J. Math. Soc. Japan
Vol. 23, No. 1, 1971

A characterization of the simple groups $\mathfrak{A}_7$ and $\mathfrak{M}_{11}$

By Hiroyoshi YAMAKI

(Received May 23, 1970)

§ 1. Introduction

It is well known that the alternating group $\mathfrak{A}_7$ of degree seven and the Mathieu simple group $\mathfrak{M}_{11}$ of degree eleven are doubly transitive permutation groups in which the stabilizers of two points are isomorphic, as a group, to the alternating groups of degree five (cf. Lüneburg [**9**; p. 95]). The purpose of this paper is to prove the following theorem.

THEOREM. *Let $\mathfrak{G}$ be a doubly transitive permutation group on the set $\Omega=\{1, 2, \cdots, n\}$ containing no regular normal subgroup. If the stabilizer $\mathfrak{R}$ of the set of points* 1 *and* 2 *is isomorphic, as a group, to the alternating group of degree five, then one of the following holds.*

(1) $n=7$ *and* $\mathfrak{G}$ *is* $\mathfrak{A}_7$,

(2) $n=12$ *and* $\mathfrak{G}$ *is* $\mathfrak{M}_{11}$.

The proof of this theorem is similar to that of our paper [**10**].

NOTATION. Let $\mathfrak{X}$ and $\mathfrak{Y}$ be the subsets of $\mathfrak{G}$. $\mathfrak{J}(\mathfrak{X})$ will denote the set of all the fixed points of $\mathfrak{X}$ and $\alpha(\mathfrak{X})$ is the number of points in $\mathfrak{J}(\mathfrak{X})$. $\mathfrak{X}\sim\mathfrak{Y}$ means that $\mathfrak{X}$ is conjugate to $\mathfrak{Y}$ in $\mathfrak{G}$. All other notations are standard.

§ 2. Preliminaries

Firstly we consider the following situation (*).

(*) *Let $\mathfrak{G}$ be a doubly transitive permutation group on the set $\Omega=\{1, 2, \cdots, n\}$ and $\mathfrak{R}$ be the stabilizer of the set of points* 1 *and* 2. *Moreover $\mathfrak{R}$ contains an involution τ and every involution of $\mathfrak{R}$ is conjugate to τ in $\mathfrak{R}$.*

Since $\mathfrak{G}$ is doubly transitive on Ω, it contains an involution I with the cycle structure $(1, 2)\cdots$ which normalizes $\mathfrak{R}$. Let $\mathfrak{H}$ be the stabilizer of the point 1. Then we have the following decomposition of $\mathfrak{G}$.

$$\mathfrak{G}=\mathfrak{H}\cup\mathfrak{H}I\mathfrak{H} \tag{2.1}$$

Let $g(2)$, $h(2)$ and d denote the number of involutions in $\mathfrak{G}$, $\mathfrak{H}$ and the coset $\mathfrak{H}IH$ for $H\in\mathfrak{H}$, respectively. Then d is the number of elements in $\mathfrak{R}$ inverted by I, that is, the number of involutions in $\mathfrak{G}$ with the cycle structure $(1, 2)\cdots$, and the following equality is obtained from (2.1).

$$g(2)=h(2)+d(n-1) \tag{2.2}$$

Let τ keep i ($i \geqq 2$) points of Ω unchanged. So we may put $\mathfrak{Z}(\tau)=\{1, 2, \cdots, i\}$. The group $C_{\mathfrak{G}}(\tau)$ is doubly transitive on $\mathfrak{Z}(\tau)$ by a theorem of Witt [**5**; p. 150] and then we have $|C_{\mathfrak{G}}(\tau)|=i(i-1)|C_{\mathfrak{G}}(\tau)\cap\mathfrak{K}|$ and $|C_{\mathfrak{H}}(\tau)|=(i-1)|C_{\mathfrak{G}}(\tau)\cap\mathfrak{K}|$. Hence there exist $(\mathfrak{G}: C_{\mathfrak{G}}(\tau))=n(n-1)|\mathfrak{K}|/i(i-1)|C_{\mathfrak{K}}(\tau)|$ involutions in $\mathfrak{G}$ each of which is conjugate to τ.

