

ON DOUBLY TRANSITIVE PERMUTATION GROUPS OF DEGREE n AND ORDER $2p(n-1)n$

HIROSHI KIMURA¹⁾

(Received December 11, 1969)

1. Introduction

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 doublytransitive permutation group on Ω of order $2p(n-1)n$ not containing a regular normal subgroup, where p is an odd prime number, and let \mathfrak{R} be the stabilizer of symbols 1 and 2. Then we have the following results:*

(I) *If \mathfrak{R} is dihedral, then \mathfrak{G} is isomorphic to either S_5 or $PSL(2, 11)$ with $n=11$.*

(II) *If \mathfrak{R} is cyclic, then \mathfrak{G} is isomorphic to one of the groups $PGL(2, *)$, $PSL(2, *)$ and the groups of Ree type.*

Here we mean by the groups of Ree type the groups which satisfy the condition of H. Ward ([7], [23]).

Notation:

$\{\dots\}$: the set ...

$\langle \dots \rangle$: the subgroup generated by ...

$N_{\mathfrak{Y}}(\mathfrak{X})$, $C_{\mathfrak{Y}}(\mathfrak{X})$: the normalizer and the centralizer of a subset \mathfrak{X} in a group \mathfrak{Y} , respectively

$Z(\mathfrak{Y})$: center of \mathfrak{Y}

$|\mathfrak{Y}|$: the order of \mathfrak{Y}

$\mathfrak{F}(\mathfrak{U})$: the set of symbols of Ω fixed by a subset \mathfrak{U} of \mathfrak{G}

$\alpha(\mathfrak{U})$: the number of symbols in $\mathfrak{F}(\mathfrak{U})$.

2. Proof of Theorem (I)

1. On the order of \mathfrak{G} . Let \mathfrak{H} be the stabilizer of the symbol 1. Let τ be an involution in \mathfrak{R} and let \mathfrak{R}_1 be a normal subgroup of \mathfrak{R} of order p generated by an element K . Let I be an involution with the cyclic structure

1) This work was supported by The Sakkokai Foundation.

(1, 2)⋯. Then I is contained in $N_{\mathfrak{G}}(\mathfrak{R})$ and hence it may be assumed that τ and I are commutative. We have the following decomposition of \mathfrak{G} :

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

The number of elements of \mathfrak{R} which are transformed into its inverse by I is equal to $p+1$. Let $g(2)$ and $h(2)$ denote the numbers of involutions in \mathfrak{G} and \mathfrak{H} , respectively. Then the following equality is obtained:

$$(2.1) \quad g(2) = h(2) + (p+1)(n-1).$$

(See [12] or [13].)

Let τ fix $i (\geq 2)$ symbols of Ω , say $1, 2, \dots, i$. By a theorem of Witt ([24, Th. 9. 4]), $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ can be considered as a doubly transitive permutation group on $\mathfrak{F}(\tau)$. Since every permutation of $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ distinct from $\langle \tau \rangle$ leaves at most one symbol of $\mathfrak{F}(\tau)$ fixed, $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ is a complete Frobenius group on $\mathfrak{F}(\tau)$. Therefore i is a power of a prime number, say q^m and $|C_{\mathfrak{G}}(\tau) \cap \mathfrak{H}| = 2(i-1)$.

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

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

It follow from (2.2) that $p+1 > h^*(2)$ and $n = i(\beta i - \beta + p)/p$, where $\beta = p+1 - h^*(2)$.

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 the following equality is obtained:

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

Since \mathfrak{G} is doubly transitive on Ω , $g^*(2)$ is a multiple of $n-1$. It follow from (2.3) that $p+1 > g^*(2)/(n-1)$ and $n = i(\beta i - \beta + p)/p$, where $\beta = p+1 - g^*(2)/(n-1)$

REMARK 1. Let β' be the number of involutions with the cyclic structures (1, 2)⋯ each of which is conjugate to τ . It is trivial that the number of involutions which are conjugate to τ and not contained in \mathfrak{H} is equal to $\beta'(n-1)$. Thus we have the following equality:

$$p(n-1)n/i(i-1) = p(n-1)/(i-1) + \beta'(n-1).$$

From (2, 2) and (2, 3) it is trivial that $\beta' = \beta$.

2. The case n is odd. Since n is odd, so is i .

Lemma 2.1. $\beta \neq p \cdot p = q$ or p is a factor of $i-1$.

Proof. If $\beta=p$, then $h^*(2)=1$. By [6, Cor. 1] \mathfrak{G} contains a regular normal subgroup (see [13, p. 235]). Since n is integer, the second part is trivial.

Lemma 2.2. *Assume $h^*(2) \neq 0$. If $\alpha(I)=1$, then $\langle K, I \rangle$ is dihedral and if $\alpha(I)=i$, then $\langle K, I \rangle$ is abelian. Moreover $h^*(2)=p$ and G has just two conjugate classes of involutions.*

Proof. Let J be an involution ($\neq 1$) with the cyclic structure $(1, 2)\dots$. Then IJ is contained in \mathfrak{R} and $J=IK'$, where K' is an element of \mathfrak{R} . Thus the number of involutions with the cyclic structures $(1, 2)\dots$ is equal to $p+1$. At first assume that $\langle I, K \rangle$ is dihedral. Then I, IK, \dots, IK^{p-1} are conjugate. Therefore if $\alpha(I)=i$, then $\beta=p$ by Remark 1, which contradicts Lemma 2.1. Thus $\alpha(I)=1$ and $h^*(2)=p$. Next assume that $\langle I, K \rangle$ is abelian. Then $I\tau, I\tau K, \dots, I\tau K^{p-1}$ are conjugate. If $\alpha(I)=1$, then $\alpha(I\tau)=i$ and $\beta=p$ by Remark 1. Hence $\alpha(I)=i$ and $\beta=1$.

2.1. The case $h^*(2)=0$. Let \mathfrak{S} be a Sylow 2-subgroup of $C_{\mathfrak{G}}(\tau)$ containing I . Then \mathfrak{S} is also a Sylow 2-subgroup of \mathfrak{G} . Since $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ is a complete Frobenius group, $\mathfrak{S}/\langle \tau \rangle$ has just one involution. If \mathfrak{S} has an element of order 4, then, since all involutions are conjugate, there exists an element S of \mathfrak{S} such that $S^2=\tau$. On the other hand $S\langle \tau \rangle$ is an involution of $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ and hence $\langle S \rangle$ and $\langle I, \tau \rangle$ are conjugate. This is impossible. Therefore $\mathfrak{S}=\langle I, \tau \rangle$. By [8] \mathfrak{G} is isomorphic to a subgroup of $PGL(2, r)$ containing $PSL(2, r)$, where $r=4$ or r is odd. By [15] the subgroups of $PGL(2, r)$ containing $PSL(2, r)$ each of which has a doubly transitive permutation representation of odd degree and a Sylow 2-subgroup of order 4 are $PSL(2, 5)$ and $PSL(2, 11)$. Since $|\mathfrak{R}|=2p$, \mathfrak{G} is isomorphic to $PSL(2, 11)$.

2.2. The case $h^*(2)=p$ and $p=q$. Let \mathfrak{P} be a Sylow p -subgroup of $C_{\mathfrak{G}}(\tau)$. \mathfrak{P} is also a Sylow p -subgroup of \mathfrak{G} and elementary abelian. Assume $m>1$. Put $|C_{\mathfrak{G}}(\mathfrak{P})|=2p^m x$. If $x=1$, then $N_{\mathfrak{G}}(\mathfrak{P})=C_{\mathfrak{G}}(\tau)$ since $\langle \tau \rangle$ is normal in $N_{\mathfrak{G}}(\mathfrak{P})$. By Sylow's theorem $[\mathfrak{G}: N_{\mathfrak{G}}(\mathfrak{P})] \equiv 1 \pmod{p}$. This is a contradiction. Thus $x>1$. Let s be a prime factor ($\neq p$) of $|C_{\mathfrak{G}}(\mathfrak{P})|$ and let \mathfrak{S} be a Sylow s -subgroup of $C_{\mathfrak{G}}(\mathfrak{P})$. If s is a factor of $|\mathfrak{H}|$, then \mathfrak{S} is conjugate to a subgroup of \mathfrak{H} and $\alpha(\mathfrak{S}) \geq 1$. Since $\alpha(\mathfrak{P})=0$, $\alpha(\mathfrak{S}) \geq 2$. Therefore $|\mathfrak{S}|=2$ since $|\mathfrak{R}|=2p$. Thus x must be a factor of n and hence p^m-1+p . Let \mathfrak{X} be a normal Hall subgroup of $C_{\mathfrak{G}}(\mathfrak{P})$ of order x . It can be seen that every element ($\neq 1$) of $C_{\mathfrak{G}}(\tau)$ is not commutative with any permutation ($\neq 1$) of \mathfrak{X} (see [12, p. 413]). This implies that $x-1 \geq 2(p^m-1)$, which is a contradiction. Thus $m=1$, $n=2p-1$ and $n-1=2(p-1)$.

