

On some doubly transitive permutation groups of degree n and order $2^l(n-1)n$

By Hiroshi KIMURA¹⁾

(Received Jan. 27, 1969)

(Revised Nov. 22, 1969)

1. Introduction.

Doubly transitive permutation groups of degree n and order $2(n-1)n$ were determined by N. Ito ([9]). Some doubly transitive permutation groups of degree n and order $4(n-1)n$ were studied in [10].

The object of this paper is to prove the following result.

THEOREM. *Let Ω be the set of symbols $1, 2, \dots, n$. Let \mathfrak{G} be a doubly transitive group on Ω of order $2^l(n-1)n$ ($l > 1$) not containing a regular normal subgroup and let \mathfrak{R} be the stabilizer of symbols 1 and 2. Assume that \mathfrak{R} is cyclic. Then \mathfrak{G} is isomorphic to one of the groups $PGL(2, *)$, $PSL(2, *)$, $PSU(3, 3^2)$ and $PSU(3, 5^2)$.*

We use the standard notation. $C_{\mathfrak{X}}(\mathfrak{Y})$ denotes the centralizer of a subset \mathfrak{Y} in a group \mathfrak{X} and $N_{\mathfrak{X}}(\mathfrak{Y})$ stands for the normalizer of \mathfrak{Y} in \mathfrak{X} . $\langle S, T, \dots \rangle$ denotes the subgroup of \mathfrak{X} generated by elements S, T, \dots of \mathfrak{X} .

2. On the degree of the permutation group \mathfrak{G} .

1. Let \mathfrak{H} be the stabilizer of the symbol 1. \mathfrak{R} is of order 2^l and it is generated by a permutation K . Let us denote the unique involution $K^{2^{l-1}}$ of \mathfrak{R} by τ . Since \mathfrak{G} is doubly transitive on Ω it contains an involution I with the cyclic structure $(1\ 2)\dots$. Then we have the following decomposition of \mathfrak{G} ;

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}I\mathfrak{H}.$$

Since I is contained in $N_{\mathfrak{G}}(\mathfrak{R})$, it induces an automorphism of \mathfrak{R} and (i) $K^I = K$ or $K\tau$, (ii) $K^I = K^{-1}\tau$ or (iii) $K^I = K^{-1}$. (For the case $l=2$, (i) $K^I = K$ or (iii) $K^I = K^{-1}$.) If an element $H'IH$ of a coset $\mathfrak{H}IH$ of \mathfrak{H} is an involution, then $IHH'I = (HH')^{-1}$ is contained in \mathfrak{R} . Hence, in the case (i) the coset $\mathfrak{H}IH$ contains just two involutions, namely $H^{-1}IH$ and $H^{-1}\tau IH$, in the case (ii) it contains just 2^{l-1} involutions, namely $H^{-1}K'IH$ for $K' \in \langle K^2 \rangle$, and in the case

1) This work was supported by The Sakkokai Foundation.

(iii), it contains just 2^l involutions, namely $H^{-1}K'IH$ for $K' \in \mathfrak{R}$. Let $g(2)$ and $h(2)$ denote the numbers of involutions in \mathfrak{G} and \mathfrak{H} , respectively. Then the following equality is obtained;

$$(2.1) \quad g(2) = h(2) + d(n-1),$$

where $d = 2, 2^{l-1}$ and 2^l for cases (i), (ii) and (iii), respectively.

2. For a set \mathfrak{T} of permutations of \mathfrak{G} , the set of all symbols fixed by \mathfrak{T} is denoted by $\mathfrak{S}(\mathfrak{T})$ and we denote the number of symbols in $\mathfrak{S}(\mathfrak{T})$ by $\alpha(\mathfrak{T})$. Let K^{2^l-j} denote the permutation of \mathfrak{R} such that $\alpha(\tau) = \alpha(K^{2^l-j}) > \alpha(K^{2^l-j-1})$ and let \mathfrak{R}_1 be the subgroup of \mathfrak{R} generated by K^{2^l-j} . Then the order of \mathfrak{R}_1 is equal to 2^j . Let \mathfrak{R}_1 keep i ($i \geq 2$) symbols of Ω , say $1, 2, \dots, i$, unchanged. It is trivial that $N_{\mathfrak{G}}(\mathfrak{R}_1) = C_{\mathfrak{G}}(\tau)$. Put $\mathfrak{S} = \mathfrak{S}(\mathfrak{R}_1) = \{1, 2, \dots, i\}$. We denote the factor group $N_{\mathfrak{G}}(\mathfrak{R}_1)/\mathfrak{R}_1$ by \mathfrak{G}_1 . By a theorem of Witt ([15, Theorem 9.4]), \mathfrak{G}_1 can be considered as a doubly transitive permutation group on \mathfrak{S} . The stabilizer of symbols 1 and 2 in \mathfrak{S} is the cyclic 2-group $\mathfrak{R}/\mathfrak{R}_1$. Thus the orders of $N_{\mathfrak{G}}(\mathfrak{R}_1)$ and $\mathfrak{H} \cap N_{\mathfrak{G}}(\mathfrak{R}_1)$ are equal to $2^i(i-1)$ and $2^i(i-1)$, respectively. Hence there exist $n(n-1)/i(i-1)$ involutions in \mathfrak{G} each of which is conjugate to τ .

At first, let us assume that n is odd. Let $h^*(2)$ be the number of involutions in \mathfrak{H} leaving only the symbol 1 fixed. Then from (2.1) and above argument the following equality is obtained;

$$(2.2) \quad h^*(2)n + n(n-1)/i(i-1) = (n-1)/(i-1) + h^*(2) + d(n-1).$$

Since i is less than n , it follows from (2.2) that $h^*(2) < d$ and hence $n = i(\beta i - \beta + 1)$, where $\beta = d - h^*(2)$. Since n is odd, i must be odd.

Next let us assume that n is even. Let $g^*(2)$ be the number of involutions in \mathfrak{G} leaving no symbol of Ω fixed. Then corresponding to (2.2) the following equality is obtained from (2.1);

$$(2.3) \quad g^*(2) + n(n-1)/i(i-1) = (n-1)/(i-1) + d(n-1).$$

It is easily proved that $g^*(2)$ is a multiple of $n-1$ (see [8] or [9]). It follows from (2.3) that $g^*(2) < d(n-1)$. Thus we have $n = i(\beta i - \beta + 1)$, where $\beta = d - g^*(2)/(n-1)$. Since n is even, i must be even.

3. We prove the theorem by induction on the degree n . Let $SL(2, 8)$ denote the two-dimensional special linear group over the field $GF(8)$ of eight elements, and let σ be the automorphism of $GF(8)$ of order three such that $\sigma(x) = X^2$ for every element x of $GF(8)$. Then σ can be considered in a usual way an automorphism of $SL(2, 8)$. Let $SL^*(2, 8)$ be the splitting extension of $SL(2, 8)$ by the group $\langle \sigma \rangle$. Then $SL^*(2, 8)$ has doubly transitive permutation representation on the set of Sylow 3-subgroups and its degree is equal to 28. The stabilizer of two symbols leaves four Sylow 3-subgroups fixed and every

involution is conjugate (see [8]).

THEOREM 1 (N. Ito, [8]). *Let \mathfrak{G} be a doubly transitive permutation group on Ω of order $2n(n-1)$ not containing a regular normal subgroup. Then \mathfrak{G} is isomorphic to either $PSL(2, 5)$ or $SL^*(2, 8)$.*

If \mathfrak{G} contains a regular normal subgroup, then its degree is equal to a power of a prime number. Thus, by Theorem 1, if $l=1$, then n is equal to 6, 28 or a power of a prime number.

3. The case n is odd.

1. Since $n = i(\beta i - \beta + 1)$ is odd, i must be odd. The group $\mathfrak{G}_1 = N_{\mathfrak{G}}(\mathfrak{R}_1)/\mathfrak{R}_1$ is a doubly transitive permutation group on $\mathfrak{Z}(\mathfrak{R}_1)$ and the stabilizer of symbols 1 and 2 is the subgroup $\mathfrak{R}/\mathfrak{R}_1$ of \mathfrak{G}_1 of order 2^{l-j} . By the inductive hypothesis, \mathfrak{G}_1 contains a regular normal subgroup and, in particular, i is equal to a power of an odd prime number, say p^m . Let \mathfrak{P} be a Sylow p -subgroup of $N_{\mathfrak{G}}(\mathfrak{R}_1)$ of order $i = p^m$. Since $\mathfrak{P}\mathfrak{R}_1/\mathfrak{R}_1$ is a regular normal subgroup of \mathfrak{G}_1 , \mathfrak{P} is elementary abelian and normal in $N_{\mathfrak{G}}(\mathfrak{R}_1)$. Let \mathfrak{B} denote the subgroup $\mathfrak{H} \cap N_{\mathfrak{G}}(\mathfrak{R}_1)$. Then the order of \mathfrak{B} is equal to $2^l(p^m - 1)$.

2. Case $n = i^2 = p^{2m}$. It can be proved in the same way as in [9, Case A] that there exists no group satisfying the conditions of the theorem in this case.

