TRANSITIVE PERMUTATION GROUPS OF DEGREE $p=2q+1$, p AND q BEING PRIME NUMBERS

NOBORU ITO[1]

1. Introduction. Let p be a prime number such that $q=\frac{1}{2}(p-1)$ is also a prime. Let Ω be the set of symbols $1, \cdots, p$, and $\mathfrak{G}$ be a nonsolvable transitive permutation group on Ω. Such permutation groups were first considered by Galois in 1832 [**I**, §327; **III**, §262]: *if the linear fractional group $LF_2(l)$ over the field of l elements, where l is a prime number not smaller than five, contains a subgroup of index l, then l equals either five or seven or eleven.* These three permutation groups will be denoted by A_5, G_7 and G_{11}. G_7 has degree 7 and order 168; G_{11} has degree 11 and order 660. Next in 1861 two permutation groups, one, which has degree 11 and order 7,920, and the other, which has degree 23 and order 10,200,960, were found by Mathieu [**16**; **17**]. These two permutation groups will be denoted by M_{11} and M_{23}.

We say that $\mathfrak{G}$ is *a permutation group of type M*, if $\mathfrak{G}$ does not contain the alternating group A_p of the same degree. Then G_7, G_{11}, M_{11} and M_{23} are permutation groups of type M. Now the following problem arises: *does there exist any permutation group of type M different from G_7, G_{11}, M_{11} and M_{23}?*

In 1902 Jordan proved the nonexistence of permutation groups of type M for $p=47$ and $p=59$ [**23**; **IV**, §116]. In 1908 Miller proved the nonexistence of permutation groups of type M for $p=83$. But he did not even write down the proof explicitly [**18**].

Now $\mathfrak{G}$ is doubly transitive by a famous theorem of Burnside. In particular, the order of $\mathfrak{G}$ is divisible by q. Let $\mathfrak{Q}$ be a Sylow q-subgroup of $\mathfrak{G}$. Let $Ns\mathfrak{Q}$ and $Cs\mathfrak{Q}$ denote the normalizer and centralizer of $\mathfrak{Q}$ in $\mathfrak{G}$. In 1955 Fryer proved remarkable theorems [**7**], which may be stated as follows. *Let the index of $Cs\mathfrak{Q}$ in $Ns\mathfrak{Q}$ be even. Then* (i) *if $\mathfrak{G}$ contains an odd permutation, $\mathfrak{G}$ coincides with the symmetric group S_p of the same degree, and* (ii) *if $\mathfrak{G}$ does not contain any odd permutation and $Ns\mathfrak{Q}$ satisfies a certain appropriate condition, $\mathfrak{G}$ coincides with A_p.*

An address under the title *Permutation groups of prime degree*, delivered before the Chicago Meeting of the Society, on April 14, 1962 by invitation of the Committee to Select Hour Speakers for Western Sectional Meetings; received by the editors June 16, 1962.

[1] This address was delivered at a time the speaker was receiving support from the National Science Foundation (G-9654).