ON DOUBLY TRANSITIVE GROUPS OF DEGREE n AND ORDER 2(n - 1)n

NOBORU ITO

Dedicated to the memory of Professor Tadasi Nakayama

Introduction

Let $\mathfrak{A}_5$ denote the icosahedral group and let $\mathfrak{H}$ be the normalizer of a Sylow 5-subgroup of $\mathfrak{A}_5$. Then the index of $\mathfrak{H}$ in $\mathfrak{A}_5$ equals six. Let us represent $\mathfrak{A}_5$ as a permutation group **A** on the set of residue classes of $\mathfrak{H}$ with respect to $\mathfrak{A}_5$. Then it is clear that **A** is doubly transitive of degree 6 and order 60 $=2\cdot5\cdot6$. Since $\mathfrak{A}_5$ is simple, **A** does not contain a regular normal subgroup.

Next let $SL(2, 8)$ denote the two-dimensional special linear group over the field $GF(8)$ of eight elements, and let s be the automorphism of $GF(8)$ of order three such that $s(x)=x^2$ for every element x of $GF(8)$. Then s can be considered in a usual way as an automorphism of $SL(2, 8)$. Let $SL^*(2,8)$ be the splitting extension of $SL(2, 8)$ by the group generated by s. Moreover let $\mathfrak{H}$ be the normalizer of a Sylow 3-group of $SL^*(2, 8)$. Then it is easy to see that the index of $\mathfrak{H}$ in $SL^*(2, 8)$ equals twenty eight. Let us represent $SL^*(2, 8)$ as a permutation group **S** on the set of residue classes of $\mathfrak{H}$ with respect to $SL^*(2, 8)$. Then it is easy to check that **S** is doubly transitive of degree 28 and order $1{,}512 = 2.27.28$. Since $SL(2, 8)$ is simple, **S** does not contain a regular normal subgroup.

The purpose of this paper is to prove the converse of these facts, namely to prove the following

Theorem. *Let Ω be the set of symbols* $1, 2, \ldots, n$. *Let $\mathfrak{G}$ be a doubly transitive group on Ω of order $2(n-1)n$ not containing a regular normal subgroup. Then $\mathfrak{G}$ is isomorphic to either* **A** *or* **S**.

1. Let $\mathfrak{H}$ be the stabilizer of the symbol 1 and let $\mathfrak{K}$ be the stabilizer of the set of symbols 1 and 2. Then $\mathfrak{K}$ is of order 2 and it is generated by an involution K whose cycle structure has the form $(1)(2)\ldots.$ Since $\mathfrak{G}$ is doubly

Received June 30, 1965.

https://doi.org/10.1017/S002776300002626X Published online by Cambridge University Press

transitive on Ω, it contains an involution I with the cycle structure $(12)\ldots$. Then we have the following decomposition of $\mathfrak{G}$:

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H} I \mathfrak{H}.$$

Since I is contained in the normalizer $Ns\mathfrak{K}$ of $\mathfrak{K}$ in $\mathfrak{G}$ and since $\mathfrak{K}$ has order two, I and K are commutative with each other. Hence for each permutation H of $\mathfrak{H}$ the residue class $\mathfrak{H}IH$ contains just two involutions, namely $H^{-1}IH$ and $H^{-1}KIH$. Let $g(2)$ and $h(2)$ denote the numbers of involutions in $\mathfrak{G}$ and $\mathfrak{H}$, respectively. Then the following equality is obtained:

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

2. Let $\mathfrak{K}$ keep i $(i \geqq 2)$ symbols of Ω, say $1, 2, \ldots, i$, unchanged. Put $\mathfrak{J} = \{1, 2, \ldots, i\}$. Then by a theorem of Witt ((4), Theorem 9.4) $Ns\mathfrak{K}/\mathfrak{K}$ can be considered as a doubly transitive permutation group on $\mathfrak{J}$. Since every permutation of $Ns\mathfrak{K}/\mathfrak{K}$ distinct from $\mathfrak{K}$ leaves by the definition of $\mathfrak{K}$ at most one symbol of $\mathfrak{J}$ fixed, $Ns\mathfrak{K}/\mathfrak{K}$ is a complete Frobenius group on $\mathfrak{J}$. Therefore i equals a power of a prime number, say p^m, and the order of $\mathfrak{H} \cap Ns\mathfrak{K}/\mathfrak{K}$ is equal to $i-1$. Since the order of $\mathfrak{K}$ is two, $Ns\mathfrak{K}$ coincides with the centralizer of $\mathfrak{K}$ in $\mathfrak{G}$. Therefore there exist $(n-1)n/(i-1)i$ involutions in $\mathfrak{G}$ each of which is conjugate to K.

