SETS OF INDEPENDENT GENERATORS OF A SUBSTITUTION GROUP*

BY

G. A. MILLER

1. Introduction

Various theorems relating to sets of independent generators of a group of finite order were developed in a previous article published in these Transactions.† The object of the present article is to extend these theorems especially along the line of substitution groups. When the order g of such a group G is of the form p^m, p being a prime number, it is known that the number of substitutions in every possible set of independent generators of G is the same, but for every other value of g there is at least one group for which this number λ is not an invariant of G,‡ viz., the cyclic group of order g. It is clear that in this group a set of independent generators can be so chosen that λ has an arbitrary value from unity to the number of distinct prime numbers which divide g, and that λ can have no other value for such a group.

If $s_1, s_2, \cdots, s_\lambda$ is a set of independent generators of G it is easy to prove that

$$s_1^{\alpha_2} s_2 s_1^{\alpha_2'}, \cdots, s_1^{\alpha_\lambda} s_\lambda s_1^{\alpha_\lambda'},$$

where the exponents $\alpha_2, \alpha_2', \cdots, \alpha_\lambda, \alpha_\lambda'$ are arbitrary integers, is a set of $\lambda - 1$ independent generators of the group H generated by these $\lambda - 1$ substitutions. In fact, if these $\lambda - 1$ generators were not independent H could be generated by some $\lambda - 2$ of them and hence G could be generated by some $\lambda - 1$ of the substitutions $s_1, s_2, \cdots, s_\lambda$ since G is evidently generated by s_1 and H. Hence it results that when H and G are not identical then $s_1, s_1^{\alpha_2} s_2 s_1^{\alpha_2'}, \cdots, s_1^{\alpha_\lambda} s_\lambda s_1^{\alpha_\lambda'}$ is also a set of independent generators of G. It can be proved in a similar manner that

$$s^{(5)} s_3 s^{(6)}, \cdots, s^{(2\lambda-1)} s_\lambda s^{(2\lambda)}$$

---

* Presented to the Society, December 29, 1917.

† Vol. 16 (1915), p. 399.

‡ G. A. Miller, Proceedings of the National Academy of Sciences, vol. 1 (1915), p. 7.

is a set of independent generators of the group generated by these substitutions whenever $s^{(5)}, s^{(6)}, \cdots, s^{(2\lambda-1)}, s^{(2\lambda)}$ are any substitutions of the group generated by s_1 and s_2, etc.

Little is known in regard to the range of values which λ can assume in case its value is not fixed. Some of the properties of the groups for which it can be equal to the number of the prime factors of g, which is evidently its largest possible value, were determined in the article to which we referred. In particular, it is known that all such groups are solvable.

It is interesting to note that when λ is both an invariant of the non-abelian group G and has this maximal value then g must be of the form $p^m q$, where p and q are prime numbers and $p - 1$ is divisible by q. This results immediately from the fact that two operators of different prime orders contained in such a group must be non-commutative and generate a group whose order is the product of these primes. Moreover, the Sylow subgroup of order p^m must be abelian and of type $(1, 1, 1, \cdots)$, and each of its substitutions of order p must be transformed into the same power of itself by a substitution of order q. As the index of this power is the same for all the subgroups of order p contained in this Sylow subgroup there is clearly one and only one such group for every value of m and every prime divisor of $p - 1$.

When G is the symmetric group of degree $n > 2$, the value of λ can clearly always be made equal to any one of the positive integers from 2 to $n - 1$, but the question whether λ can ever exceed $n - 1$ does not seem to have been answered. In fact, it does not seem to be known whether a transitive group of degree n having a set of more than $n - 1$ independent generators exists. In the following section we shall prove that every possible substitution group of degree n having k systems of intransitivity can be generated by $n - k$ of its substitutions. In the particular case where this substitution group G is of order 2^k and has $k = n/2$ systems of intransitivity it results from the theorems noted above that every possible set of independent generators of G is composed of exactly $n - k$ substitutions, so that in this special case the general theorem just noted gives the exact number of independent generators of G.

2. Substitution groups of degree n

It is easy to verify that every substitution group of degree $n < 6$ which involves k systems of intransitivity contains at least one set of $n - k$ generating substitutions and hence it must involve a set of independent generators composed of no more than $n - k$ substitutions. If there were some substitution group for which it would be impossible to find such a set of substitutions the degree of this group would therefore exceed 5. We proceed to prove that no such group exists by proving that if there is no such group of degree less than n then there can be no such group of degree n.

When G is a transitive group $k = 1$. In this case the theorem under consideration was proved in the article noted at the beginning of § 1. When G is intransitive it can be constructed by establishing some isomorphism between two constituent groups of degrees n_1 and n_2 respectively, where $n_1 + n_2 = n$. If this is an $(\alpha, 1)$ isomorphism any set of substitutions contained in G which generates the former of these two constituents must also generate the latter and hence a set of generating substitutions of G can be so chosen that the number of the substitutions in this set does not exceed $n_1 - 1$.

