THE SUBGROUP COMPOSED OF THE SUBSTITUTIONS WHICH OMIT A LETTER OF A TRANSITIVE GROUP[*]

BY

G. A. MILLER

1. Introduction

In a transitive group of order g and of degree n the subgroup G_1 composed of all the substitutions of G which omit a given letter is of order g/n. The properties of G_1 frequently throw light on the possible properties of G. In particular, when G_1 is transitive and of degree $n-1$, G must be multiply transitive, but when G_1 is of a lower degree than $n-1$, there must be at least one substitution besides identity which is commutative with every substitution of G. If the order of such a substitution is less than n its systems of intransitivity are systems of imprimitivity of G. Hence it results that, when G is primitive and G_1 is not of degree $n-1$, G must be the regular group of prime order p.

While a number of such properties relating to G_1 have been known for a long time little has been done towards determining the possible substitution groups which involve a particular G_1. For instance, when G_1 is the symmetric group of degree m, G must be the symmetric group of degree $m+1$, except in the special case when $m=2$. In this case it may also be the octic group of degree 4, as is well known, but it cannot be any other group. This theorem results directly from the facts that there is no substitution on the letters of the symmetric group of degree $m>2$ which is commutative with every substitution of this symmetric group and that a regular group of degree m can always be used as the G_1 for at least one transitive group of degree $2m$ and of order $2m^2$. In a similar manner it results that every alternating group, except the alternating group of degree 3, can appear as the G_1 of only the alternating group of the next larger degree, while the alternating group of degree 3 is also the G_1 of a group of order 18 and of degree 6.

As a special case of the theorems just stated there results the well known theorem, first proved by Ruffini, that there is no four-valued rational function on five variables. In fact, if such a function were possible there would be a transitive substitution group of order 30 and of degree 5. The G_1 of this group would have to be the symmetric group of degree 3 since there is no other group of order 6 on less than 5 letters. The fact

[*] Presented to the Society, December 27, 1924.

that there is no three-valued function on five letters follows also from well known properties of G_1. If such a function were possible there would be a transitive group of degree 5 and of order 40. The G_1 of this group would be the octic group of degree 4, since this is the only group of order 8 whose degree is less than 5. If G_1 were this octic group, the cycles of order 2 in G would involve more than 40 letters and hence G would involve substitutions of degree 5 containing cycles of order 2. This is impossible since such substitutions would be of order 6, and 6 does not divide 40. A general theorem which covers this case may be stated as follows:

If cycles which appear in as many sets of conjugates under G as under G_1 are contained in substitutions whose degree is less than $n-1$, then cycles of this order appear also in substitutions of degree n contained in G.

From the fact that the number of letters omitted by G_1 must divide the degree of G it results directly that a group of degree m cannot appear as the G_1 of a group unless the degree of this group is one of the following m numbers: $m+1,\ m+2, \cdots,\ 2m$. In particular, the number of the different transitive substitution groups which involve the same substitution group as a subgroup composed of all the substitutions which omit one letter is always finite. In fact, if this substitution group is of degree m the number of these transitive groups is clearly less than the number of the possible transitive groups on $m+1,\ m+2, \cdots, 2m$ letters. As the number of the possible substitution groups on a given number of letters is finite our theorem is obviously true. From the fact that the number of letters omitted by all the substitutions of G which omit one letter is a divisor of the degree of G_1, as well as of the degree of G, it results that the only group of degree m which is a G_1 of at least one group of each of the m degrees $m+1,\ m+2, \cdots, 2m$ is the group of order and of degree 2. From the same fact it results also that a group of prime degree p cannot be the G_1 of any group unless the degree of this group is either $p+1$ or $2p$. In the latter case this group of prime degree must also be regular.

2. The subgroup G_1 has a prime order

At the close of the preceding section it was noted that when G_1 is of a prime degree p it cannot appear in any transitive group unless the degree of G is either $p+1$ or $2p$. In the latter case G is imprimitive and G_1 is regular. There is obviously one, and only one, such group for every prime number p. Its order is $2p^2$ and it can be constructed by extending by means of a substitution of order 2 and of degree $2p$ the direct product of two regular groups of order p. Hence all the transitive substitution groups which involve as a G_1 a group of prime degree p but have themselves a degree which exceeds $p+1$ are completely determined.