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

$$h^*(2)n + (n-1)n/(i-1)i = (n-1)/(i-1) + h^*(2) + 2(n-1). \tag{2}$$

Since i is less than n, it follows from (2) that $h^*(2) \leqq 1$. Thus two cases are to be distinguished: (A) $h^*(2) = 1$ and (B) $h^*(2) = 0$. The following equalities are obtained from (2) for cases (A) and (B), respectively:

$$n = i^2 = p^{2m}, \qquad (p : \text{odd}). \tag{2. A}$$

and

$$n = i(2i-1) = p^m(2p^m - 1), \qquad (p : \text{odd}). \tag{2. B}$$

Next let us assume that n is even. Let $g^*(2)$ be the number of involutions in $\mathfrak{G}$ leaving no symbol of Ω fixed. Then corresponding to (2) the following equality is obtained from (1):

https://doi.org/10.1017/S002776300002626X Published online by Cambridge University Press

(3) $$g^*(2)+(n-1)n/(i-1)i=(n-1)/(i-1)+2(n-1).$$

Let J be an involution in $\mathfrak{G}$ leaving no symbol of Ω fixed. Let CsJ be the centralizer of J in $\mathfrak{G}$. Assume that the order of CsJ is divisible by a prime factor q of $n-1$. Then CsJ contains a permutation Q of order q. Since $n-1$, and therefore q, is odd, Q must leave just one symbol of Ω fixed. But this shows that Q cannot be commutative with J. This contradiction implies that $g^*(2)$ is a multiple of $n-1$. Now it follows from (3) that $g^*(2)\leqq n-1$. Thus again two cases are to be distinguished: (C) $g^*(2)=n-1$ and (D) $g^*(2)=0$. The following equalities are obtained from (3) for cases (C) and (D), respectively:

(3. C) $$n=i^2=2^{2m},$$

and

(3. D) $$n=i(2i-1)=2^m(2^{m+1}-1).$$

3. Case (A). Let $\mathfrak{P}'$ be a Sylow p-subgroup of $Ns\mathfrak{K}$. Let $Ns\mathfrak{P}'$ and $Cs\mathfrak{P}'$ denote the normalizer and the centralizer of $\mathfrak{P}'$ in $\mathfrak{G}$, respectively. Then, since $Ns\mathfrak{K}/\mathfrak{K}$ is a Frobenius group of degree p^m, $\mathfrak{P}'$ is elementary abelian of order p^m and normal in $Ns\mathfrak{K}$. Thus $Cs\mathfrak{P}'$ contains $\mathfrak{K}\mathfrak{P}'$. Now let $\mathfrak{P}$ be a Sylow p-subgroup of $Ns\mathfrak{P}'$. Then it follows from an elementary property of p-groups that $\mathfrak{P}$ is greater than $\mathfrak{P}'$. This implies that $Cs\mathfrak{P}'$ is greater than $\mathfrak{K}\mathfrak{P}'$. In fact, if $Cs\mathfrak{P}'=\mathfrak{K}\mathfrak{P}'$, then, since $\mathfrak{K}\mathfrak{P}'$ is a direct product of $\mathfrak{K}$ and $\mathfrak{P}'$, $\mathfrak{K}$ would be normal in $Ns\mathfrak{P}'$ and it would follow that $\mathfrak{P}=\mathfrak{P}'$. Let q ($\neq 2, p$) be a prime factor of the order of $Cs\mathfrak{P}'$ and let Q be a permutation of $Cs\mathfrak{P}'$ of order q. Then q must divide $n-1$ and hence Q must leave just one symbol of Ω fixed. But $\mathfrak{P}'$ does not leave any symbol of Ω fixed and therefore Q cannot belong to $Cs\mathfrak{P}'$. Assume that the order of $Cs\mathfrak{P}'$ is divisible by four. Let $\mathfrak{S}$ be a Sylow 2-subgroup of $Cs\mathfrak{P}'$. Then $\mathfrak{S}$ leaves just one symbol of Ω fixed. This, as above, shows that $\mathfrak{S}$ cannot be contained in $Cs\mathfrak{P}'$. Thus the order of $Cs\mathfrak{P}'$ must be of the form $2p^{m+m'}$ with $m\geqq m'>0$.