If there is an (α_1, α_2), $\alpha_2 > 1$, isomorphism between the two constituents under consideration the invariant subgroup of G which corresponds to the identity of the former constituent can be generated by less than n_2 substitutions. If we add to these substitutions a set of not more than $n_1 - 1$ substitutions of G which generate the former constituent we obtain a set of no more than $n - 2$ substitutions which generate G. Hence our theorem is proved for the special case when $k = 2$.

When k exceeds 2 at least one of the two constituents of degrees n_1, n_2 must be intransitive. If we assume that this is the constituent of degree n_1 it results from the preceding proof that this constituent can be generated by a set of $n_1 - 2$ substitutions and hence G can be generated by a set of $n - 3$ substitutions whenever it contains at least three systems of intransitivity. As this process may be repeated until we arrive at transitive constituents the following theorem has been established.

THEOREM. *Every substitution group of degree n which has k transitive constituents can be generated by $n - k$ of its substitutions.*

3. SUBSTITUTION GROUPS OF ORDER p^m, p BEING A PRIME NUMBER

From the fact that the order of every transitive group is a multiple of its degree it results that a transitive group of order p^m must be of degree p^α, where the possible values of α are subject to the following condition, when β is taken as small as possible:*

$$\frac{p^\beta - 1}{p - 1} \geqq m \geqq \alpha \geqq \beta.$$

Such a transitive group G must be imprimitive, $\alpha > 1$, and as the transitive group according to which one of its systems of imprimitivity is transformed is of a lower order than G it results that G contains an intransitive subgroup H of index p, whose p transitive constituents are conjugate under G.

When H is the direct product of its transitive constituents the commutator subgroup of G is simply isomorphic with the direct product of $p - 1$ of these

* *Encyclopédie des sciences mathématiques*, tome 1, vol. 3, p. 4.

constituents and the commutator subgroup of the remaining one. As the ϕ-subgroup of G includes its commutator subgroup it results that the number of independent generators of G cannot exceed the number of the independent generators of one of these transitive constituents of H increased by one, whenever H is such a direct product. Moreover, when G is a Sylow subgroup of the symmetric group of degree p^α the number of its independent generators has clearly this maximal value. Hence the

THEOREM. *Each of the Sylow subgroups of order p^m contained in the symmetric group of degree p^α has α independent generators.*

If n is written in the form

$$n = a_1 p^{\alpha_1} + a_2 p^{\alpha_1 - 1} + \cdots + a_{\alpha_1 + 1},$$

where each of the coefficients $a_1, a_2, \cdots, a_{\alpha_1+1}$ is either 0 or a positive integer less than p, the Sylow subgroup of order p^m of the symmetric group of degree n is the direct product of a_1 groups which are simply isomorphic with a Sylow subgroup of the symmetric group of degree p^{α_1}, a_2 groups which are simply isomorphic with a Sylow subgroup of the symmetric group of degree $p^{\alpha_1 - 1}$, etc.* Since the ϕ-subgroup of a direct product is the direct product of the ϕ-subgroups of the factors it results that the number of the independent generators of the Sylow subgroup of order p^m contained in the symmetric group of degree n is

$$a_1 \alpha_1 + a_2 (\alpha_1 - 1) + \cdots + a_{\alpha_1}.$$

It should be noted that a Sylow subgroup of order p^m contained in the symmetric group of degree p^α does not contain as many independent generators as some of the transitive subgroups of this Sylow subgroup, whenever $\alpha > 2$. A proof of this statement is furnished by the following method for constructing infinite systems of transitive groups of prime power orders, which have a larger number of independent generators than the Sylow subgroups in which they are contained.

Suppose that one of the transitive constituents H_1 of H has for its ϕ-subgroup invariant operators constituting an abelian group of type $(1, 1, 1, \cdots)$, and let t be a substitution of order p which transforms all the corresponding letters of the p transitive constituents of H in the same order among themselves. If $s_1 s_2 \cdots s_p$ is a substitution on all the letters of H, which is invariant under t and has the property that each of its factors belongs to a particular constituent of H, then the substitution

$$t' = s_1 s_2^2 \cdots s_{p-1}^{p-1}$$

may be supposed to be transformed by t into itself multiplied by $s_1 s_2 \cdots s_p$.

* G. A. Miller, American Journal of Mathematics, vol. 23 (1901), p. 173.

