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 $1, 2, \cdots, n$. In this paper we shall consider the following situation.

(*) *A group* $\mathfrak{G}$ *is doubly transitive on* Ω *and the stabilizer* $\mathfrak{K}$ *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 $\mathfrak{K}$ is a 2-group or of order $2p$, where p is prime. Thus we shall consider the case that $|\mathfrak{K}|=2^l u$, 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.

$\langle\cdots\rangle$: the subgroup generated by$\cdots$

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

$Z(\mathfrak{Y})$: 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

$\mathfrak{J}(\mathfrak{U})$: the set of symbols of Λ fixed by a subset $\mathfrak{U}$ of a permutation group on Λ

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

$\mho^1(\mathfrak{P})$: 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. $\mathfrak{K}$ 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 $\mathfrak{K}$ by $\mathfrak{K}_r$. $\mathfrak{K}_r$ is generated by an element K_r. Let I be an involution with the cycle structure $(1, 2)\cdots$. Then I is contained in $N_{\mathfrak{G}}(\mathfrak{K})$ and we have the following decomposition of $\mathfrak{G}$:

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

Let $\mathfrak{K}'=\langle K'\rangle$ be the subgroup of $\mathfrak{K}$ consisting of elements inverted by I. Set $d=|\mathfrak{K}'|$. Let $g(2)$ and $h(2)$ denote the numbers of involutions in $\mathfrak{G}$ and $\mathfrak{H}$, respectively. Then the following equality is obtained:

$$g(2)=h(2)+d(n-1)\,. \tag{2.1}$$

(See [9] or [10]).

Let τ fix i $(i\geqq 2)$ symbols of Ω, say $1,2,\cdots,i$. By a theorem of Witt [16, Th. 9.4] $C_{\mathfrak{G}}(\tau)$ acts doubly transitively on $\mathfrak{I}(\tau)$. Let $\mathfrak{K}_1=\langle K_1\rangle$ be the kernel of this permutation representation of $C_{\mathfrak{G}}(\tau)$. Put $\mathfrak{G}_1=C_{\mathfrak{G}}(\tau)/\mathfrak{K}_1$ and $|\mathfrak{K}_1|=2^{l_1}u_1$, where u_1 is odd. Then $|\mathfrak{G}_1|=i(i-1)2^{l-l_1}u/u_1$, $C_{\mathfrak{G}}(\tau)=2^l ui(i-1)$ 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:

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

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:

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

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 $\mathfrak{G}$ satisfiy $(*)$. 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 $N_{\mathfrak{G}}(\mathfrak{K}_r)$ satisfying the condition*

$\alpha(\langle J, K_r\rangle)=1$. *Let* $\tilde{\mathfrak{K}}$ *be the stabilizer of two symbols* a *and* b *in* $\mathfrak{J}(\mathfrak{K}_r)$ *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* $\mathfrak{J}(X)$ *is contained in* $\mathfrak{J}(\mathfrak{K}_2)$ *for every element* $X(\neq 1)$ or $\mathfrak{K}_r$.

Proof. Assume $\mathfrak{J}(\mathfrak{K}_2)$ does not contain $\mathfrak{J}(X)$. Then there exists an element Y of $\mathfrak{K}_2$ with the cycle structure $(a, b)\cdots$, where a and b are symbols in $\mathfrak{J}(X)$. Let J be an involution with the cycle structure $(a, b)\cdots$. Then J is contained in $N_{\mathfrak{G}}(\mathfrak{K}_r)$, $\langle YJ, X\rangle$ is conjugate to a subgroup of $\mathfrak{K}$ 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* $\mathfrak{K}_1$, *then* $\mathfrak{J}(X)=\mathfrak{J}(\tau)$.

