proof: The cases $k \leq 2$ are considered in (12.9) and (14.2). The case $k = (p-3)/2$ is considered in (13.18). It remains to show that none of the cases in which $2 < k < (p-3)/2$ may arise. This we do by tabulating the values for $-n_1, n_2$ and $1+n_1+n_2$ in each case, and observing that $-n_1 n_2 (1+n_1+n_2)$ is never a perfect square.

p	13	13	19	19	19	19	19
k	3	4	3	4	5	6	7
$-n_1$	12	12	18	18	18	18	18
n_2	40	53	58	77	96	115	134
$1+n_1+n_2$	29	42	41	60	79	98	117

§15. Some Numerical Results.

In this section we continue with the hypothesis of §12, but add that $|\Omega| = s'q + 1$, where q is a prime and s' is "small".

Since $-n_1n_2(1+n_1+n_2)$ is a perfect square, we may write

(15.1) $\quad p = \ell^2 q_1 q_2 + 1$

where q_1, q_2 are square-free, and the square-free parts of n_2q_1 and $(1+n_1+n_2)q_2$ are not divisible by primes dividing q_1 and q_2, respectively. In view of (12.9) and (13.18) we will suppose that $p > 13$. So

(15.2) $\quad 2 < k < (p-3)/2.$

Taking equivalences modulo q_1 and q_2, respectively, we get $0 \equiv n_2 \equiv k+1$ and $0 \equiv 1+n_1+n_2 \equiv k+2$. So there are positive integers m_1 and m_2 such that

(15.3) $\quad k = m_1q_1 - 1 = m_2q_2 - 2$

Substituting in (15.2), we get

(15.4) $\quad 1 \leq m_1 < \ell^2 q_2/2$ and $1 \leq m_2 \leq \ell^2 q_1/2.$

We also have

(15.5) $\quad n_2 = \{\ell^2 m_1 q_1 q_2 + (m_1 - \ell^2 q_2)\}q_1 = \ell^2 m_2 q_1 q_2^2 + (m_2 - 2\ell^2 q_1)q_2 - 1,$

and

(15.6) $\quad 1+n_1+n_2 = \{\ell^2 m_2 q_1 q_2 + (m_2 - 3\ell^2 q_1)\}q_2 = \ell^2 m_1 q_1^2 q_2 + (m_1 - 2\ell^2 q_2)q_1 + 1.$

In what follows we will show that the extra restrictions on p imply that there is an integer n, such that

$$(15.7)\begin{cases} p = n^2 + n + 1 \\ n_2 = n^3 \\ \text{and } 1 + n_1 + n_2 = (n-1)^2(n+1) \end{cases}$$

Since 6 divides p-1, if $s' < 6$, then q=2 or 3. So p=7 or 13. These cases we have excluded.

<u>p = 6q + 1</u>:

q=2 is excluded as before. q=3 is excluded by (14.3). So we have $q \geq 5$. In (15.1), $\ell^2 = 1$. We have the following possibilities:

	I	II	III	IV	V
$q_1 =$	2	3	q	6	2q
$q_2 =$	3q	2q	6	q	3
$m_1 \leq$			2		1
$m_2 \leq$	1	1		3	

I: $m_2=1$. So $x = n_2q_1 = 36q^2 - 18q - 2$, $y = (1+n_1+n_2)/q_2 = 6q-5$, and $(x,y) = 1$. Hence for some integers A and B, $x = A^2$ and $y = B^2$. So $(6q - 3/2)^2 - A^2 = 17/4$. From this we get

$$12q - 3 + 2A = 17$$

$$12q - 3 - 2A = 1.$$

These imply that q = 1. So case I does not occur.

II: $m_2=1$. $x = n_2q_1 = 36q^2 - 30q - 3$, $y = (1+n_1+n_2)/q_2 = 6q-8$, and $(x,y)=1$ or 7. Hence there is an integer B such that $6q - 8 = B^2$ or $7B^2$. This is impossible since $6q - 8 \equiv 2 \bmod 4$.

III: $m_1=1$. $x = n_2/q_1 = 6q - 5$, $y = (1+n_1+n_2)q_2 = 36q^2 - 66q + 6$, and

$(x,y) = 1$. So $y = B^2$. Hence $(12q - 11)^2 - B^2 = 97$. By the method of case I, we get $q = 5$, $p = 31$, $n_2 = 125$ and $1+n_1+n_2 = 96$ - i.e. (15.7) with $n = 5$.

