ON PRIMITIVE EXTENSIONS OF RANK 3 OF SYMMETRIC GROUPS

TOSIRO TSUZUKU*

Dedicated to the memory of Professor TADASI NAKAYAMA

1. Let Ω be a finite set of arbitrary elements and let (G, Ω) be a permutation group on Ω. (This is also simply denoted by G). Two permutation groups (G, Ω) and (G, Γ) are called isomorphic if there exist an isomorphism σ of G onto H and a one to one mapping τ of Ω onto Γ such that $(g(i))^{\tau} = g^{\sigma}(i^{\tau})$ for $g \in G$ and $i \in \Omega$. For a subset Δ of Ω, those elements of G which leave each point of Δ individually fixed form a subgroup G_{Δ} of G which is called a stabilizer of Δ. A subset Γ of Ω is called an orbit of G_{Δ} if Γ is a minimal set on which each element of G induces a permutation. A permutation group (G, Ω) is called a group of rank n if G is transitive on Ω and the number of orbits of a stabilizer G_a of $a \in \Omega$, is n. A group of rank 2 is nothing but a doubly transitive group and there exist a few results on structure of groups of rank 3 (cf. H. Wielandt [6], D. G. Higman [4]).

Now we introduce the following definition:

Definition. A permutation group (G, Ω) is an extension of rank n of a permutation group (H, Γ) if (G, Ω) is a group of rank n and there exists an orbit Δ of a stabilizer G_a, $a \in \Omega$, such that G_a is faithful on Δ, i.e., only the identity element of G_a induces the identity permutation on Δ, and (G_a, Δ) is isomorphic to (H, Γ). Moreover, if (G, Ω) is primitive (or imprimitive), it is called a primitive (or imprimitive, resp.) extension of rank n.

In this note we will prove the following theorem.

THEOREM. *Let S_n be the symmetric group of degree n.*
If S_n has a primitive extension of rank 3, *then* $n = 1, 2, 3, 5,$ *or* 7.

2. We use the following notations:

Received May 17, 1965.

* This research was supported by the National Science Foundation, G 25213.

S_n: The symmetric group of degree n (on a set Γ).

A_n: The alternating group of degree n.

G: A primitive extension of rank 3 of S_n on a set $\Omega = \{0, 1, 2, \ldots, n, \tilde{1}, \tilde{2}, \ldots, \tilde{m}\}$ which consists of $1+n+m$ letters.

H: The stabilizer G_0 of a letter, say 0, of Ω.

The orbits of H are denoted by $\Delta_0 = \{0\}$, $\Delta_1 = \{1, 2, \ldots, n\}$ and $\Delta_2 = \{\tilde{1}, \tilde{2}, \ldots, \tilde{m}\}$ and the group (H, Δ_1) is isomorphic to (S_n, Γ).

L: The stabilizer of the subset $\{0, \tilde{1}\}$ of Ω.

Ψ: The character of G induced by the principal character of H which is called the character of the permutation representation of (G, Ω). By a well known theorem (cf. Proposition 29.2 in [6]) Ψ is decomposed into three irreducible characters φ_0, φ_1 and φ_2 and one of these, say φ_0, is the principal character. We denote the degree of φ_i by f_i. If $n \geqq 3$, then $n \neq m$ by Theorem 17.7 in [6] and so $f_1 \neq f_2$ by Theorem 30.3 in [6] and we assume $f_1 < f_2$.

${}_H\Psi$: The restriction to H of Ψ. By the structure of G, ${}_H\Psi$ is equal to $1_H + 1_{S_{n-1}}^{S_n} + 1_L^{S_n}$ where 1_X is the principal character of a group X and 1_X^Y is the character of Y induced by 1_X, that is, the permutation representation of a permutation group $(Y, Y/X)$.

$$q = (m+n+1) \cdot \frac{m \cdot n}{f_1 \cdot f_2}$$

$|X|$: The order of a group X.

We use the following propositions:

Proposition 1. (*W. A. Manning, Theorem* 17.7 *in* [6]). *If* $n > 2$, *then* $n < m \leqq n(n-1)$ *and* m *divides* $n(n-1)$.

Proposition 2. (*J. S. Frame* [2]). (*i*) q *is an integer, and* (*ii*) *if* $n \neq m$ *then* q *is a square.*

Proposition 3. (*D. G. Higman* [4]). *If* $1+n+m = n^2+1$, *then* $n = 2, 3, 7$ or 57.

