ON THE GROUPS WHICH ARE THE DIRECT PRODUCTS OF TWO SUBGROUPS*

BY

G. A. MILLER

If a group is generated by two self-conjugate subgroups which have only identity in common it is said to be the direct product† of these subgroups. It is well known that every operator of one of these groups is commutative with every operator of the other.‡ Evidently one of the necessary conditions that a group ($\mathfrak{G}$) may be the direct product of two subgroups is that it contains a subgroup ($\mathfrak{G}_1$) such that every operator of $\mathfrak{G}_1$ is transformed into its various conjugates under $\mathfrak{G}$ by the operators of $\mathfrak{G}_1$; *i. e.*, each operator of $\mathfrak{G}_1$ has in all the same transforms with respect to its own operators as it has with respect to the operators of $\mathfrak{G}$. That this condition is not sufficient follows from the cyclical groups whose order is a power of a prime, from the quaternion group, and from many other known groups. This condition is explicitly employed in theoremIII.

THEOREM I.—*If* $\mathfrak{G}$ *has a solvable quotient group* $\mathfrak{G}/\mathfrak{H}$ *such that in the isomorphism of* $\mathfrak{G}$ *with* $\mathfrak{G}/\mathfrak{H}$ *to each operator of* $\mathfrak{G}/\mathfrak{H}$ *there corresponds one and only one operator of* $\mathfrak{G}$ *whose order is a divisor of the order of* $\mathfrak{G}/\mathfrak{H}$ *then* $\mathfrak{G}$ *is the direct product of* $\mathfrak{H}$ *and a subgroup which is simply isomorphic to* $\mathfrak{G}/\mathfrak{H}$.

Let $1, \mathfrak{H}_1, \mathfrak{H}_2, \cdots, \mathfrak{H}_m \equiv \mathfrak{G}/\mathfrak{H}$ be a series of groups such that each one includes the one which precedes it and some additional operators, each is self-conjugate in $\mathfrak{H}_m$, and all the quotient groups $\mathfrak{H}_a/\mathfrak{H}_{a-1}$ $(a = 1, 2, \cdots, m)$ are abelian.§ Let $1, T_2, T_3, \cdots, T_n$ be all the operators of $\mathfrak{G}$ whose orders are divisor of the order (h_m) of $\mathfrak{G}/\mathfrak{H}$; $n = h_m$. It is only necessary to prove that these n operators constitute a group.‖ In the isomorphism of $\mathfrak{G}$ and $\mathfrak{G}/\mathfrak{H}$ each one of these T's evidently corresponds to an operator of the same order

* Presented to the Society at the Columbus meeting August 26, 1899. Received for publication December 4, 1899.

† As substitution groups these groups have been known for a long time. They occupy a prominent place in the theory of intransitive groups. HÖLDER seems to have been the first to call them (as abstract groups) direct products, Mathematische Annalen, vol. 43, p. 330, 1893.

‡ DYCK, Mathematische Annalen, vol. 22, p. 79, 1883.

§ JORDAN, *Traité des substitutions*, p. 395, 1870.

‖ DYCK, l. c.

in $\mathfrak{G}/\mathfrak{K}$ and all the T's must transform each other in exactly the same manner as the corresponding operators of $\mathfrak{G}/\mathfrak{K}$ transform each other. Since $\mathfrak{K}_1$ is abelian the corresponding T's $(1, T_2, \cdots T_{h_1})$ constitute an abelian group. This group $(\mathfrak{H})$ is a self-conjugate subgroup of $\mathfrak{G}$ since $\mathfrak{K}_1$ is self-conjugate in $\mathfrak{G}/\mathfrak{K}$. This proves the theorem if $m = 1$.

When $m > 1$ we can readily prove the theorem by induction. Suppose that all the T's which correspond to $\mathfrak{K}_a$ $(a < m)$ constitute a self-conjugate subgroup $(\mathfrak{H}^a)$ of $\mathfrak{G}$ and let T_{a+1} be any one of the given n T's that corresponds to an operator of $\mathfrak{K}_{a+1}$ but is not contained in $\mathfrak{H}^a$. T_{a+1} and $\mathfrak{H}^a$ clearly generate a group whose order is a divisor of n. This group $\mathfrak{H}^{a+1}$ must be transformed into itself by all the operators of $\mathfrak{G}$ which correspond to $\mathfrak{K}_{a+1}$ since $\mathfrak{K}_{a+1}/\mathfrak{K}_a$ is abelian. If the order of $\mathfrak{H}^{a+1}$ is less than that of $\mathfrak{K}_{a+1}$ we let T_β be any one of a given n T's which corresponds to an operator of $\mathfrak{K}_{a+1}$ and is not contained in $\mathfrak{H}^{a+1}$, T_β and $\mathfrak{H}^{a+1}$ will clearly generate a larger group whose order is a divisor of n and which is self-conjugate in the subgroup of $\mathfrak{G}$ which corresponds to $\mathfrak{K}_{a+1}$. Hence we observe, by induction, that all the T's which correspond to $\mathfrak{K}_{a+1}$ constitute a self-conjugate subgroup of $\mathfrak{G}$ provided all those which correspond to $\mathfrak{K}_a$ constitute such a self-conjugate subgroup. We proved above that all those which correspond to $\mathfrak{K}_1$ constitute such a self-conjugate subgroup. Hence the proof is complete.

