ON A PROBLEM ABOUT PRIMITIVE PERMUTATION GROUPS.

Primitive permutation groups of degree p^2+p+1, where p is a prime number.

M.Sc.Dissertation. Oxford University, September 1977.

I would like to thank my supervisor, Dr. Π.M. Neumann, for his patient help and his wise suggestions. Had I worked without him, I would not have done half of this dissertation!

Christian RONSE. Queen's College, Oxford.

ON A PROBLEM ABOUT PRIMITIVE PERMUTATION GROUPS.

(Primitive permutation groups of degree p^2+p+1, where p is a prime number.)

INTRODUCTION.

It is interresting to get a good characterization of $PSL(3,p)$ and $PGL(3,p)$ as permutation groups of degree p^2+p+1. This dissertation is devoted to the study of that problem. We attempt to prove the following:

Conjecture: If G is a primitive permutation group on a set Ω of size p^2+p+1, where p is a prime number, if p^2 divides the order of G, then G is one of the following groups acting in its natural representation of degree p^2+p+1:

(i) The little projective group $PSL(3,p)$.

(ii) The general projective group $PGL(3,p)$.

(iii) The alternating group A_{p^2+p+1}.

(iv) The symmetric group S_{p^2+p+1}.

The method that we use is the study of the p-elements and Sylow p-subgroups of G.

It is clear that the condition "p^2 divides the order of G" is necessary, because there are counterexamples otherwise:

(i) Frobenius groups $Z_{p^2+p+1}\cdot Z_p$ when $p \mid \varphi(p^2+p+1)$.

(ii) The group $PSL(5,2)$ of degree $31=5^2+5+1$.

Chapter I consists of preliminary results in group theory. These results are needed in our study.

In Chapter II, we prove general results about primitive permutation groups G of degree p^2+p+1 on a set Ω and of order divisible by p^2. Most of them were proved by McDonough [9] or by Neumann and Praeger (Unpublished). Using results of O'Nan [11] and Scott [17], we prove first that G is doubly transitive. Then we prove a theorem of Tsuzuku, which asserts that the conjecture is true when p^3 divides the order of G. To do it, we prove that G contains a subgroup Q of order p^2, which fixes p+1 points of Ω and has one orbit of length p^2. Then it is possible to prove that G contains the alternating group or that $G \subseteq \mathrm{Aut}\,\Pi$, where Π is a projective plane constructed on Ω. It is easily verified that this plane Π is desarguesian. (To prove Tsuzuku's theorem, we use mainly results of Jordan [6,7]). Finally, we study the case where p^2 divides exactly the order of G. A Sylow p-subgroup P of G has an orbit Γ of length p^2, an orbit Δ of length p and a fixed point α. Then $Q=P_\Delta$ has p orbits $\Gamma_1,\dots,\Gamma_p$ on Γ. We pose $\Delta' = \Delta \cup \{\alpha\}$. Then $X=G_{\{\Delta'\}}$ acts on Δ' and on $\Psi=\{\Gamma_1,\dots,\Gamma_p\}$, and both actions have kernel $Y=G_{\Delta'}$. Thus X/Y is a group of degree p and p+1, and using the results of Cameron [2] and Frobenius [3], we obtain strong conditions on these two actions. In particular, for $\beta\in\Delta$, $X_{\alpha\beta}$ has two orbits on Ψ, and three on $\Omega\setminus\{\alpha\beta\}$. This allows us to prove that G is triply primitive on Ω. We prove also that $p>11$ and $p\equiv 7$ (mod. 8). Moreover, G is not quadruply transitive on Ω.

It seems that such group cannot exist, because there is no known group which has faithful transitive actions of degree p and p+1, where p is a prime bigger than 11.

In Chapter III, we are always concerned with the case where p^2 divides exactly the order of G. In order to get more informations about the problem, we study properties of the elements of $G \setminus X$. Then we consider subgroups M of G which contain Q but are not contained in X, with support $\Omega' \subseteq \Omega \setminus \{\alpha, \beta\}$ ($\beta \in \Delta$), and such that for any $g \in M$, $(\Omega' \cap \Delta')^g = \Omega' \cap \Delta'$ or $(\Omega' \cap \Delta')^g \cap (\Omega' \cap \Delta') \neq \emptyset$. Then $M_{\{\Omega' \cap \Delta'\}} = M \cap X$ is a subgroup of X, and the properties of the two actions of X (on Σ and Δ') give us precise informations about M. In particular M/K, where $K = \bigcap_{g \in M} (M \cap X)^g$ is a soluble $\frac{3}{2}$-transitive group of degree $1+kp$ and rank $1+k$, where $1 \leq k \leq \frac{p-1}{2}$. We have other conditions on M and M/K. We hope that with these results the problem could be settled and the conjecture proved.

NOTATIONS AND DEFINITIONS.

All groups and geometries will be supposed finite. For abstract groups, we will use the definitions and notations of [5], and for permutation groups, we will use those of [19]. We will also use the notation "$P \in \mathcal{S}_p(G)$" to mean that P is a Sylow p-subgroup of G. If X is a permutation group on Ω, then we write fix X for the set of points of Ω which are fixed by X.

Chapter I. Preliminaries.

In our study, we will need some general group-theoretic results. This chapter is devoted to the proof of these results.

§1. Some transfer-theoretic results.

One of the uses of transfer is to get normal p-complements, or more generally normal complements in groups. We will prove a generalisation of Burnside's transfer theorem. If $K \lneq H \leq G$, we say that K is weakly closed in H if for any $g \in G$, $K^g \lneq H$ implies that $K^g = K$. (cfr. [5,p.255]).

Proposition 1.1. Let p be a prime number dividing the order of a group G, and let $P \in \mathcal{S}_p(G)$. If P is abelian and contains a subgroup $Q \neq 1$ such that $N_G(P)$ centralizes Q, then any subgroup of Q is weakly closed in P. Moreover, if $V: G \longrightarrow P$ is the transfer, then $Q \cap \ker V = 1$. In fact, for $x \in Q$, $xV = x^{[G:P]}$.

Proof. Take a subset X of P, and let $g \in G$. If $X^g \leq P$, then X and X^g are normal in P, and hence there is $h \in N_G(P)$ such that $X^g = X^h$ [5,7.11]. If $X \subseteq Q$, then $h \in C_G(X)$ and $X^g = X$. Therefore, any subgroup of Q is weakly closed in P. Now take $x \in Q$, then there exist $g_i \in G$ and integers m_i such that $xV = \prod_i (g_i^{-1} x^{m_i} g_i)$, $g_i^{-1} x^{m_i} g_i \in P$ for each i and $\sum_i m_i = [G:P]$. As $x^{m_i} \in Q$, it follows that $(x^{m_i})^{g_i} = x^{m_i}$ and hence $xV = x^{\sum m_i} = x^{[G:P]}$. As $[G:P]$ and $|Q|$ are coprime, it follows that $Q \cap \ker V = 1$.

Proposition 1.2. Let G be a group with an abelian Sylow p-subgroup P for some prime p. If Q is a direct factor of P, then Q is a direct factor of $C_G(Q)$.

Proof. We may write $P=Q \times R$, where R is a subgroup of P. Now $P \in \mathcal{S}_p(C_G(Q))$, and we may apply proposition 1.1 to $C_G(Q)$: we have the homomorphism $V: C_G(Q) \longrightarrow P$, with $xV=x^{[C(Q):P]}$ for $x \in Q$. Therefore $Q \leq \mathrm{Im}V$, and let H be the subgroup of $C_G(Q)$ consisting of the elements g such that $gV \in R$. Then $H \triangleleft C_G(Q)$, $HQ=C_G(Q)$ and $H \cap Q=1$. Thus $C_G(Q)= Q \times H$ and hence Q is a direct factor of $C_G(Q)$.

Note that this result is a consequence of [4].

§2. On the limit of transitivity of permutation groups which do not contain the alternating group.

Here we prove a theorem due to Jordan [7]. Altough it was stated for odd primes, it is also valid for the prime 2. We will show some consequences of it.

Let p be a prime number.

Lemma 2.1. If H is a transitive group on a set Ω of size p^a, if H has a transitive normal p-subgroup P, if the nonabelian simple group S is a composition factor of H, then S is a section of GL(a,p).

Proof. Take a counterexample (H,Ω) of minimal degree p^b. If H is imprimitive, then let $\Psi=\{B_1,\dots,B_{p^t}\}$ be a complete set of imprimitivity blocks. Then H acts on Ψ with kernel H_{Ψ} and image H^{Ψ}. If S is a composition factor of H^{Ψ}, then P^{Ψ} is a normal p-subgroup of H^{Ψ}, transitive on Ψ, and so S is a section of $GL(t,p) \leq GL(a,p)$ by minimality of H. Hence S is a compsition factor of H_{Ψ}. Now H_{Ψ} is normal in $H_{\{B_1\}}^{B_1} \times \dots \times H_{\{B_{p^t}\}}^{B_{p^t}}$, and so S is a composition factor of some $H_i=H_{\{B_i\}}^{B_i}$. But $P_i=P_{\{B_i\}}^{B_i} \triangleleft H_i$ and P_i is transitive on B_i. Hence S is a section of $GL(b-t,p) \leqslant GL(a,p)$ in this case. If H is primitive, then $H \leqslant AGL(b,t) \leqslant AGL(a,t)$ because P is soluble [19,11.5]. But then S is a section of $AGL(a,p)$, and as $GL(a,p) \cong AGL(a,p)/(Z_p)^a$, S is a section of $GL(a,p)$. Therefore we have a contradiction in each case, and the proposition must be true.

<u>Theorem 2.2</u>. Let p be a prime number, let m, q be integers such that $p^m \leqslant q < p^{m+1}$ and $p \nmid q$. Let G be a (k+1)-fold transitive group of degree $d=qp^n+k$ which does not contain A_d. Then one of the following holds:

(i) $k<5$.

(ii) $k \leqslant q$.

(iii) A_k is a section of $GL(m+n,p)$.

<u>Proof</u>. Suppose that G is (k+1)-fold transitive on the set $\mathcal{N}$ of size d, that $k>q$, $k \geqslant 5$ and $G \not\geq A_d$. Then we prove that (iii) holds. Suppose first that $n>0$.

Let $\Delta \leqslant \mathcal{N}$, $|\Delta|=k$. Let $P \in \mathcal{S}_p(G_\Delta)$. As G is transitive on $\Gamma=\mathcal{N}\setminus\Delta$ and $|\Gamma|=qp^n$, any orbit of P on Γ has length at least p^n [19,3.4]. Let $\mathcal{N}_1,\ldots,\mathcal{N}_r$ be these orbits. Then $r \leqslant q < k$. By Witt's lemma [19,9.4], $N=N_G(P)$ is k-fold transitive on Δ, that is $N^\Delta \cong S_k$. By a theorem of Jordan [19,13.9], $N_\Gamma^{\Delta} \not\geq A_k$, and as $N_\Gamma^\Delta \triangleleft N^\Delta$, we must get $N_\Gamma^\Delta=1$, because A_k is the only non-trivial normal subgroup of S_k (since $k \geqslant 5$). We have thus $N^\Gamma/N_\Delta{}^\Gamma \cong N^\Gamma/(N_\Delta N_\Gamma)^\Gamma \cong \dfrac{N/N_\Gamma}{N_\Delta N_\Gamma/N_\Gamma}$

$\cong N/N_\Delta N_\Gamma$, and similarly $S_k \cong N^\Delta \cong N^\Delta/N_\Gamma{}^\Delta \cong N/N_\Delta N_\Gamma$.