$m_1=2$. $x = n_2/q_1 = 12q - 4$, $y = (1+n_1+n_2)q_2 = 72q^2 - 60q + 6$, and $(x,y) = 1$. Hence $3q - 1 = B^2$. But -1 is not a square mod 3. So this case cannot occur with $m_1 = 2$.

IV: $m_2=1$. $x = n_2q_1 = 36q^2 - 66q - 6$, $y = (1+n_1+n_2)/q_1 = 6q - 17$, and $(x,y) = 1$. So $x = A^2$. That is, $(12q - 11)^2 - 4A^2 = 145 = 5.29$. Hence $12q - 11 = 73$ or 17. So $q = 7$ or $7/3$. Thus we have (15.7) with $n = 6$.

$m_2=2$. $x = n_2q_1 = 72q^2 - 60q - 6$, $y = (1+n_1+n_2)/q_2 = 12q - 16$, and $(x,y) = 1$ or 7. So $3q - 4 = B^2$ or $7B^2$. And therefore, $B^2 \equiv -1 \bmod 3$.

$m_2=3$. $x = n_2q_1 = 108q^2 - 54q - 6$, $y = (1+n_1+n_2)/q_2 = 18q - 15$, and $(x,y) = 1$. So $18q - 15 = B^2$. Thus $B^2 \equiv 3 \bmod 9$.

V. $m_1=1$. $x = n_2/q_1 = 6q - 2$, $y = (1+n_1+n_2)q_2 = 36q^2 - 30q + 3$, and $(x,y) = 1$. So $36q^2 - 30q + 3 = B^2$. Hence $(12q- 5)^2 - 4B^2 = 13$. This implies that $q = 1$. So this case does not arise.

If $6 < s' < 12$, we must have $q = 2$ or 3. The only prime of the form $s'q + 1$ in this range is 19, and this case is dealt with in (14.3).

<u>$p = 12q + 1$</u>:

For $q = 2$, $12.2 + 1$ is not a prime. For $q = 3$, $p = 37$. Since $(37k + 1, 37k - 34) = (35, 2k+1)$ and $2 < k < 17$, the highest common factor of n_2 and $1+n_1+n_2$ is 1 except when $k = 3$, in which case it is 7. So $37k + 1 = A^2$ or $7A^2$ and $37k - 34 = B^2$ or $7B^2$. Hence $A = 18, 6$ or 3. This gives $37k = 323$, 34 or 62. So this case does not occur.

For $q \geq 5$, we have $\ell^2 = 4$ in (15.1). So the following cases arise:

	I	II
q_1 =	3	q
q_2	q	3
$m_1 \leq$		5
$m_2 \leq$	6	

I: $x = n_2q_1 = 3(4m.3q^2 + (m-24)q - 1) = 36mq^2 + (3m - 72)q - 3$ and $y = (1+n_1+n_2)/q_2 = 4m.3q + (m-36) = 12mq + (m-36)$, where $1 \leq m \leq 6$. So $(x,y) = (18 - m, 12q - 1).(m , 3)$. We consider the various values of m separately.

(i) m=1. $(x,y) = 1$ or 17. Since $y \equiv -35 \equiv 1$ and $17 \equiv 2 \bmod 3$, we cannot have $(x,y) = 17$. Hence $x = A^2$. Thus $(24q - 23)^2 - A^2 = 577$, which is a prime. So we get $q = 13$. This gives n_1, n_2 and $1+n_1+n_2$ as in (15.7) with $n = 12$.

(ii) m=2. $(x,y) = 1$. Hence $24q - 34 = B^2$. So $B^2 \equiv 2 \bmod 4$.

(iii) m=3. $(x,y) = 3$ or 15. So $12q - 11 = B^2$ or $5B^2$.

The second case implies $B^2 \equiv -1 \bmod 3$. So we have $36q^2 - 21q - 1 = A^2$. Thus $(24q - 7)^2 - 16A^2 = 65 = 5.13$. This gives $24q - 7 = 33$ or 9, both of which are impossible.

(iv) m=4. $(x,y) = 1$ or 7. If $(x.y) = 1$, then $x = A^2$. So $(24q - 5)^2 - 4A^2 = 37$. From this we obtain $q = 1$, which is impossible. The alternative is $(24q - 5)^2 - 28A^2 = 37$. Modulo 16, this equation yields $25 + 4A^2 \equiv 5$. So $A^2 \equiv -1 \bmod 4$, which is impossible.