Put $i'=\alpha(K)$, By a theorem of Witt ([24, Th. 9.4]) $|N_{\mathfrak{G}}(\mathfrak{R}_1)|=2pi'(i'-1)$ and $|N_{\mathfrak{G}}(\mathfrak{R}_1)|=2p(i'-1)$. Since $n=2p-1$, K has just one p -cycle in its cycle decomposition. Thus $i'=p-1$. Since $i'-1=p-2$ is a factor of $n-1$

$=2(p-1)$, $p=3$. Therefore $n=5$ and $i'=2$. Thus \mathfrak{G} is isomorphic to S_5 .

2.3. The case $h^*(2)=p$ and $p \neq q$. Assume $\alpha(I)=1$. Then $\langle I, K \rangle$ is dihedral. Put $i'=\alpha(\mathfrak{R}_1)$. At first we shall prove that $i'=2=\alpha(K)$. Let j be a symbol of $\mathfrak{F}(\mathfrak{R}_1)$. If $\mathfrak{F}(\tau)$ does not contain j , then τ and $K\tau$ are involutions with the cyclic structures $(j, j^\tau)\cdots$. Since $\beta=1$, by Remark 1. $\tau=K\tau$, which is a contradiction. Thus $\mathfrak{F}(\mathfrak{R}_1)=\mathfrak{F}(\tau)$. Assume i' is odd. Then $\mathfrak{F}(I) \cap \mathfrak{F}(\mathfrak{R}_1)$ has just one symbol k of Ω . I, IK, \dots, IK^{p-2} and IK^{p-1} leave only the symbol k fixed and an involution of $C_{\mathfrak{G}}(I)$ which is conjugate to I under \mathfrak{G} is equal to I since $h^*(2)=p$. Thus by [6] \mathfrak{G} contains a regular normal subgroup. Therefore i' is even and since $N_{\mathfrak{G}}(\mathfrak{R})=N_{\mathfrak{G}}(\mathfrak{R}_1)$ and $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is a complete Frobenius group, i' is a power of two, say $2^{m'}$. Let \mathfrak{R} be a normal subgroup of $N_{\mathfrak{G}}(\mathfrak{R})$ containing \mathfrak{R}_1 such that $\mathfrak{R}/\mathfrak{R}_1$ is a regular normal subgroup of $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}_1$. $\mathfrak{R}/\mathfrak{R}_1$ is an elementary abelian group of order $2^{m'}$. Let R be an element of \mathfrak{R} of order 4. Then R^2 is contained in \mathfrak{R}_1 and is conjugate to τ . But as in § 2.2.1 it may be proved that $C_{\mathfrak{G}}(\tau)$ does not contain an element of order 4. Let \mathfrak{S} be a Sylow 2-subgroup of \mathfrak{R} containing τ . Then \mathfrak{S} is elementary abelian. Thus $C_{\mathfrak{G}}(\tau)$ contains \mathfrak{S} . Since a Sylow 2-subgroup of $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ is cyclic or (generalized) quaternion, $\mathfrak{S}/\langle \tau \rangle$ is of order 2 and hence $m'=1$. Since $C_{\mathfrak{G}}(I\tau)$ contains \mathfrak{R}_1 and $\alpha(I\tau)=i$, $C_{\mathfrak{G}}(\tau)$ contains a subgroup which is conjugate to \mathfrak{R}_1 . Let \mathfrak{B} be a subgroup of $C_{\mathfrak{G}}(\tau)$ which is conjugate to \mathfrak{R}_1 . Since $i-1$ is divisible by p , we may assume that \mathfrak{B} is contained in a subgroup of $C_{\mathfrak{G}}(\tau)$ which is conjugate to $\mathfrak{H} \cap C_{\mathfrak{G}}(\tau)$ under $C_{\mathfrak{G}}(\tau)$. Thus $\mathfrak{F}(\tau) \cap \mathfrak{F}(\mathfrak{B})$ contains a symbol of Ω . On the other hand, since $i'=2$ $\mathfrak{F}(I\tau) \cap \mathfrak{F}(\mathfrak{R}_1)$ contains no symbol of Ω , which is a contradiction.

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

3. The case n is even. Since n is even, so is i , say 2^m .

Lemma 2.3. *If $g^*(2) \neq 0$, then $g^*(2)=n-1$ or $p(n-1)$ and \mathfrak{G} has just two classes of involutions.*

Proof. We may assume $\alpha(I)=0$. If \mathfrak{F} is an involution with the cyclic structure $(1, 2)\cdots$, then IJ is contained in \mathfrak{R} . If $\langle K, I \rangle$ is dihedral, then I, IK, \dots, IK^{p-1} are conjugate and hence $\beta=1$. If $\langle K, I \rangle$ is abelian, then $I\tau, I\tau K, \dots, I\tau K^{p-1}$ are conjugate and hence $\beta=p$. Thus the proof is completed.

Let \mathfrak{S} be a Sylow 2-subgroup of $C_{\mathfrak{G}}(\tau)$. Then $S/\langle \tau \rangle$ is a regular normal subgroup of $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ and elementary abelian. Since $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ is a complete Frobenius group on $\mathfrak{F}(\tau)$, every element ($\neq \tau$) of $\mathfrak{S}/\langle \tau \rangle$ is conjugate to $I\langle \tau \rangle$ under $H \cap C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$. Therefore every element ($\neq 1, \tau$) of \mathfrak{S} is conjugate to I or $I\tau$ under $\mathfrak{H} \cap C_{\mathfrak{G}}(\tau)$. Thus \mathfrak{S} is elementary abelian.

3.1 The case $g^*(2)=0$. Since $g^*(2)=0$ and \mathfrak{S} is a Sylow 2-subgroup of

\mathfrak{G} , all involutions of \mathfrak{S} are conjugate under $N_{\mathfrak{G}}(\mathfrak{S})$. Thus $|N_{\mathfrak{G}}(\mathfrak{S})| = (2^{m+1} - 1) |C_{\mathfrak{G}}(\tau)|$. Since $n = 2^m \{(p+1)(2^m - 1) + p\} / p$ and $n - 1 = (2^m - 1)\{(p+1)2^m + p\} / p$ and $2^m - 1$ is divisible by p , $2^{m+1} - 1$ is a factor of $\{(p+1)(2^m - 1) + p\}\{(p+1)2^m + p\}$. The following equality is obtained:

$$(p - 1)(3p + 1) = x(2^{m+1} - 1).$$

Set $2^m - 1 = rp$. This implies that;

$$\begin{aligned} x &\equiv -1 \pmod{p}; \quad x = yp - 1 \quad \text{and} \quad y > 0; \\ 3p - 2 &= 2ryp - 2r + y; \quad (2ry - 3)p = 2r - y - 2. \end{aligned}$$

If $y > 1$, then $2ry - 3 > 2r - y - 2$. If $y = 1, p = 1$.

This is a contradiction.

Thus there exists no group satisfying the conditions of Theorem, (I) in this case.

3.2. The case $g^*(2) = p(n - 1)$. Assume $\alpha(I) = 0$. From the proof of Lemma 2.3 $\langle K, I \rangle$ is dihedral. Since $\alpha(I) = 0$ and $\mathfrak{F}(K)^I = \mathfrak{F}(K)$, $\alpha(K)$ is even. Since $\beta = 1$, as in 2.3 $\mathfrak{F}(\mathfrak{R}_1) = \mathfrak{F}(K)$. Since $\mathfrak{F}(\tau)$ contains $\mathfrak{F}(K)$ and $\alpha(I) = 0$, $\mathfrak{F}(I\tau) \cap \mathfrak{F}(K)$ is empty. Since \mathfrak{R}_1 is contained in $C_{\mathfrak{G}}(I\tau)$ and $I\tau$ is conjugate to τ , \mathfrak{R}_1 acts on $\mathfrak{F}(I\tau)$ and $i = \alpha(I\tau) \equiv 0 \pmod{p}$, which is a contradiction.

Thus there exists no group satisfying the conditions of Theorem, (I) in this case.

3.3. The case such that $g^*(2) = n - 1$ and $i - 1$ is not divisible by p . Let \mathfrak{B} be a normal 2-complement in $\mathfrak{H} \cap C_{\mathfrak{G}}(\tau)$. Then every Sylow subgroup of \mathfrak{B} is cyclic since $C_{\mathfrak{G}}(\tau) / \langle \tau \rangle$ is a Frobenius group. As in [12, Case C] \mathfrak{G} has a normal subgroup \mathfrak{A} , which is a complement of \mathfrak{B} . Let \mathfrak{H}' be a normal subgroup of H of order $p(i^2 - 1)$. Then $\mathfrak{B} = \mathfrak{A} \cap \mathfrak{H}'$ is a normal subgroup of \mathfrak{H} and τ induces a fixed point free automorphism of \mathfrak{B} . Therefore \mathfrak{B} is abelian. Since \mathfrak{A} is a product of \mathfrak{B} and a Sylow 2-subgroup of \mathfrak{A} , \mathfrak{A} is solvable ([18]). Thus \mathfrak{G} is solvable and hence it contains a regular normal subgroup.

