MULTIPLY TRANSITIVE SUBSTITUTION GROUPS*

BY

G. A. MILLER

1. INTRODUCTION

A substitution group G of degree n is said to be r-fold transitive if each of the $n(n-1)\cdots(n-r+1)$ permutations of its n letters taken r at a time is represented by at least one substitution of G. It is not sufficient to say that each of its possible sets of r letters is transformed into every one of these sets by the substitutions of G. For instance, in each of the semi-metacyclic groups of degree p, p being a prime number of the form $4n+3$, every possible pair of its letters is transformed into every other such pair by the substitutions of the group and yet these groups are only simply transitive. Another well known definition of an r-fold transitive group of degree n is that this group contains a transitive subgroup of each of the degrees n, $n-1, \cdots, n-r+1$. It is obvious that these two definitions are equivalent and that if a group is r-fold transitive it is also $(r-\alpha)$-fold transitive, where α is a positive integer $\leqq r-1$.

It is not difficult to prove that a necessary and sufficient condition that a primitive group of degree n be r-fold transitive, $r>1$, is that it contain a doubly transitive group of degree $n-r+2$. This may have to coincide with the group itself if the group is only doubly transitive. To prove that such a group G must contain a triply transitive group of degree $n-r+3$, whenever $r>2$ it is only necessary to note that G involves a substitution which transforms at least one letter of the doubly transitive group of degree $n-r+2$ into a letter of this group while it transforms another letter of this group into a letter not involved therein since G is primitive. Hence G involves at least two primitive subgroups of degree $n-r+2$ which have at least one common letter but do not have all their letters in common. It must therefore involve two such primitive groups which have all except one letter of each in common. These two groups obviously generate a triply transitive group since they themselves are doubly transitive. When $r>3$ we may repeat this argument and prove the existence in G of a four-fold transitive group of degree $n-r+4$, etc. It must therefore contain a transitive group of each of the degrees $n, n-1, \cdots, n-r+1$.

---

* Presented to the Society, September 11, 1925; received by the editors in December, 1925.

The number of the largest transitive subgroups of degree $n-\alpha$, $\alpha \leqq r-1$, is obviously $n(n-1)\cdots(n-\alpha+1)$ and each of these conjugate subgroups is invariant under an intransitive subgroup of degree n which has for one of its transitive constituents the symmetric group of degree α. A necessary and sufficient condition that G be symmetric is that this intransitive group be the direct product of its transitive constituents, and if one such intransitive group is the direct product of its transitive constituents every one of them must have this property. In all other multiply transitive groups these intransitive groups, for $\alpha=2$, have at least one transitive constituent whose order is equal to the order of this intransitive group. A necessary and sufficient condition that all these intransitive groups are dimidiations, when $n>4$, is that G is an alternating group. In this case they are always dimidiations between symmetric groups. Hence the following theorem:

If G is an r-fold transitive group of degree n then each of its subgroups of order g_α and of degree $n-\alpha$, $\alpha \leqq r-1$, which is not contained in a larger subgroup of this degree, is transitive and is invariant under an intransitive group of degree n and of order $g_\alpha \cdot \alpha!$ but under no larger group. This intransitive group has for one of its transitive constituents the symmetric group of degree α, and its other transitive constituent is simply isomorphic with this intransitive group whenever G is not symmetric or alternating, and only then when $\alpha>2$.

From the preceding theorem it results directly that whenever $r>3$ the largest transitive groups of degree $n-r+1$ contained in G cannot be cyclic since the group of isopmorphisms of a cyclic group is abelian. In fact when G is not alternating or symmetric, the largest transitive subgroups of degree $n-\alpha$ must be invariant under a group of this degree whose order is $\alpha!$ times the order of this largest transitive group, and the corresponding quotient group must be the symmetric group of degree α. In particular, when $n-\alpha$ is a prime number p then $n \leqq p+2$. When G is exactly r-fold transitive, $n-2>r>1$, it can obviously not contain a transitive group of degree $n-r$ but it may possibly contain such groups of a lower degree. If such a transitive group appears in G it must be imprimitive and G must involve also imprimitive groups of a larger degree. In fact, the largest transitive subgroups of the former degree are known to be imprimitive, and since G is primitive two such subgroups which have the largest possible number of common letters must have a common system of imprimitivity since they cannot generate a group whose degree is only one larger than their common degree. The letters which appear in one of these subgroups but not in the other form one set of a system of imprimitivity of this group.