Now let $\mathfrak{P}''$ be a Sylow p-subgroup of $Cs\mathfrak{P}'$. Then clearly $\mathfrak{P}''$ is normal in $Ns\mathfrak{P}'$. Let $\mathfrak{V}$ be a Sylow p-complement of $Ns\mathfrak{K}$, which is a stabilizer in $Ns\mathfrak{K}$ of a symbol of $\mathfrak{J}$. Then decompose all the permutations ($\neq 1$) of $\mathfrak{P}''$ into $\mathfrak{V}$-conjugate classes. If $P\neq 1$ is a permutation of $\mathfrak{P}''$ and if $Cs\mathfrak{P}$ denotes the centralizer of P in $\mathfrak{G}$, then it can be seen, as before, that the order of $\mathfrak{V}\cap Cs\mathfrak{P}$

https://doi.org/10.1017/S002776300002626X Published online by Cambridge University Press

equals at most two. Thus every $\mathfrak{B}$-conjugate class contains either p^m-1 or $2(p^m-1)$ permutations and the following equality is obtained:

$$p^{m+m'}-1=x(p^m-1).$$

This implies in turn that;

$$x\equiv 1 \pmod{p^m} \text{ and } x>1; \ x=yp^m+1 \text{ and } y>0;$$
$$p^{m'}=(y-1)(p^m-1)+p^m; \ y=1 \text{ and finally } m'=m.$$

Thus $\mathfrak{P}''$ is a Sylow p-subgroup of $\mathfrak{G}$.

Now since the order of $Ns\mathfrak{K}$ equals $2(p^m-1)p^m$, $\mathfrak{K}$ is not contained in the center of any Sylow 2-subgroup of $\mathfrak{G}$. But obviously $Ns\mathfrak{K}$ contains a central element of some Sylow 2-subgroup of $\mathfrak{G}$. Let J be such a "central" involution in $Ns\mathfrak{K}$ (and of $Ns\mathfrak{P}''$). Then J leaves just one symbol of Ω fixed and therefore, as before, J is not commutative with any permutation $(\neq 1)$ of $\mathfrak{P}''$. Thus $\mathfrak{P}''$ must be abelian. By assumption $\mathfrak{P}''$ cannot be normal in $\mathfrak{G}$. Let $\mathfrak{D}$ be a maximal intersection of two distinct Sylow p-subgroups of $\mathfrak{G}$, one of which may be assumed to be $\mathfrak{P}''$. Assume that $\mathfrak{D}\neq 1$ and let $Ns\mathfrak{D}$ and $Cs\mathfrak{D}$ denote the normalizer and the centralizer of $\mathfrak{D}$ in $\mathfrak{G}$, respectively. Then, as it is well known, any Sylow p-subgroup of $Ns\mathfrak{D}$ cannot be normal in it. On the other hand, since $\mathfrak{P}''$ is abelian, it is contained in $Cs\mathfrak{D}$. Moreover, as before, the prime to p part of the order of $Cs\mathfrak{D}$ is at most two. This implies that $\mathfrak{P}''$ is normal in $Ns\mathfrak{D}$. Thus it must hold that $\mathfrak{D}=1$. Using Sylow's theorem the following equality is now obtained:

$$2(n-1)n/xn=yn+1.$$

This implies that $y=1$, $x=1$ and $n=3$.
Thus there exists no group satisfying the conditions of the theorem in Case (A).

4. Case (B). Likewise in Case (A) let $\mathfrak{P}$ be a Sylow p-subgroup of $Ns\mathfrak{K}$. Then, as before, $\mathfrak{P}$ is elementary abelian of order p^m and normal in $Ns\mathfrak{K}$. Since, however, $n=p^m(2p^m-1)$ in this case, $\mathfrak{P}$ is a Sylow p-subgroup of $\mathfrak{G}$. Let $Ns\mathfrak{P}$ and $Cs\mathfrak{P}$ denote the normalizer and the centralizer of $\mathfrak{P}$ in $\mathfrak{G}$, respectively. Let the orders of $Ns\mathfrak{P}$ and $Cs\mathfrak{P}$ be $2\,(p^m-1)p^m x$ and $2p^m y$, respectively. If $x=1$, then from Sylow's theorem it should hold that $(2p^m-1)(2p^m+1)\equiv 1 \pmod{p}$, which, since p is odd, is a contradiction. Thus x is

