Oyama, T.
Osaka J. Math.
1 (1964), 91-101

ON THE GROUPS WITH THE SAME TABLE OF CHARACTERS AS ALTERNATING GROUPS

TUYOSI OYAMA

(Received May 26, 1964)

1. Introduction

It was proved by H. Nagao that a finite group which has the same table of characters as a symmetric group S_n is isomorphic to S_n. The purpose of this paper is to prove the following theorem.

Theorem. *If a finite group G has the same table of characters as an alternating group A_n, then G is isomorphic to A_n.*

As is shown in [2], a group G as in the theorem has the same order as A_n, therefore the theorem is trivial for $n=2$ and 3. Furthermore, the degrees of corresponding irreducible characters of G and A_n coincide with each other, the numbers of elements of corresponding conjugate classes of G and A_n are the same, and G has the same multiplication table of conjugate classes as A_n. From the last fact it follows that G is simple for $n\geqq 5$. Since it is known that a simple group of order 60 or 360 is isomorphic to A_5 or A_6, the theorem is true for $n=5$ and 6.

Now we shall give here an outline of the proof of the theorem which will be given in the next section. An alternating group A_n is isomorphic to the group generated by $a_1, a_2, \cdots, a_{n-2}$ with the following defining relations;

$$(*)\begin{cases} a_1^3=1,\ a_2^2=a_3^2=\cdots=a_{n-2}^2=1 \\ (a_ia_{i+1})^3=1 \qquad (i=1,2,\cdots,n-3) \\ (a_ia_j)^2=1 \qquad (i=1,2,\cdots,n-4,\ i+1<j) \end{cases}$$

(For the proof, see [1], Note C). The proof of the theorem is carried out by showing the existence of elements $a_1, \cdots, a_{n-2}$ in G which satisfy the above relations.

Let $C^*(i_1^{\alpha_1}, i_2^{\alpha_2}, \cdots)$ be the totality of elements of A_n which can be expressed as a product of α_1 cycles of length i_1, α_2 cycles of length $i_2, \cdots$ such as each of letters occurs in only one cycle of them, where we assume $i_r>1$ except for $C^*(1)$. In A_n, $C^*(i_1^{\alpha_1}, i_2^{\alpha_2},\cdots)$ is itself a conjugate class or a union of two conjugate classes with the same number of elements. Let G be a group with the same table of characters as A_n, and let $C(i_1^{\alpha_1}, i_2^{\alpha_2},\cdots)$ be the conjugate class or the union of two conjugate classes corresponding to $C^*(i_1^{\alpha_1}, i_2^{\alpha_2},\cdots)$. Then $\{C(i_1^{\alpha_1}, i_2^{\alpha_2},\cdots)\}$ has the same multiplication table as $\{C^*(i_1^{\alpha_1}, i_2^{\alpha_2},\cdots)\}$ and the number of elements of $C(i_1^{\alpha_1}, i_2^{\alpha_2},\cdots)$ is $\dfrac{n!}{(n-i)!\cdot\alpha_1!\cdot i_1^{\alpha_1}\cdot\alpha_2!\cdot i_2^{\alpha_2}\cdots}$, where $i=\sum_r \alpha_r i_r$. The following multiplication tables will be used frequently.

$$(\mathrm{M}_1)\quad C(2^2)\cdot C(2^2)=\frac{n!}{8\cdot(n-4)!}C(1)+\{(n-4)(n-5)+2\}\cdot C(2^2)+\frac{3}{2}(n-3)(n-4)C(3)+5C(5)+4C(2,4)+6C(2^2,3)+6C(2^4)+9C(3^2)$$

$$(\mathrm{M}_2)\quad C(3)\cdot C(3)=\frac{n!}{3(n-3)!}C(1)+\{1+3(n-3)\}\cdot C(3)+8C(2^2)+2C(3^2)+5C(5).$$

$$(\mathrm{M}_3)\quad C(3)\cdot C(2^2)=C(2^2,3)+4C(2,4)+4(n-4)C(2^2)+5C(5)+3(n-3)C(3).$$

Lemma 1 and 2 in the next section will be useful to determine the orders of elements in $C(3)$, $C(2^2)$ and $C(5)$. After proving several lemmas, we shall show that there are elements a_1 in $C(3)$ and a_2, $b_1,\cdots$, b_{n-4} in $C(2^2)$ such that $a_1a_2\in C(3)$, $a_1b_i\in C(2^2)$, $a_2b_i\in C(3)$ (Lemma 11, 12, 13). Then it will be proved that the elements a_1, a_2, $a_3=b_1$, $a_4=b_1b_2b_1,\cdots$, $a_{n-2}=b_{n-5}b_{n-4}b_{n-5}$ satisfy the relations (*).

2. Proof of Theorem

In this section, we assume that G is a finite group with the same table of characters as A_n with $n=4$ or $n\geqq 7$.

Lemma 1. *If the order of an element of $C(i_1^{\alpha_1},i_2^{\alpha_2},\cdots)$ is a prime power p^m, then $i=\sum_r \alpha_r i_r\equiv 0\ (p)$.*

Proof. As A_n is a doubly transitive group G has a irreducible character χ of degree $n-1$ such that $\chi(a)=n-1-i$ for $a\in C\ (i_1^{\alpha_1}, i_2^{\alpha_2},\cdots)$. Since $a^{p^m}=1$, we have $\chi(a)=\sum_{r=1}^{n-1}\omega_r$, where $\omega_r^{p^m}=1$. Thus $\sum\omega_r=n-1-i$, and $(n-1-i)^{p^m}=(\sum\omega_r)^{p^m}\equiv\sum\omega_r^{p^m}\equiv n-1\ (\mathfrak{p})$, where $\mathfrak{p}$ is a prime ipeal divisor of p in the field of p^mth root of unity. Therefore $n-1\equiv n^{p^m}-1-i^{p^m}\equiv n-1-i\ (p)$, and hence $i\equiv 0\ (p)$.