Therefore A_k is a composition factor of $N^\Gamma/N_\Delta{}^\Gamma$, and hence of N^Γ. As $P \triangleleft N$, N permutes the orbits $\mathcal{N}_1,\ldots,\mathcal{N}_r$ of P, and as $r<k$, A_k is not a composition factor of

$N^{\{\mathfrak{A}_1,\ldots,\mathfrak{A}_r\}}$. Hence it is one of $(N_{\{\mathfrak{A}_1\}},\ldots,\{\mathfrak{A}_r\})^{\Gamma}$, which is a normal subgroup of $N_{\{\mathfrak{A}_1\}}^{\mathfrak{A}_1} X \ldots X\ N_{\{\mathfrak{A}_r\}}^{\mathfrak{A}_r}$. So A_k is a composition factor of $N_{\{\mathfrak{A}_i\}}^{\mathfrak{A}_i}$ for some i. Now $|\mathfrak{A}_i| = p^a$, where $a \leq m+n$ (since $|\mathfrak{A}_i| \leq qp^n$), and $P^{\mathfrak{A}_i} \trianglelefteq N_{\{\mathfrak{A}_i\}}^{\mathfrak{A}_i}$. Applying Lemma 2.1, A_k is a section of $GL(a,p) \leq GL(m+n,p)$, and (iii) holds.

Now suppose that $n=0$. Then $d=q+k<2k$, and G is more than $\frac{1}{2}d$-fold transitive, and must then contain A_d, which is impossible.

<u>Remark</u>: The theorem is still true if we suppose that G is k-fold transitive and contains a p-subgroup P fixing exactly k points and whose non-trivial orbits are in number not bigger than q or k-1.

As a consequence, we can easily prove some known results like theorem 13.11 of [19], which is due to Miller.

Now we prove a consequence that we will need:

<u>Proposition 2.3</u>. Let p be a prime number bigger than 3. If G is a (p+2)-fold transitive group of degree $d=p^2+p+1$, then G contains A_d.

<u>Proof</u>. Take $k=p+1$, $q=1$, $n=2$. Then $k \geq 5$, $k>q$, and G is a (k+1)-fold transitive group of degree qp^n+k. Now A_k is not a section of $GL(2,p)$. Hence, by Theorem 2.2, G must contain A_d.

§3. <u>Constructing Steiner systems from multiply transitive permutation groups.</u>

A Steiner system $S(t,k,v)$ is a pair $(\mathfrak{A},\mathfrak{B})$ of sets, where $|\mathfrak{A}|=v$, $\mathfrak{B} \subseteq 2^{\mathfrak{A}}$, each element of $\mathfrak{B}$ has cardinal k and t elements of $\mathfrak{A}$ belong to exactly one element of $\mathfrak{B}$.

The elements of $\mathcal{A}$ are called "points" and those of $\mathcal{B}$ "blocks".

Let G be a t-fold transitive group on a set $\mathcal{A}$, with $|\mathcal{A}|=v>t>1$. Suppose that for some $\Delta\subseteq\mathcal{A}$, with $|\Delta|=t-1$, $G_{\{\Delta\}}$ has imprimitivity blocks of size b on $\mathcal{A}\setminus\Delta$, where b is a non-trivial divisor of v-t+1. Let $B_1,\ldots,B_m$ be these blocks, where bm=v-t+1. If we take another subset Δ' of $\mathcal{A}$ of size t-1, then $\Delta'=\Delta^g$ for some $g\in G$, and $B_1{}^g,\ldots,B_m{}^g$ are imprimitivity blocks of $G_{\{\Delta'\}}$ on $\mathcal{A}\setminus\Delta'$. For any t distinct points $\alpha_1,\ldots,\alpha_t\in\mathcal{A}$, let us define $B(\alpha_1,\ldots,\alpha_t)$ $=\{\alpha_1,\ldots,\alpha_t\}\cup B$, where B is the imprimitivity block of $G_{\{\alpha_1,\ldots,\alpha_t\}}$ containing α_t. We have the following properties:

(i) $|B(\alpha_1,\ldots,\alpha_t)|=t-1+b$

(ii) If $\beta\in B(\alpha_1,\ldots,\alpha_t)\setminus\{\alpha_1,\ldots,\alpha_t\}$, then $B(\alpha_1,\ldots,\alpha_t)$ $=B(\alpha_1,\ldots,\alpha_{t-1},\beta)$.

(iii) If $\{\alpha_1,\ldots,\alpha_{t-1}\}=\{\beta_1,\ldots,\beta_{t-1}\}$, then $B(\alpha_1,\ldots,\alpha_t)$ $=B(\beta_1,\ldots,\beta_{t-1},\alpha_t)$.

(iv) For $g\in G$, $B(\alpha_1{}^g,\ldots,\alpha_t{}^g)=B(\alpha_1,\ldots,\alpha_t)^g$.

Let $\mathcal{B}=\left\{B(\alpha_1,\ldots,\alpha_t)\,\middle|\,\alpha_i\in\mathcal{A},\ \alpha_i\neq\alpha_j \text{ for } i\neq j\right\}$.

<u>Proposition 3.1</u>. The system $(\mathcal{A},\mathcal{B})$ is a Steiner system S(t,t-1+b,v) if and only if for pairwise distinct points $\alpha_1,\ldots,\alpha_t$, we have $B(\alpha_1,\ldots,\alpha_t)=B(\alpha_1,\ldots,\alpha_{t-2},\alpha_t,\alpha_{t-1})$.

<u>Proof</u>. If $(\mathcal{A},\mathcal{B})$ is a Steiner system S(t,t-1+b,v), then $B(\alpha_1,\ldots,\alpha_t)=B(\alpha_1,\ldots,\alpha_{t-2},\alpha_t,\alpha_{t-1})$, because these blocks both contain the t points $\alpha_1,\ldots,\alpha_t$. Suppose now that $B(\alpha_1,\ldots,\alpha_t)=B(\alpha_1,\ldots,\alpha_{t-2},\alpha_t,\alpha_{t-1})$ for any pairwise distinct points $\alpha_1,\ldots,\alpha_t$. Then we apply (iii) and hence $B(\alpha_1,\ldots,\alpha_t)=B(\beta_1,\ldots,\beta_t)$ if $\{\alpha_1,\ldots,\alpha_t\}=\{\beta_1,\ldots,\beta_t\}$. We prove now that if $\beta_1,\ldots,\beta_t$ are pairwise distinct elements of $B(\alpha_1,\ldots,\alpha_t)$, then $B(\beta_1,\ldots,\beta_t)=B(\alpha_1,\ldots,\alpha_t)$.

We do it by induction on $k=|\{\alpha_1,\dots,\alpha_t\}\setminus\{\beta_1,\dots,\beta_t\}|$. If $k=0$, then the result follows by the above remark. If $k>0$, then $\alpha_{j_1}=\beta_{\ell_1},\dots,\alpha_{j_{t-k}}=\beta_{j_{t-k}}$, and we have $B(\alpha_1,\dots,\alpha_t)$ $=B(\alpha_{j_1},\dots,\alpha_{j_t})$ and $B(\beta_1,\dots,\beta_t)=B(\beta_{\ell_1},\dots,\beta_{\ell_t})$. Now $\beta_{\ell_t}\in B(\alpha_{j_1},\dots,\alpha_{j_t})\setminus\{\alpha_{j_1},\dots,\alpha_{j_t}\}$, and therefore $B(\alpha_{j_1},\dots,\alpha_{j_{t-1}},\beta_{\ell_t})=B(\alpha_{j_1},\dots,\alpha_{j_t})$. Now $k-1=$ $|\{\alpha_{j_1},\dots,\alpha_{j_{t-1}},\beta_{\ell_t}\}\setminus\{\beta_{\ell_1},\dots,\beta_{\ell_t}\}|$, and so $B(\beta_{\ell_1},\dots,\beta_{\ell_t})$ $=B(\alpha_{j_1},\dots,\alpha_{j_{t-1}},\beta_{\ell_t})$. Therefore $B(\alpha_1,\dots,\alpha_t)=B(\beta_1,\dots,\beta_t)$, which is what we had to show. We get then a Steiner system, because for any t distinct points $\beta_1,\dots,\beta_t$, any block $B(\alpha_1,\dots,\alpha_t)$ containing $\beta_1,\dots,\beta_t$ is equal to $B(\beta_1,\dots,\beta_t)$.

We make now the following definition [10]: A permutation group G on $\mathcal{N}$ is generously t-fold transitive on $\mathcal{N}$ if for any $\Delta\subseteq\mathcal{N}$ with $|\Delta|=t+1$, $G_{\{\Delta\}}^{\Delta}\cong S_{t+1}$. G is almost generously t-fold transitive if $G_{\{\Delta\}}^{\Delta}\supseteq A_{t+1}$ for such Δ. We have the following implications:

G is (t+1)-fold transitive $\Rightarrow$ G is generously t-fold transitive $\Rightarrow$ G is almost generously t-fold transitive $\Rightarrow$ G is t-foldtransitive.

Proposition 3.2. The system $(\mathcal{N},\mathcal{B})$ is a Steiner system $S(t,t-1+b,v)$ whenever one of the following holds:

(i) G is generously t-fold transitive on $\mathcal{N}$.

(ii) G is almost generously t-fold transitive on $\mathcal{N}$, and $t\geq 3$.

Proof. Let $\gamma\in B(\alpha_1,\dots,\alpha_t)\setminus\{\alpha_1,\dots,\alpha_t\}$, where $\alpha_1,\dots,\alpha_t$ are pairwise distinct points of $\mathcal{N}$. If there is $g\in G$ such that $\gamma^g=\gamma$, g stabilizes $\{\alpha_1,\dots,\alpha_t\}$ and $\alpha_t{}^g=\alpha_{t-1}$, then $\gamma=\gamma^g\in B(\alpha_1,\dots,\alpha_t)^g=B(\alpha_1{}^g,\dots,\alpha_t{}^g)=B(\dots,\alpha_t,\dots,\alpha_{t-1})$ $=B(\alpha_1,\dots,\alpha_{t-2},\alpha_t,\alpha_{t-1})$ by properties (iii) and (iv) defined above. It is easily seen that such a permutation exists if G is generously t-fold transitive or if G is almost generously t-fold transitive with $t \geq 3$ (Take $g=(\gamma)(\alpha_{t-1},\alpha_t)(\alpha_1)\ldots(\alpha_{t-2})\ldots$ in the first case and $g=(\gamma)(\alpha_t,\alpha_{t-1},\alpha_{t-2})(\alpha_1)\ldots(\alpha_{t-3})\ldots$ in the second case. Hence $B(\alpha_1,\ldots,\alpha_t)\setminus\{\alpha_1,\ldots,\alpha_t\} \subseteq B(\alpha_1,\ldots,\alpha_t,\alpha_{t-1})$ and thus $B(\alpha_1,\ldots,\alpha_t)=B(\alpha_1,\ldots,\alpha_{t-2},\alpha_t,\alpha_{t-1})$. By Proposition 3.1, the result follows.

