K. Harada
Nagoya Math. J.
Vol. 38 (1970), 27–40

A CHARACTERIZATION OF THE SIMPLE GROUP $U_3(5)$

KOICHIRO HARADA*

Dedicated to Professor Katuzi Ono

0. In this note we consider a finite group G which satisfies the following conditions:

(0. 1) G is a doubly transitive permutation group on a set Ω of $m+1$ letters, where m is an odd integer ≥ 3,

(0. 2) if H is a subgroup of G and contains all the elements of G which fix two different letters α, β, then H contains unique permutation $h_0 \neq 1$ which fixes at least three letters,

(0. 3) every involution of G fixes at least three letters,

(0. 4) G is not isomorphic to one of the groups of Ree type.

Here we mean by groups of Ree type the groups which satisfy the conditions of H. Ward [13] and the minimal Ree group of order $(3-1)3^3$ (3^3+1).

We shall prove the following theorem.

THEOREM. *The simple group* $U_3(5)$ *is the only group with the properties* $(0,1) \sim (0,4)$.

(*Remark:* A theorem of R. Ree [8] seems to be incomplete).

The theorem is proved in a usual argument. Final identification of $U_3(5)$ is completed by a theorem of rank 3-groups due to D.G. Higman.

Our notation is standard and will be explained when first introduced.

1. Before proving our theorem, we quote here various results proved by R. Ree [8].

Received November 4, 1968

* The author expresses his gratitude to Prof. Gorenstein who has pointed out a gap in his original proof. This research was partially supported by National Science Foundaticn grant GP-7952X.

Let G be a finite group with the properties $(0,1)$, $(0,2)$ and $(0,3)$, and B the subgroup of G which contains all the elements that leave a fixed letter α invariant. Choose an involution w of $G-B$ and set $H=B\cap B^w$ and $\alpha^w=\beta$. Then $(0,2)$ and $(0,3)$ imply that h_0 is a unique involution of H. Set $H_0=\langle h_0\rangle$. Then the following results hold.

(1. A) $H^w=w^{-1}Hw=H,\ wh_0=h_0w,\ |G|=m(m+1)|H|$.

(1. B) All the involutions of G are contained in a single conjugate class (Prop. 1. 9 [8]).

(1. C) B contains normal subgroup U of order m which acts regularly on $\Omega-\{\alpha\}$ (1. 13 [8]).

(1. D) G admits a decomposition

$$G=UH\cup UHwU,\quad UH\cap UHwU=\phi.$$

Every element of UH is written uniquely in the form uh where $u\in U,\ h\in H$. Every element of $UHwU$ is written uniquely in the form u_1hwu_2, where $u_1,\ u_2\in U,\ h\in H$ (Prop. 1. 15 [8]).

(1. E) For every prime p, the Sylow p-subgroups of H are cyclic (Prop. 1. 25 [8]).

(1. F) $C(h_0)/H_0$ is a Zassenhaus group of order $q(q+1)\frac{|H|}{2}$, where q is the order of $C_U(h_0)$ (Prop. 1. 26 [8]).

(1. G) Denote by n the number of involutions in the subset Hw. Then the following equality holds (Prop. 1. 27 [8]);

$$m=(qn+n+1)q.$$

2. Let G be a group satisfying the conditions $(0.\ 1)\sim(0.\ 4)$. In this section we shall determine the structure of $C(h_0)$.

If the index $[H:H_0]$ is odd, then G is isomorphic to one of the groups of Ree type as R. Ree has proved. Therefore in the rest of this note we assume that $[H:H_0]$ is even. First we quote two theorems due to Schur [9].

THEOREM (2. A). *Let q be a power of an odd prime, and Y a subgroup of order 2 contained in the center of a group X. If X/Y is isomorphic to $PSL(2,q)$, then X is isomorphic to $SL(2,q)$ or a direct product of Y with a group isomorphic to $PSL(2,q)$.*

THEOREM $(2, B)$. *Let q be a power of an odd prime and Y a subgroup of order 2 contained in the center of X. If X/Y is isomorphic to $PGL(2,q)$ and if X contains at least two involutions, then X is the direct product of Y with $PGL(2,q)$ or isomorphic to the subgroup $\mathfrak{K}_q = \langle SL(2,q), U\rangle$ of $GL(2,q^2)$, where $U = \begin{pmatrix} u^{2^{r-1}+1} & 0 \\ 0 & u^{2^{r-1}-1} \end{pmatrix}$, u is an element of order 2^{r+1} in the multiplicative group of $GF(q^2)$ and $q-1=2^r \cdot s$, s an odd integer.* (*Remark*: $\mathfrak{K}_q$ is $\mathfrak{K}'_q$ in the notation of ([9], p. 122).