At first, let us assume that n is odd. Let $h^*(2)$ be the number of involutions in $\mathfrak{H}$ leaving only the point 1 fixed. Thus from (2.2) the following equality is obtained.

$$h^*(2)n+(\mathfrak{G}: C_{\mathfrak{G}}(\tau))=(\mathfrak{H}: C_{\mathfrak{H}}(\tau))+h^*(2)+d(n-1) \tag{2.3}$$

Hence we have

$$n=i(\mathfrak{K}: C_{\mathfrak{K}}(\tau))^{-1}\{(d-h^*(2))i-(d-h^*(2))+(\mathfrak{K}: C_{\mathfrak{K}}(\tau))\}. \tag{2.4}$$

Next, let us assume that n is even. Let $g^*(2)$ be the number of involutions in $\mathfrak{G}$ which are semi-regular on Ω. Then corresponding to (2.3) the following equality is obtained from (2.2).

$$g^*(2)+(\mathfrak{G}: C_{\mathfrak{G}}(\tau))=(\mathfrak{H}: C_{\mathfrak{H}}(\tau))+d(n-1) \tag{2.5}$$

Hence we have

$$n=i(\mathfrak{K}: C_{\mathfrak{K}}(\tau))^{-1}\{(d-g^*(2)/n-1)i-(d-g^*(2)/n-1)+(\mathfrak{K}: C_{\mathfrak{K}}(\tau))\}. \tag{2.6}$$

Put $\beta=d-h^*(2)$, if n is odd and put $\beta=d-g^*(2)/n-1$, if n is even.

PROPOSITION 1. *Let $\mathfrak{G}$ satisfy* (*). *Then*

$$n=i(\mathfrak{K}: C_{\mathfrak{K}}(\tau))^{-1}\{\beta i-\beta+(\mathfrak{K}: C_{\mathfrak{K}}(\tau))\}.$$

Moreover i is even if n is even and i is odd if n is odd.

PROOF. The result follows from (2.4) and (2.6).

PROPOSITION 2 (Kimura [7]). *In our situation* (*), *β is the number of involutions with the cycle structure* $(1, 2)\cdots$ *each of which is conjugate to τ. Moreover* $\beta>0$.

PROOF. Let β' be the number of involutions with the cycle structure $(1, 2)\cdots$ each of which is conjugate to τ. Then

$$\beta'(n-1)+(\mathfrak{H}: C_{\mathfrak{H}}(\tau))=(\mathfrak{G}: C_{\mathfrak{G}}(\tau)).$$

This implies that

$$\beta'=(\mathfrak{K}: C_{\mathfrak{K}}(\tau))(n-i)/i(i-1)=\beta.$$

Since $\mathfrak{G}$ is doubly transitive on Ω, β must be positive.

PROPOSITION 3 (Galois). *Let $\mathfrak{G}$ be a doubly transitive group of degree n. If $\mathfrak{G}$ contains a solvable normal subgroup, then $\mathfrak{G}$ contains a regular normal* *subgroup and n is a prime power.*

PROOF. See Huppert [5; p. 159].

In the following of this paper, let $\mathfrak{G}$ be a group satisfying the condition of our theorem and we use the same notation as the preceding paragraph. Clearly $\mathfrak{G}$ satisfies the condition (*).

Since $\mathfrak{K}$ is $\mathfrak{A}_5$, $\mathfrak{K}$ is generated by the elements K, τ and μ subject to the following relations:

$$K^3=\tau^2=\mu^2=(K\tau)^3=(\tau\mu)^3=(K\mu)^2=1 \tag{2.7}$$

Put $\tau_1=K^{-1}\tau K$ and $\mathfrak{B}=\langle\tau, \tau_1\rangle$. Then $\mathfrak{B}$ is a four group and a Sylow 2-subgroup of $\mathfrak{K}$. Since the number of Sylow 2-subgroup of $\mathfrak{K}$ is odd, we may assume that $[I, \mathfrak{B}]\subset\mathfrak{B}$ and $[I, \tau]=1$. Moreover $|C_{\mathfrak{K}}(\tau)|=4$, $|C_{\mathfrak{G}}(\tau)|=4(i-1)i$ and $|C_{\mathfrak{H}}(\tau)|=4(i-1)$. Proposition 1 implies that $n=i(\beta i-\beta+15)/15$.

