TRANSITIVE PERMUTATION GROUPS OF DEGREE $p=2q+1$, p AND q BEING PRIME NUMBERS

NOBORU ITO[1]

1. Introduction. Let p be a prime number such that $q=\frac{1}{2}(p-1)$ is also a prime. Let Ω be the set of symbols $1, \cdots, p$, and $\mathfrak{G}$ be a non-solvable transitive permutation group on Ω. Such permutation groups were first considered by Galois in 1832 [**I**, §327; **III**, §262]: *if the linear fractional group $LF_2(l)$ over the field of l elements, where l is a prime number not smaller than five, contains a subgroup of index l, then l equals either five or seven or eleven.* These three permutation groups will be denoted by A_5, G_7 and G_{11}. G_7 has degree 7 and order 168; G_{11} has degree 11 and order 660. Next in 1861 two permutation groups, one, which has degree 11 and order 7,920, and the other, which has degree 23 and order 10,200,960, were found by Mathieu [**16**; **17**]. These two permutation groups will be denoted by M_{11} and M_{23}.

We say that $\mathfrak{G}$ is *a permutation group of type M*, if $\mathfrak{G}$ does not contain the alternating group A_p of the same degree. Then G_7, G_{11}, M_{11} and M_{23} are permutation groups of type M. Now the following problem arises: *does there exist any permutation group of type M different from G_7, G_{11}, M_{11} and M_{23}?*

In 1902 Jordan proved the nonexistence of permutation groups of type M for $p=47$ and $p=59$ [**23**; **IV**, §116]. In 1908 Miller proved the nonexistence of permutation groups of type M for $p=83$. But he did not even write down the proof explicitly [**18**].

Now $\mathfrak{G}$ is doubly transitive by a famous theorem of Burnside. In particular, the order of $\mathfrak{G}$ is divisible by q. Let $\mathfrak{Q}$ be a Sylow q-subgroup of $\mathfrak{G}$. Let $Ns\mathfrak{Q}$ and $Cs\mathfrak{Q}$ denote the normalizer and centralizer of $\mathfrak{Q}$ in $\mathfrak{G}$. In 1955 Fryer proved remarkable theorems [**7**], which may be stated as follows. *Let the index of $Cs\mathfrak{Q}$ in $Ns\mathfrak{Q}$ be even. Then* (i) *if $\mathfrak{G}$ contains an odd permutation, $\mathfrak{G}$ coincides with the symmetric group S_p of the same degree, and* (ii) *if $\mathfrak{G}$ does not contain any odd permutation and $Ns\mathfrak{Q}$ satisfies a certain appropriate condition, $\mathfrak{G}$ coincides with A_p.*

An address under the title *Permutation groups of prime degree*, delivered before the Chicago Meeting of the Society, on April 14, 1962 by invitation of the Committee to Select Hour Speakers for Western Sectional Meetings; received by the editors June 16, 1962.

[1] This address was delivered at a time the speaker was receiving support from the National Science Foundation (G-9654).

He also verified the above mentioned results of Jordan and Miller.

In 1958 Parker and Nikolai, using computers (UNIVAC Scientific Computer, Model 1103A), verified the nonexistence of further permutation groups of type M for $p \leqq 4079$ [22]. As a result of their computation, they are led to the conjecture; for $p > 23$ there exists no permutation group of type M.

However up to now, there exists no theorem which assures the nonexistence of permutation groups of type M for a set of prime numbers containing possibly infinitely many members. Therefore, our primary intention is to establish two theorems of this nature.

THEOREM V. *Let p be a prime number >23 satisfying the following conditions*:

(1) $q=\frac{1}{2}(p-1)$ *and* $r=\frac{1}{4}(p-3)$ *are also prime numbers,*

(2) $p-4$ *is a prime number, and,*

(3) p *is not of the form* $18m^2+5$, *where m is an odd integer.*

Then there exists no permutation group of type M for p.

For instance, $p=222{,}647$ satisfies the conditions of Theorem V.

THEOREM VIII. *Let p be a prime number >23 satisfying the following conditions*:

(1) $q=\frac{1}{2}(p-1)$, $r=\frac{1}{4}(p-3)$ *and* $s=\frac{1}{8}(p-7)$ *are also prime numbers, and,*

(2) $p-6$ *is a prime number.*

Then there exists no permutation group of type M for p.

For instance, $p=178{,}799$ satisfies the conditions of Theorem VIII.

The condition (3) in Theorem V can be dropped if it can be shown that the only permutation groups of type M which are not triply transitive are isomorphic to either G_7 or G_{11}. *In case G is not doubly primitive* [**V**, §10], Wielandt proved in 1955 that $\mathfrak{G}$ *is isomorphic to* G_7 (for a proof see [**11**]). Hence in further investigations, we shall assume the double primitivity of $\mathfrak{G}$. Then an interesting result for permutation groups of degree $2q$ due to Wielandt [**29**] may be useful in this connection.

Furthermore the condition (2) in Theorem VIII can be dropped, if the conjecture of Schreier concerning the solvability of the outer automorphism group of a simple group is true, because of the following remarkable theorem of Wielandt [**30**]: *every permutation group which does not contain the alternating group of the same degree is at most septuply transitive, if the above conjecture of Schreier is true.*

We prove Theorems V and VIII by successively showing that $\mathfrak{G}$ has higher and higher degree of transitivity. Since $\mathfrak{G}$ is already

doubly transitive by a theorem of Burnside, our first step is to show the triple transitivity of $\mathfrak{G}$. In order to do this and to proceed further, our present method requires us to assume that (not only p, $q=\frac{1}{2}(p-1)$ but also) $r=\frac{1}{4}(p-3)$ is a prime number, even though some parts of our proofs do not depend on this assumption. Hence throughout this paper we impose

ASSUMPTION a: *$r=\frac{1}{4}(p-3)$ is a prime number.*

It should be mentioned here that $p=7$, 11 and 23 satisfy this assumption. (It is convenient to admit 1 as a prime number.) Hence throughout this paper we make the further

ASSUMPTION b: *p is greater than* 23.

Then the triple transitivity of $\mathfrak{G}$ is an easy consequence of the above mentioned theorem of Wielandt [29] (see Theorem I in §2).

In our proof of quadruple transitivity of $\mathfrak{G}$ we can assume that $\mathfrak{G}$ is a permutation group of type M, and that $\mathfrak{G}$ does not contain any odd permutation. Let $\mathfrak{P}$ be a Sylow p-subgroup. Let $Ns\mathfrak{P}$ and $Cs\mathfrak{P}$ be the normalizer and centralizer of $\mathfrak{P}$ in $\mathfrak{G}$ respectively. Then we have that $\mathfrak{P}=Cs\mathfrak{P}$ and $Ns\mathfrak{P}$ has order pq. It is rather easy to show that q divides the order of $\mathfrak{G}$ only to the first power, $\mathfrak{Q}=Cs\mathfrak{Q}$ and $Ns\mathfrak{Q}$ has order either $q(q-1)$ or qr. Now our proof mainly relies on the following results of Frobenius [5; 6; 25] and Brauer [3] (see Theorem II in §3).

PROPOSITION A (FROBENIUS). *Let X^0_0 and X_{00} be irreducible characters of S_p corresponding to Young diagrams*

$$\begin{array}{l} 0 \quad 0 \cdots 0 \\ 0 \\ 0 \end{array}$$

and

$$\begin{array}{l} 0 \quad 0 \cdots 0 \\ 0 \quad 0. \end{array}$$

Then $\mathfrak{G}$ is quadruply transitive, if and only if X^0_0 restricted on $\mathfrak{G}$ and X_{00} restricted on $\mathfrak{G}$ are irreducible characters of $\mathfrak{G}$. We have that

$$X^0_0(S) = \tfrac{1}{2}(\alpha(S) - 1)(\alpha(S) - 2) + \beta(S)$$

and

$$X_{00}(S) = \tfrac{1}{2}\alpha(S)(\alpha(S) - 3) + \beta(S),$$

for every permutation S of S_p, where $\alpha(S)$ denotes the number of symbols

of Ω fixed by S and $\beta(S)$ denotes the number of transpositions in the cycle structure of S. In particular, the degrees of X_0^0 and X_{00} are equal to $(q-1)p+1$ and $(q-1)p$, respectively.

PROPOSITION B (BRAUER). *The degree of an irreducible character X of $\mathfrak{G}$ is congruent to either 1 or 0 or -1 or $-\delta_p q$ modulo p and either 1 or 0 or -1 or $\delta_q r$ modulo q, where δ_p and δ_q are equal to ± 1, respectively. Furthermore if the order of $N_S\Omega$ equals $q(q-1)$, then $\delta_q r$ can be omitted above. We say that X has p-type A or D or B or C, according as the degree of X is congruent to 1 or 0 or -1 or $-\delta_p q$ modulo p, respectively. Similarly we say that X has q-type A or D or B or C, according as the degree of X is congruent to 1 or 0 or -1 or $-\delta_q r$ modulo q, respectively. Let P be an element of order p of $\mathfrak{G}$. Then we have that $X(P)=1$ or 0 or -1, according as X has p-type A or D or B. Let Q be an element of order q of $\mathfrak{G}$. Then we have that $X(Q)=1$ or 0 or -1, according as X has q-type A or D or B. There exist just two irreducible characters of p-type C which take the same value at any p-regular element and the sum of whose value at P equals δ_p. If the order of $N_S\Omega$ equals qr, then there exist just two irreducible characters of q-type C which take the same value at any q-regular element and the sum of whose value at Q equals δ_q.*

The significance of Proposition B lies in the fact that it eliminates all but a few possibilities for the decompositions of X_0^0 restricted on $\mathfrak{G}$ and X_{00} restricted on $\mathfrak{G}$ into irreducible characters of $\mathfrak{G}$. Considering this, it seems to be unnecessary to assume that $r=\frac{1}{4}(p-3)$ is a prime number; but there are some critical cases, which seem to be difficult to handle without this assumption. In one such case a theorem of Manning concerning uniprimitive[2] permutation groups is very useful [14].

There are many results about quadruply transitive permutation groups that are now available to us. One such result which is due to Parker [21, Theorem 2] has an immediate and useful consequence:

PROPOSITION D (PARKER). *The order of every permutation group $\mathfrak{G}$ of type M is divisible by $r=\frac{1}{4}(p-3)$ only to the first power.*

Now it is rather easy to prove the following theorem.

THEOREM III. *Every permutation group $\mathfrak{G}$ of type M does not contain an odd permutation.*

In other words, *if a nonsolvable transitive permutation group of degree*

[2] *Uniprimitive* means primitive, but not doubly transitive. This terminology is due to Professor Wielandt.

p contains an odd permutation, then it is equal to S_p. At this point we want to propose the following question: *let l be a prime number greater than three. Let* x *be a nonsolvable transitive permutation group of degree l. If* x *contains an odd permutation, then is* $\mathfrak{X}$ *equal to the symmetric group S_l of degree l?*

Let $\mathfrak{H}$ be the maximal subgroup of $\mathfrak{G}$ consisting of all the permuations each of which fixes the symbol 1 of Ω. Then using a theorem of Bochert [1] concerning the minimum degree[3] of quadruply transitive permutation groups, we can associate with $\mathfrak{H}$ a (definite) subgroup $\mathfrak{A}$ of $\mathfrak{H}$, which can be faithfully represented as a permutation group of type M with degree q (Lemma 13 in §5).

Our proof of the quintuple transitivity of $\mathfrak{G}$ (Theorem IV in §5) requires at first the triple transitivity of $\mathfrak{A}$ (as a permutation group of degree q). Then it heavily relies again on the above mentioned results of Frobenius and Brauer (Propositions A and B), and moreover on the following theorem due to Frame [4, Theorem B]:

PROPOSITION E (FRAME). *Let Λ be the set of symbols $1, \cdots, n$. Let $\mathfrak{X}$ be a transitive permutation group on Λ. Let $\mathfrak{Y}$ be the subgroup of $\mathfrak{X}$ consisting of all the permutations of $\mathfrak{X}$ each of which fixes the symbol 1 of Λ. Let Λ_i $(i=1, \cdots, k)$ be the domains of transitivity of $\mathfrak{Y}$ on Λ. Let l_i denote the length of Λ_i $(i=1, \cdots, k)$. Put $N=n^{k-2}l_1 \cdots l_k$. Let $1_{\mathfrak{Y}}^{*}$ be the character of $\mathfrak{X}$ induced by the principal character $1_{\mathfrak{Y}}$ of $\mathfrak{Y}$. Let*

$$1_{\mathfrak{Y}}^{*} = \sum_{i=1}^{l} e_i X_i \qquad (e_i = 1; i = 1, \cdots, l)$$

be the decomposition of $1_{\mathfrak{Y}}^{*}$ into irreducible characters of $\mathfrak{X}$. Let x_i denote the degree of X_i $(i=1, \cdots, l)$. Put

$$D = x_1^{e_1^2} \cdots x_l^{e_l^2}.$$

Then the number N/D is a rational integer. Furthermore, if $X_1, \cdots, X_l$ are rational characters, then it is a perfect square.