Since we have assumed that the index $[H:H_0]$ is even, $C(h_0)/H_0$ is isomorphic to $PSL(2,q)$, $PGL(2,q)$ or M_q by a theorem of H. Zassenhaus [14]. Since $C(h_0)$ contains at least two involutions h_0, w and the Schur multiplier of M_q is trivial, we have $C(h_0) \cong Z_2 \times PSL(2,q)$ or $Z_2 \times M_q$, if $C(h_0)/H_0 \cong PSL(2,q)$ or M_q. Here Z_i is a cyclic group of order i. Therefore $H \cong Z_2 \times Z_{\frac{q-1}{2}}$ or $Z_2 \times Y_{q-1}$ where Y_{q-1} is a group of order $q-1$. This contradicts with the fact that a Sylow 2-subgroup H is cyclic (note that $q \equiv 1 \pmod 4$ for the former case). The case $C(h_0)/H_0 \cong PGL(2,q)$ with $q \equiv -1 \pmod 4$ is eliminated by R. Ree ([8] p. 803). Therefore we must have $C(h_0)/H_0 \cong PGL(2,q)$ and $q \equiv 1 \pmod 4$. We easily see that $C(h_0)$ is not isomorphic to $Z_2 \times PGL(2,q)$. Therefore $C(h_0)$ is isomorphic to the group $\mathfrak{K}_q$ which is described in Theorem (2. B). Clearly we have $|C(h_0)| = 2(q-1)q(q+1)$.

We shall study the structure of $\mathfrak{K}_q$ nd describe below. Since these facts are proved easily we state without proof. Put $W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $V = \begin{pmatrix} v & 0 \\ 0 & v^{-1} \end{pmatrix}$ where v is an element of order $q-1$ in the multiplicative group of $GF(q^2)$.

(2. A) A Sylow 2-subgroup $\mathfrak{S}$ of $\mathfrak{K}_q$ is a semi-dihedral group of order 2^{r+2}.

$$\mathfrak{S} = \langle U, W \mid W^{-1}UW = U^{-1} \cdot U^{2^r} \rangle.$$

(2. B) $\mathfrak{K}_q$ contains a cyclic subgroup $\mathfrak{H}$ of order $2(q-1)$.

$$\mathfrak{H} = \langle U \cdot V \rangle.$$

(2. C) $\mathfrak{H}$ is a normal subgroup of index 2 of $N_{\mathfrak{K}_q}(\mathfrak{H}) = \langle \mathfrak{H}, W \rangle$.

(2. D) The subset $\mathfrak{H}W$ contains $q-1$ involutions (note that $(U \cdot V)^W = (U \cdot V)^{-q}$).

(2. E) If I is a non central involution of $\mathfrak{K}_q$ and X is an element of order x, where $x \mid q+1$, then

$$C_{\mathfrak{R}_q}(I) \cong C_{\mathfrak{R}_q}(X) \cong Z_2 \times Z_{q+1}.$$

3. Now we back to our group G. On account of (2. D), we easily see that Hw contains $q-1$ involutions. Using (1. G), we can conclude that $m = q^3$ and $|G| = 2(q-1)q^3(q^3+1)$. Next we shall apply the theory of modular characters developed by R. Brauer [1] where he has given a detailed discussion on groups with semi-dihedral Sylow 2-subgroups and on groups with a special type of abelian Sylow p-subgroups. We summarize here his results.

(3. A) Let G_1 be a finite group with a semi-dihedral Sylow 2-subgroup S_1 of order 2^n; $S_1 = \langle \tau, \sigma \mid \tau^2 = \sigma^{2^{n-1}} = 1,\ \sigma^\tau = \sigma^{-1}\cdot J,\ J = \sigma^{2^{n-2}} \rangle$. Furthermore let us assume that there does not exists a normal subgroup of index 2. Then the principal 2-block $B_0(2)$ of G_1 consists of $4+2^{n-2}$ characters $X_\mu, X^{(j)}$ with $0 \leq \mu \leq 4$, and $j = \pm 1,\ 2,\ \pm 3,\ 4, \cdots \pm (2^{n-2}-1)$. X_μ $(0 \leq \mu \leq 3)$ are all characters of odd degrees in $B_0(2)$. If $\xi = J \cdot \rho$ has the 2-factor J, then

(3. 1) $$X_1(\xi) = -\delta_1 + \delta_1 \phi_1^J(\rho),\quad X_2(\xi) = \delta_2 - \delta_2 \phi_1^J(\rho),\quad X_3(\xi) = -\delta_3.$$

Here δ_1, δ_2, δ_3 are signs and $\pm \phi_1^J$ is a suitable irreducible character of the principal 2-block of $C_{G_1}(J)/\langle J \rangle$; $\phi_1^J(1) \equiv 2 + 2^{n-2} \pmod{2^{n-1}}$. If ρ is 2-regular, all $X^{(j)}(\rho)$ are equal. In particular, all have the same degree. Furthermore,

(3. 2) $$1 + \delta_1 X_1(1) = \delta_1 X^{(j)}(1) = -\delta_2 X_2(1) - \delta_3 X_3(1),\quad 1 + \delta_2 X_2(1) = \delta_2 X_4(1).$$