(v) m=5. $(x,y) = 1$ or 13. Thus $y = 60q - 31 = B^2$ or $13B^2$. In both

cases $B^2 \equiv -1 \bmod 3$.

(vi) m=6. $(x,y) = 3$. So $y/3 = 24q - 10 = B^2$. Hence $B^2 \equiv 2 \bmod 4$.

II. $x = n_2/q_1 = 4m.3q + (m-12) = 12mq + (m-12)$ and $y = (1+n_1+n_2)q_2 = 3\{4m.3q^2 + (m-24)q + 1\} = 36mq^2 + (3m - 72)q + 3$, where $1 \leq m \leq 5$. In this case, $(x,y) = (12q - 1, 6 - m).(m,3)$.

(i) m=1. $(x,y) = 1$ or 5. In the second case $12q - 11 = 5A^2$. So $A^2 \equiv -1 \bmod 3$. In the first case $y = B^2$. That is, $(24q - 23)^2 - 16B^2 = 481 = 13.17$. Hence $24q - 23 = 241$ or 15. So $q = 11$, and we get (15.17) with $n = 11$.

(ii) m=2. $(x,y) = 1$. Then $x = A^2$. So $A^2 = 24q - 10 \equiv 2 \bmod 4$.

(iii) m=3. $(x,y) = 3$. So $y = 3B^2$. Hence $(24q - 7)^2 - 16B^2 = 33 = 3.11$. Thus $24q - 7 = 17$ or 7. We get $q = 1$, which is impossible.

(iv) m=4. $(x,y) = 1$. Then $x = A^2$. So $A^2/4 = 12q - 2 \equiv 2 \bmod 4$.

(v) m=5. $(x,y) = 1$. Then $x = A^2$. So $A^2 = 60q - 7 \equiv 3 \bmod 10$, and this is not possible.

§16. p = 43.

In this section we show that there is no group of degree 43 satisfying the hypothesis of §12.

Suppose that there is such a group G. From the results of Jordan, Manning and Weiss on the order of, and degrees of the elements in, a primitive group -- see Wielandt [14] Theorems (13.10) and (14.1) - we find that the only primes which may divide $|G|$ are 2,3,5,7,41 and 43, and that for $g \in G$

(16.1) $\alpha_5(g) \geq 5$, if g has order 5.

From (13.18), G is not 4-transitive. So, if 41 divides $|G|$,

the 2-point stabilisers must be soluble, by Burnside's Theorem. Hence $|G| = 43.42.41.z$ where x divides 40. From §15, $1+n_1+n_2 = 175$. So 5^2 divides $|G|$. This contradiction implies that 41 does not divide $|G|$.

Let S be a Sylow 5-subgroup of G.

(16.2) Lemma: 7 does not divide $|N_G(S)|$.

Proof: Suppose otherwise. If 7 also divides $|C_G(S)|$, then $C_G(S)$ has an orbit of length 35. As S centralises $C_G(S)$, it must act semiregularly on this orbit. But then S contains a 5-cycle, since 5^2 divides $|G|$. This contradicts (16.1). Let g be an element of order 7 in $N_G(S)$. Then $1 \neq |S:C_S(g)| \equiv 1 \bmod 7$. So 5^6 divides $|S|$. But this again contradicts (16.1), and so establishes the lemma.

Let $\Delta = fx_\Omega(S)$. Then $|\Delta| \equiv 3 \bmod 5$, and by (16.1), $|\Delta| \leq 18$. Since (2.15) implies that $|N_G(S)|$ is divisible by 7, 13 or 17 in the cases $|\Delta| = 8$, 13 or 18 respectively, we have

(16.3) Lemma: $|\Delta| = 3$.

(16.4) Lemma: S has one orbit of length 5^2.

Proof: Suppose otherwise. Then S has 8 orbits of length 5. Choose an element $g \in S - \{1\}$ for which $|mv(g)|$ takes the minimum value. Put $\Gamma = fx_\Omega(g)$. We first show that $|\Gamma| \geq 13$. This is clearly true if 5^3 divides $|S|$. If $|S| = 5^2$, S has at most 6 subgroups of index 5. Hence some such subgroup must occur as the kernel of the representation of S on at least two non-trivial orbits.

Let H be the group generated by all Sylow 5-subgroups of G containing $\langle g \rangle$. We examine the action of H on Γ. Clearly H centralises $\langle g \rangle$ and fixes its non-trivial orbits.

