

# ON THE REPRESENTATION GROUPS OF GIVEN ABSTRACT GROUPS\*

BY

G. A. MILLER

## § 1. *Introduction.*

The abstract group  $G$  is said to be a *representation group* (Darstellungsgruppe) of the finite abstract group  $G'$  whenever  $G$  is one of the largest groups involving a quotient group which is simply isomorphic with  $G'$  as regards a subgroup  $M$  which is contained both in the central and also in the commutator subgroup of  $G$ . A number of fundamental theorems relating to representation groups were developed by I. SCHUR in two memoirs published in the *Journal für Mathematik*.† J. A. DE SEGUIER suggested some simplifications relating to these memoirs.‡ The objects of the present article are to establish a few additional theorems bearing directly on this subject, and to exhibit other points of contact with known developments. It is hoped that the method of approach here adopted will also throw additional light on some of the known results relating to this important system of groups. In particular, we shall not employ the theory of group characters, which was used by I. Schur.

When  $G'$  is abelian it results directly from the definition of the representation groups that the group of inner isomorphisms of  $G$  is abelian and hence  $G$  must be either abelian or metabelian.§ As every metabelian group is known to be the direct product of its Sylow subgroups, it follows that every representation group  $G$  of an abelian group is the direct product of the Sylow subgroups of  $G$ . Every invariant subgroup whose complementary group is abelian is known to be contained in the commutator subgroup. Hence  $M$  is the commutator subgroup of  $G$  whenever  $G$  is abelian, and as the commutator subgroup of a direct product is the direct product of the commutator subgroups of the factors,  $G$  is the direct product of representation groups of the Sylow subgroups of  $G'$ . That is, *a representation group of any abelian group is a direct*

\* Presented to the Society (Chicago), March 21, 1913.

† Vol. 127 (1904), p. 20, and vol. 132 (1907), p. 85.

‡ *Paris Comptes Rendus*, vol. 145 (1907), p. 303.

§ A metabelian group is a non-abelian group whose group of inner isomorphisms is abelian. W. BURNSIDE, *Theory of Groups of Finite Order*, second edition, 1911, p. 57, uses this term with a more general meaning.

product of representation groups of the Sylow subgroups of this abelian group. This theorem is therefore a special result from known theorems on metabelian groups and on commutator subgroups.

Since the group of inner isomorphisms of a group cannot be cyclic\* and since every quotient group of a cyclic group is cyclic, it results that the representation group of a cyclic group is simply isomorphic with this cyclic group. In other words, when  $G$  is cyclic,  $M$  reduces to the identity. It is easy to see that a necessary and sufficient condition that an abelian group is its own representation group is that this abelian group is cyclic, and that a non-cyclic abelian group has always at least two different representation groups. In particular, the representation groups of the non-cyclic group of order  $p^2$  are the two non-abelian groups of order  $p^3$ , since the orders of the commutators of a metabelian group must divide the orders of operators in its group of inner isomorphisms.†

## § 2. Commutators and commutator subgroups.

The commutator of the two operators  $s$  and  $t$  will be written in the form  $s^{-1} t^{-1} s t = c$ . Since

$$(s^{-1} t^{-1} s)^n = (c t^{-1})^n = c t^{-1} c t \cdot t^{-2} c t^2 \cdot \dots \cdot t^{-(n-1)} c t^{n-1} \cdot t^{-n},$$

there results the elementary theorem that if the  $n$ th power of one element of a commutator is commutative with the other element, then the continued product of the  $n$  conjugates of their commutator under the former element is the identity. In particular, *If the square of an operator is commutative with another operator, their commutator is transformed into its inverse by the former of these two operators. If a commutator is commutative with one of its two elements its order is a divisor of the index of the lowest power to which this element must be raised to be commutative with the other element.*‡

The wide application of these elementary theorems may be inferred from the fact that every possible non-abelian group of finite order contains at least one commutator, besides the identity, which is commutative with at least one of the elements of the commutator. In the case of a non-abelian group whose commutator subgroup is abelian this theorem is almost self-evident. If such a group is metabelian each of its commutators is commutative with all of the operators of the group. If it is not abelian, the commutators formed by an operator in the commutator subgroup and any operator which is not commutative with it will have the required property. As every non-abelian

\* Paris Comptes Rendus, vol. 128 (1889), p. 229.

† W. B. FITE, These Transactions, vol. 3 (1902), p. 334.

