

ON THE GROUPS WHICH HAVE THE SAME GROUP OF ISOMORPHISMS*

BY

G. A. MILLER

The main object of this paper is the determination of all the possible groups whose group of isomorphisms is either the symmetric group of order 6 or the symmetric group of order 24. We shall also determine the infinite system of groups whose group of cogredient isomorphisms is the former of these two symmetric groups. It will be proved that this system includes one and only one group (which is not the direct product of an abelian and a non-abelian group) for every power of 2.

It is well known that every simple isomorphism of a group G with itself may be obtained by transforming G by means of operators that transform it into itself.† In what follows we shall generally employ this method of making G simply isomorphic with itself.

In a few cases it will be convenient to employ two special methods, which we proceed to explain.

The first of these two methods may be employed when G contains a subgroup H' which is composed entirely of operators which are selfconjugate under G and which is also simply isomorphic to a quotient group of G with respect to a selfconjugate subgroup which includes H' . In this case we may evidently multiply all of the operators of each one of the various divisions of G with respect to this quotient group by the corresponding operator of H' and thus obtain a simple isomorphism of G with itself.—To illustrate this method we may employ the direct product G_{12} of the symmetric group of order 6 and an operator s_1 of order two. If we multiply each of the six operators of G_{12} which are not contained in its cyclical subgroup of order 6 by s_1 we obtain a simple isomorphism of G_{12} with itself. It is evident that this isomorphism corresponds to the selfconjugate operator of order two in the group of isomorphisms of G_{12} .‡—It is important to observe that any operator t_1 of the group of isomorphisms of G which is obtained in this manner is selfconjugate under this group of isomorphisms whenever H' is composed of characteristic operators

* Presented to the Society December 23, 1899. Received for publication January 18, 1900.

† FROBENIUS: Berliner Sitzungsberichte, 1895, p. 184.

‡ The group of isomorphisms of G_{12} is simply isomorphic to G_{12} .

of G and each of the divisions of G which is multiplied by the same operator of H' corresponds to itself in every simple isomorphism of G with itself. To prove this we let s_a and t_2 represent any operator of G and its group of isomorphisms respectively. If $t_2^{-1}s_a t_2 = s_b$ and $t_1^{-1}s_b t_1 = h_1 s_b$ then $(t_2^{-1}t_1 t_2)^{-1}s_b t_2^{-1}t_1 t_2 = h_1 s_b$; i. e., $t_2^{-1}t_1 t_2 = t_1$.*

The second of these special methods of making G simply isomorphic with itself can be employed when G is an abelian group which contains operators whose order exceeds two. In this case we may write after each operator of G its a power, where a is any integer prime to the order of G †, and thus obtain a simple isomorphism of G with itself. It is easy to prove that such an isomorphism of G with itself must correspond to a selfconjugate operator t_3 in its group of isomorphisms. For if $t_2^{-1}s_a t_2 = s_b$ and $t_3^{-1}s_b t_3 = s_b^a$ then

$$(t_2 t_3 t_2^{-1})^{-1} s_a t_2 t_3 t_2^{-1} = s_a^a,$$

i. e., $t_2 t_3 t_2^{-1} = t_3$. Hence we have

THEOREM I. *If an abelian group contains operators whose order exceeds two its group of isomorphisms contains selfconjugate operators.‡*

We proceed to give a few other elementary theorems (II... VI) in the form in which we shall need them in what follows. Theorem V will not be directly employed but it may be useful for the purpose of arriving at some of the following results by different methods.

THEOREM II. *If a group G is generated by two characteristic subgroups which have only identity in common its group of isomorphisms is the direct product of the groups of isomorphisms of these two characteristic subgroups.*

Any isomorphism of G with itself is completely determined by the operators which correspond to any set of generators of G . Hence the isomorphisms of the given characteristic subgroups with themselves will completely determine the isomorphism of G with itself. Since G is the direct product of these subgroups their isomorphisms are entirely independent of each other and hence the group of isomorphisms of G is the direct product of their groups of isomorphisms.

