Nagao, H.
Osaka J. Math.
2 (1965), 327-341

ON MULTIPLY TRANSITIVE GROUPS IV

HIROSI NAGAO

(Received August 20, 1965)

Let G be a 4-fold transitive group on $\Omega=\{1, 2, \cdots, n\}$, $H=G_{1,2,3,4}$ the subgroup of G consisting of all the elements fixing the four letters 1, 2, 3 and 4 and let N be the normalizer of H in G. Let Δ denote the set of all the letters fixed by H. Then N fixes Δ and it induces a permutation group N^{Δ} on Δ. From the Jordan's theorem [5] (cf. [4], Theorem 5. 8. 1) and the Witt's lemma [8], we have one of the following four cases:

CASE I. $N^{\Delta} = S_4$,
CASE II. $N^{\Delta} = S_5$,
CASE III. $N^{\Delta} = A_6$,
CASE IV. $N^{\Delta} = M_{11}$.

Here M_{11} denotes the Mathieu group of degree 11. (For the Mathieu groups we refer to [8].)

The purpose of this paper is to show that, except in CASE I, G must be one of the known groups. Namely we shall prove the following theorem.

Theorem. *If $N^{\Delta}=S_5$, A_6 or M_{11}, then G must be S_5, A_6 or M_{11} respectively.*

We shall state here the Witt's lemma in full because of its importance in the following.

Lemma (Witt). *Let G be a t-fold transitive group on Ω and H the subgroup of G consisting of all the elements fixing t letters. Suppose that a subgroup U of H is conjugate in H to every group V which lies in H and which is conjugate to U in G. Then the normalizer of U in G is t-fold transitive on the set of the letters left fixed by U.*

The typical examples of U satisfying the assumption are H itself and Sylow p-subgroups of H.

In the proof of the theorem, we also make use of the fact ([4], p. 80) that a 4-fold transitive group of degree less than 35 is, except the symmetric and alternating groups, one of the four Mathieu groups.

NOTATION. For a set X let $|X|$ denote the number of the elements of X. For a set S of permutations on Ω the set of the letters left fixed by S will be denoted by $I(S)$. If a subset Δ of Ω is a fixed block of S, i.e. if $\Delta^S=\Delta$, then the restriction of S on Δ will be denoted by S^Δ. For a permutation group G on Ω the subgroup of G consisting of all the elements fixing the letters $i, j, \cdots, k$ will be denoted by $G_{i, j, \cdots, k}$. For a premutation x let $\alpha_i(x)$ denote the number of i-cycles (cycles of length i) of x. So $\alpha_1(x)$ is the number of the letters left fixed by x.

1. CASE III. $N^\Delta=A_6$, $|\Delta|=6$.

Throughout the remainder of this paper it will be assumed that G is a 4-fold transitive group on $\Omega=\{1, 2, \cdots, n\}$, H denotes $G_{1,2,3,4}$, N is the normalizer of H in G and Δ denotes $I(H)$.

In this section, we treat the case in which $N^\Delta=A_6$ and prove the following

Proposition 1. *If $N^\Delta=A_6$ then G must be A_6.*

Proof. Let us first consider the map

$$\varphi_1 : i \rightarrow G_{1,2,3,i}$$

from $\Omega-\{1, 2, 3\}$ into the set of subgroups of G. Let $I(G_{1,2,3,i}) =\{1, 2, 3, i, j, k\}$. Then the inverse image $\varphi_1^{-1}(G_{1,2,3,i})$ consists of three letters i, j and k. Hence we have

$$(1) \qquad n \equiv 0 \pmod 3 .$$

Now let a be an involution of G and let $r=|I(a)|$. Then, by Proposition 1 in [6], we have

$$(2) \qquad n=r^2+2 .$$

Suppose that $r\geq 4$. Then we may assume that a fixes the three letters 1, 2 and 3. Consider the map

$$\varphi_2 : i \rightarrow G_{1,2,3,i}$$

from $I(a)-\{1, 2, 3\}$ into the set of subgroups of G, and let $I(G_{1,2,3,i}) =\{1, 2, 3, i, j, k\}$. Since a normalizes $G_{1,2,3,i}$ and it is an even permutation on $I(G_{1,2,3,i})$, j and k belong to $I(a)$. Hence each inverse image of φ_2 consists of three letters, and we have

$$(3) \qquad r \equiv 0 \pmod 3 .$$

From (2) and (3) we have

$$n \equiv 2 \qquad (\text{mod } 3).$$

which conflicts with (1).

Thus it is shown that $r \leq 3$ and $n = r^2 + 2 \leq 11$. Then, by the remark at the end of the introduction, G must be A_6.