Theorem V is now obtained as a corollary of Theorem IV.

The sextuple transitivity of $\mathfrak{G}$ follows easily from the quintuple transitivity of $\mathfrak{G}$ (Theorem VI in §6).

Now let us assume that not only p, $q=\frac{1}{2}(p-1)$, $r=\frac{1}{4}(p-3)$, but also $s=\frac{1}{8}(p-7)$ is a prime number. Then we can apply to $\mathfrak{A}$ our above reviewed theorems. This, together again with results of Frobenius, Brauer and Frame (Propositions A, B and E), leads us to the septuple and octuple transitivity of $\mathfrak{G}$ (Theorems VII and IX).

[3] The word *Class* is used in older literatures. This terminology is also due to Professor Wielandt.

Theorem VIII is now obtained as a corollary of Theorem VII.

In any event we show that $\mathfrak{G}$ has a high degree of multiple transitivity. In this circumstance we should like to mention interesting results of Holyoke [9], Miller [20] and Witt [31] concerning multiply transitive permutation groups, though we could not use them in this paper. The theorem of Miller led Parker to his above mentioned theorem (Proposition D). Furthermore, it may be possible to make full use of some interesting results of Bochert [1], Luther [13], Manning [15], Weiss [27] and Wielandt [28] concerning the minimum degree of multiply transitive permutation groups. Here we can refer to one theorem of Manning [15; **III**, Theorem V], which implies the following proposition.

PROPOSITION F (MANNING). *Every permutation group $\mathfrak{G}$ of type M is at most elevenfold transitive.*[4]

Finally it should be mentioned that quite a number of very interesting papers are dedicated to G_7, G_{11}, M_{11} and M_{23}. For instance we want to mention Miller [19], Jordan [12], Witt [31] and M. Hall [8].

2. **Triple transitivity.** We use the same notation as in §1. We want to emphasize here that we have Assumptions a and b.

LEMMA 1. *Let $\mathfrak{G}$ be a permutation group of type M. Then the order of $\mathfrak{Q}$ is equal to q. Let Q be an element of $\mathfrak{Q}$ with order q. Then the cycle structure of Q consists of two q-cycles.*

PROOF. By a theorem of Burnside [II, p. 234] $\mathfrak{G}$ is doubly transitive. Therefore the order of $\mathfrak{G}$ is divisible by q. If the order of $\mathfrak{Q}$ is greater than q, $\mathfrak{G}$ contains a q-cycle. Then by a theorem of Jordan [V, 13.9] $\mathfrak{G}$ must contain A_p. This contradiction shows that the order of $\mathfrak{Q}$ is equal to q.

THEOREM I. *$\mathfrak{G}$ is triply transitive.*

PROOF. We can assume that $\mathfrak{G}$ is a permutation group of type M. Since $\mathfrak{G}$ is not equal to G_7 by Assumption b, by a theorem of Wielandt [11, Theorem 1] $\mathfrak{G}$ is doubly primitive. Hence $\mathfrak{H}$ is a primitive permutation group of degree $2q$. Let us assume that $\mathfrak{G}$ is not triply transitive. Then $\mathfrak{H}$ is not doubly transitive. Therefore, by a theorem of Wielandt [29], there exists an odd integer m such that $2q=m^2+1$. Hence we have that $4r=m^2-1=(m+1)(m-1)$, which by Assump-

[4] We shall show in the following that $\mathfrak{G}$ contains an element T of order 3 such that $\alpha(T)=r$ (see Lemma 11). This, together with the mentioned theorem of Manning, proves Proposition F.

tion a implies that $m+1=2r$ and $m-1=2$. Thus we have obtained that $r=2$, $q=5$ and $p=11$, contradicting Assumption b.

3. **Quadruple transitivity.** Our main purpose of this section is to prove the following theorem.

THEOREM II. $\mathfrak{G}$ *is quadruply transitive.*

In order to prove this theorem, we can evidently assume that $\mathfrak{G}$ is a permutation group of type M and that $\mathfrak{G}$ does not contain any odd permutation. Then we can show, first of all, the following two lemmas.

LEMMA 2. (i) *The order of* $Ns\mathfrak{P}$ *equals* pq, (ii) *the order of* $Cs\mathfrak{Q}$ *equals* q *and* (iii) $\mathfrak{G}$ *is simple.*

PROOF. (i) If the order of $Ns\mathfrak{P}$ is even, let us consider an involution I in $Ns\mathfrak{P}$. It is easy to see that the cycle structure of I consists of q transpositions. Thus I is an odd permutation, in contradiction to the assumption. If the order of $Ns\mathfrak{P}$ equals p, then by the splitting theorem of Burnside $\mathfrak{G}$ contains a normal subgroup of index p, which necessarily coincides with $\mathfrak{H}$. Then the transitivity of $\mathfrak{G}$ implies that $\mathfrak{H}=1$ and $\mathfrak{G}$ becomes solvable, in contradiction to the assumption.

(ii) If the order of $Cs\mathfrak{Q}$ is greater than q, then by Lemma 1 $Cs\mathfrak{Q}$ contains an element V, whose cycle structure consists of a single $2q$-cycle. Thus V is odd, in contradiction to the assumption.

(iii) If $\mathfrak{G}$ is not simple, let $\mathfrak{N}$ be a proper normal subgroup ($\neq 1$) of $\mathfrak{G}$. Since $\mathfrak{G}$ is doubly transitive, $\mathfrak{N}$ is transitive and therefore $\mathfrak{N}$ contains $\mathfrak{P}$. Then using Sylow's theorem we have that $(Ns\mathfrak{P})\mathfrak{N}=\mathfrak{G}$. Therefore, we see that $\mathfrak{G}:\mathfrak{N}=q$ and $\mathfrak{N}\cap Ns\mathfrak{P}=\mathfrak{P}$. But the latter fact implies as before that $\mathfrak{N}$ is solvable. Then $\mathfrak{G}$ becomes solvable, too, in contradiction to the assumption.

LEMMA 3. *The order of* $Ns\mathfrak{Q}$ *equals either* qr *or* $q(q-1)$.

PROOF. By Lemma 2, (ii) we see that the order of $Ns\mathfrak{Q}$ is a divisor of $q(q-1)$. If it is equal to q, then by the splitting theorem of Burnside $\mathfrak{G}$ contains a normal subgroup of index q contradicting the simplicity of $\mathfrak{G}$. If it is equal to $2q$, then by a previous result [11, Theorem 2] $\mathfrak{G}$ is isomorphic to either G_7 or G_{11}, in contradiction to the assumption.

Now we use the following notation: (X, Y) denotes a nonprincipal irreducible character of $\mathfrak{G}$, which has p-type X and q-type Y ($X, Y=A, B, C, D$). Then Proposition B enables us to compute the least possible and the next least possible degree of the nonprincipal irreducible characters of $\mathfrak{G}$ as follows:

Type	Least Possible Degree	Next Least Possible Degree	
(A, A)	$qp+1$		
(A, B)	$(q-2)p+1$	$2(q-1)p+1$	
(A, C)	$(q-r-1)p+1$	$(2q-r-1)p+1$	$\delta_q=1$
	$(r-1)p+1$	$(q+r-1)p+1$	$\delta_q=-1$
(A, D)	$(q-1)p+1$		
(B, A)	$2p-1$	$(q+2)p-1$	
(B, B)	$qp-1$		
(B, C)	$(q-r+1)p-1$	$(2q-r+1)p-1$	$\delta_q=1$
	$(r+1)p-1$	$(q+r+1)p-1$	$\delta_q=-1$
(B, D)	$p-1$	$(q+1)p-1$	
(C, A)	$\frac{1}{2}(p+1)$	$\frac{1}{2}((2q+1)p+1)$	$\delta_p=1$
	$\frac{1}{2}(3p-1)$	$\frac{1}{2}((2q+3)p-1)$	$\delta_p=-1$
(C, B)	$\frac{1}{2}((2q-3)p+1)$		$\delta_p=1$
	$\frac{1}{2}((2q-1)p-1)$		$\delta_p=-1$
(C, D)	$\frac{1}{2}((2q-1)p+1)$		$\delta_p=1$
	$\frac{1}{2}(p-1)$	$\frac{1}{2}((2q+1)p-1)$	$\delta_p=-1$
(D, A)	p	$(q+1)p$	
(D, B)	$(q-1)p$		
(D, C)	$(q-r)p$	$(2q-r)p$	$\delta_q=1$
	rp	$(q+r)p$	$\delta_q=-1$
(D, D)	qp		

We need the following results of Brauer and Tuan [3; 26]:

PROPOSITION C (BRAUER, TUAN). *If $\mathfrak{G}$ possesses an irreducible character of degree $\frac{1}{2}(p-1)$ or $\frac{1}{2}(p+1)$, then it is isomorphic to $LF_2(p)$.*

On the other hand, we have the following lemma.

LEMMA 4. *$\mathfrak{G}$ cannot be isomorphic to $LF_2(p)$.*

PROOF. Since $\mathfrak{G}$ contains a subgroup of index p, we have, by the first mentioned theorem of Galois [III, §262], that $p=5$ or 7 or 11. This contradicts Assumption b.

Lemma 4 removes the possibility of an appearance of an irreducible character of $\mathfrak{G}$ of type (C, A) with $\delta_p=1$ or of type (C, D) with $\delta_p=-1$ as an irreducible part of X_0^0 restricted on $\mathfrak{G}$ or X_{00} restricted on $\mathfrak{G}$.

Using this fact we can show the following two lemmas.

LEMMA 5. *There are only four possible cases of the decomposition of X_0^0 restricted on $\mathfrak{G}$ into the irreducible characters of $\mathfrak{G}$:*

(i) *X_0^0 restricted on $\mathfrak{G}$ is irreducible.*

(ii) *$X_0^0=(A, B)+(D, A)$, where the degrees of (A, B) and (D, A) are equal to $(q-2)p+1$ and p, respectively.*

(iii) $X_0^0=(A, C)_1+(A, C)_2+(B, A)$, *where the degrees of* $(A, C)_i$ $(i=1, 2)$ *and* (B, A) *are equal to* $(r-1)p+1$ *with* $\delta_q=-1$ *and* $2p-1$, *respectively.*

(iv) $X_0^0=(A, C)_1+(A, C)_2+(B, D)+(D, A)$, *where the degrees of* $(A, C)_i$ $(i=1, 2)$. (B, D) *and* (D, A) *are equal to* $(r-1)p+1$ *with* $\delta_q=-1$, $p-1$ *and* p, *respectively.*

PROOF. Since $X_0^0(P)=1$, by Proposition B an irreducible character of $\mathfrak{G}$ of p-type A or p-type C with $\delta_p=1$ must appear as an irreducible part of X_0^0 restricted on $\mathfrak{G}$. Since $\mathfrak{G}$ is doubly transitive, by a theorem of Frobenius [6] the principal character of $\mathfrak{G}$ does not appear here. Let us assume that X_0^0 restricted on $\mathfrak{G}$ is reducible. Then we see from the table on page 172, that either a character (A, B) with degree $(q-2)p+1$ or a pair of characters $(A, C)_i$ $(i=1, 2)$ with degree $(r-1)p+1$ and $\delta_q=-1$ must appear. Again by inspecting the table on page 172 we see the validity of Lemma 5.

LEMMA 6. *There are only five possible cases of the decomposition of* X_{00} *restricted on* $\mathfrak{G}$ *into the irreducible characters of* $\mathfrak{G}$:

(i) X_{00} *restricted on* $\mathfrak{G}$ *is irreducible.*

(ii) $X_{00}=(A, B)+(B, D)$, *where the degree of* (A, B) *and* (B, D) *are equal to* $(q-2)p+1$ *and* $p-1$, *respectively.*

(iii) $X_{00}=(A, C)_1+(A, C)_2+(B, D)_1+(B, D)_2$, *where the degrees of* $(A, C)_i$ $(i=1, 2)$ *and* $(B, D)_i$ $(i=1, 2)$ *are equal to* $(r-1)p+1$ *with* $\delta_q=-1$ *and* $p-1$, *respectively.*

(iv) $X_{00}=(A, C)_1+(A, C)_2+2(B, D)$, *where the degrees of* $(A, C)_i$ $(i=1, 2)$ *and* (B, D) *are equal to* $(r-1)p+1$ *with* $\delta_q=-1$ *and* $p-1$, *respectively.*

(v) $X_{00}=(D, C)_1+(D, C)_2$, *where the degree of* $(D, C)_i$ $(i=1, 2)$ *is equal to* rp *with* $\delta_q=-1$.