<u>Proposition 3.3</u>. If for pairwise distinct points $\alpha_1,\ldots,\alpha_t$ we have $B(\alpha_1,\ldots,\alpha_t)=\{\alpha_1,\ldots,\alpha_t\}\cup B$, where B is the union of all orbits of $G_{\alpha_1,\ldots,\alpha_t}$ on $\Omega\setminus\{\alpha_1,\ldots,\alpha_t\}$ which have some prescribed lengths, then $(\Omega,\mathcal{B})$ is a Steiner system $S(t,t-1+b,v)$.

<u>Proof</u>. It follows by hypothesis that $B(\alpha_1,\ldots,\alpha_{t-2},\alpha_t,\alpha_{t-1})$ $=B(\alpha_1,\ldots,\alpha_t)$. Hence we have a Steiner system by Proposition 3.1.

It can easily be shown that if all orbits of $G_{\alpha_1,\ldots,\alpha_t}$ on $\Omega\setminus\{\alpha_1,\ldots,\alpha_t\}$ have pairwise distinct length, then G is generously t-fold transitive.

Note that the group G is a subgroup of the automorphism group of the system $(\Omega,\mathcal{B})$.

We can find another way of constructing Steiner systems $S(t,k,v)$ from t-fold transitive groups.

<u>Proposition 3.4</u>: Let G be a t-fold transitive group on a set Ω, with $|\Omega|=v$. Suppose that there is some $\Delta\subseteq\Omega$ such that $|\Delta|=k>t$ and for $g\in G$, $\Delta^g=\Delta$ or $|\Delta\cap\Delta^g|<t$. If $\mathcal{B}=\{\Delta^g \mid g\in G\}$, then $(\Omega,\mathcal{B})$ is a Steiner system $S(t,k,v,)$, whose automorphism group contains G.

Proof. If we take t pairwise distinct points $\alpha_1,\dots,\alpha_t$, then there is an element g of G such that $\{\alpha_1,\dots,\alpha_t\}^g \subseteq \Delta$, because G is t-fold transitive. But then $\{\alpha_1,\dots,\alpha_t\} \subseteq \Delta^{g^{-1}}$ (a block): any t points lie in a block. If they were in another block $\Delta^h \neq \Delta^{g^{-1}}$, then we would have $\Delta^{hg} \neq \Delta$ and $t \leq |\Delta^h \cap \Delta^{g^{-1}}| = |\Delta^{hg} \cap \Delta|$, which contradicts the hypothesis. Hence $(\mathcal{A},\mathcal{B})$ is a Steiner system S(t,k,v) and G is an automorphism group of $(\mathcal{A},\mathcal{B})$.

Note that the result is still true if we suppose only that G is transitive on the subsets of size t of $\mathcal{A}$.

§4. Some assumed results and more propositions.

Proposition 4.1 [11]. If G is a primitive group on a set $\mathcal{A}$, if p^2 divides the order of G and if G contains an element of order p with less than p cycles of length p, then G is doubly transitive.

Proposition 4.2 [17]. If G is a primitive permutation group on a set $\mathcal{A}$, if for some prime divisor p of $|G|$, a Sylow p-subgroup P has 0 or 1 fixed point and all non-trivial orbits of length p, then $|P|=p$ or G is doubly transitive.

Proposition 4.3 [13]. If G is a doubly transitive group of degree n=kp+t (where p is prime) which does not contain A_n, if p divides $|G|$ and if a Sylow p-subgroup P of G has t fixed points and k orbits of length p, then either $|P|=p$ or $n \leq 12$.

Proposition 4.4 [14]. If G is a doubly transitive group of degree n which does not contain A_n, if the stabilizer H of two points has order divisible by p, if a Sylow p-subgroup Q of H has no orbit of length exceeding p, then $|Q|=p$.

Proposition 4.5 [16]. If G is a group of order not divisible by n^2, if G has a quadruply transitive action on a set Δ of size n+1 and a transitive action on a set Γ of size n, then n=3.

We prove now a proposition about primitive groups of degree 2p, where p is a prime.

Proposition 4.6. Let G be a primitive group of degree 2p on a set Ω, with p prime. If G contains an insoluble group H with two orbits of length p on Ω, then G is doubly transitive.

Proof. Suppose that G is simply transitive. Then [19,31.2] G has rank 3, with subdegrees 1, s(2s+1), (s+1)(2s+1), where $2p=(2s+1)^2+1$. Let Γ_1 and Γ_2 be the two orbits of H on Ω. Then H acts faithfully on each, otherwise G would be doubly transitive by [19,13.1](In fact, G would contain A_{2p}). Let $\gamma \in \Omega$ and $g \in G$. Then H^g is doubly transitive on Γ_1^g and Γ_2^g. If $\gamma \in \Gamma_i \cap \Gamma_j^g$, then H_γ is transitive on $\Gamma_i \setminus \{\gamma\}$ and $(H^g)_\gamma$ is transitive on $\Gamma_j^g \setminus \{\gamma\}$. Now $|\Gamma_i \setminus \{\gamma\}| = |\Gamma_j^g \setminus \{\gamma\}| = p-1 = 2s(s+1) > s(2s+1)$. Hence $(\Gamma_i \cup \Gamma_j^g) \setminus \{\gamma\} \subseteq \Delta(\gamma)$, where $\Delta(\gamma)$ is the orbit of length (s+1)(2s+1) of G_γ. Therefore $(s+1)(2s+1) \geq |(\Gamma_i \cup \Gamma_j^g) \setminus \{\gamma\}|$ $= p+p-1-|\Gamma_i \cap \Gamma_j^g|$, and $|\Gamma_i \cap \Gamma_j^g| \geq 2p-1-(s+1)(2s+1) = s(2s+1)$. Now, as G is primitive, there is some $g \in G$ such that $\Gamma_2 \neq \Gamma_1^g \neq \Gamma_1$, and we get $|\Gamma_1^g \cap \Gamma_2| \geq s(2s+1)$, $|\Gamma_1^g \cap \Gamma_1| \geq s(2s+1)$, and so $p = |\Gamma_1^g \cap \Gamma_1| + |\Gamma_1^g \cap \Gamma_2| \geq 2s(2s+1)$, that is $2s^2+2s+1 \geq 4s^2+2s$, and hence $s^2 \leq ½$, which is impossible, because $p > 1$.

Chapter II. Primitive groups of degree p^2+p+1, where p is a prime number.

Let G be a primitive group on a set Ω of size $n=p^2+p+1$ (where p is prime), such that p^2 divides the order of G. Let P be a Sylow p-subgroup of G; it fixes a point α of Ω. We may suppose that $p>3$, because groups of degree 7 and 13 are known.

§5. The general case - A theorem of Tsuzuku.

Proposition 5.1. G is doubly transitive.

Proof. P fixes a point α of Ω. We look at the other orbits of P on Ω. If P has p+1 orbits of length p, then G is doubly transitive by proposition 4.2. If P has k orbits of length p and n-kp fixed points on Ω, where $k \leq p$, then the pointwise stabilizer Q of one of these orbits of length p has order divisible by p and contains an element with less than p cycles of length p. Hence, by Proposition 4.1, G is doubly transitive. If P has an orbit Γ of length p^2, then G_α has an orbit containing Γ. If G was not doubly transitive, then G_α would have another orbit Δ, and by [19,18.1], we would have $P^\Delta \neq 1$, and so $|\Delta| \geq p$. But $|\Delta| \leq n-1-|\Gamma| = p$, and we would have $|\Delta| = p$, and hence $|P| = p$ by [15], which is impossible. Hence G is doubly transitive.

Proposition 5.2 [9]. P has a fixed point α, an orbit Δ of length p and an orbit Γ of length p^2.

Proof. As G_α is transitive on $\Omega \setminus \{\alpha\}$, which has size divisible by p, α is the only fixed point of P on Ω. If P had no orbit of length p^2, then it would have p+1 orbits of length p, and we would have $|P| = p$ by Proposition

4.3, which is impossible. Hence P has an orbit Γ of length p^2, and therefore it has also an orbit Δ of length p, otherwise it would fix another point more than α on $\mathcal{U}$.

<u>Lemma 5.3 [9]</u>. If p^3 divides the order of P, then P_Δ is transitive on Γ.

<u>Proof</u>. For $\beta \in \Delta$, $P_\Delta \in \mathcal{S}_p(G_{\alpha\beta})$. If P_Δ was not transitive on Γ, then we would have $|P_\Delta|=p$ by proposition 4.4, and hence $|P|=p^2$, which is impossible. Hence P_Δ is transitive on Γ. (We may also use Proposition 4.1).

In his thesis, Mc Donough [9] gave elementary proofs of these two results. We reproduce them here:

<u>Alternative proof of 5.2</u>. If P has $p+1$ orbits $\mathcal{U}_1,\dots,\mathcal{U}_{p+1}$ of length p on $\mathcal{U}$, then write $i\sim j$ if $P_{\mathcal{U}_i}=P_{\mathcal{U}_j}$. It is an equivalence relation. As p^2 divides the order of P, for each i there is some j such that $i\not\sim j$. Take now such i in an equivalence class of size r, where $r\leq \frac{1}{2}(p+1)$ (there is such a class, since there are at least two equivalence classes of $\sim$). Take j such that $i\not\sim j$. Pose $\Lambda=\mathrm{fix}\ P_{\mathcal{U}_i}$ and $\Theta=\mathrm{fix}\ P_{\mathcal{U}_j}$. For $\beta\in\mathcal{U}_i$, $R=P_{\mathcal{U}_i}\in\mathcal{S}_p(G_{\alpha\beta})$, and by Witt's lemma, $N=N_G(R)$ is doubly transitive on Λ. If S is the subgroup of $C_G(R)$ stabilizing all non-trivial orbits of R, then $S\triangleleft N$ and $S^\Lambda\neq 1$, since $S\supseteq P$. Hence S is transitive on Λ. Now, for each $\mathcal{U}_i$ outside Λ, $S^{\mathcal{U}_i}=R^{\mathcal{U}_i}$, which has order p. Therefore, $[S:S_{\mathcal{U}\setminus\Lambda}]$ is a power of p, and as $(p,|\Lambda|)=1$, $T=S_{\mathcal{U}\setminus\Lambda}$ is transitive on Λ. Similarly, we get a group U fixing $\mathcal{U}\setminus\Theta$ and transitive on Θ. Now $\Lambda\cap\Theta=\{\alpha\}$, and if we take $g\in U$ such that $\alpha^g\neq\alpha$, then $\langle T,T^g\rangle=M$ has support $\Lambda\cup\{\alpha^g\}$ and is doubly transitive on it. As $|\Lambda|=rp+1$, M has a support of size $rp+2$, and by

[19,13.2], G is $n-(rp+2)+2=(p^2-(r-1)p+1)$-fold transitive. As $r\leq \frac{1}{2}(p+1)$, we get $p^2-(r-1)p+1 \geq p^2+p+1-\frac{1}{2}p(p+1)=\frac{1}{2}p(p+1)+1 \geq p+2$, and G is $(p+2)$-fold transitive. But then $G=A_n$ or S_n by Proposition 2.3, and we get a contradiction, because a Sylow p-subgroup of A_n (or S_n) has an orbit of length p^2. The result follows.