COROLLARY. *If the order of an abelian group is $p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots (p_1, p_2, p_3, \dots$ being different prime numbers) its group of isomorphisms is the direct product of the groups of isomorphisms of its subgroups of orders $p_1^{a_1}, p_2^{a_2}, p_3^{a_3}, \dots$.*

* The operators of the group of isomorphisms of G may be supposed to transform G into itself and to be fully determined by the way in which they transform the operators of G . Cf. BURNSIDE, *Theory of Groups of a Finite Order*, 1897, p. 226; also MILLER, *Bulletin of the American Mathematical Society*, vol. 5, 1899, p. 245.

† The order of G diminished by unity is evidently a suitable value for a .

‡ It is well known that the group of isomorphisms of a group which does not contain any operator whose order exceeds 2 is simple except in case the order of the group is 4.

THEOREM III. *The group of isomorphisms of an abelian group A is abelian when A is cyclical and it is non-abelian when A is non-cyclical.*

When A is cyclical its group of isomorphisms is simply isomorphic to the operators which transform a generator of A into its various powers which are prime to its order. Hence this group of isomorphisms is abelian. When A is non-cyclical it contains a non-cyclical group P whose order is a power of a single prime number. Since P is generated by its operators of highest order* its group of isomorphisms is simply isomorphic to a transitive substitution group whose degree is equal to the number of these operators of highest order. As the order of this transitive group clearly exceeds its degree it is non-abelian. Hence the group of isomorphisms of A must also be non-abelian.

THEOREM IV. *The necessary and sufficient condition that a cyclical group of order n is the group of isomorphisms of some group is that n is of the form $p^a(p-1)$, p being an odd prime number.*

The group of isomorphisms of a non-abelian group cannot be cyclical since its group of cogredient isomorphisms cannot be cyclical.† Hence this theorem follows directly from the preceding theorem and the well known forms of numbers which have primitive roots. It may be observed that a cyclical group of an odd order cannot be a group of isomorphisms and that there is no group which has a cyclical group of order 8, 14, 24, 26, ... as a group of isomorphisms.

THEOREM V. *If the order of an abelian group A is divisible by an odd prime number p its group of isomorphisms contains an operator of order $p-1$.*

Let p^a be the highest power of p that divides the order of A . It follows from theorem II that we may confine our attention to the group P of order p^a which is contained in A . Since P is abelian a simple isomorphism of P with itself may be obtained by writing after each one of its operators the a power of this operator, a being any number prime to p . If p^b is the highest order of an operator of P and if a is so chosen that it belongs to exponent $p-1$ modulo p^b , the given simple isomorphism of P with itself will clearly correspond to an operator of order $p-1$ in its group of isomorphisms.

THEOREM VI. *If an operator A_1 of the group of cogredient isomorphisms G_1 of the group G is of order p^a (p being any prime number) and if some operator of G_1 transforms A_1 into its k power, then at least one operator of order p^a corresponds to A_1 in the isomorphism between G and G_1 whenever*

* It is easy to see that any abelian group is generated by its operators of highest order and that its group of isomorphisms can be represented as a transitive substitution group whose degree is equal to the number of these operators of highest order.

† Comptes Rendus, 1899, vol. 128, p. 229; cf. FITE, Bulletin of the American Mathematical Society, 1899, vol. 6, p. 11.

$k \not\equiv 1 \pmod{p}$; when $k \equiv 1 \pmod{p^\gamma}$ but $\not\equiv 1 \pmod{p^{\gamma+1}}$ then at least one operator of order $p^{\alpha+\gamma'}$ ($\gamma' \equiv \gamma$) corresponds to A_1 in the given isomorphism between G and G_1 .

Let H be the subgroup of G which corresponds to identity in the given isomorphism between G and G_1 and let p' be the highest power of p which divides the order of H . To the subgroup of G_1 which is generated by $A_1^{p'^{\alpha-1}}$ there corresponds an abelian group which includes a group P of order p^{l+1} . Let S be an operator of P of the lowest order which corresponds to $A_1^{p'^{\alpha-1}}$. The operator S may evidently be used as one of the independent generators of P . Since some operators of G_1 transform $A_1^{p'^{\alpha-1}}$ into its k th power the corresponding operators of G must transform S into its k power multiplied by some operator of H . The p power of this transform must equal S^p since each of the operators of H is commutative to every operator of G . As this is clearly impossible unless $S^p = 1$ the first part of the theorem is proved.*