3. Case $n = p^m(\beta p^m - \beta + 1)$ with $\beta > 1$ and $\beta, \beta - 1 \not\equiv 0 \pmod{p}$. In this case it can be proved in the same way as in [10, § 2.5] that there is no group satisfying the conditions of the theorem in this case.

4. Case $n = p^m(\beta p^m - \beta + 1)$ with $\beta > 1$ and $\beta \equiv 0 \pmod{p}$. Since $\beta \geq 3$, d must be greater than 2 and hence $\langle K, I \rangle$ is dihedral or semi-dihedral.

Consider the cyclic structure of K and it can be seen that $n - i = \beta p^m(p^m - 1)$ is divisible by 2^l . Set $p = 2^k q + 1$, where $q (> 0)$ is odd. Since $2^l \geq \beta \geq p$, β is not divisible by 2^{l-k} and therefore $p^m - 1$ must be divisible by 2^{k+1} . Hence m is even.

At first assume that the order of $N_{\mathfrak{G}}(\mathfrak{R})$ is divisible by 2^{l+2} . Since $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is a complete Frobenius group on $\mathfrak{Z}(\mathfrak{R})$, any Sylow subgroup of a complement $\mathfrak{H} \cap N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is cyclic or quaternion (ordinary or generalized). Hence there exists a subgroup \mathfrak{S} of $N_{\mathfrak{G}}(\mathfrak{R})$ such that $\mathfrak{S} \supseteq \langle I, K \rangle$ and $\mathfrak{S}/\mathfrak{R}$ is a cyclic group of order 4. \mathfrak{S} contains S such that $S^2 \equiv I(\mathfrak{R})$, S induces an automorphism of \mathfrak{R} of order 4 and S^2 and I induce the same automorphism. But it is easily seen that, for any automorphism ζ of \mathfrak{R} of order 4, $K^{\zeta^2} = \tau K$. This is a contradiction since $\langle K, I \rangle$ is dihedral or semi-dihedral.

Next assume that the order of $N_{\mathfrak{G}}(\mathfrak{R})$ is not divisible by 2^{l+2} . Let \mathfrak{S} be a Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R}_1)$ containing $\langle I, K \rangle$. Since m is even, the order

of \mathfrak{S} is greater than 2^{l+2} . By the assumption of the order of $N_{\mathfrak{G}}(\mathfrak{R})$, $\mathfrak{S} \cap N_{\mathfrak{G}}(\mathfrak{R}) = \langle K, I \rangle$ is a Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R})$. Therefore $N_{\mathfrak{S}}(\langle K, I \rangle)$ is greater than $N_{\mathfrak{G}}(\mathfrak{R})$. Let $S (\neq 1)$ be a permutation of $N_{\mathfrak{S}}(\langle K, I \rangle) - \langle K, I \rangle$. Since K^S is contained in $\langle K, I \rangle$, we have $K^S = K'I$, where K' is a permutation of \mathfrak{R} . Hence, if $\langle K, I \rangle$ is dihedral, then $(K^S)^2 = 1$ and the order of K equals 2 and, if $\langle K, I \rangle$ is semi-dihedral, then $(K^S)^4 = 1$ and the order of K equals 4. This is a contradiction.

Thus there exists no group satisfying the conditions of the theorem in this case.

5. Case $n = p^m(\beta p^m - \beta + 1)$ with $\beta - 1 = 0 \pmod{p}$.

At first we shall prove that the order of $C_{\mathfrak{G}}(\mathfrak{B})$ is equal to $2^{j'} p^{m+m'} y$, where $j' \geq j$, $m' > 0$ and y is a factor of $\beta p^m - (\beta - 1)$ and not divisible by p . Assume that the order of $C_{\mathfrak{G}}(\mathfrak{B})$ is equal to $2^{j'} p^m$. Let \mathfrak{R}' be a Sylow 2-subgroup of $C_{\mathfrak{G}}(\mathfrak{B})$. Every element ($\neq 1$) of \mathfrak{B} leaves no symbol of Ω fixed. Then \mathfrak{R}' must leave at least two symbols of Ω fixed. Therefore \mathfrak{R}' is conjugate to a subgroup of \mathfrak{R} containing \mathfrak{R}_1 . Since $C_{\mathfrak{G}}(\mathfrak{B})$ is a direct product of \mathfrak{R}' and \mathfrak{B} , \mathfrak{R}' is normal in $N_{\mathfrak{G}}(\mathfrak{B})$. Since the order of $N_{\mathfrak{G}}(\mathfrak{R}')$ is a factor of the order of $N_{\mathfrak{G}}(\mathfrak{R}_1)$, the order of $N_{\mathfrak{G}}(\mathfrak{R}_1)$ is greater than or equal to the order of $N_{\mathfrak{G}}(\mathfrak{B})$. This contradicts the order of $N_{\mathfrak{G}}(\mathfrak{B})$. Hence the order of $C_{\mathfrak{G}}(\mathfrak{B})$ is equal to $2^{j'} p^m y$, where y is odd and $y > 1$. Let $q (\neq 2, p)$ be a prime factor of the order of $C_{\mathfrak{G}}(\mathfrak{B})$ and let Q be a permutation of $C_{\mathfrak{G}}(\mathfrak{B})$ of order q . If q is a factor of $n-1$, then Q leaves just one symbol of Ω fixed and hence Q cannot be contained in $C_{\mathfrak{G}}(\mathfrak{B})$. Thus q is a factor of n and so is y . Next assume that y is not divisible by p . Let \mathfrak{X}' be a normal p -complement in $C_{\mathfrak{G}}(\mathfrak{B})$. Since \mathfrak{R}' is cyclic, \mathfrak{X}' has a normal 2-complement \mathfrak{Y}' . Since \mathfrak{Y}' is a normal Hall subgroup of \mathfrak{X}' , \mathfrak{Y}' is normal even in $N_{\mathfrak{G}}(\mathfrak{B})$. Let $Y' (\neq 1)$ be a permutation of \mathfrak{Y}' . Then Y' does not leave any symbol of Ω fixed. If $\mathfrak{B} \cap G_{\mathfrak{G}}(Y')$ contains an involution τ' , then τ' is conjugate to τ under \mathfrak{G} and, since $C_{\mathfrak{G}}(\tau')$ contains Y' , the order of $C_{\mathfrak{G}}(\tau')$ is divisible by the order of Y' . But since $C_{\mathfrak{G}}(\tau')$ is conjugate to $C_{\mathfrak{G}}(\tau) = N_{\mathfrak{G}}(\mathfrak{R}_1)$ and the order of $N_{\mathfrak{G}}(\mathfrak{R}_1)$ and y are relatively prime, the order of $\mathfrak{B} \cap C_{\mathfrak{G}}(Y')$ is odd. Let q be a prime factor of the order of $\mathfrak{B} \cap C_{\mathfrak{G}}(Y')$ and let Q be a permutation of $\mathfrak{B} \cap C_{\mathfrak{G}}(Y')$ of order q . Then Q leaves at least one symbol of Ω fixed and hence it leaves at least two symbols of Ω fixed, which is a contradiction. Thus $\mathfrak{B} \cap C_{\mathfrak{G}}(Y') = (1)$. Hence we have the following relation;

$$y-1 = |\mathfrak{Y}'| - 1 \geq |\mathfrak{B}|,$$

$$\text{i. e., } y \geq 2^l(p^m - 1) + 1 = 2^l p^m - (2^l - 1).$$

On the other hand y is a factor of $\beta p^{m-1} - (\beta - 1)p^{-1}$. This is a contradiction. Hence y is divisible by p .

Let us assume $p^{m'} < 2^l$. Let \mathfrak{A} be a normal 2-complement of $C_{\mathfrak{G}}\mathfrak{P}$. Then \mathfrak{A} is normal in $N_{\mathfrak{G}}(\mathfrak{P})$. Let \mathfrak{P}' be a Sylow p -subgroup of \mathfrak{A} . By the Frattini argument $N_{\mathfrak{G}}(\mathfrak{P}) = \mathfrak{A}(N_{\mathfrak{G}}\mathfrak{P}' \cap N_{\mathfrak{G}}(\mathfrak{P}))$. Since the order of \mathfrak{A} is odd, we may assume that \mathfrak{R} is a subgroup of $N_{\mathfrak{G}}(\mathfrak{P}') \cap N_{\mathfrak{G}}(\mathfrak{P})$. Thus there exists a homomorphism π of \mathfrak{R} into $\text{Aut } \mathfrak{P}'/\mathfrak{P}$. If τ is contained in $\ker \pi$, then τ acts trivially on $\mathfrak{P}'/\mathfrak{P}$ and \mathfrak{P} . Therefore τ acts also trivially on \mathfrak{P}' and $C_{\mathfrak{G}}\tau$ contains \mathfrak{P}' ([4, Theorem 5.3.2]). Hence we have $\ker \pi = 1$ and $\text{Aut } \mathfrak{P}'/\mathfrak{P}$ contains a cyclic subgroup of order 2^l . But the order ($= p^{m'}$) of $\mathfrak{P}'/\mathfrak{P}$ is less than 2^l . This is a contradiction. If $m' \leq m$, then $p^{m'} < 2^l$. Thus we may assume $p^{m'} > 2^l$. Then $m' > m$.

