

# INFINITE SYSTEMS OF INDIVISIBLE GROUPS\*

BY

G. A. MILLER

## § 1. *Introduction.*

A group is said to be *divisible* (*zerfallend*) if it is the direct product of two groups, neither of which is the identity. If it is not such a direct product it is said to be *indivisible* or *prime*.† Among the indivisible groups the simple groups occupy the most important place. Divisible groups are necessarily composite but there are also many types of composite groups which are not divisible. Each indivisible group may be used to construct an infinite system of distinct divisible groups by forming successive direct products with this group as a factor. That is, by forming the direct product of two groups which are simply isomorphic with the given group  $H$ , and then forming the direct product of a group which is simply isomorphic with  $H$  and the direct product just found, etc. Such successive direct products we shall call successive *powers of the given group*. The two infinite systems formed by the successive powers of two distinct indivisible groups have no group in common.‡

FROBENIUS and STICKELBERGER proved that the cyclic *primary* groups, that is, the cyclic groups whose orders are powers of a single prime number, are the only abelian groups which are indivisible.§ Hence every divisible abelian group is a direct product of cyclic primary groups, and every such direct product is an abelian group. Moreover, every abelian group is completely determined by its cyclic primary factor groups. In the articles cited, MACLAGAN-WEDDERBURN and REMAK extended this theorem by proving that every divisible group is completely determined by the factor groups when ever it is represented as a direct product of indivisible groups.

As there is only one indivisible abelian group of a given order an abelian indivisible group can be completely defined by giving its order. The infinite system of indivisible abelian groups will be represented by the symbol  $S_1$ . The main object of the present paper is to study infinite systems of indivisible groups which are such that no two distinct groups of the same system have a

\*Presented to the Society (Chicago), April 5, 1912.

† MACLAGAN-WEDDERBURN, *Annals of Mathematics*, series 2, vol. 10 (1909), p. 173.

‡ REMAK, *Crelle's Journal*, vol. 139 (1911), p. 293.

§ FROBENIUS and STICKELBERGER, *Crelle's Journal*, vol. 86 (1879), p. 217.

common order. It is hoped that this classification will serve to exhibit more clearly some fundamental common properties of known categories of groups and also to extend our knowledge as regards the groups which have such common properties. The rapid increase in the number of known groups calls for improvements of the methods of classification and for a determination of common properties which may serve as a suitable basis of classification. As each indivisible group may be used to construct an infinite system of divisible groups by forming its successive powers, and as the two infinite systems of such groups which may be derived from two distinct indivisible groups have no group in common, it is clear that infinite systems of indivisible groups afford large possibilities for group construction.

In what follows we shall direct attention to a still larger source for group construction by showing how we may construct an infinite system of distinct *indivisible* groups by starting with any given non-abelian indivisible group, and by proving that two of these systems cannot have any group in common unless one of the two systems is contained entirely in the other system. We shall also obtain a formula by means of which the number of operators of highest order in any one of such an infinite system of indivisible groups can be readily determined. These developments call for a determination of additional general theorems relating to divisible groups. Several such theorems are given in the following section and these constitute perhaps the most important part of the present paper.

Some of the best known infinite categories of non-abelian groups are so elementary as to offer little interest from the standpoint of group construction. For instance, the Hamiltonian groups are merely direct products of the quaternion group and powers of groups of  $S_1$ , and every such direct product is Hamiltonian provided either all the factors selected from  $S_1$  are of odd order or the group of order 2 constitutes the only factor of even order selected from  $S_1$ .<sup>\*</sup> Hence the quaternion group is the only indivisible group among the totality of Hamiltonian groups. A closely related infinite category of groups is the one formed by the direct products of the octic group and powers of the group of order 2. There is one and only one such group of order  $2^\alpha$ ,  $\alpha > 2$ , and it has been proved that this infinite system of groups is composed of all the non-abelian groups in which no more than one fourth of the operators have orders larger than 2.<sup>†</sup>

Two important infinite systems of indivisible groups received attention very early as a result of their prominent position in the theory of substitution groups; viz., the symmetric and the alternating groups. The systems of

<sup>\*</sup> MILLER, Bulletin of the American Mathematical Society, vol. 4 (1898), p. 514.

<sup>†</sup> MILLER, Annals of Mathematics, ser. 2, vol. 7 (1906), p. 55.

abstract groups which are separately simply isomorphic with these substitution groups will be denoted by  $S_2$  and  $S_3$  respectively. Each of these two systems has its first group in common with  $S_1$ , but otherwise no two of the three infinite systems  $S_1, S_2, S_3$  have a common group. System  $S_3$  is especially important, since all of its groups, with the exception of the one of order 12, are simple. General abstract definitions of the groups of these two infinite systems were first given by MOORE,\* and their Sylow subgroups have been studied by RADZIG † and by FINDLAY.‡

As none of the groups of systems  $S_2$  and  $S_3$  contains a subgroup of index 2 which is a direct product of two simply isomorphic groups, it results from the theorem to which we referred above that each of the groups in these two systems, except the first group, can be used to construct an infinite system of indivisible groups, and that no two of these systems have a common group. In fact, it will appear that the first group of  $S_2$  may also be used in this way but that the first one of  $S_3$  does not have this property.