For any pair $\gamma, \delta \in \Gamma$, $\gamma \neq \delta$, there is a Sylow 5-subgroup of $G_{\gamma,\delta}$

containing $\langle g \rangle$. Hence H can have at most one fixed point.

Suppose $fx_\Omega(H) = \{\alpha\}$. Then for any pair $\gamma, \delta \in \Gamma - \{\alpha\}, \gamma \neq \delta$, and for any Sylow 5-subgroup S' in $H_{\gamma,\delta}$, we have $fx_\Omega(S') = \{\alpha,\gamma,\delta\}$. As $|\Gamma| \geq 13$, the remaining orbits of H in Γ have lengths at least 5. Let Φ be one such orbit. Suppose $\gamma, \delta \in \Phi, \gamma \neq \delta$. Choose S' as above. Since Φ is a union of S'-orbits, $|\Phi| \equiv 2 \bmod 5$, and the remaining orbits have lengths divisible by 5. This implies that $\Phi = \Gamma - \{\alpha\}$. Let $\gamma \in \Phi$, and let Ψ be an orbit of H_γ in $\Phi - \{\gamma\}$. Choosing $\delta \in \Psi$, the above argument gives $|\Psi| \equiv 1 \bmod 5$. While, for $\delta \in \Phi - \Psi \cup \{\gamma\}$, we get $|\Psi| \equiv 0 \bmod 5$. Hence $\Psi = \Phi - \{\gamma\}$. So H is 2-transitive on Φ. Since $|\Gamma| = 13$ or 18, this implies that $|H|$ is divisible by 11 or 17. This contradiction yields the fact that $fx_\Omega(H) = \phi$.

Let Φ be an orbit of H in Γ. Choose $\gamma, \delta \in \Phi, \gamma \neq \delta$, and choose S' as before. If $fx_\Omega(S') \subseteq \Phi$, then $|\Phi| \equiv 3 \bmod 5$, and the remaining orbits have lengths divisible by 5. This is possible only if $\Phi = \Gamma$. If $fx_\Omega(S') \not\subseteq \Phi$, then $|\Phi| \equiv 2 \bmod 5$, and some other orbit Φ' satisfies $|\Phi'| \equiv 1 \bmod 5$. As $|\Phi'| > 1$, the same argument applied to Φ' yields $|\Phi'| \equiv 2$ or $3 \bmod 5$. So this case cannot occur. That is, H is transitive on Γ. Let $\alpha \in \Gamma$. Let Ψ be an orbit of H_α in $\Gamma - \{\alpha\}$. Then $|\Psi| \equiv 1$ or $2 \bmod 5$. If $|\Psi| \equiv 1 \bmod 5$, then there is a second non-trivial orbit Ψ' of H_α, with $|\Psi'| \equiv 1 \bmod 5$. Moreover, $\Gamma = \{\alpha\} \cup \Psi \cup \Psi'$. Since 13 does not divide $|G|$, we have $|\Gamma| = 18$. So $\{|\Psi|, |\Psi'|\} = \{6,11\}$ or $\{1,16\}$. The first case cannot occur since 11 does not divide $|G|$. Let α' denote the second fixed point of H_α. Then the sets $\{\alpha g, \alpha' g\}$, $g \in H$, form a complete block system of H in Γ. Let S be a Sylow 5-subgroup of $H_{\alpha,\alpha'}$, and put $fx_\Omega(S) = \{\alpha, \alpha', \beta\}$. Then β' must

belong to some non-trivial orbit of S; and this is impossible. There is one case remaining, in which $|\Psi| \equiv 2 \bmod 5$. As before, $\Psi = \Gamma - \{\alpha\}$. So H is 2-transitive on 18 points. This is not possible since 17 does not divide $|G|$. This completes the proof of (16.4).

(16.5) Theorem: There is no insoluble 2-transitive group of degree 43, in which a Sylow 43-subgroup has index 3 in its normaliser.

Proof: We have already seen that if such a group G exists, it must have a Sylow 5-subgroup S with three fixed points α, β and γ, three orbits of length 5 Δ_1, Δ_2 and Δ_3, and one orbit of length 5^2 Δ_4. Put $\{\alpha,\beta,\gamma\} = \Delta$.

