

GROUPS IN WHICH A LARGE NUMBER OF OPERATORS MAY CORRESPOND TO THEIR INVERSES*

BY

W. A. MANNING

An abelian group may be defined by the property that, in an automorphism of the group, more than three fourths its operators may be placed in a one to one correspondence with their inverses.† It may be of interest to know the groups possessing the property that five eighths or more of the operators may be made to correspond to their inverses. The principal object of this paper, however, is to establish the following elementary theorem (I) and to illustrate the use that may be made of it in certain problems.

THEOREM I. *A group that has two invariant subgroups with nothing in common but the identity can be set up as a multiple isomorphism between two groups of lower order.*

Let a group (G) of order $k_1 k_2 x$ have the two invariant subgroups K_1 and K_2 of order k_1 and k_2 respectively. If K_1 and K_2 have only the identity in common, every operator of K_1 is commutative with every operator of K_2 . It may be assumed that G is not merely the direct product of K_1 and K_2 . Let $1, r_2, r_3, \dots$, be the operators of K_1 and $1, s_2, s_3, \dots$, those of K_2 . Now

$$\begin{array}{ll}
 (1_a) & (1_b) \\
 G = K_2 + r_2 K_2 + \dots + r_{k_1} K_2 & G/K_2 = K_1 \\
 + t_2 K_2 + t_2 r_2 K_2 + \dots + t_2 r_{k_1} K_2 & + t'_2 K_1 \\
 + t_3 K_2 + t_3 r_2 K_2 + \dots + t_3 r_{k_1} K_2 & + t'_3 K_1 \\
 + \dots & + \dots \\
 + t_x K_2 + t_x r_2 K_2 + \dots + t_x r_{k_1} K_2, & + t'_x K_1,
 \end{array}$$

* Presented to the Society (San Francisco) September 30, 1905. Received for publication November 19, 1905.

† MILLER, *Annals of Mathematics*, ser. 2, vol. 7 (1906), p. 55.

$$\begin{array}{ll}
 (2_a) & (2_b) \\
 G = K_1 + s_2 K_1 + \dots + s_{k_2} K_1 & G/K_1 = K_2 \\
 + t_2 K_1 + t_2 s_2 K_1 + \dots + t_2 s_{k_2} K_1 & + t''_2 K_2 \\
 + t_3 K_1 + t_3 s_2 K_1 + \dots + t_3 s_{k_2} K_1 & + t''_3 K_2 \\
 + \dots & + \dots \\
 + t_x K_1 + t_x s_2 K_1 + \dots + t_x s_{k_2} K_1, & + t''_x K_2.
 \end{array}$$

The operators t'_i and t''_i ($i = 2, 3, \dots, x$) correspond to $t_i K_2$ and $t_i K_1$ in (1_a) and (1_b) respectively. Let $\{K_1, K_2\}$ be called H . It is clear that $(G/K_2)/K_1 = (G/K_1)/K_2 = G/H$. We may write G/K_2 and G/K_1 as substitution groups on different sets of letters and by multiplying corresponding divisions in the order given in (1_b) and (2_b) obtain

$$G' = H + t'_2 t''_2 H + t'_3 t''_3 H + \dots + t'_x t''_x H.$$

That G' is simply isomorphic to G remains to be proved. The order of G' is clearly $k_1 k_2 a^x$. If in G , $t_i r_\alpha s_\lambda t_j r_\beta s_\mu = t_k r_\gamma s_\nu$, from (1_a) and (1_b) $t'_i r_\alpha t'_j r_\beta = t'_k r_\gamma$ and from (2_a) and (2_b) $t''_i s_\lambda t''_j s_\mu = t''_k s_\nu$. Hence in G' , $(t'_i t''_i r_\alpha s_\lambda)(t'_j t''_j r_\beta s_\mu) = t'_i r_\alpha t'_j r_\beta t''_i s_\lambda t''_j s_\mu = t'_k r_\gamma t''_k s_\nu = t'_k t''_k r_\gamma s_\nu$ and the truth of our theorem is now evident.

COROLLARY I. If an invariant subgroup of G has nothing but the identity in common with the commutator subgroup of G , G is a multiple isomorphism between an abelian and a non-abelian group.

COROLLARY II. Groups whose invariant operators are not all powers of a single one among them can be set up by establishing isomorphisms between groups of lower order.

COROLLARY III. All metabelian* groups of order p^m can be constructed by setting up isomorphisms between metabelian groups of lower order in which the groups of invariant operators are cyclic.