## § 2. *Some properties of divisible groups and of their subgroups.*

Suppose that the non-abelian group  $G$  is the direct product of the  $\lambda$  subgroups  $H_1, H_2, \dots, H_\lambda$ . It is evident that the group of inner isomorphisms of  $G$  is the direct product of the groups of inner isomorphisms of  $H_1, H_2, \dots, H_\lambda$ ; that the commutator subgroup of  $G$  is the direct product of the commutator subgroups of  $H_1, H_2, \dots, H_\lambda$ ; that the central of  $G$  is the direct product of the centrals of  $H_1, H_2, \dots, H_\lambda$ ; and that each of the largest abelian subgroups of  $G$  is a direct product of largest abelian subgroups from each of the factor groups  $H_1, H_2, \dots, H_\lambda$ . If  $S^{(\alpha)}$  represents the various operators of  $H_\alpha$ ,  $1 \leq \alpha \leq \lambda$ , every operator of  $G$  is of the form

$$S^{(1)} S^{(2)} \dots S^{(\lambda)}.$$

In any subgroup  $K$  of  $G$  the operators  $S^{(\alpha)}$ , where  $\alpha$  has any one of the values  $1, 2, \dots, \lambda$ , constitute a subgroup§ of  $H_\alpha$ , and  $K$  is formed by certain isomorphisms between these constituent subgroups, if we include under the term isomorphism direct products even when one or more of the factors become the identity. A necessary and sufficient condition that  $K$  has only the identity in common with each of the factor groups  $H_1, H_2, \dots, H_\lambda$  is that it is simply isomorphic with at least two of these constituent subgroups. Hence we have the following theorem: *If  $K$  is an invariant subgroup under  $G$  and has*

\* Proceedings of the London Mathematical Society, vol. 28 (1896), p. 363; cf. DICKSON, *Linear Groups*, 1901, p. 287.

† *Dissertation*, Berlin, 1895.

‡ These Transactions, vol. 5 (1904), p. 263.

§ The term subgroup is used here, and in what follows, in its most general sense, including both the identity, and the entire group.

*only the identity in common with each of the factor subgroups  $H_1, H_2, \dots, H_\lambda$ , then each operator of  $K$  is invariant under  $G$ .* That is, if an invariant subgroup of  $G$  involves no operator besides the identity from any one of the factor subgroups  $H_1, H_2, \dots, H_\lambda$ , it must be contained in the central of  $G$ , and it must be simply isomorphic with subgroups in the centrals of at least two of the factor subgroups  $H_1, H_2, \dots, H_\lambda$ . As a special case of this theorem we have the known theorem that every invariant subgroup of  $G$  which has only the identity in common with each of the factor subgroups  $H_1, H_2, \dots, H_\lambda$  is abelian.\*

The italicized theorem of the preceding paragraph may readily be deduced from the fact that the cross-cut† of any invariant subgroup  $K$  of  $G$  and of a factor subgroup  $H_\alpha$  is an invariant subgroup of  $H_\alpha$ , and the quotient group of the constituent of  $K$  contained in  $H_\alpha$ , which corresponds to this cross-cut, is composed of invariant operators under  $G$ . This fact results directly from the theorem that the cross-cut of two invariant subgroups of any group includes all the commutators which can be formed when the two elements of each one of these commutators are selected from both of these two invariant subgroups. The italicized theorem of the preceding paragraph may also be regarded as a special case of the following theorem: *The cross-cut of the commutator subgroup of  $G$  and any other invariant subgroup of  $G$  is the direct product of subgroups of the commutator subgroups of the factor groups  $H_1, H_2, \dots, H_\lambda$ .*

Since the group of inner isomorphisms of a group is necessarily non-cyclic it results that only one of the factor groups  $H_1, H_2, \dots, H_\lambda$  is non-abelian whenever the group of inner isomorphisms of  $G$  involves a cyclic subgroup of prime index. This must also be the case whenever the order of the group of inner isomorphisms of  $G$  is the product of less than four prime factors. If the order of any non-abelian solvable group  $G'$  is divisible by a prime  $p$  which does not divide the order of its group of inner isomorphisms then  $G'$  is the direct product of its Sylow subgroup whose order is a power of  $p$  and a subgroup whose order is prime to  $p$ . The truth of this theorem becomes evident if we recall that to the identity in the group of inner isomorphisms there corresponds the central of  $G'$ , and hence this central is a direct product having the given Sylow subgroup as a factor. As the group of inner isomorphisms is solvable and its order is prime to  $p$  the theorem is established.‡

It was observed above that if a group is the direct product of two or more non-abelian groups its group of inner isomorphisms is also a direct product, but it is evidently not true that every group whose group of inner isomorphisms is a direct product is itself such a product. It follows from the preceding paragraph, however, that a necessary and sufficient condition that any group

\* Cf. MACLAGAN-WEDDERBURN, *Annals of Mathematics*, series 2, vol. 10 (1909), p. 174.