Lemma 2. *Let $a \in C(i_1^{\alpha_1}, i_2^{\alpha_2}, \cdots)$. If $C(i_1^{\alpha_1}, i_2^{\alpha_2}, \cdots)$ is a conjugate class of G, and $a^k \in C(1) \cup C(i_1^{\alpha_1}, i_2^{\alpha_2}, \cdots)$ for any k, then the order of a is a prime number.*

Proof. Suppose that the order of a is k_1k_2, where $k_1 \neq 1$, $k_2 \neq 1$. By the assumption $a^{k_1} \in C(i_1^{\alpha_1}, i_2^{\alpha_2}, \cdots)$, and the order of a^{k_1} is k_2, which is less than k_1k_2. This is a contradiction. Therefore the order of a is a prime.

Lemma 3. *If G has the same table of characters as A_4, then G is isomorphic to A_4.*

Proof. Now $G = C(1) \cup C(2^2) \cup C(3)$, where $C(2^2)$ is a conjugate class and $C(3)$ is a union of two conjugate classes $C_1(3)$ and $C_2(3)$.

Since the order of G is *12*, G has elements of the order *3* and *2*. Let a be an element of order *2*, then by Lemma 1 a is not in $C(3)$, therefore $a \in C(2^2)$, and an element b of order *3* is in $C(3) = C_1(3) \cup C_2(3)$. Let $b \in C_1(3)$. Since $C_1(3) \cdot C(2^2) \supset C_1(3)$, there exist elements a_1 and a_2 such that $a_1 \in C_1(3)$, $a_2 \in C(2^2)$ and $a_1a_2 \in C_1(3)$, i.e. $a_1^3 = 1$, $a_2^2 = 1$ and $(a_1a_2)^3 = 1$. Therefore $H = \{a_1, a_2\}$ is a homomorphic image of A_4. If the order of H is *6*, then A_4 has a normal subgroup K of the order *2* such that A_4/K is isomorphic to H. But A_4 has no normal subgroup of the order *2*. Therefore the order of H is *12*, and so G is isomorphic to A_4.

From now on we assume that $n \geqq 7$. Then $C(i_1^{\alpha_1}, i_2^{\alpha_2}, \cdots)$ occuring in the multiplication tables (M_1), (M_2) and (M_3) are themselves conjugate classes in G. We shall denote by $n(x)$ the order of the normalizer $N(x)$ of an elemente x, and if x is in a conjugate class $C(i_1^{\alpha_1}, i_2^{\alpha_2}, \cdots)$ then $n(x)$ is also denoted by $n(i_1^{\alpha_1}, i_2^{\alpha_2}, \cdots)$. Since $N(x) \subseteqq N(x^k)$, $n(x)$ is a divisor of $n(x^k)$.

Lemma 4. *If $a \in C(3)$, then $a^k \in C(3) \cup C(1)$ and the order of a is 3.*

Proof. From the multiplication table (M_2) $C(3) \cdot C(3) = C(1) \cup C(3) \cup C(2^2) \cup C(3^2) \cup C(5)$. Since $n(3)$ does not divide $n(2^2)$, $n(3^2)$ and $n(5)$, a^k does not belong to $C(2^2) \cup C(3^2) \cup C(5)$. Thus $a^2 \in C(3) \cup C(1)$. If $a^{k-1} \in C(3) \cup C(1)$, then $a^k = a^{k-1} \cdot a \in C(3) \cdot C(3)$ and hence $a^k \in C(3) \cup C(1)$. Therefore by an induction on k, we have $a^k \in C(3) \cup C(1)$. for all k. By Lemma 2 the order of a is a prime, and by Lemma 1 it is *3*.

Lemma 5. *If $a \in C(2^2)$, then $a^2 = 1$.*

Proof. From the multiplication table (M_1) $C(2^2) \cdot C(2^2) = C(1) \cup C(2^2) \cup C(3) \cup C(5) \cup C(2, 4) \cup C(2^2, 3) \cup C(2^4) \cup C(3^2)$, where $C(2^4)$ is omitted for $n = 7$. By the same argument as in the proof of Lemma 4, $a^k \notin C(5) \cup C(2, 4)$

$\cup C(2^2, 3) \cup C(3^2)$. If a^k is contained in $C(2^4)$, then $\frac{n(2^4)}{n(2^2)} = \frac{4! \cdot 2^4 \cdot (n-8)!}{8 \cdot (n-4)!}$ $= \frac{2^4 \cdot 3}{(n-4)(n-5)(n-6)(n-7)}$ must be an integer. But this is impossible except for $n=8$.

Now in the case of $n=8$, since $n(2^2)$ does not divide $n(3)$, $a^k \notin C(3)$. Therefore it is easily seen that $a^k \in C(1) \cup C(2^2) \cup C(2^4)$. From the multilication table (M_2), there are two elements b_1, b_2 of $C(3)$ such that $a=b_1b_2$, and $a^2=b_1b_2b_1b_2=(b_1b_2b_1^{-1}) \cdot b_1^{-1} \cdot b_2 \in C(3)^3$. It is easily seen that $C(3)^3$ does not contain $C(2^4)$, hence $a^2 \notin C(2^4)$, and $a^2 \in C(2^2) \cup C(1)$.

Suppose that $a^2 \notin C(1)$. Then $a^2 \in C(2^2)$. If $a^k \in C(2^4)$ for some k, then $a^{2k}=(a^2)^k \in C(2^4)$. Since $a^{kk'} \in C(2^2) \cup C(2^4) \cup C(1)$, and $n(2^4)$ does not divide $n(2^2)$, $a^{kk'} \in C(2^4) \cup C(1)$ for all k', Hence by Lemma 1 and 2, the order of an element of $C(2^4)$ is *2*, and therefore $a^{2k}=1$. This is a contradiction. Thus $a^k \notin C(2^4)$ and $a^k \in C(2^2) \cup C(1)$ for all k. By Lemma 1 and 2, we have $a^2=1$, which contradicts the first assumption. Thus this lemma is proved for $n=8$.

