On the Alternating Groups

Dedicated to Prof. Shôkichi Iyanaga on his 60th birthday

By Takeshi KONDO

Introduction. Let A_m be the alternating group on m letters $\{1, 2, \cdots, m\}$. Put $m=4n+r$, where n and r are non-negative rational integers and $0\leq r\leq 3$. Define n elements α_k $(1\leq k\leq n)$ of A_m as follows:

$$\alpha_k=(1, 2)(3, 4)\cdots(4k-3, 4k-2)(4k-1, 4k) .$$

In the present paper, we shall prove the following result.

THEOREM. *Let G be a finite group satisfying the following conditions:*

There exist n involutions $\tilde{\alpha}_1, \tilde{\alpha}_2, \cdots, \tilde{\alpha}_n$ in G and a one-to-one mapping φ from $\bigcup_{i=1}^{n} C_{A_m}(\alpha_i)$ to $\bigcup_{i=1}^{n} C_G(\tilde{\alpha}_i)$ such that φ induces an isomorphism between $C_{A_m}(\alpha_i)$ and $C_G(\tilde{\alpha}_i)(1\leq i\leq n)$. Here $\bigcup_{i=1}^{n} C_{A_m}(\alpha_i)$ (resp. $\bigcup_{i=1}^{n} C_G(\tilde{\alpha}_i)$) denotes the set-theoretic union in A_m (resp. G).

Then if $m\geq 8$, G is isomorphic to A_m.

This is a generalization of W. J. Wong [6]. The idea of the proof is due to D. Held [4]. Further, in our proof, we shall use the results of W. J. Wong [6] and D. Held [3], which imply our theorem for $m=8, 9$ and 10.

The author wishes to express his hearty thanks to Professor H. Nagao, who proves a lemma (1.8).

Throughout the present paper, $m, n, r, \alpha_k(1\leq k\leq n)$, φ and G will be used in the same meaning as above. S_l (resp. A_l) denote the symmetric group (resp. the alternating group) on l letters. For a set Ω, S_Ω (resp. A_Ω) denote the symmetric group (resp. the alternating group) on the set Ω. If $x, y, \cdots$ are elements of a group H, $\langle x, y, \cdots\rangle$ denotes a subgroup of H generated by $x, y, \cdots$. Moreover, $[x, y]=x^{-1}y^{-1}xy$ and $x^y=y^{-1}xy$.

§ 1. Preliminaries

1.1. We shall define some elements in A_m as follows:

$$\pi_k=(4k-3,\ 4k-2)(4k-1,\ 4k) \qquad (1\leq k\leq n),$$
$$\pi_k'=(4k-3,\ 4k)(4k-2,\ 4k-1) \qquad (1\leq k\leq n) ,$$

$$\mu_i=(1,2)(4i+1,4i+2) \qquad (1\leq i\leq n-1)\ ,$$

$$\mu_n=\begin{cases} 1, & \text{if } r=0 \text{ or } 1 \\ (1,2)(4n+1,4n+2), & \text{if } r=2 \text{ or } 3\ , \end{cases}$$

$$\tau_{ij}=(4i-3,4j-3)(4i-2,4j-2)(4i-1,4j-1)(4i,4j) \qquad (1\leq i,\ j\leq n \text{ and } i\neq j)\ ,$$

$$u_i=(4i-3,\ 4i-2,\ 4i-1) \qquad (1\leq i\leq n)\ ,$$

$$u_{n+1}=\begin{cases} 1, & \text{if } r=0, 1 \text{ or } 2\ , \\ (4n+1,4n+2,4n+3)\ , & \text{if } r=3\ . \end{cases}$$

We note that $\alpha_k=\pi_1\pi_2\cdots\pi_k$ $(1\leq k\leq n)$. We have

(1) $$C_{A_m}(\alpha_k)=(W_k\times X_k)\langle\mu_k\rangle \qquad (1\leq k\leq n)\ .$$

Here, W_k is the centralizer of α_k in $A_{\Omega'}$, $W_k\langle\mu_k\rangle$ is isomorphic to the centralizer of α_k in $S_{\Omega'}$, $X_k=A_{\Omega''}$ and $X_k\langle\mu_k\rangle$ is isomorphic to $S_{\Omega''}$ where $\Omega'=\{1,2,\cdots,4k\}$ and $\Omega''=\{4k+1,\cdots,m\}$.

1.2. LEMMA. *Put* $S=\langle\pi_1,\pi_1',\cdots,\pi_n,\pi_n'\rangle$. *Then we have* $C_{A_m}(S)=S\times X_n$.

PROOF. From (1), it follows that

$$C_{A_m}(\langle\pi_1,\pi_2,\cdots,\pi_k\rangle)=(\langle\pi_1,\pi_1',\cdots,\pi_k,\pi_k'\rangle\times X_k)\langle\mu_1,\mu_2,\cdots,\mu_k\rangle\ .$$

In particular, we have

$$C_{A_m}(\langle\pi_1,\pi_2,\cdots,\pi_n\rangle)=(S\times X_n)\langle\mu_1,\mu_2,\cdots,\mu_n\rangle\ .$$

Since $[\pi'_{i+1},\mu_i]=\pi_i$ $(1\leq i\leq n-1)$, we get

$$C_{A_m}(S)=S\times X_n\ .$$

1.3. LEMMA. *The representatives of conjugacy classes of involutions of* $C_{A_m}(\alpha_n)$ *are as follows:* (i) $\pi_1\pi_2\cdots\pi_s\pi'_{s+1}\cdots\pi'_{s+t}$ $(0<s+t\leq n)$ *and* $\pi_1'\pi_2'\cdots\pi_n'\pi_n$, *when* $r=0$ *or* 1, *and* (ii) $\pi_1\pi_2\cdots\pi_s\pi'_{s+1}\cdots\pi'_{s+t}$ $(0<s+t\leq n)$ *and* $\pi_1\pi_2\cdots\pi_s\pi'_{s+1}\cdots\pi'_{s+t}\mu_{n-1}\mu_n$ $(0\leq s\leq n-1,\ 0\leq t\leq n-1-s)$, *when* $r=2$ *or* 3.