When G_1 is regular and of degree p the group G of degree $p+1$ is clearly impossible unless $p+1$ is either 3 or of the form 2^α. In the latter case G contains the abelian group of order 2^α and of type $(1, 1, 1, \cdots)$ as a characteristic subgroup, while all of the remaining substitutions are of order and degree p. Since the order of the group of isomorphisms of this abelian group is not divisible by p^2 it results that all of its subgroups of order p are conjugate, and hence there is only one such group of order $p\cdot 2^\alpha$. This completes a proof of the following theorem:

The regular group of odd prime order p is always the G_1 of one and only one transitive group of degree $2p$. In the special case when p is of the form $2^\alpha - 1$ it is also the G_1 of one and only one group of degree $p+1$. It cannot be the G_1 of any other transitive group.

The regular group of order 2 is obviously the G_1 of the octic group and also of the symmetric group of degree 3.

The developments which precede clearly constitute a special case of those which relate to the groups whose G_1 is of prime order p but involves $k > 1$ cycles. When the corresponding G is of degree $kp+1$ it is well known that it involves a characteristic regular group of order $kp+1$ and that all its remaining substitutions are regular and of degree kp. At least one such group is evidently always possible when $kp+1$ is of the form 2^α. It is also always possible when $p=2$ since any abelian regular group of order $2k+1$ may be extended by a substitution of order 2 and of degree $2k$ which transforms into their inverses all the substitutions of this regular group. As these are the only possible groups of degree $2k+1$ when G_1 is generated by a substitution of order 2 and of degree $2k$ it results that *the number of the transitive groups of degree $2k+1$ which have for their G_1 the group of order 2 and of degree $2k$ is exactly the same as the number of the abstract abelian groups of order $2k+1$, k being an arbitrary positive integer.*

When G_1 is of order 2 and of degree 2^α the degree of G is of the form $2^\alpha + 2^\beta$ where $\beta \leqq \alpha$, according to a theorem noted above. It is not difficult to prove that β can have every integral value from 0 to α. As β can have no other value according to the general theorem to which we have just referred it results that when G_1 is of order 2 and of degree 2^α the possible degrees of G are completely known. To prove that β can have every value from 0 to α it is only necessary to note that when β has any one of these values it is possible to construct a regular abelian group of order $2^\alpha + 2^\beta$ which involves a subgroup of order 2^β and of type $(1, 1, 1, \cdots)$ while the order of the remaining substitutions exceeds 2. Hence there is a substitution of order 2 and of degree 2^α which transforms every substitution of this regular group into its inverse.

In fact, the number of the substitutions which have this property is obviously $2^{\alpha-\beta}+1$. In the special case when $\beta=0$ we thus obtain one of the generalized dihedral groups noted at the close of the next to the preceding paragraph. While all the possible groups are known in this case this is not true in general. In fact, when $\beta>0$ it is sometimes possible to extend a non-abelian regular group so as to obtain one of the groups in question, as may be seen from the fact that when $\alpha=3$ and $\beta=2$ the regular tetrahedral group may be extended by means of a substitution of order 2 and of degree 2^α so as to obtain a group whose G_1 is of order 2 and of degree 2^α.

The preceding developments exhibit the interesting fact that G_1 can be so chosen that the number of the different possible degrees of the corresponding transitive groups exceeds any given number, since when G_1 is of order 2 and of degree 2^α the number of such possible degrees is exactly $\alpha+1$, where α is an arbitrary positive integer. Hence the theorem noted in the Introduction of the present article, which states that a given G_1 can appear in only a finite number of transitive groups as the subgroup composed of all the substitutions which omit a given letter, does not imply that there is a number which cannot be exceeded by the number of the different transitive groups which involve the same group for their G_1. In fact, such a number does not exist, according to the theorem just proved.

We noted above that when β has one extreme value, viz., 0, the possible groups are well known. When β has the other extreme value, viz., α, it is easy to prove that G involves a subgroup of half its order which can be constructed by establishing a (2,2) isomorphism between two regular groups of order $2^{\alpha-1}$. To prove this theorem it may first be noted that, when β has this maximal value G_1 has two conjugates under G, and hence it must be transformed into itself by exactly one-half of the substitutions of G. These substitutions constitute a subgroup of one-half of the order of G and they include the two conjugates of G_1 since these conjugates involve no common letter and are therefore commutative. Since all of the remaining substitutions of G are of degree $2^{\alpha+1}$ this subgroup must be intransitive and involve two systems of intransitivity.