‡ Bulletin of the American Mathematical Society, vol. 4 (1898), p. 137.

solvable group must involve a non-abelian group whose commutator subgroup is abelian, it results that every solvable group must involve a commutator which satisfies the condition in question.

It remains to prove that every insolvable group has a commutator, besides the identity, which is commutative with at least one of its elements. If there were an insolvable group which did not have this property, there would be such a group of smallest order. Each subgroup of this group would therefore be abelian, otherwise such a subgroup would contain a commutator which would satisfy the condition in question. As every insolvable group is known to contain at least one non-abelian subgroup,\* we arrive at a contradiction by assuming that an insolvable group exists which does not contain a commutator besides the identity, which is commutative with at least one of its elements. This completes a proof of the theorem: *Every possible non-abelian group of finite order contains at least one commutator besides the identity which is commutative with at least one of the elements of the commutator.*

If both of the elements of a commutator are commutative with this commutator, the metabelian group generated by these two elements has a cyclic commutator subgroup, and this commutator subgroup is generated by the commutator of these two elements. It is known that if a commutator is commutative with one of its elements, the  $\alpha$ th power of this commutator is the commutator of the  $\alpha$ th power of this element and the other element of the given commutator.† Hence it results directly that the group generated by the commutator of these two elements is the commutator subgroup of the group generated by the elements. As an illustration of this elementary theorem, we may observe that if  $G'$  is an abelian group having two invariants  $(m_1, m_2)$  the representation group of  $G'$  has a cyclic commutator subgroup whose order is the highest common factor of the two numbers  $m_1$  and  $m_2$ . The order of this  $G$  is therefore the product of  $m_1 m_2$  and this highest common factor.

The number of the distinct commutators in the representation group of a group  $G'$  of order  $g'$  is evidently always less than  $g'^2$ , since a commutator is not affected if one or both of its elements are multiplied by operators which are commutative with these elements. Hence a commutator is not changed if either one of its elements is replaced by any other element of  $G$  which is found in the same co-set as the given element, with respect to  $M$ . This is clearly a special case of the elementary theorem that *the number of the distinct commutators of a group is always less than the square of the order of its central quotient group*. Although this theorem can easily be generalized, this special case is sufficient for our object in view in the next section, viz., to establish an infinite system

\* These Transactions, vol. 4 (1903), p. 398.

† Bulletin of the American Mathematical Society, vol. 4 (1898), p. 137.

of groups whose commutator subgroups involve operators which are not commutators.

To exhibit some of the applications of the elementary theorems of this section we may consider the representation group of the icosahedral group. As each of the operators of this group is transformed into its inverse by an operator of order 2 contained in the group, it results that every group which has the icosahedral group as a central quotient group must be such that each of its co-sets which corresponds to an operator of order 3 in the icosahedral group must involve at least one commutator of order 3, while each of those which correspond to operators of order 5 must involve at least one commutator of this order. Since each of the operators of order 2 in the icosahedral group is transformed into itself multiplied by an operator of order 2, it results that the co-sets which correspond to operators of order 2 in the given isomorphisms must involve commutators which are transformed into their inverses, and hence their orders must divide 4. In particular, the representation group of the icosahedral group is such that it involves operators of orders 4, 3, and 5 in the co-sets which correspond to operators of orders 2, 3, and 5 respectively in this icosahedral group. As a special case we have the result that *the representation group of the icosahedral group is of order 120*.\* This group of order 120 may be distinguished by the facts that it contains only one operator of order 2 and is isomorphic with the icosahedral group.

### § 3. Representation groups of non-cyclic abelian groups.

From the theorems of the preceding section, especially from those of the last three paragraphs, it is very easy to find the order of the representation groups  $G$  of any non-cyclic abelian group  $G'$ . Suppose that the invariants of  $G'$  are  $m_1, m_2, \dots, m_\lambda$ , and that each of these invariants is divisible by all those which follow it. The commutator subgroup  $M$  of  $G$  will clearly contain  $\lambda - 1$  invariants which are equal to  $m_1$ ,  $\lambda - 2$  which are equal to  $m_2$ ,  $\dots$ , and one which is equal to  $m_{\lambda-1}$ . Hence the order of  $M$  is given by the formula

$$m_1^{\lambda-1} m_2^{\lambda-2} \dots m_{\lambda-1},$$

and the order of  $G$  is

$$m_1^\lambda m_2^{\lambda-1} \dots m_{\lambda-1}^2 m_\lambda.^\dagger$$

The number of the invariants of  $M$  is therefore  $\frac{1}{2}\lambda(\lambda - 1)$ , if we assume that these invariants have been so chosen that they can be arranged linearly so that each of them is a divisor of all those which follow it. In what follows we shall always assume that the invariants of an abelian group have been selected in this manner, unless the contrary is explicitly stated.