In the case of $n \neq 8$, we have seen $a^k \notin C(2^4)$ for any integer k, hence $a^2 \in C(2^2) \cup C(3) \cup C(1)$. Now $a^3=a^2 \cdot a \in \{C(2^2) \cup C(3) \cup C(1)\} \cdot C(2^2)$, and so from the multiplication tables (M_1) and (M_3) and by considering the orders of normalizers of elements it is seen that $a^3 \in C(2^2) \cup C(3) \cup C(1)$. Now if $a^3 \in C(3)$, then by Lemma 4 $(a^3)^3=1$, but by Lemma 1 the order of a can not be 3^2, $a^3 \notin C(1)$, thus $a^3 \in C(2^2)$. If $a^k \in C(3)$ for some k, then for $b=a^3$, $b^k \in C(3)$ since $b \in C(2^2)$. On the other hand, $b^k=(a^k)^3=1$ since $a^k \in C(3)$ and the order of an element of $C(3)$ is *3*. This is a contradiction. Thus $a^k \notin C(3)$, therefore $a^2 \in C(2^2) \cup C(1)$. By the same argument as in the proof of Lemma 4, we have now $a^2=1$.

Lemma 6. *Any element x of $C(3^2)$ is uniquely expressed as a product of two commutative elements a, b of $C(3)$ disregarding their arrangement, and $x^3=1$.*

Proof. From $C(3) \cdot C(3) = 2C(3^2) + \cdots$, x can be expressed in exactly two ways as a product of two elements of $C(3)$. If $x=ab$ with $a, b \in C(3)$, then $x=a \cdot b=b(b^{-1}ab)=(b^{-1}ab)(b^{-1}a^{-1}bab)$. It is easily seen that $a \neq b$ and $b \neq b^{-1}ab$. Hence $a=b^{-1}ab$ i.e. $ab=ba$, and we have $(ab)^3=1$ by Lemma 4.

Lemma 7. *Any element x of $C(2^2, 3)$ can be expressed uniquely as a product of an element a of $C(3)$ and an element b of $C(2^2)$. Two elements a and b are commutative and the order of x is 6.*

Proof. From $C(3) \cdot C(2^2) = 1 \cdot C(2^2, 3) + \cdots$, the first half of the lemma is evident. Now $x=a \cdot b=(bab)(ba^{-1}bab)$, $bab \in C(3)$ and $ba^{-1}bab \in C(2^2)$, therefore $a=bab$ i. e. $ab=ba$, and so from $a^3=1$ and $b^2=1$, the order of x is *6*.

Lemma 8. *The oder of an element x of $C(5)$ is 5, and $x^k \in C(5)$ for $k \not\equiv 0$ (5).*

Proof. From $C(2^2)\cdot C(2^2)=5C(5)+\cdots$ there exist two elements a and b of $C(2^2)$ such that $x=ab$, and x is expressed in exactly five ways as a product of two elements of $C(2^2)$. Now $x=ab=b(bab)=(bab)(babab)$ $=(babab)(bababab)=(bababab)(babababab)$, and by Lemma 1 the order of element of $C(5)$ can not be *2*, *3* and *4*, and therefore it is easily seen that these five expressions of x as a product of two elements of $C(2^2)$ are all distinct. Since $x=(babababab)(babababab)$ is also an expression as a product of two elements of $C(2^2)$, and $b(ab)^4$ is not equal to b, bab, $b(ab)^2$ and $b(ab)^3$, $b(ab)^4$ must be equal to a i. e. $(ab)^5=1$. Since $(ab)^2=(aba)b$ and $(ab)^3=(ab)^{-2}$, these are contained in $C(2^2)\cdot C(2^2)$ and from the multiplication table (M_1) and Lemma 1, except the elements of $C(5)$, the order of any element of cojugate classes in $C(2^2)\cdot C(2^2)$ is not *5*. Therefore both $(ab)^2$ and $(ab)^3$ are contained in $C(5)$ and $(ab)^4=(ab)^{-1}$ is also in $C(5)$.

Lemma 9. *If $x \in C(2, 4)$, then $x^2 \in C(2^2)$ and $x^4=1$.*

Proof. Since $C(2, 4)$ is contained in $C(3)\cdot C(2^2)$, there exist an element a of $C(3)$ and an element b of $C(2^2)$ such that $x=ab$. If $x^2=1$ then $abab=1$, $aba=b$, hence $a^{-1}ba=ab$, but $a^{-1}ba$ is contained in $C(2^2)$, which is a contradiction. If $x^3=1$, then $ababab=1$. $ababa=b$, hence $a^{-1}baba=ab$, but $a^{-1}baba \sim a \in C(3)$, which is a contradiction. (Here $x \sim y$ means that x is conjugate to y.)

Since $C(2^2)\cdot C(2^2)=4C(2,4)+\cdots$ and the order of x is not 2 and 3 as proved above, we can show that the order of x is 4 by the same argument as in the proof of Lemma 8. Now $x^2=a(bab) \in C(3)\cdot C(3)$ and the only conjugate class in $C(3)\cdot C(3)$ whose elements have order 2 is $C(2^2)$, therefore $x^2 \in C(2^2)$.

Lemma 10.

(1) *Let $x=ab \in C(5)$, where a and b belong to $C(2^2)$, then setting $a^{x^i}=x^{-i}ax^i$, $x=a^{x^i}b^{x^i}$ $(i=0, 1, 2, 3, 4)$ are all of the ways to express x as a product of two elements of $C(2^2)$. The same holds for $a, b \in C(3)$ or $a \in C(3)$, $b \in C(2^2)$.*

(2) *For elements a and b of $C(2^2)$, if there exists an element y such that y does not belong to $C(5) \cup C(1)$, ay belongs to $C(2^2)$ and $y^{-1}b$ belongs to $C(2^2)$, then ab does not belong to $C(5)$.*

(3) *For an element* a *of* $C(3)$ *and an element* b *of* $C(2^2)$, *if there exists an element* y *such that* y *does not belong to* $C(3)\cup C(5)\cup C(1)$, ay *belongs to* $C(3)$ *and* $y^{-1}b$ *belongs to* $C(2^2)$, *then* ab *does not belong to* $C(5)$.