Whenever a substitution group of degree n transforms every possible set of r, $r<n$, of its letters into every other such set the group must be primitive unless $r=1$ or $n-1$. Since a transitive group of degree n could be defined as a group in which every possible set of $n-1$ of its letters is transformed into every other such set, it results directly that an r-fold transitive group could not be defined as one in which all the possible sets composed of r of its letters are transformed transitively under the group. The fact that when $1<r<n-1$ every group which transforms all its possible sets of r letters transitively must be primitive results almost directly from the definitions of intransitive and primitive groups, since in the latter groups it would be possible to choose two such sets in such a manner that they would obviously not be conjugate under the group. Hence the following theorem:

If a substitution group of degree n has the property that every possible set of r of its letters, $1<r<n-1$, is transformed transitively under the group, then this group must be primitive.

2. Regular subgroups of odd prime order

It is well known that a primitive group of degree n which is not alternating or symmetric cannot contain a regular subgroup of odd prime degree p unless n has one of the three values p, $p+1$, $p+2$. In particular, such a primitive group G of degree $p+k$ cannot be more than k times transitive whenever $k>2$. We proceed to establish the following theorem:

If a primitive group involves a regular subgroup of odd prime order p, all such subgroups generate a simple group unless p is the form $2^\alpha-1$. In this case they generate either a simple group of composite order or a subgroup of the holomorph of the abelian group of order 2^α and of type $(1, 1, 1, \cdots)$.

As regards the alternating and the symmetric groups this theorem is obviously true. In fact, in this case these regular subgroups always generate the alternating group whose degree is equal to the degree of the group. When the degree of G is p the theorem is well known and obvious. When the degree of G is $p+1$ it must be multiply transitive and to an invariant subgroup of G there must correspond an invariant subgroup of the group composed of all the substitutions of G which omit one letter. Since the latter is generated by operators of order p whenever the former is thus generated it must be simple and the former contains no invariant subgroup except the identity and possibly one of order $p+1$. The latter can exist only when $p+1=2$, since the only regular group of order $p+1$ which has an operator of order p in its group of isomorphisms is the abelian group of order 2^α and of the type $(1, 1, 1, \cdots)$.

It remains to consider the case when the degree of G is $p+2$. Since the regular subgroups of order p are transformed into themselves by twice as many substitutions under G as under a subgroup composed of all the substitutions of G which omit a given letter, it results that $p+1$ cannot be divisible by 4. That is, *a triply transitive group of degree $p+2$, p being an odd prime number, must be composed of positive substitutions, and such a group cannot exist unless p is of the form $4k+3$.* If G exists it cannot involve an invariant subgroup of order $p+2$ since a group of this order cannot have an operator of order p in its group of isomorphisms. Hence G cannot contain an invariant subgroup of order $(p+1)(p+2)$. That is, the operators of order p contained in G generate a simple group of composite order and the quotient group of G with respect to this invariant subgroup is a cyclic group of odd order. This order is a divisor of $p-1$.

A triply transitive group of degree $p+2$ is completely determined by any one of its maximal doubly transitive subgroups of degree $p+1$ in the sense that only one triply transitive group of degree $p+2$ can involve a given group of degree $p+1$ as the subgroup composed of all its substitutions which omit a given letter. In particular, the number of the triply transitive substitution groups of degree $p+2$ can certainly not exceed the number of the doubly transitive groups of degree $p+1$. It may also be noted that if the doubly transitive groups of degree $p+1$ are given it is very easy to determine all the possible triply transitive groups of the degree $p+2$, since it is only necessary to take any one of the p substitutions of order 2 and degree $p-1$ which transform into its inverse an arbitrary substitution of order p contained in this doubly transitive group and annex to this substitution a transposition composed of the remaining letter of this doubly transitive group and an arbitrary letter not found therein. A necessary and sufficient condition that the triply transitive group of degree $p+2$ exist is that the given substitution and the given doubly transitive group generate a group whose order does not exceed $p+2$ times the order of this doubly transitive group.