The fact that the two transitive constituents of this intransitive subgroup are regular follows from the degree and order of G_1. It results, in particular, that G involves at least one set of systems of imprimitivity whose constituents are of degree 2^α, as well as one whose constituents are of degree 2. Moreover, it is evident that if we can establish a (2,2) isomorphism between any two conjugate regular groups such that the group thus formed can be extended by a substitution which interchanges its systems of intransitivity, transforms it into itself, and has its square in it, we obtain a group whose G_1 is of order 2 and has two conjugates under the group. It should also be noted that the G_1 of every non-regular group of degree n has the property that it and any one of its conjugates which differs from it generates a group of degree n, for if this were not the case the group which they generate would be contained in G_1. Hence the theorem:

Every two different subgroups which are separately composed of all the substitutions which omit one letter of a transitive group of degree n must generate a group of degree n.

3. The subgroup G_1 is transitive

When G_1 is a transitive group of degree m whose subgroup composed of all the substitutions which omit one letter is of degree $m-r$, then the degree of G cannot exceed $m+r$. In fact, this degree is $m+k$, where k is a divisor of r, as may be seen directly from the fact that the k substitutions which are commutative with every substitution of G must be commutative with every substitution of G_1, but the substitutions which have the latter property and involve only the letters of G_1 constitute a group of order r whose transitive constituents are known to be regular groups. In particular, it results from these considerations that a necessary and sufficient condition that a transitive group of degree m can appear as the G_1 of a transitive group of degree $2m$ is that the former group be regular.

From the preceding paragraph it results directly that, when G_1 is a non-regular primitive group of degree m, G must be a primitive group of degree $m+1$. It is not always possible to construct such a primitive group of degree $m+1$ when G_1 is given. It was noted in the Introduction that, when G_1 is non-abelian and either alternating or symmetric, there is one and only one transitive group of degree $m+1$ whose subgroup composed of all its substitutions which omit one letter constitutes this G_1. Hence it is easy to verify that 6 is the smallest value of m such that a primitive group of degree m cannot be used as the G_1 of any transitive group whatever. In fact, neither of the two well known primitive groups of degree 6 and of orders 60 and 120 respectively can appear as the G_1 of a group of degree 7, since the cycles of order 7 would all have to be conjugate if the group were of order 840 and hence the number of the subgroups of order 7 would be 20, which is incongruent to unity modulo 7, and if the group were of order 420 there would be at most three sets of conjugate cycles of order 7, but the number of subgroups of order 7 could not be 10, 20, or 30.

It was noted in the preceding section that when G_1 is of order 2 and of degree 2^{α} it appears in transitive groups of exactly $\alpha+1$ different degrees. When G_1 is transitive and of degree 2^{α} it obviously appears also in transitive groups of $\alpha+1$ different degrees when α is 1 or 2, but when α is 3 this is not the case. In fact, a transitive group of degree 2^α can appear in transitive groups of $\alpha+1$ different degrees only when the group of degree 2^α is regular, since all such degrees must be of the form $2^\alpha+2^\beta$ where $\beta<\alpha+1$, and there is no transitive group of degree 10 whose G_1 is a regular group of degree 8. This fact results directly from Sylow's theorem, since a group of order 80 contains either 1 or 16 subgroups of order 5. If it contains only one such subgroup it must involve an abelian group of order 20, but an abelian group of this order cannot be represented on ten letters. If it contains 16 such subgroups it contains also an invariant subgroup of order 16 and this must involve five systems of intransitivity when it is represented on ten letters. Hence it could not involve a regular subgroup of order 8.

While it results from the preceding paragraph that for at least one value of α it is impossible to construct transitive groups of as many as $\alpha+1$ different degrees whose G_1 is a transitive group of degree 2^α it is easy to prove that it is always possible to construct a transitive group of degree $2^\alpha+2^{\alpha-1}$ whose G_1 is a transitive group of degree 2^α. In fact, to construct such a group in which G_1 is the regular abelian group of order 2^α and of type $(1, 1, 1, \cdots)$ we may first construct two abelian groups of order $2^{\alpha-1}$ and of degree 2^α whose two transitive constituents are regular groups of type $(1, 1, 1, \cdots)$ such that these two abelian groups have one transitive constituent in common. The direct product of these two groups is of degree $2^\alpha+2^{\alpha-1}$ and its three transitive constituents can be transformed according to the symmetric group of degree 3 so as to obtain two transitive groups of order $3\cdot 2^\alpha$ whose three Sylow subgroups of order 2^α are abelian and regular. Hence it results that *for every value of $\alpha>1$ it is possible to construct two transitive groups of degree $2^\alpha+2^{\alpha-1}$ which have for their G_1 an abelian regular group of order 2^α*. It may be noted that the two transitive groups of degree 6 which are simply isomorphic with the symmetric group of degree 4 are illustrations of this general theorem.