THEOREM II.—*If the order of a group $\mathfrak{K}$ is mn (m and n being prime to each other), and if $\mathfrak{K}$ contains a subgroup $\mathfrak{M}$ of order m which has the property that for every operator K of $\mathfrak{K}$ there is an operator M' of $\mathfrak{M}$ such that for every operator M of $\mathfrak{M}$ the transforms by K and by M' are equal,*

$$(K^{-1}MK = M'^{-1}MM'),$$

and if the quotient group $\mathfrak{K}/\mathfrak{M}$ is solvable, then $\mathfrak{K}$ is the direct product of its subgroups of orders m and n respectively.

It is clear that $\mathfrak{M}$ is a self-conjugate subgroup of $\mathfrak{K}$. Arranging all the operators of $\mathfrak{K}$ in the following manner:

$$\begin{array}{ccccccc} 1 & S_2 & S_3 & S_4 & \cdots & S_m \\ T_2 & S_2T_2 & S_3T_2 & S_4T_2 & \cdots & S_mT_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ T_n & S_2T_n & S_3T_n & S_4T_n & & S_mT_n \end{array}$$

(the first row being composed of the operators of $\mathfrak{M}$) we proceed to prove that there is one and only one operator whose order is prime to m in each row. If $\mathfrak{M}$ contains just k' operators that are commutative with each operator of $\mathfrak{M}$ there must be just k' operators in each one of the given rows that are commuta-

tive with each operation of $\mathfrak{m}$; for if T_a transforms the operators of the first row according to a given substitution there must be k' operators in the first row which transform all the operators of this row according to the inverse of this substitution. These k' operators multiplied into T_a give the required k' operators (of the row which contains T_a) that are commutative with each operator of $\mathfrak{m}$. Suppose T_a is one of these k' operators and that γ is the order of the corresponding operator in the quotient group $\mathfrak{K}/\mathfrak{m}$. From

$$(S_{a_1} T_a)^\gamma = S_{a_1}^\gamma T_a^\gamma$$

and the fact that γ is prime to m, it follows that we obtain all the operators of $\mathfrak{m}$ by raising all the operators of the row which contains T_a to the γ power. This proves that there is one and only one operator whose order is prime to m in each row and that the order of this operator is the same as that of the corresponding operator in $\mathfrak{K}/\mathfrak{m}$. Hence it follows directly from theorem I that $\mathfrak{K}$ is the direct product of $\mathfrak{m}$ and the subgroup of order n.

For use in the proof of theorem III one notices that the second hypothesis of theorem III is fulfilled if the operators M of the group $\mathfrak{m}$ are individually self-conjugate under any certain n extenders of $\mathfrak{m}$ to $\mathfrak{K}$.

THEOREM III.—*If the order of a solvable group $\mathfrak{H}$ is $h = mp^a$ (where p is a prime and a and m are integers, m being prime to p) and if all the conjugates under $\mathfrak{H}$ of every operator A of a subgroup $\mathfrak{A}$ of order p^a are conjugates of A under $\mathfrak{A}$, then $\mathfrak{H}$ is the direct product of $\mathfrak{A}$ and a subgroup $\mathfrak{m}$ of order m, and further $\mathfrak{H}$ contains certain self-conjugate subgroups $\mathfrak{n}_\gamma$ of the orders $n_\gamma = mp^\gamma$ ($\gamma = 0, 1, \cdots, a-1$).*