Thus there exists no group satisfying the conditions of Theorem, (I) in this case.

3.4. The case such that $g^*(2) = n - 1$ and $i - 1$ is divisible by p . It is trivial that \mathfrak{S} contains all involutions in $C_{\mathfrak{G}}(\tau)$. Assume $\alpha(I) = 0$. By the proof of Lemma 2.3 $\langle K, I \rangle$ is abelian.

Lemma 2.4. *Let G be an element of \mathfrak{G} . If $\mathfrak{S}^G \cap \mathfrak{S}$ contains an involution which is conjugate to τ , then G is contained in $N_{\mathfrak{G}}(\mathfrak{S})$.*

Proof. Let τ' be an involution of $\mathfrak{S}^G \cap \mathfrak{S}$ which is conjugate to τ . Then

$C_{\mathfrak{G}}(\tau')$ contains \mathfrak{S} and \mathfrak{S}^G . Since \mathfrak{S} is a normal Sylow 2-subgroup of $C_{\mathfrak{G}}(\tau)$, $\mathfrak{S} = \mathfrak{S}^G$.

Lemma 2.5. *Let η and ζ be different involutions. If $\alpha(\eta) = \alpha(\zeta) = 0$, then $\alpha(\eta\zeta) = 0$.*

Proof. See [14, Lemma 4.7]

Corollary 2.6. *A set \mathfrak{S}_1 consisting of all involutions of \mathfrak{S} each of which is not conjugate to τ and the identity element is a characteristic subgroup of \mathfrak{S} of order i .*

Lemma 2.7. *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. Put $\tau' = \tau^G$. Let J be an involution of \mathfrak{S} . Since i is even, $\alpha(\langle \tau, J \rangle) = 0$. Since every involution ($\neq \tau$) of \mathfrak{S} is conjugate to I or $I\tau$ and $\alpha(I\tau) = i$, the number of involutions of \mathfrak{S} each of which is conjugate to τ is equal to i . Since $n = i^2$, for a symbol j of Ω there exists just one involution of \mathfrak{S} which is conjugate to τ and which leaves j fixed. Let k be a symbol of $\mathfrak{S}(\tau')$ and let ζ be an involution of \mathfrak{S} such that k is contained in $\mathfrak{S}(\zeta)$. Then since $\zeta^{\tau'}$ is an element of \mathfrak{S} and k is contained in $\mathfrak{S}(\zeta^{\tau'})$, $\zeta^{\tau'} = \zeta$. Since \mathfrak{S}^G is normal in $C_{\mathfrak{G}}(\tau')$, it contains ζ . Thus $\mathfrak{S} \cap \mathfrak{S}^G$ contains ζ and hence $\mathfrak{S} = \mathfrak{S}^G$ by Lemma 2.4. Finally τ' is an element of \mathfrak{S} .

Lemma 2.8. *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. It can be proved by the same way as in the proof of [14, Lemma 4.10] that $\alpha(\tau\eta) = 0$. Assume that $|\tau\eta|$ is not equal to a power of two. If $|\tau\eta| = p^t$, then $\alpha((\tau\eta)^t) \neq 1$, since $\alpha(\tau\eta) = 0$ and n is not divisible by p . Thus $\langle (\tau\eta)^t \rangle$ is conjugate to K_1 and $\langle (\tau\eta)^t, \eta \rangle$ is dihedral. This is a contradiction. If $|\tau\eta| = p't$ for a prime number $p' (\neq 2, p)$, then $\alpha((\tau\eta)^t) = 1$ and hence $\alpha(\tau\eta) = 1$. Therefore $|\tau\eta|$ is equal to a power of two.

Lemma 2.9. *Let η be an involution which is not conjugate to τ . Then η is contained in $N_{\mathfrak{G}}(\mathfrak{S})$.*

Proof. See [14, Lemma 4.11].

Since \mathfrak{H} is solvable and $i+1$ is relatively prime to $2p(i-1)$, there exists a hall subgroup \mathfrak{B} of \mathfrak{H} of order $i+1$. Since \mathfrak{H} has a normal subgroup of index 2, by the Frattini argument it may be assumed that τ is contained in $N_{\mathfrak{G}}(\mathfrak{B})$ and hence $W^\tau = W^{-1}$ for every element W of \mathfrak{B} .

Lemma 2.10. *Let W be an element ($\neq 1$) of \mathfrak{B} . Then $S_1^W \cap S_1 = 1$.*

Proof. At first we shall prove that $\mathfrak{S}(\tau)^W \cap \mathfrak{S}(\tau) = \{1\}$. Let $a = b^W$ be a symbol ($\neq 1$) of $\mathfrak{S}(\tau)^W \cap \mathfrak{S}(\tau)$, where b is a symbol of $\mathfrak{S}(\tau)$. Then τ^W leaves the symbol a fixed. Let $\tilde{\mathfrak{R}}$ be the stabilizer of the set of symbols 1 and a . Since τ and τ^W are contained in $\tilde{\mathfrak{R}}$, there exists an element \tilde{K} of $\tilde{\mathfrak{R}}$ of order p such that $\tau^W = \tau W^2 = \tau \tilde{K}$. Therefore W is of order p . But $|W|$ is not divisible by p . This is a contradiction. Next let J be an involution of \mathfrak{S}_1 with the cyclic structure $(1, c)\dots$. Then c is contained in $\mathfrak{S}(\tau)$ and J^W has the cyclic structure $(1, c^W)\dots$. Since c^W is not contained in $\mathfrak{S}(\tau)$, J^W is not contained in $C_{\mathfrak{G}}(\tau)$. Thus we have that $\mathfrak{S}_1^W \cap \mathfrak{S}_1 = 1$.

By Lemma 2.10 there exist just $i+1$ subgroups $\mathfrak{S}_1, \dots, \mathfrak{S}_{i+1}$ such that they are conjugate under \mathfrak{B} and $\mathfrak{S}_t \cap \mathfrak{S}_u = 1$ for $t \neq u$. By Lemma 2.9 $\mathfrak{S}_t \mathfrak{S}_u$ is the direct product $\mathfrak{S}_t \times \mathfrak{S}_u$. Thus $\mathfrak{N} = \mathfrak{S}_1 \cup \dots \cup \mathfrak{S}_{i+1}$ is a group by Lemma 2.5 and the equality $g^*(2) = i^2 - 1$. Hence \mathfrak{N} is a regular normal subgroup of \mathfrak{G} .

Thus there exists no group satisfying the conditions of Theorem, (I) in this case.

This completes the proof of Theorem, (I).

3. Proof of Theorem (II)

1. On the order of \mathfrak{G} . Let \mathfrak{H} be the stabilizer of the symbol 1 . \mathfrak{R} is of order $2p$ and it is generated by a permutation K . Let us denote the unique involution K^p in \mathfrak{R} by τ . Let I be an involution with the cyclic structure $(1, 2)\dots$. Then I is contained in $N_{\mathfrak{G}}(\mathfrak{R})$ and we have the following decomposition of \mathfrak{G} :

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

Let d be the number of elements of \mathfrak{R} each of which is transformed into its inverse by I . Thus if $\langle K, I \rangle$ is abelian, then d is equal to two and if $\langle K, I \rangle$ is dihedral, then d is equal to $2p$. Let $g(2)$ and $h(2)$ denote the numbers of involutions in \mathfrak{G} and \mathfrak{H} , respectively. Then the following equality is obtained:

$$(3.1) \quad g(2) = h(2) + d(n-1).$$

(See [12] or [13].)

Let τ keep i ($i \geq 2$) symbols of Ω , say $1, 2, \dots, i$, unchanged. By a theorem of Witt ([26, Th. 9.4]), $C_{\mathfrak{G}}(\tau)$ is doubly transitive on $\mathfrak{S}(\tau)$. Let \mathfrak{R}_1 be the kernel of this permutation representation of $C_{\mathfrak{G}}(\tau)$ on $\mathfrak{S}(\tau)$. Then $\mathfrak{R}_1 = \langle \tau \rangle$ or \mathfrak{R} . Put $\mathfrak{G}_1 = C_{\mathfrak{G}}(\tau) / \mathfrak{R}_1$. Thus if $\mathfrak{R}_1 = \langle \tau \rangle$, then $|\mathfrak{G}_1| = pi(i-1)$ and if $\mathfrak{R}_1 = \mathfrak{R}$, then $|\mathfrak{G}_1| = i(i-1)$.

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 (3.1) the following equality is obtained:

$$(3.2) \quad h^*(2)n + n(n-1)/i(i-1) = (n-1)/(i-1) + h^*(2) + d(n-1).$$

It follows from (3.2) that $d > h^*(2)$ and $n = i(\beta i - \beta + 1)$, where $\beta = d - h^*(2)$.

