LIMITS OF THE DEGREE OF TRANSITIVITY OF SUBSTITUTION GROUPS.

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society, August 3, 1915.)

THE main object of the present paper is to establish an elementary theorem which gives always a smaller upper limit for the degree of transitivity of a substitution group of degree $n > 12$ which does not include the alternating group of this degree, than the one given by the commonly quoted theorem that this limit cannot exceed $\frac{1}{3}n + 1$.* The theorem to be established is a generalization of the one published by the present writer in volume 4, page 140, of this BULLETIN. In Pascal's Repertorium, loc. cit., a footnote states that the limit $\frac{1}{3}n + 1$ is actually attained by the five-fold transitive Mathieu group of degree 12. In view of the results of the present paper this footnote could be completed by adding that this limit cannot be attained for any degree which exceeds 12. It is clearly also attained when $n = 6$, although this is not mentioned in the footnote.

Let G be any transitive substitution group of degree $n = kp + r$, where p is a prime number such that $p > k$, and $r > k$, and all the symbols p, r, k represent positive integers. In what follows it will always be assumed that G is neither alternating nor symmetric on the n letters and that $k > 1$. If G is more than r-fold transitive it includes a transitive subgroup H of degree kp, and hence its order is divisible by p. A Sylow subgroup of order p^α contained in H must be intransitive and each of its transitive constituents must be of degree p, since G cannot involve a substitution composed of a single cycle of degree p, according to the well-known theorem that a primitive group which involves a cyclic substitution of degree p cannot be of degree greater than $p + 2$ unless it includes the alternating group of its own degree.

It may be assumed that H is composed of all the substitutions of G on a certain set of kp letters. Since it is assumed that

* Cf. Pascal's Repertorium der höheren Mathematik, vol. 1 (1910), p. 211; Encyclopédie des Sciences mathématiques, tome 1, vol. 1, p. 549; etc.

G is at least r-fold transitive there are at least $r!$ substitutions in G which transform among themselves the letters not contained in H according to the symmetric group on these r letters. In fact, the exact number of these substitutions is the order of H multiplied by $r!$, and all of these substitutions constitute a group H' which involves H invariantly. The Sylow subgroups of order p^α contained in H form a complete set of conjugates under H', and hence each of these Sylow subgroups is transformed into itself under H' by $r!$ times as many substitutions as under H. The largest subgroup of H' which transforms one of these Sylow subgroups into itself must have for one of its transitive constituents the symmetric group on the r letters of G which are not contained in H. We proceed to prove that this is impossible and hence that the assumption that G is more than r-fold transitive leads to an absurdity.

The Sylow subgroups of order p^α must be of degree kp, since H is transitive and its degree is divisible by p. Let P represent one of these subgroups and consider the group P' formed by all the substitutions of H' which transform the abelian group P into itself. The subgroup of P' which is composed of all the substitutions of P' which do not interchange any of the systems of intransitivity of P must be invariant. This subgroup P_1 must include P and the quotient group P_1/P must be cyclic, as we proceed to prove. It is at once evident that this quotient group is abelian, since the group of isomorphisms of the group of order p is cyclic and the transitive constituents of P_1 are all of degree p. Hence we may assume that the systems of intransitivity of P are transformed under P' according to the symmetric group of degree k. If the substitutions of P_1 did not transform into itself every subgroup of order p contained in P, it would follow that P could not contain a substitution involving a minimum number of cycles when this number is greater than unity.

When $r > 4$ it is clearly not necessary to prove that P_1/P is cyclic, since the alternating group whose degree exceeds 4 is simple. As the symmetric group of degree r constitutes a transitive constituent of P' and as the systems of intransitivity of P are transformed under P' according to a group whose order cannot exceed $k!$, it results that the part of P' which corresponds to the alternating group on $r!$ letters is the direct product of H and this alternating group. As this is impossible since G does not include the alternating group of degree n, we have established the following theorem: *A group of degree $n = kp + r$, $p > k$ and $r > k$, which is not alternating or symmetric, cannot be more than r times transitive unless $k = 1$ and $r = 2$.*

To prove that this theorem gives a much smaller upper limit for the degree of transitivity than $\frac{1}{3}n + 1$ whenever n is large, it is only necessary to use the well-known postulate of J. Bertrand, first proved by P. L. Tchebychef, that there is at least one prime number between x (exclusive) and $2x - 2$ (inclusive), whenever $x \geqq 3\frac{1}{2}$. Hence there is at least one prime number between $\sqrt{n}$ and $2\sqrt{n} - 2$ when $n > 12$, since n is an integer in the present consideration. If n is divided by this prime the quotient k is less than $\sqrt{n}$ and the remainder r must be less than $2\sqrt{n} - 2$. If this remainder does not exceed k we diminish k by unity and thus get a value of r which is less than $3\sqrt{n} - 2$ and greater than k. Hence it results from the theorem above that *when $n > 12$ a group of degree n cannot be $(3\sqrt{n} - 2)$-fold transitive.*