Let V be a matrix $(v_{\alpha\beta})$, $\alpha, \beta \in \Omega$, of degree $1+n+m$ where

$$v_{\alpha\beta} = \begin{cases} 1 & \text{if there exists an element } g \text{ of } G \text{ such that } 0^g = \beta \text{ and } \alpha \in \Delta_1^g \\ 0 & \text{otherwise.} \end{cases}$$

Obviously, all diagonal elements of V are zero and all diagonal elements of V^tV are n. By calculating the traces of V and V^tV we have the following relations among f_1, f_2, m, n and the eigenvalues of V which are introduced by H. Wielandt (Chapter V in [6]):

PROPOSITION 4.

$$n+f_1s+f_2t=0$$
$$n^2+f_1s^2+f_2t^2=(m+n+1)n$$

where s and t are eigenvalues of V which have the multiplicities f_1 and f_2 respectively.

PROPOSITION 5. (*G. Frobenius* [3]). *Let X be a subgroup of S_n. Then*

(*i*) *If X is $S_2\times S_{n-2}$, then*

$$1_X^{S_n}=1_{S_n}+\chi^{\substack{0\cdots0\\0}}+\chi^{\substack{0\cdots0\\00}}$$

where $\chi^{\substack{0\cdots0\\0}}$ and $\chi^{\substack{0\cdots0\\00}}$ are irreducible characters of S_n (corresponding to Young diagrams $\substack{0\cdots0\\0}$ and $\substack{0\cdots0\\00}$ respectively) whose degrees are $n-1$ and $\frac{n(n-3)}{2}$ respectively).

(*ii*) *If X is $S_1\times S_1\times A_{n-2}$, then*

$$1_X^{S_n}=1_{S_n}+2\,\chi^{\substack{0\cdots0\\0}}+\chi^{\substack{0\cdots0\\0\\0}}\ \chi^{\substack{0\cdots0\\00}}$$
$$+\chi^{\substack{0\\\vdots\\0}}+2\,\chi^{\substack{00\\\vdots\\0}}+\chi^{\substack{000\\\vdots\\0}}+\chi^{\substack{00\\:0\\0}}$$

where $\chi^{\substack{0\cdots0\\0\\0}}$, $\chi^{\substack{0\\\vdots\\0}}$, $\chi^{\substack{00\\\vdots\\0}}$, $\chi^{\substack{000\\\vdots\\0}}$ and $\chi^{\substack{00\\:0\\0}}$ are irreducible characters of S_n of degrees $\frac{(n-1)(n-2)}{2}$, 1, $n-1$, $\frac{(n-1)(n-2)}{2}$ and $\frac{n(n-3)}{2}$ respectively.

3. *Proof of Theorem.* In the following we assume that $n\neq 1$, 2, 3, 5 and 7. According to Proposition 1, $(n-1)!>|L|\geqq(n-2)!$.

I. The case $|L|>(n-2)!$ and L is transitive on Δ_1.

If L is a primitive subgroup of (H, Δ_1), then, by a theorem of A. Bochert (Theorem 14.2, [6]), the index of L in H is not less than $\left[\frac{n+1}{2}\right]!$, that is, $n(n-1)>\left[\frac{n+1}{2}\right]!$ and so we have $n=8$, 6 or 4. For those values of n we know some properties of primitive subgroups of S_n (cf. [1], § 166). The orders of primitive groups of degree 8, not containing A_8, are not divisible by 5, but the order of L is divisible by 5. This is impossible. The orders of primitive subgroups of S_6 (or S_4) are divisible by 5 (or 3 resp.) and so, by Proposition 1, the order of L is divisible by 5! (or 3! resp.). This is a contradiction because $(n-1)! > |L|$. Hence L is imprimitive on Δ_1 and so there exists a non-trivial block Γ of (L, Δ_1). Let r be the length of Γ. Then the order of L must divide $(r!)^{\frac{n}{r}}\left(\frac{n}{r}\right)!$. Therefore, by Proposition 1, we have

$$(n-2)! \,\Big|\, (r!)^{\frac{n}{r}}\left(\frac{n}{r}\right)!.$$

From this formula we have that $n=4$ or 6. If $n=4$ then, by the assumption $(n-2)! < |L| < (n-1)!$, $|L| = 4$ and so the degree of (G, Δ) is equal to 11 and $q = \frac{11\cdot 4\cdot 6}{f_1\cdot f_2}$. This is a contradiction because q can not be a square for positive integers f_1, f_2 satisfying $f_1+f_2=10$. In the similar way, for the case $n=6$, we have $q = \frac{22\cdot 6\cdot 15}{f_1\cdot f_2}$ or $\frac{17\cdot 6\cdot 10}{f_1\cdot f_2}$ which also show us contradictions.

