



HOKKAIDO UNIVERSITY

Title	ON SOME DOUBLY TRANSITIVE GROUPS SUCH THAT THE STABILIZER OF TWO SYMBOLS IS CYCLIC
Author(s)	Kimura, Hiroshi
Citation	Journal of the Faculty of Science Hokkaido University. Ser. 1 Mathematics, 21(3-4), 153-165
Issue Date	1971
Doc URL	https://hdl.handle.net/2115/58104
Type	departmental bulletin paper
File Information	JFS_HU_v21n3_4-153.pdf



ON SOME DOUBLY TRANSITIVE GROUPS SUCH THAT THE STABILIZER OF TWO SYMBOLS IS CYCLIC

By

Hiroshi KIMURA

1. Introduction

Let Ω be the set of symbols $1, 2, \dots, n$. In this paper we shall consider the following situation.

(*) *A group $\mathfrak{G}$ is doubly transitive on Ω and the stabilizer $\mathfrak{R}$ of the symbols 1 and 2 is a cyclic group of even order.*

The purpose of this paper is to prove the following theorem.

Theorem. *Let $\mathfrak{G}$ satisfy (*). If n is odd, then $\mathfrak{G}$ contains a regular normal subgroup.*

Remark. This theorem was proved by N. Ito and the author ([9], [11] and [12]) in the case $\mathfrak{R}$ is a 2-group or of order $2p$, where p is prime. Thus we shall consider the case that $|\mathfrak{R}| = 2^l u$, where u is odd and if $l=1$, u is not prime.

We shall prove the theorem by induction on the degree n .

Our notation is standard.

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

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

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

$O(\mathfrak{Y})$: the largest normal subgroup of $\mathfrak{Y}$ of odd order

$|\mathfrak{Y}|$, $|Y|$: the order of $\mathfrak{Y}$ and an element Y of $\mathfrak{Y}$, respectively

$\mathfrak{F}(\mathfrak{H})$: the set of symbols of A fixed by a subset $\mathfrak{H}$ of a permutation group on A

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

$O^1(\mathfrak{P})$: the subgroup of a p -group $\mathfrak{P}$ generated by the elements x^p with x in $\mathfrak{P}$

2. On the order of $\mathfrak{G}$

1. Let $\mathfrak{H}$ be the stabilizer of the symbol 1. $\mathfrak{R}$ is generated by an element

K and $|K|=2^l u$, where u is odd. Let us denote the unique involution $K^{2^{l-1}}$ by τ and a Sylow r -subgroup of $\mathfrak{R}$ by $\mathfrak{R}_r$. $\mathfrak{R}_r$ is generated by an element K_r . Let I be an involution with the cycle structure $(1, 2)\cdots$. 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 $\mathfrak{R}' = \langle K' \rangle$ be the subgroup of $\mathfrak{R}$ consisting of elements inverted by I . Set $d = |\mathfrak{R}'|$. Let $g(2)$ and $h(2)$ denote the numbers of involutions in $\mathfrak{G}$ and $\mathfrak{H}$, respectively. Then the following equality is obtained:

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

(See [9] or [10]).

Let τ fix i ($i \geq 2$) symbols of Ω , say $1, 2, \dots, i$. By a theorem of Witt [16, Th. 9.4] $C_{\mathfrak{G}}(\tau)$ acts doubly transitively on $\mathfrak{R}(\tau)$. Let $\mathfrak{R}_1 = \langle K_1 \rangle$ be the kernel of this permutation representation of $C_{\mathfrak{G}}(\tau)$. Put $\mathfrak{G}_1 = C_{\mathfrak{G}}(\tau)/\mathfrak{R}_1$ and $|\mathfrak{R}_1| = 2^l u_1$, where u_1 is odd. Then $|\mathfrak{G}_1| = i(i-1)2^{l-1}u/u_1$, $C_{\mathfrak{G}}(\tau) = 2^l ui(i-1)$ and $C_{\mathfrak{H}}(\tau) = 2^l u(i-1)$.

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

$$(2.2) \quad \begin{aligned} h^*(2)n + n(n-1)/i(i-1) \\ = h^*(2) + (n-1)/(i-1) + d(n-1). \end{aligned}$$

It follows from (2.2) 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 $\mathfrak{G}$ which fix no symbol of Ω . Then the following equality is obtained:

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

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

2. We shall prove some lemmas.

Lemma 2.1. *Let $\mathfrak{G}$ satisfy (*). Then $\beta = d$ or $d/2$. If $\beta = d/2$, then $\mathfrak{G}$ has just two conjugate classes of involutions. Moreover β equals to the number of involutions on $\mathfrak{G}$ with the cycle structures $(1, 2)\cdots$ which are conjugate to τ .*

Proof. See [12, Remark 1].

Lemma 2.2. *Let J be an involution in $N_{\mathfrak{G}}(\mathfrak{R}_r)$ satisfying the condition*

$\alpha(\langle J, K_r \rangle) = 1$. Let $\tilde{\mathfrak{K}}$ be the stabilizer of two symbols a and b in $\mathfrak{S}(\mathfrak{R}_r)$ such that $a^J = b$ and let d' be the number of elements in $\tilde{\mathfrak{K}}$ inverted by J . Then $d = d'$.

Proof. As in the above $n = i(\beta'i - \beta' + 1)$. Since $\beta' = d'$ or $d'/2$ by Lemma 2.1, $d = d'$.

Lemma 2.3. *If $\langle K_r, I \rangle$ is dihedral, where $r \neq 2$, then $\mathfrak{S}(X)$ is contained in $\mathfrak{S}(\mathfrak{R}_2)$ for every element $X (\neq 1)$ or $\mathfrak{R}_r$.*

Proof. Assume $\mathfrak{S}(\mathfrak{R}_2)$ does not contain $\mathfrak{S}(X)$. Then there exists an element Y of $\mathfrak{R}_2$ with the cycle structure $(a, b) \dots$, where a and b are symbols in $\mathfrak{S}(X)$. Let J be an involution with the cycle structure $(a, b) \dots$. Then J is contained in $N_{\mathfrak{S}}(\mathfrak{R}_r)$, $\langle YJ, X \rangle$ is conjugate to a subgroup of $\mathfrak{R}$ and hence it is cyclic. Since $\langle X, Y \rangle$ is abelian, so is $\langle J, X \rangle$, which contradicts Lemma 2.2.

Lemma 2.4. *If X is an element $(\neq 1)$ of $\mathfrak{R}_1$, then $\mathfrak{S}(X) = \mathfrak{S}(\tau)$.*

Proof. Assume $\mathfrak{S}(X)$ is greater than $\mathfrak{S}(\tau)$. By a theorem of Witt $N_{\mathfrak{S}}(\langle X \rangle)$ acts doubly transitively on $\mathfrak{S}(X)$. As in the above $|N_{\mathfrak{S}}(\langle X \rangle)| = |K| i(\beta'i - \beta' + 1)(i - 1)(\beta'i + 1)$ and $\alpha(X) = i(\beta'i - \beta' + 1)$, where $\beta' = d$ or $d/2$ by Lemma 2.1. If $\beta = \beta'$, then $\alpha(X) = n$ and $X = 1$. Thus $\beta' = d/2$ and $\beta = d$ by Lemma 2.1. Since $|\mathfrak{G}|/|N_{\mathfrak{S}}(\langle X \rangle)| = (di - d + 1)(di + 1)/(di/2 - d/2 + 1)(di/2 + 1)$ is an integer, $di/2 + 1$ is a factor of $di + 1 = 2(di/2 + 1) - 1$, which is a contradiction.

By this lemma every cycle in the cycle decomposition of $\mathfrak{R}_1$ not contained in $\mathfrak{S}(\tau)$ is $|\mathfrak{R}_1|$ -cycle.

