INDEPENDENT GENERATORS OF A GROUP OF FINITE ORDER*

BY

G. A. MILLER.

1. INTRODUCTION

A set of operators $s_1, s_2, \cdots, s_\lambda$ belonging to the group G of finite order g is called a set of independent generators of G provided that these λ operators generate G but no $\lambda - 1$ of them generate G. Sets of independent generators can generally be selected in a large number of different ways when the group G is given. When G is abelian it is always possible to select these sets in such a manner that the group generated by any number of the operators of any set has only the identity in common with the group generated by the rest of the operators of this set, but when G is non-abelian it is not always possible to select such a set of independent generators, as results directly from the properties of the quaternion group.

The term independent generators has been used mainly in reference to abelian groups. Hence it has been commonly used with the restricted meaning that the group generated by any number of a set of these generators has only the identity in common with the group generated by the rest of those in the same set. Under this restricted definition Frobenius and Stickelberger proved the very useful theorem that the number of these independent generators is an invariant of the group whenever the group is abelian and has an order which is some power of a prime number.† It has recently been proved that the number λ is also an invariant of the group under the general definition given above even when the group of order p^m, p being any prime number, is non-abelian.‡ When $\lambda = 1$, G is clearly cyclic, and hence this case offers few difficulties. When $\lambda = 2$ and each of the operators s_1, s_2 is of order 2, G is dihedral, but the general case when $\lambda = 2$ seems to present many difficulties.§

The value of λ can clearly not exceed the number of prime factors of g. In case λ is equal to this number, G must be solvable. A number of other properties possessed by all such groups were developed in a recent article

* Presented to the Society at Chicago, April 3, 1915.

† Journal für Mathematik, vol. 86 (1879), p. 219.

‡ G. A. Miller, these Transactions, vol. 16 (1915), p. 21.

§ Cf. H. Hilton, *An Introduction to the Theory of Groups of Finite Order*, 1908, p. 233.

published in the Proceedings of the National Academy of Sciences, volume 1, 1915, page 241. From these developments it is easy to deduce the following theorem: *A necessary and sufficient condition that a group G contains at least one set of independent generators composed of as many operators as there are prime factors in the order of G is that each of the Sylow subgroups of G is abelian and is generated by a set of operators of prime order each of which is transformed only into powers of itself by every Sylow subgroup whose order is a power of a smaller prime number.*

2. Groups whose orders are powers of a single prime number

If $g = p^m$, p being any prime number, the maximum value of λ is m, and when $\lambda = m$, G is the abelian group of type $(1, 1, 1, \cdots)$. When $\lambda = m - 1$ and G is abelian then all its invariants except one are equal to p while this one is equal to p^2. On the other hand, when G is non-abelian and $\lambda = m - 1$, the commutator subgroup of G is clearly of order p since this subgroup is contained in every subgroup of G whose index is p. As the pth power of every operator of G must also be contained in every subgroup of index p it results that G cannot involve any operator whose order exceeds p^2, and, if it contains operators of this order, each of them must generate the commutator subgroup of G. This follows directly from the well-known theorem that the quotient group of any group of order p^m with respect to the cross-cut of all its subgroups of index p is abelian and of type $(1, 1, 1, \cdots)$.

It is not difficult to complete the determination of all the non-abelian groups of order p^m which have $m - 1$ independent generators. In fact, every non-invariant operator of such a group G has exactly p conjugates since the commutator subgroup of G is of order p. Hence such an operator s_1 is commutative with every operator of a subgroup H_1 of index p. Let s_2 be any operator of G which is not contained in H_1. The subgroup of index p composed of all the operators of G which are commutative with s_2 has p^{m-2} operators in common with H_1. These common operators form a group K_1 composed of all the operators of G which are commutative with both s_1 and s_2. If K_1 is abelian it is the central of G. If it is non-abelian we can determine two of its operators s_3, s_4 in exactly the same manner as s_1 and s_2 were determined in G, and thus arrive at a subgroup K_2 of order p^{m-4} which is composed of all the operators of G which are commutative with each of the four operators s_1, s_2, s_3, s_4.

If K_2 is also non-abelian this process can be continued until we arrive at a subgroup K_α of order $p^{m-2\alpha}$ which is the central of G. When this central involves no operator whose order exceeds p, and $m > 2\alpha + 1$, G is clearly the direct product of a group of order $p^{2\alpha+1}$ having a central of order p and the

abelian group of order $p^{m-2\alpha-1}$ and of type $(1, 1, 1, \cdots)$. When this central involves operators of order p^2 it must be of type $(2, 1, 1, \cdots)$, and G is the direct product of a group of order $p^{2\alpha+2}$, whose central is the cyclic group of order p^2, and the abelian group of order $p^{m-2\alpha-2}$ and of type $(1, 1, 1, \cdots)$ whenever $m > 2\alpha + 2$.