<u>Alternative proof of 5.3.</u> If p^3 divides the order of P, and if P_Δ is not transitive on Γ, then P_Δ has p orbits $\Gamma_1,\dots,\Gamma_p$ on Γ, each of size p, because $P_\Delta \trianglelefteq P$. We put $i\sim j$ if $P_{\Delta\Gamma_i} \cong P_{\Delta\Gamma_j}$. This is an equivalence relation. As P is transitive on Γ, P permutes the subgroups $P_{\Delta\Gamma_i}$, and hence each equivalence class has the same size r, and $r \mid p$. Now $r\neq p$, otherwise $|P| =p^2$. Therefore $r=1$, and for each $j\neq i$, $P_{\Delta\Gamma_i}{}^{\Gamma_j}\neq 1$. Let $\gamma\in\Gamma_1$, and choose a Sylow p-subgroup W of $G_{\alpha\gamma}$ which contains $P_{\Delta\Gamma_1}$. Then W is conjugate to P_Δ, and hence it has p orbits of length p and p+1 fixed points. It has already the p-1 orbits $\Gamma_2,\dots,\Gamma_p$ of $P_{\Delta\Gamma_1}$. So it must have another one, Γ_1', included in $\Gamma_1\cup\Delta\setminus\{\alpha,\gamma\}$. If $\Gamma_1\cap\Gamma_1'=\emptyset$, then $[P_\Delta,W]=1$, because $P_\Delta{}^{\Gamma_i}=P_{\Delta\Gamma_1}{}^{\Gamma_i}=W^{\Gamma_i}$ for $i>1$. But then $\langle P_\Delta,W\rangle$ is a Sylow p-subgroup of G, and has p+1 orbits of length p, which is impossible. Hence $\Gamma_1\cap\Gamma_1'\neq\emptyset$. But then $\langle P_\Delta,W\rangle$ is transitive on $\Gamma_1\cup\Gamma_1'$, and as $(|\Gamma_1\cup\Gamma_1'|,p)=1$, the group $X=\langle x^p \mid x\in\langle P_\Delta,W\rangle\rangle$ is transitive on $\Gamma_1\cup\Gamma_1'$. But as $|\langle P_\Delta,W\rangle^{\Gamma_i}|=p$ for $i>1$, $X^{\Gamma_i}=1$ for such i. So X fixes $\Omega\setminus(\Gamma_1\cup\Gamma_1')$ and is transitive on $\Gamma_1\cup\Gamma_1'$. Now $|\Gamma_1\cup\Gamma_1'| \leq 2p-1<\frac{1}{2}n$, and hence $G=A_n$ or S_n by [19,13.5] and we get a contradiction, because P_Δ is transitive on Γ when $G=A_n$ or $G=S_n$.

We can now easily prove the result of Tsuzuku:

<u>Theorem 5.4[18]</u>. If p^3 divides the order of P, then $G=PSL(3,p)$, $PGL(3,p)$, A_n or S_n.

<u>Proof</u>. By Proposition 5.3, the group P_Δ has p+1 fixed points and an orbit Γ of length p^2. Let $g\in G$ such that $|\Gamma\cup\Gamma^g|$ is minimal for being bigger than p^2. Then (cfr. [6]), $\Gamma^g\setminus\Gamma$ is a block of $\langle P_\Delta{}^g, P_\Delta\rangle$. Hence $|\Gamma^g\setminus\Gamma|$ divides p^2, that is $|\Gamma^g\setminus\Gamma|=1$ or p. If $|\Gamma^g\setminus\Gamma|=1$, then $\langle P_\Delta{}^g, P_\Delta\rangle$ is doubly transitive of degree p^2+1, and by [19,13.2], G is (p+2)-fold transitive, and therefore $G=A_n$ or S_n by Proposition 2.3. If $|\Gamma^g\setminus\Gamma|=p$, then let $\Delta=\mathcal{U}\setminus\Gamma$. For any $h\in G$, we have: $|\Delta\cap\Delta^h|=|\mathcal{U}\setminus(\Gamma\cup\Gamma^h)|=n-|\Gamma\cup\Gamma^h|\leq n-|\Gamma\cup\Gamma^g|=1$. Hence, by proposition 3.4, $(\mathcal{U},\mathcal{B})$, where $\mathcal{B}=\{\Delta^h \mid h\in G\}$ is a Steiner system $S(2,p+1,p^2+p+1)$, that is a projective plane Π of order p. Now $G\subseteq \mathrm{Aut}\,\Pi$ and G is doubly transitive. By [12], Π is desarguesian and $PSL(3,p)\subseteq G$ (In fact, we can obtain a coordinatisation of Π over GF(p) without using [12], because we know some properties of P.)

§6. <u>The case where $|P|=p^2$: Triple primitivity.</u>

We know that for $P\in\mathcal{S}_p(G)$, P has a fixed point α, an orbit Δ of length p and an orbit Γ of length p^2. Let $\Delta'=\Delta\cup\{\alpha\}$. We suppose now that $|P|=p^2$. Pose $X=G_{\{\Delta'\}}$, $Y=G_\Delta$, and $Q=P\cap Y$. Then $|Q|=p$, $Q\in\mathcal{S}_p(Y)$ and Q is not transitive on Γ. As $Q\lhd P$, Q is half-transitive on Γ: it has p orbits $\Gamma_1,\dots,\Gamma_p$ on it, each of length p. Let $\Psi=\{\Gamma_1,\dots,\Gamma_p\}$.

Proposition 6.1. The group Y leaves each Γ_i invariant. X acts on Ψ and $X_\Psi = Y = X_{\Delta'}$. For any $Z \subseteq X$, $Z_\Psi = Z_{\Delta'} = Z \cap Y$, and in particular $C_G(Q)_\Psi = C_G(Q)_{\Delta'} = Q$. The group $C_G(Q)$ acts doubly transitively on Ψ and Δ'. The group Y acts faithfully on each Γ_i. The permutation characters of X_α on Δ and Ψ are the same.

Proof. As $Y \lhd X$ and X is transitive on Γ, Y is half-transitive on Γ. As p^2 does not divide the order of Y and Y contains Q, the orbits of Y on Γ are precisely the sets Γ_i. Now $Y \lhd X$, and so X permutes the sets Γ_i, and hence acts on Ψ. As $Q \in \mathcal{S}_p(G_{\alpha\beta})$ for $\beta \in \Delta$, $N_G(Q)$ is doubly transitive on Δ' [19,9.4]. As $C_G(Q) \lhd N_G(Q)$ and $C_G(Q) \supseteq P$, which acts nontrivially on Δ', $C_G(Q)$ is transitive on Δ'; as P is transitive on Δ, $C_G(Q)$ is doubly transitive on Δ'. In particular, X is doubly transitive on Δ'. Let $N = X_\Psi$; then $N \supseteq Y$ and $N/Y \cong N^{\Delta'}$. Now N acts faithfully on Γ, otherwise N_Γ would be a subgroup of G with degree not exceeding $p+1$, which is impossible since $p+1 < \frac{n}{3} - \frac{2\sqrt{n}}{3}$ and G does not contain A_n [19,15.1]. If $N_\alpha \neq Y$, then $N_\alpha^{\Delta} \neq 1$ and as $N_\alpha^{\Delta} \lhd X_\alpha^{\Delta}$, we must get N_α^{Δ} transitive, and hence N_α has $p+1$ orbits of length p and has order divisible by p^2, which is impossible. Therefore $N_\alpha = Y$, and if $N \neq Y$, then $N^{\Delta'}$ is regular on Δ'; hence $[N:Y] = 1$ or $p+1$. If N does not act faithfully on Γ_i, then N_{Γ_i} acts as a p'-group on Δ' and has at most $p-1$ orbits of length p on Γ, which is impossible, because G does not contain an element of order p with less than p cycles. Therefore N acts faithfully on each Γ_i, and $N^{\Delta'} \cong N/Y \cong N^{\Gamma_i}/Y^{\Gamma_i}$. By Frattini argument, $N^{\Gamma_i} = N_{N^{\Gamma_i}}(Q^{\Gamma_i}) \cdot Y^{\Gamma_i}$, and hence $N^{\Delta'} \cong \frac{N^{\Gamma_i}}{Y^{\Gamma_i}} \cong \frac{N_{N^{\Gamma_i}}(Q^{\Gamma_i})}{N_{Y^{\Gamma_i}}(Q^{\Gamma_i})}$, and so the order of $N^{\Delta'}$ divides p-1. But as $|N^{\Delta'}|=1$ or p+1, we get $|N^{\Delta'}|=1$ and hence N=Y. Therefore, $X_{\Delta'}=Y=X_{\Psi}$, and Y acts faithfully on each Γ_i. For $Z\leq X$, we have $Z_{\Psi}=Z\cap X_{\Psi}=Z\cap Y=Z\cap X_{\Delta'}=Z_{\Delta'}$, and as $C_G(Q)^{\Gamma_i}=Q^{\Gamma_i}$, we must get $C_G(Q)\cap Y=Q$, and so $C_G(Q)_{\Psi}=C_G(Q)_{\Delta'}=Q$. Hence $C_G(Q)/Q$ acts faithfully on Δ' and Ψ. Thus $C_G(Q)^{\Psi}$ must be doubly transitive, otherwise it would normalise P^{Ψ} (by Burnside's prime degree theorem), and then $C_G(Q)^{\Delta'}$ would normalise $P^{\Delta'}$, which is impossible. Now X_{α} acts on both Δ and Ψ with the same kernel Y. If X_{α}/Y is soluble, then both actions are equivalent, and hence the permutation characters of these actions are the same. If X_{α}/Y is insoluble, then X_{α} is doubly transitive on both Δ and Ψ because $p=|\Delta|=|\Psi|$ (by the same theorem of Burnside). Let π_{Δ} be the permutation character of X_{α} on Δ, and π_{Ψ} the one on Ψ. Now $\pi_{\Delta}=1+\varphi$ and $\pi_{\Psi}=1+\chi$, where φ and χ are irreducible. If $\pi_{\Delta}\neq\pi_{\Psi}$, then $\varphi\neq\chi\neq1\neq\varphi$, and $(\pi_{\Delta},\pi_{\Psi})=1$: this means that X_{α} is transitive on $\Delta\times\Psi$, and hence that p^2 divides the order of X_{α}/Y, which is impossible. Hence $\pi_{\Delta}=\pi_{\Psi}$.