PROOF. The fusion of a 2-Sylow-group of $C_{A_m}(\alpha_n)$ is the same as that of $W_n\langle\mu_n\rangle$. The conjugacy classes of $W_n\langle\mu_n\rangle$ are known (e.g. see W. Specht [5]). From this our lemma follows. The details are omitted.

1.4. LEMMA. *For a group* H, *let* $2^{r(H)}$ *be the largest of the order of elementary abelian 2-subgroups of* H. *Then we have*

(i) $r(H_1\times H_2)=r(H_1)+r(H_2)$

(ii) $r(S_l) \leq \frac{l}{2}$.

PROOF. Let A be a maximal elementary abelian 2-subgroup of $H_1 \times H_2$. Take a non-identity element x_1x_2 of A, where $x_i \in H_i$ (i=1, 2). If $A \ni y = y_1y_2$, we have, $x_1x_2 = (x_1x_2)^y = x_1^{y_1}x_2^{y_2}$. This implies that $x_1^y = x_1^{y_1} = x_1$ and $x_2^y = x_2^{y_2} = x_2$. By the maximality of A, $x_i \in A$ $(i=1, 2)$. Hence we get $A = A_1 \times A_2$, where $A_i = H_i \cap A$ $(i=1, 2)$. This proves (i). Let B be a maximal elementary abelian 2-subgroup of S_l. Assume that any element of B has no fixed letter. Then we have $|B| \leq l$. Since $l \leq 2^{l/2}$, we get $r(B) \leq l/2$. Hence we may assume that an element x of B has at least one fixed letter. Obviously, we may assume that l is even. If x has $2k$ fixed letters $(k \geq 1)$, we have $B \subseteq C_{S_l}(x) \cong U \times S_{l-2k}$, where U has a 2-Sylow-group isomorphic to that of S_{2k}. By induction on l, we get $r(U) \leq k$ and $r(S_{l-2k}) \leq (l-2k)/2$. From (i), if follows that $r(B) \leq r(U) + r(S_{l-2k}) \leq l/2$. This proves (ii).

1.5. Let H be a subgroup of S_l which is of the form $S^{(1)} \times S^{(2)} \times \cdots \times S^{(l')} \times S^{(l'+1)}$, where $S^{(i)} \cong S_4$ $(1 \leq i \leq l')$ and $S^{(l'+1)} \cong S_k$. If the length of the orbits of $S^{(i)} (1 \leq i \leq l')$ (resp. $S^{(l'+1)}$) is 1 or 4 (resp. 1 or k) and $S^{(i)} (1 \leq i \leq l')$ (resp. $S^{(l'+1)}$) has precisely one orbit of length 4 (resp. k), we say that H is naturally imbedded in S_l.

1.6. LEMMA. *Let H be as in* (1.5). *Then we have $l \geq 4l'$. Further, if $k=2$ or 3, we have $l \geq 4l'+2$.*

PROOF. Since $r(S_l) \leq l/2$ and $r(H) \geq 2l'$, we get $l \geq 4l'$. If $k=2$ or 3, we have $r(H) = 2l'+1$. Hence, we get $l \geq 4l'+2$.

1.7. LEMMA. *Let H be as in* (1.5). *If $k=0$ or 3 and N is normal subgroup of H, we have $H' \cap N \neq 1$, where H' is the commutator subgroup of H.*

PROOF. Take an element $x_1x_2 \cdots x_{l'+1}$ of H $(x_i \in S^{(i)})$. If $x_i \neq 1$, there exists an element x_i' of $S^{(i)}$ such that $[x_i, x_i'] \neq 1$. Then $1 \neq [x_i, x_i'] = [x_1x_2 \cdots x_{l'+1}, x_i'] \in H' \cap N$.

1.8. LEMMA. *Let H be as in* (1.5). *Assume that*

(i) $l-1 = 4l'+k$ $(0 \leq k \leq 3)$ *and* $l \neq 6, 7$,

(ii) *$S^{(i)}$ is conjugate in S_l to $S^{(j)}$ $(1 \leq i, j \leq l')$ and $S^{(l'+1)}$ is contained in a subgroup conjugate in S_l to $S^{(i)}$ for every i $(1 \leq i \leq l')$,*

(iii) $S^{(i)} \not\subseteq A_l$ $(1 \leq i \leq l'+1)$.

Then H is naturally imbedded in S_l.

PROOF. Let Ω be a set of l letters on which S_l operates. $S^{(1)}$ has at least one orbit Δ_1 on which $S^{(1)}$ operates faithfully. Let $\Delta_1, \Delta_2, \cdots, \Delta_\rho$ be all distinct orbits of $S^{(1)}$, each of which affords a permutation representation of $S^{(1)}$ equivalent to that of $S^{(1)}$ on Δ_1. Put $\Omega - \bigcup_{i=1}^{\rho} \Delta_i = \{i_1, i_2, \cdots, i_\sigma\}$. Define a set

$$\bar{\Omega} = \{\Delta_1, \Delta_2, \cdots, \Delta_\rho, i_1, i_2, \cdots, i_\sigma\}$$

of $\rho+\sigma$ elements. Put $K = S^{(2)} \times \cdots \times S^{(l')}$. K induces a permutation respresentation on $\bar{\Omega}$. Let N be the kernel of this representation. If $S^{(i)} \cap N \neq 1$ $(2 \leq i \leq \tau)$ and $S^{(i)} \cap N = 1$ $(\tau+1 \leq i \leq l')$, it is easy to see that

$$(2) \qquad N \cap (S^{(\tau+1)} \times \cdots \times S^{(l')}) = 1$$

and $|N \cap S^{(i)}| \geq 4$ $(2 \leq i \leq \tau)$. If c is the order of the centralizer in S_{Δ_i} of the representation of $S^{(1)}$ on Δ_i, we have

$$(3) \qquad c^\rho \geq |N| \geq 2^{2(\tau-1)} .$$

We remark that $|\Delta_1| = 4, 6, 8, 12$ or 24. Put $\lambda = |\Delta_1|$.