† The totality of operators common to two groups is called their cross-cut.

‡ These Transactions, vol. 1 (1900), p. 66.

is the direct product of its Sylow subgroups is that its group of inner isomorphisms is the direct product of its Sylow subgroups whenever it involves more than one such subgroup. This theorem follows also directly from the fact that a necessary and sufficient condition that a group is the direct product of its Sylow subgroups is that we arrive at the identity by forming the successive groups of inner isomorphisms.\* This theorem may be regarded as a special case of the following theorem. *A necessary and sufficient condition that a solvable group be a direct product of a Sylow subgroup and another subgroup is that its group of inner isomorphisms involves the corresponding Sylow subgroup as a factor of a direct product whenever it involves such a Sylow subgroup.* This theorem includes the theorem of the preceding paragraph and may be proved in an exactly similar manner.

If the order of  $G$  is a power of a single prime number the orders of each of its factor subgroups  $H_1, H_2, \dots, H_\lambda$  must be powers of the same prime. As the central of each of these factor groups exceeds unity it follows that the central of  $G$  has at least  $\lambda$  invariants. Hence it results that *a group of order  $p^m$ ,  $p$  being any prime number, whose central is cyclic must be indivisible.* A Sylow subgroup of order  $p^m$  in the holomorph of any abelian group of order  $p^a$  has exactly  $p$  invariant operators and hence such a subgroup is always indivisible. If the holomorph of an abelian group of order  $p^a$  were divisible it would therefore be a direct product of a group whose order is prime to  $p$  and of a group involving a Sylow subgroup of order  $p^m$ . This is clearly impossible, since the operators of the former could not be commutative with each operator of the latter. As the holomorph of any abelian group is the direct product of the holomorphs of its Sylow subgroups† we have the theorem: *A necessary and sufficient condition that the holomorph of an abelian group be divisible is that the order of this abelian group is divisible by at least two different prime factors.*

If a divisible group involves an indivisible Sylow subgroup of order  $p^m$  then there is one and only one factor subgroup whose order is divisible by  $p$ . Hence it results that a divisible group cannot involve an indivisible Sylow subgroup which involves operators which are non-commutative with all the operators of the group whose orders are prime to the order of this Sylow subgroup. For instance, a dihedral group whose order is the double of an odd number is indivisible since it involves operators of order 2 which are non-commutative with all of its operators of odd order and the Sylow subgroups of order 2 are indivisible.

If a primitive substitution group is a direct product it must be the direct product of two simply isomorphic simple groups of composite order.‡ Hence

\* LOEWY, *Mathematische Annalen*, vol. 55 (1902), p. 69.

† *These Transactions*, vol. 4 (1903), p. 153.

‡ MAILLET, *Thèse*, Paris, 1892, p. 31.

it results that when  $\lambda > 2$  every maximal subgroup of  $G$  either is invariant or contains an invariant subgroup of  $G$ , besides the identity. This theorem remains true when  $\lambda = 2$  provided  $G$  is not the direct product of two simply isomorphic simple groups of composite order.

§ 3. *Infinite system of indivisible groups obtained by extending given groups.*

Suppose that  $G$  is the direct product of two simply isomorphic indivisible non-abelian groups  $H_1, H_2$ . We may extend  $G$ , so as to obtain a group  $G'$  whose order is twice the order of  $G$ , by means of an operator of order 2 which transforms the corresponding operators of  $H_1$  and  $H_2$  into each other. We shall prove that this extended group is also non-abelian and indivisible. If  $G'$  were divisible it would be the direct product of two groups  $H'_1, H'_2$ . The subgroup  $G$  of index 2 under  $G'$  would then be either the direct product of one of these factor groups of  $G$  and of a subgroup of index 2 contained in the other or it would be formed by an isomorphism between  $H'_1$  and  $H'_2$  with respect to quotient groups of order 2. In the former case  $G$  would be the direct product of two subgroups  $H''_1, H''_2$  which are simply isomorphic with  $H_1$  and  $H_2$  respectively since these factor groups are indivisible.