Proof. (1) Since $C(2^2)\cdot C(2^2)=5C(5)+\cdots$, it is enough to prove that five elements $a^{x^i}(0\leqq i\leqq 4)$ are all different. If $a^{x^i}=a^{x^j}$, where $0\leqq i<j\leqq 4$, then $ax^{j-i}=x^{j-i}a$. Since the oder of x is 5, $ax=xa$, hence $ab=ba$, which shows that the order of x is not 5. This is a contradiction. The proof for $a, b\in C(3)$ or $a\in C(3)$, $b\in C(2^2)$ is similer.

(2) Suppose $x=ab\in C(5)$. Then since $x=(ay)(y^{-1}b)$ and $ay, y^{-1}b \in C(2^2)$, by (1) $ay=a^{x^i}=b(ab)^{2i-1}$. Hence $y=(ab)^{2i}$ and therefore $y\in C(5) \cup C(1)$, which is a contradiction.

(3) Assume $x=ab\in C(5)$, then by (1) ay is equal to some a^{x^i}. ay is not equal to a. If $ay=a^x$, then $ay=ba^{-1}aab=bab$. Hence $y=a^{-1}bab =a^{-1}ba^{-1}\cdot a^{-1}b=bababab\cdot a^{-1}b\sim aba=a^{-1}\cdot a^{-1}b\cdot a\in C(5)$, which is a contradiction. If $ay=a^{x^2}$, then $ay=abababaabab$. Hence $y=bababa^2bab=bababa^{-1} \cdot ba^{-1}a^{-1}b\sim baba^{-1}ba^{-1}=ba\cdot ababab\sim a\in C(3)$, which is a contradiction. If $ay=a^{x^3}$, then $ay=ababaababab$. Hence $y=baba^2babab=ba^{-1}\cdot a^{-1}ba^{-1}babab \sim a^{-1}ba^{-1}bab=babab aab\sim a\in C(3)$, which is a contradiction. If $ay=a^{x^4}$, then $ay=ab\cdot a\cdot abababab$. Hence $y=ba^2bababab\sim aba=a^{-1}\cdot a^{-1}b\cdot a\in C(5)$, which is also a contradiction. From these, x can not belong to $C(5)$.

Lemma 11. *For an element* a_1 *of* $C(3)$, *there exists an element* a_2 *of* $C(2^2)$ *such that* $a_1a_2\in C(3)$.

Proof. From$C(3)\cdot C(2^2)\supset C(3)$, this lemma is evident.

Lemma 12. *Let* $a_1\in C(3)$, $a_2\in C(2^2)$ *and* $a_1a_2\in C(3)$. *The number of the elements* b*'s in* $C(2^2)$ *such that* $a_1b\in C(2^2)$ *and* $a_2b\in C(2^2)$ *is* $\frac{1}{2}(n-4)(n-5)$. *If* $b\in C(2^2)$, $a_1\,b\in C(3)$, $a_2b\in C(2^2)$ *then* b *is either* $a_1a_2a_1^{-1}$ *or* $a_1^{-1}a_2a_1$.

Proof. From $C(2^2)\cdot C(2^2)=\{(n-4)(n-5)+2\}C(2^2)+\cdots$, for the element a_2 there are $(n-4)(n-5)+2$ elements b's in $C(2^2)$ such that $a_2b\in C(2^2)$. Let b be one of such elements. Then $a_2b\in C(2^2)$ and $a_2(a_2b)\in C(2^2)$, hence the element a_2b is also one of elements as above. Now $a_1b\in C(3)\cdot C(2^2) =C(2^2,3)\cup C(5)\cup C(2^2)\cup C(2,4)\cup C(3)$.

(1) a_1b is not contained in $C(2^2,3)\cup C(5)$.

Since $a_1b=(a_1a_2)(a_2b)$, $a_1a_2\in C(3)$ and $a_2b\in C(2^2)$, by Lemma 10 $a_1b \notin C(5)$. If $a_1b\in C(2^2, 3)$ then by Lemma 7, $a_1=a_1a_2$, which is a contradiction. Therefore $a_1b\notin C(2^2, 3)$.

(2) If there are elements b's such that $a_1b\in C(2, 4)$ or $a_1b\in C(2^2)$, then the number of elements b's such that $a_1b\in C(2, 4)$ are equal to the

number of elements b's such that $a_1b \in C(2^2)$.

If $x=a_1b \in C(2, 4)$, then from $C(3)\cdot C(2^2)=4C(2,4)+\cdots$, $x=a_1^{x^i}b^{x^i}$ ($i=0, 1, 2, 3$) are all of the ways to express x as a product of an element of $C(3)$ and an element of $C(2^2)$. For, if $a_1=a_1^x$ then $a_1=ba_1^{-1}a_1a_1b=ba_1b$, hence $a_1^{-1}=(a_1b)^2$, but $a_1^{-1} \in C(3)$ and $(a_1b)^2 \in C(2^2)$, which is a contradiction. If $a_1=a_1^{x^2}$ then $a_1=ba_1^{-1}ba_1ba_1b=ba_1\cdot ba_1^{-1}$, hence $ba_1\cdot ba_1=1$, which is a contradiction. If $a_1=a_1^{x^3}$ then $a_1=a_1ba_1ba_1^{-1}$, hence $a_1^{-1}=(a_1b)^2$, which is a contradiction. Thus $a_1^{x^i}$ are all distinct from each other. On the other hand, $a_1b=(a_1a_2)(a_2b)$, $a_1a_2 \in C(3)$ and $a_2b \in C(2^2)$, therefore a_1a_2 must be equal to some $a_1^{x^i}$. a_1a_2 is not equal to a_1. If $a_1a_2=a_1^x$ then $a_1a_2=ba_1b$, hence $a_1^{-1}a_2=(a_1b)^2$, but $a_1^{-1}a_2 \in C(3)$ and $(a_1b)^2 \in C(2^2)$, which is a contradiction. If $a_1a_2=a_1^{x^3}$ then $a_1a_2=a_1ba_1ba_1^{-1}$, hence $a_2a_1^{-1}=(ba_1)^2$, which is a contradiction. Therefore a_1a_2 must be equal to $a_1^{x^2}=ba_1ba_1^{-1}$, and therefore $a_1a_2b=ba_1ba_1^{-1}b\sim b \in C(2^2)$. Thus we can conclude that if $a_1b \in C(2, 4)$, a_1a_2b belongs to $C(2^2)$.