LEMMA 1. *One of the following holds:*

(1) $I\tau_1 I=\tau\tau_1$, $IKI=K^{-1}$, $[I, \mu]=1$, $d=10$,

$$I\sim IK\sim IK^2\sim I\tau K\tau\sim I\tau K^2\tau\sim I\mu\tau K\tau\mu$$
$$\sim I\mu\tau K^2\tau\mu\sim I\tau\sim I\mu\tau\mu\sim I\mu .$$

(2) $[I, \mathfrak{B}]=1$, $IKI=\tau K\tau$, $I\mu I=\tau\mu\tau$, $d=16$,

$$I\sim I\mu K\tau\sim I(\mu K\tau)^2\sim I(\mu K\tau)^3\sim I(\mu K\tau)^4\sim I(\tau_1\mu\tau_1 K)$$
$$\sim I(\tau_1\mu\tau_1 K)^2\sim I(\tau_1\mu\tau_1 K)^3\sim I(\tau_1\mu\tau_1 K)^4\sim I\tau_1\sim I\tau\tau_1$$
$$\sim I(\tau\mu)\sim I(\tau\mu)^2\sim I(\tau_1\tau\mu\tau_1)\sim I\tau_1(\tau\mu)^2\tau_1 .$$

(3) $[I, \mathfrak{K}]=1$, $d=16$,

$$I\tau\sim I\tau_1\sim I\tau\tau_1\sim I\rho^{-j}\tau\rho^j\sim I\rho^{-k}\tau_1\rho^k\sim I\rho^{-s}\tau\tau_1\rho^s$$

where $\rho=\mu K\tau$ *and* $1\leqq j,\ k,\ s\leqq 4$.

PROOF. Since the automorphism group of $\mathfrak{K}$ is the symmetric group of degree five, we may assume that the action of I on $\mathfrak{K}$ is the case (1), (2) or (3) by (2.7). The group $\langle I, \mathfrak{K}\rangle$ is the symmetric group of degree five or the direct product of a cyclic group of order 2 and the alternating group of degree five. Now the results follow from the structure of $\langle I, \mathfrak{K}\rangle$. Note that in the case (1) all involutions are conjugate in $\mathfrak{G}$. This proves our lemma.

LEMMA 2. $\beta=1$, 10, 15 *or* 16.

PROOF. If the case (1) of Lemma 1 holds, then $h^*(2)=g^*(2)=0$ and $\beta=d=10$. Assume that the case (2) of Lemma 1 holds. Thus if $I\sim I\tau$, then $h^*(2)=g^*(2)=0$ and $\beta=d=16$. If $I\nsim I\tau$, then $\beta=15$ or $\beta=1$ accordingly $\alpha(I)\geqq 2$ or $\alpha(I)<2$. The case (3) of Lemma 1 is the same as the case (2) of Lemma 1. This proves our lemma.

LEMMA 3. *If $\alpha(\tau)>\alpha(\mathfrak{V})$, then one of the following holds.*

(1) $i=6$ *and* $C_{\mathfrak{G}}(\tau)/\langle\tau\rangle$ *is* $\mathfrak{A}_5$,

(2) $i=28$ *and* $C_{\mathfrak{G}}(\tau)/\langle\tau\rangle$ *is* $P\Gamma L(2, 8)$,

(3) $i=p^{2m}$ *for some prime* p, $\alpha(\mathfrak{V})=\sqrt{i}=p^m$ *and* $C_{\mathfrak{G}}(\tau)/\langle\tau\rangle$ *contains a regular normal subgroup. Moreover if* i *is odd,* $C_{\mathfrak{G}}(\tau)/\langle\tau\rangle$ *contains unique involution which fixes only one point on* $\mathfrak{J}(\tau)$.

PROOF. Since $C_{\mathfrak{G}}(\tau)/\langle\tau\rangle$ is doubly transitive on $\mathfrak{J}(\tau)$ of degree i and order $2(i-1)i$, the results follow from Ito's theorem [**6**] and its proof.