Proposition 6.2 [9]. The Sylow p-subgroup P is elementary abelian and Q is a direct factor of $C_G(Q)$.

Proof. As $|P|=p^2$, P is abelian. By Proposition 1.1, if V is the transfer $C_G(Q)\longrightarrow P$, then $Q\cap\ker V=1$, because $N_{C_G(Q)}(P)\leq C_G(Q)$. If P is not elementary abelian, then P is cyclic and hence $P\cap\ker V=1$. This means that V is surjective and $C_G(Q)$ has a normal p-complement. But then $C_G(Q)/Q$ has also a normal p-complement, which is impossible because $C_G(Q)^{\Psi} \cong C_G(Q)/Q$ has no normal p'-group. Hence P is elementary abelian and so Q is a direct factor of P. By Proposition 1.2, Q is a direct factor of $C_G(Q)$.

Proposition 6.3. If $p>11$, then $p\equiv 7$ (mod.8), $C_G(Q)$ is triply transitive on Δ' and G is triply transitive on $\mathcal{U}$.

Proof. If $C_G(Q)$ is not triply transitive on Δ', then $C_G(Q)_{\alpha}^{\Delta'}$ is soluble (Burnside), and then $C_G(Q)/Q$ has p+1 Sylow p-subgroups. As it is a group of degree p, then $p\leq 11$ by [3]. Therefore, as $p>11$, $C_G(Q)$ must be triply transitive on Δ'. Now X_α has the same character π on Δ and Ψ, with $(\pi,\pi)=2$. Hence X_α has two orbits on $\Delta\times\Psi$ of respective lengths ap and bp, where a+b=p and $a<b$. Hence $X_{\alpha\{r_1\}}$ has two orbits on Δ, and of lengths a and b, and $X_{\alpha\beta}$ $(\beta\in\Delta)$ has two orbits on Ψ, also of lengths a and b. As X_α is transitive on Ψ, X must be transitive on $\Delta'\times\Psi$, and hence $X_{\{r_1\}}$ is transitive on Δ'. Therefore $X_{\{r_1\}}$ is transitive on Δ', with subdegrees 1, a, b. As $(a,b)=1$, $X_{\{r_1\}}$ is imprimitive on Δ' [19,17.5]. Hence $p+1=k(a+1)$ for some k. For each $\beta\in\Delta$, we get an orbit B_β of length a of $X_{\alpha\beta}$ on Ψ, and X_α permutes the p sets B_β. Hence they form the blocks of a (p,a,λ)-design, that is a set of p points, with blocks of size a and with λ blocks passing through any two points. The number of blocks is $p=\lambda\binom{p}{2}/\binom{a}{2}$, and hence $(p-1)\mid a(a-1)$, and similarly, $(p-1)\mid b(b-1)$. Now $p+1=k(a+1)$, and so $b=p+1-a-1=(k-1)(a+1)$. Thus $(p-1)\mid (a(a-1)b+b(b-1)a)=ab(a+b-2)=ab(p-2)$, and so $(p-1)\mid ab=a(k-1)(a+1)$. But then $(p-1)\mid a(k-1)(a+1)-(k-1)a(a-1)=2a(k-1)=2((a+1)k-k-a)$ $=2(p+1-k-a)=2(p-1)+2(2-k-a)$, and so $(p-1)\mid 2(a+k-2)$.

Obviously $k+a>2$, and so $p-1\leq 2(a+k-2)$, that is $(a+1)k-2 \leq 2(a+k-2)$, or $(a-1)(k-2)\leq 0$. Hence either $a=1$ or $k=2$ and $a=\frac{p-1}{2}$. Note that we can get this result in the proof of theorem 2 in [2]. In this theorem it is also proved that $p\equiv 7$ (mod.8) if $a\neq 1$ and that p is a Mersenne prime if $a=1$. As $p>3$, we must have $p\equiv 7$ (mod.8) in both cases. We get also $(ap,bp+p-1)=(ap,p^2+p-1)=(a,p^2+p-1)=1$ and $(bp,ap+p-1)=(bp,p^2+p-1)=(b,p^2+p-1)=1$.

For $\beta\in\Delta$, $X_{\alpha\beta}$ has orbits of lengths $p-1$, ap and bp on $\Omega\setminus\{\alpha,\beta\}$. Hence G is triply transitive on Ω or $G_{\alpha\beta}$ has orbits on $\Omega\setminus\{\alpha,\beta\}$ of the following lengths:

1°) $p-1$, ap, bp.	In case 1° and 2°, Q acts tri-
2°) $p-1$, p^2.	vially on one of these orbits.
3°) $ap+p-1$, bp.	In case 3° and 4°, the two
4°) ap, $bp+p-1$.	orbits have coprime lengths.

Hence G_α is imprimitive in these 4 cases [19, 17.5 & 18.4].

We investigate blocks of G_α on $\Omega\setminus\{\alpha\}$. Let B be an imprimitivity block of G_α on $\Omega\setminus\{\alpha\}$ containing $\beta\in\Delta$. Then $B\cap\Delta$ is a block of P on Δ, and hence $|B\cap\Delta|$ divides p. If $B\cap\Delta=\Delta$, then P stabilises B, and hence $B\cap\Gamma=\emptyset$, otherwise B would contain Γ and would be $\Omega\setminus\{\alpha\}$. If $|B\cap\Delta|=1$, then $B\cap\Gamma\neq\emptyset$, and as Q fixes Δ, Q stabilises B. Hence $B\cap\Gamma$ is a union of sets Γ_i. Now $B\cap\Gamma$ is a block of P on Γ. Hence $|B\cap\Gamma|=p$, otherwise $|B|=p^2+1$, which is impossible. Hence $|B|=p+1$ or $|B|=p$.

As the orbits of $G_{\alpha\beta}$ on $\Omega\setminus\{\alpha,\beta\}$ have pairwise distinct lengths, we may apply Proposition 3.3: G is a group of automorphisms of a Steiner system $S(2,1+b,n)$, where b is the size of an imprimitivity block of G_α on $\Omega\setminus\{\alpha\}$.

But we have proved that $b=p$ or $b=p+1$. If $b=p$, then we get a system $S(2,p+1,p^2+p+1)$, and then $G \supseteq PSL(3,p)$ as in Proposition 5.4, which is impossible, because p^3 divides the order of $PSL(3,p)$. If $b=p+1$, then the number of blocks is $\binom{p^2+p+1}{2}\Big/\binom{p+2}{2}=\frac{(p^2+p+1)p}{p+2}$, which is impossible, because this number is not an integer. So we get a contradiction, and G must be triply transitive on Ω.

Proposition 6.4. If $p \leq 11$, then $N_G(Q)$ is triply transitive on Δ' and G is triply transitive on Ω.

Proof. If X is triply transitive on Δ', then we prove the triple transitivity of G as in Proposition 6.3. Suppose now that X is not triply transitive on Δ', then $X/Y \cong C_G(Q)/Q \cong PSL(2,p)$ [3], and $X_{\alpha\beta}$ has two orbits of length $\frac{1}{2}(p-1)$ on $\Omega\setminus\{\alpha,\beta\}$. Now $(X_\alpha,\Delta) \cong (X_\alpha,\Psi)$ and so $X_{\alpha\beta}$ has 3 orbits on Ψ, of lengths 1, $\frac{p-1}{2}$ and $\frac{p-1}{2}$. The orbits of $X_{\alpha\beta}$ on $\Omega\setminus\{\alpha,\beta\}$ have lengths $\frac{1}{2}(p-1)$, $\frac{1}{2}(p-1)$, p, $\frac{1}{2}p(p-1)$, $\frac{1}{2}p(p-1)$. Any orbit of $G_{\alpha\beta}$ on $\Omega\setminus\{\alpha,\beta\}$ is a union of these. If G_α is not primitive on $\Omega\setminus\{\alpha\}$, then we get the same contradiction as in Proposition 6.3. By [19,18.4], $Q^{\Theta} \neq 1$ for any orbit Θ of $G_{\alpha\beta}$ on $\Omega\setminus\{\alpha,\beta\}$, and hence $G_{\alpha\beta}$ has no orbit of length smaller to p. We get then the following possibilities for the degrees of the orbits of $G_{\alpha\beta}$ on $\Omega\setminus\{\alpha,\beta\}$:

1) $2p-1$, $\frac{1}{2}p(p-1)$, $\frac{1}{2}p(p-1)$.

2) $\frac{1}{2}(3p-1)$, $\frac{1}{2}p(p-1)$, $\frac{1}{2}(p-1)(p+1)$.

3) p, $\frac{1}{2}(p-1)(p+1)$, $\frac{1}{2}(p-1)(p+1)$.

4) p, $\frac{1}{2}p(p-1)$, $\frac{1}{2}(p-1)(p+2)$.

5) $2p-1$, $\frac{1}{2}p(p-1)$.

6) $\frac{1}{2}(3p-1)$, $\frac{1}{2}(p-1)(2p+1)$.

7) p, $(p-1)(p+1)$.

8) $\frac{1}{2}(p-1)(p+2)$, $\frac{1}{2}p(p+1)$.

9) $\frac{1}{2}(p-1)(p+1)$, $\frac{1}{2}(p^2+2p-1)$.

10) $\frac{1}{2}p(p-1)$, $\frac{1}{2}(p^2+3p-2)$.

11) p^2+p-1.

By [19,17.5], the smallest and the longest orbits have not coprime orders. Hence we have only three possibilities:

- G is triply transitive.
- the case 2) with $p\neq 5$.
- the case 6) with $p=7$.

In the last two cases, we have an orbit Θ of length $p+\frac{1}{2}(p-1)$, with $\frac{1}{2}(p-1)\geqslant 3$. It is easy to show that $G_{\alpha\beta}$ is primitive on Θ. Hence, by [19,13.9], $G_{\alpha\beta}^{\ \Theta} \supseteq A_{\frac{1}{2}(3p-1)}$. By [1], we must have an orbit of size $\frac{3p-1}{2}\cdot\frac{3p-3}{2}$ or $|\Omega\setminus\{\alpha\}|$ is a power of 2, which is impossible. Hence G is triply transitive on Ω.

By [19,9.4], $N_G(Q)$ is triply transitive on Δ'.

<u>Theorem 6.5</u>. The group G is triply primitive on Ω.

<u>Proof</u>. Let B be a block of $G_{\alpha\beta}$ on $\Omega\setminus\{\alpha,\beta\}$ containing $\gamma\in\Delta\setminus\{\beta\}$. Then $B\cap(\Delta\setminus\{\beta\})$ is a block of $X_{\alpha\beta}$ on $\Delta\setminus\{\beta\}$, and hence $r=|B\cap(\Delta\setminus\{\beta\})|$ divides $p-1$. As $(r,p^2+p-1)=1$, $|B|=1$ or $B\nsubseteq\Delta\setminus\{\beta\}$. In this case, as Q fixes $\Delta\setminus\{\beta\}$ and is transitive on each Γ_i, $B\cap\Gamma$ is a union of some sets Γ_i. Hence $|B|=kp+r$, with $1\leq k\leq p$. If $t=\frac{p-1}{r}$, then G has t blocks conjugate to B and intersecting $\Delta\setminus\{\beta\}$. Hence $t(kp+r)\leq p^2+p-1$, that is $tk\leq p$. Now $kp+r$ divides p^2+p-1 and so $(kp+r)\mid(p^2+p-1)-t(kp+r)=p(p-tk)$, and as $(kp+r,p)=1$, we have $kp+r\mid p-tk$. But $kp+r>p\geqslant p-tk\geqslant 0$, and hence $p-tk=0$ As $t\mid p-1$, we get $t=1$, $k=p$ and $r=p-1$;

thus $|B|=p^2+p-1$. Hence $G_{\alpha\beta}$ has only trivial blocks, and therefore G is triply primitive.