PROOF. Since $X_{00}(Q)=-1$, by Proposition B an irreducible character of q-type B or q-type C with $\delta_q=-1$ must appear as an irreducible part of X_{00} restricted on $\mathfrak{G}$. Let us assume that X_{00} restricted on $\mathfrak{G}$ is reducible. Then we see from the table on page 172 that either a character (A, B) with degree $(q-2)p+1$ or a pair of characters $(A, C)_i$ $(i=1, 2)$ with degree $(r-1)p+1$ and $\delta_q=-1$ or a pair of characters $(D, C)_i$ $(i=1, 2)$ with degree rp and $\delta_q=-1$ must appear. Again by inspecting the table on page 172 we see the validity of Lemma 6.

LEMMA 7. *Case* (iv) *in Lemma* 5 *and Cases* (ii), (iii) *and* (iv) *in Lemma* 6 *cannot occur.*

PROOF. Let us suppose that one of these cases occurs. Let us con-

sider the character (B, D) (or $(B, D)_1$) of degree $p-1$. Let X_0 be the irreducible character of S_p (and, by the double transitivity, of $\mathfrak{G}$) such that its value is given by the formula $X_0(S)=\alpha(S)-1$ for every permutation S of S_p. Since $\mathfrak{G}$ is triply transitive, by a theorem of Frobenius [6] X_0 is orthogonal to both X_0^0 and X_{00}. Hence we have that (B, D) (or $(B, D)_1$) $\neq X_0$. Let $\mathfrak{R}$ be the subgroup of $\mathfrak{G}$ consisting of all the permutations in $\mathfrak{G}$ each of which fixes each of the symbols 1 and 2 of Ω. Let Y_0 be the irreducible character of S_{p-1} (and by Theorem I of $\mathfrak{H}$) such that its value is given by the formula $Y_0(T)=\alpha(T)-2$ for every permutation T of S_{p-1}, where S_{p-1} is the subgroup of S_p consisting of all the permutations each of which fixes the symbol 1 of Ω. Then we have the following three equalities, which are also due to Frobenius [5]:

$$1_{\mathfrak{R}}^{*} = 1_{\mathfrak{G}} + 2X_0 + X_0^0 + X_{00},$$
$$1_{\mathfrak{R}}^{\#} = 1_{\mathfrak{H}} + Y_0,$$
$$1_{\mathfrak{H}}^{*} = 1_{\mathfrak{G}} + X_0;$$

where $1_{\mathfrak{G}}$, $1_{\mathfrak{H}}$ and $1_{\mathfrak{R}}$ are principal characters of $\mathfrak{G}$, $\mathfrak{H}$ and $\mathfrak{R}$ respectively, $1_{\mathfrak{H}}^{*}$ and $1_{\mathfrak{R}}^{*}$ are characters of $\mathfrak{G}$ induced by $1_{\mathfrak{H}}$ and $1_{\mathfrak{R}}$ respectively, and $1_{\mathfrak{R}}^{\#}$ is the character of $\mathfrak{H}$ induced by $1_{\mathfrak{R}}$. Therefore we have the following equality:

$$Y_0^{*} = X_0 + X_0^0 + X_{00},$$

where Y_0^{*} is the character of $\mathfrak{G}$ induced by Y_0. Then by the reciprocity theorem of Frobenius (B, D) (or $(B, D)_1$) restricted on $\mathfrak{H}$ contains Y_0 as an irreducible part. Therefore we have that

$$(B, D) \text{ (or } (B, D)_1) = Y_0 + L,$$

where L is a nonprincipal (because of (B, D) (or $(B, D)_1$) $\neq X_0$) linear character of $\mathfrak{H}$. Then again by the reciprocity theorem of Frobenius we have that

$$L^{*} = (B, D) \text{ (or } (B, D)_1) + M,$$

where L^{*} is the character of $\mathfrak{G}$ induced by L and M is a nonprincipal linear character of $\mathfrak{G}$, contradicting the simplicity of $\mathfrak{G}$.

LEMMA 8. *Case* (iii) *in Lemma* 5 *cannot occur.*

PROOF. Let us assume that this case occurs. Then Case (v) in Lemma 6 cannot occur, because $\mathfrak{G}$ possesses only two irreducible characters of q-type C (Proposition B). Therefore in this case X_{00} re-

stricted on $\mathfrak{G}$ must be irreducible. Hence the norm of $1_{\mathfrak{R}}^{*}$ equals nine. Now let us consider $\mathfrak{G}$ as a permutation group on Ω_2, where Ω_2 denotes the set of vectors (x, y) having components in Ω and $x \neq y$. Then it is known [V, 28.4, 29.2] that the number of domains of transitivity of $\mathfrak{R}$ from Ω_2 equals the norm of $1_{\mathfrak{R}}^{*}$ and therefore it is nine. Put $\Gamma = \Omega - \{1, 2\}$. Now the vectors (1, 2) and (2, 1) themselves constitute domains of transitivity of $\mathfrak{R}$, and furthermore the vectors of (i, Γ) and (Γ, i) $(i = 1, 2)$, each constitutes domains of transitivity of $\mathfrak{R}$. Therefore we see that the vectors of Γ_2 are divided into three domains of transitivity of $\mathfrak{R}$, where Γ_2 is defined similarly as Ω_2. Since $\mathfrak{R}$ is transitive on Γ, every domain of transitivity of $\mathfrak{R}$ on Γ_2 contains a vector of the form $(3, \Gamma - \{3\})$. Hence we see that the symbols of $\Gamma - \{3\}$ are divided into three domains of transitivity of $\mathfrak{L}$, where $\mathfrak{L}$ denotes the subgroup of $\mathfrak{G}$ consisting of all the permutations in $\mathfrak{G}$ each of which fixes each of the symbols 1, 2 and 3 of Ω.

Let $\mathfrak{R}$ be a Sylow r-subgroup in $Ns\mathfrak{Q}$. By the triple transitivity of $\mathfrak{G}$ we can assume that $\mathfrak{R}$ is contained in $\mathfrak{L}$. Moreover the cycle structure of any element $(\neq 1)$ of $\mathfrak{R}$ consists of four r-cycles (cf. Lemma 1). Therefore $\Gamma - \{3\}$ is divided into four domains Φ_i $(i = 1, 2, 3, 4)$ of transitivity of $\mathfrak{R}$. Let $\mathfrak{L}(r)$ be a Sylow r-subgroup of $\mathfrak{L}$ containing $\mathfrak{R}$. Then by a theorem of Witt [V, 9.4] we see that $Ns\mathfrak{L}(r)/Ns\mathfrak{L}(r) \cap \mathfrak{L}$ is isomorphic to S_3 on $\{1, 2, 3\}$, where $Ns\mathfrak{L}(r)$ is the normalizer of $\mathfrak{L}(r)$ in $\mathfrak{G}$. Let T be a 3-element in $Ns\mathfrak{L}(r)$, whose cycle structure has the form $(123) \cdots$. Then T is contained in $Ns\mathfrak{L}$, where $Ns\mathfrak{L}$ denotes the normalizer of $\mathfrak{L}$ in $\mathfrak{G}$. Now we can assume, without loss of generality, that $\Phi_1, \Phi_2, \Phi_3 \cup \Phi_4$ are three domains of transitivity of $\mathfrak{L}$ from $\Gamma - \{3\}$. Then T must fix $\Phi_3 \cup \Phi_4$ and therefore each of Φ_i $(i = 1, 2, 3, 4)$. Let $\mathfrak{R}_i$ denote the maximal subgroup of $\mathfrak{L}(r)$ consisting of those permutations of $\mathfrak{L}(r)$ which fix the symbols in Φ_i $(i = 1, 2, 3, 4)$. Then T normalizes each $\mathfrak{R}_i$ $(i = 1, 2, 3, 4)$. Now $\mathfrak{L}(r)$ is an elementary abelian r-group of order at most r^4. If it is r^4, then $\mathfrak{G}$ contains an r-cycle. Hence by a theorem of Jordan [V, 13.9] $\mathfrak{G}$ coincides with A_p, in contradiction to the assumption. Therefore $\mathfrak{L}(r)$ has order at most r^3. Now T cannot centralize $\mathfrak{L}(r)$. In fact, otherwise, T must be the 3-cycle (123) and $\mathfrak{G}$ coincides with A_p, in contradiction to the assumption. If $\mathfrak{L}(r)$ has order r, then $r-1$ must be divisible by 3, which leads us to the absurdity $q = 2r+1 \equiv 0 \pmod 3$. If T centralizes one of $\mathfrak{R}_i$ $(i = 1, 2, 3, 4)$, say $\mathfrak{R}_1$, then by the complete reducibility theorem of Maschke, $\mathfrak{L}(r)$ is decomposed into the direct product of $\mathfrak{R}_1$ and a T-invariant subgroup $\mathfrak{R}_1^{*}$ of order r. T cannot centralize $\mathfrak{R}_1^{*}$, which leads us to the same contradiction as before. So we can assume that T does not centralize any of $\mathfrak{R}_i$ $(i = 1, 2, 3, 4)$.

Then it is easy to find a subgroup of $\mathfrak{L}(r)$ of order r, which is normalized, but is not centralized by T. So we have the same contradiction as before. This proves Lemma 8.

LEMMA 9. *Case* (ii) *in Lemma* 5 *cannot occur.*

PROOF. Let us assume that this case occurs. Then let us consider the character (D, A) of degree p. As in the proof of Lemma 7 we see that (D, A) restricted on $\mathfrak{H}$ is decomposed into one of the following forms:

$$(D, A) = Y_0 + 2L,$$
$$(D, A) = Y_0 + L_1 + L_2,$$
$$(D, A) = Y_0 + T,$$

where L, L_1 and L_2 are nonprincipal linear characters and T is an irreducible character of degree two of $\mathfrak{H}$. The first case cannot occur, because then we have that $L^*=2(D, A)+\cdots$ by the reciprocity theorem of Frobenius and it is absurd since the degree of L^* equals p. Let us assume that the second case occurs. Since (D, A) is a rational character, L_1 and L_2 must be algebraically conjugate with each other. Let us assume that the field of L_1 (and of L_2) is the field of mth roots of unity. Then since the degree of this field is $\phi(m)$ and since we have that $\phi(m)=2$, we obtain that $m=3$ or 4. Thus the index of the commutator subgroup $\mathfrak{H}'$ of $\mathfrak{H}$ in $\mathfrak{H}$ is divisible by either 3 or 4. Since $\mathfrak{H}$ is doubly transitive (Theorem I), $\mathfrak{H}'$ is transitive and contains $\mathfrak{Q}$. Using Sylow's theorem we have that $(Ns\mathfrak{Q})\mathfrak{H}'=\mathfrak{H}$, which implies that the order of $Ns\mathfrak{Q}$ is divisible by either 3 or 4. Since the order of $Ns\mathfrak{Q}$ is equal to either $q(q-1)$ or qr by Lemma 3, we obtain that $q=3$, $p=7$ or $q=5$, $p=11$, in contradiction to Assumption b. Hence we can assume that the last case occurs. Let $\mathfrak{K}_T$ be the kernel of T. Since (D, A) and therefore T are rational characters, the order of $\mathfrak{H}/\mathfrak{K}_T$ cannot be divisible by a prime number greater than 3. In fact, otherwise, let $H\mathfrak{K}_T$ be an element of $\mathfrak{H}/\mathfrak{K}_T$ of prime order $l>3$. Let ϵ be a primitive lth root of unity, which appears as a characteristic root of $T(H)$. Then we have that $T(H)=\epsilon+\epsilon^{-1}$, since $T(H)$ is rational. This implies that ϵ has degree two over the field of rational numbers. But this is a contradiction, because it is well known that the degree of ϵ over the field of rational numbers equals $l-1>2$. Thus, in particular, $\mathfrak{K}_T$ contains $\mathfrak{Q}$. Using Sylow's theorem we have that $(Ns\mathfrak{Q})\mathfrak{K}_T=\mathfrak{H}$, which implies that the order of $Ns\mathfrak{Q}$ is divisible by either 6 or 8 or 27, because $\mathfrak{H}/\mathfrak{K}_T$ must be nonabelian. Since the order of $Ns\mathfrak{Q}$ is equal to either $q(q-1)$ or qr by Lemma 3, this is a contradiction.

Thus we have shown that X_0^0 restricted on $\mathfrak{G}$ is irreducible.