Lemma 2.5. *If $(n, |K_1|) \neq 1$, then it is a factor of i .*

Proof. Let r be a factor of $(n, |K_1|)$ and let X be an element of $\mathfrak{R}_1$ of order r . By Lemma 2.4 $n - i$ is divisible by r and hence r is a factor of i .

Let $\mathfrak{X} (\neq 1)$ be a subgroup of $\mathfrak{R}$. By a theorem of Witt $N_{\mathfrak{S}}(\mathfrak{X})$ has a doubly transitive permutation representation on $\mathfrak{S}(\mathfrak{X})$. Let $\mathfrak{R}_1(\mathfrak{X})$ and $\mathfrak{G}_1(\mathfrak{X})$ be the kernel and the image of this representation, respectively.

Lemma 2.6. *Let $\mathfrak{X}$ be a subgroup of $\mathfrak{R}$ such that $\mathfrak{S}(\mathfrak{X})$ is contained in $\mathfrak{S}(\tau)$. If $\mathfrak{G}_1$ contains a regular normal subgroup, then $\mathfrak{G}_1(\mathfrak{X})$ has a regular normal subgroup and $\alpha(\mathfrak{X})$ is a factor of i .*

Proof. Let $\mathfrak{N}$ be a normal subgroup of $C_{\mathfrak{S}}(\tau)$ containing $\mathfrak{R}_1$ such that $\mathfrak{N}/\mathfrak{R}_1$ be a regular normal subgroup of $\mathfrak{G}_1$. It is clear that $N_{\mathfrak{S}}(\mathfrak{X}) \cap \mathfrak{N}$ is not contained in $\mathfrak{R}$. Thus $(N_{\mathfrak{S}}(\mathfrak{X}) \cap \mathfrak{N})\mathfrak{R}_1(\mathfrak{X})/\mathfrak{R}_1(\mathfrak{X})$ is normal in $\mathfrak{G}_1(\mathfrak{X})$. Hence it is a regular normal subgroup of $\mathfrak{G}_1(\mathfrak{X})$. The second part of the lemma follows from the equality $\alpha(\mathfrak{X}) = |(N_{\mathfrak{S}}(\mathfrak{X}) \cap \mathfrak{N})\mathfrak{R}_1(\mathfrak{X})/\mathfrak{R}_1(\mathfrak{X})|$.

Lemma 2.7. *If n is odd and $\mathfrak{G}_1$ contains a regular normal subgroup, then $\alpha(X)$ is odd for every element $X(\neq 1)$ of $\mathfrak{R}$.*

Proof. By Lemma 2.6 we may assume that $\mathfrak{F}(X)$ is not contained in $\mathfrak{F}(\tau)$. Put $Y=X\tau$. By the same lemma $\alpha(Y)$ is odd and $\mathfrak{G}_1(\langle X \rangle)$ satisfies (*). Therefore $\alpha(X)=\alpha(Y)(\beta'(\alpha(Y)-1)+1)$ for some integer β' and it is odd.

From now on, throughout this paper, we assume that n is odd.

3. The case $\mathfrak{G}_1$ contains a regular normal subgroup

1. Since $\mathfrak{G}_1$ contains a regular normal subgroup, i equals to a power of an odd prime number, say p^m . Let $\mathfrak{R}$ be a normal subgroup of $C_{\mathfrak{G}}(\tau)$ containing $\mathfrak{R}_1$ such that $\mathfrak{R}/\mathfrak{R}_1$ is a regular normal subgroup of $\mathfrak{G}_1$.

Lemma 3.1. *If $d/2$ is odd and $\beta=d/2$, then $\mathfrak{G}$ contains a regular normal subgroup.*

Proof. Assume $\alpha(I)=1$. By Lemma 2.6 $\alpha(\mathfrak{R}')$ is odd. Since $\mathfrak{F}(K')^I = \mathfrak{F}(K')$, the unique symbol j in $\mathfrak{F}(I)$ is contained in $\mathfrak{F}(K')$. $I, IK', \dots, IK'^{I2(\beta-2)}$ and $IK'^{I2(\beta-1)}$ fix only the symbol j and an involution in $C_{\mathfrak{G}}(I)$ which is conjugate to I under $\mathfrak{G}$ equals to I since $h^*(2)=d/2$. Thus by [5] $\mathfrak{G}$ contains a regular normal subgroup.

Lemma 3.2. *$(n, |K|)$ is a power of p .*

Proof. Assume $(n, |K|) \neq 1$. Let r be a prime factor ($\neq p$) of $(n, |K|)$ and let X be an element of order r . Then X is not contained in $\mathfrak{R}_1$ by Lemma 2.5. Set $Y=X\tau$. Then $\mathfrak{F}(Y)$ is a proper subset of $\mathfrak{F}(\tau)$. If $\mathfrak{F}(Y) = \mathfrak{F}(X)$, then r is a factor of $\alpha(Y)$ since $n-\alpha(Y)$ is divisible by r . If $\alpha(Y) < \alpha(X)$. Then $\mathfrak{R}/\mathfrak{R}_1(\langle X \rangle)$ is of even order. As in §2 we have $\alpha(X) = \alpha(Y)(\alpha(Y)\beta' - \beta' + 1)$, where β' is a factor of d . Since $\alpha(Y)$ is odd by Lemma 2.6, so is $\alpha(X)$. By the inductive hypothesis $\mathfrak{G}_1(\langle X \rangle)$ contains a regular normal subgroup and $\alpha(X)$ is a power of $\alpha(Y)$. Since n and $n-\alpha(X)$ are divisible by r , so is $\alpha(Y)$. Thus $r=p$ since $i-\alpha(Y)$ is divisible by r , which is a contradiction. This completes the proof.

Lemma 3.3. *Let $\mathfrak{P}$ be a Sylow p -subgroup of $\mathfrak{R}$. Then $\mathfrak{P}$ is normal in $\mathfrak{R}$.*

Proof. Let $\mathfrak{R}_{1,r}$ be a Sylow r -subgroup ($\neq 1$) of $\mathfrak{R}_1$, where $r \neq p$. Assume that $C_{\mathfrak{G}}(\mathfrak{R}_{1,r})$ does not contain $\mathfrak{R}$. Since $\text{Aut}(\mathfrak{R}_{1,r})$ is cyclic and every element ($\neq 1$) of $\mathfrak{R}/\mathfrak{R}_1$ is conjugate under $N_{\mathfrak{G}}(\mathfrak{R}_1)/\mathfrak{R}_1$, $i=|\mathfrak{R}/\mathfrak{R}_1|=p$ and $i < r$. Since $\langle I, \mathfrak{R} \rangle/\mathfrak{R}_1$ is dihedral, I is contained in $C_{\mathfrak{G}}(\mathfrak{R}_{1,r})$. Thus r is not a factor of β . On the other hand, by Lemma 2.4 r is a factor of $n-i=\beta i(i-1)$ and hence it is a factor of $i-1$. This is a contradiction. Thus $C_{\mathfrak{G}}(\mathfrak{R}_{1,r})$ contains

$\mathfrak{N}$. By the splitting theorem of Burnside $\mathfrak{N}$ has a normal r -complement and hence $\mathfrak{P}$ is normal in $\mathfrak{N}$. This completes the proof.

2. The case $|K_2|=2$. By Lemma 3.1 we may assume that $\beta=d$. Let $\mathfrak{S}$ be a Sylow 2-subgroup of $C_{\mathfrak{Y}}(\tau)$ containing $\langle \tau, I \rangle$. It is also a Sylow 2-subgroup of $\mathfrak{G}$. Since $(\mathfrak{S}\mathfrak{R}_1/\mathfrak{R}_1)(\mathfrak{N}/\mathfrak{R}_1)$ is a Frobenius group, $\mathfrak{S}\mathfrak{R}_1/\mathfrak{R}_1 \cong \mathfrak{S}/\langle \tau \rangle$ is cyclic or a (generalized) quaternion group. If $\mathfrak{S}/\langle \tau \rangle \geq 4$, there exists an element S of $\mathfrak{S}$ of order 4. Since all involutions are conjugate, we may assume $S^2=\tau$. Then SI is contained in $\langle \tau \rangle$, which is a contradiction. Thus $\mathfrak{S}=\langle I, \tau \rangle$. By [7] and [13] $\mathfrak{G}$ contains a regular normal subgroup.