It results from the preceding paragraph that there are always transitive groups of at least two different degrees which involve for their common G_1 a certain regular group of order 2^α but it is not known whether it is possible to construct a transitive group which appears as the common G_1 of transitive groups of a number of different degrees exceeding an arbitrarily large number. Hence we do not have here a theorem which corresponds to the theorem established in the preceding section as regards transitive groups which have for their common G_1 an intransitive group of order 2. A necessary and sufficient condition that some regular group of degree m is the G_1 of a transitive group of degree $m+1$ is that $m+1$ is a power of a prime number. If there is only one such regular group it is well known to be cyclic.

When G_1 is a transitive group of degree m and G is of degree $m+k$,

$k > 1$, then G must transform $m/k + 1$ systems of imprimitivity according to a multiply transitive group. In particular, when G_1 is a regular group which transforms each of its systems of imprimitivity, involving k letters in a set, according to a regular group, then $m/k + 1$ is either a prime number or a power of some prime number. This is obviously always the case when G_1 is abelian. From the fact that the systems of imprimitivity of such a group are transformed according to a multiply transitive group whose class is one less than its degree it results that *a regular abelian group of order m cannot appear as the G_1 of a transitive group of degree $m + k$ except when $m/k + 1$ is either a prime number or a power of such a number.*

It was noted above that the cyclic regular group of degree 4 is the G_1 of a transitive group of degree 6. It is not difficult to prove that the cyclic regular group of order m cannot be the G_1 of a transitive group of degree $m + 2$ whenever $m > 4$. Such a group G would contain $m/2 + 1$ conjugates of G_1 and hence each of these conjugates would be transformed into itself by exactly $2m$ substitutions of G. Each of these conjugates would be transformed into itself by exactly two substitutions found in each of the others. Hence all the substitutions of order 2 found in these conjugates would be commutative and would generate an abelian group which would transform each of these conjugates into itself. As this abelian group could not have more than two substitutions in common with one of these conjugates its order could not exceed 4. Hence $m/2 + 1$ could not exceed 3. That is, m could not exceed 4, which is in accord with the statement made above. This proof evidently applies also to all other regular groups which contain only one subgroup of order 2.

By a method which is somewhat similar to the one employed in the preceding paragraph it is easy to prove that many other regular groups of order m cannot appear as the G_1 of some transitive group of degree $m + 2$. In particular, when m is of the form 2^α it is well known that every possible non-cyclic group of order 2^α with the exception of 3 groups contains an invariant non-cyclic subgroup of order 4 whenever $\alpha > 3$.* We proceed to prove that when a group of order 2^α which involves a non-cyclic invariant subgroup of order 4 is represented as a regular group then its group of isomorphisms cannot involve a substitution of order 2 and of degree $2^\alpha - 2$. If such a substitution s could exist it would have to transform two of the substitutions of order 2 contained in the given invariant subgroup of order 4 into themselves multiplied by the third of its substitutions of order 2. The substitution s would also have to transform a substitution not found in the given non-cyclic subgroup of order 4 into

* G. A. Miller, these Transactions, vol. 6 (1905).

itself multiplied by one of the two substitutions of this subgroup with which it is not commutative. From this fact it follows directly that s^2 could not be identity, and hence s could not be of order 2 as was assumed.

From the preceding two paragraphs, it results that if a regular group of order 2^{α} appears as the G_1 of a transitive group of degree $2^{\alpha}+2$, $\alpha > 2$, it cannot be either cyclic or dicyclic, and it cannot contain a non-cyclic invariant subgroup of order 4. Hence it must be one of two groups, viz., the dihedral group or the group of order 2^{α} which involves operators of order $2^{\alpha-1}$ and $2^{\alpha-2}+1$ operators of order 2. The latter must be excluded since its group of isomorphisms cannot involve a substitution of order 2 and degree $2^{\alpha}-2$ when this group is represented as a regular substitution group. It remains therefore only to consider whether the regular dihedral group of order 2^{α}, $\alpha > 3$, can be the G_1 of a transitive group of degree $2^{\alpha}+2$. We proceed to prove that this is impossible.