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 the following equality is obtained:

$$(3.3) \quad g^*(2) + n(n-1)/i(i-1) = (n-1)/(i-1) + d(n-1).$$

Since \mathfrak{G} is doubly transitive on Ω , $g^*(2)$ is multiple on $n-1$. It follows from (3.3) that $d(n-1) > g^*(2)$ and $n = i(\beta i - \beta + 1)$, where $\beta = d - g^*(2)/(n-1)$.

We shall prove the following lemmas.

Lemma 3.1. *Let \mathfrak{G} be as in Theorem, (II). Assume $\langle K, I \rangle$ is dihedral. Then $\beta = p$ or $2p$. If $\beta = p$, then \mathfrak{G} has just two conjugate classes of involutions.*

Proof. Let J be an involution with the cyclic structure $(1, 2)\cdots$. Then IJ is contained in \mathfrak{R} and J is an element of $I\mathfrak{R}$. Since $\langle K, I \rangle$ is dihedral, every involution is conjugate to τ, I or $I\tau$ and the number of involutions with the cyclic structure $(1, 2)\cdots$ which are conjugate to I is equal to p . If $\beta \neq 2p$, then it may be assumed that I is not conjugate to τ and $I\tau$ is conjugate to τ . In this case Remark 1 in §2 is also true. Thus $\beta = p$ and every involution of \mathfrak{G} is conjugate to I or $I\tau$.

Next lemma is trivial since \mathfrak{G} is doubly transitive ([24, Th. 11.5]).

Lemma 3.2. *Let G be as in Theorem (II). Then \mathfrak{G} has no solvable normal subgroup.*

Lemma 3.3. *Let \mathfrak{G} be as in Theorem, (II). Assume $\langle K, I \rangle$ is dihedral. If an element of \mathfrak{G} has a 2-cycle in its cyclic decomposition, then it is an involution.*

Proof. By Lemma 2.1 $\beta = p$ or $2p$. Let $\alpha_2(G)$ denote the number of 2-cycles in the cyclic decomposition of G , is an element of \mathfrak{G} . Then, since \mathfrak{G} is doubly transitive, the following relation is well known (Frobenius, [16, Prop. 14.6]):

$$(3.4) \quad \sum_{G \in \mathfrak{G}} \alpha_2(G) = \frac{1}{2} |\mathfrak{G}|.$$

If n is odd and $\beta = p$, then it may be assumed that $\alpha(I) = 1$ and every involution is conjugate to τ or I . Since the number of involutions with the cyclic structures $(1, 2)\cdots$ which are conjugate to I is equal to p , the number of involutions not contained in \mathfrak{G} which are conjugate to I is equal to $p(n-1)$. Since $h^*(2) = p$, by Lemma 2.1 the number of involutions which is conjugate to I is equal to pn . Thus $|C_{\mathfrak{G}}(I)| = 2(n-1)$. Since $\alpha_2(\tau) = (n-i)/2 = \beta i(i-1)/2$ and $\alpha_2(I)$

$= (n-1)/2$, $[\mathfrak{G} : C_{\mathfrak{G}}(\tau)]\alpha_2(\tau) = [\mathfrak{G} : C_{\mathfrak{G}}(I)]\alpha_2(I) = \beta n(n-1)/2$. If n is odd and $\beta = 2p$, then $[\mathfrak{G} : C_{\mathfrak{G}}(\tau)]\alpha_2(\tau) = pn(n-1)$.

If n is even and $\beta = p$, then it may be assumed that $\alpha(I) = 0$. Since the number of involutions with cyclic structures $(1, 2) \dots$ which are conjugate to I is equal to p , the number of involutions which are conjugate to I is equal to $p(n-1)$. Thus $|C_{\mathfrak{G}}(I)| = 2n$. Since $\alpha_2(I) = n/2$, $[\mathfrak{G} : C_{\mathfrak{G}}(\tau)]\alpha_2(\tau) = [\mathfrak{G} : C_{\mathfrak{G}}(I)]\alpha_2(I) = pn(n-1)/2$. If n is even and $\beta = 2p$, then $[\mathfrak{G} : C_{\mathfrak{G}}(\tau)]\alpha_2(\tau) = pn(n-1)$. This proves the lemma.

Lemma 3.4. *Let \mathfrak{G} be as in Theorem, (II). Assume that $\beta = 2p$. In this case $\langle K, I \rangle$ is dihedral, and a Sylow 2-subgroup of \mathfrak{G} is elementary abelian.*

Proof. Every involution of \mathfrak{G} is conjugate to τ . If S is an element of \mathfrak{G} of order 4, then $\alpha(S) = 0$ or 1 and $\alpha(S^2) = i$. But $\alpha_2(S) = 0$ by lemma 2.3 and hence $\alpha(S^2) = 0$ or 1. This is a contradiction. Thus every 2-element ($\neq 1$) of \mathfrak{G} is of order 2. Hence a Sylow 2-subgroup of \mathfrak{G} is elementary abelian.

2. The case n is odd and \mathfrak{G}_1 contains a regular normal subgroup. Since \mathfrak{G}_1 is doubly transitive on $\mathfrak{S}(\tau)$ and contains a regular normal subgroup, i is a power of a prime number, say q^m . Let \mathfrak{R} be a normal subgroup of $C_{\mathfrak{G}}(\tau)$ containing \mathfrak{R}_1 of order $i|\mathfrak{R}_1|$ such that $\mathfrak{R}/\mathfrak{R}_1$ is a regular normal subgroup of \mathfrak{G}_1 .

2.1. Case $n = i^2$ ($\beta = 1$). By Lemma 3.1 $\langle K, I \rangle$ is abelian and $d = 2$. Therefore $h^*(2) = 1$. By [6, Cor. 1] \mathfrak{G} contains a solvable normal subgroup (see [13, 2.2]). By Lemma 3.2 there exists no group satisfying the conditions of theorem in this case.

2.2. Case $n = i(2i-1)$. By Lemma 3.1 $\langle K, I \rangle$ is abelian. At first we shall prove the following.

Lemma 3.5. *If $\mathfrak{R}_1 = \mathfrak{R}$ and $d = 2$, then $\alpha(\tau) = \alpha(K^2)$, i.e., K has no 2-cycle in its cyclic decomposition.*

Proof. Assume $\alpha(\tau) < \alpha(K^2)$. $\alpha(K^2)$ is odd and $N_{\mathfrak{G}}(\langle K^2 \rangle) / \langle K^2 \rangle$ is a doubly transitive group on $\mathfrak{S}(K^2)$ of order $2\alpha(K^2)(\alpha(K^2)-1)$ by a theorem of Witt ([24, Th. 9. 4]). By [12] $N_{\mathfrak{G}}(\langle K^2 \rangle) / \langle K^2 \rangle$ contains a regular normal subgroup and $\alpha(K^2) = i^2$. Thus $|N_{\mathfrak{G}}(\langle K^2 \rangle)| = 2pi^2(i^2-1)$. Thus n is divisible by pi^2 . This is a contradiction.

2.2-1. Case $\mathfrak{R} = \mathfrak{R}_1$ and $q \neq p$. From Lemma 3.5 $N_{\mathfrak{G}}(\langle K^2 \rangle) = C_{\mathfrak{G}}(\tau)$. Let be \mathfrak{Q} a Sylow q -subgroup of \mathfrak{R} . Then \mathfrak{Q} is elementary abelian of order i since $\mathfrak{R}/\mathfrak{R}_1$ is elementary abelian. Assume that \mathfrak{Q} is not contained in $C_{\mathfrak{G}}(\mathfrak{R})$. Since $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is a Frobenius group, $C_{\mathfrak{G}}(\mathfrak{R})$ contains \mathfrak{R} or is contained in \mathfrak{R} . From the above assumption \mathfrak{R} contains $C_{\mathfrak{G}}(\mathfrak{R})$. Therefore $[N_{\mathfrak{G}}(\mathfrak{R}) : C_{\mathfrak{G}}(\mathfrak{R})]$ is divisible by $i-1$. Since $|\text{Aut}(\mathfrak{R})| = p-1$, $i-1$ is a factor of $p-1$ and hence

$i < p$. On the other hand, $n-i=2i(i-1)$ must be divisible by $2p$. This is impossible and hence we may assume that Ω is contained in $C_{\mathfrak{G}}(\mathfrak{R})$. By the splitting theorem of Burnside Ω is normal in $N_{\mathfrak{G}}(\mathfrak{R})$. Set $|C_{\mathfrak{G}}(\Omega)|=2piy$. As in [12, Case B] we have $y > 1$. Since $n-i=2i(i-1)$ is divisible by $2p$, n is not divisible by p and hence a Sylow p -subgroup of \mathfrak{G} is contained in a subgroup which is conjugate to \mathfrak{H} . If y is divisible by p , then a Sylow p -subgroup of $C_{\mathfrak{G}}(\Omega)$ leaves just one symbol of $\mathfrak{F}(K^2)$ fixed. But every element ($\neq 1$) of Ω leaves no symbol of Ω fixed. This is a contradiction. Thus y is a factor of $2i-1$. Since $N_{\mathfrak{G}}(\mathfrak{R}) \cap C_{\mathfrak{G}}(\Omega) = C_{\mathfrak{G}}(\mathfrak{R}) \cap C_{\mathfrak{G}}(\Omega)$, there exist a normal subgroup \mathfrak{Y} of $C_{\mathfrak{G}}(\Omega)$ of order y . \mathfrak{Y} is even normal in $N_{\mathfrak{G}}(\Omega)$. Since every element ($\neq 1$) of \mathfrak{Y} leaves no symbol of Ω fixed, every element ($\neq 1$) of $\mathfrak{H} \cap N_{\mathfrak{G}}(\mathfrak{R})$ is not commutative with any element ($\neq 1$) of \mathfrak{Y} . This implies $y-1 \geq 2p(i-1)$, which is a contradiction.