To prove the second part we observe that an operator A_2 (contained in G_1) of order $p^{\gamma+1}$ is transformed into its $p^\gamma + 1$ power by some operators of G_1 . Any one of the corresponding operators of G must therefore be transformed into its $p^\gamma + 1$ power multiplied by some operator of H . As before we may select one of these operators S_1 of lowest order as one of the independent generators of (P_1) the subgroup of order $p^{l+\gamma+1}$ which corresponds to the group generated by A_2 . The $p^{\gamma+1}$ power of the given transform of S_1 must equal $S_1^{p^{\gamma+1}}$; i. e., the $p^\gamma + 1$ power of S_1 must have the same $p^{\gamma+1}$ power as S_1 has, since S_1 is an independent generator of P_1 . From this it follows that the order of $S_1^{p^\gamma}$ cannot exceed $p^{\gamma+1}$ and hence the order of S_1 cannot exceed $p^{2\gamma+1}$. This completes the proof of the theorem.

By means of these theorems it is easy to determine all the groups whose group of isomorphisms is the symmetric group of order six (G_6). If such a group K is abelian it cannot contain any operator whose order exceeds two, according to theorem I. Hence the four-group is the only abelian group whose group of isomorphisms is G_6 . If K is non-abelian its group of cogredient isomorphisms must be G_6 since a group of cogredient isomorphisms cannot be cyclical.† We shall therefore first consider the more general problem to determine all the possible groups whose group of cogredient isomorphisms is G_6 . This problem is of considerable interest in itself, especially since we arrive at a very simple infinite system of groups.

Let K' be any group whose group of cogredient isomorphisms is G_6 and let H represent the subgroup of K' which corresponds to identity in the isomorphism between K' and G_6 . The order of each operator of K' which corresponds to an operator of order three in G_6 must be divisible by three. From theorem

* Cf. HÖLDER, *Mathematische Annalen*, 1895, vol. 46, p. 351.

† *Comptes Rendus*, 1889, vol. 128, p. 229.

VI we observe that at least two of these operators (s, s^2) of K' are of order three. Let t be an operator of K' which corresponds to an operator of order two in G_6 and suppose that t is so chosen that its order 2^a is the smallest possible power of 2. The operators t and s generate a selfconjugate subgroup of K' .* We may suppose that this selfconjugate subgroup contains only one subgroup of order 3, since the number of operators of order 3 which correspond to an operator of order 3 in G_6 is 3^8 and hence at least one of the 3^8 subgroups which they generate must be transformed into itself by t .

Let 2^l be the highest power of 2 which divides the order of H and let A' represent the subgroup of order 2^l which is contained in H . Then A' and t generate an abelian group of order 2^{l+1} whose independent generators may be so chosen as to include t . Hence t^2 may be used as one of the independent generators of H and K' is the direct product of the group generated by s and t , and of the subgroup of H which is generated by all of its independent generators except t^2 .

The operators s and t^2 generate a cyclical group whose generators are transformed by t either into their $2^{a-1} + 1$ or into their $2^a + 1$ power. One of the two numbers $2^{a-1} + 1, 2^a + 1$ is congruent to 0 mod. 3 while the other is congruent to 2 mod. 3, t must, of course, transform the given generators into the power which is congruent to 2 mod. 3. As there is only one such group for every value of a we have proved

THEOREM VII. *If a group has the symmetric group of order six for its group of cogredient isomorphisms and is not the direct product of two subgroups its order is $3 \cdot 2^a$ and it contains three cyclical subgroups of order 2^a and only one subgroup of order 3. For every value of $a > 0$ there is one and only one such group. Every other group which has the symmetric group of order six for its group of cogredient isomorphisms is the direct product of one of the given groups of order $3 \cdot 2^a$ and some abelian group.*

It is now easy to see that G_6 is the only non-abelian group whose group of isomorphisms is G_6 . For if such a group K were the direct product of two subgroups one of these subgroups would have to be abelian while the other would have G_6 for its group of cogredient isomorphisms. Hence we may assume that the latter group would be one of the given groups of order $3 \cdot 2^a$. If a exceeds 1 such a group contains a characteristic operator of order 2 and a subgroup which includes this operator of order 2 and whose order is one-half the order of the group. Hence the group of isomorphisms of such a group must contain a selfconjugate operator of order 2 whenever $a > 1$. The group K must

* The general theorem may be stated as follows: If a subgroup contains at least one operator which corresponds to each operator of the group of cogredient isomorphisms of the entire group this subgroup is selfconjugate.

therefore be either G_6 or the direct product of G_6 and some abelian group. We have already seen that this abelian group could not be of order 2 and it follows directly from theorem II that it could not be of a larger order. Hence G_6 is the only non-abelian group whose group of isomorphism is G_6 .