Let $\delta \in \Delta_1$, and suppose that $fx_\Omega(S_\delta) = \Delta \cup \Delta_1$. Let $\delta' \in \Delta_1$, $\delta' \neq \delta$, and let T be a Sylow 5-subgroup of $G_{\delta,\delta'}$, containing S_δ. Then $\langle S,T\rangle \leq N_G(S_\delta)$, and $\langle S,T\rangle$ contains a group K which is at least 3-transitive on a 7-point subset Δ' of $\Delta \cup \Delta_1$. Hence $\mathrm{Alt}(\Delta') \leq K^{\Delta'}$. Moreover, K is represented on the non-trivial orbits of S_δ. If some 7-element of K does not centralise S_δ, we get $|S_\delta| \geq 5^6$, contrary to (16.1). Hence K contains a subgroup K_1 such that $K_1^{\Delta'} = \mathrm{Alt}(\Delta')$ and $K_1 \leq C_G(S_\delta)$. If Δ_4 is an orbit of S_δ, then K_1 acts trivially on $\Omega - \Delta'$. By (4.5), $\mathrm{Alt}(\Omega) \leq G$. So Δ_4 is a union of 5 orbits of S_δ of length 5, and K_1 acts transitively on the 7 non-trivial orbits of S_δ. So $C_G(S_\delta)$ has an orbit of length 35. Hence S_δ acts semiregularly on this orbit. Thus $|S_\delta| = 5$. We may assume that $S_\delta \leq K_1$. So K_1 is a central extension of S_δ by Alt(7). As the multiplicator of Alt(7) has order 6, this extension splits. So K_1^5 is isomorphic to Alt(7) and has 6 non-trivial orbits on which it acts naturally. So K_1, and hence G, contain elements of type $1^{13}.5^6$. Thus, since $|S| = 5^2$, if we take $\eta \in \Delta_2 \cup \Delta_3$, then $fx_\Omega(S_\eta) = \Delta \cup \Delta_2 \cup \Delta_3$. That is, the elements of $S_\eta - 1$ have type

$1^{13}.5^6$, those of $S_\delta - 1$ have type $1^8.5^7$, and those of $S - S_\delta \cup S_\eta$ have type $1^3.5^8$. Hence S_η is a weakly closed subgroup of S with respect to G. From (2.17), $N_G(S_\eta)$ is 2-transitive on $fx_\Omega(S_\eta)$. But this is impossible since 13 does not divide $|G|$.

There remains the case in which $fx_\Omega(S_\delta) = \Delta \cup \Delta_1 \cup \Delta_2 \cup \Delta_3$. By (16.1), $|S_\delta| = 5$. S_δ is weakly closed in S with respect to G since the elements of $S_\delta - 1$ have type $1^{18}.5^5$ and those of $S - S_\delta$ have type $1^3.5^8$. Again from (2.17), $N_G(S_\delta)$ is 2-transitive on a set of 18 points, contrary to the fact that 17 does not divide $|G|$. And so the theorem is established.

(16.6) Theorem: Let G be a 2-transitive group on a set Ω, where $|\Omega| = p = 6q+1$ and p,q are primes. Suppose that a Sylow p-subgroup has index 3 in its normaliser. Then G = Alt(7) or PSL(2,q) for q = 2, 3 or 5.

Proof: If $p \leq 13$, we obtain three of these group by (14.3). Now suppose $p > 13$. By the results of §15, $p = 31$ and 5^3 divides $|G|$, or $p = 43$.

In the case $p = 31$, (12.1) and (14.1) imply that G = Alt(31) or PSL(3,5). But a 31-cycle in Alt(31) has index 15 in its normaliser, while a 31-cycle in PSL(3,5) has index 3 in its normaliser.

The case $p = 43$ cannot occur by (16.5).

§17. $p = q^2 + q + 1$.

In this section we develope the results of §14 as follows:

(17.1) Theorem: Let Ω be a set satisfying $|\Omega| = p = q^2 + q + 1$, where p and q are primes, and $q > 2$. Then there is no group G with the

following properties:

(i) G is 2-transitive on Ω;

(ii) A Sylow p-subgroup has index 3 in its normaliser;

(iii) A Sylow q-subgroup has order q^2.

Proof: Suppose that there is such a group. From (14.1) we see that a Sylow q-subgroup S has orbits $\{\alpha\}$, Δ and Γ of lengths 1, q and q^2, respectively, and S is elementary abelian. So S has $q+1$ elements of type $1^{q+1}.q^q$ and q^2-q elements of type $1^1.q^{q+1}$.