Assume $y > 1$. Since \mathfrak{A} is solvable, there exists a subgroup \mathfrak{Y} of \mathfrak{A} of order y . Now Y is a factor of $\beta - (\beta - 1)p^{-m}$. By the Frattini argument it can be assumed that \mathfrak{R} is a subgroup of $N_{\mathfrak{G}}(\mathfrak{Y})$. Thus there exists a homomorphism π' of \mathfrak{R} into $\text{Aut } \mathfrak{Y}$. Since the orders of $C_{\mathfrak{G}}(\tau)$ and \mathfrak{Y} are relatively prime, any elements ($\neq 1$) of \mathfrak{Y} are not fixed by $\pi'(\tau)$. Therefore we have $y > 2^l$. This is impossible and hence $y = 1$. \mathfrak{P}' is normal in $N_{\mathfrak{G}}(\mathfrak{P})$. Let P' ($\neq 1$) be an element of \mathfrak{P}' . It can be seen that $\mathfrak{P} \cap C_{\mathfrak{G}}(P')$ is a subgroup of \mathfrak{R} . Hence we have the following relation;

$$p^{m+m'} - 1 = x(p^m - 1), \quad x > 1.$$

From this it is easily seen that m' is divisible by m .

If $\beta p^m - \beta + 1$ is divisible by $p^{\delta m}$ ($\delta > 1$) exactly, then $\beta - 1$ must be equal to $p^{\delta m}z + p^{(\delta-1)m} + \dots + p^m$ ($z > 1$) or $p^{(\delta-1)m} + \dots + p^m$. If $\beta - 1$ is equal to $p^{\delta m}z + p^{(\delta-1)m} + \dots + p^m$ ($z > 1$), then $2^l > p^{\delta m}$ ($\geq p^{m'}$). Therefore we may assume $\beta = p^{(\delta-1)m} + \dots + p^m + 1 = (p^{\delta m} - 1)/(p^m - 1)$ and $m' = \delta m$. \mathfrak{P}' is a Sylow p -subgroup of \mathfrak{G} .

Next we shall prove that $m = 1$ and K has only 2^l -cycles in its cyclic decomposition, i. e., $N_{\mathfrak{G}}(\mathfrak{R}) = C_{\mathfrak{G}}(\tau)$ and $\mathfrak{R} \cap \mathfrak{R}^G = 1$ or \mathfrak{R} for every element G of \mathfrak{G} . From (2.2) it can be seen that the number of involutions with the cyclic structures $(1, 2) \dots$ which are conjugate to τ is equal to β . If $\langle K, I \rangle$ is dihedral, then every involution in $I\mathfrak{R}$ is conjugate to I or IK and if $\langle K, I \rangle$ is semi-dihedral, then every involution in $I\mathfrak{R}$ is conjugate to I . Since all involutions with the cyclic structures $(1, 2) \dots$ are contained in $I\mathfrak{R}$, β is equal to $d/2$ or d . Thus $p^m + 1$ is a power of two and hence $m = 1$. Therefore \mathfrak{G}_1 is a complete Frobenius group, $\mathfrak{Z}(\tau) = \mathfrak{Z}(K)$, $N_{\mathfrak{G}}(\mathfrak{R}) = C_{\mathfrak{G}}(\tau)$ and $C_{\mathfrak{G}}(\mathfrak{R})$ contains \mathfrak{P} . Therefore the number of elements which leave only the symbol 1 fixed is equal to $2^l(n-1) - 1 - (2^l-1)(\beta i + 1)$ and the number of elements which leave i symbols of Ω fixed is equal to $(2^l-1)(\beta i - \beta + 1)(\beta i + 1)$. Let G be an element of \mathfrak{G} of order $2^l p$ ($l' \geq 1$). Then $\alpha(G) = 0$ and $\alpha(G^{p'}) = i$. Therefore the number of cyclic subgroups of \mathfrak{G} of order $2^l p$ is equal to $(\beta i - \beta + 1)(\beta i + 1)$ and those

groups are independent. Thus the number of elements of order $2^{l'}p(l' \geq 1)$ which leave no symbol of Ω fixed is equal to $(2^l-1)(i-1)(\beta i-\beta+1)(\beta i+1)$. Therefore we have

$$|\mathfrak{G}| - (n(2^l(n-1)-1-(2^l-1)(\beta i+1)) + (2^l-1)(\beta i-\beta+1)(\beta i+1) + (2^l-1)(n-1)(\beta i-\beta+1)+1) = n-1.$$

Hence \mathfrak{B}' is a regular normal subgroup of \mathfrak{G} .

Thus there exists no group satisfying the conditions of the theorem in this case.

4. The case n is even and $N_{\mathfrak{G}}(\mathfrak{R}_1)/\mathfrak{R}_1$ contains a regular normal subgroup.

1. Since $n = i(\beta i - \beta + 1)$ is even, i must be even. $\mathfrak{G}_1 = N_{\mathfrak{G}}(\mathfrak{R}_1)/\mathfrak{R}_1$ is a doubly transitive permutation group on $\mathfrak{Z}(\mathfrak{R}_1)$ containing a regular normal subgroup. In particular, i is equal to a power of 2, say 2^m .

Let \mathfrak{S} be the normal 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R}_1)$ containing \mathfrak{R}_1 such that $\mathfrak{S}/\mathfrak{R}_1$ is a regular normal subgroup of $\mathfrak{G}_1 = N_{\mathfrak{G}}(\mathfrak{R}_1)/\mathfrak{R}_1$. Since the order of $\mathfrak{H} \cap N_{\mathfrak{G}}(\mathfrak{R}_1)$ is equal to $2^l(2^m-1)$, \mathfrak{R} is a Sylow 2-subgroup of $\mathfrak{H} \cap N_{\mathfrak{G}}(\mathfrak{R}_1)$. Let \mathfrak{B} be a normal 2-complement of $\mathfrak{H} \cap N_{\mathfrak{G}}(\mathfrak{R}_1)$. The group $\mathfrak{B}\mathfrak{S}/\mathfrak{R}_1$ is a complete Frobenius group on $\mathfrak{Z}(\mathfrak{R}_1)$ with kernel $\mathfrak{S}/\mathfrak{R}_1$ and complement $\mathfrak{B}\mathfrak{R}_1/\mathfrak{R}_1 (\cong \mathfrak{B})$. Since $C_{\mathfrak{G}}(\mathfrak{R}_1) \cap \mathfrak{B}\mathfrak{S}$ is normal in $\mathfrak{B}\mathfrak{S}$, $C_{\mathfrak{G}}(\mathfrak{R}_1) \cap \mathfrak{B}\mathfrak{S}$ contains \mathfrak{S} or is contained in \mathfrak{S} ([13, 12.6.8]). If \mathfrak{S} is greater than $C_{\mathfrak{G}}(\mathfrak{R}_1) \cap \mathfrak{B}\mathfrak{S}$, since the index of \mathfrak{S} in $\mathfrak{B}\mathfrak{S}$ must be equal to a power of two, we have $m=1$. Hence \mathfrak{G} is a Zassenhaus group. Thus we have that \mathfrak{G} is isomorphic to either $PGL(2, 2^l+1)$ or $PSL(2, 2^{l+1}+1)$, where 2^l+1 and $2^{l+1}+1$ are powers of prime numbers for $PGL(2, 2^l+1)$ and $PSL(2, 2^{l+1}+1)$, respectively ([1], [8], [14] and [18]). Thus it will be assumed that \mathfrak{S} is contained in $C_{\mathfrak{G}}(\mathfrak{R}_1) \cap \mathfrak{B}\mathfrak{S}$ and m is greater than one.

Since the index of $\mathfrak{B}\mathfrak{S} \cap C_{\mathfrak{G}}(\mathfrak{R}_1)$ in $\mathfrak{B}\mathfrak{S}$ is odd and the order of $\text{Aut } \mathfrak{R}_1$ is equal to 2^{j-1} , $\mathfrak{B}\mathfrak{S} \cap C_{\mathfrak{G}}(\mathfrak{R}_1)$ is equal to $\mathfrak{B}\mathfrak{S}$. Hence $C_{\mathfrak{G}}(\mathfrak{R}_1)$ is equal to $N_{\mathfrak{G}}(\mathfrak{R}_1)$ since $N_{\mathfrak{G}}(\mathfrak{R}_1) = \mathfrak{R}\mathfrak{B}\mathfrak{S}$.