THEOREM II. Given a group G in which a certain fractional part of the operators may be made to correspond to their inverses, we can take any invariant subgroup H for which G/H is abelian, set up an isomorphism with any abelian group having the same quotient group, and, by multiplying corresponding divisions, construct a new group in which the same proportion of the operators may correspond to their inverses.

Let G have an invariant subgroup H of order h and index x , and let G/H be abelian. Also let A be an abelian group with a subgroup B of order b and index x , such that A/B is simply isomorphic to G/H . We may write G and

* FITE, Transactions of the American Mathematical Society, vol. 3 (1902), pp. 331-353.

A as regular groups on different sets of letters, and then set up an intransitive group (G') by taking the direct product of H and B , and of the operators in corresponding divisions of the tails of G and of A . Now if t be an operator which transforms the given fractional part of the operators of G into their inverses, and if t_1 transforms all the operators of A into their inverses, the operators of G' can be arranged in $hx = g$ sets of b each, with one operator of G in each set, so that tt_1 transforms every operator of a set into its inverse whenever the accompanying operator from G goes into its inverse.

Let us assume that exactly $\frac{3}{4}g$ operators of G can be made to correspond to their inverses. Since it may be assumed that G is not abelian a substitution t can be selected from G that corresponds to t^{-1} and is not invariant in G . Let $t_i (i = 1, 2, \dots, \frac{3}{4}g)$ be the totality of operators in G that correspond to their inverses. Form the $\frac{3}{4}g$ products tt_i . At least $\frac{1}{2}g$ of the products tt_i correspond to $(tt_i)^{-1}$, giving $t^{-1}t_i^{-1} = t_i^{-1}t^{-1}$, so that t is commutative with $\frac{1}{2}g$ operators of G , all of which correspond to their inverses. This subgroup (H) in which t is invariant is abelian, since all its operators correspond to their inverses. Next let s be an operator not in H and which corresponds to s^{-1} . Since half the products st_i correspond to their inverses, s is commutative with half the operators of H . Hence H includes a subgroup (F) of order $\frac{1}{4}g$ all of whose operators are invariant in G . The group of cogredient isomorphisms, G/F , is axial. The converse is true. We have

$$G = F + tF + sF + stF.$$

From this we get $s^{-1}ts = tc$, where c , the commutator, is an operator of F ; $s^{-2}ts^2 = tc^2 = t$, so that $c^2 = 1$. Hence $t^{-1}st = sc$, and the commutator subgroup of G is of order 2.

It may be assumed that G is not a direct product of, or multiple isomorphism between, an abelian and a non-abelian group. Let us suppose that the order of F is $2^{m-2}r$, where r is an odd number. Since G/F is axial, the result of taking odd powers of $tF(sF)$ is merely a permutation of the operators in each division. Hence $tF(sF)$ involves operators of order a power of 2. But F is the direct product of two groups, K of order 2^{m-2} , and K' of order r . Then G in turn is the direct product of $\{K, t, s\}$ and K' , contrary to the assumption just made. If a and b are two operators of F , and if $t^2 = a$, $b^2 = a^{-1}$, it follows that $(tb)^2 = 1$, so that $t(s)$ may be assumed to have been so selected that $t^2(s^2)$ is not the square of an operator of F . Then t^2 and s^2 are independent generators of F , or the identity. By virtue of theorem I, corollary I, F has only one operator of order 2, the commutator, and in consequence F is cyclic.*

We may have $G = \{t, s\}$, where $t^{2^{m-1}} = s^{2^{m-1}} = 1$, $t^2 = s^2$, $s^{-1}ts = t^{1+2^{m-3}}$. There is one such group for all values of m greater than 3. When $m = 3$, G

* BURNSIDE, *Theory of Groups*, 1897, p. 75.

is the quaternion or octic group. If $t^{2^{m-1}} = s^2 = 1$, $sts = t^{1+2^{m-2}}$, st is of order 2^{m-1} since $stst = t^2 t^{2^{m-2}}$, and we have the same series of groups as that just given. There remains the hypothesis that $t^2 = s^2 = 1$. F is generated by an operator r of order 2^{m-2} , and $trt = srs = r$, $sts = tr^{2^{m-3}}$. There is one such group whenever m is greater than 3. All other groups in which $\frac{3}{4}g$ operators may correspond to their inverses may be formed by means of theorem II.*

Let us suppose if possible that $\frac{3}{4}g + x$ ($0 < x < \frac{1}{2}g$) operators of G correspond to their inverses. A non-invariant operator t which corresponds to t^{-1} is commutative with at least $\frac{1}{2}g + 2x$ operators of G . In this subgroup H (of order $h = \frac{1}{2}g$), $\frac{2}{3}h + 2x$ operators, perhaps more, correspond to their inverses.