Proof. Assume $\mathfrak{J}(X)$ is greater than $\mathfrak{J}(\tau)$. By a theorem of Witt $N_{\mathfrak{G}}(\langle X\rangle)$ acts doubly transitively on $\mathfrak{J}(X)$. As in the above $|N_{\mathfrak{G}}(\langle X\rangle)|=|K|i(\beta' i-\beta'+1)(i-1)(\beta' i+1)$ 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 $|\mathfrak{G}|/|N_{\mathfrak{G}}(\langle X\rangle)|=(di-d+1)(di+1)/(di/2-d/2+1)(di/2+1)$ 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 $\mathfrak{K}_1$ not contained in $\mathfrak{J}(\tau)$ is $|\mathfrak{K}_1|$-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 $\mathfrak{K}_1$ 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 $\mathfrak{K}$. By a theorem of Witt $N_{\mathfrak{G}}(\mathfrak{X})$ has a doubly transitive permutation representation on $\mathfrak{J}(\mathfrak{X})$. Let $\mathfrak{K}_1(\mathfrak{X})$ 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* $\mathfrak{K}$ *such that* $\mathfrak{J}(\mathfrak{X})$ *is contained in* $\mathfrak{J}(\tau)$. *If* $\mathfrak{G}_1$ *is 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 $C_{\mathfrak{G}}(\tau)$ containing $\mathfrak{K}_1$ such that $\mathfrak{N}/\mathfrak{K}_1$ be a regular normal subgroup of $\mathfrak{G}_1$. It is clear that $N_{\mathfrak{G}}(\mathfrak{X})\cap\mathfrak{N}$ is not contained in $\mathfrak{K}$. Thus $(N_{\mathfrak{G}}(\mathfrak{X})\cap\mathfrak{N})\mathfrak{K}_1(\mathfrak{X})/\mathfrak{K}_1(\mathfrak{X})$ 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 $\alpha(\mathfrak{X})=|(N_{\mathfrak{G}}(\mathfrak{X})\cap\mathfrak{N})\mathfrak{K}_1(\mathfrak{X})/\mathfrak{K}_1(\mathfrak{X})|$.

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 $\mathfrak{K}$.*

Proof. By Lemma 2.6 we may assume that $\mathfrak{J}(X)$ is not contained in $\mathfrak{J}(\tau)$. 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 $\mathfrak{N}$ be a normal subgroup of $C_{\mathfrak{G}}(\tau)$ containing $\mathfrak{K}_1$ such that $\mathfrak{N}/\mathfrak{K}_1$ 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 $\alpha(\mathfrak{K}')$ is odd. Since $\mathfrak{J}(K')^I=\mathfrak{J}(K')$, the unique symbol j in $\mathfrak{J}(I)$ is contained in $\mathfrak{J}(K')$. $I, IK', \cdots, IK'^{2(\beta-2)}$ and $IK'^{2(\beta-1)}$ 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 $\mathfrak{K}_1$ by Lemma 2.5. Set $Y=X\tau$. Then $\mathfrak{J}(Y)$ is a proper subset of $\mathfrak{J}(\tau)$. If $\mathfrak{J}(Y)=\mathfrak{J}(X)$, then r is a factor of $\alpha(Y)$ since $n-\alpha(Y)$ is divisible by r. If $\alpha(Y)<\alpha(X)$. Then $\mathfrak{K}/\mathfrak{K}_1(\langle X\rangle)$ 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 $\alpha(Y)$. Tnus $r=p$ 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 $\mathfrak{N}$. Then $\mathfrak{P}$ is normal in $\mathfrak{N}$.*

Proof. Let $\mathfrak{K}_{1,r}$ be a Sylow r-subgroup $(\neq 1)$ of $\mathfrak{K}_1$, where $r\neq p$. Assume that $C_{\mathfrak{G}}(\mathfrak{K}_{1,r})$ does not contain $\mathfrak{N}$. Since Aut $(\mathfrak{K}_{1,r})$ is cyclic and every element $(\neq 1)$ of $\mathfrak{N}/\mathfrak{K}_1$ is conjugate under $N_{\mathfrak{H}}(\mathfrak{K}_1)/\mathfrak{K}_1$, $i=|\mathfrak{N}/\mathfrak{K}_1|=p$ and $i<r$. Since $\langle I, \mathfrak{N}\rangle/\mathfrak{K}_1$ is dihedral, I is contained in $C_{\mathfrak{G}}(\mathfrak{K}_{1,r})$. 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 $C_{\mathfrak{G}}(\mathfrak{K}_{1,r})$ 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 $C_{\mathfrak{G}}(\tau)$ containing $\langle\tau, I\rangle$. It is also a Sylow 2-subgroup of $\mathfrak{G}$. Since $(\mathfrak{S}\mathfrak{K}_1/\mathfrak{K}_1)(\mathfrak{N}/\mathfrak{K}_1)$ is a Frobenius group, $\mathfrak{S}\mathfrak{K}_1/\mathfrak{K}_1\cong\mathfrak{S}/\langle\tau\rangle$ is cyclic or a (generalized) quaternion group. If $\mathfrak{S}/\langle\tau\rangle\geqq 4$, 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 $C_{\mathfrak{G}}(\tau)$ is that of $\mathfrak{G}$.