LEMMA 10. *Case* (v) *in Lemma* 6 *cannot occur.*

PROOF. Let us assume that this case occurs. Then the norm of $1_{\mathfrak{R}}^*$ equals eight. Let us consider $\mathfrak{G}$ as a permutation group on Ω_2. Then as in Lemma 8 the number of domains of transitivity of $\mathfrak{R}$ on Ω_2 is eight. Put $\Gamma=\Omega-\{1, 2\}$. Then we see as before that the vectors of Γ_2 are divided into two domains of transitivity of $\mathfrak{R}$ and that the symbols of $\Gamma-\{3\}$ are divided into two domains of transitivity of $\mathfrak{L}$. Now we use the notation $\mathfrak{N}$, Φ_i $(i=1, 2, 3, 4)$, $\mathfrak{L}(r)$, $\mathfrak{N}_i$ $(i=1, 2, 3, 4)$ and T just as in the proof of Lemma 8. If the two domains of transitivity of $\mathfrak{L}$ from $\Gamma-\{3\}$ have the form such as $\Phi_1\cup\Phi_2$ and $\Phi_3\cup\Phi_4$, then T must fix each of Φ_i $(i=1, 2, 3, 4)$ and hence normalize each of $\mathfrak{N}_i$ $(i=1, 2, 3, 4)$, which leads us to a contradiction as in the proof of Lemma 8. Therefore, we can assume that the two domains of transitivity of $\mathfrak{L}$ from $\Gamma-\{3\}$ have the form $\Phi_1\cup\Phi_2\cup\Phi_3$ and Φ_4, and that T transfers Φ_1 to Φ_2, Φ_2 to Φ_3 and Φ_3 to Φ_1. Then T fixes Φ_4 and normalizes $\mathfrak{N}_4$. If T does not centralize $\mathfrak{L}(r)/\mathfrak{N}_4$, then we obtain the contradiction $r\equiv 1 \pmod 3$, $q\equiv 0 \pmod 3$ as before. Hence we can assume that T centralizes $\mathfrak{L}(r)/\mathfrak{N}_4$, which implies that $\alpha(T)=r$. Since $X_{00}(T)=\frac{1}{2}r(r-3)$ and $(D, C)_1(T)=(D, C)_2(T)$, we have that $(D, C)_1(T)=\frac{1}{4}r(r-3)$. This implies, in particular, that $r\equiv 3 \pmod 4$. If $\mathfrak{G}$ contains an r-element S whose cycle structure consists of two or three r-cycles, then we have that $\alpha(S)=2r+3$ or $r+3$. Therefore we have that $(D, C)_1(S)=\frac{1}{2}r(2r+3)$ or $\frac{1}{4}r(r+3)$, which is a contradiction, because these numbers are not integers. Thus we have obtained that $\mathfrak{L}(r)=\mathfrak{R}$ has order r and T centralizes $\mathfrak{R}$.

We can represent $Ns\mathfrak{R}$ as an intransitive permutation group $P(Ns\mathfrak{R})$ of degree 7 on $\{1, 2, 3; \Phi_1, \Phi_2, \Phi_3, \Phi_4\}$. Then we know that $P(T)=(123)(\Phi_1\Phi_2\Phi_3)$. Now as long as we observe an r-regular element in $Cs\mathfrak{R}$, where $Cs\mathfrak{R}$ denotes the centralizer of $\mathfrak{R}$ in $\mathfrak{G}$, this permutation representation is faithful, since such an element fixes each of the symbols of Φ_i if it fixes Φ_i as a set $(i=1, 2, 3, 4)$. Moreover we already know that every 3-element in $Ns\mathfrak{R}$ is contained in $Cs\mathfrak{R}$. Then we see that the order of $Ns\mathfrak{R}$ is not divisible by 9. In fact, otherwise, $P(Ns\mathfrak{R})$ contains a 3-cycle (123), which comes from a 3-element of $\mathfrak{G}$. Now such an element is also the 3-cycle (123) in $\mathfrak{G}$, since it is contained in $Cs\mathfrak{R}$. Then $\mathfrak{G}$ coincides with A_p, in contradiction to the assumption.

Now let us consider $Ns\mathfrak{L}$ as a permutation group on Φ_4 and let $\mathfrak{K}_4$ be the kernel of this permutation representation. Then $\mathfrak{L}\cap\mathfrak{K}_4$ is a normal subgroup of $Ns\mathfrak{L}$. Let us consider the subgroup $(\mathfrak{L}\cap\mathfrak{K}_4)\mathfrak{R}$. Let

X be an element ($\neq 1$) of $\mathfrak{L}\cap\mathfrak{K}_4$, which is commutative with some element ($\neq 1$) of $\mathfrak{N}$. Then since X is contained in $Cs\mathfrak{N}$, we can consider $P(X)$. Since $P(X)$ fixes each of the symbols 1, 2, 3 and Φ_4, $P(X)$ must be a transposition, say $P(X)=(\Phi_1\Phi_2)$. Then the (original) cycle structure of X consists of r transpositions and X becomes an odd permutation contradicting the simplicity of $\mathfrak{G}$. Therefore there exists no such element X. Hence by a theorem of Thompson [24], $\mathfrak{L}\cap\mathfrak{K}_4$ is nilpotent. Now let us consider $Ns\mathfrak{L}$ as a permutation group on $\Phi_1\cup\Phi_2\cup\Phi_3$. Since $\mathfrak{L}\cap\mathfrak{K}_4$ fixes 1, 2, 3 and each of the symbols in Φ_4, $\mathfrak{L}\cap\mathfrak{K}_4$ is faithful on $\Phi_1\cup\Phi_2\cup\Phi_3$. Now since $Ns\mathfrak{L}$ is transitive on $\Phi_1\cup\Phi_2\cup\Phi_3$ and since the order of $\mathfrak{L}\cap\mathfrak{K}_4$ is prime to r, the lengths of domains of transitivity of $\mathfrak{L}\cap\mathfrak{K}_4$ on $\Phi_1\cup\Phi_2\cup\Phi_3$ divide 3. Since $\mathfrak{L}\cap\mathfrak{K}_4$ is nilpotent, it is a 3-group.

Now we want to show that $\mathfrak{K}$ is primitive on Γ. Let us assume that $\mathfrak{K}$ is imprimitive on Γ and let $\mathfrak{Y}$ be a maximal subgroup of $\mathfrak{K}$ containing $\mathfrak{L}$. Then $\mathfrak{Y}$ is intransitive on Γ and moves the symbol 3. Hence $\{3, \Phi_1\cup\Phi_2\cup\Phi_3\}$, or $\{3, \Phi_4\}$ is a domain of transitivity of $\mathfrak{Y}$. Thus the index of $\mathfrak{L}$ in $\mathfrak{Y}$ equals either $3r+1$ or $r+1$. Since the index of $\mathfrak{L}$ in $\mathfrak{K}$ is $4r+1$, this implies that either $4r+1/3r+1$ or $4r+1/r+1$ is an integer. This is only possible when $r=2$. This contradicts Assumption b. Thus $\mathfrak{K}$ is primitive on Γ. If $\mathfrak{K}$ is doubly transitive on Γ, then $\mathfrak{G}$ is quadruply transitive and then Case (v) in Lemma 6 cannot occur (Proposition A). Therefore $\mathfrak{K}$ is not doubly transitive on Γ. Now if $\mathfrak{L}$ is doubly transitive on Φ_4, then by a theorem of Manning [14] the length of $\Phi_1\cup\Phi_2\cup\Phi_3$ must divide $r(r-1)$. Then we have that $r\equiv 1 \pmod 3$ and $q\equiv 0 \pmod 3$. This is a contradiction. Therefore $\mathfrak{L}$ is not doubly transitive on Φ_4. Therefore by a theorem of Burnside [II, p. 234] $\mathfrak{L}/\mathfrak{L}\cap\mathfrak{K}_4$ is metacyclic and has an order dividing $r(r-1)$. Since we already know that $r\equiv 3 \pmod 4$ and that $\mathfrak{L}\cap\mathfrak{K}_4$ is a 3-group, 4 is the highest power of 2 dividing the order of $\mathfrak{G}$. This implies, in particular, that there exists an involution J^* in $\mathfrak{L}$, which normalizes, but does not centralize $\mathfrak{N}$. In fact, if J^* centralizes $\mathfrak{N}$, then J^* fixes all the symbols in Φ_4 and is contained in $\mathfrak{L}\cap\mathfrak{K}_4$. But $\mathfrak{L}\cap\mathfrak{K}_4$ is a 3-group and does not contain J^*. Hence we have that $\alpha(J^*)\leqq 7$.

Now an ordinary transfer argument implies that all the involutions in $\mathfrak{G}$ are conjugate with each other, because $\mathfrak{G}$ is simple.

Since by a theorem of Witt [V, 9.4] $Ns\mathfrak{N}/Ns\mathfrak{N}\cap\mathfrak{L}$ is doubly transitive on $\{1, 2, 3\}$, $Ns\mathfrak{N}$ contains a 2-element (=involution, in our case) J such that $J^{-1}TJ=T^{-1}$. Then $P(J)$ has a cycle structure, such as $P(J)=(23)(\Phi_1\Phi_2)$. If J does not centralize $\mathfrak{N}$, then we must have that $\alpha(J)=3$, $\beta(J)=2r$ and $(D, C)_1(J)=r$. Let us assume that

$(\mathfrak{D}, \mathfrak{C})_1(J)$[5] possesses a characteristic roots 1 and b characteristic roots -1. Then we have that $a+b=rp$ and $a-b=r$. This implies that $b=rq$, namely that b is odd. Then the determinant of $(\mathfrak{D}, \mathfrak{C})_1(J)$ is -1, contradicting the simplicity of $\mathfrak{G}$. Thus J must centralize $\mathfrak{R}$ and we have that $\alpha(J)=2r+1$. Since $\alpha(J)=\alpha(J^*)$, we have the contradiction $r \leqq 3$.

Thus we have shown that X_{00} restricted on $\mathfrak{G}$ is irreducible. Therefore by Proposition A $\mathfrak{G}$ is quadruply transitive.

Then using Proposition D and from the proofs of Lemmas 8 and 10 we see the validity of the following lemma.

LEMMA 11. *T always centralizes $\mathfrak{R}$ and $\langle T \rangle$ is a Sylow 3-group of $Ns\mathfrak{R}$.*

4. **Proof of Theorem III.** Let us assume that there exists a permutation group $\mathfrak{G}$ of type M, which contains an odd permutation. Let $\mathfrak{G}^*$ be the subgroup of $\mathfrak{G}$ consisting of all the even permutations in $\mathfrak{G}$. Then the index of $\mathfrak{G}^*$ in $\mathfrak{G}$ equals two. Using Sylow's theorem we have that $(Ns\mathfrak{P})\mathfrak{G}^*=\mathfrak{G}$. Since the order of $Ns\mathfrak{P} \cap \mathfrak{G}^*$ equals qp by Lemma 2, we have that the order of $Ns\mathfrak{P}$ equals $p(p-1)$. Hence $Ns\mathfrak{P}$ contains a cyclic subgroup $\mathfrak{Z}$ of order $2q$. Since $\mathfrak{P}$ is transitive on Ω, we can assume that $\mathfrak{Z}$ is contained in $\mathfrak{H}$. $\mathfrak{Z}$ is a direct product of $\mathfrak{Q}$ and a subgroup $\mathfrak{J}$ of order two. $Ns\mathfrak{Q}$ contains a Sylow r-subgroup $\mathfrak{R}$ of $\mathfrak{G}$ (Proposition D, Lemma 3). Since $\mathfrak{H}$ is doubly transitive on $\Omega-\{1\}$ by Theorem I, we can choose $\mathfrak{P}$, $\mathfrak{Q}$ and $\mathfrak{R}$ so that $\mathfrak{R}$ is contained in $\mathfrak{L}$. Now let Φ_i $(i=1, 2, 3, 4)$ be the domains of transitivity of $\mathfrak{R}$ on $\Gamma-\{3\}$ such that $\{2, \Phi_1, \Phi_2\}$ and $\{3, \Phi_3, \Phi_4\}$ are the two domains of transitivity of $\mathfrak{Q}$ on $\Omega-\{1\}$. Then we can represent $Cs\mathfrak{R}$ as a permutation group $P(Cs\mathfrak{R})$ of degree 7 on $\{1, 2, 3; \Phi_1, \Phi_2, \Phi_3, \Phi_4\}$. The kernel of this permutation representation is $\mathfrak{R}$.

Since $Cs\mathfrak{Q}=\mathfrak{Q}\times\mathfrak{J}$ (Lemma 2, (ii)) and $\mathfrak{R} \subseteq Ns\mathfrak{Q}$, we see that $\mathfrak{J}$ is contained in $Cs\mathfrak{R}$. Let I be the generator of $\mathfrak{J}$. Since I exchanges two domains of transitivity of $\mathfrak{Q}$ on $\Omega-\{1\}$, the cycle structure of $P(I)$ has one of the following two forms:

$$P(I) = (23)(\Phi_1\Phi_3)(\Phi_2\Phi_4)$$

and

$$P(I) = (23)(\Phi_1\Phi_4)(\Phi_2\Phi_3).$$

On the other hand, by a theorem of Witt [**V**, 9.4] $Ns\mathfrak{R}/Ns\mathfrak{R} \cap \mathfrak{L}$ is isomorphic to S_3. Let T be a 3-element in $Ns\mathfrak{R}$, whose cycle structure has the form: $T=(123)\cdots$. By Lemma 11 T is contained in $Cs\mathfrak{R}$.