Suppose that just $\frac{3}{4}h$ operators of H correspond to their inverses. These groups H are known. If F_1 is the subgroup of invariant operators of H , and if H_1 is an abelian subgroup of half the order of H , then

$$H = F_1 + t_1 F_1 + s_1 F_1 + s_1 t_1 F_1 \quad \text{and} \quad G = H + sH,$$

where s is any operator of $G - H$ that corresponds to s^{-1} . It is clear that s is not commutative with all the operators of H , for in that event $\frac{3}{4}g$ operators of G would correspond to their inverses. Now s is commutative with just half the operators of G . Hence s is commutative with just half the operators of H , which form a subgroup (K) of H . Can all the operators of F_1 be invariant in G ? To answer this question we note that if one operator in a division of G with respect to F_1 corresponds to its inverse, all the operators of that division do so, since the operators of F_1 all do so. But no integral multiple of $\frac{1}{2}$ is equal to $\frac{3}{4}$ or lies between $\frac{3}{4}$ and $\frac{3}{4}$. Now s is commutative with half the operators of H , and is not commutative with all the operators of H_1 (H_1 includes F_1) so that there is an operator s'_1 in the tail $H - H_1$, commutative with s . The number of operators in the set $H_1 s'_1$ commutative with s is the same as the number of operators in H possessing this property. Hence s is commutative with just half the operators of H_1 . In the same way s is seen to be commutative with just half the operators of F_1 . These operators, invariant in G , form a subgroup F' . If one operator in a division of G with respect to F' corresponds to its inverse all the operators of that division do so. Then we have to see if it is possible for $\frac{1}{6}g$ operators of G to correspond to their inverses. Let a be an operator of F_1 which is not in F' : $sa \neq as$. Of the 8 divisions of $G - H$ with respect to F' , not both the sets in a division of $G - H$ with respect to F_1 can have all operators corresponding to their inverses. For example, if st_1 corresponds to $(st_1)^{-1}$, $st_1 a$ does not correspond to $(st_1 a)^{-1}$. Hence, instead of 11, at most 10 divisions of G taken with respect to F' contain operators which correspond to their inverses.

If H is abelian, all its operators correspond to their inverses since more than half do so, and s is commutative with half the operators of H , so that $\frac{3}{4}g$ oper-

ators of G correspond to their inverses, contrary to hypothesis. Now more than two thirds and less than three fourths of the operators of H correspond to their inverses when this condition is imposed on G , the same is true of a subgroup H' of H , and so on indefinitely, an absurdity when G is of finite order.

Except when $g/h = 2$ and $h/h' = 3$, for some pair of groups in the chain G, H, H', \dots above, the preceding reasoning shows that if the number of operators which correspond to their inverses is just $\frac{2}{3}g$, the subgroup H is of index 3. Neglecting for the moment the exceptional case, we distribute the operators of G in three sets H, uH, vH , where u is an operator that corresponds to u^{-1} . Since u cannot be commutative with all the operators of H without making G abelian, v can correspond to v^{-1} , so that one half the operators of each set uH and vH correspond to their inverses. Half the operators of H are invariant in the entire group. They form a subgroup F , with respect to which the quotient group is the non-abelian group of order 6. Then G has an abelian subgroup of order $\frac{1}{2}g$. We may write

$$G = (F + sF + s^2F) + tF + tsF + ts^2F.$$

We have $t^{-1}st = ssa$, where a is a certain operator of F ; $t^{-2}st^2 = s(sa)^3 = s$, whence $(sa)^3 = 1$; $t^{-1}sat = (sa)^2$. Put $sa = c$. Then $G = \{F, c\} + t\{F, c\}$, and is a $(k, 3)$ isomorphism between an abelian group of order $2k$ and the non-abelian group of order 6.

Let t be commutative with all the operators of a subgroup H of order $\frac{1}{2}g$, and let just two thirds of the operators of H correspond to their inverses. We are at liberty to assume that H is one of the groups determined in the preceding paragraph and that every non-invariant operator which corresponds to its inverse is invariant in a subgroup of order $\frac{1}{2}g$. Consider an operator u of H that corresponds to u^{-1} and that is commutative with only $\frac{1}{6}g$ operators of H . Since $\frac{1}{2}g$ operators of G are commutative with u , two thirds of the operators of $G - H$ are commutative with u . Now if v' be one of these operators of $G - H$ commutative with u , we see that u is commutative with the same number of operators in $v'H$ as in H , a contradiction.