2. CASE IV. $N^{\Delta} = M_{11}$, $\Delta = 11$.

In this section, we shall prove the following

Proposition 2. *If $N^{\Delta} = N_{11}$ then G must be M_{11}.*

We proceed by way of contradiction. From now on it will be assumed that G is a counter-example to the proposition with the least possible degree and all elements belong to G.

By a series of steps we shall show that every element of order 4 has no 2–cycles. Then it will be shown that there is a subgroup of H which satisfies the assumption of the Witt's lemma. From this fact we have $n \leq 11$, which contradicts the assumption for G.

(i) Let x be an involution and $r = |I(x)|$. Then

$$n = r^2 + 2.$$

For the proof, see Proposition 1 in [6].

(ii) If an element x fixes at least four letters, then

$$(\alpha_1(x) - 2)(\alpha_1(x) - 3) \equiv 0 \qquad (\text{mod } 72).$$

As a special case, the degree n satisfies the relation

$$(n-2)(n-3) \equiv 0 \qquad (\text{mod } 72).$$

Proof. We may assume that $\{1, 2\} \subset I(x)$. For a subset $\{i_1, i_2\}$ of $I(x) - \{1, 2\}$, x normalizes $G_{1, 2, i_1, i_2}$. Let $\Delta' = I(G_{1, 2, i_1, i_2}) = \{1, 2, i_1, i_2, \cdots, i_9\}$. Since $x^{\Delta'}$ is an element of M_{11} fixing the four letters $1, 2, i_1, i_2$, it is the unit. Hence $\Delta' \subset I(x)$. Consider the map

$$\varphi : \{i_1, i_2\} \rightarrow G_{1, 2, i_1, i_2}$$

from the family of the subsets of $I(x) - \{1, 2\}$ consisting of two letters into the set of subgroups of G. By the consideration above, each inverse image of φ consists of ${}_9C_2$ subsets.

Hence we have

$$\frac{(\alpha_1(x) - 2)(\alpha_1(x) - 3)}{2} \equiv 0 \qquad (\text{mod } {}_9C_2),$$

which implies our assertion.

(iii) If an element x has a 2-cycle, then

$$\alpha_2(x) = \frac{\alpha_1(x)(\alpha_1(x)-1)}{2} + 1$$

Proof. Let us first assume that $\alpha_2(x) \geq 2$. We may assume that $x = (1, 2)(k, l)\cdots$. Then x normalizes $G_{1,2,k,l}$. Let $\Delta' = I(G_{1,2,k,l})$. Since $(x^{\Delta'})^2$ is an element of M_{11} fixing the four letters $1, 2, k, l$, it is the unit, and hence $x^{\Delta'}$ is an involution of M_{11}. Therefore $\alpha_1(x) \geq 3$. Now, for a subset $\{i_1, i_2\}$ of $I(x)$, let $\Delta'' = I(G_{1,2,i_1,i_2})$. Then, by the same argument as above, we can see that $x^{\Delta''}$ is an involution of M_{11} and hence it is of the following form:

$$x^{\Delta''} = (1, 2)(i_1)(i_2)(i_3)(k_1, l_1)(k_2, l_2)(k_3, l_3)\,.$$

Considering the map

$$\varphi : \{i_1, i_2\} \to \{(k_1, l_1),\ (k_2, l_2),\ (k_3, l_3)\}$$

from the family of the subsets of $I(x)$ consisting of two letters into the family of the sets of three 2-cycles of x different from $(1, 2)$, we have, in the same way as in the proof of Proposition 1 in [6], the following relation:

$$\frac{1}{3}(\alpha_2(x)-1) = \frac{1}{3}\frac{\alpha_1(x)(\alpha_1(x)-1)}{2}\,.$$

This implies our assertion.

Next assume that $\alpha_2(x) = 1$. If $\alpha_1(x) \geq 2$, then, in the same way as above, we can see that $\alpha_2(x) \geq 3$. Hence $\alpha_1(x)$ must be 0 or 1 and in either case our relation holds.

(iv) If x is an element of order 4, then x has no 2-cycles.

Proof. We assume, by way of contradiction, that $\alpha_2(x) > 0$. Then from (iii) we have

$$(1) \qquad \alpha_2(x) = \frac{\alpha_1(x)(\alpha_1(x)-1)}{2} + 1\,.$$

Let $s = \alpha_1(x)$ and $r = \alpha_1(x^2)$. Then from (1)

$$(2) \qquad r = s + 2\alpha_2(x) = s^2 + 2\,.$$

Let us first assume that $s \geq 4$. Then by (ii)

$$(s-2)(s-3) \equiv 0 \qquad (\mathrm{mod}\ 72)$$

and

$$(3) \qquad (r-2)(r-3) \equiv 0 \pmod{72}.$$

Since $s-2$ and $s-3$ are relatively prime, $s-2\equiv 0 \pmod 9$ or $s-3\equiv 0 \pmod 9$. If $s-2\equiv 0 \pmod 9$, then