Lemma 3.4. *If the order of a Sylow 2-subgroup $\mathfrak{K}_{1,2}$ of $\mathfrak{K}_1$ 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 $C_{\mathfrak{G}}(\mathfrak{V})$ containing $\mathfrak{K}_2$ and let $\mathfrak{S}$ be a Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{V})=C_{\mathfrak{G}}(\tau)$ containing $\mathfrak{S}'$, where $\mathfrak{V}$ is a subgroup of $\mathfrak{K}_1$ of order 4. Since Aut $(\mathfrak{V})=2$ and $N_{\mathfrak{G}}(\mathfrak{V})$ contains I, $[\mathfrak{S}:\mathfrak{S}']=2$ and it may be assume that $\mathfrak{S}=\langle\mathfrak{S}', I\rangle$. By Lemma 2.2 $\langle J, \mathfrak{V}\rangle$ is dihedral for every involution $J(\neq\tau)$ in $N_{\mathfrak{G}}(\mathfrak{V})$. Thus τ is the unique involution in $\mathfrak{S}'$ and hence $\mathfrak{S}'$ is cyclic since $Z(\mathfrak{S}')$ contains $\mathfrak{V}$. $\mathfrak{S}$ is dihedral or semi-dihedral and contained in $N_{\mathfrak{G}}(\mathfrak{K}_2)$. By Lemma 2.6 $\mathfrak{G}_1(\mathfrak{K}_2)$ contains a regular normal subgroup and $\mathfrak{S}/\mathfrak{K}_2$ is contained in a complement of a Frobenius group. Thus $\mathfrak{S}/\mathfrak{K}_2$ is cyclic or a (generalized) quaternion group and hence $\mathfrak{S}=\langle K_2, I\rangle$.

Lemma 3.5. *Let $\mathfrak{K}_{1,2}$ be as in Lemma 3.4. If $\mathfrak{K}_{1,2}=\langle\tau\rangle$ 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 $\mathfrak{V}$ be a subgroup of $\mathfrak{K}_2$ of order 4. Let $\mathfrak{S}'$ be a Sylow 2-subgroup of $C_{\mathfrak{G}}(\mathfrak{V})$ and let $\mathfrak{S}$ be a Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{V})$ 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 $i-1=(\alpha(\mathfrak{V})-1)(\beta'\alpha(\mathfrak{V})+1)$. Since $\langle IK_1, \mathfrak{V}\mathfrak{K}_1/\mathfrak{K}_1\rangle$ is dihedral of order$\geqq 4$, by Lemma 2.1 β' is even. Thus $\mathfrak{S}$ is a Sylow 2-subgroup of $C_{\mathfrak{G}}(\tau)$. 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 cyclie decomposition $(1, 2)\cdots$

which is conjugate to $K_2\mathfrak{K}_1$. Let J be a 2-element in $\bar{J}$. Then $(\alpha(J,\tau)\geqq 2$ and hence $|J|>2$. On the other hand J is contained in $I\mathfrak{K}$ and every 2-element $(\neq 1)$ of $I\mathfrak{K}-\mathfrak{K}$ 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 $|K_{1,2}|\geqq 4$. All involutions in $I\mathfrak{K}$ are conjugate. Since $\mathfrak{G}$ is doubly transitive on Ω, all involutions in $\mathfrak{G}$ are conjugate. Since $|K_{1,2}|\geqq 4$ and $(IK_2)^2=\tau$, $\alpha(IK_2)=1$ and IK_2 is not conjugate to an element of $\mathfrak{K}_{1,2}$. 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 $\mathfrak{J}(\tau)$ and has also two classes of involutions since $\alpha(\langle I,\tau\rangle)=1$ and $|K_2^2|\geqq 4$. 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 $\mathfrak{K}_2$ is not contained in $\mathfrak{K}_1$, then d and $d-1$ are not divisible by p.*