PROPOSITION 4.1. *Let \mathfrak{G} be as in Theorem and let \mathfrak{R}_1 and \mathfrak{G}_1 as above. Assume that \mathfrak{G}_1 contains a regular normal subgroup and $N_{\mathfrak{G}}(\mathfrak{R}_1)$ is equal to $C_{\mathfrak{G}}(\mathfrak{R}_1)$. Let \mathfrak{S} be as above. Then \mathfrak{S} contains an involution ($\neq \tau$).*

PROOF. If \mathfrak{R}_1 is equal to \mathfrak{R} , then \mathfrak{S} is a normal Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R})$ and hence it contains I . Therefore it can be assumed that \mathfrak{R}_1 is less than \mathfrak{R} and $I \notin \mathfrak{S}$. Assume that τ is the unique involution in \mathfrak{S} . Since $\mathfrak{S}/\mathfrak{R}_1$ is an elementary abelian group of order 2^m and $m \geq 2$, \mathfrak{S} is a quaternion group (ordinary or generalized) and hence $m=2$ (and $i=4$). Thus we have $\alpha(K) = \dots = \alpha(K^{2^l-j-1}) = 2 < \alpha(K^{2^l-j}) = 4$. Since $\mathfrak{R}\mathfrak{S}$ is a Sylow 2-subgroup of

$N_{\mathfrak{G}}(\mathfrak{R}_1)$, it may be assumed that I is contained in the coset $K^{2^l-j-1}\mathfrak{S}$ and hence we have $IK^{2^l-j-1}=S$, where S is an element ($\in K_1$) of \mathfrak{S} . Thus $(K^{2^l-j-1})^I = S^2K^{-2^l-j-1}$. Since $N_{\mathfrak{G}}(\mathfrak{R}_1) = C_{\mathfrak{G}}(\mathfrak{R}_1)$, we have $K^{2^l-j} = S^4K^{-2^l-j}$ and $S^4 = K^{2^l-j+1}$. At first assume that $S^4 = 1$. Then $j=1$ and $(K^{2^l-2})^I = K^{-2^l-2}\tau = K^{2^l-2}$. This implies $d=2$. Hence $n=16$ or 28 . Since $n-i$ and $i-\alpha(K)$ are divisible by 2^l and 2^{l-1} , respectively, the order of \mathfrak{R} is equal to four. It can easily be seen that there exists no group satisfying the conditions of Proposition in these cases. Next assume that $S^4 \neq 1$ (i. e., $j \neq 1$). Then $(K^{2^l-j-1})^I = K^{2^l-j-1}$ or $K^{2^l-j-1}\tau$ and hence $d=2$. This implies $n=16$ or 28 . Since $n-i$ is divisible by 2^l and $j > 1$, we have $n=28$, $l=3$ and $j=2$. By [15] \mathfrak{G} must be isomorphic to $PSU(3, 3^2)$. But a Sylow 2-subgroup of $PSU(3, 3^2)$ is isomorphic to $Z_4 \sim Z_2$ and it does not contain a quaternion group of order 16. This is a contradiction. Thus the proof is completed.

COROLLARY 4.2. *Let $\mathfrak{G}, \mathfrak{S}$ be as in Proposition 4.1. If d is equal to two, then \mathfrak{S} contains an involution τ' such that it is conjugate to τ .*

PROOF. By Proposition, \mathfrak{S} contains an involution $\eta (\neq \tau)$ with the cyclic structure $(1 a) \dots$, where a is a symbol of $\mathfrak{Z}(\mathfrak{R}_1)$. Then $\eta\tau$ has also the cyclic structure $(1 a) \dots$. Hence since \mathfrak{G} is doubly transitive, there exist two involutions with the cyclic structure $(1, b)$, where b is any symbol of \mathfrak{Q} , such that those are conjugate to η or $\eta\tau$. If τ is neither conjugate to η nor $\eta\tau$, then $g^*(2)$ is greater than $(n-1)$. This contradicts the inequality $g^*(2) < d(n-1)$.

By the above proposition, since $N_{\mathfrak{G}}(\mathfrak{R}_1)/\mathfrak{R}_1$ is doubly transitive, we may assume that I is contained in \mathfrak{S} . Since $\mathfrak{B}\mathfrak{S}/\mathfrak{R}_1$ is complete Frobenius group, all elements ($\neq 1$) of $\mathfrak{S}/\mathfrak{R}_1$ are conjugate under $\mathfrak{B}\mathfrak{R}_1/\mathfrak{R}_1$. Thus every permutation ($\neq \mathfrak{R}_1$) of \mathfrak{S} can be represented in the form $V^{-1}IVK'$, where V and K' are permutations of \mathfrak{B} and \mathfrak{R}_1 , respectively.

2. Case $\mathfrak{R}_1 = \mathfrak{R}$. In this case \mathfrak{S} is a normal Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R})$. Let S be an element of order 2^l in \mathfrak{S} . Since S^2 is contained in \mathfrak{R} , $S^{2^{l-1}}$ is equal to τ . Assume that I is conjugate to τ . Since $C_{\mathfrak{G}}(\mathfrak{R})$ and $C_{\mathfrak{G}}(I)$ are conjugate and K is contained in $C_{\mathfrak{G}}(I)$, $K^{2^{l-1}}$ must be equal to I . This is a contradiction.

Thus there exists no group satisfying the conditions of the theorem in this case.

3. Case $\mathfrak{R} \cong \mathfrak{R}_1 \cong \langle \tau \rangle$. Since \mathfrak{R}_1 is greater than $\langle \tau \rangle$, a group $\langle K, I \rangle$ is neither dihedral nor semi-dihedral and therefore d is equal to two. By Corollary 4.2 it may be assumed that I is conjugate to τ .

LEMMA 4.3. *If \mathfrak{R}_1 is greater than $\langle \tau \rangle$ and less than \mathfrak{R} , then the order of \mathfrak{R}_1 is equal to four and I is not contained in $C_{\mathfrak{G}}(\mathfrak{R})$.*

PROOF. At first assume that the order of \mathfrak{R}_1 is greater than four. Let \mathfrak{S}' be a Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R}_1)$. Let S be an element of \mathfrak{S}' of order

2^{l-1} . The index of \mathfrak{S} in \mathfrak{S}' is equal to 2^{l-j} . Therefore $S^{2^{l-j}}$ is contained in \mathfrak{S} and, since $\mathfrak{S}/\mathfrak{R}_1$ is elementary abelian, $S^{2^{l-j+1}}$ is contained in \mathfrak{R}_1 . Since j is greater than 2, $S^{2^{l-j+1}}$ is not identity element. Thus we have that $S^{2^{l-2}}$ is equal to τ . Since IKI is equal to K or $K\tau$, I is contained in $C_{\mathfrak{G}}(K^2)$ and hence K^2 is contained in $C_{\mathfrak{G}}(I)$. Since $N_{\mathfrak{G}}(\mathfrak{R}_1) = C_{\mathfrak{G}}(\tau)$ is conjugate to $C_{\mathfrak{G}}(I)$, we have that $(K^2)^{2^{l-2}} = \tau$ must be equal to I . This is a contradiction.

Next assume that I is contained in $C_{\mathfrak{G}}\mathfrak{R}$. Let \mathfrak{S}' be as above. Let S be an element of \mathfrak{S}' of order 2^l . Then $S^{2^{l-j}}$ is contained in \mathfrak{S} , $S^{2^{l-j+1}}$ is contained in K_1 and finally $S^{2^{l-1}}$ is equal to τ . Since K is contained in $C_{\mathfrak{G}}(I)$ and $C_{\mathfrak{G}}(I)$ is conjugate to $C_{\mathfrak{G}}(\tau)$, $K^{2^{l-1}}$ must be equal to I . This is a contradiction. Thus the proof is completed.

LEMMA 4.4. *Let \mathfrak{R}_1 be as in Lemma 4.3. Then the order of \mathfrak{R} is equal to 8.*

PROOF. Assume that the order of \mathfrak{R} is greater than 8. Then $\langle K^{2^{l-3}}, I \rangle$ is abelian since $d=2$ and $l>3$. Let η be an involution of $N_{\mathfrak{G}}(\langle K^{2^{l-3}} \rangle)$. Then $\langle K^{2^{l-3}}, \eta \rangle$ must be abelian, for if it is not abelian, then $\langle K^{2^{l-3}}, I \rangle$ is dihedral and hence $d \neq 2$.

At first we shall prove that a coset $K^{2^{l-3}}\mathfrak{S}$ does not contain an element of order 4. By Lemma 4.3 the order of \mathfrak{R}_1 is equal to 4. Let $K^{2^{l-3}}S$ be an element of order 4 in $K^{2^{l-3}}\mathfrak{S}$, where S is an element of \mathfrak{S} . Then S is not contained in $C_{\mathfrak{G}}(K^{2^{l-3}})$. Set $S = I^V K_1$, where K_1 and V are elements of \mathfrak{R}_1 and \mathfrak{B} , respectively. Then $K^{2^{l-3}}I^V$ must be of order 4. Thus it may be assumed that S is equal to I^V not contained in $C_{\mathfrak{G}}(K^{2^{l-3}})$, where V is an element of \mathfrak{B} . $(K^{2^{l-3}}S)^2$ is an element of \mathfrak{S} and therefore is equal to τ , I^W or $I^W\tau$, where W is an element of \mathfrak{B} . If $(K^{2^{l-3}}S)^2 = \tau$, then $(K^{2^{l-3}}S)^s = (K^{-2^{l-3}})\tau$ and hence $S \in N_{\mathfrak{G}}(\langle K^{2^{l-3}} \rangle)$. Thus $\langle K^{2^{l-3}}, S \rangle$ must be abelian. This is a contradiction. If $(K^{2^{l-3}}S)^2 = I^W$ or $I^W\tau$, then $(K^{2^{l-3}}S)^s = K^{-2^{l-3}}I^W$ or $K^{-2^{l-3}}I^W\tau$, respectively. Hence

$$K^{2^{l-2}} = (K^{2^{l-2}})^s = (K^{-2^{l-3}}I^W)^2$$

and

$$(K^{-2^{l-3}}I^W)^2 = K^{2^{l-2}}K^{2^{l-3}}.$$

Thus I^W is contained in $N_{\mathfrak{G}}(\langle K^{2^{l-3}} \rangle)$ and therefore $\langle I^W, K^{2^{l-3}} \rangle$ must be abelian. Hence $K^{2^{l-2}}K^{2^{l-3}} = K^{-2^{l-3}}$. Thus the order of \mathfrak{R} must be equal to $l-1$. This is a contradiction.