Case (α), $\lambda=4$. Since $c=1$ in this case, we have $N=1$. Hence K operates faithfully on $\bar{\Omega}$. By (1.6), we have $4(l'-1) \leq \rho+\sigma$. Since $l=4\rho+\sigma$, we obtain $l-4l' \geq 3\rho-4$. If $\rho \geq 3$, we get $l-5 \geq 4l'$, which is impossible on account of the assumption (i).

Subcase (α_1), $\rho=2$. First, we assume $k \geq 2$. Since K' is generated by elements of order 3 and $\rho=2$, K' leaves Δ_i invariant $(i=1, 2)$. From this and $c=1$, it follows that every element of K' fixes any element of Δ_i $(i=1, 2)$. On the other hand, K operates on $\{i_1, i_2, \cdots, i_{l-8}\}$. If the kernel N_0 of this representation is non-trivial, it follows from (1.7) that $K' \cap N_0 \neq 1$. This is impossible since K operates faithfully on Ω. Hence K operates faithfully on $\{i_1, i_2, \cdots, i_{l-8}\}$. From (1.6), we get $4(l'-1) \leq l-8$. This is imposible if $k \leq 2$. Next, we assume $k=3$. Put

$$K_1 = S^{(2)} \times \cdots \times S^{(l')} \times S^{(l'+1)} ,$$

where $S^{(l'+1)} \cong S_3$. By the same argument as above, K_1 operates faithfully on $\{i_1, i_2, \cdots, i_{l-8}\}$. From (1.6) we get $4(l'-1)+2 \leq l-8$, which is impossible on account of the assumption (i).

Subcase (α_2), $\rho=1$. From the assumption (ii), it follows that $S^{(i)}$ $(1 \leq i \leq l')$ has unique faithful orbit $\Delta^{(i)}$ of length 4 and $\Delta^{(i)} \cap \Delta^{(j)} = \phi$ $(i \neq j)$. By the assumption (iii), $S^{(i)}$ $(1 \leq i \leq l')$ fixes any element in $\Omega - \bigcup_{i=1}^{l'} \Delta^{(i)}$. This implies our lemma in the case $\lambda=4$.

Case (β), $\lambda=6$. Since $c=2$, from (3) we get $(\rho/2)+1\geq\tau$. Then it follows from (2) and (1.6) that $4(l'-\tau)\leq\rho+\sigma$. Since $l=6\rho+\sigma$, we get $l-4l'\geq 3\rho-4$. If $\rho\geq 3$, we have $l-5\geqq 4l'$, which is impossible.

Subcase (β_1), $\rho=2$. By the same argument as in the subcase (α_1), K operates faithfully on $\{i_1, i_2 \cdots, i_{l-12}\}$. Then (1.6) yields that $4(l'-1)\leq l-12$, which is impossible.

Subcase (β_2), $\rho=1$. By the assumption (ii), $S^{(i)}$ $(1\leq i\leq l')$ has unique faithful orbit $\Delta^{(i)}$ of length 6 and we have $\Delta^{(i)}\cap\Delta^{(j)}=\phi$ $(i\neq j)$. This implies that $l=|\Omega|\geq 6l'$. If $k\leq 2$, it follows that $l=6$ or 7, which is impossible on account of the assumption (i). If $k=3$, $S^{(l'+1)}$ has a faithful orbit Δ such that $|\Delta|\geq 3$ and $\Delta\cap\Delta^{(i)}=\phi$ $(1\leq i\leq l')$. Hence we have $l=|\Omega|\geq 6l'+3$. This is impossible since $l=4l'+4$.

Case (γ), $\lambda=8$. Since $c=2$, we obtain $(\rho/2)+1\geq\tau$ from (3). By (2) and (1.6) we have $4(l'-\tau)\leq\rho+\sigma$. Since $l=8\rho+\sigma$, we have $l-4l'\geq 5\rho-4$. If $\rho\geq 2$, we get $l-6\geq 4l'$ which is impossible. If $\rho=1$, K operates faithfully on $\{i_1, i_2, \cdots i_{l-8}\}$. (1.6) yields that $4l'\leq l-4$. Then $k=3$ and $K_1=S^{(1)}\times\cdots\times S^{(l'+1)}$ operates faithfully on $\{i_1, i_2, \cdots, i_{l-8}\}$. (1.6) yields that $4(l'-1)+2\leq l-8$, which is impossible.

Case (δ) $\lambda=12$. In this case, we have $c\leq 4$.[1] By (2) and (3) we obtain $4l'\leq 5\rho+\sigma+4$. Since $l=12\rho+\sigma$, we get $l-4l'\geq 7\rho-4$. If $\rho\geq 2$, we have $l-10\geq 4l'$, which is impossible. If $\rho=1$, K operates faithfully on $\{i_1, i_2, \cdots, i_{l-12}\}$. (1.6) yields $4(l'-1)\leq l-12$, which is impossible.

Case (ε), $\lambda=24$. Since $c=24$, we get $2^{5\rho}\geq 24^{\rho}\geq 2^{2(\tau-1)}$ from (3). Hence $5\rho/2+1\geq\tau$. Then we have $l-4l'\geq 13\rho-4$. This yields $l-9\geq 4l'$, which is impossible. This completes the proof of our lemma.

§ 2. Conjugacy classes of involutions of G.

2.1. Let G and φ be as in the introduction. For a subset X of $\bigcup_{k=1}^{n} C_{A_m}(\alpha_k)$, $\tilde{X}$ denotes the image of X by φ.

2.2. LEMMA. *Any involution of $C_G(\tilde{\alpha}_n)$ is conjugate in G to one of $\tilde{\alpha}_1, \tilde{\alpha}_2, \cdots, \tilde{\alpha}_n$.*

PROOF. We shall show that $\tilde{\pi}_1\cdots\tilde{\pi}_s\tilde{\pi}'_{s+1}\cdots\tilde{\pi}'_{s+t}$ (resp. $\tilde{\pi}_1'\cdots\tilde{\pi}_n'\tilde{\pi}_n$) is conjugate to $\tilde{\alpha}_{s+t}$ (resp. $\tilde{\alpha}_n$) in G. Suppose that $s=0$. Since π_t' is conjugate to π_n' in $W_n\langle\mu_n\rangle$ and $\pi_n'^{u_n}=\pi_n$ and $[\pi_i', u_n]=1$ in $C_{A_m}(\alpha_{n-1})$ $(1\leq i\leq n-1)$, $\tilde{\pi}_1'\tilde{\pi}_2'\cdots\tilde{\pi}_t'$ is conjugate to

[1] S_4 has two inequivalent faithful transitive representation of degree 12, one of which has $c=2$ and the other has $c=4$.