From now on we may assume $|K_2|>2$.

3. The case $\langle K_2, I \rangle$ is dihedral or semi-dihedral. Since d is divisible by 4, by Lemma 2.1 a Sylow 2-subgroup of $C_{\mathfrak{Y}}(\tau)$ is that of $\mathfrak{G}$.

Lemma 3.4. *If the order of a Sylow 2-subgroup $\mathfrak{R}_{1,2}$ of $\mathfrak{R}_1$ is greater than two and $\langle K_2, I \rangle$ is dihedral or semi-dihedral, then it is a Sylow 2-subgroup of $\mathfrak{G}$.*

Proof. Let $\mathfrak{S}'$ be a Sylow 2-subgroup of $C_{\mathfrak{Y}}(\mathfrak{Y})$ containing $\mathfrak{R}_2$ and let $\mathfrak{S}$ be a Sylow 2-subgroup of $N_{\mathfrak{Y}}(\mathfrak{Y})=C_{\mathfrak{Y}}(\tau)$ containing $\mathfrak{S}'$, where $\mathfrak{Y}$ is a subgroup of $\mathfrak{R}_1$ of order 4. Since $\text{Aut}(\mathfrak{Y})=2$ and $N_{\mathfrak{Y}}(\mathfrak{Y})$ contains I , $[\mathfrak{S}:\mathfrak{S}']=2$ and it may be assume that $\mathfrak{S}=\langle \mathfrak{S}', I \rangle$. By Lemma 2.2 $\langle J, \mathfrak{Y} \rangle$ is dihedral for every involution $J(\neq \tau)$ in $N_{\mathfrak{Y}}(\mathfrak{Y})$. Thus τ is the unique involution in $\mathfrak{S}'$ and hence $\mathfrak{S}'$ is cyclic since $Z(\mathfrak{S}')$ contains $\mathfrak{Y}$. $\mathfrak{S}$ is dihedral or semi-dihedral and contained in $N_{\mathfrak{Y}}(\mathfrak{R}_2)$. By Lemma 2.6 $\mathfrak{G}_1(\mathfrak{R}_2)$ contains a regular normal subgroup and $\mathfrak{S}/\mathfrak{R}_2$ is contained in a complement of a Frobenius group. Thus $\mathfrak{S}/\mathfrak{R}_2$ is cyclic or a (generalized) quaternion group and hence $\mathfrak{S}=\langle K_2, I \rangle$.

Lemma 3.5. *Let $\mathfrak{R}_{1,2}$ be as in Lemma 3.4. If $\mathfrak{R}_{1,2}=\langle \tau \rangle$ and $\langle K_2, I \rangle$ is dihedral or semi-dihedral, then $|K_2|=4$ or $\langle K_2, I \rangle$ is a Sylow 2-Subgroup of $\mathfrak{G}$.*

Proof. Assume $|K_2|>4$. Let $\mathfrak{Y}$ be a subgroup of $\mathfrak{R}_2$ of order 4. Let $\mathfrak{S}'$ be a Sylow 2-subgroup of $C_{\mathfrak{Y}}(\mathfrak{Y})$ and let $\mathfrak{S}$ be a Sylow 2-subgroup of $N_{\mathfrak{Y}}(\mathfrak{Y})$ containing $\mathfrak{S}'$. As in the proof of Lemma 3.4, it may be assume that $\mathfrak{S}=\langle \mathfrak{S}', I \rangle$. As in § 2 $i-1=(\alpha(\mathfrak{Y})-1)(\beta'\alpha(\mathfrak{Y})+1)$. Since $\langle IK_1, \mathfrak{Y}\mathfrak{R}_1/\mathfrak{R}_1 \rangle$ is dihedral of order ≥ 4 , by Lemma 2.1 β' is even. Thus $\mathfrak{S}$ is a Sylow 2-subgroup of $C_{\mathfrak{Y}}(\tau)$. As in the proof of Lemma 3.4, we have $\mathfrak{S}=\langle K_2, I \rangle$.

Lemma 3.6. *Let $K_{1,2}$ be as in Lemma 3.5. If $K_{1,2}=\langle \tau \rangle$ and $\langle K_2, I \rangle$ is dihedral of order 8, then there exists no group.*

Proof. Let $\bar{J}$ be an element of $\mathfrak{G}_1$ with the cyclic decomposition $(1, 2)\cdots$

which is conjugate to $K_2\mathfrak{R}_1$. Let J be a 2-element in $\bar{J}$. Then $(\alpha(J, \tau) \geq 2$ and hence $|J| > 2$. On the other hand J is contained in $I\mathfrak{R}$ and every 2-element ($\neq 1$) of $I\mathfrak{R} - \mathfrak{R}$ is an involution. This is a contradiction.

3-1. The case $\langle K_2, I \rangle$ is dihedral. By [7] and [13] $\mathfrak{G}$ contains a regular normal subgroup.

3-2. The case $\langle K_2, I \rangle$ is semi-dihedral. At first assume $|K_{1,2}| \geq 4$. All involutions in $I\mathfrak{R}$ are conjugate. Since $\mathfrak{G}$ is doubly transitive on Ω , all involutions in $\mathfrak{G}$ are conjugate. Since $|K_{1,2}| \geq 4$ and $(IK_2)^2 = \tau$, $\alpha(IK_2) = 1$ and IK_2 is not conjugate to an element of $\mathfrak{R}_{1,2}$. By [17] $\mathfrak{G}$ has a normal subgroup $\mathfrak{G}'$ of index 2 and $\langle K_2^2, I \rangle$ is a Sylow 2-subgroup of $\mathfrak{G}'$. $\mathfrak{G}'$ is also doubly transitive. By [7] and [13] $\mathfrak{G}'$ contains a regular normal subgroup and so is $\mathfrak{G}$.

Next assume $K_{1,2} = \langle \tau \rangle$. A Sylow 2-subgroup of $\mathfrak{G}_1$ is isomorphic to $\langle K_2, I \rangle / \langle \tau \rangle$. Since $\alpha(\langle I, \tau \rangle) = 1$, $\mathfrak{G}_1$ has two classes of involutions. By [6, Theorem 7.7.3] $\mathfrak{G}_1$ has a normal subgroup $\mathfrak{G}_1'$ of index 2, but no normal subgroup of index 4. $\mathfrak{G}_1'$ is doubly transitive on $\mathfrak{F}(\tau)$ and has also two classes of involutions since $\alpha(\langle I, \tau \rangle) = 1$ and $|K_2^2| \geq 4$. Thus $\mathfrak{G}'$ has a normal subgroup $\mathfrak{G}_1''$ of index 2, but no normal subgroup of index 4. $\mathfrak{G}_1''$ must be a normal subgroup of $\mathfrak{G}_1$ of index 4, which is a contradiction. Thus there exists no group in this case.

4. The case $d/2$ is odd. By Lemma 3.1 it may be assume that $\beta = d$, that is, $\mathfrak{G}$ has one conjugate class of involutions.