Next let S be an element of order 2^{l-1} in $\mathfrak{R}\mathfrak{S}$, and let \bar{S} be the image of S by the natural homomorphism of $\mathfrak{R}\mathfrak{S}$ onto $\mathfrak{R}\mathfrak{S}/\mathfrak{S}$. If the order of \bar{S} is equal to 2^{l-2} , then $S^{2^{l-3}}$ is contained in a coset $K^{2^{l-3}}S$. This contradicts the first part in the proof. Hence we have that the order of \bar{S} is less than 2^{l-2} and hence $S^{2^{l-3}}$ is contained in S . Therefore $S^{2^{l-2}}$ is equal to τ . Since $C_{\mathfrak{G}}(I)$ is conjugate to $N_{\mathfrak{G}}(\mathfrak{R}_1)$ and K^2 is contained in $C_{\mathfrak{G}}(I)$, $K^{2^{l-1}} = I$. This is a contradiction. Thus the proof is completed.

By two lemmas the orders of \mathfrak{R} and \mathfrak{R}_1 are equal to 8 and 4, respectively. Clearly $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is a complete Frobenius group on $\mathfrak{Z}(\mathfrak{R})$. Apply the argument in § 2 to $N_{\mathfrak{G}}(\mathfrak{R}_1)/\mathfrak{R}_1$ and we obtain that $\alpha(\mathfrak{R})$ must be a power of two and $i = \alpha(\mathfrak{R})^2$. Thus a Frobenius kernel of $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is a Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$. Since, by Lemma 4.3, I is not contained in $C_G(K)$, a Sylow 2-subgroup of $N_G(K)$ is greater than $C_{\mathfrak{G}}(\mathfrak{R})$ ([13, 12.6.8]). Since the order of $N_{\mathfrak{G}}(\mathfrak{R})/C_{\mathfrak{G}}(\mathfrak{R})$ is a power of two, $\alpha(K) - 1$ must be equal to one and hence $\alpha(K) = 2$. Thus we have $i = 4$ and $n = 16$ or 28 . Since $n - i$ must be divisible by the order of \mathfrak{R} , we have $n = 28$. \mathfrak{G} satisfies the conditions of the theorem in [15] and hence \mathfrak{G} is isomorphic to $PSU(3, 3^2)$.

4. Case $\mathfrak{R}_1 = \langle \tau \rangle$. We shall prove that $d = 2$ or the order of \mathfrak{R} is equal to four, $\langle K, I \rangle$ is dihedral and $i = 4$. In this case every permutation ($\in \mathfrak{R}_1$) of \mathfrak{S} can be represented uniquely in the form I^V or $I^V\tau$, where V is any permutation of \mathfrak{B} . Thus every permutation ($\neq 1$) of \mathfrak{S} is of order 2 and hence \mathfrak{S} is elementary abelian. Set $\mathfrak{R}_2 = \langle K^{2^{l-j'}} \rangle$, where $\alpha(\tau) > \alpha(K^{2^{l-2}}) = \dots = \alpha(K^{2^{l-j'}}) > \alpha(K^{2^{l-j'-1}})$. Set $i' = \alpha(K_2)$. Then we may assume $\mathfrak{Z}(\mathfrak{R}_2) = \{1, 2, \dots, i'\}$. Apply the argument in § 2 to $N_{\mathfrak{G}}(\mathfrak{R}_1)/\mathfrak{R}_1$, and we have $i = i'(\beta'i' - \beta' + 1)$. Hence i' is equal to a power of two, say $2^{m'}$. By the inductive hypothesis $N_{\mathfrak{G}}(\mathfrak{R}_2)/\mathfrak{R}_2$ contains a regular normal subgroup. Let \mathfrak{S}_2 be a normal 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R}_2)$ containing \mathfrak{R}_2 such that $\mathfrak{S}_2/\mathfrak{R}_2$ is a regular normal subgroup of $N_{\mathfrak{G}}(\mathfrak{R}_2)/\mathfrak{R}_2$ and let \mathfrak{B}_2 be a 2-complement of $\mathfrak{H} \cap \mathfrak{N}_{\mathfrak{G}}(\mathfrak{R}_2)$. Then $\mathfrak{B}_2\mathfrak{S}_2/\mathfrak{R}_2$ is a complete Frobenius group on $\mathfrak{Z}(\mathfrak{R}_2)$. Thus $C_{\mathfrak{G}}(\mathfrak{R}_2) \cap \mathfrak{B}_2\mathfrak{S}_2$ contains \mathfrak{S}_2 or is less than \mathfrak{S}_2 .

If $C_{\mathfrak{G}}(\mathfrak{R}_2) \cap \mathfrak{B}_2\mathfrak{S}_2$ is less than \mathfrak{S}_2 , then I is not contained in $C_{\mathfrak{G}}(\mathfrak{R}_2)$ and, since the order of $\mathfrak{B}_2\mathfrak{S}_2/C_{\mathfrak{G}}(\mathfrak{R}_2) \cap \mathfrak{B}_2\mathfrak{S}_2$ is a power of two, m' must be equal to one. Thus $i' = 2$ and $\mathfrak{R}_2 = \mathfrak{R}$. On the one hand, it is trivial that $i - 2$ must be divisible by 2^{l-1} . On the other hand, i is of a form $2(2\beta' - \beta' + 1)$ where β' is less than or equal to 2^{l-1} and hence β' is odd. Therefore we have $l = 2$, $\beta' = 1$ and $i = 4$.

If $C_{\mathfrak{G}}(\mathfrak{R}_2) \cap \mathfrak{B}_2\mathfrak{S}_2$ contains \mathfrak{S}_2 , then $K^I = K$ or K_τ and hence $d = 2$.

5. Case $|\mathfrak{R}| = 4$, $\mathfrak{R}_1 = \langle \tau \rangle$ and $K^I = K^{-1}$. Let \mathfrak{R}_2 and \mathfrak{S}_2 be as in § 4.4. Since $\mathfrak{R}_2 = \mathfrak{R}$, $\mathfrak{S}_2/\mathfrak{R}$ is a regular normal subgroup of $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ and $N_{\mathfrak{G}}(\mathfrak{R}) = \mathfrak{R} + I\mathfrak{R}$. Since $\langle K, I \rangle$ is dihedral, involutions with the cyclic structure $(12) \dots$ are I , IK , IK^2 and IK^3 , and I and IK are conjugate to IK^2 and IK^3 , respectively. Therefore $g^*(2) = 0$ or $2(n - 1)$.

If $g^*(2) = 0$, then $n = 4(4 \cdot 4 - 3) = 4 \cdot 13$. Let \mathfrak{P}_{13} be a Sylow 13-subgroup of \mathfrak{G} . Since every involution leaves four symbols of \mathcal{Q} fixed, the order of $C_{\mathfrak{G}}(\mathfrak{P}_{13})$ is equal to 13. Thus the index of $N_{\mathfrak{G}}(\mathfrak{P}_{13})$ in \mathfrak{G} is a multiple of $17 \cdot 4$. This contradicts the Sylow's theorem.

If $g^*(2) = 2(n - 1)$, then $n = 4(2 \cdot 4 - 1) = 4 \cdot 7$. Let η be an involution leaving

no symbol of Ω fixed. Then, since $g^*(2) = 2(n-1)$, $G_{\mathfrak{G}}\eta$ must be equal to $2n$. Let \mathfrak{P}_7 be a Sylow 7-subgroup of \mathfrak{G} contained in $C_{\mathfrak{G}}\eta$. Using Sylow's theorem \mathfrak{P}_7 is normal in $C_{\mathfrak{G}}\eta$. Hence the order of $N_{\mathfrak{G}}(\mathfrak{P}_7)$ is a multiple of $8 \cdot 7$. This contradicts the Sylow's theorem.

Thus there exists no group satisfying the conditions of the theorem in this case.

6. Case $\mathfrak{R}_1 = \langle \tau \rangle$, $d = 2$ and $n = i^2$. In this case a normal subgroup \mathfrak{S} of $N_{\mathfrak{G}}(\mathfrak{R}_1)$ is an elementary abelian 2-group. We shall prove several lemmas.

LEMMA 4.5. \mathfrak{S} contains every involution of $N_{\mathfrak{G}}(\mathfrak{R}_1)$.