If more than $\frac{5}{8}g$ and less than $\frac{2}{3}g$ operators of G correspond to their inverses, t is invariant in a subgroup H of index less than 4.

Let H be of order $h = \frac{1}{3}g$. More than $\frac{3}{4}h$ operators of H correspond to their inverses, so that H is abelian, and all its operators correspond to their inverses. We write G in the three sets H, uH, vH . In $G - H$ there are more than $\frac{7}{4}g$ and less than $\frac{1}{3}g$ operators that correspond to their inverses. If u corresponds to u^{-1} and no operator of vH does so, between $\frac{7}{2}h$ and $\frac{2}{3}h$ operators of H are invariant in G , an impossibility. If v also corresponds to its inverse, more than $\frac{7}{4}h$ and less than $\frac{1}{3}h$ operators of H are invariant in G . Hence H cannot be of index 3.

Let H be of order $\frac{1}{2}g$. There is an operator u in $G - H$ which corresponds to u^{-1} . It is commutative with half the operators of H which form a subgroup K , invariant in G . Then H is not abelian. We now write

$$G = K + tK + uK + utK.$$

Since t and u are both commutative with every operator of K , $3x$ operators of K , tK , uK , correspond to their inverses whenever x operators of K do so. The maximum number of operators of utK that correspond to their inverses is $\frac{1}{4}g - x$, since ut does not correspond to $t^{-1}u^{-1}$. Then $3x + \frac{1}{4}g - x > \frac{5}{8}g$, $2x > \frac{3}{4}h$. But this is absurd because H is not abelian. This proves that if more than $\frac{5}{8}g$ operators of G correspond to their inverses, just $\frac{3}{8}g$, $\frac{3}{4}g$, or all do so.

From the preceding paragraphs it is clear that if just $\frac{5}{8}g$ operators of G correspond to their inverses, t cannot be commutative with just $\frac{1}{4}g$ operators of G . We first assume that there is an operator t which is invariant in a subgroup H of index 4, and not invariant in a larger subgroup. Then H is abelian. Write G in the sets H, uH, vH, wH . Just half the operators of a set uH correspond to their inverses. Since no operator from $G - H$ is commutative with t , just half the operators of H are invariant in G . Let F be the group composed of the invariant operators of G . When G is not the direct product an abelian and a non-abelian group its order is a power of 2. The operator of G/F that corresponds to tF is of order 2. The group of cogredient isomorphisms G/F is neither quaternion, cyclic, of type $(2, 1)$,* nor, when G/F is octic, is the operator corresponding to tF invariant. Let G/F be octic and arrange G thus:

$$G = F + s^2F + sF + s^3F + tF + ts^2F + tsF + ts^3F.$$

By hypothesis, $ts^2 \neq s^2t$, so that $t^{-1}st = s^3a$ (a belonging to F),

$$t^{-1}s^4t = s^{12}a^4 = s^4, \quad (s^2a)^4 = 1, \quad t^{-1}s^2at = (s^2a)^{-1}$$

The commutator subgroup of G is cyclic of order 4. Let us suppose that the invariant abelian subgroup F has an operator b of order 2 other than $(s^2a)^2$, the commutator of order 2. Then $\{b\}$ and $\{s^2a\}$ are two invariant subgroups of G with nothing but the identity in common, and according to theorem I, corollary I, G is an isomorphism between two groups of lower order, one abelian and one non-abelian. Making the same assumption in regard to the non-abelian constituent we continue until we have a group G with only the one operator of order 2, $(s^2a)^2$, in F . But an abelian group of order 2^m with only one operator of order 2 is cyclic. Now let s^4 be taken as an operator of highest order in F . Since $\{F, s\}$ is cyclic, $t^{-1}st = s^3s^{4x}$, $t^{-1}s^4t = s^{12}s^{16x} = s^4$, $s^8 = 1$, and

* MILLER, Comptes Rendus de l'Académie des Sciences, vol. 128 (1899), p. 229.