Just as a characteristic subgroup which appears in every other characteristic subgroup but is not the identity has been called the fundamental characteristic subgroup so we may define the term *fundamental invariant subgroup* as an invariant subgroup which is not the identity but appears in every other possible invariant subgroup of the group. From the preceding developments it follows almost directly that *if a substitution composed of a single cycle involving an odd prime number p of letters appears in a primitive group then all such substitutions found in this group generate a fundamental invariant subgroup of the group unless $p+1$ is of the form 2^α and the group is*

contained in the holomorph of the abelian group of order 2^α *and of type* $(1, 1, 1, \cdots)$.

3. Substitutions composed of two cycles of odd prime order

If a primitive group G which is neither alternating nor symmetric involves a substitution s_1 *composed of two cycles of prime order p the degree of G cannot exceed* $2p+6$. Since the primitive groups whose class does not exceed six are all well known,* we shall assume in what follows that $p>3$. Suppose that the degree of G is larger than $2p+6$. Since G is primitive it contains a substitution s_2 which is similar to s_1 and involves at least one letter of s_1 and also at least one letter not found in s_1. The group generated by s_1 and s_2 cannot have three systems of intransitivity since it cannot contain a transitive constituent of order p, nor can it contain a substitution composed of a single cycle of order p according to the preceding section. The proof of the fact that it cannot contain a transitive constituent of order p results almost directly from the following theorem: *If a group contains two transitive subgroups which have at least one letter in common it must also contain two conjugate transitive subgroups which have all their letters in common except possibly those found in a system of imprimitivity of one of these groups. In particular, if one of these groups is primitive the given transitive subgroups involve all except possibly one of the letters of this primitive group.*

If the group generated by s_1 and s_2 is transitive it may be assumed according to the theorem stated above that the degree of this group is either $2p+1$ or $2p+2$. In the former case it would have to be primitive, and hence this is impossible. If in the latter case it is imprimitive its systems of imprimitivity are permuted under the group according to a doubly transitive group of degree $p+1$. If this group of degree $2p+2$ could be found in an imprimitive group of degree $2p+4$, its systems of imprimitivity would be transformed according to a triply transitive group of degree $p+2$. According to the preceding section this imprimitive group of degree $2p+4$ could not appear in an imprimitive group of degree $2p+6$ and hence the group of degree $2p+6$ would be at least doubly transitive. Since the substitution s_1 can not appear in a group of degree $2p+k$, $k>2$, which is as much as k times transitive, it has been proved that the group generated by s_1 and s_2 cannot be assumed to be transitive. It should be noted that the proof of the theorem that a group of degree $2p+k$, $k>2$, cannot be more than k times transitive implies that such a group cannot be as much as k times transitive when it involves a substitution composed of two cycles of order p.†

* Cf. W. A. Manning, these Transactions, vol. 4 (1903), p. 351.

† G. A. Miller, Bulletin of the American Mathematical Society, vol. 4 (1898), p. 143.

It remains to consider the case when every pair of substitutions such as s_1 and s_2 generates a group which has two and only two transitive constituents and the order of each transitive constituent exceeds p. By extending the group generated by s_1 and s_2 by the other similar substitutions, we cannot construct a group whose degree exceeds $2p+4$ without arriving at an intransitive group which has alternating transitive constituents. Such an intransitive group would have a class which could not exceed 6 and must therefore be excluded. Hence we have the result, just as in the preceding cases, that the degree of G cannot exceed $2p+6$, and the theorem announced in the first paragraph of this section has been established.