LEMMA 4. *If $\alpha(\tau)>\alpha(\mathfrak{V})$, then $\beta=10$, 15, or 16.*

PROOF. There exist two points j and k in $\mathfrak{J}(\tau)-\mathfrak{J}(\mathfrak{V})$ such that $\tau_1=(j, k)\cdots$ and so $\tau\tau_1=(j, k)\cdots$. Double transitivity and Lemma 2 imply that $\beta=10$, 15, or 16. This proves our lemma.

§ 3. The case n is odd

In the following if $h^*(2)>0$, then without loss of generality we may assume that $\alpha(I)=1$.

LEMMA 5. *If $h^*(2)=1$, then there exists no group satisfying the condition of our theorem.*

PROOF. Let $\mathfrak{S}$ be a Sylow 2-subgroup of $\mathfrak{G}$ containing I. Since n is odd, I is isolated in $\mathfrak{S}$ with respect to $\mathfrak{G}$. Then it follows from the Z^*-theorem of Glauberman [**5**; p. 628] that I is contained in the center of $\mathfrak{G}/O(\mathfrak{G})$. Proposition 3 implies that $\mathfrak{G}$ contains a regular normal subgroup. This proves our lemma.

LEMMA 6. *If $\alpha(\tau)>\alpha(\mathfrak{V})$, then there exists no group satisfying the condition of our theorem.*

PROOF.[1] By Lemmas 4 and 5, $h^*(2)=0$. Note that $N_{\mathfrak{G}}(\mathfrak{V})$ contains no Sylow 2-subgroup of $\mathfrak{G}$ by Lemma 3. If $[I, \mathfrak{V}]=1$, then $I\mathfrak{K}$ contains no element of order 4 by Lemma 1. Now a Sylow 2-subgroup of $\mathfrak{G}$ is elementary abelian which is impossible. Thus $\langle I, \mathfrak{K}\rangle$ is a symmetric group of degree five. We can consider $\mathfrak{G}$ as a permutation group on the set $\tilde{\Omega}=\{\{i, j\}\mid i, j\in\Omega\}$ of unordered pairs of the points in Ω. Then $\langle I, \mathfrak{K}\rangle$ is the stabilizer of $\{1, 2\}$ in $\tilde{\Omega}$. Let $\mathfrak{U}$ be a four group in $\langle I, \mathfrak{K}\rangle$ with $\mathfrak{U}\nsim\mathfrak{V}$ in $\langle I, \mathfrak{K}\rangle$. If $\alpha(\mathfrak{U})=1$, then by a theorem of Witt [**5**; p. 150] $N_{\mathfrak{G}}(\mathfrak{V})$ is transitive on the set of fixed points of $\mathfrak{V}$ on $\tilde{\Omega}$ which is a union of the $\mathfrak{V}$-orbits of length 2 and the pairs of the fixed points of $\mathfrak{V}$ in Ω. This contradicts $\alpha(\tau)>\alpha(\mathfrak{V})$. If $\alpha(\mathfrak{U})=\alpha(\mathfrak{V})$, then $h^*(2)=0$ implies that every four group fixes $\sqrt{i}$ points in Ω. Let $\mathfrak{S}$ be a Sylow 2-subgroup of $\mathfrak{G}$ contained in $C_{\mathfrak{G}}(\tau)$. If $\mathfrak{S}$ is not a maximal class, $\mathfrak{S}$

1) The idea of this proof is due to R. Noda.

contains a normal four group. This is impossible. Now $\mathfrak{S}$ is dihedral or quasi-dihedral (cf. [**5**; p. 339]). By theorems of Gorenstein-Walter [**3**] and Lüneburg [**8**], we may assume that $\mathfrak{S}$ is quasi-dihedral. On the other hand since $\mathfrak{S}/\langle\tau\rangle$ is a dihedral Sylow 2-subgroup of $C_{\mathfrak{G}}(\tau)/\langle\tau\rangle$, Lemma 3 implies that $C_{\mathfrak{G}}(\tau)$ has a normal 2-complement. Applying theorems of Gorenstein [**2**] and Lüneburg [**8**] we get a contradiction. The proof is complete.