$$(r-2)(r-3) = s^2(s^2-1) \not\equiv 0 \pmod 9,$$

which contradicts (3). Hence $s\equiv 3 \pmod 9$. In the same way we have $s\equiv 3 \pmod 8$, and hence $s\equiv 3 \pmod{72}$. Therefore from (2) we have

$$(4) \qquad r \equiv 11 \pmod{72}.$$

On the other hand, since $n=r^2+2$ by (i) and $(n-2)(n-3)\equiv 0 \pmod{72}$ by (ii), $r^2(r^2-1)\equiv 0 \pmod{72}$. But, by (4),

$$r^2(r^2-1) \equiv 11^2(11^2-1) \equiv 48 \not\equiv 0 \pmod{72},$$

which is a contradiction.

Next assume that $s=\alpha_1(x)\leq 3$. Then, from (2), r must be one of the following numbers: 2, 3, 6 or 11. If $r=2$ or 3 then $n=r^2+2\leq 11$ and G must be M_{11} which contradicts the assumption for G. If $r=6$ then

$$(r-2)(r-3) = 12 \not\equiv 0 \pmod{72},$$

which conflicts with (ii). If $r=11$, then $n=r^2+2=123$ and

$$(n-2)(n-3) \not\equiv 0 \pmod{72},$$

which conflicts also with (ii).

(v) Let P be a 2-subgroup of G and c an arbitrary central involution of P. If there is an element x of order 4 in P then $I(x)=I(c)$.

Proof. Since x commutes with c, x takes the letters of $I(c)$ into themselves and it takes also the 2-cycles of c into themselves. If x fixes a 2-cycle (i, j) of c, then by (iv) x fixes the two letters i and j. Then xc is of order 4 and has a 2-cycle (i, j), which contradicts (iv). Thus x fixes no 2-cycles of c, and hence $I(x)\subset I(c)$. On the other hand, from (iv), it follows that $I(x^2)=I(x)$ and, by (i), the two involutions x^2 and c fix the same number of letters. Therefore we have $I(x)=I(c)$.

(vi) Let P be a Sylow 2-subgroup of $H=G_{1,2,3,4}$. Then P contains an element of order 4.

Proof. Since $N^{\Delta}=M_{11}$, G contains at least one element x of order 4. If P contains no elements of order 4, then $|I(x)|\leq 3$. Since $|I(x)|$

$=|I(x^2)|$ by (iv) and x^2 is an involution, we have $n\leq 11$. Hence G must be M_{11}, which contradicts the first assumption for G.

(vii) Let P be a Sylow 2-subgroup of H, c a central involution of P and let $I(c)=\{1,2,\cdots,r\}$. Then $U=P_{1,2,\cdots,r}$ satisfies the assumption in the Witt's lemma.

Proof. Let a be an element of order 4 in P. Then from (v) $I(a)=\{1,2,\cdots,r\}$ and $a\in U$. Now assume that $V=x^{-1}Ux\subset H$ for $x\in G$ and let P' be a Sylow 2-subgroup of H containing V. Then there is an element h of H such that $P'=h^{-1}Ph$. Let $U'=h^{-1}Uh$, $a'=h^{-1}ah$ and $I(a')=\{1',2',\cdots,r'\}$. Then, since $I(a')=I(a)^h$, $U'=P'_{1',2',\cdots,r'}$. Since $x^{-1}ax$ is an element of order 4 in P', we have $I(x^{-1}ax)=I(a')$ by (v). Hence V fixes each letter in $I(a')$ and we have $V\subset U'$. Compairing the orders we have $V=U'$.

(viii) Let U be as in (vii) and let $\Gamma=I(U)$. Then $|\Gamma|=11$.

Proof. Let M be the normalizer of U in G. By (vii) and the Witt's lemma, M^Γ is a 4-fold transitive group on Γ. Since $M_{1,2,3,4}\subset H$,

$$I(H)\subset I(M_{1,2,3,4})\cap I(U) = I((M^\Gamma)_{1,2,3,4})$$

and hence $|I((M^\Gamma)_{1,2,3,4})|\geq 11$. On the other hand, as stated in the introduction, $|I((M^\Gamma)_{1,2,3,4})|$ is not greater than 11. Therefore $|I((M^\Gamma)_{1,2,3,4})|=11$, and by the minimal nature of the degree of G, M^Γ must be M_{11}. Hence $|\Gamma|=11$.

