SUBSTITUTIONS WHICH TRANSFORM A REGULAR GROUP INTO ITS CONJOINT*

BY G. A. MILLER

In a recent article which appeared in this Bulletin† under a similar heading it was proved that a necessary and sufficient condition that there exists a substitution t of order 2 which is commutative with every substitution of the group of isomorphisms of a regular group R, transforms R into its conjoint, and involves only letters of R, is that R involves substitutions whose order exceeds 2. In what follows it will be assumed that R satisfies this condition, and hence R may represent any abstract group except the abelian group of order 2^m and of type $(1, 1, 1, \cdots)$. While in the previous article the main emphasis was laid on a method of determining t as a substitution on the letters of R, and comparatively little attention was then paid to the fact that t is commutative with every substitution of the group of isomorphisms of R, it is this fact which will receive the main attention in the present article, since it throws much light on the infinite system of substitution groups which are separately groups of isomorphisms of regular substitution groups.

To simplify the considerations which follow we note here the well known facts that the totality of the substitutions on the letters of R which transform R into itself, in the sense that they transform every substitution of R into such a substitution, constitutes a group H, known as the holomorphs of R, and that the subgroup H_1, composed of all the substitutions of H which omit a given letter, is simply isomorphic with the group of isomorphisms of R. There are always at least two such sub-groups in H, and t is not necessarily commutative with every substitution in each of

* Presented to the Society, September 9, 1927.

† Vol. 32 (1926), p. 631.

these subgroups. It must, however, be commutative with every substitution of such a subgroup whenever t transforms into their inverses all the cycles which involve a letter which is neither in t nor in the subgroup in question. In what follows such a subgroup will be implied when we speak of the group of isomorphisms of R in connection with t.

When R is abelian then t is one of the substitutions of H which transform every substitution of R into its inverse and omit at least one letter of R. In this case the degree of t cannot be less than $r/2$, where r is the order of R. On the other hand, the degree of t is $r/4$ whenever R is the direct product of the octic group and an abelian group of order 2^m and of type $(1, 1, 1, \cdots)$. Since this infinite category of groups is characterized by the fact that it is composed of all the groups which involve operators whose order exceeds 2 but the number of such operators is relatively less than in any other group,* it is clear that t is never of a smaller degree than $r/4$, and that it is of this degree only when R belongs to the category just noted. From the obvious fact that when R is the quaternion group it can be transformed into its conjoint by a transposition, while t is of degree 6 in this case, it results directly that it may sometimes be possible to transform R into its conjoint by means of a substitution which is of a lower degree than t. In what follows we shall use t_1 to represent a substitution of lowest degree which transforms R into its conjoint, except that t_1 cannot be the identity when R is abelian and therefore coincides with its conjoint.

It is easy to see that the degree of t_1 can never be less than $r/4$ since the product of t_1 and any of its conjugates under H must be found in H, in view of the fact that every substitution which transforms R into its conjoint must also transform this conjoint into R. Moreover, the degree of this product cannot be less than $r/2$, whenever this product is not the identity, since the number of letters omitted by any substitution of H_1 is equal to the number of substitutions

* G. A. Miller, Comptes Rendus, vol. 141 (1905), p. 591.

of R with which this substitution is commutative and hence H cannot involve any substitution besides the identity which involves less than $r/2$ letters. From this it results also that when t_1 is of degree $r/4$ then R must be non-abelian, and that a conjugate of t_1 cannot involve the same letters as t_1 involves unless it is identical with t_1. Hence, whenever t_1 is of degree $r/4$, it is of order 2 and has exactly four distinct conjugates under H. The continued product of these conjugates is invariant under H and hence is a characteristic substitution of R. In what follows we shall assume that t_1 is of degree $r/4$.

If H_1 omits a letter of t_1 all of its substitutions must be commutative with t_1 and hence t_1 is also commutative with every substitution of the group of isomorphisms of R. It therefore results that when R can be transformed into its conjoint by a substitution of degree $r/4$ and t is not of this degree then there are at least three different substitutions of order 2 which are commutative with every substitution in its group of isomorphisms. Since t_1 is commutative with one-fourth of the substitutions of R and transforms R into its conjoint it results that the central of R must be composed of one-fourth of its substitutions. Since the central quotient group is always non-cyclic it results that R involves three abelian subgroups of index 2. Hence the following theorem.

THEOREM I. *A regular group cannot be transformed into its conjoint by a substitution which is not the identity but involves less than one-fourth of the letters of this regular group, and when it is transformed into its conjoint by a substitution which involves exactly one-fourth of its letters its order must be divisible by* 8 *and it must be non-abelian but involve three abelian subgroups of index* 2.