[5] $(\mathfrak{D}, \mathfrak{C})_1$ denotes a representation of $\mathfrak{G}$ corresponding to the character $(D, C)_1$.

Since T is not a 3-cycle, the cycle structure of $P(T)$ is one of the following eight forms:

$$P(T) = (123)(\Phi_1\Phi_2\Phi_3),$$
$$P(T) = (123)(\Phi_1\Phi_3\Phi_2),$$
$$P(T) = (123)(\Phi_1\Phi_2\Phi_4),$$
$$P(T) = (123)(\Phi_1\Phi_4\Phi_2),$$
$$P(T) = (123)(\Phi_1\Phi_3\Phi_4),$$
$$P(T) = (123)(\Phi_1\Phi_4\Phi_3),$$
$$P(T) = (123)(\Phi_2\Phi_3\Phi_4)$$

and

$$P(T) = (123)(\Phi_2\Phi_4\Phi_3).$$

Now let us consider the commutator of $P(T)$ and $P(I)$, $P(T^{-1}ITI)$, which is also contained in $Cs\mathfrak{N}$. It is easy to see that the part of $P(T^{-1}ITI)$ on $\{1, 2, 3\}$ is a 3-cycle and the part of it on $\{\Phi_1, \Phi_2, \Phi_3, \Phi_4\}$ is an involution. Therefore we see that $(T^{-1}ITI)^{2r}$ is a 3-cycle. Hence $\mathfrak{G}$ contains A_p and coincides with S_p. This contradiction shows the validity of Theorem III.

5. **Quintuple transitivity.** We begin with the following lemma.

LEMMA 12. *Let $\mathfrak{G}$ be a permutation group of type M. Then we have that $\mathfrak{L}\cap Ns\mathfrak{N}\neq\mathfrak{L}\cap Cs\mathfrak{N}$.*

PROOF. Let us assume that $\mathfrak{L}\cap Ns\mathfrak{N}=\mathfrak{L}\cap Cs\mathfrak{N}$. Then by the splitting theorem of Burnside $\mathfrak{L}$ contains a normal subgroup $\mathfrak{S}$ of index r. Let $\mathfrak{M}$ be the subgroup of $\mathfrak{G}$ consisting of all the permutations in $\mathfrak{G}$ each of which fixes each of the symbols 1, 2, 3, 4 of Ω. Then clearly $\mathfrak{S}$ contains $\mathfrak{M}$ as a subgroup of index four. Since $\mathfrak{L}$ is transitive on $\Omega-\{1, 2, 3\}$ (Theorem II) and $\mathfrak{S}$ is normal in $\mathfrak{L}$, $\mathfrak{S}$ is semitransitive on $\Omega-\{1, 2, 3\}$ [V, §11]. The domain of transitivity of $\mathfrak{S}$ containing the symbol 4 of Ω has length four, since the index of $\mathfrak{M}$ in $\mathfrak{S}$ equals four. Hence the length of all the domains of transitivity of $\mathfrak{S}$ on $\Omega-\{1, 2, 3\}$ equals four and the number of domains of transitivity of $\mathfrak{S}$ on $\Omega-\{1, 2, 3\}$ is r. Therefore we see that the order of $\mathfrak{S}$ has the form 2^u3^v. Let $\mathfrak{S}(3)$ be a Sylow 3-group of $\mathfrak{S}$ such that $\mathfrak{N}$ normalizes $\mathfrak{S}(3)$. Then we have that $\mathfrak{S}(3)\neq 1$, since a conjugate element of T is contained in $\mathfrak{L}$, because of the fact that $\alpha(T)=r\geqq 3$ and the triple transitivity of $\mathfrak{G}$. Let Φ be the set of symbols of Ω which are fixed by every element of $\mathfrak{S}(3)$. Then we see that Φ contains at least $r+3$ ele-

ments, because $\mathfrak{S}(3)$ fixes each of three symbols 1, 2 and 3 of Ω and has to fix at least one symbol of Ω in each of r domains of transitivity of $\mathfrak{S}$ of length four. This implies, in particular, that $\alpha(T) \geqq r+3$, which contradicts the fact $\alpha(T)=r$.

Now we prove the following key lemma.

LEMMA 13. *Let $\mathfrak{G}$ be a permutation group of type M. Then $\mathfrak{H}$ contains a subgroup $\mathfrak{A}$, which can be faithfully represented as a transitive permutation group of type M and of degree q.*

PROOF. Let $\{1\}, \{2\}, \{3\}; \Phi_1, \Phi_2, \Phi_3, \Phi_4$ be the domains of transitivity of $\mathfrak{N}$ on Ω such that $\{1\}, \Psi_1 = \{2, \Phi_1, \Phi_2\}$ and $\Psi_2 = \{3, \Phi_3, \Phi_4\}$ are the domains of transitivity of $\mathfrak{Q}$ on Ω. Then we can represent $Ns\mathfrak{N}$ as a permutation group $P(Ns\mathfrak{N})$ of degree 7 on $\{1, 2, 3; \Phi_1, \Phi_2, \Phi_3, \Phi_4\}$. Now we want to show that there exists an r-regular element S of $Ns\mathfrak{N} - Cs\mathfrak{N}$ such that S fixes $\{1\}, \Psi_1, \Psi_2$. If the order of $\mathfrak{L} \cap Ns\mathfrak{N}/\mathfrak{L} \cap Cs\mathfrak{N}$ is divisible by a prime number $l>2$, then let S be an l-element of $\mathfrak{L} \cap Ns\mathfrak{N} - \mathfrak{L} \cap Cs\mathfrak{N}$. Then we have that $l>3$ by Lemma 11. Hence it is clear that $P(S)=1$, because the lengths of domains of transitivity of $P(Ns\mathfrak{N})$ are at most four. Therefore we can assume that $\mathfrak{L} \cap Ns\mathfrak{N}/\mathfrak{L} \cap Cs\mathfrak{N}$ is a cyclic 2-group. Let S^* be a 2-element of $\mathfrak{L} \cap Ns\mathfrak{N}$ such that S^* and $\mathfrak{L} \cap Cs\mathfrak{N}$ generate $\mathfrak{L} \cap Ns\mathfrak{N}$. By Lemma 12 we have that S^* does not belong to $\mathfrak{L} \cap Cs\mathfrak{N}$. If $P(S^*)=1$, then we can put $S=S^*$. Now we can assume as before that $P(T)=(123)(\Phi_1\Phi_2\Phi_3)$. Then if the cycle structure of $P(S^*)$ consists of one or two transpositions, then it is easy to see that a transform of S^* by some element of $\langle T \rangle$ fixes $\{1\}, \Psi_1$ and Ψ_2 and we can choose such an element as S. Hence we can assume that the cycle structure of $P(S^*)$ consists of one 4-cycle. If S^{*2} is not contained in $Cs\mathfrak{N}$, then we can consider S^{*2} instead of S^* from the beginning and we will obtain an element S. Hence we can assume that S^{*2} is contained in $Cs\mathfrak{N}$ and different from the identity. Then $\mathfrak{L} \cap Cs\mathfrak{N}$ contains an involution S^{*2}. If $\mathfrak{L} \cap Cs\mathfrak{N}$ contains an involution I such that the cycle structure of $P(I)$ consists of one transposition, then by a theorem of Bochert [1] $\mathfrak{G}$ contains A_p, because of its quadruple transitivity (Theorem II). This is a contradiction. Therefore, $\mathfrak{L} \cap Cs\mathfrak{N}$ does not contain such an involution. Now it is easy to show that $\mathfrak{L} \cap Cs\mathfrak{N}$ is a direct product of $\mathfrak{N}$ and an elementary abelian subgroup $\mathfrak{V}$ of order four, because $P(S^{*2})$ and $P(T)$ are not commutative with each other. Let $\mathfrak{W}$ be a Sylow 2-subgroup of $\mathfrak{L} \cap Ns\mathfrak{N}$ such that T normalizes $\mathfrak{W}$. There exists such a subgroup $\mathfrak{W}$, because $\mathfrak{L} \cap Ns\mathfrak{N}$ is normal in $Ns\mathfrak{N}$. Then $\mathfrak{W}$ has order eight and is isomorphic to either a dihedral group or an abelian group of type (4, 2). Hence T must commute with an element ($\neq 1$) of $\mathfrak{V}$. But

since every element ($\neq 1$) of $\mathfrak{V}$ is not commutative with T, this is a contradiction.

Now let $\mathfrak{A}$ be the subgroup of $\mathfrak{G}$ consisting of all the permutations each of which fixes $\{1\}$, Ψ_1 and Ψ_2. Then $\mathfrak{A}$ is contained in $\mathfrak{H}$ and contains $\mathfrak{Q}$, $\mathfrak{R}$ and $\mathfrak{S}$. Let us represent $\mathfrak{A}$ as a permutation group on Ψ_1. If this permutation representation of $\mathfrak{A}$ is not faithful, let $A(\neq 1)$ be an element of prime order contained in the kernel. Then we have that $\alpha(A) \geqq q+2$, because A fixes at least one symbol on Ψ_2 since the length of Ψ_2 equals q. Since $\mathfrak{G}$ is quadruply transitive by Theorem II, we have by a theorem of Bochert [1] that $p-\alpha(A) \geqq \frac{1}{2}p-1$, which implies that $q+3/2 \geqq \alpha(A)$. This contradiction proves the faithfulness of this permutation representation of $\mathfrak{A}$ on Ψ_1 (and similarly on Ψ_2). If $\mathfrak{A}$ is solvable, then $\mathfrak{A} \cap \mathfrak{K}$ must be cyclic by a theorem of Burnside [**II**, p. 234]. But $\mathfrak{A} \cap \mathfrak{K}$ contains $\mathfrak{R}$ and S, where S, by definition, does not centralize $\mathfrak{R}$. This contradiction shows the nonsolvability of $\mathfrak{A}$. If $\mathfrak{A}$, as a permutation group on Ψ_1, contains A_q, then $\mathfrak{A}$ is, in particular, triply transitive on Ψ_1 and on Ψ_2. Hence by a previous result [**10**, Satz 4] all the subgroups of $\mathfrak{A}$ of index q are conjugate with each other. So the cycle structure of a permutation of $\mathfrak{A}$ on Ψ_1 and Ψ_2 is similar. Therefore $\mathfrak{A}$ contains a permutation whose cycle structure consists of two 3-cycles. Then again by a theorem of Bochert [1] we have that $6 \geqq \frac{1}{2}p-1$, which implies that $p \leqq 13$. This contradicts Assumption b. Thus $\mathfrak{A}$ is a permutation group of type M and of degree q.

Now we want to prove the following theorem, which is the main result of this section.

THEOREM IV. *Let $\mathfrak{G}$ be a permutation group of type M and of degree p. If $\mathfrak{A}$ in Lemma 13 is triply transitive, then $\mathfrak{G}$ is quintuply transitive. If the order of $Ns\mathfrak{Q}$ equals $q(q-1)$, then $\mathfrak{A}$ is always triply transitive.*

PROOF. (I): *The case where the order of $Ns\mathfrak{Q}$ equals $q(q-1)$.* $Ns\mathfrak{Q}$ contains a cyclic subgroup $\mathfrak{Z}$ of order $2r$. $\mathfrak{Z}$ is a direct product of $\mathfrak{R}$ and a subgroup $\mathfrak{J}$ of order two. Let J be an involution in $\mathfrak{J}$. Now we use the same notation as in the proof of Lemma 13. Since J is an even permutation (Theorem III), J does not permute Ψ_1 and Ψ_2 and so fixes each of them. Thus J is contained in $\mathfrak{A}$. Since $\mathfrak{A}$ contains $\mathfrak{K}$, too, we see that the order of $\mathfrak{A} \cap Ns\mathfrak{Q}$ equals $q(q-1)$. Therefore by a theorem of Wielandt [**V**, 27.1] $\mathfrak{A}$ is triply transitive on Ψ_1 (and on Ψ_2).

Furthermore since J fixes 1, Ψ_1 and Ψ_2 and is elementwise commutative with $\mathfrak{R}$, J fixes the symbols 2 and 3 of Ω and is contained in $\mathfrak{L} \cap Cs\mathfrak{R}$. Therefore as before $\mathfrak{L} \cap Cs\mathfrak{R}$ is a direct product of $\mathfrak{R}$ and an elementary abelian subgroup $\mathfrak{V}$ of order four. Then since $\mathfrak{L} \cap Cs\mathfrak{R}$

is semi-regular on $\Omega-\{1, 2, 3\}$ [V, §4] and the order of $\mathfrak{L}\cap Cs\mathfrak{R}$ equals $4r$, $\mathfrak{L}\cap Cs\mathfrak{R}$ is regular and transitive on $\Omega-\{1, 2, 3\}$. Thus we have the factorization: $\mathfrak{L}=\mathfrak{M}(\mathfrak{L}\cap Cs\mathfrak{R})$ and $\mathfrak{M}\cap Cs\mathfrak{R}\cap\mathfrak{L}=1$.

