for each a in the set 1, 2, . . . , $(l-3)/2$, such that δ is a unit in $k(\zeta)$ with $\delta(\zeta^r)^{r^{2a}} = \delta(\zeta)\gamma^l$, and $B_a \equiv 0 \pmod{l}$.

[1] Vandiver, these PROCEEDINGS, **15**, 203 (1929).
[2] *Jour. für die Reine und Angewandte Mathematik*, **157**, 230–238 (1927).
[3] *Ann. Math.* (2), **21**, 78 (1919).
[4] *Trans. Amer. Math. Soc.*, **29**, 156 (1927).

GROUPS OF DEGREE n INVOLVING ONLY SUBSTITUTIONS OF LOWER DEGREES

BY G. A. MILLER

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS

Communicated July 7, 1938

Every transitive group of degree n involves at least $n-1$ substitutions of this degree but an intransitive group of degree n does not necessarily involve any substitution whose degree is as large as n. Such intransitive groups exist only when $n > 4$ and there is obviously only one such group of degree 5, viz., the group formed by a 3, 1 isomorphism between the symmetric group of degree 3 and the group of degree 2. Whenever n is odd and exceeds 3 it is clearly possible to construct similarly a group of degree n which does not involve any substitution whose degree is as large as n by dimidiating the dihedral group of degree $n-2$ and the group of degree 2. Exactly half of the substitutions of this group are of degree $n-1$ while the remaining substitutions thereof appear in the cyclic subgroup of degree $n-2$ and are either of degree zero or of degree $n-2$.

From the preceding paragraph it results that when n is odd and exceeds 3 it is always possible to construct at least one group of degree n which does not involve any substitution of this degree and has one transitive constituent of degree $n-2$. We proceed to prove that such a group cannot be constructed when n is an even number. If this were possible the transitive constituent of degree $n-2$ of such a group would involve a subgroup of index 2 containing all its substitutions of degree $n-2$ since none of its other substitutions would be of as large a degree as $n-2$. Hence all of these other substitutions would be of degree $n-3$ since this is the average number of letters in the substitutions of this constituent. As $n-3$ is supposed to be odd each of these substitutions of degree $n-3$ involves an odd cycle and an odd power of such a substitution would involve less than $n-3$ letters but would appear among the given substitutions of degree $n-3$. As this is impossible it results that *a necessary and sufficient condition*

that there exists a group of degree n > 3 *which involves no substitution of degree* n *but has a transitive constituent of degree* n $- 2$ *is that* n *is odd.*

Suppose that n is the sum of two distinct prime numbers p, q, $p > q$, and that a group has two transitive constituents of degree p and q, respectively. If $p - 1$ is divisible by q it is clearly possible to construct a group of degree n which involves no substitution of degree n by establishing a p, 1 isomorphism between a subgroup of the metacyclic group of order $p(p - 1)$ and the group of degree q. On the other hand, when $p - 1$ is not divisible by q it is impossible to construct a group of degree n which does not involve a substitution of degree n since every invariant subgroup of a transitive group of degree p involves all of its substitutions of order p and its quotient group under the entire group is cyclic and has an order which divides $p-1$.[1] For the same reason when $n = 2p$, where p is an odd prime number, it is impossible to construct a group of degree n which does not contain a substitution of degree n. Hence there results the following theorem: *When* n *is the sum of two prime numbers it is impossible to construct a group of degree* n *which has these numbers for the degrees of its transitive constituents and involves no substitution of degree* n *unless the larger of them is congruent to unity with respect to the smaller.*

If at least one of the constituent groups of a group involves no substitution whose degree is equal to the degree of this constituent then the entire group cannot involve a substitution whose degree is equal to the degree of the group. In particular, if at least one of the factor groups of a direct product involves no substitution whose degree is equal to the degree of this factor group then the entire group will obviously have the same property. Since the degree of such a factor group need not exceed 5 it results that whenever $n > 6$ there is at least one direct product of degree n which has the property that it contains no substitution whose degree is equal to the degree of this direct product. It is easy to verify that no such group exists whenever $n < 7$ and that the only group of degree 6 which contains no substitution of this degree is composed of the positive substitutions of the group of order 8 and degree 6 which has three transitive constituents.