When $p > 2$ all the operators of order p contained in G constitute a subgroup of index p whenever G involves at least one operator whose order exceeds p. The independent generators of this subgroup can be selected in the manner employed to select those of G. If none of the operators of order p^2 is contained in the central of G there must be an operator of order p^2, contained in G, which is non-commutative with some operators in the central of the subgroup composed of all the operators of G whose orders divide p, but which is commutative with every non-invariant operator in a set of independent generators of this subgroup. Hence the following theorem has been established: *If a non-abelian group of order p^m, $p > 2$, contains a set of $m - 1$ independent generators then these generators can be so chosen that at most one of them has an order which exceeds p and that each of them is commutative with at least $m - 3$ of the others.*

From what precedes it results that when $m > 3$ there are exactly three non-abelian groups of order p^m, $p > 2$, which have a set of $m - 1$ independent generators and a central of order p^{m-2}. When $m > 5$ there are three more such groups having a central of order p^{m-4}, etc. In general, if m is even the number of the groups of order p^m, $p > 2$, which have a set of $m - 1$ independent generators is $3(m - 2)/2 + 1$. When m is odd the number of these groups is $3(m - 1)/2$. One of these groups and only one is abelian.

When $p = 2$ and G involves a non-invariant operator s_1 of order 2 all the operators of G which are commutative with s_1 constitute a subgroup of index 2. Half of those operators of G which are not contained in this subgroup are of order 2 and the rest are of order 4. In fact, all the products obtained by multiplying s_1 into these operators must be contained among them, and if s_1 is multiplied into such an operator of order 2 or 4 the product will be respectively of order 4 or 2. Hence s_1 and any one s_2 of these operators of order 2 will generate the octic group. Every operator of this octic group is commutative with every operator of the group generated by the remaining independent generators of G if these generators are selected from the subgroup K_1 of index 4, composed of all the operators of G which are commutative with each of the two operators s_1, s_2.

If the subgroup K_1 contains an operator s_3 of order 2 which is non-invariant it must also contain another operator s_4 of order 2 such that s_3 and s_4 generate the octic group and that each operator of this octic group is commutative with all the operators of a subgroup K_2 of order 2^{m-4} contained in K_1. Hence

it results that G contains a subgroup K_α of order $2^{m-2\alpha}$ which involves all the invariant operators of order 2 and hence the commutator subgroup of G, and that G can be obtained by extending K_α by means of α octic groups. When K_α is non-abelian all its non-invariant operators are of order 4 and have a common square. Hence K_α is Hamiltonian, and it must therefore be the direct product of the quaternion group and an abelian group of type $(1, 1, 1, \cdots)$ *. When K_α is abelian it is either of type $(1, 1, 1, \cdots)$ or of type $(2, 1, 1, \cdots)$. Hence the following theorem has been established: *If a non-abelian group of order 2^m has a set of $m - 1$ independent generators and is not Hamiltonian it can be formed by extending successively by means of an octic group, having its commutator subgroup in common with the group already obtained and having each of its operators commutative with every operator of this group, one of the following three groups: the Hamiltonian group of order 2^β, the abelian group of type $(1, 1, 1, \cdots)$, the abelian group of type $(2, 1, 1, \cdots)$.*

When $m = 3$ the quaternion and the octic group are the only two non-abelian groups, and they have $m - 1$ independent generators. When $m > 3$ there are evidently three and only three groups which have $m - 1$ independent generators and also the four-group for their group of inner isomorphisms. The numbers of operators of order 4 in these three groups are respectively 2^{m-2}, 2^{m-1}, $2^{m-1} + 2^{m-2}$. When $m > 5$ there are also three such groups whose group of inner isomorphisms is of order 16. When $m > 7$ there are three additional groups whose group of inner isomorphisms is of order 2^6, etc. Hence it results that the number of the groups of order p^m which have $m - 1$ independent generators is independent of the value of p. That is, *the number of the groups of order p^m, p being any prime number, which possess a set of $m - 1$ independent generators is either $3(m - 1)/2$ or $3(m - 2)/2 + 1$, according as m is odd or even.*

From the method explained above it results directly that when K_α is abelian and of type $(1, 1, 1, \cdots)$, all the operators in the set of $m - 1$ independent generators selected in the given manner are of order 2 and that the number of the operators of order 4 in G is given by the formula

$$N_1 = 2^{m-2} + 2 \cdot 2^{m-4} + 2^2 \cdot 2^{m-6} + \cdots + 2^{\alpha-1} \cdot 2^{m-2\alpha} = 2^{m-1} - 2^{m-\alpha-1}.$$

When K_α is the abelian group of type $(2, 1, 1, \cdots)$, a set of independent generators can be so chosen that all of these $m - 1$ operators, with the exception of one, are of order 2, and the number of the operators of order 4 in this group is equal to 2^{m-1}. Finally, when K_α is the Hamiltonian group a set of $m - 1$ independent generators can be so selected that only two of them are of order 4, and the number of the operators of order 4 in this group is given by the formula