$\tilde{\pi}_1' \cdots \tilde{\pi}_{t-1}'\tilde{\pi}_n$ which is conjugate to $\tilde{\pi}_1'\tilde{\pi}_2' \cdots \tilde{\pi}_t'$ in $C_G(\tilde{\alpha}_n)$. Hence we may assume that $s \geq 1$. Since $\pi_i'^{u_i} = \pi_i$ and $[\pi_j', u_i] = 1$ in $C_{A_m}(\alpha_s)$ $(s+1 \leq i, j \leq s+t$ and $i \neq j)$, we get that $\tilde{\pi}_1 \cdots \tilde{\pi}_s\tilde{\pi}_{s+1}' \cdots \tilde{\pi}_{s+t}'$ is conjugate to $\tilde{\alpha}_{s+t}$ in G. Since $\pi_n^{u_n} = \pi_n\pi_n'$ and $[\pi_i', u_n] = 1$ $(1 \leq i \leq n-1)$ in $C_{A_m}(\alpha_{n-1})$, it follows that $\tilde{\pi}_1' \cdots \tilde{\pi}_n'\tilde{\pi}_n$ is conjugate to $\tilde{\alpha}_n$ in G.

Futhermore, $\pi_1\pi_2 \cdots \pi_s\pi_{s+1}' \cdots \pi_{s+t}'\mu_{n-1}\mu_n$ is conjugate to $\pi_1 \cdots \pi_s\pi_{s+1}' \cdots \pi_{s+t}' \times \pi_{s+t+1}$ in $C_{A_m}(\alpha_1)$. From this and the fact obtained above, follows that $\tilde{\pi}_1 \cdots \tilde{\pi}_s\tilde{\pi}_{s+1}' \times \cdots \tilde{\pi}_{s+t}'\tilde{\mu}_{n-1}\tilde{\mu}_n$ is conjugate to $\tilde{\alpha}_{s+t+1}$ in G. Then (1, 3) implies our lemma.

2.3. LEMMA. *A 2 Sylow-subgroup of $C_G(\tilde{\alpha}_n)$ is that of G.*

PROOF. Let D be a 2-Sylow-subgroup of $C_G(\tilde{\alpha}_n)$ and F be that of G containing D. Then we have $D = F \cap C_G(\tilde{\alpha}_n)$. If z is in the center of F, $[z, D] = 1$ and in particular, $[z, \tilde{\alpha}_n] = 1$. Hence we get $z \in Z(D)$. By (2.2), there exists an element x of G such that $z^x = \tilde{\alpha}_k$ for some k. Since $C_G(z)^x = C_G(\tilde{\alpha}_k)$ and

$$|C_G(\tilde{\alpha}_k)|_2 = |C_{A_m}(\alpha)|_2 \leq |C_{A_m}(\alpha_n)|_2 = |C_G(\tilde{\alpha}_n)|_2 \,^{2)},$$

we have $|C_G(z)|_2 \leq |C_G(\tilde{\alpha}_n)|_2 = |D|$. This yields $F = D$.

2.4. LEMMA. *G has n conjugacy classes of involutions whose representatives are $\tilde{\alpha}_1, \tilde{\alpha}_2, \cdots, \tilde{\alpha}_n$.*

PROOF. By (2.2) and (2.3), it is sufficient to see that $\tilde{\alpha}_i$ is not conjugate to $\tilde{\alpha}_j$ $(i \neq j)$. This follows from the fact that $C_{A_m}(\alpha_i)$ is not isomorphic to $C_{A_m}(\alpha_j)$.

§ 3. The proof of the Theorem.

3.1. We shall prove our theorem by induction on m. First, we note that our theorem holds good for $m=8$, 9, or 10. By W. J. Wong's theorem [6], our theorem is true for $m=8$. D. Held [3] proved that, if G_0 is a finite group satisfying the condition that (i) G_0 has no normal subgroup of index 2 and (ii) G_0 has an involution a such that $C_{G_0}(a)$ is isomorphic to $C_{A_8}(\alpha_2)$, then G_0 is isomorphic to A_8, A_9 or a semidirect product of L and E, where $L \cong PSL(2, 7)$, E is an elementary abelian group of order 8 and $G_0 \triangleright E$. It is easy to see that the last group does not satisfy the assumption of our theorem. If $m=9$, our assumption yields that G has no normal subgroup of index 2. This turns out by examining fusion of involutions

2) For a set X, if $|X| = 2^a b$ and $(2\ b) = 1$, $|X|_2 = 2^a$.

of G and applying the focal subgroup theorem. From this it follows that our theorem is true for $m=9$. Similarly, D. Held's theorem [4] yields that if $m=10$, G is isomorphic to A_{10}. Hence we shall assume that $m\geqq 11$.

3.2. LEMMA. *$C_G(\tilde{u}_n)=\langle\tilde{u}_n\rangle\times U_0$, $U_0\cong A_{m-3}$ and U_0 contains $\tilde{\pi}_i$ and $\tilde{\pi}_i'$* $(1\leq i\leq n-1)$.

PROOF. Put $\Omega=\{i\mid 1\leq i\leq m\}-\{4n-3, 4n-2, 4n-1\}$ or $\{i\mid 1\leq i\leq m\}-\{4n+1, 4n+2, 4n+3\}$ according to whether $r\leq 2$ or $r=3$. Then we have $|\Omega|=m-3$.