Now let c be as in (vii) and let $|I(c)|=r$. Then by (viii) $r\leq 11$. If $r\leq 3$ then $n\leq 11$ and G must be M_{11}, which contradicts the assumption for G. If $r\geq 4$, then by (ii)

$$(r-2)(r-3)\equiv 0 \qquad (\mathrm{mod}\ 72)\,.$$

Hence $r=11$ and $n=123$. But then

$$(n-2)(n-3)\not\equiv 0 \qquad (\mathrm{mod}\ 72)\,,$$

which conflicts with (ii)

3. Case II. $N^\Delta=S_5$, $|\Delta|=5$.

In this section, we shall prove the following

Proposition 3. *If $N^\Delta=S_5$, then G must be S_5.*

We proceed by way of contradiction. From now on it will be assumed that G is a counter-example to the proposition with the least possible degree and all elements belong to G.

The proof in this case is rather involved. As in CASE IV, we shall first show that every element of order 4 has no 2-cycles.

We first remark that G can not be a symmetric group since $N^{\Delta}=S_5$ and G is not S_5.

(i) The degree n is odd.

Proof. Consider the map

$$\varphi : i \to G_{1,2,3,i}$$

from $\Omega-\{1,2,3\}$ into the set of subgroups of G. Let $I(G_{1,2,3,i}) =\{1,2,3,i,i'\}$. Then the inverse image $\varphi^{-1}(G_{1,2,3,i})$ consists of two letters i and i'. Hence $n-3$ is even and n is odd.

(ii) Let a be an involution of G. If $r=\alpha_1(a)\geq 4$ then

$$r \equiv 3 \pmod{6}.$$

Proof. We may assume that $\{1,2,3\}\subset I(a)$. Consider first the map

$$\varphi_1 : i \to G_{1,2,3,i}$$

from $I(a)-\{1,2,3\}$ to the set of subgroups of G. Let $I(G_{1,2,3,i}) =\{1,2,3,i,i'\}$. Then a normalizes $G_{1,2,3,i}$ and hence i' lies in $I(a)$. Therefore each inverse image of φ_1 consists of two letters. Hence $r-3$ is even and r is odd.

For a 2-cycle (k,l) of a, consider next the map

$$\varphi_2 : \{i_1, i_2\} \to G_{k,l,i_1,i_2}$$

from the family of the subsets of $I(a)$ consisting of two letters into the set of subgroups of G. Let $I(G_{k,l,i_1,i_2})=\{k,l,i_1,i_2,i_3\}$. Then, since a normalizes G_{k,l,i_1,i_2}, i_3 lies in $I(a)$ and the inverse image $\varphi_2^{-1}(G_{k,l,i_1,i_2})$ consists of three subsets $\{i_1,i_2\}$, $\{i_1,i_3\}$, $\{i_2,i_3\}$.

Hence we have

$$\frac{r(r-1)}{2} \equiv 0 \pmod{3},$$

$$r(r-1) \equiv 0 \pmod{6}. \tag{1}$$

In the same way, considering the map

$$\varphi_3 : \{i_1, i_2\} \to G_{1,2,i_1,i_2}$$

from the family of the subsets of $I(a)-\{1,2\}$ consisting of two letters into the set of subgroups of G, we have

$$(2) \qquad (r-2)(r-3) \equiv 0 \pmod{6}.$$

From (1) and (2) it follows that $r\equiv 0 \pmod{6}$ or $r\equiv 3 \pmod{6}$. But, since r is odd, we have

$$r \equiv 3 \pmod{6}.$$

(iii) If u is an element of order 3, then u fixes just two letters.

Proof. Assume first that $s=\alpha_1(u)\neq 0$. For a 3-cycle (k, l, m) of u, consider the map

$$\varphi_1 : i \rightarrow G_{k,l,m,i}$$

from $I(u)$ into the set of subgroups of G. Then u normalizes $G_{k,l,m,i}$ and, in the same way as in the proof of (ii), we have

$$(1) \qquad s \equiv 0 \pmod{2}.$$

Let us assume now that $s\geq 3$. Then, by (1), s is not less than 4. We may assume that $\{1, 2, 3\}\subset I(u)$. Consider the map

$$\varphi_2 : i \rightarrow G_{1,2,3,i}$$

from $I(u)-\{1, 2, 3\}$ into the set of subgroups of G. Then, in the same way as above, we have

$$s-3 \equiv 0 \pmod{2},$$

which conflicts with (1). Thus it is shown that $s\leq 2$. By (1) s is not 1. Hence $s=0$ or 2 and $n\equiv 0 \pmod{3}$ or $n\equiv 2 \pmod{3}$ according as $s=0$ or $s=2$.

Since $N^{\Delta}=S_5$ there is an element x of the following form:

$$x = (1)(2)(3, 4, 5)\cdots.$$

Let the order of x be $3^k m$, where m is prime to 3. Then $k\geq 1$ and $v=x^{3^{k-1}m}$ is an element of order 3 fixing two letters 1 and 2. Hence $n\equiv 2 \pmod{3}$ and s must be equal to 2.