2.2-2. Case $\mathfrak{R}=\mathfrak{R}_1$ and $p=q$. Let \mathfrak{P} be a Sylow p -subgroup of $N_{\mathfrak{G}}(\mathfrak{R})$. Then \mathfrak{P} is normal in $N_{\mathfrak{G}}(\mathfrak{R})$. Since $N_{\mathfrak{G}}(\mathfrak{R})/C_{\mathfrak{G}}(\mathfrak{R})$ is isomorphic to a subgroup of $\text{Aut}(\langle K^2 \rangle)$, \mathfrak{P} is contained in $C_{\mathfrak{G}}(\mathfrak{R})$ and K^2 is an element of $Z(\mathfrak{P})$. Remark that $C_{\mathfrak{G}}(\mathfrak{P})$ is contained in $N_{\mathfrak{G}}(\mathfrak{R})$. Since $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is a Frobenius group with the kernel $\mathfrak{R}/\mathfrak{R}$, $C_{\mathfrak{G}}(\mathfrak{P})=Z(\mathfrak{P})\langle \tau \rangle$. This proves $C_{\mathfrak{G}}(\mathfrak{P})=Z(\mathfrak{P})\langle \tau \rangle$ and $\langle \tau \rangle$ is a normal Sylow 2-subgroup of $C_{\mathfrak{G}}(\mathfrak{P})$, and hence $\langle \tau \rangle$ is even normal in $N_{\mathfrak{G}}(\mathfrak{P})$. Therefore $N_{\mathfrak{G}}(\mathfrak{P})=C_{\mathfrak{G}}(\tau)=N_{\mathfrak{G}}(\mathfrak{R})$. Since \mathfrak{P} is a Sylow p -subgroup of \mathfrak{G} , from Sylow's theorem we must have that $(2p^m-1)(2p^m+1) \equiv 1 \pmod{p}$, which is a contradiction.

2.2-3. Case $\mathfrak{R}_1=\langle \tau \rangle$ and $p \neq q$. If $\alpha(K)$ is even, then the number of p -cycles contained in the cyclic decomposition of K is odd. Since I induces a permutation on the set of thoes p -cycles, I leaves at least one p -cycle fixed and hence it must leave at least p symbols of $\mathfrak{H}(\tau)$. This is a contradiction. Hence $\alpha(K)$ is odd. If $\alpha(K)=\alpha(K^2)$, then $n-i=2i(i-1)$ is divisible by p and so is $n-1$. If $\alpha(K) < \alpha(K^2)$, then by [12] $\alpha(K^2)=(\alpha(K))^2$ since $\alpha(K)$ is odd and $N_{\mathfrak{G}}(\langle K^2 \rangle)/\langle K^2 \rangle$ is a doubly transitive permutation group on $\mathfrak{F}(K^2)$. If n is divisible by p , so is $\alpha(K^2)$ since $n-\alpha(K^2)$ is divisible by p . Thus $\alpha(K)$ is divisible by p . On the other hand, since $i-\alpha(K)$ is divisible by p and $p \neq q$, $\alpha(K)$ is not divisible by p . Thus we may assume that n is not divisible by p .

Let Ω be a Sylow q -subgroup of $C_{\mathfrak{G}}(\tau)$ which is normal in $C_{\mathfrak{G}}(\tau)$. Then Ω is a Sylow q -subgroup of \mathfrak{G} . Set $|C_{\mathfrak{G}}(\Omega)|=2q^m y$. If $y=1$, then $N_{\mathfrak{G}}(\Omega)=C_{\mathfrak{G}}(\tau)$ and $[\mathfrak{G}: N_{\mathfrak{G}}(\Omega)]=(2i-1)(2+1) \equiv -1 \pmod{q}$, which contradicts the Sylow's theorem. Thus $y > 1$. Let s be a prime factor ($\neq q$) of $C_{\mathfrak{G}}(\Omega)$ and let \mathfrak{S} be a Sylow s -subgroup of $C_{\mathfrak{G}}(\Omega)$. Assume $\alpha(\mathfrak{S}) \geq 1$. Since every element ($\neq 1$) of Ω fixes no symbol of Ω , we have $\alpha(\mathfrak{S}) \geq i$ and \mathfrak{S} is conjugate to a subgroup of \mathfrak{R} . If $s=2$, then $|\mathfrak{S}|=2$ and if $s=p$, then $|\mathfrak{S}|=p$. Thus y is a factor of pn . Assume that y is divisible by p . Let \mathfrak{P} be a Sylow p -subgroup of $C_{\mathfrak{G}}(\Omega)$.

Since n is not divisible by p , \mathfrak{P} is conjugate to a subgroup of \mathfrak{H} and hence $\alpha(\mathfrak{P}) \geq i$ as above. Thus \mathfrak{P} is conjugate to $\langle K^2 \rangle$. By Frattini argument τ is contained in $N_{\mathfrak{G}}(\mathfrak{P})$. Since $C_{\mathfrak{G}}(\mathfrak{Q})$ contains a normal subgroup of index 2 and $\langle K, I \rangle$ is abelian, $\langle \mathfrak{P}, \tau \rangle$ is abelian. Thus \mathfrak{P} is contained in $C_{\mathfrak{G}}(\tau)$. On the other hand any element ($\neq 1$) of $\mathfrak{P}\langle \tau \rangle / \langle \tau \rangle$ is not commutative with every element of $\mathfrak{Q}\langle \tau \rangle / \langle \tau \rangle$, for if an element ($\neq 1$) of $\mathfrak{P}\langle \tau \rangle / \langle \tau \rangle$ is commutative with every element of $\mathfrak{Q}\langle \tau \rangle / \langle \tau \rangle$, then $\mathfrak{F}(\mathfrak{P}) \supset \mathfrak{F}(\tau)$ and $\mathfrak{R}_1 = \mathfrak{R}$. Therefore y is a factor of $2q^m - 1$.

Let \mathfrak{Y} be a normal subgroup of $C_{\mathfrak{G}}(\mathfrak{Q})$ of order y . \mathfrak{Y} is normal in $N_{\mathfrak{G}}(\mathfrak{Q})$. Let Y be an element ($\neq 1$) of \mathfrak{Y} . Set $\mathfrak{X} = C_{\mathfrak{G}}(Y) \cap C_{\mathfrak{H}}(\tau)$. Then $|\mathfrak{X}|$ is odd and $\alpha(\mathfrak{X}) \geq 2$ since $\alpha(Y) = 0$ and y is prime to $|C_{\mathfrak{G}}(\tau)|$. Since $C_{\mathfrak{H}}(\tau)$ is contained in $N_{\mathfrak{G}}(\mathfrak{Q})$, it acts on \mathfrak{Y} . If $|\mathfrak{X}| = 1$, then $y - 1 \geq 2b(q^m - 1)$. Thus \mathfrak{X} is conjugate to $\langle K^2 \rangle$, $y = 2q^m - 1$ and all elements ($\neq 1$) of \mathfrak{Y} are conjugate under $C_{\mathfrak{G}}(\tau)$. Therefore $2q^m - 1$ must equal to a power of a prime number r ($\neq p$) and \mathfrak{Y} must be an elementary abelian r -group.

Next assume that $|N_{\mathfrak{G}}(\langle K^2 \rangle)|$ is divisible by $2q^m - 1$. Since by a theorem of Witt $|N_{\mathfrak{G}}(\langle K^2 \rangle)| = 2p\alpha(K^2)(\alpha(K^2) - 1)$, $\alpha(K^2)$ is divisible by $2q^m - 1$. Since $\alpha(K)$ is odd, by [13] $\alpha(K^2)$ is equal to a power of a prime number. Thus $\alpha(K^2) = 2q^m - 1$ and $|N_{\mathfrak{G}}(\langle K^2 \rangle)| = 4p(2q^m - 1)(q^m - 1)$. But $|\mathfrak{S}|$ is not divisible by $4(q^m - 1)$. This proves that $C_{\mathfrak{G}}(\mathfrak{Y}) = \mathfrak{Q}\mathfrak{Y}$ and hence $N_{\mathfrak{G}}(\mathfrak{Y}) = N_{\mathfrak{G}}(\mathfrak{Q})$. On the other hand, it is easily seen that $[\mathfrak{G} : N_{\mathfrak{G}}(\mathfrak{Q})] = 2q^m + 1$. Thus $2q^m + 1 \equiv 2 \pmod{r}$, which contradicts the Sylow's theorem.