Let S_0 be the set of elements of type $1^{q+1}.q^q$ in S together with 1. Let $S_1,\ldots,S_q$ denote the remaining subgroups of order q in S.

We first show that $C_G(S) = S$. Certainly $C_G(S)$ acts semi-regularly on Γ. Let K be the subgroup of $C_G(S)$ which acts trivially on Γ. Then $C_G(S) = SK$. If K is non-trivial on $\{\alpha\} \cup \Delta$, then $\langle K \rangle^{N_G(S_0)}$ is transitive on $\{\alpha\} \cup \Delta$ and trivial on Γ. By (4.5), $Alt(\Omega) \leq G$, contrary to hypothesis. Hence $K = 1$.

The group $N_G(S)/S$ may be considered as a group of linear transformations of the 2-dimensional vector space S over GF(q), for which S_0 is an invariant subspace. By Masckhe's theorem, $N_G(S)/S$ is completely reducible. If S_0 has more than one complement which admits $N_G(S)/S$, then the elements of $N_G(S)/S$ induce automorphisms of the form $g \mapsto g^r$, $(r,q) = 1$, $g \in S$. So in this case, $N_G(S) \cap C_G(S_i) = S$ for $i = 0,1,\ldots,q$. The alternative is that S_0 has exactly one complement, S_1 say, admitting $N_G(S)/S$. Suppose $i \geq 2$ and $h \in N_G(S) \cap C_G(S_i)$. Then $\langle h \rangle$ has three distinct invariant subspaces in S; so it must induce 'scalar multiplication' in S. As $h \in C_G(S_i)$, its eigenvalue is 1. So $h \in C_G(S) = S$. We have thus established that, in both cases,

(17.2) $C_G(S_i) \wedge N_G(S) = S$, for $i = 2,3,\ldots,q$.

Now $C_G(S_i)/S_i$, for $i \geq 2$, acts as a permutation group on the $q+1$ non-trivial orbits of S_i. Let M be the subgroup of $C_G(S_i)$ which fixes Δ, as a set. Then $S \leq M$. Let - denote images in M/S. Then $N_{\bar{M}}(\bar{S}) = \overline{N_M(S)} \leq \overline{N_G(S) \wedge C_G(S_i)} = \bar{S} \leq N_{\bar{M}}(\bar{S})$. So $N_{\bar{M}}(\bar{S}) = \bar{S}$. As $\bar{S}$ is a Sylow q-subgroup of $\bar{M}$, $\bar{M}$ has a normal q-complement $\bar{T}$, say, where $S_i \leq T$. Thus $T = S_i \times T_1$, for some normal q'-subgroup T_1 of M. And $M = T_1 S$. Since M acts transitively on Γ, T_1 acts semiregularly on the set of S_i-orbits in Γ. Hence T_1 fixes each of these orbits, as sets. But T_1 centralises S_i. So T_1 acts trivially on Γ. By considering $\langle T_1 \rangle^{N_G(S_0)}$, as before, we find that $T_1 = 1$. So $M = S$. Thus

(17.3) $|C_G(S_i)| \leq q^2(q+1)$ for $i = 2,3,\ldots,q$.

Hence, if $g \in S_i - 1$, $i \geq 2$, we have

(17.4) $1 + u(g)^2 + v(g)^2 + (p-1)(1+u(g)+v(g))^2/3 \leq q^2(q+1)$.

From (12.4), $n_2(1+n_1+n_2)$ is divisible by q, since n_1 is divisible by q to the first power only. We consider the cases in which q divides n_2 and q divides $1+n_1+n_2$ separately.

Case I: $n_2 \equiv 0 \bmod q$.

Then $n_2 = kp + 1 \equiv k + 1 \equiv 0 \bmod q$. So $k = k_1 q - 1$. Thus

$$(17.5) \quad \begin{cases} n_2 = [k_1 q^2 + (k_1-1)q + (k_1-1)]q, \\ 1+n_1+n_2 = k_1 q^3 + (k_1-2)q^2 + (k_1-2)q + 1. \end{cases}$$

If q divides $k_1 - 1$, then q^2 divides n_2. Then (12.4) implies that q^3 divides n_2. So q^3 divides $|G|$, contrary to hypothesis. Hence

(17.6) $k_1 \not\equiv 1 \bmod q$.

From (12.8) and (13.18), $k_1 q - 1 < (q^2+q-2)/2$. So

(17.7) $k_1 < (q+1)/2$.