As all the operators of one of the subgroups  $H'_1, H'_2$  are commutative with some of the operators of  $G'$  which are not in  $G$ , it results that this subgroup, say  $H'_1$ , must be formed by establishing a simple isomorphism between  $H_1$  and  $H_2$ . As only invariant operators of  $G$  are commutative with every operator of  $H'_1$ , it follows that  $H'_2$  is abelian. As this is contrary to the hypothesis it results that  $G$  must be formed by establishing an isomorphism, with respect to a quotient group of order 2, between  $H'_1$  and  $H'_2$ , if  $G'$  is divisible. This hypothesis implies that  $G$  contains a subgroup of index 2 which is a direct product of two groups  $H'''_1, H'''_2$ . All the operators of each of these groups, taken separately, are commutative with some operators of  $G'$  which are not contained in  $G$ . Hence  $H'''_1$  and  $H'''_2$  are formed by establishing a simple isomorphism either between  $H_1$  and  $H_2$  or between subgroups of these groups. This must be a simple isomorphism between  $H_1$  and  $H_2$  in one case, as the direct product of  $H'''_1$  and  $H'''_2$  could otherwise not be of index 2 under  $G$ . If  $H'''_1$  were a simple isomorphism between  $H_1$  and  $H_2$  and  $H'''_2$  were a simple isomorphism between subgroups of index 2 contained in  $H_1$  and  $H_2$  respectively, it would clearly not be possible for all the operators of  $H'''_1$  to be commutative with all those of  $H'''_2$ . Hence we have arrived at a contradiction by assuming that  $G'$  is divisible, and it must therefore always be indivisible.

If we suppose that the common order of  $H_1$  and  $H_2$  is  $h_1$  it results that the order of  $G'$  is  $2h_1^2$ . As we can extend the square of  $G'$  in a similar way, since  $G'$  satisfies the conditions imposed on  $H_1$ , it results that we obtain by this

process an infinite system of indivisible groups of order  $2^{2n-1} h_1^{2^n}$ ,  $n$  being an arbitrary integer  $\geq 0$  and  $h_1$  being the order of  $H_1$ . The distinct factors of composition of each of these groups are the same as those of  $H_1$  whenever one of the factors of composition of  $H_1$  is 2. If this condition is not satisfied, 2 must be added to the factors of composition of  $H_1$  to obtain the distinct factors of composition of this infinite system of indivisible groups. Some of these results may be expressed in the form of a theorem as follows: *If we extend the square of any non-abelian indivisible group by means of an operator of order 2 which transforms the corresponding operators of the factors of this square into each other, we obtain another non-abelian indivisible group.* By repeating this operation we may therefore construct, by starting with any non-abelian indivisible group, an infinite system of such groups, which is such that no two of the groups of the system have the same order.

The order of the operators of highest order in  $G'$  is twice the order of the operators of highest order in  $H_1$ . Hence the order of the operators of highest order in the group of order  $2^{2n-1} h_1^{2^n}$  in the given infinite system of indivisible groups derived from  $H_1$  is  $2^n$  times that of the operators of highest order in  $H_1$ . The number of these operators of highest order is easily seen to be

$$2 \cdot 2^{2^1-1} \cdot 2^{2^2-1} \dots 2^{2^{n-1}-1} h_1^{1+2+2^2+\dots+2^{n-1}} l = 2^{2^n-n-1} h_1^{2^n-1} l,$$

where  $l$  is the number of the operators of highest order contained in  $H_1$ .

Since each one of the largest abelian subgroups of a direct product must be the direct product of largest abelian subgroups of each of the factor groups, it results that the index of the former subgroups is the product of the indices of the latter. From this it follows directly that the infinite system of indivisible groups derived from  $H_1$  in the given manner cannot involve more than one group which involves an abelian subgroup of index 2, and if there is one such group it must be  $H_1$ . If  $H_1$  involves no abelian subgroup of index 2 the method employed above to prove that  $G'$  is indivisible yields also the result that  $G'$  involves only one subgroup of index 2 which is a square. Hence it results that there are never more than two groups including  $H_1$ , in the infinite system of indivisible groups derived from  $H_1$  in the given manner, which have the property that they involve a subgroup of index 2 which is a square.

We proceed to prove now that if we derive, in the given manner, two infinite systems of indivisible groups from two given non-abelian indivisible groups  $H_1$  and  $H'_1$ , then no group of the one system can be simply isomorphic with a group of the other system unless one of these systems is contained entirely in the other. Suppose that  $H_1$  and  $H'_1$  are two distinct groups which have the property that neither of them involves a subgroup of index 2 which is the square of a non-abelian indivisible group. The group  $G'$  derived from  $H_1$  contains the square of  $H_1$ . We may suppose that  $H_1$  is represented as a

regular substitution group and that this square is the product of two regular substitution groups on distinct sets of letters. These simply isomorphic regular substitution groups will again be represented by  $H_1$  and  $H_2$ , and their product by  $G$ .