Proof. Since $\mathfrak{K}/\mathfrak{K}_1$ 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 $i'=\alpha(\widetilde{K}_2)$ for some $\widetilde{K}_2$ in $\mathfrak{K}_2$. 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 $|\mathfrak{K}|$ is not divisible by p. Let $\mathfrak{P}$ be a Sylow p-subgroup of $\mathfrak{N}$. Then it is an elementary abelian Sylow p-subgroup of $\mathfrak{G}$ and normal in $C_{\mathfrak{G}}(\tau)$ by Lemma 3.3. Set $|C_{\mathfrak{G}}(\mathfrak{P})|=2^{l_1}u_1 iy$. If $y=1$, then $\langle\tau\rangle$ is normal in $C_{\mathfrak{G}}(\mathfrak{P})$ and hence in $N_{\mathfrak{G}}(\mathfrak{P})$. $[\mathfrak{G}:N_{\mathfrak{G}}(\mathfrak{P})]=(di-d+1)(di+1)\equiv -d+1$ (mod 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 $\alpha(\mathfrak{S})\geqq 1$ and hence $\alpha(\mathfrak{S})\geqq i$. Therefore $\mathfrak{S}$ is contained in $\mathfrak{K}_1$. Thus y is odd. Let r be a prime factor of $(y, |\mathfrak{K}|(n-1))$ and let $\mathfrak{R}$ be a Sylow r-subgroup of $C_{\mathfrak{G}}(\mathfrak{P})$. Since by Lemma 3.2 $(r,n)=1$, $\alpha(R)\geqq 1$ hence $\alpha(R)\geqq i$. By the Frattini argument it may be assume that $N_{\mathfrak{G}}(\mathfrak{N})$ contains τ. Since $\alpha(\mathfrak{N})$ is odd by Lemma 2.7 and $\mathfrak{J}(\mathfrak{N})^{\tau}=\mathfrak{J}(\mathfrak{N})$, $\alpha(\langle\mathfrak{N}, \tau\rangle)\geqq 1$. Therefore $\mathfrak{J}(\mathfrak{N})$ is contained in $\mathfrak{J}(\tau)$ and $\mathfrak{N}$ is a subgroup of $\mathfrak{K}_1$, 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 $C_{\mathfrak{H}}(\tau)$ 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 $\mathfrak{K}'\mathfrak{K}_2$ by Lemma 2.3, $[C_{\mathfrak{H}}(\tau):C_{\mathfrak{H}}(\tau)\cap C_{\mathfrak{H}}(Y)]$ is a multiple of $2^{l-1}d(i-1)$. Thus we have the following:

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

From this $l=1$ and $\mathfrak{K}_2=\langle\tau\rangle$, 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 $\mathfrak{K}'$ acts on $\mathfrak{P}'/\mathfrak{P}$. Since, for every element $X(\neq 1)$ of $\mathfrak{K}'$, $C_{\mathfrak{G}}(X)$ is contained in $C_{\mathfrak{G}}(\tau)$ by Lemma 2.3 and a theorem of Witt, $C_{\mathfrak{P}'}(X)=C_{\mathfrak{P}}(X)$. By [6, Theorem 5.3.15] every element $(\neq 1)$ of $\mathfrak{K}'$ induces a fixed point free automorphism of $\mathfrak{P}'/\mathfrak{P}$. Therefore $y-1$ is divisible by d. Thus $d=p^{(f-1)m}+p^{(f-2)m}+\cdots+p^{m}+1$. 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 $|\mathfrak{K}|$ 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 $|\mathfrak{K}|$ is divisible by p, but $(d,p)=1$. Let $\mathfrak{P}$ a Sylow p-subgroup of $\mathfrak{N}$. Set $\mathfrak{P}'=\mathfrak{P}\mathfrak{K}_p$. Put $|C_{\mathfrak{G}}(\mathfrak{P}')|=2^{l_1}u_1'|Z(\mathfrak{P}')|y$, where $2^{l_1}u_1'=|C_{\mathfrak{K}_1}(\mathfrak{P}')/Z(\mathfrak{P}')\cap\mathfrak{K}_p|$. 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 $[\mathfrak{G}:N_{\mathfrak{G}}(\mathfrak{K}')]=[\mathfrak{G}:C_{\mathfrak{G}}(\tau)][C_{\mathfrak{G}}(\tau):N_{\mathfrak{G}}(\mathfrak{P}')]\equiv -d+1 \pmod p$, which is a contradiction. Thus $y\neq 1$. As in the previous case, y is a factor of $di-d+1$. Since $N_{\mathfrak{G}}(\mathfrak{K}_p)$ contains $C_{\mathfrak{G}}(\mathfrak{P}')$ and $C_{\mathfrak{G}}(\tau)$ does not contain $C_{\mathfrak{G}}(\mathfrak{P}')$, $\mathfrak{J}(\mathfrak{K}_p)$ is not contained in $\mathfrak{J}(\tau)$ by a theorem of Witt. As in §2, $\alpha(K_p)=\alpha(K_p\tau)(\beta'(\alpha K_p\tau)-1)+1)$. Since $\mathfrak{G}_1(\mathfrak{K}_p)$ 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. $[N_{\mathfrak{G}}(\mathfrak{K}_p):C_{\mathfrak{G}}(\mathfrak{P}')]=|\mathfrak{K}|\alpha(K_p)(\alpha(K_p)-1)/2u_1'|Z(\mathfrak{P}')|y$. 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 $\mathfrak{K}'$, $C_{\mathfrak{G}}(X)$ is contained in $C_{\mathfrak{G}}(\tau)$ by Lemma 2.3 and a theorem of

Witt, $C_{\mathfrak{P}''}(X)$ is contained in $Z(\mathfrak{P}')$. By [6, Theorem 5.3.15] every element $(\neq 1)$ of $\mathfrak{K}'$ 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 $[N_{\mathfrak{G}}(\mathfrak{K}_p):N_{\mathfrak{G}}(\mathfrak{K}_p)\cap C_{\mathfrak{G}}(\tau)]$ is divisible by y and $|N_{\mathfrak{G}}(\mathfrak{K}_p)\cap C_{\mathfrak{G}}(\tau)|$ is divisible by $|\mathfrak{K}_p|\alpha(K_p\tau)$, $|N_{\mathfrak{G}}(\mathfrak{K}_p)|$ is divisible by $|\mathfrak{K}_p|\alpha(K_p\tau)y$. Thus $d(i-1)+1=\beta'(\alpha(K_p\tau)-1)+1$. Since $d\geqq\beta'$, $d=\beta'$ and $i=\alpha(K_p\tau)$. This implies that $\mathfrak{K}_p$ is contained in $\mathfrak{K}_1$, which is a contradiction.

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

4–3. The case that $d\neq 2$, $\mathfrak{K}_1$ contains $\mathfrak{K}_2$ 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 $\mathfrak{K}_2$ is cyclic.*

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

By this lemma $\mathfrak{S}/\mathfrak{K}_2$ is cyclic. Put $\mathfrak{S}/\mathfrak{K}_2=\langle A\mathfrak{K}_2\rangle$. 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 $|\mathfrak{S}/\mathfrak{K}_2|=2^s$. 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 $|B|=2^{s+1}\geqq 2^l$.*