If we set $l = \phi_1^J(1) - 1$, then

(3. 3) $$l \equiv 1 + 2^{n-2} \pmod{2^{n-1}}$$

and by (3. 1) we have

(3. 4) $$X_1(J) = \delta_1 l,\quad X_2(J) = -\delta_2 l,\quad X_3(J) = -\delta_3.$$

Furthermore we have

(3. 5) $$X_2(1) \equiv -l \pmod{2^n},$$

(3. 6) $$\delta_1\delta_2\delta_3 = 1 \quad x_1 x_2 = l^2 x_3.$$

(3. B) Let G_1 be a group with a Sylow p-subgroup P such that the following conditions are satisfied;

(3. a) P is abelian: $P \neq 1$,

(3. b) $N(P)/C(P)$ is cyclic of order m,

(3. c) If $\xi \in N(P) - C(P)$, then ξ does not commute with any element $\pi \neq 1$ of P.

Then the principal block $B_0(p)$ consists of $r = \frac{|P|-1}{m}$ "exceptional" characters $Y^{(j)}$ and $s \leq m$ "non exceptional" characters $Y_0 = 1, Y_1, \cdots, Y_{s-1}$ such that for p-singular elements ξ with the p-factor $\pi \in P$, we have

$$Y_i(\xi) = a_i:$$

Here $a_0, \cdots, a_{s-1}$ are non-zero rational integers. Moreover there exist integers $d, \delta = \pm 1$ such that

$$(d-\delta)^2 + (r-1)d^2 + \sum_{i=0}^{s-1} a_i^2 = m+1.$$

For p-regular ρ, all $Y^{(j)}(\rho)$ take the same value and

$$(rd-\delta)Y^{(j)}(\rho) + \sum_{i=0}^{s-1} a_i Y_i(\rho) = 0.$$

(3. B′) If $m = 2$ in (3. B) we may assume $d = 0$. Then $s = 2$, $a_i = \delta$, $Y^{(j)}(1) = Y_1(1) = \delta$.

4. To apply (3·A) to our group G, we must show that G has no normal subgroup of index 2. By way of contradiction, let us assume that N is a normal subgroup of index 2 of G. Then $N \cap C(h_0)$ is a normal subgroup of $C(h_0)$ of index 2. Therefore $N \cap C(h_0)$ is isomorphic to $SL(2, q)$. This implies that a Sylow 2-subgroup of N is a generalized quaternion group. By the double transitivity of G and the assumption $|\Omega| =$ even, we see that N has no normal subgroup of odd order. Therefore a theorem of R. Brauer and M. Suzuki [2] shows that H_0 is the center of N, hence the center of G. This is clearly impossible.

We shall prove some lemmas. Let us assume $G_1 = G$ in (3. A).

LEMMA (4. 1). $X_1(1) = q^3$, $X_2(1) = q^2 - q + 1$, $X_3(1) = q(q^2 - q + 1)$, $X_4(1) = q^2 - q$, $X^{(j)}(1) = q^3 + 1$, $\delta_1 = 1$, $\delta_2 = \delta_3 = -1$.

Proof. Since G is doubly transitive on Ω, there exists an irreducible character Y of degree q^3. As $Y(1)$ is odd, Y belongs to a 2-block of maximal defect. On the other hand we easily see that G contains no 2-regular element $\neq 1$ of maximal 2-defect. Therefore $Y \in B_0(G)$. As

$Y(J)=q$, we have $Y=X_1$ or X_2 and $l=\pm q$ by (3. 4). Since $q\equiv 1 \pmod{2^{n-2}}$ and $l\equiv 1+2^{n-2} \pmod{2^{n-1}}$, we have $l=q$. On account of (3. 5), we can conclude $Y\neq X_2$. Therefore $Y=X_1$ and $\delta_1=1$. On account of (3. 2), (3. 6) we easily have our lemma.

LEMMA (4. 2). *Let p be an odd prime dividing $q+1$ and P a Sylow p-subgroup of $C(h_0)$, then P is cyclic and $|N(P)/C(P)|=2$.*

Proof. Comparing the structure of $C(h_0)$ we see that P is cyclic. Let K be a Sylow 2-subgroup of $C(P)\cap C(h_0)$, then $K\cong Z_2\times Z_2$ and $C(K)\subset C(P)$ by (2. E). Furthermore K is a Sylow 2-subgroup of $C(P)$. By Frattini argument, we have $N(P)=(N(P)\cap N(K))\cdot C(P)$. Hence

$$N(P)/C(P)\cong\frac{N(P)\cap N(K)}{C(P)\cap N(K)}\cong\frac{L}{M}\quad\text{where}\quad L=\frac{N(P)\cap N(K)}{C(K)},$$
$$M=\frac{C(P)\cap N(K)}{C(K)}.$$

This implies $N(P)/C(P)$ is isomorphic to a factor group of a subgroup of the symmetric group of degree 3. Since $N(P)/C(P)$ must be cyclic, we can conclude $|N(P)/C(P)|=2$ (note that $|N(P)/C(P)|$ is divisible by 2).