Case $r\leq 2$. A_Ω contains α_k $(1\leq k\leq n-1)$. For $1\leq k\leq n-1$, we have by (1),

$$C_{A_m}(u_n)\cap C_{A_m}(\alpha_k)=\langle u_n\rangle\times C_{A_\Omega}(\alpha_k)\ .$$

Hence we get

$$C_G(\tilde{u}_n)\cap C_G(\tilde{\alpha}_k)=\langle\tilde{u}_n\rangle\times\widetilde{C_{A_\Omega}(\alpha_k)}\ .$$

Put $\mathfrak{g}=C_G(\tilde{u}_n)/\langle\tilde{u}_n\rangle$. Denote by ψ the canonical homomorphism from $C_G(\tilde{u}_n)$ to $\mathfrak{g}$. Involutions $\psi(\tilde{\alpha}_1)$, $\psi(\tilde{\alpha}_2), \cdots, \psi(\tilde{\alpha}_{n-1})$ of $\mathfrak{g}$ and a mapping $\psi\varphi$ from $C_{A_\Omega}(\alpha_k)$ into $\mathfrak{g}$ satisfy the condition of the theorem with $m-3$ in place of m. By induction assumption, $\mathfrak{g}$ is isomorphic to A_{m-3}. Since the order of the Schur multipliers of A_{m-3} $(m\geqq 11)$ is prime to 3, we have $C_G(\tilde{u}_n)=\langle\tilde{u}_n\rangle\times U_0$, $U_0\cong A_{m-3}$. Since u_n, π_i and π_i' $(1\leq i\leq n-1)$ are contained in $C_{A_m}(\alpha_{n-1})$ and $[u_n, \pi_i]=[u_n, \pi_i']=1$ $(1\leq i\leq n-1)$, U_0 contains $\tilde{\pi}_i$ and $\tilde{\pi}_i'$ $(1\leq i\leq n-1)$.

Case $r=3$. Put $\mathfrak{g}=C_G(\tilde{u}_{n+1})/\langle\tilde{u}_{n+1}\rangle$. If ψ is the canonical homomorphism from $C_G(\tilde{u}_{n+1})$ to $\mathfrak{g}$, involutions $\psi(\tilde{\alpha}_1), \cdots \psi(\tilde{\alpha}_n)$ of $\mathfrak{g}$ and a mapping $\psi\varphi$ from $C_{A_\Omega}(\alpha_k)$ into $\mathfrak{g}$ satisfy the condition of the theorem. In the same way as above, we get

$$C_G(\tilde{u}_{n+1})=\langle\tilde{u}_{n+1}\rangle\times U_1,\quad\text{where}\quad U_1\cong A_{m-3}\ .$$

Since u_n is conjugate to u_{n+1} in $C_{A_m}(\alpha_{n-1})$, $\tilde{u}_n$ is conjugate to $\tilde{u}_{n+1}$ in G. Hence we get

$$C_G(\tilde{u}_n)=\langle\tilde{u}_n\rangle\times U_0,\quad\text{where } U_0\cong A_{m-3}\ .$$

3.3. Put $\tilde{u}_1=\tilde{u}_n^{\tilde{\tau}_{1n}}$. (Note that $\tilde{u}_1$ has not been defined, since $u_1\notin\bigcup_{k=1}^{n}C_{A_m}(\alpha_k)$.) For $2\leq i\leq n-1$, we have $\tilde{u}_i=\tilde{u}_n^{\tilde{\tau}_{in}}$, since $u_i=u_n^{\tau_{in}}$ in $C_{A_m}(\alpha_{i-1})$. In the case $r=2$ or 3, we define an element x of $C_{A_m}(\alpha_{n-1})$ as follows:

$$x=\begin{cases}(4n-3,\ 4n+1)(4n-2,\ 4n+2), & \text{if}\quad r=2\\ (4n+1,\ 4n-3,\ 4n+2,\ 4n-2)(4n-1,\ 4n+3) & \text{if}\quad r=3.\end{cases}$$

3.4. LEMMA. *We have*

(i) $[\tilde{u}_1, \tilde{\pi}_i]=[\tilde{u}_1, \tilde{\pi}_i']=1\qquad(2\leq i\leq n)$,

(ii) $[\tilde{u}_1, \tilde{\tau}_{ij}]=1 \quad (2\leq i, j\leq n)$,

(iii) $[\tilde{u}_1, \tilde{\mu}_1\tilde{\mu}_n]=1$ *if* $r\geq 2$, *and*

(iv) $[\tilde{u}_1, \tilde{x}]=1$.

PROOF. Since $\pi_i^{\tau_{1n}}=\pi_i$ $(2\leq i\leq n-1)$ and $\pi_1^{\tau_{1n}}=\pi_n$ in $C_{A_m}(\alpha_n)$, we have $\tilde{\pi}_i^{\tilde{\tau}_{1n}}=\tilde{\pi}_i$ $(2\leq i\leq n-1)$ and $\tilde{\pi}_1^{\tilde{\tau}_{1n}}=\tilde{\pi}_n$. This yields that $[\tilde{u}_1, \tilde{\pi}_i]=[\tilde{u}_1, \tilde{\pi}_i']=1$ $(2\leq i\leq n)$ by (3.2) and (3.3). This proves (i). τ_{ij} $(1\leq i, j\leq n-1)$ is contained in $C_{A_m}(\alpha_{n-1})$ and $[\tau_{ij}, u_n]=1$ $(1\leq i, j\leq n-1)$. Futher we have

$$\tau_{ij}^{\tau_{1n}}=\begin{cases}\tau_{ij}, & \text{if } 1\neq i<j\leqslant n-1\,,\\ \tau_{in}, & \text{if } 1=i<j\leqslant n-1\,.\end{cases}$$

From this and (3.3), it follows that $[\tilde{u}_1, \tilde{\tau}_{ij}]=1$ $(2\leq i, j\leq n)$. If $r\geq 2$, we have $[\tau_{1n}, \mu_1\mu_n]=1$ in $C_{A_m}(\alpha_n)$ and $[u_n, \mu_1\mu_n]=1$ in $C_{A_m}(\alpha_{n-1})$. From this and (3.3), (iii) follows. We have $[u_n, x^{\tau_{1n}}]=1$ in $C_{A_m}(\alpha_{n-1})$. Then we get $[\tilde{u}_1, \tilde{x}]=[\tilde{u}_n, \tilde{x}^{\tilde{\tau}_{1n}}]=1$.