If this transitive substitution group  $G'$  on  $2h_1$  letters contains a second subgroup of index 2 which is a square, this subgroup may be supposed to be the direct product of  $K_1$ ,  $K_2$  and it must involve half the operators of  $G$ . These operators are obtained by establishing an isomorphism between  $H_1$  and  $H_2$  with respect to a quotient group of order 2. The subgroup generated by them will be denoted by  $K$ . If  $K$  were the direct product of  $K_1$  and a subgroup of index 2 contained in  $K_2$ , all the operators of  $K_1$  would be commutative with operators of  $G'$  which are not contained in  $G$ . Hence  $K_1$  would be simply isomorphic with  $H_1$ . It remains only to consider the case when  $K$  is obtained by establishing an isomorphism between  $K_1$  and  $K_2$  with respect to a quotient group of order 2. Hence there must be operators in  $G'$  which are not in  $G$  and are separately commutative with each of the operators of two subgroups of index 2 contained respectively in  $K_1$  and  $K_2$ . As these two subgroups are simply isomorphic with corresponding subgroups of  $H_1$  and  $H_2$ , since each of their substitutions, besides the identity, must involve all the letters of  $G'$ , and as every substitution of the one is commutative with every substitution of the other, it results that  $K_1$  and  $K_2$  cannot differ from  $H_1$  and  $H_2$  unless each of these groups involves an abelian subgroup of index 2.

We proceed to prove that the groups  $K_1$  and  $K_2$  can be obtained by extending an abelian group of odd order by means of an operator of order 2 which transforms each operator of this abelian group into its inverse whenever these groups are not simply isomorphic with  $H_1$  and  $H_2$ . In fact, it results from the above that  $K$  is a substitution group such that all of its substitutions besides the identity involve all the letters of  $G'$ . Hence  $K$  is a simple isomorphism between two regular groups. As all the substitutions of  $K_1$  are commutative with  $K_2$  it results that  $K_1$  cannot involve any invariant substitution besides the identity, since such a substitution could not interchange systems of intransitivity of  $G$ , and hence it and  $K_2$  would generate substitutions which would not involve all the letters of  $G'$ .

If a non-abelian group contains an abelian subgroup of index 2 but does not contain any invariant operator besides the identity, it is obtained by extending this abelian subgroup by an operator of order 2 which transforms each operator of this subgroup into its inverse and this subgroup is of odd order.\* Hence we have established the following useful theorem: *The indivisible group obtained by extending the direct product of two simply isomorphic non-abelian indivisible groups by means of an operator of order 2 which transforms the*

\*These Transactions, vol. 10 (1909), p. 472.



corresponding operators of these factor groups into each other cannot involve a second subgroup of index 2 which is such a direct product, unless each of the given non-abelian indivisible groups can be obtained by extending an abelian group of odd order by means of an operator of order 2 which transforms each operator of this abelian group into its inverse. From this theorem and the results proved above we deduce the theorem: If  $H_1$  and  $H'_1$  are two non-abelian indivisible groups which do not involve a subgroup of index 2 which is the direct product of two simply isomorphic non-abelian indivisible groups, then there is no common group in the two infinite systems of indivisible groups, derived from  $H_1$  and  $H'_1$  by the process of forming successively the direct product and extending this product by means of an operator of order 2, which transforms the corresponding operators of this direct product into each other.

It may be observed that when  $H_1$  can be obtained by extending an abelian group of odd order by means of an operator of order 2 which transforms each operator of this abelian group into its inverse then  $G'$  will always contain more than one subgroup of index 2 which is the square of a group. These subgroups are, however, simply isomorphic, according to the proof given above, and hence the entire system is always independent of the choice of its first possible indivisible non-abelian group whenever this first group can be chosen in more than one way. In what follows we shall consider several infinite systems of indivisible groups which have elementary defining equations and which seem to be especially important. The infinite systems of such groups which may be derived from any given non-abelian indivisible group by the general methods given above will not be considered in the remaining sections of this article.

#### § 4. *Several infinite systems of known groups which are indivisible.*

One of the most important systems of non-abelian groups is that composed of the dihedral groups. Since the group of inner isomorphisms of a dihedral group  $G$  is dihedral, it results from the preceding section that such a group cannot be the direct product of two non-abelian groups, as its group of inner isomorphisms involves a cyclic subgroup of prime index. It results therefore, that either  $G$  is indivisible or it is the direct product of a subgroup of its central and another subgroup. As the order of this central cannot exceed 2 unless  $G$  is the four-group and as the operator of order 2 in the central is a commutator whenever the order of the dihedral group is divisible by 8, it results that *a necessary and sufficient condition that the dihedral group be a direct product is that its order is divisible by 4 but not by 8*. If its order exceeds 4 and is divisible by 4 but not by 8, it is evident that  $G$  is the direct product of the group of order 2 and of the dihedral group whose order is half the order of  $G$ . The system of indivisible dihedral groups is therefore composed of one and only

one group of every even order which is not the product of 4 and some odd number. This system will hereafter be denoted by  $S_4$ . The first groups of  $S_2$  and  $S_4$  are identical but otherwise the system  $S_4$  has clearly no group in common with any of the systems  $S_1, S_2, S_3$ .