LEMMA (4. 3). $q+1=2\cdot 3^b$, $b\geq 1$. *If P is a Sylow 3-group of G, then* $[N(P):C(P)]>2$.

Proof. By way of contradiction, let p be a prime $\neq 2, 3$ dividing $q+1$. Then, since $(q+1,\ q^2-q+1)=1$ or 3, Sylow p-subgroup of G is cyclic and $|N(P)/C(P)|=2$ by Lemma (4. 2). We can apply the previously described theorem (3. B′) of R. Brauer. We get a generalized character

$$\varphi=1-\delta Y^{(j)}+\delta Y$$

which vanishes on every p-regular element. Since $|P|>3$ and G does not have two characters of same odd degree, we conclude $Y(1)$ is odd. Since $q^2-q+1\equiv 3$, $q(q^2-q+1)\equiv -3 \pmod{|P|}$. We have $Y=X_1$. Since $q^3\equiv -1 \pmod{|P|}$, we have $\delta=-1$ and $Y^{(j)}(1)=q^3-1$. On the other hand we easily see $q^3-1\nmid |G|=2(q-1)q^3(q^3+1)$. This is a contradiction. As $q>1$, the former part of the lemma follows. Since $3|q+1$, we have $(q+1,\ q^2-q+1)=3$. Therefore a Sylow 3-subgroup P of G is of order 3^{b+1} and P is abelian by (4. 2). Suppose $[N(P):C(P)]=2$. Then, if $Z(N(P))\cap P=1$, the condition (3. c) of (3. B) is satisfied. We can apply same argument as above and easily get a contradiction. If $Z(N(P)) \cap P > 1$, then G contains a normal subgroup N of index 3. By Frattini argument we easily get a contradiction, for a Sylow 2-subgroup of G is self-normalizing.

LEMMA (4. 4). $q+1=2\cdot 3=6$, *i.e.* $b=1$.

Proof. By way of contradiction let us assume $b>1$. Then a Sylow 3-subgroup P of G is of order 3^{b+1}. By Lemma (4. 2), P is abelian. If P is cyclic, then we easily conclude that $[N(P):C(P)]=2$. This is impossible by the previous lemma. Therefore $P \cong Z_{3^b} \times Z_3$. As $b>1$, P has a characteristic series

$$P > P_1 > P_2 \cdots > P_{b+1} = \{1\},$$

such that $[P_i : P_{i+1}]=3$. This forces $N(P)/C(P)$ to be a 2-group. Let T be a Sylow 2-subgroup of $N(P)$. Then T operates on $\Omega_1(P) = \mho^{b-1}(P) \times Q$, where $\Omega_1(P)$ is the group generated by all elements of order p in P and $\mho^{b-1}(P)$ is the group generated by all $x^{p^{b-1}}$, $x \in P$. Since T operates completely reducibly on $\Omega_1(P)$ we may assume Q is invariant by T. By a well known theorem of Burnside two elements of P are conjugate in G if and only if they are conjugate in $N(P)$. So any element of $Q-\{1\}$ is not conjugate to an element of $\mho^{b-1}(P)$. This implies that an element of $Q-\{1\}$ is not conjugate to any element of $C(h_0)$. In particular T operates on Q as a fixed point free automorphism of Q, for $C(h_0)$ contains one conjugate class of elements of order 3. This forces $|T|=2$. This is impossible. We have thus proved that $q=5$ and $G = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7$.

5. In sections $1 \sim 4$, we have proved that G satisfies the following properties;

(5. a) G is a doubly transitive permutation group of degree $126 = 5^3+1$.

(5. b) B has a regular normal subgroup U.

(5. c) B/U is a cyclic subgroup of order 8.