PROOF. Set $\mathfrak{S}' = \mathfrak{R}\mathfrak{S}$. Then \mathfrak{S}' be a Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R}_1)$. If a coset $K^{2^{l-2}}\mathfrak{S}$ does not contain an involution, then the proof is complete. Let $K^{2^{l-2}}S$ be an involution in a coset $K^{2^{l-2}}\mathfrak{S}$, where S is a permutation of \mathfrak{S} . Then $(K^{2^{l-2}})^S = K^{-2^{l-2}}$. Therefore, since S is an involution, d must be greater than two. This is a contradiction.

LEMMA 4.6. Let G be an element of \mathfrak{G} . Then $\mathfrak{S}^G \cap \mathfrak{S} = 1$ or \mathfrak{S} .

PROOF. Let τ' be an involution of $\mathfrak{S}^G \cap \mathfrak{S}$. If τ' is conjugate to τ , then, since $C_{\mathfrak{G}}(\tau')$ contains \mathfrak{S}^G and \mathfrak{S} , \mathfrak{S}^G coincide with \mathfrak{S} by Lemma 4.5. Thus an involution of \mathfrak{S} which is conjugate to τ in \mathfrak{G} is conjugate to τ in $N_{\mathfrak{G}}(\mathfrak{S})$. By Corollary 4.2, I or $I\tau$ is conjugate to τ in G . On the other hand, I or $I\tau$ is not conjugate to τ in \mathfrak{G} , since $g^*(2) = n-1$. Hence the number of involutions of \mathfrak{S} each of which is conjugate to τ is equal to i and the number of involutions of \mathfrak{S} each of which leaves no symbol of Ω fixed is equal to $i-1$. Hence the order of $N_{\mathfrak{G}}(\mathfrak{S})$ is equal to $2^{li^2}(i-1)$ and the following relation is obtained;

$$n-1 = g^*(2) \leq (i-1)[\mathfrak{G} : N_{\mathfrak{G}}(\mathfrak{S})] = n-1.$$

Thus $\mathfrak{S}^G \cap \mathfrak{S} = 1$ or \mathfrak{S} .

LEMMA 4.7. Let η and ζ be different involutions. If $\alpha(\eta) = \alpha(\zeta) = 0$, then $\alpha(\eta\zeta) = 0$.

PROOF. Let a be a symbol of $\mathfrak{S}(\eta\zeta)$. Let $(a, b) \dots$ and $(b, c') \dots$ be the cyclic structure of η and ζ , respectively. Then $a = c'$. Since $g^*(2) = n-1$, there exists just one involution leaving no symbol of Ω fixed with the cyclic structure $(a, b) \dots$ and hence $\eta = \zeta$.

COROLLARY 4.8. A set \mathfrak{S}_1 consisting of all involutions of \mathfrak{S} each of which is not conjugate to τ and identity element is a characteristic subgroup of \mathfrak{S} . In particular $N_{\mathfrak{G}}(\mathfrak{S}_1) = N_{\mathfrak{G}}(\mathfrak{S})$.

By Corollary 4.8, there exists just $i+1$ subgroups $\mathfrak{S}_1, \mathfrak{S}_2, \dots, \mathfrak{S}_{i+1}$ which are conjugate in \mathfrak{G} and $\mathfrak{S}_s \cap \mathfrak{S}_t = 1$ for $s \neq t$.

LEMMA 4.9. Let τ' be an involution of $N_{\mathfrak{G}}(\mathfrak{S})$. If τ' is conjugate to τ , then τ' is contained in \mathfrak{S} .

PROOF. Set $\tau^G = \tau'$. Since the order of \mathfrak{S} is even, it is trivial that there

exists an element ζ of \mathfrak{S} with $\zeta\tau' = \zeta$. \mathfrak{S}^g is normal in $C_{\mathfrak{G}}(\tau')$ and it contains ζ and τ' by Lemma 4.5. Thus $\mathfrak{S} \cap \mathfrak{S}^g$ contains ζ and hence $\mathfrak{S} = \mathfrak{S}^g$ by Lemma 4.6. Finally τ' is an element of \mathfrak{S} .

LEMMA 4.10. *Let η be an involution which is not contained in \mathfrak{S} . If $\alpha(\eta) = 0$, then $\alpha(\tau\eta) = 0$ and the order of $\tau\eta$ is equal to 2^r with $r > 1$.*

PROOF. Assume $\alpha(\tau\eta) \neq 0$. Let a be a symbol of $\mathfrak{Z}(\tau\eta)$. It is trivial that a is not a symbol of $\mathfrak{Z}(\tau)$. Thus let $(a, b) \dots$ and $(b, c') \dots$ be the cyclic structures of τ and η , respectively. Then $a = c'$ and $\tau\eta\tau = (a, b) \dots$. Since $g^*(2) = n - 1$, there exists just one involution with the cyclic structure $(a, b) \dots$ such that it leaves no symbol of Ω fixed. Thus we have $\tau\eta\tau = \eta$. Therefore η must be contained in \mathfrak{S} and hence $\alpha(\tau\eta) = 0$. Next assume that the order of $\tau\eta$ is not equal to 2^r . Let p be an odd prime factor of the order of $\tau\eta$ and let pq be the order of $\tau\eta$. Then the order of $(\tau\eta)^q$ is equal to p and hence $\alpha((\tau\eta)^q) = 1$. Therefore $\alpha(\tau\eta) = 1$. Thus the order of $\tau\eta$ is equal to a power of two.

LEMMA 4.11. *Let η be an involution which is not conjugate to τ . Then η is contained in $N_{\mathfrak{G}}(\mathfrak{S})$.*

PROOF. Let us assume that η is not contained in \mathfrak{S} . By Lemma 4.10, the order of $\tau\eta$ is equal to 2^r with $r > 1$. Thus $\tau(\tau\eta)^{2^r} = \tau$. Set $\gamma_{\tau,\eta}(s) = \tau(\tau\eta)^{2^s} = \tau \overset{\tau\eta}{\curvearrowright} \dots \overset{\tau\eta}{\curvearrowright} \tau$. Then $\gamma_{\tau,\eta}(r-1)$ is contained in $C_{\mathfrak{G}}(\tau)$ and hence by Lemma 4.5, it is contained in \mathfrak{S} . Since $\gamma_{\tau,\eta}(r-1) = \tau^i \tau \eta^{(r-2)}$, $\gamma_{\tau,\eta}(r-2)$ is contained in $N_{\mathfrak{G}}(\mathfrak{S})$ by Lemma 4.6. By Lemma 4.9 it is contained in \mathfrak{S} . Continuing in the similar way, it can be shown that $\gamma_{\tau,\eta}(1) = \tau^\eta$ is contained in S . By Lemma 4.6, η is contained in $N_{\mathfrak{G}}(\mathfrak{S})$.

By Lemma 4.11, $N_{\mathfrak{G}}(\mathfrak{S}) = N_{\mathfrak{G}}(\mathfrak{S}_1)$ contains \mathfrak{S}_t ($2 \leq t \leq i+1$). Similarly $N_{\mathfrak{G}}(\mathfrak{S}_t)$ contains \mathfrak{S}_1 . Therefore $\mathfrak{S}_1\mathfrak{S}_t$ is the direct product $\mathfrak{S}_1 \times \mathfrak{S}_t$. In the similar way it can be proved that every element of \mathfrak{S}_t is commutative with any element of $\mathfrak{S}_{t'}$ ($1 \leq t, t' \leq i+1$). Thus $\mathfrak{N} = \mathfrak{S}_1 \cup \dots \cup \mathfrak{S}_{i+1}$ is a group. Hence \mathfrak{N} is a regular normal subgroup of \mathfrak{G} .

Thus there exists no group satisfying the conditions of the theorem in this case.

7. Case $\mathfrak{R}_1 = \langle \tau \rangle$, $d = 2$ and $n = i(2i-1)$. In this case $g^*(2) = 0$. Hence every involution is conjugate to τ . The order of \mathfrak{G} is equal to $2^{l+m}(2^{m+1}-1)(2^{m+1}+1)(2^m-1)$.

Set $\mathfrak{S}' = \mathfrak{R}\mathfrak{S}$. Since $\mathfrak{S}'/\mathfrak{S}$ is a cyclic Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{S})/\mathfrak{S}$, $N_{\mathfrak{G}}(\mathfrak{S})/\mathfrak{S}$ is solvable and hence $N_{\mathfrak{G}}(\mathfrak{S})$ is solvable. We shall prove that the order of $N_{\mathfrak{G}}(\mathfrak{S})$ is equal to $2^{l+m}(2^m-1)(2^{m+1}-1)$. Remark that Lemma 4.5 is also true for this case. Let $\tau' = \tau^G$ be an element of \mathfrak{S} , where G is an element of \mathfrak{G} . The same argument as in the proof of Lemma 4.6 shows that G is contained in $N_{\mathfrak{G}}(\mathfrak{S})$. Thus every element ($\neq 1$) of \mathfrak{S} is conjugate to τ under $N_{\mathfrak{G}}(\mathfrak{S})$.

Hence the index of $C_{\mathfrak{G}}(\tau)$ in $N_{\mathfrak{G}}(\mathfrak{S})$ is equal to $2^{m+1}-1$.