2.2-4. Case $\mathfrak{R}_1 = \langle \tau \rangle$ and $p = q$. Then, since $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is a complete Frobenius group on $\mathfrak{F}(\mathfrak{R})$ and $i - \alpha(K)$ is divisible by p , $\alpha(\mathfrak{R})$ is equal to a power of p , say $p^{m'}$. If $i'' = \alpha(K^2) > \alpha(K)$, then $\alpha(K^2) = \alpha(K)^2 = p^{2m'}$ by [12].

Let \mathfrak{P}' be a normal p -subgroup of $C_{\mathfrak{G}}(\tau)$ such that $\mathfrak{P}'\langle \tau \rangle / \langle \tau \rangle$ is a regular normal subgroup of $C_{\mathfrak{G}}(\tau) / \langle \tau \rangle$. Set $\mathfrak{P} = \mathfrak{P}'\langle K^2 \rangle$. Then \mathfrak{P} is a Sylow p -subgroup of \mathfrak{G} . Since $N_{\mathfrak{G}}(\mathfrak{R}) = N_{\mathfrak{G}}(\langle K^2 \rangle) \cap C_{\mathfrak{G}}(\tau)$, $N_{\mathfrak{G}}(\mathfrak{P})$ contains $N_{\mathfrak{G}}(\mathfrak{R})$. Set $|C_{\mathfrak{G}}(\mathfrak{P})| = 2y|Z(\mathfrak{P})|$. Let \mathfrak{S} be a Sylow 2-subgroup of $C_{\mathfrak{G}}(\mathfrak{P})$. If $|\mathfrak{S}| > 2$, then $\alpha(\mathfrak{S}) = 1$. Therefore $C_{\mathfrak{G}}(\mathfrak{S})$ is contained in a subgroup which is conjugate to \mathfrak{H} . But \mathfrak{P} is not contained in any subgroup which is conjugate to \mathfrak{H} . Therefore $|\mathfrak{S}| = 2$. Similarly it may be proved that y and $n - 1$ are relatively prime and hence y is a factor of $2i - 1$. If $y = 1$, then $\langle \tau \rangle$ is normal in $C_{\mathfrak{G}}(\mathfrak{P})$ and hence in $N_{\mathfrak{G}}(\mathfrak{P})$. $N_{\mathfrak{G}}(\mathfrak{P})$ is contained in $C_{\mathfrak{G}}(\tau)$. Since $[C_{\mathfrak{G}}(\tau) : N_{\mathfrak{G}}(\mathfrak{P})] \equiv 1 \pmod{p}$,

$$\begin{aligned} [\mathfrak{G} : N_{\mathfrak{G}}(\mathfrak{P})] &= [\mathfrak{G} : C_{\mathfrak{G}}(\tau)][C_{\mathfrak{G}}(\tau) : N_{\mathfrak{G}}(\mathfrak{P})] \\ &= (2p^m - 1)(2p^m + 1)[C_{\mathfrak{G}}(\tau) : N_{\mathfrak{G}}(\mathfrak{P})] \equiv -1 \pmod{p}, \end{aligned}$$

which is a contradiction. Thus $y > 1$. On the other hand, it is trivial that $C_{\mathfrak{G}}(\mathfrak{P})$ is contained in $N_{\mathfrak{G}}(\langle K^2 \rangle)$. $[N_{\mathfrak{G}}(\langle K^2 \rangle) : C_{\mathfrak{G}}(\mathfrak{P})] = 2pi''(i'' - 1)/2y|Z(\mathfrak{P})|$.

Since $i''-1$ is a factor of $n-1$, y is a factor of pi'' and hence y is equal to a power of p . This is a contradiction.

Thus there exists no group satisfying the conditions of Theorem, (II) in the case $n=i(2i-1)$.

2.3. Case $n=i(pi-p+1)$. In this case $\langle K, I \rangle$ is dihedral. At first we shall prove that $\alpha(K)$ is odd. If $\mathfrak{R}_1=\mathfrak{R}$, then $\alpha(\tau)=\alpha(\mathfrak{R})$. Therefore it may be assumed that $\mathfrak{R}_1=\langle \tau \rangle$. Assume that $\alpha(\mathfrak{R})$ is even. Since $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ is a complete Frobenius group, $\alpha(\mathfrak{R})$ is a power of two, say $2^{m'}$. Let \mathfrak{G} be a Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R})$ containing I . Then $\mathfrak{S}\mathfrak{R}/\mathfrak{R}$ is a regular normal subgroup of $N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$ and every element ($\neq 1$) of $\mathfrak{S}\mathfrak{R}/\mathfrak{R}$ is conjugate to $I\mathfrak{R}$ under $\mathfrak{H} \cap N_{\mathfrak{G}}(\mathfrak{R})/\mathfrak{R}$. Thus every element ($\neq 1$,) of \mathfrak{S} can be represented in the form IK' , where V and K' are elements of $\mathfrak{H} \cap N_{\mathfrak{G}}(\mathfrak{R})$ and \mathfrak{R} , respectively. Therefore \mathfrak{S} is elementart abelian. Since $N_{\mathfrak{G}}(\mathfrak{R})/C_{\mathfrak{G}}(\mathfrak{R})$ is cyclic and τ is unique involution in $C_{\mathfrak{G}}(\mathfrak{R})$, $\mathfrak{S}=\langle \tau, I \rangle$ and $m'=1$. Thus $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ is a Zassenhaus group on $\mathfrak{F}(\tau)$. Since $C_{\mathfrak{G}}(\tau)/\langle \tau \rangle$ is not exactly doubly transitive and contains a regular normal subgroup, i is a power of two by [4, Th. 3]. Thus $\alpha(K)$ is odd.

Since $\alpha(K)$ is odd, I leaves a symbol a of $\mathfrak{F}(K)$ fixed. Assume $\alpha(I)=1$. Since IK' is conjugate to I , it leaves only the symbol a fixed, where K' is an element of $\langle K^2 \rangle$. Let G be an element of \mathfrak{G} with cyclic structure $(l, (1, a)\dots$. Then $C_{\mathfrak{G}}(I)$ is contained in \mathfrak{H}^G . Every involution of \mathfrak{H}^G which is not conjugate to τ is of the form IK' , where K' is an element of $\langle K^2 \rangle$. Thus there exists no involution ($\neq 1$) of $C_{\mathfrak{G}}(I)$ which is conjugate to I . By [6, Cor. 1] \mathfrak{G} contains a solvable normal subgroup.

Thus there exists no group satisfying the conditions of Theorem, (II) in this case.

2.4. Case $n=i(2pi-2p+1)$. By Lemma 2.4 a Sylow 2-subgroup of \mathfrak{G} is elementart abelian. By [22] and Lemma 3.2 \mathfrak{G} contains a normal subgroup \mathfrak{F} such that $\mathfrak{G}/\mathfrak{F}$ has odd order and \mathfrak{F} is the direct product of a 2-subgroup \mathfrak{S}' and a finite number of simple group \mathfrak{F}_j , where \mathfrak{F}_j is isomorphic to one of the groups $\text{PSL}(2, r)$ (where $r \equiv 3$ or $5 \pmod{8}$) or r is equal to a power of two), the Janko group of order 175, 560 and the group of Ree type. Since $Z(\mathfrak{F})$ is a normal subgroup of G , $Z(\mathfrak{F})=1$ by Lemma 2.2. By [18, 4.6.3.] \mathfrak{S}' is a characteristic subgroup. Again $\mathfrak{S}'=1$ by Lemma 2.2. Let τ_1 and τ_2 be involutions in \mathfrak{F}_j and $\mathfrak{F}_{j'}$, ($j \neq j'$), respectively. Then it is trivial by [18, 4.6.3.] that $\tau_1\tau_2$ and τ_1 are not conjugate in \mathfrak{G} . Since \mathfrak{G} has just one conjugate class of involutions, \mathfrak{F} is simple.

Assume that $C_{\mathfrak{F}}(\tau)$ is a 2-subgroup or isomorphic to $\langle \tau \rangle \times \text{PSL}(2, r')$, where $r' \equiv 3$ or $5 \pmod{8}$. Let \mathfrak{B} be a normal 2-complement of \mathfrak{R} of order $i|\mathfrak{R}_1|/2$. Then \mathfrak{B} is normal in $C_{\mathfrak{G}}(\tau)$. It is trivial that $C_{\mathfrak{F}}(\tau) \cap \mathfrak{B}=1$.