\* Quarterly Journal of Mathematics, vol. 41 (1910), p. 170.

† I. SCHUR, Crelle's Journal, vol. 132 (1907), p. 113.

We proceed to determine some properties of representation groups of a non-cyclic abelian group. We shall especially study the representation group which is characterized by the fact that a set of independent generators of  $G'$  may be so chosen that to each one of these generators there corresponds at least one operator of the same order in  $G$ . Such a representation group will be called the *principal representation group* of the abelian group  $G'$ . It follows directly from the general theory of isomorphisms that there is only one such group.\* For instance, the principal representation group of the four-group is the dihedral group of order 8, and the principal representation group of every other non-cyclic group of order  $p^2$  is the non-abelian group of order  $p^3$  which involves no operator of order  $p^2$ .

Every metabelian group whose group of inner isomorphisms is of odd order is conformal with an abelian group;† that is, a  $(1, 1)$  correspondence can be established between the operators of such a metabelian group and those of an abelian group so that two corresponding operators have always the same order. In particular, every metabelian group of odd order is conformal with some abelian group. The fact that *every representation group of any abelian group of odd order is conformal with some abelian group* is evidently a special case of this theorem. The orders of the operators of such a representation group are therefore completely determined by the invariants of the conformal abelian group.

If  $G'$  is an abelian group of order  $p^m$ ,  $p$  being any odd prime number, and if the invariants of  $G'$  are  $p^{a_1}, p^{a_2}, \dots, p^{a_\lambda}$ , then the principal representation group of  $G'$  is conformal with the abelian group which has  $\lambda$  invariants each of which is equal to  $p^{a_1}$ ,  $\lambda - 1$  each equal to  $p^{a_2}$ ,  $\dots$ , one equal to  $p^{a_\lambda}$ . The total number of the invariants of this abelian group is therefore equal to  $\frac{1}{2}\lambda(\lambda + 1)$ . This is the largest number of invariants that an abelian group which is conformal with a representation group of  $G'$  can have. It is however possible that more than one of the representation groups are conformal with abelian groups having this number of invariants. The smallest number of invariants that an abelian group which is conformal with a representation group of  $G'$  can have is evidently  $\frac{1}{2}\lambda(\lambda + 1) - \lambda + 1$ . When  $G'$  is the non-cyclic group of order  $p^2$ ,  $p$  being odd, this number is 2, as it evidently should be according to this formula.

When  $G'$  is the abelian group of order  $2^m$  and of type  $(1, 1, \dots)$ , the principal representation group of  $G'$  contains evidently exactly

$$-1 + (m + 1) \cdot 2^{\frac{1}{2}m(m-1)}$$

\* Bulletin of the American Mathematical Society, vol. 3 (1897), p. 218.

† Bulletin of the American Mathematical Society, vol. 2 (1896), p. 140; vol. 6 (1900), p. 337.

operators of order 2. A necessary and sufficient condition that this representation group is conformal with an abelian group is that  $m + 1$  is a power of 2. The representation groups of an abelian group of order  $2^m$  are therefore sometimes, but not always, conformal with abelian groups. It may be observed that when a set of independent generators of the abelian group  $G'$  of order  $2^m$  and of type  $(1, 1, 1, \dots)$  has been so chosen that each of these generators corresponds to an operator of order 2 in the principal representation group of  $G'$ , then every other operator of order 2 in  $G'$  will correspond to operators of order 4 in this representation group. It is clearly always possible to find at least one representation group of this abelian group such that all of its operators, besides those in the commutator subgroup, are of order 4. The quaternion group is the simplest illustrative example of these representation groups.

The maximal order of an operator in the representation group of an abelian group  $G'$  is evidently equal to the product of the orders of the largest operator in  $M$  and the largest operator of  $G'$ . Moreover, a representation group of  $G'$  can always be constructed so that to each one of a set of independent generators of  $G'$  there corresponds an operator whose order is equal to the order of this generator multiplied by the order of an arbitrary operator in  $M$ . In fact, each of the operators which correspond to a set of independent generators of  $G'$  can be so selected as to generate an arbitrary operator of  $M$ . As a special case of this we have the theorem: *The principal representation group of  $G'$  contains no operator whose order exceeds that of the largest operator in  $G'$  when the order of  $G'$  is odd. When the order of  $G'$  is even, the order of the largest operator in its principal representation group cannot exceed twice that of the largest operator in  $G'$ .* This maximum order is attained only when the Sylow subgroup of order  $2^m$  in  $G'$  has at least two equal largest invariants.