Now we have that $P(T)=(123)(\Phi_1\Phi_2\Phi_3)$ and that T fixes all the symbols in Φ_4. Since $\mathfrak{G}$ is quadruply transitive (Theorem II), we can assume, by at most a renumeration of Φ_i $(i=1, 2, 3, 4)$, that the symbol 4 of Ω lies in Φ_4.

Since $\mathfrak{A}$ is triply transitive on Ψ_1 and on Ψ_2, all the subgroups of $\mathfrak{A}$ of index q are conjugate with each other [10, Satz 4]. $\mathfrak{R}$ is contained in $\mathfrak{A}$ and fixes only the symbols 1, 2 and 3 of Ω. Therefore every element of $\mathfrak{A}$ which fixes the symbol 2 of Ψ_1 fixes the symbol 3 of Ψ_2 and conversely. Similarly the symbol 4 of Ψ_2 corresponds with a symbol, say 5, of Ψ_1. Let $\mathfrak{B}$ be the subgroup of $\mathfrak{A}$ consisting of all the permutations of $\mathfrak{A}$, each of which fixes each of the symbols 1, 2, 3, 4 and 5 of Ω. Since $\mathfrak{A}$ is triply transitive on Ψ_1 and on Ψ_2, $\mathfrak{B}$ is transitive on $\Gamma_1=\Psi_1-\{2, 5\}$ and on $\Gamma_2=\Psi_2-\{3, 4\}$. The length of Γ_i equals $q-2$ $(i=1, 2)$. $\mathfrak{B}$ is contained in $\mathfrak{M}$. Let us assume that $\mathfrak{M}$ is intransitive on $\Omega-\{1, 2, 3, 4\}$. The set $\{5, \Gamma_i\}$ $(i=1$ or 2) cannot be a domain of transitivity of $\mathfrak{M}$, because then $\mathfrak{M}$ contains a subgroup of index $2r=q-1$ contradicting Proposition D. Hence $\mathfrak{M}$ must fix the symbol 5 of Ω. Since $\mathfrak{L}$ is transitive on $\Omega-\{1, 2, 3\}$, $\mathfrak{L}$ contains a permutation which transforms the symbol 4 of Ω to the symbol 5 of Ω. Such a permutation is contained in the normalizer $Ns\mathfrak{M}$ of $\mathfrak{M}$ in $\mathfrak{G}$. Then the index of $\mathfrak{M}$ in $\mathfrak{L}\cap Ns\mathfrak{M}$ equals two. In fact, otherwise, $\mathfrak{M}$ must fix one more symbol of $\Omega-\{1, 2, 3, 4, 5\}$, which implies that $q-2=1$, contradicting Assumption b. Since $\mathfrak{L}=\mathfrak{M}(\mathfrak{L}\cap Cs\mathfrak{R})$ and $\mathfrak{M}\cap\mathfrak{L}\cap Cs\mathfrak{R}=1$, $\mathfrak{L}\cap Ns\mathfrak{M}$ admits the factorization: $\mathfrak{L}\cap Ns\mathfrak{M}=\mathfrak{M}(\mathfrak{L}\cap Ns\mathfrak{M}\cap Cs\mathfrak{R})$ and $\mathfrak{M}\cap\mathfrak{L}\cap Ns\mathfrak{M}\cap Cs\mathfrak{R}=1$, where $\mathfrak{L}\cap Ns\mathfrak{M}\cap Cs\mathfrak{R}$ has order two. Let J' be an involution in $\mathfrak{L}\cap Ns\mathfrak{M}\cap Cs\mathfrak{R}$. Then J' has a cycle structure of the form (45) $\cdots$. Now since T fixes the symbol 4 of Ω by assumption and is not commutative with J', T cannot fix the symbol 5 of Ω. So let us assume that T transfers the symbol 5 of Ω to a symbol, say 6, of Ω. Then since T fixes the symbol 4 of Ω and normalizes $\mathfrak{M}$, $Ns\mathfrak{M}$ and $\mathfrak{L}$, the element $T^{-1}J'T$ is contained in $\mathfrak{L}\cap Ns\mathfrak{M}$. But $T^{-1}J'T$ has a cycle structure of the form (46) $\cdots$. Then $\mathfrak{M}$ must fix the symbol 6 of $\Omega-\{1, 2, 3, 4, 5\}$. This implies that $q-2=1$, contradicting Assumption b. Therefore $\mathfrak{M}$ must be transitive on $\Omega-\{1, 2, 3, 4\}$ in this case.

(II): *The case where the order of* $Ns\mathfrak{Q}$ *equals* qr. In this case $\mathfrak{A}$ is triply transitive on Ψ_1 and on Ψ_2 by assumption. Now we show that $\mathfrak{L}\cap Cs\mathfrak{R}=\mathfrak{R}$. In fact, otherwise, we have, as before, that $\mathfrak{L}\cap Cs\mathfrak{R}=\mathfrak{B}\times\mathfrak{R}$, where $\mathfrak{B}$ is an elementary abelian subgroup of order four.

Then $\mathfrak{A}$, as a permutation group on Ψ_1, contains an odd permutation, which is one of the involutions in $\mathfrak{B}$. This implies that the order of $Ns\mathfrak{Q}$ equals $q(q-1)$. Therefore the situation here is quite similar to Case (I), but it is more difficult. Let us assume that the symbols 2 and 5 of Ψ_1 correspond with the symbols 3 and 4 of Ψ_2. As in Case (I) we see that $\mathfrak{M}$ fixes the symbol 5 of Ω.

Let us assume that $\mathfrak{M}$ admits Γ_1 and Γ_2 as domains of transitivity. Then $\mathfrak{M}$ fixes 1, Ψ_1 and Ψ_2, and is contained in $\mathfrak{A}$. Hence $\mathfrak{M}$ is contained in $\mathfrak{B}$. Since conversely $\mathfrak{B}$ is evidently contained in $\mathfrak{M}$, we have that $\mathfrak{B}=\mathfrak{M}$. Since $\mathfrak{Q}$ and $\mathfrak{R}$ are contained in $\mathfrak{A}$ and $Ns\mathfrak{Q}=\mathfrak{Q}\mathfrak{R}$, $Ns\mathfrak{Q}$ is contained in $\mathfrak{A}$. Therefore using Sylow's theorem we have that $\mathfrak{H}:\mathfrak{A}\equiv 1 \pmod{q}$. On the other hand, we have that

$$\begin{aligned}\mathfrak{H}:\mathfrak{A} &= \mathfrak{H}:\mathfrak{M}/\mathfrak{A}:\mathfrak{B}\\ &= 2q(2q-1)(2q-2)/q(q-1)\\ &= 4(2q-1).\end{aligned}$$

Hence we have that $5\equiv 0 \pmod{q}$, contradicting Assumption b. Therefore $\{5\}$ and $\Gamma_1\cup\Gamma_2$ are the domains of transitivity of $\mathfrak{M}$ on $\Omega-\{1, 2, 3, 4\}$.

$\mathfrak{H}$ is simple, because $Ns\mathfrak{Q}$; $\mathfrak{Q}=r$ and $\mathfrak{H}$ is triply transitive (Theorem II).

Now we are in a similar situation as in the proofs of Lemmas 7 and 8. In the first place, we have the following three equations of Frobenius [5]:

$$\begin{aligned}1_{\mathfrak{L}}^{\mathfrak{H}} &= 1_{\mathfrak{H}} + 2Y_0 + Y_{\underset{0}{0}} + Y_{00},\\ 1_{\mathfrak{L}}^{0} &= 1_{\mathfrak{R}} + Z_0,\\ 1_{\mathfrak{R}}^{\mathfrak{H}} &= 1_{\mathfrak{H}} + Y_0,\end{aligned}$$

where $1_{\mathfrak{L}}$ is the principal character of $\mathfrak{L}$, $1_{\mathfrak{L}}^{\mathfrak{H}}$ is the character of $\mathfrak{H}$ induced by $1_{\mathfrak{L}}$, $1_{\mathfrak{L}}^{0}$ is the character of $\mathfrak{R}$ induced by $1_{\mathfrak{L}}$, $Y_{\underset{0}{0}}$ and Y_{00} are irreducible characters of S_{p-1} such that their values are given by the formulae

$$Y_{\underset{0}{0}}(T) = \tfrac{1}{2}(\alpha(T)-2)(\alpha(T)-3) - \beta(T)$$

and

$$Y_{00}(T) = \tfrac{1}{2}(\alpha(T)-1)(\alpha(T)-4) + \beta(T)$$

for every permutation T of S_{p-1}, respectively, and Z_0 is the irreducible character of S_{p-2} (and of $\mathfrak{R}$ by Theorem II) such that its value is given by the formula $Z_0(U)=\alpha(U)-3$ for every permutation U of S_{p-2}, where S_{p-2} is the subgroup of S_p consisting of all the permutations each of which fixes each of the symbols 1 and 2 of Ω. $Y_{\underset{0}{0}}$ restricted on $\mathfrak{H}$ and Y_{00} restricted on $\mathfrak{H}$ may be reducible. From the

above three equations of Frobenius we obtain the following equation:

$$Z_0^{\sharp} = Y_0 + \underset{0}{Y_0} + Y_{00}.$$

In the next place, let us consider $\mathfrak{H}$ as a permutation group on $(\Omega - \{1\})_2$, where the notation is to be similarly understood as Ω_2. Then it is known [V, 28.4, 29.2] that the number of domains of transitivity of $\mathfrak{L}$ from $(\Omega - \{1\})_2$ equals the norm of $1_{\mathfrak{L}}^{\sharp}$. Put $\Delta = \Omega - \{1, 2, 3\}$ and $\mathrm{E} = \Omega - \{1, 2, 3, 4\}$. Then the vectors (2, 3) and (3, 2) themselves constitute domains of transitivity of length 1 of $\mathfrak{L}$, and furthermore the vectors of (i, Δ) and (Δ, i) $(i = 2, 3)$ each constitute domains of length $2(q-1)$ of $\mathfrak{L}$. Since $\mathfrak{L}$ is transitive on Δ (Theorem II), every domain of transitivity of $\mathfrak{L}$ on Δ_2 contains a vector of the form (4, E). Since $\mathfrak{M}$ is transitive on $\mathrm{E} - \{5\}$, the vectors of Δ_2 are divided into two domains of transitivity of $\mathfrak{L}$. One, which contains the vector (4, 5), has length $2(q-1)$, and the other has length $4(q-1)(q-2)$. Therefore the norm of $1_{\mathfrak{L}}^{\sharp}$ equals eight and $Y_0^0 + Y_{00}$ is decomposed into three irreducible characters of $\mathfrak{H}$.

Now the rest of our proof rests on Proposition E of Frame. First of all we show that Y_{00} restricted on $\mathfrak{H}$ cannot be irreducible and therefore Y_0^0 restricted on $\mathfrak{H}$ must be irreducible. In fact, let us assume that Y_{00} restricted on $\mathfrak{H}$ is irreducible. In our case we have in the notation of Proposition E that

$$\begin{aligned} N &= (2q(2q-1))^6(2(q-1))^4 2(q-1)4(q-1)(q-2) \\ &= 2^{13}q^6(2q-1)^6(q-1)^6(q-2). \end{aligned}$$

On the other hand the degree of Y_{00} equals $q(2q-3)$. But it is clear that $2q-3$ does not divide N. This contradicts Proposition E.

Now let $Y_{00} = Y_1 + Y_2$ be the decomposition of Y_{00} restricted on $\mathfrak{H}$ into irreducible characters of $\mathfrak{H}$. We have here by a theorem of Frobenius [6] that $Y_i \neq Y_0$ $(i = 1, 2)$, because $\mathfrak{H}$ is triply transitive. Since the degree of Y_{00} is odd, the degrees of Y_1 and Y_2 are different, and therefore they are rational characters. Since

$$1_{\mathfrak{L}}^{\sharp} = 1_{\mathfrak{H}} + 2Y_0 + \underset{0}{Y_0} + Y_1 + Y_2$$

is the decomposition of $1_{\mathfrak{L}}^{\sharp}$ into irreducible characters of $\mathfrak{H}$, all the irreducible components of $1_{\mathfrak{L}}^{\sharp}$ are rational. Therefore by Proposition E the number N/D is a perfect square. Now we have that

$$(*) \qquad \begin{aligned} \frac{N}{D} &= \frac{(2q(2q-1))^6(2(q-1))^4 2(q-1)4(q-1)(q-2)}{(2q-1)^4(2q-1)(q-1)y_1y_2} \\ &= 2^{13}q^6(2q-1)(q-1)^5(q-2)/y_1y_2, \end{aligned}$$

where y_i denotes the degree of Y_i $(i = 1, 2)$.