Let \mathfrak{B} be a normal 2-complement of $\mathfrak{H} \cap N_{\mathfrak{G}}(\mathfrak{R}_1)$. Since $N_{\mathfrak{G}}(\mathfrak{S})$ is solvable, there exists a Hall subgroup \mathfrak{A} of order $(2^m-1)(2^{m+1}-1)$ of $N_{\mathfrak{G}}(\mathfrak{S})$ containing \mathfrak{B} . Since $\mathfrak{S}\mathfrak{B}/\mathfrak{R}_1$ is a complete Frobenius group of degree 2^m , all Sylow subgroups of \mathfrak{B} are cyclic. Let r be the least prime factor of the order of \mathfrak{B} . Let \mathfrak{R} be a Sylow r -subgroup of \mathfrak{B} . Then \mathfrak{R} is cyclic and leaves only the symbol 1 fixed. Hence $N_{\mathfrak{G}}(\mathfrak{R})$ is contained in \mathfrak{H} . Let \mathfrak{R}' be a Sylow 2-subgroup of $C_{\mathfrak{G}}(\mathfrak{R})$. Since \mathfrak{R} is a Sylow 2-subgroup of \mathfrak{H} and $C_{\mathfrak{G}}(\mathfrak{R})$ is a subgroup of \mathfrak{H} , \mathfrak{R}' is conjugate to a subgroup of \mathfrak{R} . Thus it may be assumed that \mathfrak{R}' is a subgroup of \mathfrak{R} . Using Sylow's theorem, we obtain that $N_{\mathfrak{G}}(\mathfrak{R}) = C_{\mathfrak{G}}(\mathfrak{R})(N_{\mathfrak{G}}(\mathfrak{R}) \cap N_{\mathfrak{G}}(\mathfrak{R}')) = C_{\mathfrak{G}}(\mathfrak{R})(N_{\mathfrak{G}}(\mathfrak{R}) \cap \mathfrak{B}\mathfrak{R}')$ since \mathfrak{R}_1 is a subgroup of \mathfrak{R}' . Let CVK' be an element of $N_{\mathfrak{G}}(\mathfrak{R})$ of odd order u , where C , V and K' are elements of $C_{\mathfrak{G}}(\mathfrak{R})$, \mathfrak{B} and \mathfrak{R} , respectively. Then $(CVK')^u = C'(VK')^u$, where C' is an element of $C_G(R)$, and $(VK')^u = C'^{-1}$. Set $s = |(VK')^u|/|K'|$, where $|(VK')^u|$ and $|K'|$ are orders of $(VK')^u$ and K' , respectively. Then s is an odd integer and $(VK')^{us}$ is contained in a Sylow 2-subgroup of $C_{\mathfrak{G}}(\mathfrak{R})$ and hence so is VK' . In particular CVK' is an element of $C_{\mathfrak{G}}(\mathfrak{R})$. Hence we obtain that $N_{\mathfrak{G}}(\mathfrak{R}) \cap \mathfrak{A} = C_{\mathfrak{G}}(\mathfrak{R})(N_{\mathfrak{G}}(\mathfrak{R}) \cap \mathfrak{B}\mathfrak{R}') \cap \mathfrak{A} = C_{\mathfrak{G}}(\mathfrak{R})(N_{\mathfrak{G}}(\mathfrak{R}) \cap \mathfrak{B}) \cap \mathfrak{A} = C_{\mathfrak{G}}(\mathfrak{R}) \cap \mathfrak{A}$. By the splitting theorem of Burnside \mathfrak{A} has the normal r -complement. Continuing in the similar way, it can be shown that \mathfrak{A} has the normal subgroup \mathfrak{B} of order $2^{m+1}-1$, which is a complement of \mathfrak{B} . Every permutation ($\neq 1$) of \mathfrak{B} leaves no symbol of Ω fixed and hence it is not commutative with any permutation ($\neq 1$) of \mathfrak{B} . Let B be a permutation of \mathfrak{B} of a prime order, say q . Then all the permutations are conjugate to either B or B^{-1} under \mathfrak{B} . This implies that \mathfrak{B} is an elementary abelian q -group of order q^s . Then it follows that $2^{m+1}-1 = q^s$. Hence $s=1$ and \mathfrak{B} is cyclic of order q . \mathfrak{B} is also cyclic.

Let the order of $N_{\mathfrak{G}}(\mathfrak{B})$ be equal to $\frac{1}{2}x(q-1)q$. If the order of $C_{\mathfrak{G}}(\mathfrak{B})$ is even, then there exists an involution τ' in $C_{\mathfrak{G}}(\mathfrak{B})$ which is conjugate to τ and such that $C_G(\tau')$ contains \mathfrak{B} . But the orders of $C_{\mathfrak{G}}(\tau)$ and \mathfrak{B} are relatively prime. Hence, since $C_{\mathfrak{G}}(\tau')$ is conjugate to $C_{\mathfrak{G}}(\tau)$, the order of $C_{\mathfrak{G}}(\mathfrak{B})$ is odd. Therefore, since the order of the automorphism group of \mathfrak{B} is equal to $q-1 = 2^{m+1}-2$, the order of $N_{\mathfrak{G}}(\mathfrak{B})$ is not divisible by four.

Using Sylow's theorem we obtain the following congruence;

$$2^{l-1}(q+1)(q+2)/x \equiv 1 \pmod{q}.$$

This implies that $2^{l-1}(q+1)(q+2) = x(yq+1)$, where y is positive since x is less than $2^{l-1}(q+1)(q+2)$. Then we have that $x = zq + 2^l$, where $2^{l-1} \geq z \geq 0$. It can be proved that z must be equal to 0 or 2^{l-1} . If $z=0$, then the order of $N_{\mathfrak{G}}(\mathfrak{B})$ is equal to $2^l q \frac{1}{2}(q-1)$ and hence, since $l > 1$, it is divisible by four. If $z=2^{l-1}$,

then the order of $N_{\mathfrak{G}}(\mathfrak{B})$ is equal to $2^{l-1}(q+2) \frac{1}{2} q(q-1)$. Let Y be a permutation ($\neq 1$) of odd prime order dividing $(q+2) \frac{1}{2} (q-1)$ which is contained in $N_{\mathfrak{G}}(\mathfrak{B})$. Since Y leaves just one symbol of Ω fixed, Y is not contained in $C_{\mathfrak{G}}(\mathfrak{B})$. Hence we obtain the following ;

$$q-1 \geq |N_{\mathfrak{G}}(\mathfrak{B})/C_{\mathfrak{G}}(\mathfrak{B})| > \frac{1}{2} (q+2)(q-1).$$

But this is impossible.

Thus there exists no group satisfying the conditions of the theorem in this case.

5. The case n is even and $N_{\mathfrak{G}}(\mathfrak{R}_1)/\mathfrak{R}_1$ does not contain a regular normal subgroup.

1. Since $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is a complete Frobenius group and hence it contains a regular normal subgroup, \mathfrak{R}_1 is a proper subgroup of \mathfrak{R} .

2. Case $\mathfrak{R}_1 = \langle \tau \rangle$ and $2^l \leq 8$. By inductive hypothesis, if $2^l = 4$, then $\mathfrak{G}_1 = N_{\mathfrak{G}}(\mathfrak{R}_1)/\mathfrak{R}_1$ is isomorphic to either $PSL(2, 5)$ or $SL^*(2, 8)$ and, if $2^l = 8$, then \mathfrak{G}_1 is isomorphic either $PGL(2, 5)$ or $PSL(2, 9)$.

At first assume that $d = 2$. If $2^l = 8$, then $i = 6$ or 10 . Hence $n - i = \beta i(i - 1)$ ($\beta = 1$ or 2) is not divisible by 8 . But $n - i$ must be divisible by the order of \mathfrak{R} . This is a contradiction. If \mathfrak{G}_1 is isomorphic to $PSL(2, 5)$, then $i = 6$ and, since $n - i$ must be divisible by 4 , n is equal to $6(2 \cdot 6 - 1) = 6 \cdot 11$. Let \mathfrak{P}_{11} be a Sylow 11 -subgroup of \mathfrak{G} . It is trivial that, since $g^*(2) = 0$ and the order of $N_{\mathfrak{G}}(\mathfrak{R}_1)$ is equal to $6 \cdot 5 \cdot 4$, the order of $C_{\mathfrak{G}}(\mathfrak{P}_{11})$ is odd. Since the order of $C_{\mathfrak{G}}(\mathfrak{P}_{11})$ and $n - 1$ are relatively prime, the order of $C_{\mathfrak{G}}(\mathfrak{P}_{11})$ is equal to 11 or 33 . The index of $C_{\mathfrak{G}}(\mathfrak{P}_{11})$ in $N_{\mathfrak{G}}(\mathfrak{P}_{11})$ is a factor of 10 . Thus this contradicts the Sylow's theorem.