https://doi.org/10.1017/S002776300002626X Published online by Cambridge University Press

greater than one. If $y=1$, then $\mathfrak{K}$ would be normal in $Ns\mathfrak{P}$, and this would imply that $x=1$. Thus y is greater than one. Now y is prime to $2p$. In fact, y is obviously prime to p. If y is even, then let $\mathfrak{S}$ be a Sylow 2-subgroup of $Cs\mathfrak{P}$. Since then the order of $\mathfrak{S}$ must be greater than two, $\mathfrak{S}$ leaves just one symbol of Ω fixed. Hence $\mathfrak{S}$ cannot be contained in $Cs\mathfrak{P}$. Thus y must be odd. Therefore by a theorem of Zassenhaus ((5), p. 125) $Cs\mathfrak{P}$ contains a normal subgroup $\mathfrak{Y}$ of order y. $\mathfrak{Y}$ is normal even in $Ns\mathfrak{P}$.

Now likewise in Case (A) let $\mathfrak{V}$ be a Sylow p-complement of $Ns\mathfrak{K}$ and let us consider the subgroup $\mathfrak{Y}\mathfrak{V}$. Since $\mathfrak{Y}$ is a subgroup of $Cs\mathfrak{P}$, any permutation $(\neq 1)$ of $\mathfrak{Y}$ does not leave any symbol of Ω fixed. In particular, every prime factor of the order of $\mathfrak{Y}$ must divide $2p^m-1$. Since p^m-1 and $2p^m-1$ are relatively prime, it follows that every permutation $(\neq 1)$ of $\mathfrak{V}$ is not commutative with any permutation $(\neq 1)$ of $\mathfrak{Y}$. This implies that y is not less than $2p^m-1$. Thus it follows that $y=2p^m-1$ and that all the permutations $(\neq 1)$ of $\mathfrak{Y}$ are conjugate under $\mathfrak{V}$. Therefore $2p^m-1$ must be equal to a power of a prime, say q^l, and $\mathfrak{Y}$ must be an elementary abelian q-group. Let $Ns\mathfrak{Y}$ and $Cs\mathfrak{Y}$ denote the normalizer and the centralizer of $\mathfrak{Y}$ in $\mathfrak{G}$, respectively. Then it can be easily seen that $Cs\mathfrak{Y}=\mathfrak{P}\mathfrak{Y}$. Hence $Ns\mathfrak{Y}$ is contained in $Ns\mathfrak{P}$ and therefore we obtain that $Ns\mathfrak{Y}=Ns\mathfrak{P}$. On the other hand, it is easily seen that the index of $Ns\mathfrak{P}$ in $\mathfrak{G}$ is equal to $2p^m+1$. But then we must have that $2p^m+1\equiv 2 \pmod q$, which contradicts the theorem of Sylow.

Thus there exists no group satisfying the conditions of the theorem in Case (B).

5. Case (C). Since $n=2^{2m}$, $\mathfrak{H}$ contains a normal subgroup $\mathfrak{U}$ of order $n-1$. Let $\mathfrak{V}$ be a Sylow 2-complement of $Ns\mathfrak{H}$ leaving the symbol 1 fixed. Then $\mathfrak{V}$ is contained in $\mathfrak{U}$. Since $Ns\mathfrak{K}/\mathfrak{K}$ is a complete Frobenius group of degree 2^m, all the Sylow subgroups of $\mathfrak{V}$ are cyclic. Let l be the least prime factor of the order of $\mathfrak{V}$. Let $\mathfrak{L}$ be a Sylow l-subgroup of $\mathfrak{V}$. Let $Ns\mathfrak{L}$ and $Cs\mathfrak{L}$ denote the normalizer and the centralizer of $\mathfrak{L}$ in $\mathfrak{G}$. Then $\mathfrak{L}$ is cyclic and clearly leaves only the symbol 1 fixed. Hence $Ns\mathfrak{L}$ is contained in $\mathfrak{H}$. Because $Cs\mathfrak{L}$ contains $\mathfrak{K}$, using Sylow's theorem, we obtain that $Ns\mathfrak{L}=Cs\mathfrak{L}(Ns\mathfrak{K}\cap Ns\mathfrak{L})=Cs\mathfrak{L}(\mathfrak{K}\mathfrak{V}\cap Ns\mathfrak{L})$. Then it is easily seen that $Ns\mathfrak{L}=Cs\mathfrak{L}$. By the splitting theorem of Burnside $\mathfrak{G}$ has the normal l-complement. Continuing in the similar way, it can be shown that $\mathfrak{G}$ has the normal subgroup $\mathfrak{S}$, which is a complement of $\mathfrak{B}$. In particular, $\mathfrak{S} \cap \mathfrak{U} = \mathfrak{D}$ is a normal subgroup of $\mathfrak{U}$, which is a complement of $\mathfrak{B}$ and has order $2^m + 1$. Consider the subgroup $\mathfrak{D}\mathfrak{K}$. Then since every permutation $(\neq 1)$ of $\mathfrak{D}$ leaves just one symbol of Ω fixed, K is not commutative with any permutation $(\neq 1)$ of $\mathfrak{D}$, and therefore $\mathfrak{D}$ is abelian. $\mathfrak{S}$ is the product of $\mathfrak{D}$ and a Sylow 2-subgroup of $\mathfrak{G}$. Hence $\mathfrak{S}$, and therefore $\mathfrak{G}$, is solvable ((3)). Then $\mathfrak{G}$ must contain a regular normal subgroup.