Since the degree of Y_{00} is divisible by q two cases arise concerning the q-types of Y_1 and Y_2: (1) Both Y_1 and Y_2 have q-type D, and (2) one, say Y_1, has q-type A and the other, Y_2, has q-type B.

We know already that $\mathfrak{L}\cap Cs\mathfrak{R}=\mathfrak{R}$, and since $Ns\mathfrak{R}/\mathfrak{L}\cap Ns\mathfrak{R}$ is isomorphic to S_3 on $\{1, 2, 3\}$, $\mathfrak{H}\cap Ns\mathfrak{R}/\mathfrak{L}\cap Ns\mathfrak{R}$ has order two. Therefore we see that the order of $\mathfrak{H}\cap Cs\mathfrak{R}$ is not greater than $2r$. Hence using a theorem of Brauer [3, Theorem 10] we see that the degrees of rational irreducible characters of $\mathfrak{H}$ are congruent to either 1 or 0 or -1 modulo r. And so as in Proposition B we can speak of r-types of the (rational) irreducible characters of $\mathfrak{H}$. Since the degree of Y_{00} is congruent to -1 (mod r), we can assume in Case (1) that one, say Y_1, has r-type D and the other, Y_2, has r-type B. In Case (2) two cases must be distinguished: (i) Y_1 has r-type D and Y_2 has r-type B, and (ii) Y_1 has r-type B and Y_2 has r-type D.

We shall proceed to eliminate case after case.

Case (1). We can put that $y_1=arq$ and $y_2=(br-1)q$ with $a+b=4$, where a and b are positive integers. Hence three subcases are to be distinguished: (1, a) $y_1=3rq$ and $y_2=(r-1)q$, (1, b) $y_1=2rq$ and $y_2=(2r-1)q$, and (1, c) $y_1=rq$ and $y_2=(3r-1)q$.

Subcase (1, a). Since $q\equiv -1$ (mod 3) and $q-1=2r$ $(r>5)$, dividing (*) by q^4r^4, we have that $A=2^{19}(2q-1)(q-2)/3(q-3)$ is a perfect square. Then it is easy to see that the prime power factor decomposition of $q-3$ has the following form: $q-3=2^B5^C$, where B is an odd number, because A is a perfect square. Now if we have that $C=0$, then dividing A by 2^{19-B} we have that $(2q-1)(q-2)=3D^2$, where D is an integer. Since $q\equiv 3$ (mod 4), this implies that $1\equiv 3D^2$ (mod 4). This is a contradiction. Hence we can assume that $C>0$. Since $(2q-1, q-2)=3$, we can put $2q-1=3^E5^FG^2$, where E, F and G are integers and $E>0$ and $F\geqq C$. Hence we have that $5=(2q-1)-2(q-3)=3^E5^FG^2-2^{B+1}5^C$, which implies that $C=1$ and $1=3^E5^{F-1}G^2-2^{B+1}$. Since B is odd, we have a contradiction that $1\equiv -1$ (mod 3).

Subcase (1, b). Dividing (*) by q^4, we have that $2^{13}(2q-1)(q-1)^4$ is a perfect square. This is absurd, because the exponent of 2 is evidently odd.

Subcase (1, c). Dividing (*) by q^4r^4, we have that

$$A = 2^{19}(2q - 1)(q - 2)/(3q - 5)$$

is a perfect square. Then it is easy to see that the prime power factor decomposition of $3q-5$ has the following form: $3q-5=2^B7^C$, where B is odd, because A is a perfect square. This is a contradiction, because it implies that $1\equiv -1$ (mod 3).

Case (2, i). We can put that $y_1=(ar-1)q+1$ and $y_2=brq-1$ with $a+b=4$, where a and b are positive integers. As before three subcases are to be distinguished: (2, i, a) $y_1=(3r-1)q+1$ and $y_2=rq-1$, (2, i, b) $y_1=(2r-1)q+1$ and $y_2=2rq-1$, and (2, i, c) $y_1=(r-1)q+1$ and $y_2=3rq-1$.

Subcase (2, i, a). Dividing (*) by q^6r^4, we have that

$$2^{19}(2q-1)/(3q-2)(q+1)$$

is a perfect square. Since $3q-2$ is odd and bigger than $2q-1$, this is a contradiction.

Subcase (2, i, b). Dividing (*) by q^6, we have that

$$2^{16}(2q-1)(q-2)r^3/(q^2-q-1)$$

is a perfect square. Since the exponent of r equals three (odd), this is a contradiction.

Subcase (2, i, c). Dividing (*) by q^6r^4, we have that

$$A = 2^{19}(2q-1)/(3q^2-3q-2)$$

is a perfect square. Then it is easy to see that the prime power factor decomposition of $3q^2-3q-2$ has the following form: $3q^2-3q-2=2^B11^C$, where B is odd, because A is a perfect square. Furthermore it is easy to see that $q\equiv -1$ or $-2 \pmod 5$, since we have assumed that $r>5$. If $q\equiv -1 \pmod 5$, then we have that $-1\equiv 2^B \pmod 5$. If $q\equiv -1 \pmod 5$, then we have that $1\equiv 2^B \pmod 5$. Both of these congruences give us a contradiction, because B is odd.

Case (2, ii). We can put that $y_1=(ar-2)q+1$ and $y_2=(br+1)q-1$ with $a+b=4$, where a and b are non-negative integers. Now by the reciprocity theorem of Frobenius Y_2 restricted on $\mathfrak{R}$ contains Z_0 as an irreducible component. Since the degree of Z_0 is $2(q-1)$, we have that $b\geqq 1$. Hence as before three subcases are to be distinguished: (2, ii, a) $y_1=(3r-2)q+1$ and $y_2=(r+1)q-1$, (2, ii, b) $y_1=(2r-2)q+1$ and $y_2=(2r+1)q-1$, and (2, ii, c) $y_1=(r-2)q+1$ and $y_2=(3r+1)q-1$.

Subcase (2, ii, a). Dividing (*) by q^6r^4, we have that

$$2^{19}(2q-1)/(q+2)(3q-1)$$

is a perfect square. Then $q+2$, as an odd number, must divide $2q-1$, which implies that $q=3$. This is a contradiction.

Subcase (2, ii, b). Dividing (*) by q^6r^4, we have that

$$2^{17}(2q-1)(q-2)/(q^2-3q+1)(q+1)$$

is a perfect square. Since q^2-3q+1 is odd and $q+1\equiv 0 \pmod 3$, we have that $3(q^2-3q+1)\leqq(2q-1)(q-2)$, which implies that $q^2+1\leqq 4q$. This is a contradiction, because we have assumed that $q>11$.

Subcase (2, ii, c). Since we have assumed that $r>5$, dividing (*) by q^6r^4, we have that $2^{19}(2q-1)(q-2)/(q^2-5q+2)(3q+2)$ is a perfect square. Since $3q+2$ and $q-2$ are relatively prime, $3q+2$ must divide $2q-1$. This is absurd.

Thus the proof of Theorem IV is completed.

PROOF OF THEOREM V. Let $\mathfrak{G}$ be a permutation group of type M and of degree p. Then by a theorem of Wielandt [**29**] the assumption (3) of Theorem V assures the triple transitivity of $\mathfrak{A}$. Therefore by Theorem IV $\mathfrak{G}$ is quintuply transitive. Hence the order of $\mathfrak{G}$ is divisible by $p-4$. Thus $\mathfrak{G}$ contains a $(p-4)$-cycle. Therefore by a classical theorem of Jordan [**V**, 13.9] $\mathfrak{G}$ contains A_p. This contradiction shows the validity of Theorem V.

The following list shows all prime numbers between 4,080 and 250,000 satisfying the conditions of Theorem V (see [**22**] for prime numbers $\leqq$4,079). 5,927; 6,047; 7,607; 7,727; 13,967; 15,647; 20,327; 28,607; 44,687; 51,287; 57,287; 58,967; 77,767; 89,087; 93,287; 148,727; 165,527; 168,527; 174,767; 192,887; 195,047; 210,207 and 222,647.

6. Sextuple transitivity. We want to prove the following theorem.

THEOREM VI. *Let $\mathfrak{G}$ be a permutation group of type M and of degree p. If $\mathfrak{A}$ is triply transitive, then $\mathfrak{G}$ is sextuply transitive.*

PROOF. We use the same notation as in the proof of Theorem IV. Let $\mathfrak{N}$ be the subgroup of $\mathfrak{G}$ consisting of all the permutations in $\mathfrak{G}$ each of which fixes each of the symbols 1, 2, 3, 4 and 5 of Ω. Then by definition $\mathfrak{B}$ is contained in $\mathfrak{N}$. If $\mathfrak{N}$ is intransitive on $\Omega-\{1,2,3,4,5\}$ then $\mathfrak{N}$ fixes Γ_1 and Γ_2 and is contained in $\mathfrak{A}$. Therefore $\mathfrak{N}$ is contained in $\mathfrak{B}$ and we have that $\mathfrak{N}=\mathfrak{B}$. We know also that $Ns\mathfrak{Q}$ is contained in $\mathfrak{A}$. Therefore using Sylow's theorem we see that $\mathfrak{H}:\mathfrak{A}\equiv 1 \pmod q$. On the other hand, we have that

$$\begin{aligned}\mathfrak{H}:\mathfrak{A} &= (\mathfrak{H}:\mathfrak{N})/(\mathfrak{A}:\mathfrak{B})\\ &= 2q(2q-1)(2q-2)(2q-3)/q(q-1)\\ &= 4(2q-1)(2q-3).\end{aligned}$$

Hence we have that $11\equiv 0 \pmod q$ contradicting Assumption b.

7. Septuple transitivity. The purpose of this section is to prove the following theorem.

THEOREM VII. *Let p, $q=\frac{1}{2}(p-1)$, $r=\frac{1}{4}(p-3)$ and $s=\frac{1}{8}(p-7)$ be prime numbers. Let $\mathfrak{G}$ be a permutation group of type M and of degree p. Then $\mathfrak{G}$ is septuply transitive.*

PROOF. We use the same notation as before. Since q, $r=\frac{1}{2}(q-1)$ and $s=\frac{1}{4}(q-3)$ are prime numbers, $\mathfrak{A}$ is quadruply transitive by Theorem II. Therefore $\mathfrak{G}$ is sextuply transitive by Theorem VI. Let the symbol 6 of Ω belong to Ψ_1. Let $\mathfrak{D}$ be the subgroup of $\mathfrak{G}$ consisting of all the permutations of $\mathfrak{G}$ each of which fixes each of the symbols 1, 2, 3, 4, 5 and 6 of Ω. Since $\mathfrak{A}$ is quadruply transitive, by a previous result [10, Satz 4] all the subgroups of $\mathfrak{A}$ of index q are conjugate with each other. So the cycle structure of a permutation of $\mathfrak{A}$ on Ψ_1 and Ψ_2 is similar. Then let us assume that the symbol 6 of Ψ_1 corresponds with a symbol, say 7, of Ψ_2. Let $\mathfrak{C}$ be the subgroup of $\mathfrak{A}$ consisting of all the permutations of $\mathfrak{A}$ each of which fixes each of the symbols 1, 2, 3, 4, 5, 6 and 7 of Ω. Put $\Delta_1=\Psi_1-\{2, 5, 6\}$ and $\Delta_2=\Psi_2-\{3, 4, 7\}$. Then since $\mathfrak{A}$ is quadruply transitive on Ψ_1 and on Ψ_2, $\mathfrak{C}$ is transitive on Δ_1 and on Δ_2. Now $\mathfrak{C}$ is contained in $\mathfrak{D}$.

Hence even if $\mathfrak{G}$ is not septuply transitive, only the following four cases are possible for the decomposition of $\Omega-\{1, 2, 3, 4, 5, 6\}$ into the domains of transitivity of $\mathfrak{D}$: (1) $\mathfrak{D}$ fixes $\{7\}$, Δ_1 and Δ_2, (2) $\mathfrak{D}$ fixes Δ_1 and $\Gamma_2=\{7, \Delta_2\}$, (3) $\mathfrak{D}$ fixes $\{7, \Delta_1\}$ and Δ_2 and (4) $\mathfrak{D}$ fixes $\{7\}$ and $\Delta_1\cup\Delta_2$.

Case (1). In this case $\mathfrak{D}$ coincides evidently with $\mathfrak{C}$. Therefore as before we have that $\mathfrak{H}:\mathfrak{A}\equiv 1 \pmod q$ and

$$\begin{aligned}\mathfrak{H}:\mathfrak{A} &= (\mathfrak{H}:\mathfrak{C})/(\mathfrak{A}:\mathfrak{C})\\ &= 2q(2q-1)(2q-2)(2q-3)(2q-4)/q(q-1)(q-2)\\ &= 8(2q-1)(2q-3).\end{aligned}$$

Hence we have that $23\equiv 0 \pmod q$. This contradicts the theorem of Jordan mentioned in the Introduction.

