

ON THE LIMIT OF TRANSITIVITY OF THE MULTIPLY TRANSITIVE SUBSTITUTION GROUPS THAT DO NOT CONTAIN THE ALTERNATING GROUP.

BY DR. G. A. MILLER.

(Read before the American Mathematical Society at the Meeting of December 29, 1897.)

WE shall first state a few known principles in the form in which we shall employ them. A k times transitive group (G) involving the following n elements

$$a_1, a_2, a_3, \dots, a_n$$

contains a simply transitive subgroup (G_1) which is composed of all the substitutions of G that do not contain any one of the following $k - 1$ elements

$$a_1, a_2, a_3, \dots, a_{k-1}$$

It also contains a doubly transitive subgroup (G_2) which is composed of all the substitutions of G that do not contain any one of the following $k - 2$ elements

$$a_1, a_2, a_3, \dots, a_{k-2}$$

etc.

It follows from the definition of a k times transitive group that G contains a subgroup (K_1) which has for one of its transitive constituents the symmetric group of degree k . This constituent cannot be multiply isomorphic to the other constituent of K_1 , since G does not include the alternating group of degree n . Hence these two constituents of K_1 have a 1, a isomorphism to each other, a being the number of the substitutions of G that do not contain any one of the following k elements

$$a_1, a_2, a_3, \dots, a_k$$

Since these a substitutions form a selfconjugate subgroup of the second constituent of K_1 , which corresponds to identity in the symmetric group of degree k , the order of K_1 must be $ak!$ while that of G is $a(n - k + 1)(n - k + 2) \dots (n - 1)n$.

G contains also a subgroup (K_2) which has for one of its transitive constituents the symmetric group of degree $k - 1$ and for the other constituent a transitive group which has

an $a(n - k + 1)$, 1 isomorphism to this symmetric group. The self-conjugate subgroup of the transitive constituent, corresponding to identity in the symmetric group, is G_1 . Similarly, G contains a subgroup (K_s) which has for one of its transitive constituents the symmetric group of degree $k - 2$ and for the other an at least doubly transitive group which has an $a(n - k + 1)(n - k + 2)$, 1 isomorphism to this symmetric group. G_2 corresponds to identity in this isomorphism, etc. The orders of K_2, K_3, \dots are $a(n - k + 1)(k - 1)!, a(n - k + 1)(n - k + 2)(k - 2)!, \dots$

What precedes includes the following:

THEOREM I. *When a group of degree n is k times transitive there must be an at least β times transitive group of degree $(n - k + \beta)$, ($\beta = 1, 2, 3, \dots, k - 2$), whose quotient group with respect to some selfconjugate subgroup is the symmetric group of degree $k - \beta$.*

COROLLARY. *When no at least a times transitive group of degree n is isomorphic to the symmetric group of degree k a group of degree $n + k$ cannot be more than $k + a - 1$ times transitive.*

In order to employ this corollary it is necessary to know the quotient groups of the a times transitive groups of degree n . It is not necessary to consider the alternating or the symmetric group of degree n , since the primitive groups that include such a group are either alternating or symmetric. The simplest case occurs when n is a prime number (p). We shall begin with this case.

All the subgroups of order p that are found in a transitive group of degree p are conjugate. Since such a group is primitive all its selfconjugate subgroups, except identity, are transitive and, therefore, include all the substitutions of order p . If the order of such a selfconjugate subgroup is equal to the order of the group divided by a there are a times as many substitutions of the group that transform a given subgroup of order p into itself as there are substitutions having this property in the selfconjugate subgroup. The quotient group with respect to the given selfconjugate subgroup must, therefore, be isomorphic to the metacyclic group of degree p or to one of its subgroups. Hence we have the

LEMMA I. *The quotient group of any transitive group of degree p with respect to a selfconjugate subgroup that exceeds identity is cyclical.*

If we let $a = 1$ and $k = 3$ in the given corollary we obtain by means of this lemma that a group of degree $p + 3$ cannot be more than three times transitive. Hence we have the

THEOREM II. *A transitive group of degree p cannot occur as a*

subgroup of any primitive group except those of degree p , $p + 1$, and $p + 2$.*

COROLLARY. A group of degree $p + k$, $k > 2$, cannot be more than k times transitive.