$x=0$ or 1. In both cases the groups are known and five eighths of their operators can be made to correspond to their inverses. There remains the hypothesis that $s^4 = 1$. F is generated by an operator r of order 2^{m-3} , commutative with both s and t ; $\{F, s\}$ is of type $(m-3, 2)$, and either $t^2 = 1$ or $t^2 = r$. Now $(st)^2 = stst = stst^{-1}t^2 = ss^3r_4t^2 = r_4t^2$, where r_4 is of order 4. If $t^2 = r$, $(st)^2 = rr_4$, so that when $m > 5$ st is of the same order as t , and $\{t\}$ and $\{st\}$ have half their operators in common. This is the G_3 given by Professor MILLER* in a memoir "On the Groups of order p^m which contain operators of order p^{m-2} ". When $m = 5$, $r^4 = 1$, $s^{-1}ts = ts^2r$, $(st)^2 = 1$, and this G_{32} has only two cyclic subgroups of order 8. We may suppose t replaced by $t' = st$. This replacement transforms $\{r, s\}$ in the same way that t does. If $t^2 = r^{2^{m-3}} = s^4 = 1$, consider the subgroup G' of order 32 generated by $r_4 = r^{2^{m-3}}$, s and t . It is the group last mentioned. One and only one group G of order 2^m can be constructed from G' by adjoining an operator r commutative with every operator of G' and such that its 2^{m-5} th power is r_4 .

Let G/F be of type $(1, 1, 1)$. G cannot have just one commutator, for then every operator would be commutative with just half the operators of G , contrary to the assumption in regard to t . The commutators are invariant, since G is metabelian, and moreover are all of order 2. The commutator subgroup is then of order 4 or 8. Let it be of order 4. We may suppose G deprived of its abelian constituents so that F is the direct product of two cyclic groups of orders 2^α and 2^β . Then G is a $(2^\alpha, 2^\beta)$ isomorphism between two non-abelian groups G_1 and G_2 of orders $2^{\alpha+3}$ and $2^{\beta+3}$ respectively. Every operator of $G_1(G_2)$ is invariant in half of $G_1(G_2)$. But the group of cogredient isomorphisms of $G_1(G_2)$ cannot be of order 8,† from which we conclude that one fourth of the operators of $G_1(G_2)$ are invariant and three fourths correspond to their inverses. If we write G_1 and G_2 with respect to the subgroups composed of half the invariant operators and, setting up an isomorphism between the quotient groups of order 8, multiply corresponding divisions, three fourths of the operators of the resulting group can be made to correspond to their inverses unless invariant operators of one constituent be made to correspond to non-invariant operators of the other. There is one group of order 2^m , $m > 3$, which we may use for G_1 and G_2 and if all possible values are given to α and β , there are $(m-3)/2$ or $(m-4)/2$ groups of order 2^m , as m is odd or even. If the commutator subgroup of G is of order 8, we have the same conditions until it comes to setting up the final isomorphism. Note that if between two of the constituent groups invariant operators of the one are multiplied only into invariant operators of the other,

* MILLER, Transactions of the American Mathematical Society, vol. 3 (1902), p. 383.

† YOUNG, American Journal of Mathematics, vol. 15 (1893), p. 71.

the resulting group has, not an axial commutator subgroup, but a commutator subgroup of order 2. Then we have to make invariant operators of one constituent correspond to non-invariant operators in both the other constituents. This can be done. The number of these groups of order 2^{m+3} is $(m^2 - \alpha^2)/12$, when $m \equiv \pm \alpha \pmod{6}$ and $0 \leq \alpha \leq 3$.

There remains the hypothesis that every non-invariant operator t that corresponds to its inverse is commutative with half the operators of G , which make up a subgroup H . The square of every operator that corresponds to its inverse is invariant. $G_1 = H + sH$ and if s corresponds to s^{-1} , s is commutative with half the operators of H which then form an invariant subgroup K . If x operators of K correspond to their inverses, we have $3x + (\frac{1}{2}g - x) \cong \frac{5}{2}g$, so that $x = \frac{3}{16}g = \frac{3}{4}k$ and just one fourth of the operators of the division stK correspond to their inverses. The invariant operators of K are the invariant operators of G . The group of cogredient isomorphisms of G is abelian of type $(1, 1, 1, 1)$. We write $K = F_1 + t_1 F_1 + s_1 F_1 + s_1 t_1 F_1$, $G = K + tK + sK + stK$. To $sts_1 t_1$ corresponds $t^{-1} s^{-1} t_1^{-1} s_1^{-1}$, or, since these 4 operators severally correspond to their inverses, $t^{-1} s^{-1} t_1^{-1} s_1^{-1} = s^{-1} t^{-1} s_1^{-1} t_1^{-1}$, whence, $tst^{-1} s^{-1} = t_1 s_1 t_1^{-1} s_1^{-1}$. Then the commutator subgroup of G is of order 2. Conversely when the commutator subgroup is of order 2 and t, s, t_1, s_1 , severally correspond to $t^{-1}, s^{-1}, t_1^{-1}, s_1^{-1}$, $sts_1 t_1$ corresponds to $(sts_1 t_1)^{-1}$. These metabelian groups are known.*

* FITE, l. c.