<u>Proposition 6.6.</u> X is not quadruply transitive on Δ' and G is not quadruply transitive on $\mathcal{U}$.

<u>Proof.</u> Suppose that X is quadruply transitive on Δ'. Then p^2 does not divide $|X/Y|$ and X/Y acts on Ψ and Δ'. As $|\Psi|=p$ and $|\Delta'|=p+1$, we get p=3 by proposition 4.5, which is impossible. Hence X is not quadruply transitive on Δ'. Therefore G is not quadruply transitive on $\mathcal{U}$, otherwise $N_G(Q)$ would be quadruply transitive on Δ' [19,9.4], and X would also be quadruply transitive on Δ'.

<u>Proposition 6.7.</u> $p>11$.

<u>Proof.</u> If p=5 or p=11, then $q=p^2+p-1$ is prime. But then $G_{\alpha\beta}$ $(\beta\in\Delta)$ is a transitive group of prime degree, but not a Frobenius group. Hence $G_{\alpha\beta}$ is doubly transitive by Burnside's prime degree theorem, which is impossible, because G is not quadruply transitive. Therefore $5\neq p\neq 11$. If p=7, then X/Y acts faithfully and triply transitively on Δ' and acts faithfully on Ψ; but we can see that no group acts in such a way on sets of lengths 8 and 7. Therefore $p\neq 7$, and we conclude that $p>11$.

Most results of this chapter were proved by Mc Donough [9] or by Neumann and Praeger (unpublished). In the following chapter, we will prove some new results in the case where p^2 divides exactly the order of G.

Chapter III. Further results in the case where $|P|=p^2$.

§7. General properties of the elements of $G\setminus X$.

Proposition 7.1. For $i=1,\dots,p$, $G_{\{\Gamma_i\}} \subseteq X$.

Proof. Suppose that $x \in G$ stabilizes Γ_i but not Δ'. We know by Proposition 6.2 that $C_G(Q)=Q \times C$, and C acts doubly transitively on Δ' and Ψ. Each orbit of C intersects Γ_i in one point, and hence $C_{\{\Gamma_i\}}=C_{\Gamma_i}$ has p orbits of length $p-1$ on $\Gamma\setminus\Gamma_i$ and one orbit on Δ'. Let $H=\langle C_G(Q)_{\{\Gamma_i\}}, (C_{\{\Gamma_i\}})^x\rangle$. As $\Gamma_i^{\,x}=\Gamma_i$, Γ_i is an orbit of H and $H^{\Gamma_i}=Q^{\Gamma_i}$. Now there is an orbit of $(C_{\{\Gamma_i\}})^x$ which intersects both Δ' and $\Gamma\setminus\Gamma_i$, otherwise we would have $\Delta'=\Delta'^{\,x}$ or $\Delta'^{\,x}$ would be the union of orbits of length $p-1$. Hence H is transitive on $\Delta' \cup (\Gamma\setminus\Gamma_i)=\Omega\setminus\Gamma_i$. Now $[H:H_{\Gamma_i}] =p$, and hence H_{Γ_i} is transitive on $\Omega\setminus\Gamma_i$ because $(|\Omega\setminus\Gamma_i|,p)=1$ [19,17.1]. But then G is quadruply transitive by [19,13.1], which contradicts Proposition 6.6. Hence $G_{\{\Gamma_i\}} \subseteq X$.

Corollary. If $\Gamma_i^{\,x}=\Gamma_j$, then $x \in X$ (because there is $y \in X$ with $\Gamma_j^{\,y}=\Gamma_i$ and hence $\Gamma_j^{\,yx}=\Gamma_j$).

Proposition 7.2. If $x \in G\setminus X$, then $|\Gamma^x\setminus\Gamma|>1$.

Proof. Suppose that $|\Gamma^x\setminus\Gamma|=1$. Let $\{\beta\}=\Gamma^x\setminus\Gamma$. Then $\beta^y=\alpha$ for some $y \in X$, and $\Gamma^{xy}\setminus\Gamma=\{\alpha\}$. Let $H=\langle P,Q^{xy}\rangle$. Then H is transitive on $\Gamma\cup\Gamma^{xy}=\Omega\setminus\Delta$ and $H^{\Delta}=P^{\Delta}$. Hence $[H:H_\Delta]=p$ and as $(p,|\Gamma\cup\Gamma^{xy}|)=1$, H_Δ must be transitive on $\Gamma\cup\Gamma^{xy}$ [19,17.1] and therefore G must be quadruply transitive on Ω [19,13.1], which is impossible. Hence $|\Gamma^x\setminus\Gamma|\neq 1$ and so $|\Gamma^x\setminus\Gamma|>1$.

Proposition 7.3. If for $x \in G$, $\Gamma_i^{\,x}=\Gamma_i\setminus\{\delta\}\cup\{\gamma\}$, where $\gamma\in\Delta'$ and $\delta\in\Gamma_i$, then $(X_\alpha,\Delta)\cong(X_\alpha,\Psi)$ and $|\Gamma^x\setminus\Gamma|=p$.

We prove first the following lemma:

<u>Lemma 7.4</u>. For any $x \in G$ and $i=1,\ldots,p$, $\Gamma_i^x \cap \Gamma \neq \emptyset$.

<u>Proof</u>. Suppose that $\Gamma_i^x \cap \Gamma = \emptyset$. Then $\Gamma_i^x \subseteq \Delta'$ and hence for $g \in Q^x$, $|\Gamma^g \setminus \Gamma| \leq 1$. Therefore $Q^x \leq X$ by proposition 7.2. But then Q^x is a subgroup of X which has order p and fixes p points of Γ, which is impossible. Hence $\Gamma_i^x \cap \Gamma \neq \emptyset$.

<u>Proof of 7.3</u>. We know that $C_G(Q)=Q \times C$, $C_{\gamma\{\Gamma_i\}}=C_{\gamma\Gamma_i}$ and $C_G(Q)_{\gamma\{\Gamma_i\}}=Q \times C_{\gamma\Gamma_i}$. Let $D=C_{\gamma\Gamma_i}$. We know that D has p orbits of length $p-1$ on $\Gamma\setminus\Gamma_i$ and two orbits Δ_a and Δ_b on $\Delta'\setminus\{\gamma\}$, of respective lengths a and b, as in Proposition 6.3. Let $H=\langle Q^x, Q, D\rangle = \langle Q^x, C_G(Q)_{\gamma\{\Gamma_i\}}\rangle$. Then $\Pi = \{\gamma\}\cup\Gamma_i$ is an orbit of H and $\Gamma\setminus\Gamma_i$ is contained in an orbit of H. By Proposition 7.2 , $|\Gamma^x\setminus\Gamma| > 1$, and hence $(\Gamma\setminus\Gamma_i)^x \neq \Gamma\setminus\Gamma_i$. By Lemma 7.4, there is a Γ_j such that Γ_j^x intersects both $\Gamma\setminus\Gamma_i$ and $\Delta'\setminus\{\gamma\}$. If $\Delta_a \cap \Gamma^x \neq \emptyset \neq \Delta_b \cap \Gamma^x$, then H is transitive on $(\Gamma\setminus\Gamma_i)\cup\Delta_a\cup\Delta_b=\Theta$, and then $p^3=|Q|.|\Theta|$ divides $|H|=|\Theta|.|H_\eta|$ $(\eta \in \Gamma\setminus\Gamma_i)$, which is impossible. Hence either $\Delta_a \cap \Gamma^x \neq \emptyset = \Delta_b \cap \Gamma^x$ or $\Delta_b \cap \Gamma^x \neq \emptyset = \Delta_a \cap \Gamma^x$.
We may suppose the first. Then Π, $\Lambda = \Delta_a \cup (\Gamma\setminus\Gamma_i)$ and Δ_b are the orbits of H on Ω. If H_Π is transitive on Λ, then $K=\langle H_\Pi, X_{\Gamma_i}\rangle$ is transitive on $\Delta'\cup\Gamma=\Omega\setminus\Gamma_i$ and fixes Γ_i pointwise. But then G is quadruply transitive on Ω [19,13.1], which is impossible. Hence H_Π is not transitive on Λ. Now H_Π contains D, which has <u>a</u> fixed points and p orbits of length $p-1$. Hence H_Π is half-transitive on Λ, with orbits of length t, where $t \geq p-1$. We write $t=s(p-1)+r$ and $k=|\Lambda|/t$; of course $k>1$. Then $p(p-1)+a$ $=k(s(p-1)+r)=ks(p-1)+kr$. Now D fixes at least r points on each orbit of H_Π on Λ, and <u>a</u> points on Λ. Hence $kr \leq a$.

If kr=a, then $p(p-1)=|\Lambda|-a=|\Lambda|-kr=ks(p-1)$, and so ks=p. But then $k \mid (ks,kr)=(p,a)=1$ (because $a<p$), which is impossible. Therefore $kr<a$. But as $0\leq kr<a\leq p-1$ and $kr\equiv a$ (mod. $p-1$), we conclude that kr=0 and $a=p-1$. As $X_{\gamma\{\Gamma_1\}}$ has the same orbits on Δ' as D, we conclude that $(X_\gamma,\Delta'\setminus\{\gamma\})\cong(X_\gamma,\Psi)$ and so $(X_\alpha,\Delta)\cong(X_\alpha,\Psi)$. Since kr=0, we have r=0 and ks=p+1. Let L be the subgroup of H leaving all orbits of H_π on Λ invariant. Then H/L acts faithfully on the set of these k orbits. If $s>1$, then $k\leq\frac{p+1}{2}<p$ and so H/L is a group of degree smaller than p, and hence a p'-group. But then $Q\leq L$, $Q^x\leq L$ and so $H=\langle Q,Q^x,D\rangle\leq L$, which is impossible. Therefore s=1 and H_π has orbits of length p-1. Hence Δ_a must be one of them, because D stabilizes it and has p orbits of length p-1 on $\Lambda\setminus\Delta_a$. Therefore Δ_a is a block of H on Λ, and so Q^x fixes no point of Δ_a. If $\beta\in\Delta_a\setminus\Gamma^x$, then $\beta^{x^{-1}}\notin\Gamma$ and $\beta^{x^{-1}}$ is fixed by Q; but then β is fixed by Q^x, which is impossible. Hence $\Delta_a\subseteq\Gamma^x\setminus\Gamma$, and so $|\Gamma^x\setminus\Gamma|\geq|\Delta_a\cup\{\gamma\}|=p$. Now $\Delta_b=\{\beta\}$ for some $\beta\in\Delta'$. If $\beta\in\Gamma^x$, then β would be moved by Q^x, which is impossible. Hence $\beta\notin\Gamma^x$ and $\Gamma^x\setminus\Gamma=\Delta_a\cup\{\gamma\}$. Therefore $|\Gamma^x\setminus\Gamma|=p$.