This important corollary is due to Jordan.†

When a primitive group is of degree $2p$ its order is divisible by p but not by p^2 ; for, if its order were divisible by p^2 it would contain a commutative subgroup of this order and hence it would have to contain a transitive subgroup of degree p . All its subgroups of order p must therefore be conjugate and all its substitutions of this order must be included in every selfconjugate subgroup, except identity. Hence every quotient group with respect to a selfconjugate subgroup whose order exceeds unity is isomorphic to the subgroup which includes all the substitutions that transform a given subgroup of order p into itself.

Since every simple isomorphism of a metacyclic group, or one of its subgroups, to itself can be obtained by transforming it by means of given substitutions, it follows that the quotient group, with respect to a selfconjugate subgroup whose order exceeds 2, of the given subgroup that contains all the substitutions of the primitive group which transform the cyclical subgroup of order p into itself is commutative. It is either cyclical or contains a cyclical subgroup of half its order. Hence we obtain the following

LEMMA II. *The quotient group of any primitive group of degree $2p$ with respect to a selfconjugate subgroup whose order exceeds unity is commutative. It is either cyclical or it contains a cyclical subgroup of half its order.*

We consider now the nonprimitive groups of degree $2p$ which contain two systems of nonprimitivity without containing also p such systems and whose orders are not divisible by p^2 . The subgroup which includes all the substitutions that do not interchange the systems of nonprimitivity is formed by making a transitive group of degree p simply isomorphic to itself. Hence every selfconjugate subgroup whose order exceeds unity includes all the substitutions of order p . In exactly the same way as we pursued above we obtain the following:

LEMMA III. *The quotient group, with respect to any selfconjugate subgroup except unity, of any nonprimitive group of degree $2p$ which contains two systems of nonprimitivity without containing also p such systems and whose order is not divisible by p^2 is com-*

* Such a transitive group occurs in every symmetric or alternating group whose degree exceeds $p - 1$, but we do not consider these groups in this paper

† *Bulletin de la Société Mathématique de France*, vol. 1, p. 41.

mutative. It is either cyclical or it contains a cyclical subgroup of half its order.

The nonprimitive groups of degree $2p$ which contain p systems of nonprimitivity are isomorphic to transitive groups of degree p . The selfconjugate subgroup which corresponds to identity in this isomorphism is of order 2^a . It is easy to see that the quotient group of such a nonprimitive group cannot be the symmetric group of order 6 when $p > 3$; for if we take a quotient group with respect to a selfconjugate subgroup that includes all of the given 2^a substitutions it is either a cyclical group or a transitive group of degree p . If the given selfconjugate subgroup includes only half of the given 2^a substitutions the quotient group contains a selfconjugate subgroup of order 2, and if it includes less than half the order of the quotient group is divisible by 4. Hence we have

LEMMA IV. *A transitive group of degree $2p$, $p > 3$, which does not contain any regular substitution of degree p cannot be isomorphic to the symmetric group of order 6.*

Letting $a = 1$ and $k = 3$ in the corollary under theorem I we observe by means of this lemma and the fact that no group of degree 7 or 9 is more than 3 times transitive; that a group of degree $2p + 3$ cannot be more than 3 times transitive. Hence we have the

THEOREM III. *A group of degree $2p + k$, $k > 2$, cannot be more than k times transitive.**

It may happen that this theorem will give a lower limit of transitivity than the corollary under theorem II., *e. g.*, $17 = 2 \times 7 + 3$ or $13 + 4$. Hence a group of this degree cannot be more than 3 times transitive, according to this theorem and no more than 4 times according to the given corollary. On the contrary, $100 = 97 + 3$ or $2 \times 47 + 6$. Hence a group of degree 100 cannot be more than 3 times transitive according to the given corollary and no more than 6 times according to this theorem.

It may be observed that we have used only K_2 in seeking for these limits of transitivity. K_3, K_4, \dots are, in general, not so suitable to find low limits, since the corresponding symmetric groups are of lower degrees. As the degree of K_1 is not always equal to $n - k$, it also does not appear to be as suitable for this purpose as K_2 . For low limits of transitivity of the groups of a general degree we must refer to the articles of Jordan and Bochert in recent volumes of *Liouville's Journal* and *Mathematische Annalen* respectively.

CHICAGO, October, 1897.

* In the corresponding theorem Jordan assumes that $k > 3$ when p is of the form $3m + 1$, *loc. cit.*