II. The case $|L| > (n-2)!$ *and* L *is intransitive on* Δ_1.

Since L is a subgroup of $S_r \times S_{n-r}$ with a positive integer r, we have the relation $(n-2)! \lneqq r!(n-r)!$ Hence we have the following cases (we assume $r \leqq n-r$): $r=1$ or 2.

(i) $r=1$: Since $L \leqq S_1 \times S_{n-1}$ and $(n-1)! > |L| > (n-2)!$, L must be $S_1 \times A_{n-1}$. Now we take up an element σ_0 of H which is a cycle of length 3 as an element of (H, Δ_1). Then we see that, as an element of (H, Δ_2), σ_0 is the product of disjoint two cycles of length 3. Therefore σ_0 is the product of disjoint three cycles of length 3 and $\Psi(\sigma) = 3n-8$. Let σ be an element of H which is the product of disjoint r cycles of length 3 as an element of (H, Δ_1). Then, in the similar manner, σ is the product of exactly disjoint $3r$ cycles of length 3. This concludes that if an element σ of H is conjugate to σ_0 in G then they are conjugate in H already. Hence the number of elements which are conjugate to σ_0 is

$[G : H]\cdot$*the number of elements of* H *which are conjugate to* $\sigma_0/\Psi(\sigma)$

$$= \frac{(3n+1)\cdot n!}{(3n-8)\cdot 3\cdot (n-3)!}$$

$$= \frac{(3n+1)n(n-1)(n-2)}{3(3n-8)}$$

Since this number is an integer, $3n-8$ must divide $8\cdot 5\cdot 2$ and this concludes $n=16$, 8, 6 or 4. If $n=16$, then, in the similar manner, the number of elements of G which are conjugate to an elements σ_1 of H which is a cycle of length 5 as an element of (H, Δ_1) is equal to $\dfrac{49\cdot 16!}{34\cdot 5\cdot 11!}$ and, since this number is not an integer, we have a contradiction. If $n=8$, then the number of elements of G which are conjugate to an element σ_2 of H which is the product of disjoint two cycles of length 2 as an elements of (H, Δ_1) is equal to $\dfrac{25\cdot 8!}{13\cdot 2^2\cdot 2\cdot 4!}$ and, since this number is not an integer, we have a contradiction. If n is either 6 or 4, the degree of (G, Ω) is a prime number and so, by theorems of Galois (Theorem 11.6 in [6]) and Burnside (Theorem 11.7 in [6]), (G, Ω) is a Frobenius group. This is a contradiction.

(ii) $r=2$: Since L is a subgroup of $S_2\times S_{n-2}$ and $(n-1)!>|L|>(n-2)!$, L must be $S_2\times S_{n-2}$. Then $H^{\Psi}=3\, 1_{S_n}+2\,\chi^{\substack{0\cdots0\\0}}+\chi^{\substack{0\cdots0\\00}}$ and so we have the following possibilities

$$f_1=n \qquad\qquad 2n-1$$
$$\text{or}$$
$$f_2=\frac{n(n-1)}{2} \qquad\qquad \frac{(n-1)(n-2)}{2}.$$

In the first case, according to Proposition 3, we have

$$n+sn+\frac{tn(n-1)}{2}=0$$
$$n^2+s^2n+\frac{t^2n(n-1)}{2}=\frac{n(n^2+n+2)}{2}$$

and so $n=\dfrac{t^2+4t}{2-t^2}$, that is, n is 2 or 5 which has been excluded. In the second case we have

$$q=\frac{n^2+n+2}{2}\times\frac{n^2(n-1)}{2(n-1)\cdot\dfrac{(n-1)(n-2)}{2}}=\frac{n^2(n^2+n+2)}{2(2n-1)(n-2)},$$

but this is not a square for any integer n. This is a contradiction, by Proposition 2.