As a very special but interesting result from what precedes we may note the elementary fact, stated in the Introduction, that every possible non-cyclic abelian group has more than one representation group and that each of these representation groups is metabelian. In fact, such a non-cyclic group has a non-cyclic Sylow subgroup, and the principal representation group of this subgroup does not involve any operator whose order is equal to that of the largest operator which occurs in some one of the representation groups, unless the invariants of this Sylow subgroup are all equal to 2. In this special case we have observed that the number of distinct representation groups is at least equal to 2. A number of theorems relating to the possible number of different representation groups of a given abstract group were established by I. SCHUR in the memoirs to which we referred in the Introduction.

The representation groups of abelian groups furnish many simple illustrations of groups whose commutator subgroups involve operators which are not

commutators. W. B. FITE gave one example of such a group.\* A very elementary infinite system of such groups may be established by observing that the representation groups of the abelian group of order  $p^m$  and of type  $(1, 1, 1, \dots)$  have a commutator subgroup of order  $p^{1m(m-1)}$  while it has been observed that the number of their distinct commutators is less than  $p^{2m}$ . That is, *the commutator subgroup of a representation group of the abelian group of order  $p^m$  and of type  $(1, 1, 1, \dots)$  contains operators which are not commutators whenever  $m > 4$ .* As this theorem is true for every value of the prime number  $p$  and every value of  $m > 4$ , it establishes the existence of a doubly infinite system of such groups. It is also very easy to establish such systems in the case when the abelian group is not of type  $(1, 1, 1, \dots)$ .

#### § 4. Representation groups of non-abelian groups of order $p^m$ .

If  $G'$  is a non-abelian group of order  $p^m$ ,  $p$  being a prime number, it contains at least one series of invariant subgroups  $H_1, H_2, \dots, H_{m-1}$  of order  $p, p^2, \dots, p^{m-1}$  respectively, such that each of them is contained in all those which follow it. If one element of a commutator is in  $H_\alpha$ ,  $\alpha = 1, 2, \dots, m-1$ , the commutator is found in  $H_{\alpha-1}$ , and if both of these elements are in  $H_\alpha$  the commutator is in  $H_{\alpha-2}$ , and the same commutator results from an element in  $H_{\alpha-1}$  and an element in  $H_\alpha$ . In particular, all the possible commutators of  $G'$  must be contained in  $H_{m-2}$ , as is well known.

Suppose that  $G'$  is the central quotient group of a group  $K$ . The commutators of  $K$  which have one element in the subgroup corresponding to  $H_1$  must have orders which divide  $p$ , according to § 2. All the operators of order  $p$  in the subgroup corresponding to the identity of  $K$  clearly generate a subgroup which involves no operator of order  $p^2$ . Similarly, the commutators of  $K$  which have one element in the subgroup corresponding to  $H_2$  must have orders which divide  $p^2$ , and all the operators whose orders divide  $p^2$ , in the subgroup of  $K$  which corresponds to  $H_1$ , generate a subgroup which involves no operator of order  $p^3$ .

We proceed to prove, by complete induction, that all the commutators of  $K$ , which have one element in the subgroup of  $K$  which corresponds to  $H_\alpha$ , have orders which divide  $p^\alpha$ , and all the operators of  $K$  whose orders divide  $p^\alpha$  and which correspond to  $H_{\alpha-1}$  generate a group involving no operator of order  $p^{\alpha+1}$ . In fact, if  $s_\alpha$  is any operator of  $K$  contained in the subgroup corresponding to  $H_\alpha$  and if  $t$  is any other operator of  $K$ , we have the equation:

$$(t^{-1} s_\alpha t)^p = t^{-1} s_\alpha^p t = (C_\alpha s_\alpha)^p = C_\alpha s_\alpha C_\alpha s_\alpha^{-1} \cdot s_\alpha^2 C_\alpha s_\alpha^{-2} \cdot \dots \cdot s_\alpha^{p-1} C_\alpha s_\alpha^{1-p} \cdot s_\alpha^p.$$

\* These Transactions, vol. 3 (1902), p. 340.