* G. A. Miller, Paris Comptes Rendus, vol. 126 (1898), p. 1408.

$$N_3 = 2^{m-2} + 2 \cdot 2^{m-4} + 2^2 \cdot 2^{m-6} + \cdots + 2^{\alpha-1} \cdot 2^{m-2\alpha} + 2^\alpha \cdot 3 \cdot 2^{m-2\alpha-2}$$
$$= 2^{m-1} + 2^{m-\alpha-2}.$$

The category of groups for which K_α is the abelian group of type $(2, 1, 1, \cdots)$ can be defined by the fact that it is composed of all the non-abelian groups of order 2^m which contain a set of $m - 1$ independent generators and contain also invariant operators of order 4. All groups of this category are conformal with abelian groups, but no group belonging to one of the other two categories can be conformal with an abelian group as results directly from the formulas giving the number of operators of order 4 in such groups. From what precedes it is clear that the groups of order p^m which involve a set of $m - 1$ independent generators constitute elementary infinite categories of groups whose groups of inner isomorphisms are abelian, of type $(1, 1, 1, \cdots)$, and have orders which are even powers of p. The last named fact is also a special case in reference to the group of inner isomorphisms of a metabelian group whose commutator subgroup is cyclic.*

If a group G of order a power of p is generated by two operators of order p, its commutator subgroup must be cyclic when $p = 2$. For all larger values of p this commutator subgroup may have an arbitrarily large number of independent generators. To prove this fact, let $s_1, s_2, \cdots, s_\lambda$ be a set of independent generators of the abelian group of order p^λ and of type $(1, 1, 1, \cdots)$. Let t_1 and t_2 be two operators of order p in the group of isomorphisms of this abelian group, such that t_1 is commutative with each of the given independent generators having an odd subscript, and transforms each one of those with an even subscript into itself multiplied by the one having the next higher odd subscript; while t_2 is commutive with those having an even subscript and transforms each of the others into itself multiplied by the operator bearing the next higher subscript. The only exception to this rule is that s_λ is commutative with each of the operators t_1 and t_2. If $t_2^{-1} t_1 t_2 = s_1 t_1$, it results directly that t_1 and t_2 generate a group of order $p^{\lambda+2}$, which has the given abelian group for its commutator subgroup. Hence the following theorem: *There is no upper limit for the possible order of a group of order a power of p which can be generated by two operators of order p. When $p = 2$ the commutator subgroup of such a group must be cyclic, but when p is odd there is no upper limit to the number of possible independent generators of such a commutator subgroup.*

3. Substitution groups of degree n

If a transitive substitution group of degree n possesses a set of independent generators composed of transpositions it must be primitive since a transposition cannot interchange two or more systems of imprimitivity of an im-

* Cf. W. B. Fite, these Transactions, vol. 3 (1902), p. 342.

primitive substitution group. From this fact and from the well-known theorem that a primitive group which involves a transposition is symmetric it results directly that *a necessary and sufficient condition that a transitive substitution group contains a set of independent generators composed of transpositions is that it is the symmetric group.* The number of the substitutions in a set of independent generators, composed of transpositions, of a transitive group of degree n is therefore always $n-1$, and one such possible set is as follows: $(a_1 a_2)$, $(a_1 a_3)$, $\cdots$, $(a_1 a_n)$.

When the order of a substitution group G is not a power of a prime number it is often possible to select two or more different sets of independent generating substitutions of G in such ways that the number of the substitutions in these sets is not the same. We proceed to prove that every possible substitution group of degree n contains at least one set of independent generators which does not involve more than $n-1$ substitutions. For small values of n it is easy to verify this theorem directly. If the theorem were not universally true there would be some smallest value of $n > 2$ such that at least one substitution group K of degree n would not involve a set of independent generators composed of less than n substitutions, but every substitution group of degree $n' < n$ would contain at least one set of independent generators involving no more than $n-1$ substitutions.

It is evident that K could not be intransitive; for, if it were intransitive, each of its transitive constituents could be generated by a smaller number of substitutions than its degree, and hence K itself could be generated by less than n substitutions. If K were imprimitive one of its sets of k systems of imprimitivity would be permuted according to a substitution group of degree k which could be generated by less than k substitutions. The invariant subgroup of K corresponding to the identity of this substitution group could not involve a transitive constituent whose degree would exceed n/k. Hence this subgroup could be generated by a set composed of no more than $n-k$ different substitutions. From this it results directly that K could be generated by less than n substitutions which is contrary to our hypothesis. Finally, if K were primitive its subgroup composed of all its substitutions omitting a given letter would be maximal. As this subgroup could be generated by a number of substitutions which does not exceed $n-2$, K could be generated by a set involving at most one more substitution. This completes a proof of the theorem: *In every possible substitution group of degree n there is at least one set of independent generators which does not involve more than* $n-1$ *substitutions of the group.*

UNIVERSITY OF ILLINOIS.