Case (2). In this case $\mathfrak{D}$ coincides again with $\mathfrak{C}$. But it is impossible, because every permutation of $\mathfrak{A}$, which fixes the symbol 6 of Ψ_1, must fix the symbol 7 of Ψ_2.

Case (3). Let $\mathfrak{D}_7$ be the subgroup of $\mathfrak{D}$ consisting of all the permutations of $\mathfrak{D}$ each of which fixes the symbol 7 of Ω. Then the index of $\mathfrak{D}_7$ in $\mathfrak{D}$ equals $q-2$. Since $\mathfrak{D}_7$ fixes $\{7\}$, Δ_1 and Δ_2, it fixes $\{1\}$, Ψ_1 and Ψ_2. Therefore $\mathfrak{D}_7$ is contained in $\mathfrak{A}$. Then $\mathfrak{D}_7$ coincides with $\mathfrak{C}$. Hence as before we have that $\mathfrak{H}:\mathfrak{A}\equiv 1 \pmod q$ and

$$\begin{aligned}\mathfrak{H}:\mathfrak{A} &= (\mathfrak{H}:\mathfrak{D}_7)/(\mathfrak{A}:\mathfrak{C})\\ &= 2q(2q-1)(2q-2)(2q-3)(2q-4)(q-2)/q(q-1)(q-2)\\ &= 8(2q-1)(2q-3)(q-2).\end{aligned}$$

Hence we have that $49\equiv 0 \pmod q$. This contradicts Assumption b.

Case (4). Let $\mathfrak{S}$ be a Sylow s-subgroup of $\mathfrak{A}$. Then by Proposition D

the order of $\mathfrak{S}$ equals s. Moreover $\mathfrak{S}$ fixes only the symbols 1, 2, 3, 4, 5, 6 and 7 of Ω (Lemma 3). Let Λ_i $(i=1, \cdots, 8)$ be the domains of transitivity of $\mathfrak{S}$ on $\Omega-\{1, 2, 3, 4, 5, 6, 7\}$ such that $\Delta_1=\Lambda_1\cup\Lambda_2\cup\Lambda_3\cup\Lambda_4$ and $\Delta_2=\Lambda_5\cup\Lambda_6\cup\Lambda_7\cup\Lambda_8$. Let $\mathfrak{G}(s)$ by a Sylow s-subgroup of $\mathfrak{G}$ containing $\mathfrak{S}$. Then since we have assumed that q is bigger than 5, $\mathfrak{G}(s)$ is an elementary abelian subgroup of order at most s^8 and admits Λ_i $(i=1, \cdots, 8)$ as the domains of transitivity on $\Omega-\{1, 2, 3, 4, 5, 6, 7\}$. Thus $\mathfrak{G}(s)$ fixes $\{1\}$, Ψ_1 and Ψ_2. Hence $\mathfrak{G}(s)$ is contained in $\mathfrak{A}$. Therefore we have that $\mathfrak{G}(s)=\mathfrak{S}$, namely s divides the order of $\mathfrak{G}$ only to the first power.

Let $Ns\mathfrak{S}$ and $Cs\mathfrak{S}$ denote the normalizer and centralizer of $\mathfrak{S}$ in $\mathfrak{G}$. Then by a theorem of Witt [**V**, 9.4] $Ns\mathfrak{S}/\mathfrak{D}\cap Ns\mathfrak{S}$, as a permutation group on $\{1, 2, 3, 4, 5, 6, 7\}$, is sextuply transitive (Theorem VI), and therefore equals S_7. On the other hand, since the order of $\mathfrak{S}$ equals s, $Ns\mathfrak{S}/Cs\mathfrak{S}$ and $\mathfrak{D}\subseteq Ns\mathfrak{S}/\mathfrak{D}\cap Cs\mathfrak{S}$ are cyclic groups whose orders divide $s-1$. Therefore $Cs\mathfrak{S}/\mathfrak{D}\cap Cs\mathfrak{S}$, as a permutation group on $\{1, 2, 3, 4, 5, 6, 7\}$, contains A_7. Now let $\mathfrak{W}$ be the Sylow s-complement of $Cs\mathfrak{S}$: $Cs\mathfrak{S}=\mathfrak{S}\times\mathfrak{W}$. Then let us represent $\mathfrak{W}$ as a permutation group of degree 8 on $\{\Lambda_i$ $(i=1, \cdots, 8)\}$. This is possible, because $\mathfrak{W}$ is contained in $Ns\mathfrak{S}$. Moreover, this permutation representation of $\mathfrak{W}$ is faithful. In fact, otherwise, let W be an element of $\mathfrak{W}$ which is contained in the kernel of this permutation representation. Clearly W fixes all the symbols of Λ_i, if it fixes Λ_i as a whole $(i=1, \cdots, 8)$. Therefore, W, as a permutation on Ω, moves at most seven symbols. Hence if $W\neq 1$, this implies, by a theorem of Bochert [1] that $7\geqq\frac{1}{2}p-1$ (Theorem II), which contradicts Assumption b. Now since the order of $\mathfrak{W}$, which is isomorphic to $Cs\mathfrak{S}/\mathfrak{S}$, is a multiple of $\frac{1}{2}(7!)$, it is easy to see that $\mathfrak{W}$, as a permutation group on $\{\Lambda_i$ $(i=1, \cdots, 8)\}$, contains a 3-cycle. Therefore the minimum degree of $\mathfrak{G}$ equals at most $3s+6$. But since $\mathfrak{G}$ is sextuply transitive, we have, by a theorem of Manning [**15**, III, Theorem II], that $5(3s+6)>3p=3(8s+7)$, which is obviously a contradiction.

Thus the proof of Theorem VII is completed.

PROOF OF THEOREM VIII. Let $\mathfrak{G}$ be a permutation group of type M and of degree p. Then since by Theorem VII $\mathfrak{G}$ is septuply transitive, the order of $\mathfrak{G}$ is divisible by $p-6$. Hence $\mathfrak{G}$ contains a $(p-6)$-cycle. Therefore by a classical theorem of Jordan [**V**, 13.9], $\mathfrak{G}$ contains A_p. This contradiction shows the validity of Theorem VIII.

The following list shows all prime numbers between 4,080 and 250,000 satisfying the conditions of Theorem VIII (see [**22**] for prime numbers $\leqq$4,079). 9,839; 11,279; 51,599; 84,719; 96,959 and 178,799.

8. Octuple transitivity.

THEOREM IX. *Under the same conditions as in Theorem* VII $\mathfrak{G}$ *is octuply transitive.*

PROOF. We use the same notation as in the proof of Theorem VII. Let $\mathfrak{U}$ be the subgroup of $\mathfrak{G}$ consisting of all the permutations of $\mathfrak{G}$ each of which fixes each of the symbols $1, \cdots, 7$ of Ω. Then $\mathfrak{C}$ is contained in $\mathfrak{U}$. If $\mathfrak{U}$ is intransitive on $\Omega - \{1, \cdots, 7\}$, then $\mathfrak{U}$ fixes each of Δ_i $(i=1, 2)$ and is contained in $\mathfrak{A}$. Hence we have that $\mathfrak{U}=\mathfrak{C}$. Therefore as before we have that $\mathfrak{H}:\mathfrak{A}\equiv 1 \pmod{q}$ and

$$\begin{aligned}\mathfrak{H}:\mathfrak{A} &= (\mathfrak{H}:\mathfrak{U})/(\mathfrak{A}:\mathfrak{C}) \\ &= 2q(2q-1)(2q-2)(2q-3)(2q-4)(2q-5)/q(q-1)(q-2) \\ &= 8(2q-1)(2q-3)(2q-5).\end{aligned}$$

Hence we have that $121\equiv 0 \pmod{q}$, contradicting Assumption b.

REFERENCES

I. W. Burnside, *Theory of groups of finite order*, Cambridge, 1911.

II. R. D. Carmichael, *Introduction to the theory of groups of finite order*, Boston, 1937.

III. L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Leipzig, 1901.

IV. J.-A. de Séguier, *Groupes de substitutions*, Paris, 1912.

V. H. Wielandt, *Permutationsgruppen, Vorlesungsausarbeitungen von J. André*, Tübingen, 1955.

1. A. Bochert, *Ueber die Classe der transitiven Substitutionengruppen.* I, Math. Ann. **40** (1892), 176–193; II, Math. Ann. **49** (1897), 133–144.

2. R. Brauer, *On groups whose order contains a prime number to the first power.* I, Amer. J. Math. **64** (1942), 401–420.

3. ———, *On permutation groups of prime degree and related classes of groups*, Ann. of Math. **44** (1943), 57–79.

4. J. S. Frame, *The double cosets of a finite group*, Bull. Amer. Math. Soc. **47** (1941), 458–467.

5. G. Frobenius, *Über die Charaktere der symmetrischen Gruppe*, S.-B. Preuss. Akad. Wiss. Berlin (1900), 516–534.

6. ———, *Über die Charaktere der mehrfach transitiven Gruppen*, S.-B. Preuss. Akad. Wiss. Berlin (1904), 528–571.

7. K. D. Fryer, *A class of permutation groups of prime degree*, Canad. J. Math. **7** (1955), 24–34.

8. M. Hall, *On a theorem of Jordan*, Pacific J. Math. **4** (1954), 219–226.

9. T. C. Holyoke, *On the structure of multiply transitive permutation groups*, Amer. J. Math. **74** (1952), 787–796.

10. N. Ito, *Über die Gruppen $PSL_n(q)$, die eine Untergruppe von Primzahlindex enthalten*, Acta Sci. Math. (Szeged) **21** (1960), 206–217.

11. ———, *A note on transitive groups of degree p*, Osaka Math. J. **14** (1962), 213–218.

12. C. Jordan, *Recherches sur les substitutions*, J. Math. Pures Appl. (2) **17** (1872), 351–363.

13. C. F. Luther, *Concerning primitive groups of class u.* I, Amer. J. Math. **55** (1933), 77–101; II, Amer. J. Math. **55** (1933), 611–618.

14. W. A. Manning, *A theorem concerning simply transitive primitive groups*, Bull. Amer. Math. Soc. **35** (1929), 330–332.

15. ———, *The degree and class of multiply transitive groups.* I, Trans. Amer. Math. Soc. **18** (1917), 463–479; II, Trans. Amer. Math. Soc. **31** (1929), 643–653; III, Trans. Amer. Math. Soc. **35** (1933), 585–599.

16. É. Mathieu, *Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables*, J. Math. Pures Appl. (2) **6** (1861), 241–323.

17. ———, *Sur la fonction cinq fois transitive de* 24 *quantités*, J. Math. Pures Appl. (2) **18** (1873), 25–46.

18. G. A. Miller, *Transitive groups of degree* $p=2q+1$, p *and* q *being prime numbers*, Quart. J. Math. Oxford Ser. **39** (1908), 210–216.

19. ———, *Sur plusieurs groupes simples*, Bull. Soc. Math. France **28** (1900), 266–267.

20. ———, *Limits of the degree of transitivity of substitution groups*, Bull. Amer. Math. Soc. **22** (1915), 68–71.

21. E. T. Parker, *On quadruply transitive groups*, Pacific J. Math. **9** (1959), 829–836.

22. E. T. Parker and P. J. Nikolai, *A search for analogues of the Mathieu groups*, Math. Comp. **12** (1958), 38–43.

23. J.-A. de Séguier, *Sur les équations de certains groupes*, J. Math. Pures Appl. (5) **8** (1902), 253–308.

24. J. Thompson, *Finite groups with fixed-point-free automorphisms of prime order*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 578–581.

25. T. Tsuzuku, *On multiple transitivity of permutation groups*, Nagoya Math. J. **18** (1961), 93–109.

26. H. F. Tuan, *On groups whose orders contain a prime number to the first power*, Ann. of Math. **45** (1944), 110–140.

27. M. J. Weiss, *The limit of transitivity of a substitution group*, Trans. Amer. Math. Soc. **32** (1930), 262–283.

28. H. Wielandt, *Abschätzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad*, Schr. Math. Sem. und Inst. Angew. Math. Univ. Berlin **2** (1934), 151–174.

29. ———, *Primitive Permutationsgruppen vom Grad* $2p$, Math. Z. **63** (1956), 478–485.

30. ———, *Über den Transitivitätsgrad von Permutationsgruppen*, Math. Z. **74** (1960), 297–298.

31. E. Witt, *Die* 5*-fach transitiven Gruppen von Mathieu*, Abh. Math. Sem. Univ. Hamburg **12** (1938), 256–264.

UNIVERSITY OF ILLINOIS