Lemma 3.7. *If $\mathfrak{R}_2$ is not contained in $\mathfrak{R}_1$, then d and $d-1$ are not divisible by p .*

Proof. Since $\mathfrak{R}/\mathfrak{R}_1$ is even and $\alpha(\langle I, \tau \rangle) = 1$, $\mathfrak{G}_1$ has two conjugate classes of involutions. As in §2 $i = i'(\beta'i' - \beta' + 1)$, where $i' = \alpha(\bar{K}_2)$ for some $\bar{K}_2$ in $\mathfrak{R}_2$. By Lemma 2.1 and 2.3, $\beta' = d/2$. Thus $d/2 - 1$ is divisible by p . This proves the lemma.

4-1. The case $|\mathfrak{R}|$ is not divisible by p . Let $\mathfrak{P}$ be a Sylow p -subgroup of $\mathfrak{R}$. Then it is an elementary abelian Sylow p -subgroup of $\mathfrak{G}$ and normal in $C_{\mathfrak{G}}(\tau)$ by Lemma 3.3. Set $|C_{\mathfrak{G}}(\mathfrak{P})| = 2^i u_1 i y$. If $y = 1$, then $\langle \tau \rangle$ is normal in $C_{\mathfrak{G}}(\mathfrak{P})$ and hence in $N_{\mathfrak{G}}(\mathfrak{P})$. $[\mathfrak{G} : N_{\mathfrak{G}}(\mathfrak{P})] = (di - d + 1)(di + 1) \equiv -d + 1 \pmod{p}$, which contradicts the Sylow's theorem. Thus $y \neq 1$. Let $\mathfrak{S}$ be a Sylow 2-subgroup of $C_{\mathfrak{G}}(\mathfrak{P})$ containing τ . Then $\alpha(\mathfrak{S}) \geq 1$ and hence $\alpha(\mathfrak{S}) \geq i$. Therefore $\mathfrak{S}$ is contained in $\mathfrak{R}_1$. Thus y is odd. Let r be a prime factor of $(y, |\mathfrak{R}|(n-1))$ and let $\mathfrak{R}$ be a Sylow r -subgroup of $C_{\mathfrak{G}}(\mathfrak{P})$. Since by Lemma 3.2 $(r, n) = 1$, $\alpha(R) \geq 1$ hence $\alpha(R) \geq i$. By the Frattini argument it may be

assume that $N_{\mathfrak{G}}(\mathfrak{R})$ contains τ . Since $\alpha(\mathfrak{R})$ is odd by Lemma 2.7 and $\mathfrak{F}(\mathfrak{R})^{\tau} = \mathfrak{F}(\mathfrak{R})$, $\alpha(\langle \mathfrak{R}, \tau \rangle) \geq 1$. Therefore $\mathfrak{F}(\mathfrak{R})$ is contained in $\mathfrak{F}(\tau)$ and $\mathfrak{R}$ is a subgroup of $\mathfrak{R}_1$, which is a contradiction. Thus y is a factor of $di - d + 1$.

At first assume y does not equal to a power of p . Let r be a prime factor ($\neq p$) of y and let $\mathfrak{Y}$ be a Sylow r -subgroup of $C_{\mathfrak{G}}(\mathfrak{P})$. Since there exists a normal subgroup of $C_{\mathfrak{G}}(\mathfrak{P})$ of order iy , by [6, Theorem 6.2.2] and Lemma 3.2 it may be assume that $C_{\mathfrak{G}}(\tau)$ normalizes $\mathfrak{Y}$. Let Y be an element ($\neq 1$) of $\mathfrak{Y}$. Then $\alpha(Y) = 0$. Since $N_{\mathfrak{G}}(\langle X \rangle)$ is contained in $C_{\mathfrak{G}}(\tau)$ for every element $X (\neq 1)$ of $\mathfrak{R}'\mathfrak{R}_2$ by Lemma 2.3, $[C_{\mathfrak{G}}(\tau) : C_{\mathfrak{G}}(\tau) \cap C_{\mathfrak{G}}(Y)]$ is a multiple of $2^{i-1}d(i-1)$. Thus we have the following:

$$d(i-1) \geq y-1 \geq 2^{i-1}d(i-1).$$

From this $l=1$ and $\mathfrak{R}_2 = \langle \tau \rangle$, which is a contradiction.

Next assume y is a power of p . Let $\mathfrak{P}'$ be a Sylow p -subgroup of $C_{\mathfrak{G}}(\mathfrak{P})$. Then $\mathfrak{P}'$ is normal in $C_{\mathfrak{G}}(\mathfrak{P})$ and of order iy . Therefore $\mathfrak{R}'$ acts on $\mathfrak{P}'/\mathfrak{P}$. Since, for every element $X (\neq 1)$ of $\mathfrak{R}'$, $C_{\mathfrak{G}}(X)$ is contained in $C_{\mathfrak{G}}(\tau)$ by Lemma 2.3 and a theorem of Witt, $C_{\mathfrak{G}}(X) = C_{\mathfrak{G}}(X)$. By [6, Theorem 5.3.15] every element ($\neq 1$) of $\mathfrak{R}'$ induces a fixed point free automorphism of $\mathfrak{P}'/\mathfrak{P}$. Therefore $y-1$ is divisible by d . Thus $d = p^{(f-1)m} + p^{(f-2)m} + \dots + p^m + 1$. Since d is even, so is f . Thus d is divisible by $i+1$ and d is not factor of $i-1$ since $d/2$ is odd. This proves the following:

Lemma 3.8. *If $|\mathfrak{R}|$ is not divisible by p , then $\mathfrak{G}$ has a regular normal subgroup or there exists a prime factor of d which is prime to $i-1$ and $d-1$ is divisible by p .*

4-2. The case $|\mathfrak{R}|$ is divisible by p , but $(d, p) = 1$. Let $\mathfrak{P}$ a Sylow p -subgroup of $\mathfrak{R}$. Set $\mathfrak{P}' = \mathfrak{P}\mathfrak{R}_p$. Put $|C_{\mathfrak{G}}(\mathfrak{P}')| = 2^{i_1}u_1'|Z(\mathfrak{P}')|y$, where $2^{i_1}u_1' = |C_{\mathfrak{G}_1}(\mathfrak{P}')/Z(\mathfrak{P}') \cap \mathfrak{R}_p|$. If $y=1$, then $\langle \tau \rangle$ is normal in $C_{\mathfrak{G}}(\mathfrak{P}')$ and $N_{\mathfrak{G}}(\mathfrak{P}')$ is contained in $C_{\mathfrak{G}}(\tau)$. Therefore $\mathfrak{P}'$ is a Sylow p -subgroup of $\mathfrak{G}$ and $[\mathfrak{G} : N_{\mathfrak{G}}(\mathfrak{R}')] = [\mathfrak{G} : C_{\mathfrak{G}}(\tau)][C_{\mathfrak{G}}(\tau) : N_{\mathfrak{G}}(\mathfrak{P}')] \equiv -d+1 \pmod{p}$, which is a contradiction. Thus $y \neq 1$. As in the previous case, y is a factor of $di - d + 1$. Since $N_{\mathfrak{G}}(\mathfrak{R}_p)$ contains $C_{\mathfrak{G}}(\mathfrak{P}')$ and $C_{\mathfrak{G}}(\tau)$ does not contain $C_{\mathfrak{G}}(\mathfrak{P}')$, $\mathfrak{F}(\mathfrak{R}_p)$ is not contained in $\mathfrak{F}(\tau)$ by a theorem of Witt. As in §2, $\alpha(K_p) = \alpha(K_p\tau)(\beta'(\alpha(K_p\tau) - 1) + 1)$. Since $\mathfrak{G}_1(\mathfrak{R}_p)$ has a regular normal subgroup by inductive hypothesis and $\alpha(K_p\tau)$ is a power of p by Lemma 2.6, $\alpha(K_p)$ is a power of p . $[N_{\mathfrak{G}}(\mathfrak{R}_p) : C_{\mathfrak{G}}(\mathfrak{P}')] = |\mathfrak{R}'|\alpha(K_p)(\alpha(K_p) - 1)/2u_1'|Z(\mathfrak{P}')|y$. Thus y is a power p and $d-1$ is divisible by p .