Closely related to the system of indivisible groups  $S_4$  is the system of dicyclic groups. A dicyclic group may be defined as a group that can be generated by two non-commutative operators of order 4 whose product generates their common square.\* There is one and only one such group of every order which exceeds 4 and is divisible by 4. As the group of inner isomorphisms of a dicyclic group is dihedral and as the invariant operator of order two in such a group is generated by each one of its operators of order 4, it results from the theorem quoted in the preceding paragraph that a dicyclic group is necessarily indivisible. We shall denote the infinite system of these groups by  $S_5$  and it is clear that  $S_5$  does not have any group in common with any of the systems  $S_1, \dots, S_4$ . The first group of  $S_5$  is the quaternion group. In the following section we shall discuss a category of groups which includes  $S_4$  and  $S_5$ .

It is well known that there is one and only one non-abelian group of order  $p^m$ ,  $p$  being a prime and  $m > 3$ , which involves  $p$  cyclic subgroups of order  $p^{m-1}$ . This group exists also when  $m = 3$  and  $p > 2$ . As the central of this group is cyclic it must be indivisible and hence all these groups constitute an infinite system of indivisible groups, which will be denoted by  $S_6$ . It is clear that  $S_6$  does not have any group in common with any of the systems  $S_1, \dots, S_5$ . A closely related infinite system of indivisible group is constituted by the groups of order  $2^n$  which involve three subgroups of order  $2^{n-1}$  which are dihedral, dicyclic and cyclic respectively. There is one and only one such group for every value of  $n > 3$ , and the centrals of these groups are cyclic. This infinite system of indivisible groups will be denoted by  $S_7$  and it is clear that  $S_7$  does not have any group in common with any of the systems  $S_1, \dots, S_6$ .

It was observed in the preceding section that the holomorph of any cyclic group is the direct product of the holomorphs of its Sylow subgroups, and that the latter holomorphs are always indivisible. As the order of the holomorph of a cyclic group of order  $p^\sigma$  is  $p^{2\sigma-1}(p-1)$  it is easy to see that the orders of the holomorphs of two such cyclic groups cannot be equal unless these cyclic groups are identical. In fact, an equation of the form  $p^{2\sigma-1}(p-1) = q^{2\beta-1}(q-1)$  where  $p$  and  $q$  are primes is impossible, since the larger of these two primes could not divide the member of the equation in which it does not explicitly appear. Hence the holomorphs of the indivisible cyclic groups constitute an infinite system of indivisible groups which is such that no two of its group have the same order. This system will be

\* Another definition of dicyclic groups is given by HILTON, *Finite Groups*, 1908, p. 150.

denoted by  $S_3$ , and it is composed of all the indivisible holomorphs of cyclic groups.

We proceed to prove that the holomorphs of the abelian groups of order  $p^a$ ,  $p$  being any prime, and of type  $(1, 1, 1, \dots)$  constitute an infinite system of indivisible groups which is such that no two of its groups are of the same order. It is well known that the order of the holomorph of the given group is  $p^a (p^a - 1) (p^a - p) \cdots (p^a - p^{a-1})$ , and hence we have first to prove that if  $p$  and  $q$  are any two different primes it is impossible to find values for  $\alpha$  and  $\beta$  such that the equation

$$p^a (p^a - 1) (p^a - p) \cdots (p^a - p^{a-1}) = q^\beta (q^\beta - 1) (q^\beta - q) \cdots (q^\beta - q^{\beta-1})$$

is satisfied. To prove this it is only necessary to observe that we may write this equation in the form

$$p^{\alpha_1} r = q^{\beta_1} s,$$

where  $r < p^{\alpha_1}$  and  $s < q^{\beta_1}$ . Moreover, if this equation were true  $r = l_1 q^{\beta_1}$  and  $s = l_2 p^{\alpha_1}$ , where  $l_1$  and  $l_2$  are natural numbers. Hence we have the two contradictory relations

$$rs < p^{\alpha_1} q^{\beta_1} \quad \text{and} \quad rs = l_1 l_2 p^{\alpha_1} q^{\beta_1}.$$

As the assumption that the equation

$$p^a (p^a - 1) (p^a - p) \cdots (p^a - p^{a-1}) = q^\beta (q^\beta - 1) (q^\beta - q) \cdots (q^\beta - q^{\beta-1})$$

could be satisfied led to a contradiction we have established the theorem: *The orders of the holomorphs of two abelian groups each of which involves only operators of the same prime order, besides the identity, cannot be equal unless these abelian groups are identical.*

From this theorem and from the preceding section, it results directly that the holomorphs of the abelian groups whose orders are powers of a single prime and whose type is  $(1, 1, 1, \dots)$  constitute an infinite system of indivisible groups which is such that no two of its groups have the same order. This system will be denoted by  $S_9$ , and it is composed of all the indivisible holomorphs of the abelian groups which involve no operator whose order is the square of a prime number.