Proof. Since $n-i=di(i-1)$ is divisible by 2^l, $i-1$ is divisible by 2^{l-1} and $2^s\geqq 2^{l-1}$. Since Aut $(\mathfrak{K}_2)$ is isomorphic to $Z_2\times Z_{2^{l-2}}$, if $l>4$ or $l=4$, then $B^{2^{l-2}}$ 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 $\mathfrak{K}_2$. $\langle\tau\rangle$ is a characteristic subgroup of $\mathfrak{S}$. Therefore $\eta=\tau$ and $|B|\geqq 2^{s+1}$. $\alpha''_{2^t}(B)\neq 0$ 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 unger $\mathfrak{G}$ 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 $I=A^{2^{s-1}}X$, where X is an element of $\mathfrak{K}_2$. Since $A^{2^{s-1}}$ is contained in $Z(\mathfrak{S})$, $A^{2^s}X^2=\tau X^2=1$. 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 PSL$(2, q)$, Sz(q) and PSU$(3, q^2)$, where $q=2^m\geqq 4$. Here PSL$(2, q)$ is the 2-dimensional projective special linear group over GF(q), the field of q elements; Sz(q) is the Suzuki group over GF(q), here m is odd; PSU$(3, q^2)$ is the 3-dimensional projective special unitary group over GF(q^2). If $\mathfrak{G}_1'$ is isomorphic to PSL$(2, q)$, Sz(q) or 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 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. $O(\mathfrak{K}')$ *has a normal complement* $\mathfrak{U}$ *in* $\mathfrak{H}$.

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

Lemma 4.3. *$C_{\mathfrak{H}}(\tau)$ 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, $C_{\mathfrak{H}}(\tau)\cap\mathfrak{H}$ has a normal Sylow 2-subgroup. This proves the lemma.

2. The case $\mathfrak{G}_1'$ is isomorphic to 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 $\mathfrak{R}_1\times$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 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 $\alpha(\mathfrak{R}_1\times\mathfrak{S})=1$, $N_{\mathfrak{G}}(\mathfrak{R}_1\times\mathfrak{S})=N_{\mathfrak{H}}(\mathfrak{R}_1\times\mathfrak{S})$ and by Lemma 4.3 $[N_{\mathfrak{H}}(\mathfrak{R}_1\times\mathfrak{S}) : C_{\mathfrak{H}}(\tau)]=2q-1$ and hence $|N_{\mathfrak{H}}(\mathfrak{R}_1\times\mathfrak{S})|=|\mathfrak{R}|(i-1)(2q-1)$. But $[\mathfrak{H} : N_{\mathfrak{H}}(\mathfrak{R}_1\times\mathfrak{S})]=(2(q-1)i+1)/(2q-1)$ 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 $|\mathfrak{R}_2|>2$. $\mho^1(Z(\mathfrak{R}_2\times\mathfrak{S}))=\langle\mathfrak{R}_2^2\rangle$ is a characterisic 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 $\mathfrak{T}$ 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 $\mathfrak{T}$ is normal in $\mathfrak{H}$. Since $h^*(2)=q-1$ and $O(\mathfrak{R}')$ acts fixed-point-freely on $Z(\mathfrak{T})$, it is elementary abelian of order q. If $\tau Z(\mathfrak{T})$ is a normal subset of $\mathfrak{T}$, $q\geqq[\mathfrak{T} : C_{\mathfrak{T}}(\tau)]=2q^3/2q$ since the number of involutions in $\tau Z(\mathfrak{T})$ which are cojugate to τ equals to q, which is a contradiction. Thus $\mathfrak{T}/Z(\mathfrak{T})$ is non-abelian. Let $Z_2(\mathfrak{T})$ is a normal subgroup of $\mathfrak{T}$ containing $Z(\mathfrak{T})$ such that $Z_2(\mathfrak{T})=Z(\mathfrak{T}/Z(\mathfrak{T}))$. Since $O(\mathfrak{R}')$ is considered as a group of fixed point free automorphisms of $Z(\mathfrak{T}/Z(\mathfrak{T}))$, $Z_2(\mathfrak{T})\geqq q^2$.

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

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

If $|\mathfrak{T}/Z_2(\mathfrak{T})|=2$, then $\mathfrak{T}=\langle\tau\rangle\mathfrak{B}$, where $\mathfrak{B}=Z_2(\mathfrak{T})$. If $|\mathfrak{T}/Z_2(\mathfrak{T})|>2$, then there exists a subgroup $\mathfrak{B}$ of $\mathfrak{T}$ containing $Z_2(\mathfrak{T})$ such that $\mathfrak{T}=\langle\tau\rangle\mathfrak{B}$. Since every involution in $\mathfrak{H}$ which is conjugate to τ is already conjugate under $\mathfrak{B}$. Thus the focal subgroup of $\mathfrak{T}$ 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 $\mathrm{PSU}(3, q^2)$. 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 $\mathrm{GF}(q^2)$ of order 2 and B is an inner automorphism induced by an element of $N_{\mathfrak{G}'}(0(\mathfrak{K}))$. But such automorphism does not fix every element of $0(\mathfrak{K})$. Since $\mathfrak{K}$ is abelian, this is a contradiction.