For an element $g \in S - 1$ we find that $u(g) \equiv 0$ and $v(g) \equiv 0 \bmod q$ by evaluating the inner products of χ_1 and χ_2 with χ_0 on the subgroup $\langle g \rangle$. Put $u(g) = qu'(g)$ and $v(g) = qv'(g)$. We then consider the expression $\#\{g_1^{\cdot} g_2^{\cdot} = x\}$ where x is a p-element and $g_1, g_2 \in S - 1$. By (2.6), this is

$$\frac{|G|}{|C_G(g_1)|.|C_G(g_2)|}\left\{1 - \frac{qu'(g_1)u'(g_2)}{q+1} + \frac{qv'(g_1)v'(g_2)}{[k_1q^2+(k_1-1)q+(k_1-1)]}\right.$$
$$\left. - \frac{[1+q(u'(g_1)+v'(g_1))][1+q(u'(g_2)+v'(g_2))]}{[k_1q^3+(k_1-2)q^2+(k_1-2)q+1]}\right\}$$

Since $|C_G(g_i)|$, i=1 and 2, and $|G|$ are divisible by q^2 exactly, the numerator of the expression inside the chain brackets is also divisible by q^2. So we get

(17.8) $$k_1(k_1-1) - (k_1-1)u'(g_1)u'(g_2) + v'(g_1)v'(g_2)$$
$$- (k_1-1)(2+v'(g_1)+v'(g_2)+u'(g_1)+u'(g_2)) \equiv 0 \bmod q.$$

Let $g \in S$ have type $1^1.q^{q+1}$. Then $u'(g) = 0$. Taking $g_1 = g_2 = g$ in (17.8) we get

(17.9) $$(k_1-1)(k_1-2) - 2(k_1-1)v'(g) + v'(g)^2 \equiv 0 \bmod q.$$

If g is chosen to lie in S_i, for some $i \geq 2$, we have from (17.4) the inequality

(17.10) $$1 + q^2v'(g)^2 + q(q+1)(1+qv'(g))^2/3 \leq q^2(q+1).$$

The only possibilities for (17.10) are $v'(g) = -1, q=3$ and $v'(g) = 0$, q arbitrary. The former on substitution in (17.9) gives $k_1^2 - k_1 + 1 \equiv 0 \bmod 3$. So $k_1 \equiv 2 \bmod 3$. From (17.17), $k_1 < 2$. As $k_1 > 0$, we have a contradiction in this case.

The case $v'(g) = 0$ implies that $k_1 \equiv 1$ or $2 \bmod q$. By (17.6),

$k_1 \equiv 1$ is excluded. Because of (17.7), we must have $k_1 = 2$. So $n_2/q = 2q^2+q+1$ and $1+n_1+n_2 = 2q^3+1$. Since $(q+1, 2q^2+q+1) = 2$, $(q+1, 2q^3+1) = 1$ and $(2q^2+q+1, 2q^3+1) = 1$ or 11, we have the possibilities

	(i)	(ii)
$q+1$	$2A^2$	$2A^2$
$2q^2+q+1$	$2B^2$	$22B^2$
$2q^3+1$	C^2	$11C^2$

In (i), $B^2 - A^2 = q^2$. So $A = (q^2-1)/2$. Thus $4q+4 = (q^2-1)^2$. This equation is inconsistent with $q \geq 3$. In (ii), we have $q \equiv 3 \bmod 11$. Hence $A^2 \equiv 2 \bmod 11$. However, 2 is not a square mod 11. This completes the exclusion of case I.

Case II: $n_2 \equiv -1 \bmod q$.

Then $n_2 = kp + 1 \equiv k + 1 \equiv -1 \bmod q$. So $k = k_1 q - 2$. Thus

$$(17.11)\quad \begin{cases} n_2 = k_1 q^3 + (k_1-2)q^2+(k_1-2)q-1; \\ 1+n_1+n_2 = [k_1 q^2+(k_1-3)q+(k_1-3)]q. \end{cases}$$

If q divides k_1-3, we find, as in case I, that q^3 divides $|G|$, contrary to hypothesis. So

$$(17.12)\quad k_1 \not\equiv 3 \bmod q.$$

From (12.8) and (13.18), $k_1 q - 2 < (q^2+q-2)/2$. Hence

$$(17.13)\quad k_1 \leq (q+1)/2.$$

As in case I, we find that $u(g) \equiv 0$ and $v(g) \equiv -1 \bmod q$ for any element $g \in S - 1$. Put $u(g) = qu'(g)$ and $v(g) = qv'(g) - 1$.