Each one of the self-conjugate subgroups of $\mathfrak{A}$ is clearly also a self-conjugate subgroup of $\mathfrak{H}$. Hence there must be a p^β, 1 (β being one of the numbers $1, 2, \cdots, a-1$) isomorphism between $\mathfrak{H}$ and each one of a series of groups

$$\mathfrak{G}_{a-1}, \mathfrak{G}_{a-2}, \mathfrak{G}_{a-3}, \cdots, \mathfrak{G}_0$$

whose orders are divisible by $p^{a-1}, p^{a-2}, p^{a-3}, \cdots, p^0$ respectively but by no higher power of p. According to theorem II, $\mathfrak{G}_1$ is the direct product of its subgroups of orders p and m. Suppose that $\mathfrak{G}_\beta$ ($\beta < a-1$) is the direct product of its subgroups of orders p^β and m. To the subgroup of order m in $\mathfrak{G}_\beta$ there must correspond a subgroup of order pm in $\mathfrak{G}_{\beta+1}$. From theorem II it follows that this subgroup of order pm is the direct product of its subgroups of orders p and m. $\mathfrak{G}_{\beta+1}$ must therefore be the direct product of its subgroups of orders $p^{\beta+1}$ and m whenever $\mathfrak{G}_\beta$ is the direct product of its subgroups of orders p^β and m. Since $\mathfrak{G}_1$ is the direct product of its subgroups of orders p and m it

follows from what has just been proved that $\mathfrak{H}$ must be the direct product of its subgroups of orders p^α and m. The remainder of the theorem follows directly from this property.

Every group of order $2m$, m being any odd number, contains a self-conjugate subgroup of order m.* If it contains a self-conjugate subgroup of order 2 it is evidently the direct product of these two self-conjugate subgroups.

If a group is the direct product of two subgroups its group of cogredient isomorphisms is the direct product of the groups of cogredient isomorphisms of these two subgroups.† The converse of this is not generally true but we may readily prove that it is true if the conditions mentioned in the following theorem are satisfied.

THEOREM IV.—*If the group of cogredient isomorphisms* ($\mathfrak{G}'$) *of a group* ($\mathfrak{G}$) *is the direct product of two subgroups* ($\mathfrak{M}$, $\mathfrak{N}$) *whose orders* (m, n) *are prime to each other, then* $\mathfrak{G}$ *is also the direct product of two subgroups.*

COROLLARY.—*If a group* ($\mathfrak{L}$) *has an abelian group of cogredient isomorphisms whose order is not a power of a single prime number then* $\mathfrak{L}$ *is the direct product of two subgroups.*‡

All the operators of $\mathfrak{G}$ which are commutative with each one of its operators constitute the subgroup ($\mathfrak{G}_1$) of order g_1 which corresponds to identity of $\mathfrak{G}'$ in the isomorphism of $\mathfrak{G}$ and $\mathfrak{G}'$. Let

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots, \quad n = q_1^{\beta_1} q_2^{\beta_2} \cdots, \quad g_1 = p_1^{\alpha_1'} p_2^{\alpha_2'} \cdots q_1^{\beta_1'} q_2^{\beta_2'} \cdots r_1^{\gamma_1} r_2^{\gamma_2} \cdots,$$

where

$$p_1, p_2, \cdots, \quad q_1, q_2, \cdots, \quad r_1, r_2, \cdots,$$

are distinct prime numbers; and let G_α be any operator of $\mathfrak{G}$ which corresponds to a given operator M_α of $\mathfrak{M}$ in the given isomorphism of $\mathfrak{G}$ and $\mathfrak{G}'$. $G_\alpha^{m_\alpha}$ (m_α being the order of M_α) must occur in $\mathfrak{G}_1$. If the order of $G_\alpha^{m_\alpha}$ contains a factor $(q_1^{\beta_1''} q_2^{\beta_2''} \cdots r_1^{\gamma_1'} r_2^{\gamma_2'} \cdots)$ which is prime to m, $G_\alpha^{m_\alpha}$ must be the direct product of an operator of $\mathfrak{G}_1$ of order $q_1^{\beta_1''} q_2^{\beta_2''} \cdots r_1^{\gamma_1'} r_2^{\gamma_2'} \cdots$ and an operator of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots$. In this case $\mathfrak{G}_1$ must contain some operator G_1 such that the order of $(G_1 G_\alpha)^{m_\alpha}$ does not contain any factor that is prime to m.

We may therefore assume that to each operator of $\mathfrak{M}$ in the given isomorphism of $\mathfrak{G}$ and $\mathfrak{G}'$ there corresponds some operator of $\mathfrak{G}$ whose order does not involve any factor that is prime to m. Hence $\mathfrak{G}$ contains a subgroup of order $p_1^{\alpha_1+\alpha_1'} p_2^{\alpha_2+\alpha_2'} p_3^{\alpha_3+\alpha_3'} \cdots$ which includes all the operators of $\mathfrak{G}$ whose orders do not

*FROBENIUS, Berliner Sitzungsberichte, 1895, p. 180.

†Bulletin of the American Mathematical Society, vol. 5, p. 294, 1899.