Therefore $[C_{\mathfrak{G}}(\tau): C_{\mathfrak{F}}(\tau)]$ and hence $[\mathfrak{G}: \mathfrak{F}]$ are divisible by i . On the other hand, since \mathfrak{F} is a normal subgroup of \mathfrak{G} , F is transitive and hence $[\mathfrak{G}: \mathfrak{F}]$ is a factor of $p(n-1)$. Thus $i=p$, $\mathfrak{R}_1=\mathfrak{R}$ and $C_{\mathfrak{G}}(\tau)=N_{\mathfrak{G}}(\mathfrak{R})$. Since $N_{\mathfrak{G}}(\mathfrak{R})C_{\mathfrak{G}}(\mathfrak{R})$ is cyclic and τ is unique involution in $C_{\mathfrak{G}}(\mathfrak{R})$, a Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R})$ is a four group and so is a Sylow 2-subgroup of \mathfrak{G} .

Thus by [8, Th. 1] \mathfrak{G} is isomorphic to a subgroup of $PGL(2, r)$ containing $PSL(2, r)$, where $r \equiv 3$ or $5 \pmod{8}$. By [15, Satz 1] \mathfrak{G} has no doubly transitive permutation of degree n .

Thus there exist no group satisfying the conditions of Theorem, (II) in this case.

3. The case n is odd and \mathfrak{G}_1 does not contain a regular normal subgroup. Since \mathfrak{G}_1 does not contain a regular normal subgroup, $\mathfrak{R}_1=\langle \tau \rangle$. By [2, Th. 1] \mathfrak{G} is isomorphic to one of the simple groups $PSL(2, 2^m)$ and the Suzuki groups $Sz(2^m)$, where $2^m-1=p$. Therefore $\langle I, K \rangle / \langle \tau \rangle$ is dihedral and so is $\langle K, I \rangle$. Since \mathfrak{G}_1 is a Zassenhaus group, $\alpha(K)=2$. By Lemma 2.1 $\beta=p$ or $2p$. By Lemma 2.3 $\alpha(K^2)=2$.

If $\beta=2p$, then every involution is conjugate to τ . Since is unique element ($\neq 1$) of \mathfrak{R} which leaves at least three symbols of Ω fixed, by [17, Th. 8.7] n must be even. This is a contradiction.

3.1. Case $\beta=p$. By a theorem of Witt $N_{\mathfrak{G}}(\langle K^2 \rangle)=\langle I, K \rangle$. Therefore $N_{\mathfrak{G}}(\langle K^2 \rangle)=C_{\mathfrak{G}}(\langle K^2 \rangle)=\mathfrak{R}$. Since $\langle K^2 \rangle$ is a Sylow p -subgroup of \mathfrak{G} , by the splitting theorem of Burnside \mathfrak{G} has the normal p -complement \mathfrak{X} of order $2(n-1)$.

At first assume \mathfrak{G}_1 is isomorphic to $Sz(2^m)$. Then $i=2^{2m}+1$. Since $n-1=2^{3m}(2^{2m}-2^m+1)=2^{3m}\{(2^m+1)^2-3 \cdot 2^m\}$, $n-1$ is divisible by 3 exactly. Let Ω be a Sylow 3-subgroup of \mathfrak{X} . By the Frattini argument it may be assumed that $\langle K^2 \rangle$ is contained in $N_{\mathfrak{G}}(\Omega)$. Since $C_{\mathfrak{G}}(\langle K^2 \rangle)=2p$, K^2 induces a fixed point free automorphism of Ω . This is a contradiction.

Next assume \mathfrak{G}_1 is isomorphic to $PSL(2, 2^m)$. Then $n=2^{3m}+1$ and \mathfrak{X} is a Sylow 2-subgroup of G . By [7, Th. 5.3.5.] there exists a normal subgroup \mathfrak{U} of \mathfrak{X} of order 2^{3m} such that $\mathfrak{X}=\langle \tau \rangle \mathfrak{U}$. Since every involution in \mathfrak{G} which is conjugate to τ is conjugate under \mathfrak{U} , $\mathfrak{U} \tau$ contains no involution which is conjugate to τ . By Thompson's theorem \mathfrak{G} has a normal subgroup \mathfrak{N} of order $p(n-1)n$ such that $\mathfrak{G}=\langle \tau \rangle \mathfrak{N}$. Since \mathfrak{G} is doubly transitive and \mathfrak{U} is transitive on $\Omega-\{1\}$, \mathfrak{N} is a doubly transitive permutation group on Ω . By [2, Th. 1] \mathfrak{N} is isomorphic to either $PSL(2, 2^m)$ or $Sz(2^m)$. This is a contradiction.

4. The case n is even and \mathfrak{G}_1 contains a regular normal subgroup. Since n is even, so is i . \mathfrak{G}_1 is a doubly transitive permutation group on $\mathfrak{X}(\tau)$ containing a regular normal subgroup. In particular i is a power of two, say 2^m .

Let \mathfrak{C} be a Sylow 2-subgroup of $C_{\mathfrak{G}}(\tau)$ of order 2^{m+1} such that $\mathfrak{C}\mathfrak{R}_1/\mathfrak{R}_1$ is

a regular normal subgroup of \mathfrak{G}_1 . All elements ($\neq 1$) of $\mathfrak{S}\mathfrak{R}_1/\mathfrak{R}_1$ are conjugate under $\mathfrak{B}/\mathfrak{R}_1$, where $\mathfrak{B}=\mathfrak{G} \cap C_{\mathfrak{G}}(\tau)$. Thus every element ($\in \mathfrak{R}_1$) of $\mathfrak{S}\mathfrak{R}_1$ can be represented in the form $I^V K'$, where V and K' are elements of \mathfrak{B} and \mathfrak{R}_1 , respectively, since I is contained in $\mathfrak{S}\mathfrak{R}_1$. Therefore every 2-element ($\neq 1$) of $\mathfrak{S}\mathfrak{R}_1$ is of order 2 and hence \mathfrak{S} is elementary abelian.

4.1. Case $\langle K, I \rangle$ is dihedral. If $\mathfrak{R}_1 = \langle \tau \rangle$, then $I^K = IK^2$ is contained in \mathfrak{S} . Since \mathfrak{S} is elementary abelian, $(I)(IK^2) = K^2$ must be of order 2, which is a contradiction. Thus we assume $\mathfrak{R}_1 = \mathfrak{R}$. Then $N_{\mathfrak{G}}(\mathfrak{R}) = C_{\mathfrak{G}}(\tau)$. Since \mathfrak{G}_1 is a Frobenius group and $C_{\mathfrak{G}}(\mathfrak{R})$ does not contain $\mathfrak{S}\mathfrak{R}$, $C_{\mathfrak{G}}(\mathfrak{R})$ is contained in $\mathfrak{S}\mathfrak{R}$. Since τ is unique involution in $C_{\mathfrak{G}}(\mathfrak{R})$, $\mathfrak{S}\mathfrak{R}/C_{\mathfrak{G}}(\mathfrak{R})$ is isomorphic to $\mathfrak{S}/\langle \tau \rangle$ of order 2^m which is elementary abelian. Since $N_{\mathfrak{G}}(\mathfrak{R})/C_{\mathfrak{G}}(\mathfrak{R})$ is cyclic, m must be equal to one. Set $\alpha(K^2) = i'$. Assume $i' > 2$. Then by a theorem of Witt $N_{\mathfrak{G}}(\langle K^2 \rangle)/\langle K^2 \rangle$ is doubly transitive on $\mathfrak{F}(K^2)$ and the stabilizer of 1 and 2 is of order 2. As in §2 we have $i' = i(\beta'i - \beta' + 1)$, where $\beta' = 1$ or 2. Hence $i' = 4$ or 6. On the other hand $n - i' = \beta i(i - 1) - (i' - i)$ is divisible by p and so is $i' - i$ since $\beta = p$ or $2p$, which is a contradiction. Thus $i' = 2$. Thus \mathfrak{G} is a Zassenhaus group. Therefore \mathfrak{G} is isomorphic to either $PGL(2, 2p+1)$ or $PSL(2, 4p+1)$, where $2p+1$ and $4p+1$ are power of prime numbers for $PGL(2, 2p+1)$ and $PSL(2, 4p+1)$, respectively ([4], [11] and [25]).

4.2. Case $n = i^2$. Since $\beta = 1$, by Lemma 2.1 $\langle K, I \rangle$ is abelian and hence \mathfrak{S} is normal in $C_{\mathfrak{G}}(\tau)$. It can be seen that Lemma 4.5, 4.6, Corollary 4.8, Lemma 4.8, 4.10 and 4.11 in [14] are also true in this case (see Lemma 2.8). Therefore we can construct a regular normal subgroup of \mathfrak{G} .

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

4.3. Case $n = i(2i - 1)$. Since $g^*(2) = o$, all involutions are conjugate. Since $\langle K, I \rangle$ is abelian by Lemma 2.1, \mathfrak{S} is normal in $C_{\mathfrak{G}}(\tau)$. \mathfrak{S} is also a Sylow 2-subgroup of \mathfrak{G} . Let τ' be an involution of $\mathfrak{S} \cap \mathfrak{S}^G$, where G is an element of \mathfrak{G} . $C_{\mathfrak{G}}(\tau')$ contains \mathfrak{S} and \mathfrak{S}^G . Therefore $\mathfrak{S} = \mathfrak{S}^G$ and Sylow 2-subgroups are independent. Since all involutions are conjugate under $N_{\mathfrak{G}}(\mathfrak{S})$, $|N_{\mathfrak{G}}(\mathfrak{S})| = 2pi(i - 1)(2i - 1)$. By [3], [21, Th. 2] and Lemma 3.2 \mathfrak{G} contains a normal subgroup \mathfrak{G}' which is isomorphic to $PSL(2, 2^{m+1})$ since Sylow 2-subgroups of the Suzuki groups and the projective unitary groups are not elementary abelian.