Let $\mathfrak{P}''$ be a Sylow p -subgroup of $C_{\mathfrak{G}}(\mathfrak{P}')$. Since, for every element $X (\neq 1)$ of $\mathfrak{R}'$, $C_{\mathfrak{G}}(X)$ is contained in $C_{\mathfrak{G}}(\tau)$ by Lemma 2.3 and a theorem of

Witt, $C_{\mathfrak{B}'}(X)$ is contained in $Z(\mathfrak{P}')$. By [6, Theorem 5.3.15] every element ($\neq 1$) of $\mathfrak{R}'$ induces a fixed point free automorphism of $\mathfrak{P}''/Z(\mathfrak{P}')$. Therefore $y-1$ is divisible by d . Thus $d=p^{(f-1)m}+p^{(f-2)m}+\cdots+p^m+1$ and $y=p^{fm}$. Since $[N_{\mathfrak{G}}(\mathfrak{R}_p):N_{\mathfrak{G}}(\mathfrak{R}_p)\cap C_{\mathfrak{G}}(\tau)]$ is divisible by y and $|N_{\mathfrak{G}}(\mathfrak{R}_p)\cap C_{\mathfrak{G}}(\tau)|$ is divisible by $|\mathfrak{R}_p|\alpha(K_p\tau)$, $|N_{\mathfrak{G}}(\mathfrak{R}_p)|$ is divisible by $|\mathfrak{R}_p|\alpha(K_p\tau)y$. Thus $d(i-1)+1=\beta'(\alpha(K_p\tau)-1)+1$. Since $d\geq\beta'$, $d=\beta'$ and $i=\alpha(K_p\tau)$. This implies that $\mathfrak{R}_p$ is contained in $\mathfrak{R}_1$, which is a contradiction.

By Lemma 3.7, 3.8 and the case 4-2 we may assume that $d\neq 2$, $\mathfrak{R}_1$ contains $\mathfrak{R}_2$ and there exists a prime factor of d which is prime to $i-1$.

4-3. The case that $d\neq 2$, $\mathfrak{R}_1$ contains $\mathfrak{R}_2$ and there exists a prime factor of d which is prime to $i-1$.

Lemma 3.9. *A factor group of a Sylow 2-subgroup of $C_{\mathfrak{G}}(\tau)$ by $\mathfrak{R}_2$ is cyclic.*

Proof. Let $\mathfrak{S}$ be a Sylow 2-subgroup of $C_{\mathfrak{G}}(\tau)$ containing $\langle I, K_2 \rangle$. Then $\mathfrak{S}=\mathfrak{S}\mathfrak{R}_1/\mathfrak{R}_1$ is cyclic or a (generalized) quaternion group since $\mathfrak{S}\mathfrak{R}_1/\mathfrak{R}_1$ is a Frobenius group. Assume that $\mathfrak{S}$ is a quaternion group. Let $\mathfrak{H}$ be the stabilizer of $\mathfrak{J}(\langle I, K_2 \rangle)$. Let r be a prime factor of d which is prime to $i-1$ and let $\mathfrak{R}'_r=\langle K'_r \rangle$ be a Sylow r -subgroup of $\mathfrak{R}'$. Since $\text{Aut}(\mathfrak{R}'_r)$ is cyclic, $\mathfrak{R}'_r$ is not contained in $\mathfrak{R}_1$. If $\overline{\mathfrak{R}'_r}=\mathfrak{R}'_r\mathfrak{R}_1/\mathfrak{R}_1$ is contained in $0(C_{\mathfrak{S}}(\tau)/\mathfrak{R}_1)$, then by the Frattini argument it may be assumed that $\mathfrak{S}$ normalizes $\overline{\mathfrak{R}'_r}$, which is a contradiction. By [3] $(IK'_{r^{-1}}IK'_r)\mathfrak{R}_1$ is contained in $0(C_{\mathfrak{S}}(\tau)/\mathfrak{R}_1)$. This implies that $K'^2_r\mathfrak{R}_1$ is contained in $0(C_{\mathfrak{S}}(\tau)/\mathfrak{R}_1)$, which is a contradiction. This proves the lemma.

By this lemma $\mathfrak{S}/\mathfrak{R}_2$ is cyclic. Put $\mathfrak{S}/\mathfrak{R}_2=\langle A\mathfrak{R}_2 \rangle$. If $\mathfrak{S}$ is abelian, it is of type $(2^s, 2^t)$. If $s\neq t$, then $\mathfrak{G}$ has a normal 2-complement by the splitting theorem of Burnside. If $s=t$, then $\mathfrak{G}$ has also a solvable normal subgroup by [2, Theorem 1, p. 317].

Next assume that $\mathfrak{S}$ is non-abelian. Put $|\mathfrak{S}/\mathfrak{R}_2|=2^s$. Let $\alpha'_{2^t}(S)$ and $\alpha'_{2^t}(S)$ be the numbers of 2^t -cycles in the cycle decomposition of an element S of $\mathfrak{S}$ contained in $\mathfrak{J}(\tau)$ and $\Omega-\mathfrak{J}(\tau)$, respectively.

Lemma 3.10. *An element B of $\mathfrak{S}$ is contained in $A\langle A^2, K_2 \rangle$ if and only if $\alpha'_{2^s}(B)=(i-1)/2^s$ and $\alpha'_{2^{s+1}}(B)=di(i-1)/2^{s+1}$. $B^{2^s}=\tau$ and $|B|=2^{s+1}\geq 2^t$.*

Proof. Since $n-i=di(i-1)$ is divisible by 2^t , $i-1$ is divisible by 2^{t-1} and $2^s\geq 2^{t-1}$. Since $\text{Aut}(\mathfrak{R}_2)$ is isomorphic to $Z_2\times Z_{2^{l-2}}$, if $l>4$ or $l=4$, then $B^{2^{t-2}}$ or B^2 is contained in $Z(\mathfrak{S})$, respectively. The Burnside's argument implies that the unique involution in $\langle B \rangle$ is conjugate under $N_{\mathfrak{G}}(\mathfrak{S})$. On the other hand, since $[\mathfrak{S}, \mathfrak{S}]$ is contained in $\mathfrak{R}_2$. $\langle \tau \rangle$ is a characteristic subgroup of $\mathfrak{S}$. Therefore $\eta=\tau$ and $|B|\geq 2^{s+1}$. $\alpha'_{2^t}(B)\neq 0$ if and only if $|B|=2^t$.

Since $n-i$ is divisible by 2^{s+1} exactly, $|B|=2^{s+1}$. Since $\alpha'_1(I)=1$ and $\alpha'_2(I)=(i-1)/2$, $\alpha'_{2^s}(B)=(i-1)/2^s$. This completes the proof.

Let $\mathfrak{S}^*$ be the focal subgroup of $\mathfrak{S}$ in $\mathfrak{G}$. Let C be an element of $\mathfrak{S}$ which is conjugate under $\mathfrak{G}$ to an element B of $A\langle A^2, K_2 \rangle$. From Lemma 3.8 C is contained in $A\langle A^2, K_2 \rangle$ and BC^{-1} is contained in $\langle A^2, K_2 \rangle$. By [6, Theorem 7.3.1] $\mathfrak{G}$ has a normal subgroup $\mathfrak{G}'$ of index 2 and $\mathfrak{S}'=\langle A^2, K_2 \rangle$ is a Sylow 2-subgroup of $\mathfrak{G}'$.

Lemma 3.11. $\langle A^2, K_2 \rangle$ is abelian.