Hence

$$C_{a-1} s_a^p = C_a C_{a-1}^{(1)} C_a C_{a-1}^{(2)} C_a \cdots C_{a-1}^{(p-1)} C_a \cdot s_a^p$$

$$C_{a-1} = C_a C_{a-1}^{(1)} C_a^{-1} \cdot C_a^2 C_{a-1}^{(2)} C_a^{-2} \cdots C_a^{p-1} C_{a-1}^{(p-1)} C_a^{1-p} \cdot C_a^p.$$

All the operators between periods, except possibly the last, in this final equation are commutators which correspond to  $H_{a-2}$ . Hence we may assume that they together with  $C_{a-1}$  cannot generate any operator whose order exceeds  $p^{a-1}$ . This proves that the order of  $C_a$  cannot exceed  $p^a$ .

If  $t_1, t_2$  are two operators of  $K$  which correspond to  $H_{a-1}$  and whose orders divide  $p^a$ , the order of their product must also divide  $p^a$  as may be seen from the following equations

$$(t_1 t_2)^p = t_1 t_2 t_1 t_2^{-1} t_2^2 t_1 t_2^{-2} \cdots t_2^{p-1} t_1 t_2^{1-p} \cdot t_2^p$$

$$= t_1 C_{a-2}^{(1)} t_1 C_{a-2}^{(2)} t_1 \cdots C_{a-2}^{(p-1)} t_1 \cdot t_2^p$$

$$= C_{a-2} t_1^p t_2^p.$$

As each of these three operators has an order which divides  $p^{a-1}$ , and as it corresponds to  $H_{a-2}$ , it has been proved, by complete induction, that *all the commutators of  $K$  involving one element which corresponds to  $H_a$  must have orders which divide  $p^a$* . As a special case we have the theorem: *The order of every representation group of a group of order  $p^m$ ,  $p$  being any prime number, is of the form  $p^m$ , and the orders of all its commutators divide  $p^{m-1}$ .*

The preceding theorem is useful to find an upper limit for the order of a representation group of a group of order  $p^m$ . In particular, this order is always finite since both the orders of the commutators and the number of the distinct commutators are finite whenever  $m$  is finite. For the sake of illustration we shall consider the representation groups of the non-abelian group of order  $p^3$ . Not more than two independent generators of  $M$  can arise from commutators involving elements which correspond to the invariant operators of this abelian group, and not more than one additional independent generator of  $M$  can arise from the commutators whose elements correspond to the non-invariant operators of this non-abelian group of order  $p^3$ . As the orders of all of these independent generators divide  $p$ , it results that the order of a representation group of a non-abelian group of order  $p^3$  cannot exceed  $p^6$ . It is evident that the non-abelian group of order  $p^3$  which is conformal with the abelian group of type  $(1, 1, 1)$  has a representation group of order  $p^6$ , for all odd values of  $p$ ; while the non-abelian group which is conformal with the abelian group of type  $(2, 1)$  is its own representation group for all odd values of  $p$ .\*

In general, it is evident from the theorem stated above that the subgroup

\* These Transactions, vol. 10 (1909), p. 395.



$M$ , which is called the *multiplier* of  $G'$ , can not have more than  $m - 1$  independent generators arising from commutators which have an element corresponding to  $H_1$  in  $G'$ , and that the orders of all these independent generators divide  $p$ . Similarly, there cannot be more than  $m - 2$  additional generators in  $m$ , arising from commutators involving elements which correspond to  $H_2$ , and the orders of each of these divides  $p^2$ , etc. As the orders of these independent generators cannot always have this upper limit, since  $G'$  is non-abelian, it results directly that the order of  $M$  is always less than  $p^k$ , where

$$k = m - 1 + 2(m - 2) + 3(m - 3) \cdots + m - 1.$$

In the special case considered in the preceding paragraph the order of  $M$  has its maximal value according to this formula, but it is evident that  $M$  will generally have a much lower order.

In conclusion it seems desirable to direct attention to a very elementary general theorem which is illustrated by the representation groups of the special categories of groups considered above; viz., the theorem that *if a group  $G'$  has more than one representation group all of these representation groups have the same commutator subgroup*. In fact, if they did not have the same commutator subgroup we could establish an isomorphism between them with respect to their common quotient group  $G'$  and thus obtain a larger representation group of  $G'$ . As special cases of this theorem we have the results that in all the representation groups of  $G'$  the multipliers are simply isomorphic, and if a group is generated by its commutators it has only one representation group. Both of these theorems were explicitly stated by I. Schur in the memoirs to which we referred in the Introduction.