Conversely suppose $a_1b \in C(2^2)$. Now $a_1a_2b \in C(3)\cdot C(2^2)$, and $(a_1a_2b)^2 =a_1a_2ba_1a_2b=a_1a_2a_1^{-1}ba_2b=a_1a_2a_1^{-1}a_2=a_1^{-1}a_2a_1 \in C(2^2)$. But for a conjugate class in $C(3)\cdot C(2^2)$, if a square of it's element belongs to $C(2^2)$, then this class must be $C(2, 4)$. Therefore $a_1a_2b \in C(2, 4)$. Thus our assertion is proved.

(3) If $a_1b \in C(3)$, then b is either $a_1a_2a_1^{-1}$ or $a_1^{-1}a_2a_1$.

Let b_1 and b_2 belong to $C(2^2)$, and $a_2b_i \in C(2^2)$, $a_1b_i \in C(3)$, and $b_1 \neq b_2$ ($i=1, 2$). From (1) $a_1a_2b_i \in C(3) \cup C(2, 4) \cup C(2^2)$ and $a_1a_2\cdot a_2b \in C(3)$, hence from (2) $a_1a_2b_i \in C(3)$. Now $b_1b_2=b_1a_1\cdot a_1^{-1}b \in C(3)\cdot C(3)=C(1) \cup C(3) \cup C(2^2) \cup C(3^2) \cup C(5)$ and $b_1 \neq b_2$, therefore the order of b_1b_2 is *2, 3* or *5*.

Assume $a_2b_1b_2 \neq 1$. As $a_2(b_1b_2)=(b_1b_2)a_2$, the order of $a_2b_1b_2$ is *2, 6* or *10*. But $a_2b_1b_2=a_2b_1a_1\cdot a_1^{-1}b \in C(3)\cdot C(3)$. Thus from the multiplication table (M_2) $a_2b_1b_2 \in C(2^2)$ and therefore $b_1b_2 \in C(2^2)$, and hence by (1) $a_1b_1b_2 \in C(3) \cup C(2, 4) \cup C(2^2)$. If $a_1b_1b_2 \in C(2^2)$, then $a_1b_1b_2\cdot a_1b_1b_2=1$, $a_1b_1b_2a_1b_2b_1=1$, hence $b_1a_1b_1a_1^{-1}b_2a_1^{-1}=1$, and therefore $b_1a_1b_1a_1=a_1b_2a_1^{-1}$, but the left belongs to $C(3)$ and the right belongs to $C(2^2)$, which is a contradiction. If $a_1b_1b_2 \in C(2, 4)$, then by $C(3)\cdot C(2^2)=4C(2, 4)+\cdots$, $a_1b_1b_2$ is expressed in exactly four ways as a product of an element of $C(3)$ and an element of $C(2^2)$. But $a_1(b_1b_2)=(a_1b_1)b_2=(a_1b_2)b_1=(a_1a_2)(a_2b_1b_2)=(a_1a_2b_1)(b_2a_2)$, and it is easily seen that these are distinct five ways of expressions of $a_1b_1b_2$ as a product of an element of $C(3)$ and an element of $C(2^2)$, which is a contradiction. Thus $a_1b_1b_2 \notin C(2, 4)$. If $a_1b_1b_2 \in C(3)$, then by $C(3)\cdot C(3)=8C(2^2)+\cdots$, b_2 is expressed in exactly eight ways as a product of two elements of $C(3)$. But $b_2=(b_1a_1)(a_1^{-1}b_1b_2)=(b_1b_2a_1)(a_1^{-1}b_1)=(b_1a_1^{-1})(a_1b_1b_2)=(b_1b_2a_1^{-1})(a_1b_1)=a_1(a_1^{-1}b_2) =(b_2a_1)a_1^{-1}=a_1^{-1}(a_1b_2)=(b_2a_1^{-1})a_1=(b_1a_2a_1^{-1})(a_1a_2b_1b_2)$, and it is easily seen that these are distnct nine ways of expressions of b_2 as a product of two elements of $C(3)$, which is a contradiction. Thus $a_1b_1b_2 \notin C(3)$. Hence $a_2b_1b_2$ must be equal to *1*, and therefore $b_2=a_2b_1$, which means that b_2 is uniquely determined by b_1. Now take $a_1a_2a_1^{-1}$, then $a_1a_2a_1^{-1} \in C(2^2)$, $a_1(a_1a_2a_1^{-1})=a_2a_1a_2 \in C(3)$, and $a_2(a_1a_2a_1^{-1})=a_1^{-1}a_2a_1 \in C(2^2)$. Therefore b such that $a_1b \in C(3)$ and $a_2b \in C(2^2)$ is either $a_1a_2a_1^{-1}$ or $a_2 \cdot a_1a_2a_1^{-1}=a_1^{-1}a_2a_1$.

(4) From the proofs above, there are exactly $\frac{1}{2}(n-4)(n-5)$ elements b's such that $a_1b \in C(2^2)$.

Lemma 13. *Let* $a_1 \in C(3)$, $a_2 \in C(2^2)$, $a_1a_2 \in C(3)$, *then there are* $n-4$ *elements* b*'s in* $C(2^2)$ *such that* $a_1b \in C(2^2)$, $a_2b \in C(3)$.