Proof. If $|K_2|=4$, then the lemma is trivial. Put $I=A^{2^{t-1}}X$, where X is an element of $\mathfrak{K}_2$. Since $A^{2^{t-1}}$ is contained in $Z(\mathfrak{S})$, $A^{2^t}X^2=\tau X^2=1$. Thus X is of order 4 and X is commutative with A^2 . Therefore I is an element of $Z(\mathfrak{S}')$. If $\langle A^2, K_2 \rangle$ is non-abelian, then $I=\tau$ as in the proof of Lemma 3.10. Thus $\langle A^2, K_2 \rangle$ is abelian.

As in the case that $\mathfrak{S}$ is abelian, $\mathfrak{G}'$ contains a solvable normal subgroup and so is $\mathfrak{G}$. Therefore $\mathfrak{G}$ contains a regular normal subgroup.

4. The case $\mathfrak{G}_1$ does not contain a regular normal subgroup

1. Since $\mathfrak{G}_1$ does not contain a regular normal subgroup, by inductive hypothesis $\mathfrak{K}/\mathfrak{K}_1$ is of odd order. By [1] $\mathfrak{G}_1$ contains a normal subgroup $\mathfrak{G}_1'$ which (as a permutation group) is isomorphic to one of the simple groups $\text{PSL}(2, q)$, $\text{Sz}(q)$ and $\text{PSU}(3, q^2)$, where $q=2^m \geq 4$. Here $\text{PSL}(2, q)$ is the 2-dimensional projective special linear group over $\text{GF}(q)$, the field of q elements; $\text{Sz}(q)$ is the Suzuki group over $\text{GF}(q)$, here m is odd; $\text{PSU}(3, q^2)$ is the 3-dimensional projective special unitary group over $\text{GF}(q^2)$. If $\mathfrak{G}_1'$ is isomorphic to $\text{PSL}(2, q)$, $\text{Sz}(q)$ or $\text{PSU}(3, q^2)$, then i equals to $q+1$, q^2+1 or q^3+1 , respectively.

Lemma 4.1. $N_{\mathfrak{G}}(\mathfrak{K}_1)=C_{\mathfrak{G}}(\mathfrak{K}_1)$ and $\mathfrak{K}' \cap \mathfrak{K}_1=\langle \tau \rangle$.

Proof. Let $\mathfrak{K}_{1,r}$ be a Sylow r -subgroup of $\mathfrak{K}_1$. Then $N_{\mathfrak{G}}(\mathfrak{K}_{1,r})=C_{\mathfrak{G}}(\tau)$ by Lemma 2.4 and a theorem of Witt. The center of a Sylow 2-subgroup of $\mathfrak{G}_1'$ is elementary abelian of order q and its all involutions are conjugate under $\mathfrak{K}/\mathfrak{K}_1$. Since $\text{Aut}(\mathfrak{K}_{1,r})$ is cyclic, $C_{\mathfrak{G}}(\mathfrak{K}_{1,r})$ contains a Sylow 2-subgroup of $C_{\mathfrak{G}}(\tau)$. Since $\mathfrak{G}_1'$ is simple, it is a subgroup of $C_{\mathfrak{G}}(\mathfrak{K}_{1,r})/\mathfrak{K}_1$. Since $\mathfrak{K}$ is cyclic, $C_{\mathfrak{G}}(\mathfrak{K}_{1,r})/\mathfrak{K}_1$ equals to $\mathfrak{G}_1$. From this $N_{\mathfrak{G}}(\mathfrak{K}_{1,r})=C_{\mathfrak{G}}(\mathfrak{K}_{1,r})$ and $\langle \mathfrak{K}_{1,r}, I \rangle$ is abelian. This completes the proof.

By this lemma $d=2(q-1)$.

Lemma 4.2. $0(\mathfrak{K}')$ has a normal complement $\mathfrak{U}$ in $\mathfrak{G}$.

Proof. Let $\mathfrak{K}'_r$ be a Sylow r -subgroup of $\mathfrak{K}'$. Then it is also Sylow

r -subgroup of $\mathfrak{G}$. By Lemma 2.3 $\mathfrak{F}(\mathfrak{R}_r')$ is contained in $\mathfrak{F}(\tau)$ and hence $\mathfrak{F}(\mathfrak{R}_r') = \{1, 2\}$. By the theorem of Witt $N_{\mathfrak{G}}(\mathfrak{R}_r') = \langle I, \mathfrak{R}_r' \rangle$. Thus $N_{\mathfrak{F}}(\mathfrak{R}_r') = C_{\mathfrak{F}}(\mathfrak{R}_r')$ and $\mathfrak{H}$ has a r -complement. This proves the lemma.

Lemma 4.3. $C_{\mathfrak{F}}(\tau)$ has a normal Sylow 2-subgroup.

Proof. Let $\mathfrak{N}$ be a normal subgroup of $C_{\mathfrak{G}}(\tau)$ containing $\mathfrak{R}_1$ such that $\mathfrak{N}/\mathfrak{R}_1 = \mathfrak{G}_1'$. Since $(C_{\mathfrak{N}}(\tau) \cap \mathfrak{H})/\mathfrak{R}_1$ has a normal Sylow 2-subgroup, by Lemma 4.1 and the splitting theorem of Burnside, $C_{\mathfrak{F}}(\tau) \cap \mathfrak{H}$ has a normal Sylow 2-subgroup. This proves the lemma.

2. The case $\mathfrak{G}_1'$ is isomorphic to $\text{PSL}(2, q)$. In this case $\mathfrak{G}_1' = \mathfrak{G}_1$ since $\mathfrak{R}/\mathfrak{R}_1$ contains an element with $(i-2)$ -cycle in its cycle decomposition. By Lemma 4.1 $\mathfrak{R}_1$ is contained in $Z(C_{\mathfrak{G}}(\tau))$. By [15] $C_{\mathfrak{G}}(\tau)$ is isomorphic to $\mathfrak{R}_1 \times \text{PSL}(2, q)$. Therefore a Sylow 2-subgroup of $C_{\mathfrak{G}}(\tau)$ contained in $\mathfrak{H}$ is isomorphic to $\mathfrak{R}_2 \times \mathfrak{S}$, where $\mathfrak{S}$ is isomorphic to a Sylow 2-subgroup of $\text{PSL}(2, q)$ which is elementary abelian of order q .

Assume $\beta = d$, that is, $\mathfrak{G}$ has one class of involutions. Then $\mathfrak{R}_2 \times \mathfrak{S}$ is a Sylow 2-subgroup of $\mathfrak{G}$. Since it is abelian, by Burnside argument all involutions in $\mathfrak{R}_2 \times \mathfrak{S}$ are conjugate under $N_{\mathfrak{G}}(\mathfrak{R}_1 \times \mathfrak{S})$. Thus $[N_{\mathfrak{G}}(\mathfrak{R}_1 \times \mathfrak{S}) : C_{\mathfrak{G}}(\tau) \cap N_{\mathfrak{G}}(\mathfrak{R}_1 \times \mathfrak{S})] = 2q - 1$. Since $\alpha(\mathfrak{R}_1 \times \mathfrak{S}) = 1$, $N_{\mathfrak{G}}(\mathfrak{R}_1 \times \mathfrak{S}) = N_{\mathfrak{F}}(\mathfrak{R}_1 \times \mathfrak{S})$ and by Lemma 4.3 $[N_{\mathfrak{F}}(\mathfrak{R}_1 \times \mathfrak{S}) : C_{\mathfrak{F}}(\tau)] = 2q - 1$ and hence $|N_{\mathfrak{F}}(\mathfrak{R}_1 \times \mathfrak{S})| = |\mathfrak{R}|(i-1)(2q-1)$. But $[\mathfrak{H} : N_{\mathfrak{F}}(\mathfrak{R}_1 \times \mathfrak{S})] = (2(q-1)i+1)/(2q-1)$ is not integer, which is a contradiction.

Next assume $\beta = d/2$. Then $n = q^3 + 1$.