In what precedes, two substitution groups of a given degree are said to be identical whenever they are conjugate under the symmetric group of this degree. It is often desirable to consider two such groups as distinct whenever one of them contains at least one substitution which does not appear in the other. If this is done there are 10 groups of degree 5 which have the property that none of them contains a substitution of this degree since such a group is transformed into itself by 12 substitutions on these 5 letters. Similarly there are 15 groups of degree 6 which separately do not involve a substitution of this degree since each of them is transformed into itself by 48 substitutions on these 6 letters. In what follows we shall employ the latter of these two methods of enumerating substitution groups unless the

contrary is stated. There are therefore 210 groups on 7 letters, each being of degree 5, which separately have the property that none of them involves a substitution which is equal to the degree of the group, and there are 105 groups on 7 letters, each being of degree 6, which separately have the same property.

It was noted above that whenever $n > 6$ there is always at least one direct product of degree n which does not contain a substitution of this degree. We proceed to prove that there is then also at least one group of this degree involving no substitution of this degree but in which every constituent group contains at least one substitution whose degree is equal to the degree of this constituent. When n is odd such a group can obviously be constructed by establishing a dimidiation between the dihedral group of degree $n - 2$ and the group of degree 2 on the remaining letters. When n is even the dihedral group of degree $n - 4$ involves $(n - 4)/2$ substitutions of degree $n - 6$ and the same number of substitutions of degree $n - 4$ besides the cyclic subgroup of this order. Hence we can establish an isomorphism between this dihedral group and the intransitive group of order 4 on the remaining letters so that no substitution has a degree which exceeds $n - 2$ and all the substitutions are of this degree except those in the cyclic subgroup of order $(n - 4)/2$. As every constituent group of this group involves at least one substitution whose degree is equal to the degree of this constituent there results the following theorem: *There is at least one group of every degree* n > 6 *which has the property that it does not involve any substitution of degree* n *and that each of its constituent groups involves at least one substitution whose degree is equal to the degree of this constituent.*

To obtain an expression for the number of the groups in each of the two categories noted in the preceding paragraph it may be observed that when n is odd the given cyclic group of degree $n - 2$ can be chosen in $n(n - 1)\ldots 3/(n - 2)$ ways and one such group corresponds to each of these cyclic subgroups. When n is even the given cyclic group of degree $n - 4$ can be selected in $n(n - 1)\ldots\ldots 5/(n - 4)$ ways but for each of these cyclic subgroups there are three of the required groups. Hence the number of the possible groups which satisfy the given condition in this case is $3n(n - 1)\ldots 5/(n - 4)$. When n is odd the given number of these groups exceeds $(n - 1)!/2$. This is of interest in connection with the question of the relative number of substitutions and subgroups in the symmetric group of degree n.

If a group of degree n is constructed by establishing a simple isomorphism between symmetric groups of degree m it necessarily involves substitutions of degree n. To prove this theorem it may first be noted that when $m \neq 6$ then transpositions of these various symmetric groups correspond to each other in this simple isomorphism in view of the fact that when $m > 6$ a transposition is transformed into itself by more substitu-

tions of the symmetric group than any other substitution of order 2 contained therein. Hence these transpositions correspond to each other in such a simple isomorphism except possibly when $m = 6$. In this particular case the positive substitutions of order 4 of such a symmetric group correspond to each other and hence the resulting group contains substitutions of degree n and does not require further consideration here. In all other cases a transposition and a cyclic substitution of degree $m - 1$ which involves one and only one letter of this transposition generate the symmetric group of degree m. The latter therefore corresponds also to such a substitution. As the product of these two substitutions is cyclic and of degree m it results that every group of degree n which is formed by a simple isomorphism between symmetric groups involves at least one substitution of degree n.

Suppose that a group has the property that all its operators appear in two sets of conjugate subgroups which are separately neither invariant nor contain any invariant subgroup of the entire group besides the identity. Such a group can be represented as a transitive substitution group with respect to each of these sets of conjugate subgroups and these two transitive representations of the group can be placed into a simple isomorphism in such a way that the resulting group of degree n contains no substitution of degree n. As an illustration of such a group we cite the symmetric group of degree 4 which may be represented as a transitive group of degree 4 with respect to its subgroups of order 6 and as a transitive group of degree 6 with respect to its cyclic subgroups of order 4. The two groups thus obtained can be placed either into a simple isomorphism or into a 4, 4 correspondence so as to obtain a group of degree 10 which involves no substitution whose degree exceeds 9. In the alternating group of degree 5 all the substitutions appear either in the conjugate subgroups of order 12 or in the conjugate subgroups of orders 5 or 10. Simple isomorphisms between these groups can therefore be established in more than one way so as to obtain groups containing no substitution whose degree is equal to the degree of the group.

[1] G. A. Miller, *Bull. Amer. Math. Soc.*, **4**, 141 (1893).