In his paper [11], M. Suzuki has characterized the projective (full) unitary group of dimension 3 over a field of q^2 elements. In particular he has characterized $PGU(3, 5^2)$ but not $PSU(3, 5^2) = U_3(5)$. It is hoped to characterize $PSU(3, q^2)$ by the property of the centralizer of its involution or by the property of its doubly transitive permutation representation. In this note, however, it is sufficient to characterize $U_3(5)$ only. So we shall apply a theorem of rank 3-groups due to D.G. Higman [5]. Our procedure is as follows. First we shall construct a subgroup H of G which is isomorphic to A_7: the alternating group of degree seven. Let n_p be a number of Sylow p-subgroup of G where $p=3, 5, 7$. We compute n_p. Clearly $n_5=126$. Since a Sylow 5-subgroup of G satisfies the TI-property, a 5-element does not commute with any p-element, $p=3,7$. Since a 2-element does not commute with any 7-element, n_7 is divisible by $2^3 \cdot 5^3$ which is equal to -1 modulo 7. By Sylow's theorem we conclude $n_7=2^4 \cdot 3 \cdot 5^3$. This implies that the normalizer $N(S_7)$ of a Sylow 7-subgroup S_7 of G is of order $3 \cdot 7$. Since, as we easily see, G does not contains a normal subgroup of index 7, $N(S_7)$ is a Frobenius group. Since a Sylow 3-group S_3 of G is not cyclic, S_3 is an elementary abelian group of order 9. Comparing the structure of $GL(2,3)$, we conclude that n_3 is divisible by $5^3 \cdot 7$ which is equal to -1 modulo 3. Hence $n_3=2 \cdot 5^3 \cdot 7$ or $2^3 \cdot 5^3 \cdot 7$. Suppose $n_3=2^3 \cdot 5^3 \cdot 7$. Then $N(S_3)$ is a Frobenius group of order $2 \cdot 3^2$. This contradicts Lemma (4. 2). Hence $[N(S_3):S_3]=8$. We next show that the elements of order 3 of G form a single conjugate class. To show this it is sufficient to see that every element of order 3 is conjugate to an element of $C(h_0)$. Indeed, if $\pi \in S_3$ is not commutative with any 2-element $\neq 1$ of $N(S_3)$, then π has 8 conjugate element in $N(S_3)$. This implies that all elements of order 3 of G are contained in a single conjugate class. Thus we have done. We consider the group $C(\pi_1)$ where π_1 is an element of order 3. Clearly $C(\pi_1)$ is a 2,3-group. Comparing the structure of $C(h_0)$, we get $|C(\pi_1)|=2^2 \cdot 3^2$ and a Sylow 2-subgroup of $C(\pi_1)$ is a four-group. An easy argument shows that $C(\pi_1)$ is 3-closed or 2-closed. If the former case occurs, then a Sylow 2-subgroup S of $N(S_3)$ is a dihedral group and the center σ of S is commutative with at least one element $\neq 1$ of S_3. By complete reducibility σ is commutative with every element of S_3. This is impossible, since $|C(h_0)|$ can not be divisible by 9. Therefore $C(\pi_1)$ is 2-closed. And we get $C(\pi_1)=\langle \pi_1 \rangle \times A$ where A is isomorphic to the alternating group of degree 4. Since π_1 is a real element, we have $[N(\langle \pi_1 \rangle):C(\pi_1)]=2$. Let τ be a 2-element in $N(\langle \pi_1 \rangle)-C(\pi_1)$ then by complete reducibity of $C(\pi_1)/[A,A]$ we may assume A is invariant by τ. Since G does not contains a non cyclic abelian subgroup of order 8, τ induces an outer automorphism of A. This implies $\langle \tau \rangle \cdot A \cong S_4$. Therefore we can choose three elements $\pi_3, \pi_4, \pi_5 \in \langle \tau \rangle \cdot A - A$, such that

$$\pi_3^2 = \pi_4^2 = \pi_5^2 = 1, \quad (\pi_3\pi_4)^3 = (\pi_4\pi_5)^3 = 1, \quad (\pi_3\pi_5)^2 = 1.$$

These elements are the canonical generators of $\langle\tau\rangle \cdot A \cong S_4$ in the sense of Dickson [3]. Next consider $N(\langle\pi_4\pi_5\rangle) = (\langle\pi_4\pi_5\rangle \times B) \cdot \langle\pi_4\rangle$ where $C(\pi_4\pi_5) = \langle\pi_4\pi_5\rangle \times B$ and $B \cdot \langle\pi_4\rangle \cong S_4$. And choose an involution π_2 of B commutative with $\pi_4 \cdot \pi_2$ is uniquely determined. Furthermore $\langle\pi_1, \pi_2\rangle \cong A_4$. We shall show that $\pi_1, \cdots, \pi_5$ satisfy the relation of canonical generators of A_7:

$$\pi_1^3 = \pi_2^2 = \pi_3^2 = \pi_4^2 = \pi_5^2 = 1,$$
$$(\pi_1\pi_2)^3 = (\pi_2\pi_3)^3 = (\pi_3\pi_4)^3 = (\pi_4\pi_5)^3 = 1,$$
$$(\pi_1\pi_3)^2 = (\pi_1\pi_4)^2 = (\pi_1\pi_5)^2 = (\pi_2\pi_4)^2 = (\pi_2\pi_5)^2 = (\pi_3\pi_5)^2 = 1.$$