4. Substitutions composed of three or more cycles of odd prime order

Suppose that G is of degree $3p+k$, $p>3$, $k>3$, and assume that G is k-fold transitive. From the preceding section it results that there is no substitution in G composed of two cycles of order p, and hence the order of G is not divisible by p^2 when $k>5$. If G involves a substitution s composed of three cycles of order p, all of its subgroups of order p must be conjugate under G. In fact, the subgroups of order p which are contained in a group H composed of all the substitutions of G which omit k letters must be conjugate under H. Hence the subgroup composed of all the substitutions of G which transform into itself a subgroup of order p must have for one of its transitive constituents the symmetric group of degree k. To the identity of this constituent there must correspond the subgroup of H which transforms into itself the given subgroup of order p.

As k was assumed to be 4, for the present, it is obvious that to the invariant subgroup of order 4 in the symmetric constituent of degree k there has to correspond a subgroup involving substitutions in each co-set corresponding to this subgroup of order 4 which do not interchange the systems of intransitivity of the given subgroup of order p. Since this subgroup of order 4 is non-cyclic while the group of isomorphisms of the group of order p is cyclic, it results that G must involve substitutions containing no more than four letters. Since this is impossible, it has been proved that G cannot exist for $k=4$ and hence it cannot exist for larger values of k. It has therefore been proved that a substitution group of degree $3p+k$, $k>3$, which is k-fold transitive cannot involve any substitution composed of three cycles of odd prime order. *In particular, a group of degree* $3p+k$, $p>3$, $k>3$, *cannot be more than k-fold transitive.*

Suppose that G is of degree $lp+k$, $p>3$, $p>k>l$, and suppose that G contains a substitution of order p and of degree lp. If G is k-fold transitive

each of its Sylow subgroups of order p^m is invariant under an intransitive group which has for one of its transitive constituents the symmetric group of degree k. Each one of the l systems of intransitivity of the Sylow subgroup of order p^m is transformed into itself by at least some of the substitutions which correspond to each one of the substitutions of the alternating group of degree k contained in the given symmetric constituents of degree k. Hence it results that G must involve the substitutions of this alternating group. This is obviously impossible and hence G cannot be k-fold transitive if it involves substitutions of order p and of degree lp. If G were $(k+1)$-fold transitive it would clearly involve such substitutions. We have therefore established the following theorem:

*If a substitution group is of degree $lp+k$, p being a prime number, $p>l<k$, then this group cannot be more than k-fold transitive, $k>2$, unless it is the alternating or the symmetric group.**

If in the preceding theorem we assume that $p>\sqrt{n}$, where n is the degree of G, it results that k may be selected so as not to exceed $p+l+1$. In fact, if k were greater than this number, we could increase the value of l by unity and thus reduce the value of k by p, provided l is less than $p-1$, as it will be when p is properly chosen, according to the well known theorem that for every integer $x>7$ there is at least one prime p such that

$$x/2<p\leqq x-3\ .\dagger$$

Hence it results that when p is a prime number which exceeds the smallest integer greater than $\sqrt{n}$ it may be assumed that p is not larger than $2\sqrt{n}-1$. Hence k can always be so selected as not to exceed $5\sqrt{n}/2$. For large values of n this obviously gives a much smaller upper limit for the multiplicity of a transitive group than the limit commonly given, viz., $n/3+1$.‡

It should be added that in view of the fact that the prime numbers are usually much closer together than the given formula due to P. L. Tschebychef indicates, the theorem given at the close of the preceding paragraph is much more useful than the formula $n/3+1$ for the determination of the upper limit of the multiplicity of transitivity. For instance, p may be so selected that by means of this theorem it follows directly that no group whose degree does not exceed 200 can be more than 8-fold transitive without involving the alternating group.

* G. A. Miller, Bulletin of the American Mathematical Society, vol. 22 (1915), p. 70.

† Cf. G. A. Miller, School Science and Mathematics, vol. 21 (1921), p. 874.

‡ Cf. Pascal's *Repertorium der höheren Mathematik*, vol. 1, 1910, p. 211.

UNIVERSITY OF ILLINOIS,
URBANA, ILL.