Lemma 4.4. $\mathfrak{R}_2 = \langle \tau \rangle$.

Proof. Assume $|\mathfrak{R}_2| > 2$. $\mathcal{O}^1(Z(\mathfrak{R}_2 \times \mathfrak{S})) = \langle \mathfrak{R}_2^2 \rangle$ is a characteristic subgroup of $\mathfrak{R}_2 \times \mathfrak{S}$. Therefore $\langle \tau \rangle$ is normal in $N_{\mathfrak{G}}(\mathfrak{R}_2 \times \mathfrak{S})$, which is a contradiction.

Let $\mathfrak{I}$ be a Sylow 2-subgroup of $\mathfrak{H}$ containing $\mathfrak{R}_2 \times \mathfrak{S}$. By Lemma 4.4 $\mathfrak{R}_2 \times \mathfrak{S}$ is elementary abelian. By Lemma 4.1, 4.2 and the splitting theorem of Burnside $\mathfrak{I}$ is normal in $\mathfrak{H}$. Since $h^*(2) = q - 1$ and $0(\mathfrak{R}')$ acts fixed-point-freely on $Z(\mathfrak{I})$, it is elementary abelian of order q . If $\tau Z(\mathfrak{I})$ is a normal subset of $\mathfrak{I}$, $q \geq [\mathfrak{I} : C_{\mathfrak{I}}(\tau)] = 2q^3/2q$ since the number of involutions in $\tau Z(\mathfrak{I})$ which are conjugate to τ equals to q , which is a contradiction. Thus $\mathfrak{I}/Z(\mathfrak{I})$ is non-abelian. Let $Z_2(\mathfrak{I})$ is a normal subgroup of $\mathfrak{I}$ containing $Z(\mathfrak{I})$ such that $Z_2(\mathfrak{I}) = Z(\mathfrak{I}/Z(\mathfrak{I}))$. Since $0(\mathfrak{R}')$ is considered as a group of fixed point free automorphisms of $Z(\mathfrak{I}/Z(\mathfrak{I}))$, $Z_2(\mathfrak{I}) \geq q^2$.

Lemma 4.5. $\mathfrak{I}/Z_2(\mathfrak{I})$ is elementary abelian.

Proof. If $\mathfrak{S}/Z_2(\mathfrak{I})$ contains an element of order 4, then $|\mathfrak{I}/Z_2(\mathfrak{I})| \geq 2(q-1) + (q-1) + 1 > 2q$ by [6, Theorem 5.3.15], which is a contradiction. This

proves the lemma.

If $|\mathfrak{I}/Z_2(\mathfrak{I})|=2$, then $\mathfrak{I}=\langle\tau\rangle\mathfrak{B}$, where $\mathfrak{B}=Z_2(\mathfrak{I})$. If $|\mathfrak{I}/Z_2(\mathfrak{I})|>2$, then there exists a subgroup $\mathfrak{B}$ of $\mathfrak{I}$ containing $Z_2(\mathfrak{I})$ such that $\mathfrak{I}=\langle\tau\rangle\mathfrak{B}$. Since every involution in $\mathfrak{H}$ which is conjugate to τ is already conjugate under $\mathfrak{B}$. Thus the focal subgroup of $\mathfrak{I}$ is contained in $\mathfrak{B}$. By [6, Theorem 7.3.1] $\mathfrak{G}$ has a normal subgroup $\mathfrak{G}'$ of index 2. $\mathfrak{G}'$ is doubly transitive on Ω . By [1] $\mathfrak{G}'$ contains a normal subgroup $\mathfrak{G}''$ which is isomorphic to $\text{PSU}(3, q^2)$. τ induces an automorphism η of order 2. Since η is not an inner automorphism, by [15] it may be assumed that $\eta=AB$, where A is the automorphism of $\text{GF}(q^2)$ of order 2 and B is an inner automorphism induced by an element of $N_{\mathfrak{G}''}(0(\mathfrak{R}))$. But such automorphism does not fix every element of $0(\mathfrak{R})$. Since $\mathfrak{R}$ is abelian, this is a contradiction.

3. The case $\mathfrak{G}_1'$ is isomorphic to $\text{Sz}(q)$. Let $\mathfrak{R}$ be as in the proof of Lemma 4.3. As in the above case, $\mathfrak{R}$ is isomorphic to $\mathfrak{R}_1 \times \text{Sz}(q)$. Let $\mathfrak{R}_2 \times \mathfrak{C}$ be a Sylow 2-subgroup of $\mathfrak{R}$ contained in $\mathfrak{H}$. Here $\mathfrak{C}$ is isomorphic to a Sylow 2-subgroup of $\text{Sz}(q)$ and $Z(\mathfrak{C})$ is elementary abelian of order q .

Assume $\beta=d$. Then $\mathfrak{R}_2 \times \mathfrak{C}$ is a Sylow 2-subgroup of $\mathfrak{G}$. The number of involutions of $Z(\mathfrak{R}_2 \times \mathfrak{C})$ equals to $2q-1$. As in the above case, $N_{\mathfrak{H}}(\mathfrak{R}_2 \times \mathfrak{C}) = |\mathfrak{R}|(i-1)(2q-1)$. But $[\mathfrak{H} : N_{\mathfrak{H}}(\mathfrak{R}_2 \times \mathfrak{C})] = (2(q-1)i+1)/(2q-1)$ is not integer, which is a contradiction.

Next assume $\beta=d/2$. Since $n-1=q^3(q^2-q+1)=q^3((q+1)^2-3q)$, $n-1$ is divisible by 3 exactly. Let $\mathfrak{R}$ be a Sylow 3-subgroup of $\mathfrak{H}$ containing $\mathfrak{R}_3$. Then $\mathfrak{R}_3$ is normal in $\mathfrak{R}$. By Lemma 4.2 and [6, Theorem 6.2.2] it may be assumed that $N_{\mathfrak{G}}(\mathfrak{R})$ contains $0(\mathfrak{R}')$. Since $N_{\mathfrak{G}}(0(\mathfrak{R}'))=\langle I, K \rangle$, $0(\mathfrak{R}')$ induces a fixed point free group of automorphisms of $\mathfrak{R}/\mathfrak{R}_3$, which is a contradiction.

4. The case $\mathfrak{G}_1'$ is isomorphic to $\text{PSU}(3, q^2)$.

Lemma 4.6. *For every element $X(\neq 1)$ of $\mathfrak{R}$, $\mathfrak{I}(X)$ is contained in $\mathfrak{I}(\tau)$.*

Proof. Let X be an element of $\mathfrak{R}$ not contained in $\mathfrak{R}'\mathfrak{R}_2$. If $\mathfrak{I}(X)$ is not contained in $\mathfrak{I}(\tau)$, $\mathfrak{G}_1(\langle X \rangle)$ satisfies (*) by Lemma 2.4. Since $\alpha(X\tau)=q+1$, as in §2 $\alpha(X)=(q+1)(\beta'q+1)$, where $\beta'=d$ or $d/2$. Since $\mathfrak{G}_1(\langle X \rangle)$ contains a regular normal subgroup by inductive hypothesis, $\alpha(X)$ equals to a power of a prime number r . If $\beta'=q-1$, then $\alpha(X)=q^3+1$. Therefore $q^3+1=9$ and $q=2$, which is a contradiction. If $\beta=2(q-1)$, then $(q+1, 2q(q-1)+1)=5$. Therefore

$$r=5; q+1=5; \alpha(X)=5^3; i=65; n=65 \cdot 5 \cdot 77$$

By a theorem of Witt $|N_{\mathfrak{G}}(\langle X \rangle)|=|K|5^3(5^3-1)$. Since n is not divisible by 5^3 , $[\mathfrak{G} : N_{\mathfrak{G}}(\langle X \rangle)]$ is not an integer, which is a contradiction. Thus $\mathfrak{I}(X)$ is contained in $\mathfrak{I}(\tau)$. By Lemma 2.3 and 2.4 $\mathfrak{I}(Y)$ is contained in $\mathfrak{R}(\tau)$ for

every element $Y (\neq 1)$ of $\mathfrak{R}'\mathfrak{R}_2$. This completes the proof.