We must prove only one relation $(\pi_2\pi_3)^3 = 1$, for the other relations are automatically satisfied from our choice of these elements. Since $\langle\pi_2, \pi_3\rangle \subset C(\pi_5) \cong \mathfrak{K}_5$, then $\langle\pi_2, \pi_3\rangle$ is a dihedral group of order 12, 8, 4, or 6. Suppose $[\pi_2, \pi_3] = 1$, then since G contains no elementary abelian subgroup of order 8, we have $\pi_2\pi_3 = \pi_5$. Hence $\pi_2 = \pi_5\pi_3 \in C(\pi_1)$. This is impossible as $\langle\pi_1, \pi_2\rangle \cong A_4$. Suppose $|\langle\pi_2, \pi_3\rangle| = 12$ or 8. Take an involution π of the center of $\langle\pi_2, \pi_3\rangle$. If $\pi \neq \pi_5$, then $\langle\pi_2, \pi_3\rangle$ is contained in $C(\pi_5, \pi)$. This is impossible by (2, E). Hence $\pi = \pi_5$. This implies $(\pi_2\pi_3)^2 = \pi_5$ or $(\pi_2\pi_3)^3 = \pi_5$. Suppose $(\pi_2\pi_3)^2 = \pi_5$ then $\pi_2\pi_3\pi_2 = \pi_5\pi_3 \in C(\pi_1)$. Since $C(\pi_1)$ is 2-closed and is invariant by π_4 we get $[\pi_3^{\pi_2}, \pi_3^{\pi_2\pi_4}] = 1$. This implies $[\pi_3, \pi_3^{\pi_4}] = 1$. Since $\pi_4\pi_3\pi_4 = \pi_3\pi_4\pi_3$, we get $\pi_4 \in C(\pi_3)$ which is impossible. Suppose $(\pi_2\pi_3)^3 = \pi_5$ then $\pi_2^{\pi_3\pi_2} \in C(\pi_1)$. Therefore $[\pi_2^{\pi_3\pi_2}, \pi_2^{\pi_3\pi_2\pi_4}] = 1$. Since $[\pi_2, \pi_4] = 1$, we get $[\pi_2^{\pi_3}, \pi_2^{\pi_3\pi_4}] = 1$. Since $\pi_3\pi_4 = \pi_4\pi_3\pi_4\pi_3$ we get $[\pi_2^{\pi_3}, \pi_2^{\pi_3\pi_4\pi_3}] = [\pi_2, \pi_2^{\pi_3}]^{\pi_4\pi_3} = 1$. This implies $\pi_2\pi_3\pi_2\pi_3 = \pi_3\pi_2\pi_3\pi_2$. Hence $(\pi_2\pi_3)^4 = 1$. This case has already been ruled out. Thus we have proved $H = \langle\pi_1, \pi_2, \cdots, \pi_5\rangle \cong A_7$.

H is a subgroup of index 50, as $|G| = 126000$, $|H| = 2520$. Therefore G has a permutation representation R of degree 50. We next show that R is a rank 3-representation and its subdegrees are 1, 7, 42. There are 14 conjugate classes in G. As this is easy to see, we just list the order of their representatives;

$$1,\ 2,\ 4,\ 8,\ 8,\ 3,\ 6,\ 5,\ 5,\ 5,\ 5,\ 10,\ 7,\ 7.$$

We compute the degrees of irreducible characters of G. By Lemma (4. 1) we have already known that there exist irreducible characters of degrees 1, 125, 21, 105, 20, 126, 126, 126. Since the normalizer of a Sylow 7-group is a Frobenius group we can apply (3. B) and we get a following euqality

$$1 \pm d - (125) - (20) = 0$$

where d is the degree of an exceptional character. Hence $d = 144$. Thus we have two irreducible characters of degree 144. Let Z_i ($i = 1, 2, 3, 4$) be an irreducible character except those previously stated. Then $Z_i(1)$ must be divisible by $2 \cdot 7$, for Z_i is not contained in a block of p-defect 0, where $p = 2$ or 7. Put $Z_i(1) = 14z_i$. Then

$$126000 = 1 + 125^2 + 21^2 + 105^2 + 20^2 + 3 \cdot 126^2 + 2 \cdot 144^2 + 14^2 \sum z_i^2.$$

Hence $\sum z_i^2 = 48$. Hence $\{z_i | 1 \leq i \leq 4\} = \{2, 2, 2, 6\}$. Thus we have determined all the degrees of irreducible characters of G. And we can conclude that the permutation representation R is of rank 3. Considering the subgroup structure of A_7 we easily see that the subdegrees are 1, 7, 42. Therefore G is isomorphic to $U_3(5)$ by a theorem of D.G. Higman [5].

6. In this section we consider the following problem: Is the condition (0. 3) essential? Our answer is more or less negative. Indeed we can show the following theorem.

THEOREM. *Let G be a group satisfying the conditions*

(0. 1) *G is a doubly transitive permutation group on a set of $m+1$ letters, where m is an odd integer ≥ 3.*

(0. 2′) *if H is a subgroup of G and contains all the elements of G which fix two different letters α, β then H contains exactly one involution h_0 and h_0 is a unique permutation of H which fixes at least three letters.*

(0. 3′) *G does not contain a regular normal subgroup.*

Then G is isomorphic to $U_3(5)$ or one of the groups of Ree type.

Remark. (0. 2′) is stronger than (0. 2), §0. However (0. 2) and (0. 3) imply (0. 2′).