If we extend the group obtained by establishing a simple isomorphism between the transitive constituents of H by means of the group obtained by replacing s_1 in t' successively by the substitutions of the ϕ-subgroup of H_1 and then extend the group thus obtained by means of t there results a group whose ϕ-subgroup is simply isomorphic with the ϕ-subgroup of H_1 and which has therefore $n_1 + 1$ more independent generators than H_1 has, p^{n_1} being the order of the ϕ-subgroup of H_1.

Starting with the regular abelian group of order p^m and of type $(1, 1, 1, \cdots)$, and extending the intransitive group obtained by establishing a $(1, 1)$ correspondence between p such groups in such a way that each substitution is commutative with t by the simply isomorphic group obtained by establishing a $(1, 1)$ correspondence between $p - 1$ of these groups according to t' there results an H such that when it is extended by t we obtain a transitive group of degree p^{m+1} which has for its ϕ-subgroup p^m invariant operators constituting the abelian group of type $(1, 1, 1, \cdots)$ and of order p^m. Hence it results that *there is a transitive group of degree* p^{m+k}, *m and k being arbitrary positive integers, which has* $k(m + 1)$ *independent generators.*

The maximum number of independent generators in such a group of degree p^c corresponds to a maximum value of the expression $(c - m)(m + 1)$ and hence it is equal to $\frac{1}{4}(c + 1)^2$ when c is odd, and to $\frac{1}{4}(c^2 + 2c)$ when c is even. The former value corresponds to $m = \frac{1}{2}(c - 1)$, while the latter presents itself in two cases, viz., when m is either $c/2$ or $(c/2) - 1$. The ratio between the number of independent generators of a Sylow subgroup of order p^β contained in the symmetric group of degree p^c and those of certain of its transitive subgroups must therefore approach zero as c approaches infinity.

If the order of a transitive group of degree p^2 is of the form p^m the value of m must be one of the p numbers $2, 3, \cdots, p + 1$. Moreover, there is at least one such transitive group for each of these values of m. We proceed to prove that with the exception of the cyclic group each one of these possible groups has exactly two independent generators. This result follows directly from the properties of one of the largest of these groups, which is a Sylow subgroup of the symmetric group of degree p^2 and hence may be supposed to contain each of the others.

Let t be a substitution of order p which is not contained in the H of this Sylow subgroup, and let s represent a substitution of degree p contained in H. The $p - 1$ substitutions $s_1, s_2, \cdots, s_{p-1}$ which satisfy the equations

$$t^{-1} s t = s_1 s, \qquad t^{-1} s_1 t = s_2 s_1, \qquad \cdots, \qquad t^{-1} s_{p-2} t = s_{p-1} s_{p-2}$$

are clearly of degrees $2p, 3p, \cdots, p^2$ respectively, and the last of these $p - 1$ substitutions is invariant under the Sylow subgroup under consideration.

Hence t and s_{p-1} generate a transitive group of order p^2, t and s_{p-2} generate a transitive group of order p^3, $\cdots$, t and s_1 generate a transitive group of order p^{p+1}. Moreover, each of these transitive groups involves all the substitutions of the H of said Sylow subgroup which together with t do not generate a transitive group of larger order. Hence it results that *every non-cyclic transitive group of degree p^2 and of order p^m has exactly two independent generators.*

By means of this theorem it is easy to determine all the transitive substitution groups of degree p^2 whose order is of the form p^m. From the preceding paragraph it results that whenever $m > 2$ the central of such a group is of order p and that t and s' generate a group which involves no substitution of order p^2 whenever $s'_{p-1} = 1$, s' being any substitution of H and s'_1, s'_2, $\cdots$, s'_{p-1} being the successive commutators corresponding to s_1, s_2, $\cdots$, s_{p-1} of the preceding paragraph. If we use for t any substitution of order p^2 contained in the Sylow subgroup of order p^{p+1} mentioned above we obtain a second group of each of the orders p^2, p^3, $\cdots$, p^p. The number of substitutions of order p^2 in each of these groups is equal to the order of the group multiplied by $(p-1)/p$. Each of these substitutions of order p^2 generates the same subgroup of order p. Hence it results that *there are exactly two transitive groups of degree p^2 and of each of the orders p^2, p^3, $\cdots$, p^p, while there is only one such group of order p^{p+1}.* The total number of transitive groups of degree p^2 which have an order of the form p^m is therefore $2p-1$.

It is well known that the enumeration of the possible substitution groups of a given degree is a very difficult problem when this degree is large, and even for the smaller degrees it has been effected mainly by tentative methods. Hence it may be of interest to note that the formula of the preceding paragraph gives the complete enumeration of the prime power transitive groups of degree p^2, and seems to be the first formula giving a complete enumeration of all the transitive groups of a composite degree and of given orders when the number of these groups for the same degree has no upper limit. That is, the number of these groups of the same degree increases indefinitely with p.

UNIVERSITY OF ILLINOIS