Proof. From $C(3)\cdot C(2^2)=4(n-4)C(2^2)+\cdots$, for a_1 there are $\frac{3}{2}(n-3)(n-4)$ elements b's such that $a_1b \in C(2^2)$, and for such b's, since a_1b and $a_1^{-1}b$ belong to $C(2^2)$ and $a_1(a_1b)$ and $a_1(a_1^{-1}b)$ belong to $C(2^2)$, a_1b and $a_1^{-1}b$ are included $\frac{3}{2}(n-3)(n-4)$ element b's, and b, a_1b and $a_1^{-1}b$ are all distinct. For such elements b_1, b_2 the sets $\{b_1, a_1b_1, a_1^{-1}b_1\}$ and $\{b_2, a_1b_2, a_1^{-1}b_2\}$ are the same set or have no common element. Now $a_2b=a_2a_1\cdot a_1b \in C(3)\cdot C(2^2) =C(2^2, 3)\cup C(2, 4)\cup C(2^2)\cup C(5)\cup C(3)$.

(1) a_2b is not in $C(2^2, 3)$.

$a_2b=a_2a_1\cdot a_1^{-1}b=a_2a_1^{-1}\cdot a_1b$, hence by Lemma 7 if $a_2b \in C(2^2, 3)$, then $a_2a_1 =a_2a_1^{-1}$, and this is a contradiction. Therefore $a_2b \notin C(2^2, 3)$.

(2) There are $\frac{1}{2}(n-4)(n-5)$ elements b's such that $a_2b \in C(2^2)$, and for such b, a_2a_1b and $a_2a_1^{-1}b$ belong to $C(2, 4)$.

By Lemma 12 there are $\frac{1}{2}(n-4)(n-5)$ elements b's such that $a_2b \in C(2^2)$. Now $a_2a_1b \in C(3)\cdot C(2^2)$ and $(a_2a_1b)^2=a_2a_1ba_2a_1b=a_2a_1a_2a_1^{-1}=a_1^{-1}a_2a_1 \in C(2^2)$, hence from the multiplication table (M_3), $a_2a_1b \in C(2, 4)$ and in the same way we have $a_2a_1^{-1}b \in C(2, 4)$.

(3) If $a_2b \in C(3)$, then a_2a_1b and $a_2a_1^{-1}b \in C(5)$.

$a_2a_1b \in C(3)\cdot C(2^2)$ and $a_2a_1b=a_2a_1a_2\cdot a_2b \in C(3)\cdot C(3)$, therefore $a_2a_1b \in C(2^2) \cup C(3)\cup C(5)$. If $a_2a_1b \in C(2^2)$, then by (2) $a_2\cdot a_1^{-1}a_1b=a_2b \in C(2, 4)$, which is a contradiction. If $a_2a_1b \in C(3)$, then $a_2a_1ba_2a_1ba_2a_1b=1$, therefore $b=a_1^{-1}a_2a_1^{-1}a_2ba_2ba_1^{-1}a_2a_1 \sim a_2ba_2ba_1=ba_2a_1 \sim a_2a_1b \in C(3)$, which is a contradiction, Thus $a_2a_1b \in C(5)$, and in the same way we have $a_2a_1^{-1}b \in C(5)$.

(4) If $a_2b \in C(2, 4)$, then a_2a_1b or $a_2a_1^{-1}b \in C(2^2)$.

For ba_2b, which belongs to $C(2^2)$, $a_2\cdot ba_2b \in C(2^2)$, and $a_1\cdot ba_2b=ba_1^{-1}a_2b \in C(3)$. By Lemma 12 ba_2b must be equal to $a_1^{-1}a_2a_1$ or $a_1a_2a_1^{-1}$. If $ba_2b =a_1^{-1}a_2a_1$ then $a_1b\cdot a_2=a_2\cdot a_1b$, hence $(a_2a_1b)^2=1$, but $a_2a_1b \in C(3)\cdot C(2^2)$, and from the multiplication table (M_3), $a_2a_1b \in C(2^2)$. If $ba_2b=a_1a_2a_1^{-1}$, then $a_2\cdot ba_1=ba_1\cdot a_2$, and in the same way we have $a_2ba_1=a_2a_1^{-1}b \in C(2^2)$.

(5) From (2), (4) there are $\frac{3}{2}(n-4)(n-5)$ elements b's such that $a_2b \in C(2^2)\cup C(2, 4)$, and since $\frac{3}{2}(n-3)(n-4)-\frac{3}{2}(n-4)(n-5)=3(n-4)$, there are $3(n-4)$ elements b's such that $a_2b \in C(3)\cup C(5)$.

(6) There are $n-4$ elements b's such that $a_2b \in C(3)$.

From (3), (5), the number of elements b's such that $a_2b \in C(5)$ is at least $2(n-4)$. Let $a_2b_1 \in C(5)$, $a_2b_2 \in C(5)$ and $b_1 \neq b_2$, then b_i, $b_ia_2b_i$, $b_ia_2b_ia_2b_i$ and $b_ia_2b_ia_2b_ia_2b_i$ $(i=1, 2)$ are all distinct elements in $C(2^2)$ and their products with a_2 belong to $C(5)$. For, if $b_1(a_2b_1)^j=b_2(a_2b_2)^k$, $(0 \leqq j, k \leqq 3)$, then $(a_2b_1)^{j+1}=(a_2b_2)^{k+1}$, and as the order of a_2b_1 and a_2b_2 are 5, there exists an integer r such that $a_2b_1=(a_2b_2)^r$. Hence $b_1b_2=(b_2a_2)^{r-1}$ i. e. $b_1b_2 \in C(5)$. But $b_1b_2=b_1a_1 \cdot a_1^{-1}b_2$ and by Lemma 10 $b_1b_2 \notin C(5)$, which is a contradiction. Thus for the element a_2, the number of the elements d's such that $d \in C(2^2)$ and $a_2d \in C(5)$ is at least $8(n-4)$. But from $C(2^2) \cdot C(2^2) = 5C(5)+\cdots$, the number of such d's is just $8(n-4)$. Therefore there are $2(n-4)$ elements b's such that $a_2b \in C(5)$, and so the number of elements b's such thac $a_2b \in C(3)$ is $n-4$.