Proof. By way of contradiction we assume that there exists a group G which satisfies the conditions (0. 1), (0. 2′) and (0. 3′) but is isomorphic to neither $U_3(5)$ nor one of the group of Ree type. In particular we assume that G has at least two conjugate classes of involutions. We shall use the same notation as in §0 ~ §5. Our proof proceeds in the following steps.

(6. A). The index $[H : H_0]$ is an odd integer > 1.

Suppose $H=H_0$. Then G is a doubly transitive permutation group of order $2m(m+1)$ and of degree $m+1$. N. Ito [6] has studied the groups with this property and has proved that $PSL(2,5)$ and the minimal Ree group are only such groups. Since $PSL(2,5)$ does not satisfy (0. 2′), we get a contradiction. Next suppose $[H:H_0]$ is even. Then $C(h_0)$ is isomorphic to the group $\mathfrak{K}_q$ (see §2). Since the Sylow 2-subgroups of $C(h_0)$ are semidihedral, a Sylow 2-subgroup of $C(h_0)$ is isomorphic to that of G. Since G does not have a normal subgroup of index 2 (see §4), all the involutions of G are contained in a single conjugate class. This is again a contradiction.

(6. B). Let n be the number of involutions of Hw which are conjugate to h_0 in G, then the following equality holds

$$m=q(qn+n+1).$$

This is a slight modification of (1. G). The proof of this statement is trivial if we refer the proof of (1. G) ([8], p. 801).

(6. C). The involutions of Hw are divided into two classes under conjugation by $N(H)=\langle H,w\rangle$. Each class contains the same number of involutions. These two classes are also G-conjugate classes.

Since $[H:H_0]$ is odd, we may set

$$H=H_0\times H_1$$

where H_1 is a group of odd order. If hw is an involution, then $whw=h^{-1}$. Therefore Hw contains n_1 involutions, where

$$n_1=|M|,\quad M=\{h\in H\,|\,whw=h^{-1}\}.$$

Since H_1 is odd, each coset $h_1C_{H_1}(w)$ of H_1 by $C_{H_1}(w)$ contains exactly one element which is inverted by w. Therefore

$$n_1=2\cdot|H_1|/|C_{H_1}(w)|.$$

On the other hand w has $|N(H)|/|C_{N(H)}(w)|=4\cdot|H_1|/4\cdot|C_{H_1}(w)|=n_1/2$ conjugate elements in a subset Hw. This implies (6. C).

By (6. C), we can conclude that G contains exactly two conjugate classes of involutions, since a suitable conjugate element of every involution of G is contained in $N(H)-H=Hw$.

(6. D). $C(h_0)/H$ does not contain a regular normal subgroup.

R. Ree has proved ([8], p. 807) that if $C(h_0)/H_0$ contains a regular normal subgroup, then

(6. 1) $q+1=2^r$, $[H:H_0]=r$. $|C(h_0)|=r\cdot 2^{r+1}(2^r-1)$, where r is an odd prime. Furthermore he has proved that a set Hw contains exactly two involutions h_0w, w and if H_1 is a subgroup of order r of H then

(6. 2) $$N(H_1)=C(H_1)=H\cup Hw.$$

By the above results and (6. C), we conclude $n=1$. Therefore

(6. 3) $$m=(q+2)q,\quad |G|=r\cdot 2^{2r+1}(2^{2r}-1).$$

(6. 2) implies that H_1 is Sylow r-subgroup and G has a normal r-complement N. For every prime $p\,|\,2^{2r}-1$ there exists at least one Sylow p-subgroup P of N which is invariant by H_1. By (6. 2) again, we see that H_1 induces a fixed point free automorphism on P. Therefore $2^{2r}-1\equiv 1 \pmod{r}$. This forces $r=2$. This is impossible. We have proved (6. D).

(6. E). $C(h_0)\cong Z_2\times PSL(2,q)$ with $q+1\equiv 0 \pmod 4$.

This is a direct consequence from a classification theorem of the Zassenhaus group due to H. Zassenhaus [14], W. Feit [4], N. Ito [6] and from the fact that $[H:H_0]$ is odd.

(6. F). U is an abelian group.

By (6. E), $\langle H,w\rangle=N(H)$ is a generalized dihedral group of order $2(q-1)$. Therefore Hw contains $q-1$ involutions. By (6. C) we have $n=q-1/2$. Therefore $m=q(q^2+1)/2$. Let p be an odd prime dividing $q-1$ (note that $\frac{q-1}{2}=[H:H_0]>1$). Then a Sylow p-subgroup of H induces a fixed point free automorphism on U. Hence U is nilpotent [12]. Let R be a subgroup of order $\frac{q^2+1}{2}$ of U. Then, since HR is a Frobenius group and $|H|=q-1$ we see that R contains no characteristic subgroups. This implies that R is an elementary abelian r-group for some prime r. Since a subgroup Q of order q of U is abelian, the statement (6. F) is proved.