3.5. LEMMA. $[\tilde{u}_1, \tilde{X}_1]=1$.

PROOF. Since u_n normalizes $\langle\pi_n, \pi_n'\rangle$, $\tilde{u}_1$ normalizes $\langle\tilde{\pi}_1, \tilde{\pi}_1'\rangle$. By (1), we have

$$C_G(\langle\tilde{\pi}_1, \tilde{\pi}_1'\rangle)=\langle\tilde{\pi}_1, \tilde{\pi}_1'\rangle\times\tilde{X}_1, \quad \text{where} \quad \tilde{X}_1\cong A_{m-4}\,.$$

Hence $\tilde{u}_1$ normalizes $\tilde{X}_1$ and induces an inner automorphism of $\tilde{X}_1$. From (1.2) and (i) and (iii) of (3.4), it follows that $\tilde{u}_1$ must centralize $\tilde{X}_1$

3.6. LEMMA. $C_G(\tilde{u}_1)=\langle\tilde{u}_1\rangle\times U$, *where* $U\cong A_{m-3}$, *and* $U\supset\tilde{X}_1$.

PROOF. The first statement follows from (3.2) and (3.3). The second statement follows from (3.5) and the fact that $X_1'=X_1$ and $U'=U$.

3.7. LEMMA. $N_G(\langle\tilde{u}_1\rangle)=(\langle\tilde{u}_1\rangle\times U)\langle\tilde{\mu}_{n-1}\rangle$, $\tilde{u}_1^{\tilde{\mu}_{n-1}}=\tilde{u}_1^{-1}$ *and* $U\langle\mu_{n-1}\rangle\cong S_{m-3}$.

PROOF. Since $u_n^{\mu_{n-1}}=u_n^{-1}$ in $C_{A_m}(\alpha_{n-1})$ and $[\tau_{1n}, \mu_{n-1}]=1$ in $C_{A_m}(\alpha_n)$, we get $\tilde{u}_1^{\tilde{\mu}_{n-1}}=\tilde{u}_1^{-1}$. From (1) and (2.4), any involution of G does not centralize a subgroup of G isomorphic to A_{m-3}. If $U\langle\tilde{\mu}_{n-1}\rangle$ is not isomorphic to S_{m-3}, we have $U\langle\tilde{\mu}_{n-1}\rangle=\langle y\rangle\times U$, where y is an involution of $U\langle\tilde{\mu}_{n-1}\rangle$. This is impossible.

3.8. LEMMA. $N_G(\langle\tilde{u}_1\rangle)\cap C_G(\tilde{\pi}_1)=\tilde{X}_1\langle\tilde{\mu}_{n-1}\rangle$ *and* $\tilde{X}_1\langle\tilde{\mu}_{n-1}\rangle\cong S_{m-4}$.

PROOF. By (1) and (3.5), $\tilde{X}_1$ is contained in $C_U(\tilde{\pi}_1)$. $\tilde{\pi}_1$ does not centralize U, since $U\cong A_{m-3}$. Hence we have $C_U(\tilde{\pi}_1)=\tilde{X}_1$, since $\tilde{X}_1$ is a maximal subgroup of U. From (3.7), we get $N_G(\langle\tilde{u}_1\rangle)\cap C_G(\tilde{\pi}_1)=\tilde{X}\langle\tilde{\mu}_{n-1}\rangle$. The second statement follows from (1).

3.9. Let H be a group isomorphic to S_l. Then H is generated by $l-1$ element $x_1, x_2, \cdots, x_{l-1}$ satisfying the following relations:

$$x_1^2 = \cdots = x_{l-1}^2 = (x_i x_{i+1})^3 = (x_j x_k)^2 = 1 \qquad (1 \leq i, j, k \leq l-1 \text{ and } |j-k|>1)$$

(cf. [**2**; p. 287]). We call an ordered set of such generators of H *a set of canonical generators* of H. If an involution t of H is a member of a set of canonical generators of H, we say that t is *a transposition* of H. Remark that, if $l=6$, this terminology is slightly vague because of the existence of an outer automorphism of order 2 of S_6. However, in the subsequent lemmas, this will cause no troubles. Let H_0 be a group isomorphic to $A_l \cdot H_0$ is generated by $l-2$ elements $y_1, y_2, \cdots, y_{l-2}$ satisfying the following relations:

$$y_1 = \cdots = y_{l-2} = (y_i y_{i+1})^3 = (y_j y_k)^2 = 1 \qquad (1 \leq i, j, k \leq l-2 \text{ and } |j-k|>1).$$

We call an ordered set of such generators of H_0 *a set of canonical generators* of H_0.

3.10. LEMMA. *Let H and H_0 be as in* (3.9). *Assume that H_0 is a subgroup of H. Let t_1 and t_2 be transpositions in H such that $[t_1, t_2]=1$ and if $l=6$, t_1 is conjugate to t_2 in H. Then we have* (i) $C_H(t_1) = \langle t_1 \rangle \times K$, *where* $H_0 \supset K \cong S_{l-2}$, *and* (ii) $t_1 t_2$ *is a transposition of K.*

PROOF. Since $H = H_0 \langle t_1 \rangle$, we have $C_H(t_1) = \langle t_1 \rangle \times C_{H_0}(t_1)$. Put $K = C_{H_0}(t_1)$. We can find a set of canonical generators $t_1', t_2', \cdots, t_{l-1}'$ of H with $t_1' = t_1$ and $t_3' = t_2$. Then it is clear that $t_1' t_3', \cdots, t_1' t_{l-1}'$ are contained in K and they are a set of canonical generators of K. This implies our lemma.