We proceed to prove that the conditions expressed in this theorem are not only necessary but also sufficient in order that the regular group R can be transformed into its conjoint by t_1. When these conditions are satisfied R has a commutator subgroup of order 2. Let R_0 be one of its abelian subgroups

of index 2. This subgroup has two transitive constituents and involves the central of R, which has four such constituents. Let t_1 be the part of the commutator of R which appears in the last of these four constituents and let s be the substitution of order 2 which simply interchanges the corresponding letters of R_0, so that s is commutative with every substitution of R_0 and transforms t_1 into t_0. To obtain R it is obviously only necessary to extend R_0 by means of the substitution $s_0 t_0 t_1 s$, where s_0 is a substitution found both in the first transitive constituent of R_0 and also in the central of R.* The transform of R under t_1 is the conjoint of R since each of its substitutions is commutative with every substitution of R. In fact t_1 is commutative with one-half of the substitutions of R_0 and transforms each of the other substitutions of R_0 into itself multiplied by the substitution of order 2 in the second transitive constituent of R_0 which includes t_1. These transforms are obviously commutative with $s_0 t_0 t_1 s$. As the transform of $s_0 t_0 t_1 s$ under t_1 is also commutative with every substitution of R we have proved the following theorem.

THEOREM II. *A necessary and sufficient condition that a regular group can be transformed into its conjoint by a substitution which involves exactly one-fourth of its letters is that this group be non-abelian but involve more than one abelian subgroup of index* 2.

From this theorem it results that there are at least three substitutions of order 2 on the letters of the H of each of these groups which are commutative with every substitution of H_1, except possibly in the case when R is the direct product of the octic group and an abelian group of order 2^m and of type $(1, 1, 1, \cdots)$. In this special case it is obvious that there are always exactly three such substitutions in H. Hence it results that when the regular group R is non-abelian but involves more than one abelian subgroup of index 2 there

* G. A. Miller, American Journal of Mathematics, vol. 24 (1902), p. 395.

are always at least two distinct substitutions of order 2 which transform it into its conjoint and are commutative with every substitution of its group of isomorphisms. It also results directly from the same theorem that the only non-abelian groups which can be transformed into their conjoints by a transposition are the octic group and the quaternion group. It may be added that when R is any dihedral group of order $2n$, $n>2$, then t is a substitution of order 2 which transforms into its inverse a cycle of order n and involves $n-1$ or $n-2$ letters as n is odd or even. When R is the dicyclic group then t is the product of this substitution and the substitution of order 2 generated by the second cycle of order n.

If all the operators of order $k>2$ which appear in a group G are transformed according to a transitive substitution group under the group of isomorphisms of G then there are at least $\phi(k)$ substitutions on the letters of this transitive group which are commutative with each of its substitutions, $\phi(k)$ being the totient of k. This results from the fact that the subgroup composed of all the substitutions of this transitive group which omit one letter must omit at least the $\phi(k)$ letters corresponding to the operators of order k generated by a group operator of this order. In particular, there results the following theorem.

THEOREM III. *A necessary and sufficient condition that a constituent of t which involves the same letters as a transitive constituent of H involves appears in this transitive constituent is that each of the operators of G which corresponds to the letters of this constituent corresponds also to its inverse in some automorphism of G.*

This theorem explains the fact that the constituents of t appear in H when R is dihedral or dicyclic.

According to the general theorem under consideration there is always at least one substitution of order 2 on the letters of H which is commutative with every substitution

of H_1, and when there is only one such substitution it must be t. It may be of some interest to inquire what condition R must satisfy in order that there be only one such substitution. When R is abelian and $r>4$ the necessary and sufficient condition is obviously that the order of R be a power of any odd prime number and that its type be $(1, 1, 1, \cdots)$. If such an abelian group is extended by an operator of order 2 which transforms each of its operators into its inverse, there results a generalized dihedral group whose group of isomorphisms is the holomorph of this abelian group and hence t is again the only substitution of order 2 on the letters of its H which is commutative with every substitution of H_1. Another infinite system of groups in which t is the only substitution on the letters of R which is commutative with every substitution of H_1 may be constructed by extending the abelian group of order 2^m and of type $(1, 1, 1, \cdots)$ by means of an operator of prime order which is generated by any operator of order 2^m-1 in the group of isomorphisms of this abelian group. The tetrahedral group is the group of lowest order in this system. From what was noted above it results directly that whenever the order of a regular group is divisible by at least two distinct odd prime numbers there must be more than one substitution on the letters of R which is commutative with every substitution of its H_1.

THE UNIVERSITY OF ILLINOIS