(iv) Let u be an element of order 3 fixing the two letters 1 and 2. If an involution a commutes with u then a has the 2-cycle $(1, 2)$. The order of $N_G(u)\cap G_{1,2}$ is odd.

Proof. If a does not have the 2-cycle $(1, 2)$, then a fixes 1 and 2. Let the 3-cycles of u fixed by a be

$$(i_1, j_1, k_1), \cdots, (i_t, j_t, k_t).$$

Then $I(a)=\{1, 2, i_1, j_1, \cdots, k_t\}$ and hence $r=\alpha_1(a)=3t+2$. Since n is odd, r is odd and hence t must be odd. Let $t=2t'+1$. Then

$$r = 6t'+5 \equiv 5 \pmod 6,$$

which contradicts (ii). Therefore a is of the form $a=(1, 2)\cdots$, and this shows also that $N_G(u) \cap G_{1,2}$ is of odd order.

(v) Let x be an element which has a 3-cycle. Then the order of x is $3m$, where m is prime to 3. Every cycle of x with length greater than 2 has a length divisible by 3. Further $\alpha_1(x)=2$ or 0 and if $\alpha_1(x)=2$ then x is of odd order and if $\alpha_1(x)=0$ then $\alpha_2(x)=1$.

Proof. Let the order of x be $3^k m$, where m is prime to 3. Then, by the assumption, $k \geq 1$ and $u=x^{3^{k-1}m}$ is of order 3. If $k>1$ then $\alpha_1(u) \geq 3$, which contradicts (iii). Hence $k=1$. If x has a cycle of length l which is greater than 2 and prime to 3, then $\alpha_1(u) \geq l$, which contradicts (iii). Therefore every cycle of x with length greater than 2 has a length divisible by 3. By the similar reason, $\alpha_2(x) \leq 1$ and if $\alpha_1(x) \neq 0$ then $\alpha_1(x) \leq 2$ and $\alpha_2(x)=0$. Therefore if $\alpha_1(x) \neq 0$ then $\alpha_1(x)=2$ since $n \equiv 2 \pmod 3$ by (iii), and then x is of odd order by (iv). If $\alpha_1(x)=0$ and $I(u)=\{i, j\}$ then x has a 2-cycle (i, j). Hence $\alpha_2(x)=1$.

(vi) All involutions of G are conjugate.

Proof. Let a and b be two given involutions, and assume that $I(G_{1,2,3,4})=\{1, 2, 3, 4, 5\}$ for simplicity. Taking a conjugate if necessary, we may assume that $a=(1, 2)(3, 4)\cdots$. Then a normalizes $G_{1,2,3,4}$ and hence it fixes the letter 5. Thus a is of the form

$$a = (1, 2)(3, 4)(5)\cdots .$$

In the same way we may assume that b is of the form

$$b = (1, 2)(3)(4, 5)\cdots .$$

Then $ba=(1)(2)(3, 4, 5)\cdots$ and, by (v), it is of odd order. Therefore, by [4], Lemma 5.8.1, a and b are conjugate.

(vii) If a is an involution, then $\alpha_1(a) \geq 3$.

Proof. Since $N^{\Delta}=S_5$, there is an element of the form $(1)(2)(3)(4, 5)\cdots$. Now (vii) follows at once from (vi).

(viii) All involutions of $G_{1,2}$ are conjugate in $G_{1,2}$.

Proof. Let a and b be two given involutions of $G_{1,2}$. As in the proof of (vi) we may assume that a and b are of the following forms:

$$a = (1)(2)(3)(4, 5)\cdots,$$
$$b = (1)(2)(3, 4)(5)\cdots.$$

Then $ba=(1)(2)(3, 4, 5)\cdots$ is of odd order and hence a power of ba transforms a into b.

(ix) For a given invalution a, there is an element of order 3 such that $a^{-1}ua=u^{-1}$. And then ua is an involution.

Proof. Assume that $I(G_{1,2,3,4})=\{1, 2, 3, 4, 5\}$. Then we may assume that a is of the form

$$a = (1)(2)(3, 4)(5)\cdots.$$

By the quadruple transitivity of G, there is an involution b of the form $(2)(3)(4, 5)\cdots$. Then b normalizes $G_{2,3,4,5}$ and hence b fixes $I(G_{2,3,4,5})$. By the assumption $I(G_{2,3,4,5})=I(G_{1,2,3,4})=\{1, 2, 3, 4, 5\}$. Therefore b must be of the form

$$b = (1)(2)(3)(4, 5)\cdots.$$

Now, by (v), $ba=(1)(2)(3, 4, 5)\cdots$ is of order $3m$, where m is prime to 3. Since $a^{-1}(ba)a=ab=(ba)^{-1}$, $u=(ba)^m$ is a desired element. The rest of the statement is clear.