By this lemma $n-i$ is divisible by $|\mathfrak{R}|$.

Lemma 4.7. $0(\mathfrak{R})$ has normal complement $\mathfrak{T}$ in $\mathfrak{G}$.

Proof. By Lemma 4.2 $0(\mathfrak{R}')$ has a normal complement $\mathfrak{U}$ in $\mathfrak{G}$. Since $((q^3+1)(q-1), n-1)=1$, $\mathfrak{R}_r$ is a Sylow r -subgroup, where $r \neq 2$. If $\mathfrak{R}_r$ is a subgroup of $\mathfrak{R}_1$, then $N_{\mathfrak{G}}(\mathfrak{R}_r) = C_{\mathfrak{G}}(\mathfrak{R}_r)$ by Lemma 4.1. If r is a factor of $q+1$, then $|N_{\mathfrak{G}}(\mathfrak{R}_r)| = |\mathfrak{R}|q$ by Lemma 4.6 and a theorem of Witt. Since a Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{R}_r)/\mathfrak{R}_1(\mathfrak{R}_r)$ is elementary abelian, By Lemma 2.2 $C_{\mathfrak{G}}(\mathfrak{R}_r) = N_{\mathfrak{G}}(\mathfrak{R}_r)$. By the splitting theorem of Burnside $\mathfrak{G}$ has a normal r -complement. This proves the lemma.

Let $\mathfrak{R}(q)$ be a subgroup of order $(q^2-1)/e$, where $e=(q+1, 3)$. For every prime factor of $|\mathfrak{T}|$, there exists a Sylow r -subgroup $\mathfrak{P}_r$ such that $N_{\mathfrak{G}}(\mathfrak{P}_r)$ contains $\mathfrak{R}(q)$ by [6, Theorem 6.2.2]. If $r \neq 2$, then $\mathfrak{R}(q)$ is a group of fixed point free automorphisms of $\mathfrak{P}_r$ since $(|C_{\mathfrak{G}}(\tau)|, |\mathfrak{T}|)$ is a power of two. Thus $|\mathfrak{P}_r|-1$ is divisible by $(q^2-1)/e$.

Assume $\beta=d/2$. Then $n-1=q^4(q^3-q^2+1)$. Since $q \neq 2$, q^3-q^2+1 does not equal to a power of a prime number. Therefore there exist at least two Sylow subgroups $\mathfrak{P}_{r_1}$ and $\mathfrak{P}_{r_2}$ with $r_1 \neq r_2$. Thus

$$\begin{aligned} |\mathfrak{P}_{r_1}| |\mathfrak{P}_{r_2}| &\geq (2(q^2-1)/e+1) (4(q^2-1)/e+1) \\ &> q(q^2+1) > q^3-q^2+1. \end{aligned}$$

This is a contradiction.

Next assume $\beta=d$. Then $n-1=q^3(2q^4-2q^3+2q-1)$. $\mathfrak{R}_2$ is of order 4 since $\mathfrak{G}$ has one class of involutions, the exponent of a Sylow 2-subgroup of $\text{PSU}(3, q^2)$ equals to 4 and $\langle K_2, I \rangle$ is abelian.

Assume $2q^4-2q^3+2q-1=r^m$ for a prime number r . Since r^m-1 does not divisible by 4, $|N_{\mathfrak{G}}(\mathfrak{P}_r)|=2q^3$ or $4q^3$. $r=2qx-1$ for some integer x .

4-1. The case $[\mathfrak{T} : N_{\mathfrak{G}}(\mathfrak{P}_r)] = 2q^3 \equiv 1 \pmod{r}$. Since $2q^4-2q^3+2q-1 = (2q^3-1)(q-1) + 3q-2$, $(3q-2, 2q^3-1)$ divisible by r and $r \neq 3$. Thus $r=11$ and $q=2$, which is a contradiction.

4-2. The case $[\mathfrak{T} : N_{\mathfrak{G}}(\mathfrak{P}_r)] = 4q^3 \equiv 1 \pmod{r}$. Since $2r^m = (4q^3-1)(q-1) + 5q-3$, r is a factor of $(4q^3-1, 5q-3)$. Thus $r=17$ and $q=1$, which is a contradiction.

Thus $n-1$ is divisible by different two prime numbers r_1 and r_2 . $n-1 = q^3 r_1^m r_2^{m'} t$, where $r_1^m < r_2^{m'}$ and t is relatively prime to r_1 and r_2 . If $r_1^m - 1 \geq 4(q^2-1)/3$ or $r_2^{m'} - 1 \geq 10(q^2-1)/3$, then $r_1^m r_2^{m'} > 2q^4 - 2q^3 + 2q - 1$. Therefore $r_1^m - 1 = 2(q^2-1)/3$ and $r_2^{m'} - 1 = 4(q^2-1)/3$, $8(q^2-1)/3$ or $2(q^2-1)$. Since $r_1^m r_2^{m'} \neq 2q^4 - 2q^3 + 2q - 1$, $t \neq 1$ and put $t = r_3^{m''} t'$, where $(t', r_3) = 1$ and

r_3 is prime. $r_3^{m''}-1 > 4(q^2-1)$. Thus $r_2^{m'}r_3^{m''} > 2q^4-2q^3+2q-1$. This is a contradiction.

Thus Theorem is proved.

References

- [1] H. BENDER: Doubly transitive groups with no involution fixing two points (to appear).
- [2] R. BRAUER: Some applications of the theory of blocks of characters of finite groups II, *J. Alg.*, 1 (1964), 307-334.
- [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 and J. G. THOMPSON: Solvability of groups of odd order, *Pac. J. Math.*, 13 (1963), 775-1029.
- [5] G. GLAUBERMAN: Central elements in core-free groups, *J. Alg.*, 4 (1966), 403-420.
- [6] D. GORENSTEIN: *Finite groups*, Harper and Row, New York, 1968.
- [7] D. GORENSTEIN and J. H. WALTER: The characterization of finite groups with dihedral Sylow 2-subgroups, I, II, III, *J. Alg.*, 2 (1965), 85-151, 218-270, 334-393.
- [8] B. HUPPERT: *Endliche Gruppen I*, Springer, Berlin, 1968.
- [9] N. ITO: On doubly transitive groups of degree n and order $2(n-1)n$, *Nagoya Math. J.*, 27 (1966), 401-417.
- [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. KIMURA: On some doubly transitive permutation groups of degree n and order $2^2(n-1)n$, *J. Math. Soc. Japan*, 22 (1970), 263-277.
- [12] H. KIMURA: On doubly transitive permutation groups of degree n and order $2p(n-1)n$, *Osaka J. Math.*, 7 (1970), 275-290.
- [13] H. LÜNEBURG: Charakterisierungen der endlichen desarguesschen projektiven Ebenen, *Math. Zeit.*, 85 (1964), 419-450.
- [14] M. SUZUKI: Two characteristic properties of (ZT)-groups, *Osaka Math. J.*, 15 (1963), 143-150.
- [15] R. STEINBERG: Automorphisms of finite linear groups, *Can. J. Math.*, 12 (1960), 606-615.
- [16] H. WIELANDT: *Finite permutation groups*, Academic Press, New York, 1964.
- [17] W. J. WONG: On finite groups whose 2-Sylow subgroups have cyclic subgroups of index 2, *J. Austral. Math. Soc.*, 4 (1964), 90-112.

Department of Mathematics,
Hokkaido University

(Received June 11, 1970)