III. The case $|L|=(n-2)!$. Then $m=n(n-1)$ and so the degree of (G, Ω) is n^2+1. By Proposition 3, $n=57$. $m=57\cdot 56=3192$ and so $q=\dfrac{3250\cdot 57\cdot 3192}{f_1\cdot f_2}$ must be a square. Then we have the following possibilities:

$$f_1 = 624 \qquad 1520$$
or
$$f_2 = 2625 \qquad 1729.$$

On the other hand, since L is intransitive and since $|L| = 55\,!$, $L = S_1 \times S_1 \times S_{55}$ or $L = S_2 \times A_{55}$ or $L =$ the group which consists of even permutations in $S_2 \times S_{55}$. In any of those cases, since $1_{S_1 \times S_1 \times A_{55}}^{S_{67}} = 1_L^{S_{67}} +$ a sum of characters of S_{67} and since $1 + 1_{S_{66}}^{S_{67}} + 1_{S_1 \times S_1 \times A_{55}}^{S_{67}}$ is decomposed into 13 irreducible characters which have degrees 1, 1, 1, 1, 56, 56, 56, 56, 56, 57•27, 57•27, 28•55 and 28•55 respectively, f_1 and f_2 must be partial sums of these integers, but it is impossible.

Thus we complete the proof of Theorem.

4. There exist primitive extensions of rank 3 of S_n for $n = 1, 2, 3, 5$ and 7.

(i) The cyclic group of order 3 is the unique primitive extension of S_1.

(ii) The dihedral group of order 10 is the unique primitive extension of S_2

(iii) The alternating group A_5 of degree 5 is the unique primitive extension of S_3.

(iv) Let N be the elementary abelian group of order 16 and let a_1, a_2, a_3, a_4, be a minimal set of generators of N. For any element σ of S_5 a permutation on the set $\{a_1, a_2, a_3, a_4, a_5 = a_1a_2a_3a_4\}$ defined by $\begin{pmatrix} a_1, & a_2, & a_3, & a_4, & a_5 \\ a_{\sigma(1)}, & a_{\sigma(2)}, & a_{\sigma(3)}, & a_{\sigma(4)}, & a_{\sigma(5)} \end{pmatrix}$ induces an automorphism $\bar{\sigma}$ of N. Thus S_5 is identified with an automorphism group H of N. Then we can see easily that the semidirect product S_5N is the unique primitive extension of rank 3 of S_5.

(v) Let F be the finite filed consisting of 5^2 elements and let σ be the involutive automorphism of F and let $U_3(F)$ be the projective special unitary group over F of dimension 3. Then σ induces an automorphism $\bar{\sigma}$ of $U_3(F)$. $U_3(F)$ contains a $\bar{\sigma}$ invariant subgroup H which is isomorphic to A_7 and the semidirect product $\langle\bar{\sigma}\rangle H$ of groups $\langle\sigma\rangle$, which is generated by $\bar{\sigma}$, and H is isomorphic to S_7 (H. H. Mitchell; Theorem 25, [5]). $U_3(F)$ is a primitive extension of rank 3 of A_7 (D. G. Higman [4]). Then the semidirect product $\langle\bar{\sigma}\rangle U_3(F)$ is a primitive extension of rank 3 of $\langle\bar{\sigma}\rangle H \cong S_7$.

References

[1] W. Burnside, Theory of groups of finite order, 2nd ed. Cambridge University Press, London, 1911.

[2] J. S. Frame, The double cosets of a finite group, Bull. Amer. Math. Soc., **47** (1941), 458-467.

[3] G. Frobenius, (i) Über die Charakter der symmetrishen Gruppe, Sitzber. Preuss. Akad., Berlin (1900), and, (ii) Über die Charaktere der alternierenden Gruppe, ibid. (1901), 303-315.

[4] D. G. Higman, Finite permutation group of rank 3, Math. Zeitshr. **86** (1964), 145-156.

[5] H. H. Mitchell, Determination of the ordinary and modular ternary linear groups, Trans. Amer. Math. Soc. **12** (1911), 207-242.

[6] H. Wielandt, Finite permutation groups, Academic Press, New York and London, 1964.

Nagoya University and
University of Illinois