(x) All elements of order 3 are conjugate. If u is an element of order 3, then $N_G(u)$ is transitive on $\Omega-I(u)$.

Proof. We first remark that, since G is 3-fold transitive, the following follows from the results of Frobenius [2], [3]:

$$\sum_{x\in G}\alpha_3(x) = \frac{1}{3}|G|. \tag{1}$$

In the following, we shall consider the sum above. By (v), an element x with 3-cycle is expressed uniquely as a product of an element u of order 3 and a 3-regular element (i. e. an element of order prime to 3) y which commute with each other. It is then easy to see that $\alpha_3(x)$ equals $\frac{1}{3}\alpha_1^*(y)$, where $\alpha_1^*(y)$ denotes the number of the fixed letters of y belonging to $\Omega-I(u)$.

Let us assume that

$$u = (1)(2)(3, 4, 5)\cdots$$

is a fixed element of order 3 and let $\Gamma=\Omega-I(u)=\{3, 4, \cdots, n\}$. Then $N_G(u)$ induces a permutation group $N_G(u)^\Gamma$ on Γ. Since G is not a symmetric group, $N_G(u)$ is isomorphic to $N_G(u)^\Gamma$. Let $\alpha_1^*(y)$ denotes

$\alpha_1(y^\Gamma)$ for $y \in N_G(u)$ and let t be the number of the sets of transitivity of $N_G(u)^\Gamma$. If x is a 3-singular element (i. e. an element of order divisible by 3) of $N_G(u)$, then, by (v), $\alpha_1^*(x)=0$. If y is a 3-regular element of $N_G(u)$, then, as remarked above,

$$(2) \qquad \alpha_3(uy) = \frac{1}{3}\alpha_1^*(y).$$

Now, by [4], Theorem 16. 6. 13,

$$\sum_{x \in N_G(u)} \alpha_1^*(x) = t|N_G(u)^\Gamma| = t|N_G(u)|.$$

Since $\alpha_1^*(x)$ vanishes for a 3-singular element x, we have, from (2),

$$(3) \qquad \sum_y{}' \alpha_3(uy) = \frac{1}{3}t|N_G(u)|,$$

where in the left y ranges over all 3-regular elements of $N_G(u)$.

Now let the conjugate classes of G consisting of elements of order 3 be $\{u_1\}$, $\{u_2\}$,…, $\{u_k\}$. Then, from (3), we have

$$(4) \qquad \sum_{x \in G} \alpha_3(x) = \sum_i \frac{|G|}{|N_G(u_i)|}(\sum_y{}' \alpha_3(u_i y)) = \frac{1}{3}|G|(\sum_i t_i),$$

where in the second y ranges over all 3-regular elements of $N_G(u_i)$ and in the last t_i is the number of sets of transitivity of $N_G(u_i)$ which are cantained in $\Omega - I(u_i)$. From (1) and (4), we have $k=1$ and $t_1=1$.

(xi) Let u be an element of order 3 and suppose that $I(u)=\{1, 2\}$. Then the order of $N_G(u)$ is divisible by 2 to the first power, and $N_G(u) \cap G_{1,2}$ is transitive on $\{3, 4, \cdots, n\}$.

Proof. Since $N^\Delta = S_5$, there is an element of the form

$$(1, 2)(3, 4, 5)\cdots.$$

This shows that, for some element v of order 3, the order of $N_G(v)$ is even. Hence, by (x), the order of $N_G(u)$ is also even. Now, by (iv), $N_G(u) \cap G_{1,2}$ is of odd order. Hence $N_G(u) \neq N_G(u) \cap G_{1,2}$ and $|N_G(u): N_G(u) \cap G_{1,2}| = 2$. This proves the first half.

Since $N_G(u)$ is transitive on $\Gamma = \{3, 4, \cdots, n\}$ by (x), if $N_G(u) \cap G_{1,2}$ is intransitive on Γ, then Γ is the union of the two sets of transitivity of $N_G(u) \cap G_{1,2}$ and hence $|\Gamma|$ is even. This contradicts (i).

(xii) Let a be an involution of G. Then $N_G(a)$ is 3-fold transitive on $I(a)$.

