GROUPS FORMED BY SPECIAL MATRICES.

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society September 4, 1917.)

1. *Introduction.*

IT is well known that every possible substitution on n letters can be represented by a square matrix of order n which has one and only one unity element in each row and in each column while each of its other elements is 0. For brevity we shall call such a matrix in what follows an n-matrix. The determinant of an n-matrix is ± 1, according as the substitution represented by it is positive or negative. In particular, the totality of all the different n-matrices forms a group with respect to multiplication, and this group is simply isomorphic with the symmetric group of degree n. The totality of these matrices whose determinants are equal to unity also forms a group with respect to the same law of composition, which is evidently simply isomorphic with the alternating group of degree n.

Hence the theory of substitution groups is identical with the theory of the multiplication of such special matrices. The main object of the present paper is to exhibit the equivalence of the theory of imprimitive substitution groups and the theory of multiplication of another type of special matrices. We shall first consider the special case where the imprimitive group is of degree $2n$ and has n systems of imprimitivity. Hence each of these systems involves two letters.

The largest possible imprimitive group of this type is clearly of order $2^n \cdot n!$, and is simply isomorphic with the group formed by all the possible different square matrices of order n which have one and only one ± 1 element in each row and in each column, while each of their other elements is 0. Since every possible imprimitive group of degree $2n$ which has n systems of imprimitivity is conjugate with a subgroup of the former of these groups it results that *every possible imprimitive group of degree* $2n$ *which has* n *systems of imprimitivity is simply isomorphic with a group formed by square matrices of order* n *having one and only one* ± 1 *element in each row and in each column, while all their other elements are* 0.

In fact, the preceding theorem can be stated in a somewhat more general form if it is noted that the letters of such an imprimitive group can be placed in a (1, 1) correspondence with the elements of these matrices if we let the columns correspond to the systems of imprimitivity and the two letters of each system to ± 1. Such a representation may also serve to exhibit in a new light the meaning of the term systems of imprimitivity, and, if it is employed, the words " simply isomorphic " in the preceding theorem may be replaced by the somewhat stronger word " con ugate."

To obtain an elementary matrix notation for every possible imprimitive group it may be noted that every imprimitive group of degree kn which has n systems of imprimitivity is conjugate with a subgroup of the imprimitive group obtained by forming the direct product of n symmetric groups of degree k, and adjoining to this direct product substitutions which permute its systems of intransitivity according to the symmetric group of degree n. Hence it results directly that *every possible imprimitive group of degree kn which has n sys ems of imprimitivity is conjugate with a group formed by square matrices of order n having one and only one k-matrix element in each row and in each column while all its other elements are* 0. Instead of representing these non-zero elements by k-matrices they may clearly be represented by elements of a group.

2. *Special Imprimitive Groups and Their Invariant Elements.*

The totality of the square matrices of order n which have one and only one kth root of unity element in each row and in each column, while all their other elements are 0, constitute a group G_1 of order $k^n \cdot n!$, which is simply isomorphic with the imprimitive substitution group of degree kn constructed as follows: Form the direct product of n regular cyclic groups of order k, and adjoin to this direct product substitutions which separately permute its systems of intransitivity according to the symmetric group of degree n.

The totality of the *principal diagonal matrices* of G_1, i. e., those matrices whose elements outside of the principal diagonals are entirely composed of zeros, constitutes a subgroup of G_1 which is simply isomorphic with the direct product formed by n cyclic groups of order k. The central of G_1 is of order k, and is composed of the principal diagonal matrices

having equal elements, i. e., of the scalar matrices contained in G_1.

A necessary and sufficient condition that an imprimitive group of degree kn which has n systems of imprimitivity can be represented by such square matrices of order n is that the group composed of all the substitutions on the letters of one system of imprimitivity which transform this system into itself is cyclic. In particular, *a necessary and sufficient condition that a regular substitution group can be represented by square matrices of order n having one and only one kth root of unity element in each row and in each column, while each of the other elements is* 0, *is that it contains a cyclic subgroup of index n.* For instance, with respect to the subgroup of order 3, and one of the subgroups of order 2 the symmetric group of order 6 is represented as a regular group by each of the following two sets of six matrices, ω representing an imaginary cube root of unity:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}, \begin{bmatrix} \omega^2 & 0 \\ 0 & \omega \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \omega \\ \omega^2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \omega^2 \\ \omega & 0 \end{bmatrix};$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{bmatrix}.$$

Another interesting category of groups is represented by the $[\phi(m)]^n \cdot n!$ matrices, having one and only one element in each row and in each column which is any one of the $\varphi(m)$ positive integers not greater than m and prime to m, while each of the other elements is 0. When $m > 1$ these matrices represent the imprimitive substitution group constructed as follows: Form the direct product of the n regular groups which are separately simply isomorphic with the group formed by the $\varphi(m)$ positive integers less than m and prime to m. To this direct product adjoin substitutions which permute its systems of intransitivity according to the symmetric group of degree n.

The group noted in the preceding paragraph has $\phi(m)$ invariant elements, since the simply isomorphic imprimitive

group has this property. These invariant elements are represented by the principal diagonal matrices whose elements are all equal to the same positive integer. This result follows also from the method of transforming n-matrices by each other, which we proceed to explain.

If $r_1, r_2, \cdots, r_n$ and $c_1, c_2, \cdots, c_n$ represent the rows and the columns respectively, taken in order, of an n-matrix, then the substitution represented by this matrix may be denoted as follows:

$$\begin{pmatrix} r_1 & r_2 & \cdots & r_n \\ c_{a_1} & c_{a_2} & \cdots & c_{a_n} \end{pmatrix}$$

where $c_{a_1}, c_{a_2}, \cdots, c_{a_n}$ represent the columns containing the unit element in the rows represented by $r_1, r_2, \cdots, r_n$ respectively. Hence any n-matrix can be transformed by any other n-matrix by interchanging the rows and the columns of the former according to the substitution represented by the latter. If any matrix having one and only one non-zero element in each row and in each column is transformed by any other such matrix, the transformed matrix is again of this form and its non-zero elements occur in the same rows and columns irrespective of the value of these non-zero elements. Hence the theorem noted in the preceding paragraph results directly from the fact that identity is the only invariant element of the symmetric group.

While the invariant elements of the imprimitive groups considered above generate invariant subgroups, it should not be assumed that these subgroups give rise to invariant imprimitive subgroups. On the contrary, every invariant imprimitive subgroup of G_1 contains *all* its principal diagonal matrices whose determinants are equal to unity. Hence the principal diagonal matrices of any imprimitive invariant subgroup of G_1 must always include all these matrices whose determinants satisfy the equation $x^d = 1$, where d is a divisor of k. This is equivalent to the following theorem:

If an imprimitive group of degree kn has for its head H, the direct product of n regular cyclic groups of degree k, then every invariant imprimitive subgroup has for its head a subgroup of H which is simply isomorphic with the direct product of n − 1 cyclic groups of order k and of some subgroup of such a cyclic group.

By means of this theorem it is not difficult to determine all the invariant subgroups of the groups considered above.

UNIVERSITY OF ILLINOIS.