LEMMA 7. *If $\alpha(\tau)=\alpha(\mathfrak{B})$ and $h^*(2)=0$, then $n=7$ and $\mathfrak{G}$ is $\mathfrak{A}_7$.*

PROOF. The group $C_{\mathfrak{G}}(\tau)/\mathfrak{B}$ is a Frobenius group of odd degree i. Let $\mathfrak{S}$ be a Sylow 2-subgroup of $\mathfrak{G}$ containing $\langle I, \mathfrak{B}\rangle$ and contained in $C_{\mathfrak{G}}(\tau)$. Then $\mathfrak{S}/\mathfrak{B}$ is cyclic or generalized quaternion. If $[I, \mathfrak{B}]\neq 1$, then $\mathfrak{S}=\langle I, \mathfrak{B}\rangle$ is dihedral because $I\mathfrak{B}$ is a unique involution in $\mathfrak{S}/\mathfrak{B}$ and applying theorems of Gorenstein-Walter [**3**] and Lüneburg [**8**], $n=7$ and $\mathfrak{G}$ is $\mathfrak{A}_7$. Assume that $[I, \mathfrak{B}]=1$. Then by the same way as in the proof of Lemma 6, $\mathfrak{S}$ is elementary abelian and hence $\mathfrak{S}=\langle I, \mathfrak{B}\rangle$. Therefore $C_{\mathfrak{G}}(\tau)$ is solvable and by theorems of Gorenstein [**1**] and Lüneburg [**8**], we get a contradiction. The proof is complete.

LEMMA 8. *If $\alpha(\tau)=\alpha(\mathfrak{B})$ and $h^*(2)>1$, then there exists no group satisfying the condition of our theorem.*

PROOF. Since $\beta=d-h^*(2)<d-1$, Lemma 2 implies that $\beta=1$. Therefore Lemma 1 yields $[I\tau, \mathfrak{K}]=1$ which is impossible because $\mathfrak{K}$ is simple and $C_{\mathfrak{G}}(I\tau)$ is conjugate to $C_{\mathfrak{G}}(\tau)$ in $\mathfrak{G}$. The proof is complete.

§ 4. The case n is even

LEMMA 9. *If $\alpha(\tau)=\alpha(\mathfrak{B})$, then there exists no group satisfying the condition of our theorem.*

PROOF. Since n is even, $\mathfrak{B}$ is a Sylow 2-subgroup of $\mathfrak{H}$. Assume that $\mathfrak{B}\cap H^{-1}\mathfrak{B}H$ contains τ for some $H\in\mathfrak{H}$. Then $\mathfrak{Z}(\mathfrak{B})$ and $\mathfrak{Z}(H^{-1}\mathfrak{B}H)$ are contained in $\mathfrak{Z}(\tau)$. It follows that $\mathfrak{Z}(\tau)=\mathfrak{Z}(\mathfrak{B})=\mathfrak{Z}(H^{-1}\mathfrak{B}H)$ and hence $\mathfrak{K}$ contains $\mathfrak{B}$ and $H^{-1}\mathfrak{B}H$. Since $\mathfrak{K}$ is $\mathfrak{A}_5$, we have $\mathfrak{B}=H^{-1}\mathfrak{B}H$. This implies that $\mathfrak{H}$ is a (TI)-group in the sense of Suzuki [**12**] and hence $\mathfrak{H}/O(\mathfrak{H})$ is also (TI)-group. By a theorem of Suzuki [**12**; p. 69], $\mathfrak{H}/O(\mathfrak{H})$ is $PSL(2, 4)$ and $O(\mathfrak{H})$ is contained in the center of $\mathfrak{H}$. It follows from $|C_{\mathfrak{H}}(\tau)|=4(i-1)$ that $|O(\mathfrak{H})|=i-1$ and $(\mathfrak{H}: O(\mathfrak{H}))=4(\beta i+15)=60$ which is impossible because $\beta>0$ by Proposition 2. The proof is complete.

In the following we may assume that $\alpha(\tau)>\alpha(\mathfrak{B})$.