Proof. We may assume that $\{1, 2\} \subset I(a)$. Since G is doubly transitive and, by (viii), the cyclic subgroup $\langle a\rangle$ of $G_{1,2}$ satisfies the assumption for U in the Witt's lemma, $N_G(a)$ is doubly transitive on $I(a)$. To prove the 3-fold transitivity, let u be an element of order 3 such that $a^{-1}ua=u^{-1}$. We may assume that

$$u=(1)(2)(3,4,5)\cdots.$$

Let $N_G^*(u)$ be the subgroup of G consisting of all the elements x such that $x^{-1}ux=u$ or u^{-1} and let $K^*=N_G^*(u)\cap G_{1,2}$ and $K=N_G(u)\cap G_{1,2}$. Then $|K^*:K|=2$ and K is of odd order, and hence $\langle a\rangle$ is a Sylow 2-subgroup of K^*. Let $\Gamma=\{3,4,\cdots,n\}$. Then K^* and K fix Γ and, since K^Γ is transitive, $(K^*)^\Gamma$ is also transitive. Therefore, by the Witt's lemma, $N_G(a)\cap K^*$ is transitive on $I(a)-\{1,2\}$. Since $N_G(a)\cap K^*\subset N_G(a)\cap G_{1,2}$, $N_G(a)\cap G_{1,2}$ is transitive on $I(a)-\{1,2\}$. This shows that $N_G(a)$ is 3-fold transitive on $I(a)$.

(xiii) An element of order 4 has no 2-cycles.

Proof. Let x be an element of order 4 and assume that x has a 2-cycle. Since n is odd, we may assume that

$$x=(1)(2,3)\cdots.$$

Then x^2 is an involution and $\{1,2,3\}\subset I(x^2)$. Let $r=\alpha_1(x^2)$. Then, by (ii), $r\equiv 0 \pmod 3$.

Now, by (xii), there is an element z in $N_G(x^2)$ such that

$$z=\begin{pmatrix}1\,2\,3\cdots\\3\,1\,2\cdots\end{pmatrix}.$$

Let $y=z^{-1}xz$. Then

$$y=(1,2)(3)\cdots$$

and $y^2=x^2$. Since

$$xy=(1,2,3)\cdots,$$

we can apply (v) to xy. If xy fixes a letter of $I(x^2)$, then, since $\alpha_1(xy)\leq 2$ and all cycles of xy are of length divisible by 3, we have $r\equiv 1$ or $2 \pmod 3$. This is a contradiction. If xy has a 2-cycle in $I(x^2)$, then in the same way we have $r\equiv 2 \pmod 3$, which is also a contradiction. Therefore the fixed letters or the letters of 2-cycle of xy appear in some 4-cycles of x.

Let as first assume that xy fixes letter i_1 and $x=(i_1,i_2,i_3,i_4)\cdots$. Then, since xy fixes i_1 and $x^2=y^2$, y must be of the form

$$y=(i_2,i_1,i_4,i_3)\cdots$$

and xy fixes the four letters i_1, i_2, i_3 and i_4. This conflicts with (v).

Next assume that xy has a 2-cycle (i_1, k_1). Then we may assume that x and y are of the forms

$$x = (i_1, i_2, i_3, i_4)\cdots,$$
$$y = (i_2, k_1, i_4, k_3)\cdots.$$

If k_1 lies in $\{i_1, i_2, i_3, i_4\}$ then k_1 and k_3 must be i_3 and i_1 respectively. Then xy has the two 2-cycles (i_1, i_3) and (i_2, i_4), which conflicts with (v). Hence k_1 must appear in another 4-cycle and we may assume that

$$x = (i_1, i_2, i_3, i_4)(k_1, k_2, k_3, k_4)\cdots.$$

Then, since xy takes k_1 to i_1, y must be of the form

$$y = (i_2, k_1, i_4, k_3)(k_2, i_1, k_4, i_3)\cdots$$

and xy has the two 2-cycles (i_1, k_1), (i_2, k_2), which conflicts with (v).

Next we shall consider a relation between the degree n and the number of the fixed letters of an involution. In this part we make use of the celebrated theorem of Feit and Thompson and a theorem of Brauer.

(xiv) The order of $H=G_{1,2,3,4}$ is prime to $n-2$.

Proof. Let $p\neq 1$ be a common prime divisor of $n-2$ and $|H|$ and P a Sylow p-subgroup of H. Let N' denote the normalizer of P in G and let Δ' denote $I(P)$. Then, by the Witt's lemma, $(N')^{\Delta'}$ is a 4-fold transitive group and the number of the fixed letters of $(N')^{\Delta'}{}_{1,2,3,4}$ is not less than 5. Hence, by Proposition 1 and 2 and by the minimal nature of the degree of G, $(N')^{\Delta'}$ must be one of the following groups: S_5, A_6 or M_{11}. Since every set of transitivity of P in $\Omega-\Delta'$ is of length divisible by p, we have that one of the numbers $n-5$, $n-6$ or $n-11$ is divisible by p. On the other hand, $n-2$ is also divisible by p. Therefore p must be 2 or 3. But, by (i), p can not be 2. If $p=3$, then H contains an element of order 3, which conflicts with (iii).