Thus there exists no group satisfying the conditions of the theorem in Case (C).

6. Case (D). If $m = 1$, then it can be easily checked that $\mathfrak{G} = A$. Hence it will be assumed hereafter that m is greater than one.

Let $\mathfrak{S}$ be a Sylow 2-subgroup of $Ns\mathfrak{K}$ of order 2^{m+1}. Then, since $n = 2^m(2^{m+1} - 1)$ in this case, $\mathfrak{S}$ is a Sylow 2-subgroup of $\mathfrak{G}$. Let $\mathfrak{B}$ be a Sylow 2-complement of $Ns\mathfrak{K}$ of order $2^m - 1$. Then, since $Ns\mathfrak{K}/\mathfrak{K}$ is a complete Frobenius group of degree 2^m, $\mathfrak{S}/\mathfrak{K}$ is elementary abelian and normal in $Ns\mathfrak{K}/\mathfrak{K}$. Furthermore, all the elements $(\neq 1)$ of $\mathfrak{S}/\mathfrak{K}$ are conjugate under $\mathfrak{B}\mathfrak{K}/\mathfrak{K}$. Since I and K are commutative involutions, $\mathfrak{S}$ contains an involution S distinct from K. Thus every permutation $(\neq 1)$ of $\mathfrak{S}$ can be represented uniquely in the form either $V^{-1}SV$ or $V^{-1}SVK$, where V is any permutation of $\mathfrak{B}$. In fact, assume that $V^{-1}SV = V^{*-1}SV^*K$, where V and V^* are permutations of $\mathfrak{B}$. Then it follows that $V^*V^{-1}SVV^{*-1} = SK$ and $(V^*V^{-1})^2S(VV^{*-1})^2 = S$. But VV^{*-1} has an odd order, and this implies that $V = V^*$ and $K = 1$. This is a contradiction. Therefore $\mathfrak{S}$ is elementary abelian.

Let $Ns\mathfrak{S}$ denote the normalizer of $\mathfrak{S}$ in $\mathfrak{G}$. All the involutions of $\mathfrak{S}$ are conjugate in $\mathfrak{G}$ because of $g^*(2) = 0$. Hence they are conjugate already in $Ns\mathfrak{S}$ ((5), p. 133). Since $Ns\mathfrak{S}$ contains $Ns\mathfrak{K}$, it follows that the index of $Ns\mathfrak{K}$ in $Ns\mathfrak{S}$ equals $2^{m+1} - 1$. Let $\mathfrak{A}$ be a Sylow 2-complement of $Ns\mathfrak{S}$ of order $(2^{m+1} - 1)(2^m - 1)$. Then it follows that $\mathfrak{S}\mathfrak{B} = \mathfrak{S}(\mathfrak{A} \cap \mathfrak{S}\mathfrak{B})$. By a theorem of Zassenhaus ((5), p. 126) $\mathfrak{B}$ and $\mathfrak{A} \cap \mathfrak{S}\mathfrak{B}$ are conjugate in $\mathfrak{S}\mathfrak{B}$. Hence we can assume that $\mathfrak{B}$ is contained in $\mathfrak{A}$. Now every permutation $(\neq 1)$ of $\mathfrak{B}$ leaves just one symbol of Ω fixed, and all the Sylow subgroups of $\mathfrak{B}$ are cyclic. Therefore likewise in Case (C) it can be shown that $\mathfrak{A}$ has the normal subgroup $\mathfrak{B}$ of order $2^{m+1} - 1$. Every permutation $(\neq 1)$ of $\mathfrak{B}$ leaves no symbol of Ω fixed, hence it is not commutative with any permutation $(\neq 1)$ of $\mathfrak{B}$. Let B be a permutation of $\mathfrak{B}$ of a prime order, say q. Then all the permutations $(\neq 1)$ of $\mathfrak{B}$ are conjugate to either B or B^{-1} under $\mathfrak{B}$. This implies that $\mathfrak{B}$ is an elementary abelian q-group of order, say q^b. Then it follows that $2^{m+1}-1=q^b$. This implies that $b=1$ and $\mathfrak{B}$ is cyclic of order q. Hence $\mathfrak{B}$ is also cyclic.