Another interesting system of indivisible groups is generated by  $n$  operators which are such that each one of them transforms each of the remaining  $n - 1$  into its inverse. If we assume that at least one of these  $n$  operators has an order which exceeds 2 then all of them must be of order 4 and every pair of them must generate the quaternion group. For simplicity of statement we shall assume this and we shall also assume that none of these  $n$  operators is in the group generated by the remaining  $n - 1$ . Hence it results that they

generate a group of order  $2^{n+1}$ , and it is known that there is one and only one group of order  $2^\alpha$ ,  $\alpha > 2$ , which is generated by such a set of operators.\* The first one of these groups is the quaternion group, which is indivisible, while the second is the Hamiltonian group of order 16 and hence it is divisible. We proceed to determine a necessary and sufficient condition that such a group  $G$  is divisible.

Let the  $n$  generating operators, which have the property that each one of them is transformed into its inverse by each of the others, be represented by  $S_1, S_2, \dots, S_n$ . The subgroup generated by the first  $\alpha < n$  of these contains one and only one subgroup of order  $2^\alpha$  which does not involve any one of the generating operators  $S_1, S_2, \dots, S_\alpha$ . Each of the operators of this subgroup of order  $2^\alpha$  is commutative with every one of the operators  $S_{\alpha+1}, \dots, S_n$ . This subgroup contains two and only two operators which are commutative with each of the operators  $S_1, \dots, S_\alpha$ . These two operators are the commutators of  $G$ . It is known that the central of  $G$  is of order 2 when  $n$  is even and that this central is of order 4 when  $n$  is odd.† A necessary and sufficient condition that this central be the four-group is that  $n + 1$  is a multiple of 4.

According to the preceding section it results therefore that  $G$  cannot be divisible unless  $n \equiv 3 \pmod{4}$ . When  $n$  satisfies this condition the central of  $G$  is non-cyclic and  $G$  involves a subgroup of half its own order which must be indivisible, in accord with what has just been proved. As the central of this subgroup is of order 2, since its order is  $2^\beta$ ,  $\beta$  being odd, it follows that  $G$  involves an invariant operator of order 2 which is not contained in this subgroup and hence  $G$  is the direct product of the group of order 2 and an indivisible group whenever  $n \equiv 3 \pmod{4}$ . This completes a proof of the following theorem: *There is one and only one indivisible group of order  $2^\alpha$ ,  $\alpha \not\equiv 0 \pmod{4}$ , which can be generated by a set of operators satisfying the condition that each one transforms each of the others into its inverse.* When  $\alpha \equiv 0 \pmod{4}$  there is again one and only one non-abelian group which can be generated by such a set of operators, but it is the direct product of the group of order 2 and an indivisible group. The system of indivisible groups described in the italicized theorem of this paragraph will be represented by  $S_{10}$ .

§ 5. *Groups which can be generated by two operators whose common square is generated by their product.*

Let  $S_1, S_2$  be any two non-commutative operators which satisfy the conditions

$$S_1^2 = S_2^2 = (S_1 S_2)^n.$$

\*Bulletin of the American Mathematical Society, vol. 18 (1912), p. 329.

† Ibidem.

It is evident that every dihedral group, except the four-group, and that every dicyclic group can be generated by two such operators. Some of the properties of all the possible groups which can be generated by  $S_1, S_2$  when these operators are restricted only by the condition  $S_1^2 = S_2^2$  have been determined.\* In the present section we aim to determine additional properties of the special category of these groups which can be generated by  $S_1, S_2$  when the second condition stated above is added.

As  $(S_1 S_2)^n = (S_1 S_2^{-1})^n S_2^{2n} = S_1^2$  it results that  $S_1, S_2$  must satisfy the equation

$$(S_1 S_2^{-1})^n = S_2^{2(1-n)}.$$

From the fact that  $(S_1 S_2^{-1})^n$  is both invariant under the group  $G$  generated by  $S_1, S_2$  and is also transformed into its inverse by  $S_1$ ,† it follows that the order of  $(S_1 S_2^{-1})^n$  is either 1 or 2. Since  $n$  and  $1 - n$  are relatively prime, the order of  $S_1 S_2^{-1}$  is not divisible by any odd prime number which divides the order of  $S_1$ . This fact may be used to prove that the two operators  $S_1 S_2^{-1}$  and  $S_1^2$  must always generate a cyclic group whose order is one half the order of  $G$ .