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

Assume $\beta=d$. Then $\mathfrak{K}_2\times\mathfrak{S}$ is a Sylow 2-subgroup of $\mathfrak{G}$. The number of involutions of $Z(\mathfrak{K}_2\times\mathfrak{S})$ equals to $2q-1$. As in the above case, $N_{\mathfrak{H}}(\mathfrak{K}_2\times\mathfrak{S}) =|\mathfrak{K}|(i-1)(2q-1)$. But $[\mathfrak{H}:N_{\mathfrak{H}}(\mathfrak{K}_2\times\mathfrak{S})]=(2(q-1)i+1)/(2q-1)$ 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 $\mathfrak{K}_3$. Then $\mathfrak{K}_3$ 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 $0(\mathfrak{K}')$. Since $N_{\mathfrak{G}}(0(\mathfrak{K}'))=\langle I, K\rangle$, $0(\mathfrak{K}')$ induces a fixed point free group of automorphisms of $\mathfrak{R}/\mathfrak{K}_3$, which is a contradiction.

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

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

Proof. Let X be an element of $\mathfrak{K}$ not contained in $\mathfrak{K}'\mathfrak{K}_2$. If $\mathfrak{J}(X)$ is not contained in $\mathfrak{J}(\tau)$, $\mathfrak{G}_1(\langle X\rangle)$ 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 $\mathfrak{J}(X)$ is contained in $\mathfrak{J}(\tau)$. By Lemma 2.3 and 2.4 $\mathfrak{J}(Y)$ is contained in $\mathfrak{K}(\tau)$ for every element $Y(\neq 1)$ of $\mathfrak{K}'\mathfrak{K}_2$. This completes the proof.

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

Lemma 4.7. *$0(\mathfrak{K})$ has normal complement $\mathfrak{T}$ in $\mathfrak{H}$.*

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

Let $\mathfrak{K}(q)$ 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 $N_{\mathfrak{H}}(\mathfrak{P}_r)$ contains $\mathfrak{K}(q)$ by [6, Theorem 6.2.2]. If $r\neq 2$, then $\mathfrak{K}(q)$ is a group of fixed point free automorphisms of $\mathfrak{P}_r$ since $(|C_{\mathfrak{H}}(\tau)|, |\mathfrak{T}|)$ 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

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

This is a contradiction.

Next assume $\beta=d$. Then $n-1=q^3(2q^4-2q^3+2q-1)$. $\mathfrak{K}_2$ is of order 4 since $\mathfrak{G}$ has one class of involutions, the exponent of a Sylow 2-subgroup of 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, $|N_{\mathfrak{T}}(\mathfrak{P}_r)|=2q^3$ or $4q^3$. $r=2qx-1$ for some integer x.

4–1. The case $[\mathfrak{T}:N_{\mathfrak{T}}(\mathfrak{P}_r)]=2q^3\equiv 1 \pmod r$. 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 $[\mathfrak{T}:N_{\mathfrak{T}}(\mathfrak{P}_r)]=4q^3\equiv 1 \pmod r$. 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. $n-1=q^3r_1^m r_2^{m'}t$, where $r_1^m<r_2^{m'}$ and t is relatively prime to r_1 and r_2. If $r_1^m-1\geqq 4(q^2-1)/3$ or $r_2^{m'}-1\geqq 10(q^2-1)/3$, 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-subgrous, 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 $2^l(n-1)n$, J. Math. Soc. Iapan, 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 cyclicic subgroups of index 2, J. Austral. Math. Soc., 4 (1964), 90–112.

Department of Mathematics,
Hokkaido University

(Received June 11, 1970)