Let $Ns\mathfrak{B}$ denote the normalizer of $\mathfrak{B}$ in $\mathfrak{G}$. Noticing that $2^m-1=\frac{1}{2}(q-1)$, let the order of $Ns\mathfrak{B}$ be equal to $\frac{1}{2}x(q-1)q$. Since $n=\frac{1}{2}q(q+1)$, $\mathfrak{B}$ cannot be transitive on Ω, and hence it cannot be normal in $\mathfrak{G}$. Therefore x is less than $(q+1)(q+2)$. Now using the theorem of Sylow we obtain the following congruence:

$$(q+1)(q+2)/x \equiv 1 \qquad (\text{mod. } q).$$

This implies that $(q+1)(q+2)=x(yq+1)$, where, since x is less than $(q+1)(q+2)$, y is positive. Then we obtain that $x=zq+2$, where z, since q is greater than two, is non-negative. Finally we obtain that $(q+1)(q+2)=(zq+2)(yq+1)$. This implies that z is not greater than one. If $z=1$, then the order of $Ns\mathfrak{B}$ equals $\frac{1}{2}(q-1)q(q+2)$. Hence there will be a permutation $X(\neq 1)$ of order dividing $q+2$, which belongs to the centralizer of $\mathfrak{B}$. But X leaves just one symbol of Ω fixed. Then X cannot be contained in the centralizer of $\mathfrak{B}$. This contradiction implies that $z=0$, $x=2$ and $y=\frac{1}{2}(q+3)$. In particular, $\mathfrak{B}$ coincides with is own centralizer, and the order of $Ns\mathfrak{B}$ equals $(q-1)q$.

If $\mathfrak{G}$ is solvable, then $\mathfrak{G}$ must have a regular normal subgroup, which is an elementary abelian group of a prime-power order. Since $n=\frac{1}{2}q(q+1)$, it is impossible. Thus $\mathfrak{G}$ must be nonsolvable.

Let $\mathfrak{N}$ be the least normal subgroup of $\mathfrak{G}$ such that $\mathfrak{G}/\mathfrak{N}$ is solvable. Then since $\mathfrak{N}$ is transitive on Ω, $\mathfrak{N}$ contains $\mathfrak{B}$ and an involution. Since all the involutions of $\mathfrak{G}$ are conjugate, $\mathfrak{N}$ contains $\mathfrak{S}$. Using Sylow's theorem, we obtain that $\mathfrak{G}=(Ns\mathfrak{B})\mathfrak{N}$. Therefore the order of $\mathfrak{N}$ is divisible by $q+2$. Let the order of $\mathfrak{N}$ be equal to $xq(q+1)(q+2)$. Then the order of $\mathfrak{N}\cap Ns\mathfrak{B}$ is equal to $2xq$. Thus the number of Sylow q-subgroups of $\mathfrak{N}$ is equal to $\frac{1}{2}q(q+3)+1$. On the other hand, since the order of $\mathfrak{B}$ equals q, it can be easily shown that $\mathfrak{N}$ is a simple group. Therefore by a theorem of Brauer ((1)) $\mathfrak{N}$ is isomorphic to the two-dimensional special linear group $LF(2, q+1)$ over the field of $q+1=2^{m+1}$ elements. In particular, it follows that $x=1$.