Now we shall show the final contradiction. The following argument is due to M. Suzuki ([11], pp. $6\sim 7$). If η is a linear character of U satisfying $\eta(R)\neq 1$, then η has exactly $q-1$ conjugate characters in B. Hence the character φ of B induced from η is irreducible. We have s such characters, $\varphi_1\cdots\varphi_s$ where $s=\left(q\cdot\frac{q^2+1}{2}-q\right)/q-1=q\cdot\frac{q+1}{2}$. G

has s exceptional characters $E_1 \cdots E_s$ associated with $\varphi_1 \cdots \varphi_s$. The characters E_i satisfy the following properties: $E_i(x) = E_j(x)$ for any element which is not conjugate to an element of $U - \{1\}$. And $E_1 \cdots E_s$ are the only characters of G which contains φ_i and φ_j with different multiplicities for some i and j (Suzuki [10]).

B has a linear character $\zeta \neq 1$ satisfying the property that the restriction of ζ of H is invariant under w. Then the character induced from ζ is not irreducible, but a sum of two irreducible characters X and Y. Suppose that either X or Y is exceptional. Then $1^* - \zeta^*$ is the sum of at most four irreducible characters and contains all the exceptional characters (note that the inner product $\langle 1^* - \zeta^*, E_i - E_j \rangle_G = 0$ and a character of degree m can not be exceptional). Since $s \geqq 6$, this is impossible. If both restrictions $X|B$ and $Y|B$ contain φ_i, then the degrees of these two characters are not smaller than $(q-1)q \cdot \frac{q+1}{2}$. On the other hand, the sum of these degrees is equal to $m+1 = q \cdot \frac{q^2+1}{2} + 1$. This is impossible as $q \geqq 3$. Hence at least one of them, say $X|B$, does not contain φ_i. This implies that the kernel K of the representation with character X contains R.

By the double transitivity of G, $|K|$ is divisible by $1+m$. Therefore $G = H \cdot U \cdot K$. Hence there exists a normal subgroup $N \neq G$, such that $N \supset U$. Let N_0 be the minimal normal subgroup of G containing U. Then $|N_0| = md(m+1)$ where d is a divisor of $q-1$. If $d=1$, N_0 contains a regular normal subgroup of order $m+1$. This is not the case. Hence $d > 1$. Then we apply the same argument as before to N_0 in place of G. We conclude that N_0 contains a normal subgroup $N_1 \neq N_0$ satisfying $N_1 \supset U$. Since $G = H \cdot N_0$, N_0 contains a normal subgroup N_2 of G satisfying $N_2 \supset U$. This is against the minimal nature of N_0. Thus we have got a final contradiction.

References

[1] R. Brauer, Some applications of the theory of blocks of characters of finite groups III. J. of Algebra, **3** (1966), pp. 225–255.
[2] ———— and M. Suzuki, On finite groups of even order whose 2-Sylow group is a quaternion group. Proc. Nat. Acad. Sci., **45** (1959), pp. 1757–1759.
[3] L.E. Dickson, *Linear groups*. New York, Dover (1958).
[4] W. Feit, On a class of doubly transitive permutation groups. Ill. J. Math., **4** (1960), pp. 170–186.
[5] D.G. Higman, Finite permutation group of rank 3. Math. Zeit, **86** (1964), pp. 146–156.

[6] N. Ito, On a class of doubly transitive permutation groups. Ill. J. Math., **6** (1962), pp. 341–352.
[7] ——, On doubly transitive groups of degree n and order $2(n-1)n$. Nagoya Math. J., **27-1** (1966), pp. 409–417.
[8] R. Ree, Sur une famille de groupes de permutations doublement trasitifs. Canadian J. of Math., **16** (1964), pp. 797–819.
[9] I. Schur, Untersuchungen uber die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. J. fur Math., **132** (1907), pp. 85–137.
[10] M. Suzuki, On finite groups with cyclic Sylow subgroups for all odd primes. Amer. J. of Math., **77** (1955), pp. 657–691.
[11] ————, A characterization of the 3-dimensional projective unitary group over a finite field of odd characteristic. J. of Algebra, **2** (1965), pp. 1–14.
[12] J.G. Thompson, Finte groups with fixed-point-free automorphisms of prime order. Proc. Nat. Acad. Sci., **45** (1959), pp. 578–581.
[13] H.N. Ward, On Ree's series of simple groups. Trans. Amer. Math., **121** (1966), pp. 62–89.
[14] H. Zassenhaus, Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen. Hamb. Abh., **11** (1936), pp. 17–40.

Added in proof.

Quite recently O'nan [15] has characterized the simple groups $U_3(q)$, q odd, in terms of their doubly transitive permutation representation. However the case $q=5$ is exceptional.

[15] M. O'nan, A characterization of the three-dimensional projective unitary group over a finite field, (to appear).

Nagoya University
and
The Institute for Advanced Study