LEMMA 10. *If $i=6$ or 28, then there exists no group satisfying the condition of our theorem.*

PROOF. Note that by a Brauer-Wielandt's formula [**13**] we have

$$|O(\mathfrak{H})|=|C(\tau)\cap O(\mathfrak{H})|^3/|C(\mathfrak{B})\cap O(\mathfrak{H})|^2$$

and since $\mathfrak{K}$ is simple, $O(\mathfrak{H})\cap\mathfrak{K}=\{1\}$. Assume that $i=6$. Then $|C_{\mathfrak{H}}(\tau)|=2^2\cdot 5$, $|\mathfrak{H}|=2^2\cdot 3\cdot 5^3$, $2^2\cdot 3\cdot 5^2\cdot 7$ or $2^2\cdot 3\cdot 5\cdot 37$ and $|O(\mathfrak{H})|=1$ or 5. Assume that $i=28$. Then $|C_{\mathfrak{H}}(\tau)|=2^2\cdot 3^3$, $|\mathfrak{H}|=2^2\cdot 3^3\cdot 5\cdot 59$, or $2^2\cdot 3^4\cdot 5\cdot 29$ and $|O(\mathfrak{H})|$ is a factor of 3^3. On the other hand, in both cases, $\mathfrak{H}/O(\mathfrak{H})$ is isomorphic to a subgroup of $P\Gamma L(2, q)$ containing $PSL(2, q)$ for some q by a theorem of Gorenstein-Walter [3] which is impossible. This proves our lemma.

LEMMA 11. *If the case* (3) *of Lemma* 3 *holds, then* $n=12$ *and* $\mathfrak{G}$ *is* $\mathfrak{M}_{11}$.

PROOF. The group $\mathfrak{B}$ is a Sylow 2-subgroup of $\mathfrak{H}$ and hence $C_{\mathfrak{H}}(\tau)$ has a normal 2-complement. Since $C_{\mathfrak{G}}(\tau)/\langle\tau\rangle$ is a solvable doubly transitive group on $\mathfrak{J}(\tau)$ of even degree, it follows from a theorem of Huppert [4] that $C_{\mathfrak{H}}(\tau)$ has a cyclic normal 2-complement. Applying a theorem of Gorenstein-Walter [3], $\mathfrak{H}/O(\mathfrak{H})$ is $PSL(2, q)$ for some q. By Lemma 3, $\alpha(\mathfrak{B})=\sqrt{i}=2^m$ and $|N_{\mathfrak{G}}(\mathfrak{B})|=12(\sqrt{i}-1)\sqrt{i}$, $|N_{\mathfrak{H}}(\mathfrak{B})|=12(\sqrt{i}-1)$, $|C_{\mathfrak{H}}(\mathfrak{B})|=4(\sqrt{i}-1)$. It follows from the structure of $PSL(2, q)$ that $|O(\mathfrak{H})\cap C(\mathfrak{B})|=\sqrt{i}-1$. Put $|O(\mathfrak{H})\cap C(\tau)|=x(\sqrt{i}-1)$. Then x is a factor of $\sqrt{i}+1$ and $|O(\mathfrak{H})\cap C(\tau_1)|=|O(\mathfrak{H})\cap C(\tau\tau_1)|=x(\sqrt{i}-1)$. By a formula of Brauer-Wielandt [13] we have

$$\begin{aligned}|O(\mathfrak{H})|\,|O(\mathfrak{H})\cap C(\mathfrak{B})|^2&=|O(\mathfrak{H})\cap C(\tau)|\,|O(\mathfrak{H})\cap C(\tau_1)|\,|O(\mathfrak{H})\cap C(\tau\tau_1)|\\&=x^3(\sqrt{i}-1)^3\end{aligned}$$

and therefore $|O(\mathfrak{H})|=x^3(\sqrt{i}-1)$. Now we have

$$4(\sqrt{i}+1)(\beta i+15)/x^3=q(q-1)(q+1)/2\,. \tag{4.1}$$

Put $\bar{\mathfrak{H}}=\mathfrak{H}/O(\mathfrak{H})$ and in the natural epimorphism $\mathfrak{H}\to\bar{\mathfrak{H}}$, let $\bar{\tau}$, $\overline{C_{\mathfrak{H}}(\tau)}$ be the images of τ, $C_{\mathfrak{H}}(\tau)$, respectively. Since $C(\bar{\tau})\cap\bar{\mathfrak{H}}=\overline{C_{\mathfrak{H}}(\tau)}$, we have