3.11 LEMMA. $\tilde{\mu}_i$, $\tilde{\mu}_i \tilde{u}_{i+1}$ *and* $\tilde{\mu}_i \tilde{\pi}_{i+1}$ $(1 \leq i \leq n-1)$ *are transpositions in* $U \langle \tilde{\mu}_{n-1} \rangle$. *If $r=2$, so is $\tilde{\mu}_n$. Further, if $r=3$, so are $\tilde{\mu}_n$ and $\tilde{\mu}_n \tilde{u}_{n+1}$.*

PROOF. Put $S^{(i)} = \langle \tilde{\mu}_i, \tilde{\mu}_i \tilde{u}_{i+1}, \tilde{\mu}_i \tilde{\pi}_{i+1} \rangle$ $(1 \leq i \leq n-1)$. Then it is easy to see that $S^{(i)}$ is isomorphic to S_4 and $\tilde{\mu}_i$, $\tilde{\mu}_i \tilde{u}_{i+1}$ and $\tilde{\mu}_i \tilde{\pi}_{i+1}$ are a set of canonical generators of $S^{(i)}$. Put

$$S^{(n)} = \begin{cases} 1 & \text{if } r=0 \text{ or } 1, \\ \langle \tilde{\mu}_n \rangle, & \text{if } r=2, \\ \langle \tilde{\mu}_n \quad \tilde{\mu}_n \tilde{u}_{n+1} \rangle, & \text{if } r=3. \end{cases}$$

Then we have $[S^{(i)}, S^{(j)}]=1$ $(1 \leq i < j \leq n)$. From (3.4) we know that $\tilde{\tau}_{i+1, j+1}$ $(1 \leq i, j \leq n-1)$ and $\tilde{x}$ are contained in U. Since $(S^{(i)})^{\tilde{\tau}_{i+1, j+1}} = S^{(j)}$ $(1 \leq i < j \leq n-1)$, $\tilde{\mu}_{n-1}^{\tilde{x}} = \tilde{\mu}_n$

and $\tilde{u}_n^{\bar{\tau}}=\tilde{u}_{n+1}$, a subgroup $S^{(1)}\times S^{(2)}\times\cdots\times S^{(n)}$ of $U\langle\tilde{\mu}_{n-1}\rangle$ satisfies the assumption of (1.8). Then (1.8) yields our lemma.

3.12 LEMMA. *G contains a subgroup Q isomorphic to A_m. Q has a property that, for any involution t of Q, $C_G(t)$ is contained in Q.*

PROOF. $\tilde{X}_1\langle\tilde{\mu}_{n-1}\rangle$ is a subgroup isomorphic to S_{m-4} of $U\langle\tilde{\mu}_{n-1}\rangle$, which is isomorphic to S_{m-3}. Since, by [1, section 161], S_{m-3} contains exactly one conjugate class of subgroups isomorphic to S_{m-4}, $\tilde{X}_1\langle\tilde{\mu}_{n-1}\rangle$ is naturally imbedded in $U\langle\tilde{\mu}_{n-1}\rangle$ in the same meaning as in (1.5). Then (3.11) yields that there exist an involution δ_1 in $U\langle\tilde{\mu}_{n-1}\rangle-(U\cup\tilde{X}_1\langle\tilde{\mu}_{n-1}\rangle)$ and $n-1$ involutions $\delta_2,\cdots,\delta_n$ in $\tilde{X}_1\langle\tilde{\mu}_{n-1}\rangle-\tilde{X}_1$ such that

(i) $C=\{\tilde{\mu}_1, \tilde{\mu}_1\tilde{u}_2, \tilde{\mu}_1\tilde{\pi}_2, \tilde{\delta}_2, \cdots, \tilde{\mu}_k, \tilde{\mu}_k\tilde{u}_{k+1}, \tilde{\mu}_k\tilde{\pi}_{k+1}, \tilde{\delta}_k, \cdots, \tilde{\mu}_{n-1}, \tilde{\mu}_{n-1}\tilde{u}_n, \tilde{\mu}_{n-1}\tilde{\pi}_n, \tilde{\delta}_n, \tilde{\mu}_n, \tilde{\mu}_n\tilde{u}_{n+1}\}$ is a set of canonical generator of $\tilde{X}_1\langle\tilde{\mu}_{n-1}\rangle$, where the last 3-$r$ elements of C do not appear.

(ii) $(\tilde{u}_1\delta_1)^2=1$, $(\delta_1\tilde{\mu}_1)^3=1$, and every element of $C-\{\mu_1\}$ commutes with δ_1.

Let Q be a subgroup of G generated by a set $C_1=\{\tilde{u}_1, \tilde{\pi}_1, \delta_1\}\cup C$. We shall show that $\tilde{\pi}_1^{\delta_1}$ is of order 3. This implies that Q is isomopphic to A_m and C_1 is a set of canonical generators of Q. Put $y=\tilde{\pi}_2'\tilde{\tau}_{12}$, $C_2=C-\{\tilde{\mu}_1\}$ and $C_3=C-\{\tilde{\mu}_1, \tilde{\mu}_1u_2, \tilde{\mu}_1\Pi_2, \delta_2\}$. Then we have

(iii) $\langle\tilde{\pi}_1,\delta_1\rangle\subset C_G(C_2)$,

(iv) $(\tilde{\mu}_1\tilde{u}_2)^y=\tilde{\mu}_1\tilde{u}_1$ and $(\tilde{\mu}_1\tilde{\pi}_2)^y=\tilde{\mu}_1$ and

(v) $v^y=\tilde{\mu}_1v$ for any element v of C_3.