‡Cf. BURNSIDE, *Theory of Groups of a Finite Order*, p. 115, 1897.

involve any factor that is prime to m. This subgroup must be self-conjugate. In exactly the same way we may prove that $\mathfrak{G}$ contains a self-conjugate subgroup of order $q_1^{\beta_1+\beta'} q_2^{\beta_2+\beta'_2} q_3^{\beta_3+\beta'_3} \cdots$ which includes all the operators of $\mathfrak{G}$ whose orders do not involve any factor that is prime to n. If each of the r's is equal to unity $\mathfrak{G}$ is the direct product of $\mathfrak{M}$ and $\mathfrak{N}$. In general $\mathfrak{G}$ is evidently the direct product of $\mathfrak{M}$, $\mathfrak{N}$ and the subgroup of order $r_1^{\gamma_1} r_2^{\gamma_2} r_3^{\gamma_3} \cdots$ which is contained in $\mathfrak{G}$, and hence it is also the direct product of one of these three groups and the product of the other two.

If a group $\mathfrak{M}$ contains only identity as a self-conjugate operator, then it is simply isomorphic to its group of cogredient isomorphisms. If moreover $\mathfrak{M}$ is a subgroup of a group $\mathfrak{K}$ with the property of the hypothesis of theorem II, then $\mathfrak{K}$ is the direct product of $\mathfrak{M}$ and a subgroup which is simply isomorphic to $\mathfrak{K}/\mathfrak{M}$. This subgroup is composed of all the operators of $\mathfrak{K}$ which are commutative with every operator of $\mathfrak{M}$. In fact, it is evident that all the operators of a group which are commutative with every operator of any one of its self-conjugate subgroups must always constitute a self-conjugate subgroup. This subgroup may evidently be the entire group. In particular, when a complete group is self-conjugate in any group the latter is the direct product of this complete group and the corresponding quotient group.*

If $\mathfrak{G}$ is the direct product of $\mathfrak{G}_1$, $\mathfrak{G}_2$ then any group contained in $\mathfrak{G}_1$ together with any group contained in $\mathfrak{G}_2$ generates a group which is the direct product of these two generating groups. Suppose $\mathfrak{G}$ may be represented as a primitive substitution group. Then the subgroup which includes all its substitutions that do not involve a given element is maximal and not self-conjugate. From this it follows that this subgroup does not contain any self-conjugate subgroup of $\mathfrak{G}$ besides identity. Hence the given subgroup must be formed by establishing a simple isomorphism between the substitution group which are simply isomorphic to $\mathfrak{G}_1$ and $\mathfrak{G}_2$, *i. e., the necessary and sufficient condition that* $\mathfrak{G}$ *can be represented as a primitive substitution group is that* $\mathfrak{G}_1$ *and* $\mathfrak{G}_2$ *are simply isomorphic simple groups of a composite order.*† When this condition is satisfied $\mathfrak{G}$ can evidently be represented as a primitive group in only one way and the degree of this primitive group is the square root of the order of $\mathfrak{G}$.‡

From the preceding paragraph it follows directly that the degrees of the primitive groups which are the direct products of two groups have a (1, 1) correspondence to the simple groups of composite order; the first group of this kind being of degree 60 and order 3600, the second of degree 168 and order 28224,

* HÖLDER, Mathematische Annalen, vol. 46, p. 325.

† Cf. BURNSIDE, *Theory of Groups*, p. 190, 1897.

‡ Cf. MAILLET, *Thèse de Doctorat*, p. 31, Paris, 1892.

etc. These groups can be represented in a large number of different ways as imprimitive groups.

If $\mathcal{G}_1$ and $\mathcal{G}_2$ are the direct products of α and β groups respectively then $\mathcal{G}$ may be said to be the direct product of these $\alpha + \beta$ groups and it can be represented as the product of any $\alpha + \beta$ transitive substitution groups (written in distinct elements) which satisfy the condition that they are simply isomorphic to all the given $\alpha + \beta$ groups, each being associated with only one of them. Hence the necessary and sufficient condition that $\mathcal{G}$ is the direct product of γ-groups is, that it contains γ self-congugate subgroups $(\mathcal{G}_1, \mathcal{G}_2, \cdots, \mathcal{G}_\gamma)$ such that the group generated by any δ of them has only identity in common with any one of the remaining $\gamma - \delta$ and that the order of $\mathcal{G}$ is the product of the orders of these subgroups.* When $\gamma > 2$ it is clearly impossible to represent $\mathcal{G}$ as a primitive substitution group. Hence the necessary and sufficient condition that a direct product may be represented as a primitive substitution group is that it contains just two factors and that these are simply isomorphic simple groups of composite order.

CORNELL UNIVERSITY.

*HÖLDER, Mathematische Annalen, vol. 43, p. 330, 1893.