As G is triply primitive on Ω, there is an element x of $G_{\alpha\beta}$ ($\beta\in\Delta$) such that $(\Delta\setminus\{\beta\})^x\neq\Delta\setminus\{\beta\}$ and $(\Delta\setminus\{\beta\})^x\cap(\Delta\setminus\{\beta\})\neq\emptyset$. But then $|\Delta'\cap\Delta'^x|\geq 3$ and so $|\Gamma^x\setminus\Gamma|\leq p-2$. Now, for any $x\in G$ such that $|\Gamma^x\setminus\Gamma|\leq p-2$, there is $x'\in G_{\alpha\beta\gamma}$ ($\beta,\gamma\in\Delta$) such that $|\Gamma^x\setminus\Gamma|=|\Gamma^{x'}\setminus\Gamma|$. Indeed, there are at least three points α',β',γ' in $\Delta'\cap\Delta'^x$. Then $\alpha'=\alpha''^x$, $\beta'=\beta''^x$, $\gamma'=\gamma''^x$ for some $\alpha'',\beta'',\gamma''\in\Delta'$. There are $y,z\in X$ such that $\alpha^y=\alpha''$, $\beta^y=\beta''$, $\gamma^y=\gamma''$, $\alpha'^z=\alpha$, $\beta'^z=\beta$, $\gamma'^z=\gamma$. But then $x'=yxz\in G_{\alpha\beta\gamma}$, and $|\Gamma^{yxz}\setminus\Gamma|=|\Gamma^{xz}\setminus\Gamma|=|\Gamma^{xz}\setminus\Gamma^z|=|\Gamma^x\setminus\Gamma|$, because $\Gamma^z=\Gamma=\Gamma^y$.

Therefore, if for $x \in G$, $|\Gamma^x \setminus \Gamma| \leq p-2$, then we may suppose that $x \in G_{\alpha\beta\gamma}$.

§8. Certain groups containing Q.

We consider subgroups M of G, such that $Q \leq M$ but $M \nleq X$. Then M has three sorts of orbits:

1°) The orbits $\mathcal{O}_1, \ldots, \mathcal{O}_m$ which intersect both Δ' and Γ. As $M \nleq X$, we have $m \neq 0$.

2°) The orbits $\Pi_1, \ldots, \Pi_v$ which lie inside Γ, if they exist. As $Q \leq M$, each Π_i is the union of some sets Γ_j.

3°) The orbits $\Lambda_1, \ldots, \Lambda_w$ which lie inside Δ', if they exist.

We pose $\Theta_i = \mathcal{O}_i \cap \Delta'$, $\Phi_i = \mathcal{O}_i \cap \Gamma$, $\Theta = \bigcup_{i=1}^{m} \Theta_i$, $t_i = |\Theta_i|$ and $t = |\Theta| = \sum_{i=1}^{m} t_i$

We will investigate the case where M satisfies one of the following properties:

(I) For any $x \in M$, $\Gamma^x = \Gamma$ or $\Gamma^x \setminus \Gamma = \Theta$ (it is equivalent to say that $\Theta^x = \Theta$ or $\Theta^x \cap \Theta = \emptyset$) and $t < p$.

(II) For any $x \in M$, $\Gamma^x = \Gamma$ or $\Gamma^x \setminus \Gamma = \Theta$ and $t < p$. The group M has support $\Gamma \cup \Theta$ (that is each Λ_i is trivial).

(II) is a particular case of (I), and the number of points of Δ' fixed by M is $p+1-t \geq 2$. If we take $x \in G$ such that $|\Gamma^x \setminus \Gamma|$ is minimal positive, then $|\Gamma^x \setminus \Gamma| \leq p-2 < p$, and so $\langle Q, Q^x \rangle$ satisfies (II). Suppose that M satisfies (I):

Proposition 8.1. For $i=1,\ldots,m$, Θ_i is a block of M on $\mathcal{O}_i$. Moreover, for any $i,j \leq m$, $M_{\{\Theta_i\}} = M_{\{\Theta_j\}}$, and so the action of M on Σ, the set of blocks of $\mathcal{O}_i$ conjugate to Θ_i, does not depend on i. Q acts on Σ with only one fixed point, and $|\Sigma| = 1+kp$, where $1 \leq k \leq \frac{p-1}{2}$; the group M acts primitively on Σ. Moreover, $t>1$, $v>0$ and for $j=1,\dots,v$, $M_{\Pi_j} \subseteq M_\Sigma$. If $k=1$, then each $t_i>1$.

Proof. M satisfies (I). If Θ_i was not a block of M on Λ_i, then we would have some $g\in M$ such that $\Theta_i^{\,g}\neq\Theta_i$ and $\Theta_i^{\,g}\cap\Theta_i\neq\emptyset$. But then we would have $\Theta^g\neq\Theta$ and $\Theta\cap\Theta^g\neq\emptyset$, which contradicts (I). Hence Θ_i is a block of M on Λ_i. The same argument shows that $M_{\{\Theta_i\}}=M_{\{\Theta_j\}}$ for $i,j\leq m$. If Σ_i is the set of blocks of Λ_i conjugate to Θ_i, then the action of M on Σ_i is the same as the one on Σ_j. Hence M acts on Σ, which does not depend on i. As each $t_i<p$ and as Q acts without fixed point on Γ, Q may not stabilize any $\Theta_i^{\,g}$ which lies in Γ, and hence Q fixes only one point of Σ (corresponding to Θ_i). Hence $|\Sigma|=1+kp$, with $1\leq k\leq p$. Now $t>1$ by proposition 7.2. If $k>\frac{p}{2}$, then $p^2=|\Gamma|\geq|\bigcup_i\Phi_i|$ $=tkp>t\frac{p^2}{2}$, which is impossible, since $t\geq 2$. Hence $k\leq\frac{1}{2}p$, and so $k\leq\frac{p-1}{2}$. If $v=0$, then $tkp=|\bigcup_i\Phi_i|=|\Gamma|=p^2$, and so $p\mid tk$. But then $k=p$, since $t<p$. Therefore $v>0$.

For $j=1,\dots,v$, M_{Π_j} leaves some $\Gamma_i\subseteq\Pi_j$ invariant. Hence $M_{\Pi_j}\subseteq X$ by proposition 7.1, and so $M_{\Pi_j}\subseteq M_{\{\Theta_i\}}$ for some $i=1,\dots,m$. This means that M_{Π_j} fixes one point of Σ, and as $M_{\Pi_j}^{\Sigma}\triangleleft M^{\Sigma}$, we must have $M_{\Pi_j}^{\Sigma}=1$, that is $M_{\Pi_j}\subseteq M_\Sigma$.

If M was imprimitive on Σ, then a block would have size $1+lp$, with $1\leq l<k$, because Q acts on Σ with one fixed point and k orbits of length p. But then $1+lp$ divides $1+kp$ and $\frac{1+kp}{1+lp}=1+l'p$, with $l'\geq 1$; this gives $1+kp=(1+lp)(1+l'p)\geq(1+p)^2>1+p^2$, which is impossible. Therefore M is primitive on Σ. If $k=1$, then each $t_i>1$, otherwise $\Lambda_i=(\Gamma_j\setminus\{\delta\})\cup\{\gamma\}$, where $\gamma\in\Delta'$ and $\delta\in\Gamma_j$, and so $t=p$ by proposition 7.3, which is impossible.

Proposition 8.2. If M satisfies (II), then M is $\frac{3}{2}$-fold transitive of rank 1+k on Σ (that is with non-trivial subdegrees equal to p). For i=1,...,v, the group $L=M\cap X$ leaves each $\Gamma_j\leq\Pi_i$ invariant and $M_{\Pi_i}=M_\Sigma$. If $k>1$, then each $t_i=1$ (i=1,...,m), M is soluble and $M_\Sigma=1$.

Proof. The group $L=M\cap X=M_{\{\Theta_i\}}$ (i=1,...,m) fixes some point of Δ', and we may suppose that it is α. Then L has p-t+m $=|\Delta\setminus\Theta|$ +m orbits on Δ. Consider the action of L on Δ and on the sets Φ_i. Suppose that L has l non-trivial orbits on Σ, of respective sizes $m_1p,\dots,m_lp$. If Θ_i' (conjugate to Θ_i) is in the orbit of size m_jp, then $[M_{\{\Theta_i'\}}:L_{\{\Theta_i'\}}]$ $=m_jp$. As $M_{\{\Theta_i'\}}$ is transitive on Θ_i', each orbit of $L_{\{\Theta_i'\}}$ on Θ_i' has length equal to at least $\frac{t_i}{(t_i,m_jp)}$ [19,17.1]. As $(t_i,m_jp)\leq m_j$, it follows that $L_{\{\Theta_i'\}}$ has at most m_j orbits on Θ_i', and hence L has at most m_j orbits on $(\Theta_i')^L$ (the union of blocks in the orbit of length m_jp). If $\bar{k}_i$ is the number of orbits of L on Φ_i, then $\bar{k}_i\leq\sum_{j=1}^{l}m_j=k$. Let $\Psi_i=\{\Gamma_j\in\Psi\mid\Gamma_j\subseteq\Phi_i\}$ and $\Psi'=\Psi\setminus\bigcup_i\Psi_i$. Then L acts on Ψ_i with k_i orbits, where $k_i\leq\bar{k}_i\leq k$. Now $|\Psi'|$=p-kt, and L has s orbits on Ψ', with $1\leq s\leq$ p-kt. Therefore L has $(\sum_i k_i)+s$ orbits on Ψ. But $L\subseteq X_\alpha$, and we know that X_α has the same permutation character on Δ and Ψ. Hence $p-t+m=s+\sum_i k_i$. This gives:

$$p-t+m=s+\sum_i k_i\leq\sum_i\bar{k}_i+s\leq km+s\leq km+p-kt=p-t+m+(k-1)(m-t)$$
$$\leq p-t+m \text{ because } k\geq 1 \text{ and } m\leq t.$$

Therefore $k=k_i=\bar{k}_i$ for i=1,...,m, and s=p-kt, 0=(k-1)(m-t). This means first that if $k>1$, then m=t, that is $t_i=1$ for i=1,...,m. Secondly, L has p-kt$=|\Psi'|$ orbits on Ψ'; in other words L leaves each $\Gamma_j\in\Psi'$ invariant. Thirdly, L has k orbits on Ψ_i and on Φ_i. If k=1, then L is transitive on Φ_i, and hence it has two orbits on Σ: M is doubly transitive on Σ (and so it has rank 1+k). If $k>1$, then $(M^{\Sigma},\Sigma)=(M^{\Lambda_i},\Lambda_i)$, and hence L has k orbits on $\Sigma\setminus\{\vartheta\}$, where ϑ is the point of Σ corresponding to the sets Θ_i. As each non-trivial orbit of L on Σ has length not smaller than p, it follows that they have length p, and so M is $\frac{3}{2}$-fold transitive of rank 1+k on Σ. By 8.1 , we know that for i=1,...,v, we have $M_{\Pi_i}\subseteq M_{\Sigma}$ by proposition 8.1. Let us prove the converse: The group $M_{\Sigma}\leq L$, and hence M_{Σ} leaves each $\Gamma_j\subseteq\Pi_i$ invariant. As $M_{\Sigma}^{\Gamma_j}\trianglelefteq M_{\{\Gamma_j\}}^{\Gamma_j}$ and M_{Σ} has no p-element, it follows that $M_{\Sigma}^{\Gamma_j}=1$, and so $M_{\Sigma}^{\Pi_i}=1$, and therefore $M_{\Sigma}=M_{\Pi_i}$. Finally, if $k>1$, then M_{Σ} fixes each Π_j, each Λ_i and $\Delta'\setminus\Theta$ pointwise, and so $M_{\Sigma}=1$. It remains then to show that $M\cong M^{\Sigma}$ is soluble in this case: if it was not, then we would have $M\cong PSL(2,p-1)$ and p would be a Fermat prime [8], which is impossible because $p\equiv 7$ (mod.8).