From the expression for $\#\{g_1 g_2 = x\}$, where $g_1, g_2 \in S - 1$ and x is a p-element, we obtain the congruence

(17.14) $(k_1-2)(k_1-3) + (k_1-3)u'(g_1)u'(g_2) - (k_1-3)(v'(g_1)+v'(g_2))$
$+ (u'(g_1)+v'(g_1))(u'(g_2)+v'(g_2)) \equiv 0 \bmod q.$

Let $g \in S$ have type $1^1.q^{q+1}$. Then $u'(g) = 0$. Taking $g_1 = g_2 = g$ in (17.14) we get

(17.15) $(k_1-2)(k_1-3) - 2(k_1-3)v'(g) + v'(g)^2 \equiv 0 \bmod q.$

If g is chosen to lie in S_i, for some $i \geq 2$, the inequality (17.4) yields

(17.16) $1 + (qv'(g)-1)^2 + q(q+1).q^2v'(g)^2/3 \leq q^2(q+1$

The only solution of (17.16) is $v'(g) = 0$, q arbitrary. Substituting in (17.15), we get $k_1 \equiv 2$ or $3 \bmod q$. But $k_1 \not\equiv 3 \bmod q$, by (17.12). And $0 < k_1 \leq (q+1)/2$. So $k_1=2$. Thus $n_2=2q^3-1$ and $(1+n_1+n_2)/q = 2q^2-q-1$. Since $(q+1,2q^3-1) = (q+1,3) = 3$, $(q+1,2q^2-q-1) = 2$ and $(2q^3-1,2q^2-q-1) = (q-2,5) = 1$ or 5, we have the possibilities

	(i)	(ii)
$q+1$	$6A^2$	$6A^2$
$2q^3-1$	$3B^2$	$15B^2$
$2q^2-q-1$	$2C^2$	$10C^2$

In (i), we have $2(q+C)(q-C) = q+1$. This implies $C = 0$ and $q = 1$. In (ii), $q \equiv 2 \bmod 5$. So $6A^2 \equiv 3 \bmod 5$. Hence $A^2 \equiv 3$, which is impossible.

This completes the exclusion of case II, and concludes the proof of (17.1).

References

1. Blichfeldt, H. On the order of Linear Homogeneous Groups. Trans. Am. Math. Soc. 4(1903) 387-397.

2. Burnside, W. "Theory of Groups of Finite Order". Dover Publications, 1911.

3. Curtis, C.W. and Reiner, I. "Representation Theory of Finite Groups and Associative Algebras". Interscience Publishers, 1962.

4. Dembowski, P. "Finite Geometries". Springer, Berlin 1968.

5. Frobenius, G. "Uber die Characteres der symmetrischen Gruppe. Sitzgsber. preuss. Akad. Wiss. 1900, 516-534.

6. Frobenius, G. "Uber die Characteres der mehrfach transitiven Gruppen. Sitzgsber. preuss. Akad. Wiss. 1904, 558-

7. Hall, M. "Theory of Groups". Macmillan 1959.

8. Jordan, C. Theoremes sur les groupes primitifs. J. Math. Pures. Appl. 6(1871) 383-408.

9. Kantor, W.M. Jordan Groups. J. Alg. 12(1969) 471-493.

10. Marggraf, B. Uber primitive Gruppen mit transitiven Untergruppen geringeren Grades. Dissertation, Giessen 1892.

11. Tsuzuku, T. On Doubly Transitive Permutation Groups of Degree $1 + p + p^2$ where p is a Prime Number. J. Alg. 8(1968) 143-147.

12. Veblen, O. and Young, J.W. "Projective Geometry" I. Ginn, Boston 1810.

13. Wagner, A. On collineation groups of projective spaces, I. Math. Zeit. 76(1961) 411-426.

14. Wielandt, H. "Finite Permutation Groups". Academic Press, New York 1964.

15. Baker, A. Effective Methods in Diophantine problems. Proc. Symposia Pure Maths (AMS) 20(1971) 195-205.

DO3: X := X'/'P1 ; 'IF' X = CX '/' P1 * P1 'THEN' 'GOTO' DO3 ;

C OR COMMENT | CONTINUATN | FORTRAN STATEMENT | IDENTIFICATION

STATEMENT NUMBER