To prove this theorem it remains only to observe that the Sylow subgroup of order  $2^m$  in the abelian group generated by  $S_1 S_2^{-1}$  and  $S_1^2$  is cyclic. As this abelian group involves  $S_1 S_2$  and is generated by  $S_1 S_2$  and  $S_1 S_2^{-1}$ , it results that the Sylow subgroup in question is always generated by  $S_1 S_2$ . In fact, the cyclic group generated by  $S_1 S_2$  involves both  $S_1^2$  and  $S_1 S_2^{-1}$  since the former is generated, by hypothesis, by  $S_1 S_2$ . Hence the following theorem has been established. *If a group is generated by two operators whose common square is generated by their product, then it contains a cyclic subgroup of index two and this cyclic subgroup is generated by this product.*

Suppose that  $G$  is a non-abelian indivisible group which contains a cyclic subgroup  $H$  of index 2. It is clear that  $H$  cannot involve any invariant operators under  $G$  whose orders are prime numbers, for if it should involve any such operator the corresponding Sylow subgroup would be composed of invariant operators under  $G$ , and hence  $G$  would be a direct product, which is contrary to the hypothesis. Hence the invariant operators of  $G$  must have orders of the form  $2^a$  whenever  $G$  is indivisible and contains a cyclic subgroup of index 2. Moreover, every operator of odd order contained in  $G$  is transformed into its inverse by all the operators of  $G$  which are not contained in  $H$ . Hence  $G$  can be constructed by establishing an isomorphism, with regard to a quotient group of order 2, between a dihedral group whose order is twice an odd number and a group of order  $2^m$  which involves operators of order  $2^{m-1}$ . If the latter group were either dihedral or dicyclic  $G$  would be dihedral or dicyclic, and hence we do not need to consider these two cases.

\* MILLER: *Archiv der Mathematik und Physik*, ser. 3, vol. 9 (1905), p. 6.

† Ibidem.

If this group of order  $2^m$  belongs to one of the systems  $S_6$  or  $S_7$  it results from section 2 that  $G$  is indivisible, since the Sylow subgroups of order  $2^m$  are indivisible and each of them involves operators which are non-commutative with each of the operators of odd order contained in  $G$ . Hence we obtain in this way two additional systems of indivisible groups which are such that no two groups of the same system have the same order. The system obtained by selecting the Sylow subgroup of order  $2^m$  from  $S_6$  will be denoted by  $S_{11}$ , while the system obtained by selecting this Sylow subgroup from  $S_7$  will be represented by  $S_{12}$ . None of the groups of the systems  $S_{11}$  and  $S_{12}$  can be generated by two operators whose common square is generated by their product, since the given Sylow subgroups of order  $2^m$  cannot be generated in this way. We shall see that  $S_{11}$  and  $S_{12}$  are composed of all the indivisible groups which involve a cyclic subgroup of index 2 but cannot be generated by two such operators.

The only indivisible groups which involve a cyclic subgroup of index 2 and have not yet been considered are those in which the given Sylow subgroup of order  $2^m$  is cyclic and  $m > 2$ . There is one and only one such group of every order which is divisible by 8 but is not a power of 2, since such an isomorphism can be established for every dihedral group and every cyclic group of order  $2^m$ . All of these groups are indivisible since the Sylow subgroups of order  $2^m$  are indivisible and each of them involves operators which are non-commutative with every operator of odd order contained in  $G$ . This infinite system of indivisible groups will be denoted by  $S_{13}$ , and we may express a part of the preceding results in the form of the following theorem: *An indivisible group which can be generated by two operators whose common square is generated by their product belongs to one of the four systems:  $S_1$ ,  $S_4$ ,  $S_6$  and  $S_{13}$ .* The last three of these systems are composed of such indivisible groups while the first includes also other groups.

#### § 6. *List of infinite systems of indivisible groups.*

For convenience we give below a list of the infinite systems of indivisible groups which considered individually have been in what precedes. Each of these systems is composed of indivisible groups which are such that no two groups of the same system have the same order. A few groups of low orders belong to more than one of these systems but the groups of higher order are all distinct. It is hoped that these symbols may serve as a convenient means of reference.

*Symbol.*

*Description.*

- $S_1$  All the cyclic groups whose orders are powers of a single prime number.
- $S_2$  The abstract groups which are simply isomorphic with the symmetric substitution groups.

- $S_3$  The abstract groups which are simply isomorphic with the alternating substitution groups.
- $S_4$  All dihedral groups except those whose orders are the product of 4 and some odd number.
- $S_5$  All dicyclic groups.
- $S_6$  The non-abelian groups of order  $p^m$ ,  $p$  being a prime, which contain exactly  $p$  cyclic subgroups of order  $p^{m-1}$ .
- $S_7$  The groups of order  $2^n$  involving three subgroups of order  $2^{n-1}$  which are respectively cyclic, dicyclic and dihedral.
- $S_8$  The holomorphs of all the cyclic groups whose orders are powers of a single prime number.
- $S_9$  The holomorphs of the abelian groups of order  $p^m$  and of type  $(1, 1, \dots)$ .
- $S_{10}$  The non-abelian groups of order  $2^\alpha$ ,  $\alpha \not\equiv 0 \pmod{4}$ , which can be generated by a set of operators each of which transforms each of the others into its inverse.
- $S_{11}-S_{13}$  The groups containing a cyclic subgroup of index 2 and formed by an isomorphism between a dihedral group whose order is the double of an odd number and a group of order  $2^m$  contained in the systems  $S_6$ ,  $S_7$  and  $S_1$  respectively.