To prove that M^{Σ} is soluble when k=1, we need the following lemma:

<u>Lemma 8.3</u>. For i,j=1,...,p, $G_{\{\Gamma_i\cup\Gamma_j\}}\subseteq X$.

<u>Proof</u>. Suppose false. Then there is $x\in G\setminus X$ which leaves $\Gamma_i\cup\Gamma_j$ invariant. Thus $\Gamma_1\cap\Delta'\neq\emptyset$ for some $\Gamma_1\in\Psi$. By Lemma 7.4, $\Gamma_1\cap\Gamma\neq\emptyset$. By Proposition 6.2, we know that $C_G(Q)=C\times Q$ for some subgroup C of G. By Propositions 6.3 and 6.7, C is triply transitive on Δ', and hence C_{α} is doubly transitive on Ψ. Now $C_{\{\Gamma_i\}}$ is transitive on Δ' and on $\Psi\setminus\{\Gamma_i\}$. As C_{α} is doubly transitive on Ψ, it follows that $C_{\alpha\{\Gamma_i\}}$ is transitive on $\Psi\setminus\{\Gamma_i\}$. Therefore $C_{\{\Gamma_i\}}$ is transitive on $\Delta'\times(\Psi\setminus\{\Gamma_i\})$ and hence $C_{\{\Gamma_i\},\{\Gamma_j\}}$ is transitive

on Δ'. But each orbit of C intersects each $\Gamma_1 \in \Psi$ in exactly one point, and so $C_{\{\Gamma_1\}} = C_{\Gamma_1}$. Therefore $C_{\{\Gamma_i\},\{\Gamma_j\}} = C_{\Gamma_i \cup \Gamma_j}$. As $D = C_{\Gamma_i \cup \Gamma_j}$ is transitive on Δ' and as some $\Gamma_1^{x^i}$ intersects both Δ' and $\Gamma \setminus (\Gamma_i \cup \Gamma_j)$, the group $H = \langle D, Q, D^x, Q^x \rangle$ must have an orbit Λ such that $\Delta' \subseteq \Lambda \subseteq \Gamma \setminus (\Gamma_i \cup \Gamma_j)$ and $\Lambda \cap \Gamma \neq \emptyset$; then $|\Lambda| = zp+p+1$, where $1 \leq z \leq p-2$. Now H leaves $\Gamma_i \cup \Gamma_j$ invariant, and so $K = H_{\Gamma_i \cup \Gamma_j}$ is half-transitive on Λ. By proposition 7.1, $K \leq X$ because $K \leq G_{\{\Gamma_i\}}$. Therefore K leaves Δ' invariant; but $D \subseteq K$ and D is transitive on Δ'. Hence Δ' is an orbit of K, and as K is half-transitive on Λ, it follows that $p+1 = |\Delta'|$ divides $|\Lambda| = zp+p+1$. But then $p+1 \mid z$, which is impossible, since $1 \leq z \leq p$. Therefore we have a contradiction, and so $G_{\{\Gamma_i \cup \Gamma_j\}} \subseteq X$.

<u>Proposition 8.4</u>. If M satisfies (II) and if k=1, then M^{Σ} is soluble.

<u>Proof</u>. Let $N = M^{\Sigma}$. Then N acts faithfully on each Π_i and on Σ. Let $q_i = |\Pi_i|/p$. Then for $\vartheta \in \Sigma$, N_ϑ has q_i orbits on Π_i, each of length p. Hence N has q_i orbits on $\Sigma \times \Pi_i$, each of length $(p+1)p$, and for $\pi \in \Pi_i$, N_π has q_i orbits on Σ, each of length $(p+1)/q_i$. If $\Sigma_1, \ldots, \Sigma_{q_i}$ are the orbits of N_ϑ on Π_i, then $N_{\theta\Sigma_j} = N_{\Sigma} = 1$ for each j, otherwise p^2 would divide the order of N. Hence N_ϑ acts faithfully on each Σ_j. If N_ϑ is doubly transitive on $\Sigma \setminus \{\vartheta\}$, then it must also be doubly transitive on each Σ_j, and N_θ has the same permutation character on Σ and Σ_j. For $\pi \in \Sigma_j$, $N_{\vartheta\pi}$ has two orbits on Σ_j, and hence it must have two orbits on $\Sigma \setminus \{\theta\}$, of respective lengths a and b. But $N_{\theta\pi} \subseteq N_\pi$, which is half-transitive on Σ. As we may not

have $1=a=b$, it follows that N_{π} has at most two orbits on Σ, and so $q_i \leq 2$ in this case. If N_{ϑ} is not doubly transitive on $\Sigma\setminus\{\vartheta\}$, then N_{ϑ} is soluble by Burnside's prime degree theorem, and so N is a Zassenhaus group of degree p+1, N is insoluble and not triply transitive. It is known that such group must be isomorphic to PSL(2,p). Thus $|N_{\vartheta}|=\frac{1}{2}p(p-1)$, and for $\pi\in\Sigma_j$, $N_{\vartheta\pi}$ has four orbits on Σ, of respective lengths $1,1,\frac{p-1}{2}$ and $\frac{p-1}{2}$. As $N_{\vartheta\pi}\leq N_{\pi}$, which is half-transitive on Σ, it follows that N_{π} has at most two orbits on Σ, and so $q_i \leq 2$ also in this case. Therefore $|\Pi_i|\leq 2p$ in any case. By proposition 7.1, it is clear that $|\Pi_i|\neq p$ while $|\Pi_i|=2p$ is impossible by Lemma 8.3, because $M\not\leq X$. Therefore we have a contradiction, and so M^{Σ} must be soluble.

We sum up our results: If M satisfies (II), then M^{Σ} acts on Σ as a soluble primitive $\frac{3}{2}$-fold transitive group of degree 1+kp, where $1\leq k\leq\frac{p-1}{2}$. For i+1,...,v, $|\Pi_i|>2p$ and $M_{\Sigma}=M_{\Pi_i}$; the group $L=M\cap X$ stabilizes each $\Gamma_j\subseteq\Pi_i$. Note that $v\neq 0$. If k=1, then each $t_i>1$. If $k>1$, then each $t_i=1$ and so $M_{\Sigma}=1$; therefore M is soluble in this case.

REFERENCES.

[1] CAMERON,P.J. "Permutation groups with multiply transitive suborbits." Proc. London Math. Soc.(3)25(1972),427-440.

[2] CAMERON,P.J. "On groups of degree n and n-1 and highly-symmetrical edge colourings" J. London Math. Soc. (2) 9, 385-391(1975).

[3] FROBENIUS,F.G. "Über Gruppen des Grades p oder p+1." Sitz. Kön. Preusz. Akad. Wiss. Berlin (1902), 351-369.

[4] GASCHÜTZ,W. "Zur Erweiterungstheorie endlicher Gruppen." Crelle's J. 190, 93-107 (1952).

[5] GORENSTEIN,D. "Finite Groups." Harper & Row, 1968.

[6] JORDAN,C. "Théorèmes sur les groupes primitifs." J. de Math. (2) XVI (1871), 383-408.

[7] JORDAN,C. "Sur la limite de transitivité des groupes non alternés." Bull. Soc. Math. France, t.I, 40-71 (1873).

[8] McDERMOTT,J.P.J. "Characterization of some $\frac{3}{2}$-transitive groups." Math.Z. 120, 204-210 (1971).

[9] McDONOUGH,T.P. "Some problems in the theory of groups." Ph.D. Thesis, Oxford University, 1972.

[10] NEUMANN,P.M. "Generosity and characters of multiply transitive permutation groups." Proc. London Math. Soc. (3) 31, 457-481 (1975).

[11] O'NAN,M.E. "Estimation of Sylow subgroups of primitive permutation groups." Math.Z. 147, 101-111 (1976).

[12] OSTROM,T.G. & WAGNER,A. "On projective and affine planes with transitive collineation groups. Math.Z. 71, 186-199 (1959).

[13] PRAEGER,C.E. "On the Sylow subgroups of a doubly transitive permutation group." I, Math.Z.137, 155-171 (1974).

[14] PRAEGER,C.E. "On the Sylow subgroups of a doubly transitive permutation group." II, Math.Z.143,131-143 (1975).

[15] RIETZ,H.L. "On primitive groups of odd order." Amer. J. of Math. 26, 1-30 (1904).

[16] SAXL,J. "Multiply transitive permutation groups." Ph.D. Thesis, Oxford University, 197 .

[17] SCOTT,L. "A double transitivity criterion." Math.Z. 115, 7-8 (1970).

[18] TSUZUKU,T. "On doubly transitive permutation groups of degree $1+p+p^2$, where p is a prime number". J.Algebra 8 (1968), 143-147.

[19] WIELANDT,H. "Finite Permutation Groups" Academic Press, 1968.

Note added in proof:

With the results of chapter III, we can prove the following:

Proposition 8.5. The group Y is soluble and $X=N_G(Q)$.

Proof. Take x such that $|\Gamma^x \setminus \Gamma|$ is minimal positive. Then $M=\langle Y,Y^x\rangle$ satisfies (II) and we know that M acts on a set Σ, with M^Σ soluble and $p \nmid |M_\Sigma|$. Hence $Y^\Sigma \cong Y/Y_\Sigma$ is soluble and Y_Σ is a normal p'-subgroup of Y. By proposition 6.1, Y acts faithfully on each Γ_i. Therefore $Y_\Sigma=1$ and $Y \cong Y^\Sigma$ is soluble. Thus $Q=O_p(Y)$ and so Q char $Y \lhd X$, which implies that $Q \lhd X$. Now $N_G(Q)$ stabilizes Δ' and so we must have $X=N_G(Q)$.