$$(q+e)/4=(\sqrt{i}+1)/x \tag{4.2}$$

where $e=1$ or -1. It follows from (4.1) and (4.2) that

$$2(\beta i+15)/x^2=q(q-e) \tag{4.3}$$

and therefore x is also a factor of $\beta i+15$. Now $\beta i+15\equiv\beta+15(\mathrm{mod.}\sqrt{i}+1)$ implies that x is a factor of $\beta+15$. It follows from $\beta=10$, 15, or 16 that x must be 1, 3, 5, 15, 25, or 31. On the other hand, (4.2) and (4.3) imply that

$$(\beta-8)i-2(8-3ex)\sqrt{i}-(x-7e)(x+e)=0$$

and hence

$$\sqrt{i}=\{(8-3ex)\pm\sqrt{(\beta+1)x^2-6e\beta x+120-7\beta}\}/(\beta-8)\,.$$

Put $f(x, \beta)=(\beta+1)x^2-6e\beta x+120-7\beta$. Since $f(x, \beta)$ is a quadratic number, the possibilities of $f(x, \beta)$ are as follows.

$$f(1, 10) = 1, \text{ or } 121, \qquad f(5, 10) = 25, \text{ or } 625,$$
$$f(1, 15) = 121, \qquad f(1, 16) = 121,$$
$$f(31, 16) = 19321.$$

Since $\sqrt{i} = 2^m$, we must have $f(1, 10) = 1$ and therefore

$$i = 4, \qquad q = 11, \qquad n = 12.$$

Thus $\mathfrak{H}$ is $PSL(2, 11)$ and $\mathfrak{G}$ contains no regular normal subgroup by Proposition 3. Now $\mathfrak{G}$ is a simple group of order 7920. By a theorem of Parrott [11], $\mathfrak{G}$ is $\mathfrak{M}_{11}$. This proves our lemma.

The proof of our theorem is complete.

Osaka University

References

[1] D. Gorenstein, Finite groups in which Sylow 2-subgroups are abelian and centralizers of involutions are solvable, Canad. J. Math., **17** (1965), 860–896.

[2] D. Gorenstein, Finite groups the centralizers of whose involutions have normal 2-complements, Canad. J. Math., **21** (1969), 335–357.

[3] D. Gorenstein and J.H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups, I, II, III, J. Algebra, **2** (1965), 85–151, 218–270, 334–393.

[4] B. Huppert, Zweifach transitive auflösbare Permutationsgruppen, Math. Z., **68** (1957), 126–150.

[5] B. Huppert, Endliche Gruppen I, Springer, Berlin, 1967.

[6] N. Ito, On doubly transitive groups of degree n and order $2(n-1)n$, Nagoya Math. J., **27** (1966), 409–417.

[7] H. Kimura, On doubly transitive permutation groups of degree n and order $2p(n-1)n$, I, II, Osaka J. Math., **7** (1970), (to appear).

[8] H. Lüneburg, Charakterisierungen der endlichen desarguesschen projectiven Ebenen, Math. Z., **85** (1964), 419–450.

[9] H. Lüneburg, Transitive Erweiterungen endlicher Permutationsgruppen, Springer, Berlin, 1969.

[10] R. Noda and H. Yamaki, A characterization of the alternating groups of degrees six and seven, Osaka J. Math., **7** (1970), (to appear).

[11] D. Parrott, On the Mathieu groups M_{22} and M_{11}, J. Austral. Math. Soc., **11** (1970), 69–81.

[12] M. Suzuki, Finite groups of even order in which Sylow 2-groups are independent, Ann. Math., **80** (1964), 58–77.

[13] H. Wielandt, Beziehungen zwischen den Fixpunktzahlen von Automorphismengruppen einer endlichen Gruppe, Math. Z., **73** (1960), 146–158.