Suppose that there existed a transitive group G of degree $2^{\alpha}+2$ whose G_1 is the regular dihedral group of order 2^{α}, $\alpha > 3$. The subgroup G_1 must be transformed into itself by $2^{\alpha+1}$ substitutions of G. These substitutions constitute an intransitive group whose two transitive constituents are of degree 2 and 2^{α} respectively. The transitive constituent of degree 2^{α} must involve a substitution s of order 2 and of degree $2^{\alpha}-2$ which is commutative with 2 and only 2 of the substitutions of G_1. It is well known that the group of isomorphisms of G_1 is simply isomorphic with the holomorph of the cyclic group of order $2^{\alpha-1}$.* Hence this group of isomorphisms involves $2^{\alpha-1}+2^{\alpha-2}+2+1$ operators of order 2. The given substitution s must therefore transform the substitutions of order $2^{\alpha-1}$ contained in G_1 into their inverses while it transforms the non-invariant substitutions of order 2 in G_1 into themselves multiplied by operators of order $2^{\alpha-1}$. It results from this property of s that the group generated by G_1 and s is the dihedral group of order $2^{\alpha}+1$. Hence G must involve this dihedral group, represented as an intransitive group having transitive constituents of degrees 2 and 2^{α} respectively.

From the preceding paragraph it results that the substitution of order 2 which is commutative with every substitution of G must have for its constituent of degree 2^{α} the substitution of order 2 generated by a substitution of order 2^{α} found in the given dihedral group of order $2^{\alpha+1}$. There would be $2^{\alpha-1}+1$ conjugates of this dihedral group in G. Two of these conjugates would have in common $2^{\alpha}-2$ letters and hence the substitutions of order 2 which are commutative with all the substitutions found in these two conjugates and involve only their letters would have more than one

* Miller, Blichfeldt, Dickson, *Theory and Applications of Finite Groups*, 1916, p. 169.

cycle in common since they could involve only cycles which are found in the substitution of order 2 which is commutative with every substitution of G. As this is impossible we have established the following general theorem:

A regular group of order 2^α, $\alpha > 2$, cannot appear as the subgroup composed of all the substitutions which omit one letter of a transitive group of degree $2^\alpha + 2$.

The theorem noted above that a regular cyclic group of order m cannot be the G_1 of a transitive group of degree $m+2$ whenever $m > 4$ is obviously a special case of the following theorem:

If a regular abelian group of order m is the G_1 of a transitive group of degree $m+k$, then $m \leqq 2k$.

To prove this theorem it may first be noted that every two different conjugates of G_1 must involve all the letters of this transitive group G of degree $m+k$. The k substitutions which are commutative with every substitution of G must therefore have constituents of degree m in common with substitutions of these two conjugates of G_1 respectively. Hence these conjugates cannot have more than k letters in common. If they have k letters in common it results that $2m - k = m + k$, and hence $m = 2k$. If they have less than k letters in common m is evidently less than $2k$. Hence the theorem under consideration has been established. The fact that this theorem does not hold for regular non-abelian groups results directly from the group of isomorphisms of the non-cyclic group of order 9, since this is a transitive group of degree 8 whose G_1 is the non-cyclic regular group of order 6.

At the close of the preceding section it was noted that every two distinct conjugates of a subgroup composed of all the substitutions of a transitive group which omit a given letter generate a group whose degree is equal to the degree of the entire group. A special case of this theorem is that each such subgroup must involve at least half of the letters of the entire transitive group. When two such subgroups generate a transitive group it must evidently be the entire group since the subgroup composed of all the substitutions which omit one letter of this transitive group is the same as the subgroup of the entire transitive group and the degrees of these transitive groups are the same. In particular, it results that whenever the subgroup composed of all the substitutions which omit one letter of a transitive group is transitive then this subgroup and any of its conjugates which differ from it generate the entire group whenever the degree of this subgroup exceeds one-half the degree of the group. In particular, a necessary and sufficient condition that two distinct conjugates of a subgroup composed of all the substitutions which omit one letter of a transitive group generate the entire group is that they generate a transitive group.

University of Illinois,
Urbana, Ill.