Lemma 14. *If* $a_1 \in C(3)$, $a_2 \in C(2^2)$, $a_1a_2 \in C(3)$, *and* $b_i \in C(2^2)$ $(i=1, 2, 3, 4)$, $a_1b_i \in C(2^2)$, $a_2b_i \in C(3)$ *and* $b_i \neq b_j$ $(i \neq j)$, *then*

(1) $b_ib_j \in C(3)$, $(i \neq j)$.
(2) $a_2b_ib_jb_i \in C(2^2)$, $(i \neq j)$.
(3) $b_i \cdot b_jb_kb_j \in C(2^2)$, *for distinct* i, j *and* k.
(4) $b_ib_jb_i \cdot b_kb_lb_k \in C(2^2)$, *for distinct* i, j, k *and* l.

Proof. (1) $b_ib_j=b_ia_2 \cdot a_2b_j \in C(3) \cdot C(3) = C(1) \cup C(3) \cup C(2^2) \cup C(3^2) \cup C(5)$. Since $b_i \neq b_j$, $b_ib_j \notin C(1)$. Since $b_ib_j=b_ia_1 \cdot a_1^{-1}b_j$, $b_ia_1 \in C(2^2)$, $a_1^{-1}b_j \in C(2^2)$, and $a_1 \in C(3)$, by Lemma 10 $b_ib_j \notin C(5)$. If $b_ib_j \in C(3^2)$, then $b_ib_j=b_ia_2 \cdot a_2b_j$ and by Lemma 6 $b_ib_j=a_2b_j \cdot b_ia_2$ and so $a_2b_i \cdot b_j=b_jb_ia_2$. Therefore $(a_1a_2b_ib_j)^3 = a_1a_2b_ib_ja_1a_2b_ib_ja_1a_2b_ib_j = a_1a_2a_1a_2b_jb_ib_ib_ja_1a_2b_ib_j = b_ib_j \in C(3^2)$. On the other hand, $a_1a_2b_ib_j=a_1b_j \cdot b_ia_2 \in C(2^2) \cdot C(3)$ and from the multiplication table (M_3), there is no element of $C(2^2) \cdot C(3)$ such that it's third power belongs to $C(3^2)$. Therefore $b_ib_j \notin C(3^2)$. If $b_ib_j \in C(2^2)$, then b_i and b_j are commutative with each other. Now $b_ib_ja_2b_jb_i \in C(2^2)$, $a_2 \cdot b_ib_ja_2b_jb_i = a_2b_ia_2b_ja_2b_i = b_ia_2b_ib_ja_2b_i \sim b_ib_j \in C(2^2)$, and $a_1 \cdot b_ib_ja_2b_jb_i = b_ib_ja_1a_2b_jb_i \sim a_1a_2 \in C(3)$, hence by Lemma 12, $b_ib_ja_2b_jb_i$ must be equal to $a_1^{-1}a_2a_1$ or $a_1a_2a_1^{-1}$. If $b_ib_ja_2b_jb_i = a_1^{-1}a_2a_1$, then $a_1b_ib_j=a_2a_1b_ib_ja_2=(a_2a_1a_2)(a_2b_ib_ja_2)$, but $a_1(b_ib_j) \in C(3) \cdot C(2^2)$ and by the commutativity of a_1 and b_ib_j, the order of $a_1b_ib_j$ is 6, and so $a_1(b_ib_j) \in C(2^2, 3)$. Hence by Lemma 7 $b_ib_j=a_2b_ib_ja_2$ i. e. $(a_2b_ib_j)^2=1$, which is a contradiction. In the same way $b_ib_ja_2b_jb_i \neq a_1a_2a_1^{-1}$. Therefore $b_ib_j \notin C(2^2)$. Thus $b_ib_j \in C(3)$.

(2) $a_2b_i \cdot b_jb_i \in C(3) \cdot C(3)$ and $a_2b_ib_jb_i=(a_2a_1)(a_1^{-1}b_ib_jb_i)=(a_2a_1)(b_ia_1b_jb_i) \in C(2^2) \cdot C(3)$, hence from the multiplication tables (M_2) and (M_3) $a_2b_ib_jb_i \in C(3) \cup C(5) \cup C(2^2)$. If $a_2b_ib_jb_i \in C(5)$, then from $C(3) \cdot C(3) = 5C(5)+\cdots$, $a_2b_ib_jb_i$ is expressed in exactly five ways as a product of two elements

of $C(3)$. But by (1) $b_ib_jb_i=b_jb_ib_j$, hence $(a_2b_i)(b_jb_i)=(b_jb_i)(b_ib_ja_2b_ib_jb_i)=(b_ib_ja_2b_ib_jb_i)(b_ib_jb_ia_2b_jb_ia_2b_ib_jb_i)=(a_2b_j)(b_ib_j)=(b_ib_j)(b_jb_ia_2b_jb_ib_j)=(b_jb_ia_2b_jb_ib_j)(b_jb_ib_ja_2b_ib_ja_2b_jb_ib_j)$, and these six expressions are all distinct. For if $a_2b_i=b_ib_ja_2b_ib_jb_i$ then $(b_jb_i)(a_2b_i)=(a_2b_i)(b_jb_i)$, therefore $(a_2b_ib_jb_i)^3=1$, which is a contradiction. If $a_2b_i=b_jb_ia_2b_jb_ib_j$ then $b_ib_ja_2b_i=a_2b_jb_ib_j$ and the left belongs to $C(3)$, and the right belongs to $C(5)$, which is a contradiction. In the other cases, the proofs are similar. Thus $a_2b_ib_jb_i\notin C(5)$.

If $a_2b_ib_jb_i\in C(3)$, then $a_2b_ib_jb_ia_2b_ib_jb_ia_2b_ib_jb_i=1$, hence $a_2b_ib_ja_2b_ia_2\cdot b_jb_ia_2b_jb_ib_j=1$, and so $b_ib_ja_2b_ib_ja_2b_ib_ja_2b_ja_2b_ia_2b_j=1$, therefore $(a_2b_ib_j)^3\cdot a_2b_ja_2b_ia_2b_ja_2=1$. But $a_2b_ja_2b_ia_2b_ja_2\sim b_i\in C(2^2)$, therefore $(a_2b_ib_j)^3\in C(2^2)$, and from the multiplication table (M_3), $a_2b_ib_j\in C(2^2)\cup C(2^2,3)$. If $a_2b_ib_j\in C(2^2)$, then $a_1b_ib_jb_i=b_ia_1^{-1}b_jb_i\in C(2^2)$ and by the proof of (3) in Lemma 13, $a_2a_1b_ib_jb_i\in C(5)$. Since $a_2a_1b_ib_jb_i=a_2(b_ia_1^{-1}b_jb_i)=(a_2b_ib_j)(b_jb_ib_ia_1^{-1}b_jb_i)=(a_2b_ib_j)(a_1b_i)$, this contradicts (2) in Lemma 10. Thus $a_2b_ib_jb_i\notin C(3)$. Therefore $a_2b_ib_jb_i\in C(2^2)$.