Having determined the groups whose group of isomorphisms is the symmetric group of order six we proceed to consider all the possible groups whose group of isomorphisms is the symmetric group of order 24. We shall denote this group by G_{24} . It follows almost directly from theorem I that such a group L cannot be abelian. If it is non-abelian its group of cogredient isomorphisms must be the four-group, the alternating group of order 12, or G_{24} itself. We shall consider these three cases in order.

If the group of cogredient isomorphisms of L is the four-group the self-conjugate operators of L constitute a characteristic subgroup with respect to which L is isomorphic to the four-group. Any operator which transforms L into a contragredient isomorphism with itself must permute some of the divisions that correspond to the three operators of order two in the given quotient group. Hence L cannot admit any except cogredient isomorphisms with itself in which each of these divisions corresponds to itself. In particular each of the selfconjugate operators of L must correspond to itself in all such isomorphisms. From this it is not difficult to see that the order of L must be 8 and it is well known that the quaternion group is the only group of order 8 whose group of isomorphisms is G_{24} . *The quaternion group is therefore the only group which has the four-group for its group of cogredient isomorphisms and also G_{24} for its group of isomorphisms.*

There are three well-known groups which have the alternating group of order 12 for their group of cogredient isomorphisms and G_{24} for their group of isomorphisms; viz., the alternating group of order 12, the direct product of this alternating group and an operator of order two, and the group of order 24 which has no subgroup of order 12.†* We proceed to prove that *there is no other group which has this property.* Since the groups of orders 12 and 24 are well known we may confine our attention to the groups of higher orders.

Since the group of cogredient isomorphisms of L includes all its operators of order 3, L cannot contain any selfconjugate operator of this order. Hence its order must be $2^a \cdot 3$. It remains to prove $a \equiv 3$. If $a > 3$ the subgroup of order 2^a which is included in L cannot contain three cyclical subgroups of order 2^{a-1} . This is evident when the subgroup of order 2^a is abelian. If it is non-abelian suppose that s_1 and s_2 ($s_1^2 = s_2^2$) generate two subgroups of order 2^{a-1} . From the conditions that $s_1^2 = s_2^2$ and that s_1, s_2 are not commutative it follows that $s_2^{-1}s_1s_2 = s_1^{2^{a-2}+1}$ and $(s_1s_2)^2 = s_1s_2s_2^{-1}s_1s_2 = s_1^{2^{a-2}+4}$. Hence the order of

* Quarterly Journal of Mathematics, 1898, vol. 30, p. 258.

† Ibid., 1896, vol. 28, p. 274.

$s_1 s_2$ cannot exceed 2^{a-2} when $a > 3$. Since the squares of all the operators of an abelian group of order 2^{a-1} constitute a subgroup of order $2^{a-\beta-1}$, where β is the number of its independent generators, and since each of the three conjugate subgroups of order 2^{a-1} which are contained in L has at least two independent generators, the squares of all the operators of L must constitute a subgroup whose order cannot exceed 2^{a-3} .

It is now easy to see that L admits contragredient isomorphisms with itself which do not permute any of its divisions which correspond to the four-group in its group of cogredient isomorphisms whenever $a > 3$. Hence the three given groups are the only groups whose group of isomorphisms is G_{24} and whose group of cogredient isomorphisms is the alternating group of order 12.

It remains only to determine the groups which have G_{24} both for their group of isomorphisms and also for their group of cogredient isomorphisms. Such a group L must be isomorphic to G_{24} with respect to its selfconjugate operators. From theorems VI and II it follows that it must contain operators of order 3 and that its order cannot be divisible by 9. If L were to contain a selfconjugate operator of order 2 it would have a contragredient isomorphism with itself since G_{24} has a selfconjugate subgroup of order 12. Hence G_{24} is the only group whose group of isomorphisms and cogredient isomorphisms is G_{24} .

We have now examined all the possible cases and found that *there are just five groups whose group of isomorphisms is G_{24}* ; three of these are of order 24 one is of order 12, and one is of order 8.

CORNELL UNIVERSITY,
December, 1899.