Using Sylow's theorem, we obtain that $\mathfrak{G}=\mathfrak{N}(Ns\mathfrak{N})$. Therefore there exist

$q+2$ distinct Sylow 2-subgroups in $\mathfrak{G}$. Let Γ be the set of all the Sylow 2-subgroups of $\mathfrak{G}$. Then, in a usual manner, we represent $\mathfrak{G}$ as a permutation group on Γ. As it is well known, $\mathfrak{N}$, and therefore $\mathfrak{G}$, is triply transitive on Γ. Let $\mathfrak{W}$ be the stabilizer of some two symbols of Γ. Then the order of $\mathfrak{W}$ is equal to $\frac{1}{2}(q-1)q$, and hence a Sylow q-subgroup of $\mathfrak{W}$ is normal in it. Therefore we can assume that $\mathfrak{W}=\mathfrak{A}$. Thus $\mathfrak{B}$ is the stabilizer of some three symbols of Γ. Let $\mathfrak{B}^*(\neq 1)$ be any subgroup of $\mathfrak{B}$, and put $\mathfrak{G}^*=\mathfrak{N}\mathfrak{B}^*$. Then $\mathfrak{G}^*$ is triply transitive on Γ, and $\mathfrak{B}^*$ is the stabilizer of the above three symbols of Γ in $\mathfrak{G}^*$. Let f be the number of symbols in the subset Δ of Γ, each symbol of which is left fixed by $\mathfrak{B}^*$. Then by a theorem of Witt ((4), Theorem 9.4) $\mathfrak{G}^*\cap Ns\mathfrak{B}^*$ is triply transitive on Δ. Therefore $\mathfrak{A}\cap\mathfrak{G}^*Ns\mathfrak{B}^*$ has an orbit in Δ of length $f-2$. But we already know that $\mathfrak{A}\cap Ns\mathfrak{B}^*=\mathfrak{B}$. Thus it follows that $\mathfrak{A}\cap\mathfrak{G}^*\supset Ns\mathfrak{B}^*=\mathfrak{B}^*$. This implies that $f=3$ and that $Ns\mathfrak{B}^*/\mathfrak{B}$ is isomorphic to the symmetric group of degree three.

Now let $\mathfrak{U}$ be the Sylow 2-complement of $\mathfrak{H}$ of order $\frac{1}{2}(q-1)(q+2)$. Then we can assume that $\mathfrak{B}$ is contained in $\mathfrak{U}$. Since m is greater than one, it follows that $q=2^{m+1}-1$ is not less than seven. Hence the order $q+2$ of $\mathfrak{N}\cap\mathfrak{U}$ is divisible by 3. Since $\mathfrak{N}\cap\mathfrak{U}$ is cyclic, it contains only subgroup $\mathfrak{T}$ of order three. $\mathfrak{T}$ is normal in $\mathfrak{U}$. On the other hand, since $\frac{1}{2}(q-1)$ is odd, $\mathfrak{T}$ is contained in the centralizer of $\mathfrak{B}$. Thus it follows that $\mathfrak{U}\cap Ns\mathfrak{B}^*=\mathfrak{B}\mathfrak{T}$. If $q+2$ has a prime factor l distinct from 3, then let $\mathfrak{L}$ be the Sylow l-subgroup of $\mathfrak{N}\cap\mathfrak{U}$ of order, say l^c. Then l^c is not greater that $(q+2)/3$. Now the above argument shows that l^c-1 is a multiple of $\frac{1}{2}(q-1)$. This contradiction implies that $q+2$ is equal to a power of 3, say, 3^a. Thus finally we obtain the following equality:

$$q+2=2^{m+1}-1=3^a.$$

This implies that $a=2$, $m=2$ and $q=7$. Then it is easy to check that $\mathfrak{G}$ is isomorphic to **S**.

Remark. Holyoke ((2)) proved a special case of the theorem: if $\mathfrak{H}$ is a dihedral group, then $\mathfrak{G}$ is isomorphic to **A**.

Bibliography

[1] R. Brauer, On the representations of groups of finite order, Proc. Nat. Acad. Sci.

U.S.A. **25**, 290–295 (1939).

[2] T. Holyoke, Transitive extens ons of dihedral groups, Math. Zeitschr. **60**, 79–80 (1954).

[3] N. Ito, Remarks on factorizable groups. Acta Sci. Math. Szeged **15**, 83–84 (1951).

[4] H. Wielandt, Finite permutation groups, Academic Press, New York-London (1964).

[5] H. Zassenhaus, Lehrbuch der Gruppentheorie, I, Teubner, Leipzig (1937).

Mathematical Institute,
Nagoya University