(3) $(b_ib_j)(b_kb_j)=(b_ia_2)(a_2b_jb_kb_j)\in(C(3)\cdot C(3))\frown(C(3)\cdot C(2^2))=C(3)\cup C(2^2)\cup C(5)$. Assume that $b_i\neq b_jb_kb_jb_ib_jb_kb_j$, in which both sides belong to $C(2^2)$. By (2) $a_2\cdot b_jb_kb_jb_ib_jb_kb_j=b_jb_kb_ja_2b_ib_jb_kb_j\in C(3)$, $a_1\cdot b_jb_kb_jb_ib_jb_kb_j=b_jb_kb_ja_1^{-1}b_ib_jb_kb_j\in C(2^2)$. From (2) $a_2\cdot b_i\cdot b_jb_kb_jb_ib_jb_kb_j\cdot b_i=b_i\cdot b_jb_kb_jb_ib_jb_kb_j\cdot b_i\cdot a_2$, thus the left side $=a_2\cdot b_ib_jb_i\cdot b_ib_kb_i\cdot b_ib_j\cdot b_ib_jb_i\cdot b_ib_kb_i\cdot b_ib_jb_i=b_ib_jb_i\cdot b_ib_kb_i\cdot a_2b_ib_j\cdot b_ib_jb_i\cdot b_ib_kb_i\cdot b_ib_jb_i$, and transforming the right side in the same way, we have $a_2b_jb_i=b_jb_ia_2$. Hence $a_2b_jb_ib_j=b_jb_ia_2b_j$, but $a_2b_jb_ib_j\in C(2^2)$ and $b_jb_ia_2b_j\in C(3)$, which is a contradiction. Thus $b_i=b_jb_kb_jb_ib_jb_kb_j$ i. e. $(b_ib_jb_kb_j)^2=1$. Consequently, $b_ib_jb_kb_j\in C(2^2)$.

(4) $b_ib_jb_i\cdot b_kb_lb_k=(b_ib_j)(b_ib_kb_lb_k)\in C(3)\cdot C(2^2)$. From (3) $(b_ib_jb_ib_kb_lb_k)^2=b_ib_jb_i\cdot b_kb_lb_kb_ib_jb_ib_kb_lb_k=b_kb_lb_k\cdot b_ib_jb_i\cdot b_ib_jb_i\cdot b_kb_lb_k=1$. Therefore by the multiplication table (M_3), $b_ib_jb_i\cdot b_kb_lb_k\in C(2^2)$.

Lemma 15. *There are $n-2$ elements a_i $(i=1,2,\cdots,n-2)$ such that $a_1\in C(3)$, $a_2,\cdots,a_{n-2}\in C(2^2)$ and $a_ia_{i+1}\in C(3)$ $(i=1,2,\cdots,n-3)$, $a_ia_j\in C(2^2)$ $(i=1,2,\cdots,n-4,\ j>i+1)$.*

Proof. By Lemma 13, for $a_1\in C(3)$, $a_2\in C(2^2)$, and $a_1a_2\in C(3)$, there are $n-4$ elements $b_1,b_2,\cdots,b_{n-4}$ such that $b_i\in C(2^2)$, $a_1b_i\in C(2^2)$ and $a_2b_i\in C(3)$, $(i=1,2,\cdots,n-4)$. Put $a_3=b_1$, $a_4=b_1b_2b_1,\cdots,a_i=b_{i-3}b_{i-2}b_{i-3},\cdots,a_{n-2}=b_{n-5}b_{n-4}b_{n-5}$, then $a_3,a_4,\cdots,a_{n-2}\in C(2^2)$.

For $i\geqq 4$, $a_1a_i=a_1b_{i-3}b_{i-2}b_{i-3}=b_{i-3}a_1^{-1}b_{i-2}b_{i-3}\in C(2^2)$, and by (2) of Lemma 14 $a_2a_i=a_2b_{i-3}b_{i-2}b_{i-3}\in C(2^2)$. By (1) of Lemma 14 $a_3a_4=b_1\cdot b_1b_2b_1=b_2b_1\in C(3)$. For $i\geqq 5$, by (3) of Lemma 14 $a_3a_i=b_1\cdot b_{i-3}b_{i-2}b_{i-3}\in C(2^2)$. For $i\geqq 4$, $a_ia_{i+1}=b_{i-3}b_{i-2}b_{i-3}\cdot b_{i-2}b_{i-1}b_{i-2}=b_{i-2}b_{i-3}b_{i-1}b_{i-2}\in C(3)$. For $i\geqq 4$ and $j>i+1$, by (4) of Lemma 14 $a_ia_j=b_{i-3}b_{i-2}b_{i-3}\cdot b_{j-3}b_{j-2}b_{j-3}\in C(2^2)$.

Proof of Theorem:

By Lemma 15, there is a homomorphism from A_n to a subgroup H of G generated by $a_1, a_2, \cdots, a_{n-2}$. But since A_n is a simple group, A_n is isomorphic to H, and comparing the orders we have $H=G$ and $A_n \cong G$.

SUMIYOSHI HIGH SCHOOL

References

[1] W. Burnside: Theory of groups of finite order. Second edition, Cambridge Univ. Press, 1911.

[2] H. Nagao: *On the groups with the same table of characters as symmetric groups*, J. Polyt. Osaka City Univ. 8 (1957), 1–8.