Assume that $2^{m+1} - 1$ is not equal to a power of p . Since $N_{\mathfrak{G}}(\mathfrak{S})$ is solvable and $|N_{\mathfrak{G}}(\mathfrak{S}) \cap \mathfrak{G}'| = 2^{m+1}(2^{m+1} - 1)$, there exists a Hall subgroup \mathfrak{A} of $N_{\mathfrak{G}}(\mathfrak{S}) \cap \mathfrak{G}'$ of order $2^{m+1} - 1$. Let \mathfrak{B} be a subgroup of $\mathfrak{G} \cap C_{\mathfrak{G}}(\tau)$ of order $p(2^m - 1)$. By the Frattini argument we may assume that \mathfrak{B} is contained in $N_{\mathfrak{G}}(\mathfrak{A})$. Let A be an element of \mathfrak{A} of a prime order $p' (\neq p)$. Since $C_{\mathfrak{G}}(A)$ leaves the symbol

1 fixed and $\alpha(A)=0$, $\alpha(C_{\mathfrak{B}}(A))\geq 2$ and hence $C_{\mathfrak{B}}(A)$ is conjugate to a subgroup of $\langle K^2 \rangle$. $2^{m+1}-2\geq p(2^m-1)/|C_{\mathfrak{B}}(A)|$. If $|C_{\mathfrak{B}}(A)|=1$, then this relation is impossible. Thus $C_{\mathfrak{B}}(A)$ is conjugate to $\langle K^2 \rangle$, $|C_{\mathfrak{G}}(K^2)|$ is divisible by $|A|$ and all elements ($\neq 1$) of \mathfrak{A} are conjugate to either A or A^{-1} under \mathfrak{B} . This implies that \mathfrak{A} is elementary abelian of order, say p'^j . Since $p'^j=2^{m+1}-1$, $J=1$ and \mathfrak{A} is cyclic of order p' . Therefore it is trivial that $C_{\mathfrak{B}}(\mathfrak{A})$ is normal in \mathfrak{B} . Set $i''=\alpha(K^2)$. Since $\langle K, I \rangle$ is abelian, the number of p -cyclic in the cyclic decomposition of K^2 contained in $\mathfrak{S}(\tau)$ is even. Therefore i'' is even. Since $|N_{\mathfrak{G}}(\langle K^2 \rangle)|=2pi''(i''-1)$ is divisible by $|A|$ and $i''-1$ is a factor of $n-1$, i'' is divisible by p' and it is not equal to a power of a prime number. If $\mathfrak{S}(\tau)$ contains $\mathfrak{S}(K^2)$, then $\mathfrak{S}(K)=\mathfrak{S}(K^2)$ and $N_{\mathfrak{G}}(\mathfrak{R})=N_{\mathfrak{G}}(\langle K^2 \rangle)$. Therefore $C_{\mathfrak{G}}(\tau)$ must be divisible by $p'=2i-1$, which is a contradiction. Thus the kernel of the permutation representation of $N_{\mathfrak{G}}(\langle K^2 \rangle)$ in $\mathfrak{S}(K^2)$ is equal to $\langle K^2 \rangle$. Therefore $N_{\mathfrak{G}}(\langle K^2 \rangle)/\langle K^2 \rangle$ does not contain a regular normal subgroup. By [12] $i''=6$ and $i=2$ or $i''=28$ and $i=4$. Thus i'' must be equal to n , which is a contradiction.

Next assume that $2^{m+1}-1$ is a power of p , i.e., $2^{m+1}-1=p$. Let \mathfrak{B} be a Sylow p -subgroup of $N_{\mathfrak{G}}(\mathfrak{C})$ of order p^2 containing $\langle K^2 \rangle$. Then \mathfrak{B} is abelian. Since $i < p$, $\mathfrak{R}_1=\mathfrak{R}$. Since $|C_{\mathfrak{G}}(\tau)|=|N_{\mathfrak{G}}(\mathfrak{R})|$ is not divisible by p^2 and $N_{\mathfrak{G}}(\langle K^2 \rangle)$ is divisible by p^2 , $\alpha(K) < \alpha(K^2)$. By [12] the degree $\alpha(K^2)$ of a permutation group $N_{\mathfrak{G}}(\langle K^2 \rangle)/\langle K^2 \rangle$ on $\mathfrak{S}(K^2)$ is equal to i^2 , 6 or 28. Since $n-i$ is not divisible by p , $\alpha(K^2) \neq i^2$. If $\alpha(K^2)=6$ and 28, then $i=2$ and 4, respectively. Then n must be equal to $\alpha(K^2)$, which is a contradiction.

Thus there exist no group satisfying the conditions of Theorem in this case.

5. The case n is even and \mathfrak{G}_1 does not contain a regular normal subgroup.

We may assume $\mathfrak{R}_1=\langle \tau \rangle$. By [1] \mathfrak{G}_1 is isomorphic to $\text{PSL}(2, r)$, where r is power of an odd prime number and $r-1=2p$. Hence $\langle K, I \rangle$ is dihedral and $\alpha(K)=2$. By Lemma 3.3 the cyclic decomposition of K has no 2-cyclic and hence τ is unique element of \mathfrak{R} which leaves at least three symbols of Ω fixed. Therefore by [9] and [17] \mathfrak{G} is isomorphic to one of the groups of Ree type. (Remark that the order of the stabilizer of two symbols of Ω is equal to eight in the case \mathfrak{G} is isomorphic to $U_3(5)$.)

This completes the proof of Theorem.

HOKKAIDO UNIVERSITY

References

- [1] H. Bender: *Endliche zweifach transitive Permutationsgruppen deren Involutionen keine Fixpunkte haben*, Math. Z. **104** (1968), 175–204.
- [2] ———: *Doubly transitive groups with no involution fixing two points* (to appear).
- [3] R. Brauer and M. Suzuki: *On finite groups of even order whose 2-Sylow subgroup is a quaternion group*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 1757–1759.
- [4] W. Feit: *On a class of doubly transitive permutation groups*, Illinois J. Math. **4** (1960), 170–186.
- [5] ——— and J.G. Thompson: *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029.
- [6] G. Glauberman: *Central elements in core-free groups*, J. Algebra **4** (1966), 403–420.
- [7] D. Gorenstein: *Finite Groups*, Harper and Row, New York, 1968.
- [8] ——— 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.
- [9] K. Harada: *A characterization of the simple group $U_3(5)$* , Nagoya Math. J. **38** (1970), 27–40.
- [10] B. Huppert: *Endliche Gruppen I*, Springer, Berlin, 1968.
- [11] N. Ito: *On a class of doubly transitive permutation groups*, Illinois J. Math. **6** (1962), 341–352.
- [12] ———: *On doubly transitive groups of degree n and order $2(n-1)n$* , Nagoya Math. J. **27** (1966), 409–417.
- [13] H. Kimura: *On doubly transitive permutation groups of degree n and order $4(n-1)n$* , J. Math. Soc. Japan **21** (1969), 234–243.
- [14] ———: *On some doubly transitive permutation groups of degree n and order $2'(n-1)n$* , J. Math. Soc. Japan **22** (1970), 264–277.
- [15] H. Lüneburg: *Charakterisierungen der endlichen desargusschen projektiven Ebenen*, Math. Z. **85** (1964), 419–450.
- [16] H. Nagao: *Multiply Transitive Groups*, California Institute of Technology, Pasadena, California, 1967.
- [17] R. Ree: *Sur une famille de groupes de permutations doublement transitifs*, Canad. J. Math. **16** (1964), 797–819.
- [18] W.R. Scott: *Group Theory*, Prentice-Hall, Englewood Cliffs, N. J., 1964.
- [19] M. Suzuki: *On a class of doubly transitive groups*, Ann. of Math. **75** (1962), 104–145.
- [20] ———: *On a class of doubly transitive groups II*, Ann. of Math. **79** (1964), 514–589.
- [21] ———: *Finite groups of even order in which Sylow 2-subgroups are independent*, Ann. of Math. **80** (1964), 58–77.
- [22] J.H. Walter: *The characterization of finite groups with abelian Sylow 2-subgroups* (to appear).
- [23] H.N. Ward: *On Ree's series of simple groups*, Trans. Amer. Math. Soc. **121** (1966), 62–89.
- [24] H. Wielandt: *Finite Permutation Groups*, Academic Press, New York, 1964.
- [25] H. Zassenhaus: *Kennzeichnung endlicher lineare Gruppen als Permutationsgruppen*, Abh. Math. Sem. Hansischen Univ. **11** (1936), 17–40.