If \mathfrak{G}_1 is isomorphic to $SL^*(2, 8)$, then $i = 28$. Since every involution of \mathfrak{G}_1 leaves just four symbols of $\mathfrak{R}(\mathfrak{R}_1)$, we obtain that $\alpha(I) \neq 0$. Therefore, since every involution of \mathfrak{G} is conjugate to a permutation with the cyclic structure $(12) \dots$, we have that $g^*(2) = 0$ and hence $n = i(2i - 1)$. Thus the order of \mathfrak{H} is equal to $4 \cdot 3^4 \cdot 19$. Since \mathfrak{R} is cyclic, \mathfrak{H} has a normal 2 -complement Ω of order $3^4 \cdot 19$. Let \mathfrak{P}_{19} be Sylow 19 -subgroup of Ω . By Sylow's theorem \mathfrak{P}_{19} is normal in Ω . \mathfrak{P}_{19} is normal even in \mathfrak{H} . Since the order of the automorphism group of \mathfrak{P}_{19} is equal to 18 , τ must be contained in $C_{\mathfrak{G}}(\mathfrak{P}_{19})$. This is a contradiction.

Next we shall consider the case $d \neq 2$. If $2^l = 4$, then $\langle K, I \rangle$ is dihedral. If \mathfrak{G}_1 is isomorphic to $PSL(2, 5)$, then $i = 6$ and, since $n - i = i\beta(i - 1)$ must be divisible by 4 , $\beta = 2$ or 4 . Therefore $\langle K, I \rangle$ is a Sylow 2 -subgroup of \mathfrak{G} . By [4, Theorem 7.7.3] $C_{\mathfrak{G}}(\tau)$ has a normal 2 -complement and hence $C_{\mathfrak{G}}(\tau)$ is solvable.

Thus $\mathfrak{G}_1 = C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ must be solvable and this is a contradiction. If \mathfrak{G}_1 is isomorphic to $SL^*(2, 8)$, then, since for every involution η of $SL^*(2, 8)$ $\alpha(\eta) = 4$, $\alpha(\mathfrak{R}) = 4$. Hence the order of $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is equal to $4 \cdot 3$. Since I is not contained in $C_{\mathfrak{G}}(\mathfrak{R})$ and $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is a complete Frobenius group, $C_{\mathfrak{G}}(\mathfrak{R})$ is contained in a Sylow 2-subgroup. Thus the order of $N_{\mathfrak{G}}(\mathfrak{R})/C_{\mathfrak{G}}(\mathfrak{R})$ is divisible by 3. This is a contradiction.

If $2^l = 8$, then $i = 6$ or 10 . Since $n - i = \beta i(i - 1)$ must be divisible by 8, β is equal to 4 or 8. If $\langle K, I \rangle$ is dihedral, then $\langle K, I \rangle$ is a Sylow 2-subgroup of \mathfrak{G} . Thus $C_{\mathfrak{G}}(\tau)$ is solvable and also $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ is solvable. Hence $\langle K, I \rangle$ must be semi-dihedral and $d = 4$. Since $g^*(2) = 0$ and \mathfrak{G}_1 is a Zassenhaus group, all involutions are conjugate and a permutation leaving at least three symbols of \mathcal{Q} fixed is an involution. Thus \mathfrak{G} satisfies the conditions in [12]. Hence by [6] and [12] \mathfrak{G} is isomorphic to either $PSU(3, 5^2)$ or one of the groups of Ree type (see [16]). Since a Sylow 2-subgroup of a group of Ree type is elementary abelian of order 8, G is isomorphic to $PSU(3, 5^2)$.

3. Case $\mathfrak{R}_1 = \langle \tau \rangle$ and $2^l > 8$. \mathfrak{G}_1 is isomorphic to one of the groups $PSU(3, 3^2)$, $PSU(3, 5^2)$, $PGL(2, *)$ and $PSL(2, *)$. Then i is not divisible by 8. Since $n - i = \beta i(i - 1)$ is divisible by 2^l , β is divisible by 4. Thus we have that $d > 2$ and hence $\langle K, I \rangle$ is dihedral or semi-dihedral and in particular $\langle K, I \rangle/\langle \tau \rangle$ is dihedral. Therefore \mathfrak{G}_1 is isomorphic to either $PGL(2, *)$ or $PSL(2, *)$ and i is divisible by 2 exactly. Thus we have that $\beta = 2^{l-1}$ or 2^l . Thus $\langle K, I \rangle$ is a Sylow 2-subgroup of \mathfrak{G} . If $\langle K, I \rangle$ is dihedral, then $C_{\mathfrak{G}}(\tau)$ is solvable and hence $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ is solvable. If $\langle K, I \rangle$ is semi-dihedral, then $\beta = 2^{l-1}$ and $g^*(2) = 0$. Again by [6] and [12], G must be isomorphic to either $PSU(3, 5^2)$ or one of the groups of Ree type. This is a contradiction.

Thus there exists no group satisfying the conditions of the theorem in this case.

4. Case $\mathfrak{R}_1 > \langle \tau \rangle$. Since \mathfrak{R}_1 is a proper subgroup of \mathfrak{R} , the order of \mathfrak{R} is greater than 4. At first assume that $d = 2$. By inductive hypothesis i is not divisible by 8. Since $n - i = \beta i(i - 1)$ is divisible by 2^l , $\beta = 2$, $2^l = 8$ and i is divisible by 4. Thus we obtain that \mathfrak{G}_1 is isomorphic to $SL^*(2, 8)$ and $n = 2^2 \cdot 7 \cdot 5 \cdot 11$. If we consider a Sylow 19-subgroup of \mathfrak{G} , likewise in 5.2, we can obtain a contradiction.

Next we assume that $d > 2$. Then $\langle K, I \rangle/\mathfrak{R}_1$ is dihedral. Hence \mathfrak{G}_1 is isomorphic to either $PGL(2, *)$ or $PSL(2, *)$. Since $n - i$ is divisible by 2^l , we have that $\beta = 2^l$ or 2^{l-1} . Therefore $\langle K, I \rangle$ is a Sylow 2-subgroup of \mathfrak{G} . If $\langle K, I \rangle$ is dihedral, then $C_{\mathfrak{G}}(\tau)$ is solvable and hence $C_{\mathfrak{G}}(\tau)/\mathfrak{R}_1$ must be solvable. Thus $\langle K, I \rangle$ is semi-dihedral. Set $\mathfrak{G}_0 = C_{\mathfrak{G}}(\tau)/\langle \tau \rangle (= N_{\mathfrak{G}}(\mathfrak{R}_1)/\langle \tau \rangle)$. Then, since $\langle K, I \rangle/\mathfrak{R}_1$ is a Sylow 2-subgroup of \mathfrak{G}_0 and a dihedral group. Let $\eta = K^{2^{l-2}}\langle \tau \rangle$ be the involution in the center of $\langle K, I \rangle/\langle \tau \rangle$. It can be easily

proved that η is contained in the center of \mathfrak{G}_0 . Thus, by [4, Theorem 7.7.3], \mathfrak{G}_0 has a normal 2-complement and hence \mathfrak{G}_0 is solvable. Hence \mathfrak{G}_1 must be solvable. This is a contradiction.

Thus there exists no group satisfying the conditions of the theorem in this case.

Thus Theorem is proved.

Hokkaido University

References

- [1] W. Feit, On class of doubly transitive permutation groups, *Illinois J. Math.*, 4 (1960), 170-186.
- [2] W. Feit and J. G. Thompson, Solvability of groups of odd order, *Pacific J. Math.*, 13 (1963), 775-1029.
- [3] P. Fong, Some Sylow subgroups of order 32 and a characterization of $U(3, 3)$, *J. Algebra*, 6 (1967), 65-76.
- [4] D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968.
- [5] D. Gorenstein and J. H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups, I, II, III, *J. Algebra*, 2 (1965), 85-151, 218-270, 334-393.
- [6] K. Harada, A characterization of the simple group $U_3(5)$, *Nagoya Math. J.* (to appear).
- [7] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1968.
- [8] N. Ito, On a class of doubly transitive permutation groups, *Illinois J. Math.*, 6 (1962), 341-352.
- [9] N. Ito, On doubly transitive groups of degree n and order $2(n-1)n$, *Nagoya Math. J.*, 27 (1966), 409-417.
- [10] H. Kimura, On doubly transitive permutation groups of degree n and order $4(n-1)n$, *J. Math. Soc. Japan*, 21 (1969), 234-243.
- [11] H. Lüneburg, Charakterisierungen der endlichen desarguesschen projektiven Ebenen, *Math. Z.*, 85 (1964), 419-450.
- [12] R. Ree, Sur une famille de groupes de permutations doublement transitifs, *Canad. J. Math.*, 16 (1964), 797-819.
- [13] W. R. Scott, *Group theory*, Prentice-Hall, Englewood Cliffs, N. J., 1964.
- [14] M. Suzuki, On a class of doubly transitive groups, *Ann. of Math.*, 75 (1962), 105-145.
- [15] M. Suzuki, A characterization of the 3-dimensional projective unitary group over a finite field of odd characteristic, *J. Algebra*, 2 (1965), 1-14.
- [16] H. N. Ward, On Ree's series of simple groups, *Trans. Amer. Math. Soc.*, 121 (1966), 62-89.
- [17] H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.
- [18] H. Zassenhaus, Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen, *Abh. Math. Sem. Univ. Hamburg*, 11 (1936), 17-40.