If fact, (iii) follows from (i) and (ii). We have $(\tilde{\mu}_1\tilde{u}_2)^y=(\tilde{\mu}_1\tilde{u}_2)^{\tilde{\tau}_{12}}=\tilde{\mu}_1\tilde{u}_1$ and $(\mu_1\tilde{\pi}_2)^y=\tilde{\mu}_1^{\tilde{\tau}_{12}}=\tilde{\mu}_1$. This proves (iv). We shall verify (v). If $C_3\ni v\neq\delta_k$, we get $v^y=\tilde{\mu}_1v$ by using the isomorphism φ from $C_{A_m}(\alpha_n)$ to $C_G(\tilde{\alpha}_n)$ and computing directly. Suppose that $v=\delta_k$ ($k\geqq 3$). In order to verify (v) in this case, firstly we shall show that $\tilde{X}_2$ is generated by the totality of products of any two elements of C_3. We denote by C_4 the totality of products of any two elements of C_3. By (i), every elements of C_3 commutes with $\tilde{\pi}_1$, $\tilde{\pi}_2$, $\tilde{\pi}_2'$ and every elements of C_4 commutes with $\tilde{u}_1$. Since $\tilde{\pi}_1^{\tilde{u}_1}=\tilde{\pi}_1\tilde{\pi}_1'$, we get $C_4\subset C_G(\tilde{\pi}_1, \tilde{\pi}_1', \tilde{\pi}_2, \tilde{\pi}_2')$. By (i), the group generated by the set C_4 is isomorphic to A_{m-8}. Since $C_G(\tilde{\pi}_1, \tilde{\pi}_1', \tilde{\pi}_2, \tilde{\pi}_2')=\langle\tilde{\pi}_1, \tilde{\pi}_1', \tilde{\pi}_2, \tilde{\pi}_2'\rangle\times\tilde{X}_2$ and $\tilde{X}_2\cong A_{m-8}$ by the equality (1) in (1.1), $\tilde{X}_2$ must be the group generated by C_4. Since $[\tilde{\tau}_{12}, \tilde{X}_2]=1$, any element of C_4 commutes with $\tilde{\tau}_{12}$. In particular, we have $[\tilde{\tau}_{12}, \tilde{\mu}_{k-1}\tilde{\pi}_k\delta_k]=1$ ($k\geqq 3$). Hence we have $\tilde{\mu}_{k-1}\tilde{\pi}_k\delta_k=(\tilde{\mu}_{k-1}\tilde{\pi}_k\delta_k)^{\tilde{\tau}_{12}}=\tilde{\mu}_1\tilde{\mu}_{k-1}\tilde{\pi}_k\delta^{\tilde{\tau}_{12}}$ because of $\tilde{\mu}_{k-1}^{\tilde{\tau}_{12}}=\tilde{\mu}_1\tilde{\mu}_{k-1}$ and $\tilde{\pi}_k^{\tilde{\tau}_{12}}=\tilde{\pi}_k$. Then we get $\delta_k^y=\delta_k^{\tilde{\tau}_{12}}=\tilde{\mu}_1\delta_k$ since $\delta_k^{\tilde{\pi}_2'}=\delta_k$. Thus we have proved (v). By (iv), we have $(C_G(\tilde{\mu}_1\tilde{u}_2)\cap C_G(\tilde{\mu}_1\tilde{\pi}_2))^y=C_G(\tilde{\mu}_1\tilde{u}_1)\cap C_G(\tilde{\mu}_1)=$

$C_G(\tilde{a}_1)\cap C_G(\tilde{\mu}_1)$. Put $Z=C_G(\tilde{a}_1)\cap C_G(\tilde{\mu}_1)$. By (3, 6), (3, 7) and (3, 11), we have $C_G(\tilde{\mu}_1)\cap U\langle\tilde{\mu}_1\rangle=\langle\tilde{\mu}_1\rangle\times Z$ and $U\supset Z\cong S_{m-5}$. Put $W=\langle\tilde{\mu}_1 v \mid v\in C_3\rangle$. By (v), we have $Z\supset W$. From (i) it follows that W is isomorphic to S_{m-8} and the set $\{\mu_1 v \mid v\in C_3\}$ is a set of canonical generators of W. Then by applying (3.10) with $U\langle\tilde{\mu}_1\rangle$, U, Z, $\tilde{\mu}_1$ and $\tilde{\mu}_1 v$ $(v\in C_3)$ in place of H, H_0, K, t_1 and t_2 respectively, we get that W is naturally imbedded in Z in the same meaning as in (1.5). Hence we get $C_Z(W)\cong S_3$. Since $C_Z(W)\supset C_G(C_2)^v$ and $[\tilde{\pi}_1, \delta_1]\neq 1$ by (3.8), (iii) yields that $\tilde{\pi}_1\delta_1$ must be of order 3. Thus we have proved that Q is isomorphic to A_m. Obviously, there exists an isomorphism ϕ from A_m to Q such that $\phi(\pi_i)=\tilde{\pi}_i$ $(1\leq i\leq n)$. From this, it follows that $\tilde{\alpha}_1, \tilde{\alpha}_2, \cdots, \tilde{\alpha}_n$ are representatives of conjugacy classes of involutions in Q and $C_G(\tilde{\alpha}_i)$ is contained in Q because of $|C_G(\tilde{\alpha}_i)| = |C_{A_m}(\alpha_i)| = |C_Q(\tilde{\alpha}_i)|$. From these facts and (2.4), the second statement follows.

3.13 LEMMA. $G=Q$.

PROOF. By way of contradiction assume that Q is a proper subgroup of G. If any involution is not contained in $G-Q$, Q is a normal subgroup of G. Then Frattini argument yields that $G=C_G(\tilde{\alpha}_n)\cdot Q$. This contradicts (3.12). Take an involution x in $G-Q$. If y is an involution of Q, x is conjugate to y in G. Otherwise, there would exist an involution z such that $[x, z]=[y, z]=1$. Then (3.12) would imply that x is contained in Q, a contradiction. Hence G has one class of involutions. This contradicts (2.4) Hence we get $G=Q$.

This completes the proof the theorem.

College of General Education, University of Tokyo.

References

[1] W. Burnside, Theory of groups of finite order, Dover, 1955, 2nd edition.
[2] L. E. Dickson, Linear groups with an exposition of the Galois field theory, Dover, 1958.
[3] D. Held, A characterization of the alternating groups of degree eight and nine, J. Algebra, **7** (1967), 218-237.
[4] ———, A characterization of some multiply transitive permutation groups I, Illinois J. Math. (to appear).
[5] W. Specht, Eine Verallgemeinerung der symmetrischen Gruppe, Schr. Math. Sem. Berlin **1** (1932), 1-32.
[6] W. J. Wong, A characterization of the alternating group of degree eight, Proc. London Math. Soc. (3), **13** (1963), 359-383.

(Received November 15, 1967)