(xv) Let r be the number of the fixed letters of an involution. Then

$$n = r^2(r-2)+2.$$

Proof. Let us assume that $u=(1)(2)(3, 4, 5)\cdots$ is an element of order 3. Let $L=N_G(u)$, $K=L\cap G_{1,2}$ and let $L^*=N_G^*(u)$ be the subgroup consisting of all the elements x such that $x^{-1}ux=u$ or u^{-1}. Then, by (xi), K is a normal subgroup of odd order in L^* and $|L:K|=2$, and, by (ix), $|L^*:L|=2$. It is now easy to see that a Sylow 2-subgroup of L^* is a four group. By the theorem of Feit and Thompson [1] K is solvable. Let $W=K\cap G_{1,2,3}$. Since every element of W commutes with u, $W\subset H=G_{1,2,3,4}$. By (xi), $|K:W|=n-2$ and, by (xiv), it is prime to the order of W. Hence there is a Hall subgroup U of order $n-2$ in K, and then U is regular on $\{3,4,\cdots,n\}$. By the fundamental theorem of P. Hall, we have $L^*=N_{L^*}(U)K$. Let V be a Sylow 2-subgroup of $N_{L^*}(U)$. Then V is also a Sylow 2-subgroup of L^* and hence it is a four group. Now we may assume that V consists of the unit and the three involutions of the following forms:

$$a_1=(1,2)(3)(4)(5)\cdots,$$
$$a_2=(1)(2)(3)(4,5)\cdots,$$
$$a_3=a_1a_2=(1,2)(3)(4,5)\cdots,$$

where a_1 commutes with u, and a_2 and a_3 transform u into its inverse.

The four group V induces a group of automorphism of U, and hence we can apply a theorem of Brauer ([7], (1.1)). Let f_i be the number of the elements of U left invariant by a_i $(i=1,2,3)$, and let f_0 be the number of the elements of U left invariant by V. Then we have

$$f_1f_2f_3=f_0^2|U|=f_0^2(n-2).$$

Now U is regular on $\{3,4,\cdots,n\}$ and each a_i fixes the letter 3. Hence f_i is equal to the number of the fixed letters of a_i belonging to $\{3,4,\cdots,n\}$. Therefore we have $f_1=f_3=r$ and $f_2=r-2$. On the other hand, f_0 is a divisor of $|U|=n-2$ and hence it is odd. Furthermore it is a common divisor of $f_1=r$ and $f_2=r-2$. Hence we have $f_0=1$ and $r^2(r-2)=n-2$.

The rest of the proof is similar to (v)∼(viii) in the proof of Proposition 2.

Let P be a Sylow 2-subgroup of $H=G_{1,2,3,4}$, c a central involution of P and let $I(c)=\{1,2,\cdots,r\}$. If P contains no elements of order 4, then $r\leq 3$ and $n=r^2(r-2)+2\leq 11$. Then G must be S_5. Hence P contains an element of order 4 and then $U=P_{1,2,\cdots,r}$ satisfies the assumption of the Witt's lemma. Let $M=N_G(U)$ and $\Gamma=I(U)$. Then M^Γ is a 4-fold transitive group and $(M^\Gamma)_{1,2,3,4}$ fixes at least five letters. Therefore, by Proposition 1 and 2 and by the minimal nature of the degree of G, $|\Gamma|$ must be 5, 6 or 11. Thus we have $r\leq 11$. Since $r\equiv 3 \pmod 6$, $r=3$ or 9. If $r=9$ then $M^\Gamma=M_{11}$ and the involution c^Γ is a 2-cycle. But this is impossible. Hence $r=3$ and $n=11$. Then $G=M_{11}$, which contradicts the first assumption for G.

OSAKA CITY UNIVERSITY

References

[1] W. Feit and J. Thompson: *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029.
[2] G. Frobenius: *Über die Charaktere der symmetrischen Gruppen*, S.-B. Preuss. Akad. Wiss. Berlin (1900), 516–534.
[3] G. Frobenius: *Über die Charaktere der mehrfach trasitiven Gruppen*, S.-B. Preuss. Akad. Wiss. Berlin (1904), 528–571.
[4] M. Hall: The Theory of Groups, Macmillan, New York, 1959.
[5] C. Jordan: *Recherches sur les substitutions*, J. Math. Pure Appl. (2) **17** (1872), 351-363.
[6] H. Nagao and T. Oyama: *On multiply transitive groups* III, Osaka J. Math. **2** (1965), 319–326.
[7] H. Wielandt: *Beziehungen zwischen den Fixpunktzahlen von Automorphismengruppen einer endlichen Gruppe*, Math. Z. **73** (1960), 146–158.
[8] E. Witt: *Die 5-fach transitiven Gruppen von Mathieu*, Abh. Math. Sem. Univ. Hamburg **12** (1937), 256–264.