When $n \geqq 100$ this clearly gives a smaller upper limit for the degree of transitivity than $\frac{1}{3}n + 1$. That the theorem also gives a smaller upper limit when n lies between 12 and 100 can be easily verified directly. In fact, according to this theorem a group of degree 13 which is neither alternating nor symmetric cannot be more than triply transitive since $13 = 2 \cdot 5 + 3$. Such a group of degree 14 cannot be more than triply transitive since $14 = 11 + 3$, and hence such a group of degree 15 cannot be more than four-fold transitive. Such groups of degrees 16 and 17 cannot be more than triply transitive since $16 = 13 + 3$ and $17 = 2 \cdot 7 + 3$, and hence such a group of degree 18 cannot be more than four-fold transitive. Such a group of degree 19 cannot be more than four-fold transitive since $19 = 3 \cdot 5 + 4$. Such groups of degrees 20 and 22 cannot be more than triply transitive since $20 = 17 + 3$ and $22 = 19 + 3$, and hence such groups of degrees 21 and 23 cannot be more than four-fold transitive.

Similar considerations readily lead to the result that a group whose degree is less than 159, and which does not include the alternating group of its degree, cannot be as much as 8-fold transitive. In fact, by means of a table of prime numbers, it is very easy to verify that such a group can not be as much as 15-fold transitive, according to the theorem above, unless its degree exceeds 1,000, while the formula $\frac{1}{3}n + 1$ would place the upper limit of transitivity for such groups beyond 300. These illustrations may suffice to exhibit clearly that a much smaller upper limit for the degree of transitivity of a primitive group which is neither alternating nor symmetric results from the use of the present theorem than the one given by $\frac{1}{3}n + 1$, whenever n is large. When $n = 12 = 7 + 5$ the two theorems lead to the same upper limit. This is also true for the cases when n is 8 or 9. Since the groups whose degrees are less than 8 are so well known, it does not appear necessary to preserve the formula $\frac{1}{3}n + 1$ as an upper limit of the degree of transitivity of substitution groups which do not include the alternating group, especially since the theorem proved above is based upon such very elementary considerations.

UNIVERSITY OF ILLINOIS.

THE PERMUTATIONS OF THE NATURAL NUMBERS CAN NOT BE WELL ORDERED.

BY PROFESSOR A. B. FRIZELL.

(Read before the American Mathematical Society, February 27, 1915.)

LET us tabulate the natural numbers according to the number of their prime factors, viz., the nth row shall consist of the products $\pi(\nu, n)$ of n primes in order of magnitude. Form a new rectangular array wherein the nth column shall be composed of numbers from the nth row of the first scheme but arranged in rows by their column indices ν in the former, so that now the ith row contains those products $\pi(\nu, n)$ for which ν is a product of i primes. We obtain an infinite matrix of series

$$\begin{array}{l}
3,\ 5,\ 11,\ 17,\ 31, \cdots;\ 6,\ 9,\ 14,\ 21,\ 33, \cdots; \\
\quad 12,\ 18,\ 27,\ 30,\ 50, \cdots;\ 24,\ 36,\ 54,\ 60,\ 90, \cdots; \cdots \\
7, 13,\ 23,\ 29,\ 43, \cdots;\ 10, 15,\ 25,\ 26,\ 38, \cdots; \\
\quad 20,\ 28,\ 44,\ 45,\ 66, \cdots;\ 40,\ 56,\ 84,\ 88, 126, \cdots; \cdots \\
19, 37,\ 61,\ 71, 103, \cdots;\ 22, 34,\ 51,\ 57,\ 82, \cdots; \\
\quad 42,\ 52,\ 76,\ 92, 116, \cdots;\ 81, 100, 140, 152, 210, \cdots; \cdots \\
53, 89, 151, 173, 251, \cdots; 46, 69, 111, 121, 161, \cdots; \\
\quad 70, 105, 154, 171, 236, \cdots; 135, 196, 276, 306, 376, \cdots; \cdots \\
\qquad \cdot \quad \cdot \quad \cdot \qquad\qquad\qquad \cdot \quad \cdot \quad \cdot
\end{array}$$

It is proposed to form permutations of the natural numbers