NON-ABELIAN GROUPS IN WHICH EVERY SUBGROUP IS ABELIAN[*]

BY

G. A. MILLER AND H. C. MORENO

Several years ago DEDEKIND and others investigated the groups in which every subgroup is invariant, and found that the theory of these groups presents remarkably few difficulties except such as are involved in abelian groups. The non-abelian groups in which every subgroup is abelian present a parallel example of simple and general results. The following are some of the most important ones: All such groups are solvable. Their orders cannot be divided by more than two distinct primes. Every commutator is of prime order. When the order is $p^{\alpha} q^{\beta}$, (p and q being prime; α, $\beta > 0$), there are just q^{β} subgroups of order p^{α} and there is only one subgroup of order q^{β}. The former are cyclic and the latter is of type $(1, 1, 1, \cdots)$. When the order is p^{α}, there are just $p+1$ subgroups of order $p^{\alpha-1}$ and none of them involves more than three invariants. If there are three invariants at least one of them must be of order p.

Let G represent any non-abelian group in which every subgroup is abelian. We shall first prove that G is solvable. If G is represented as a transitive substitution group it will be either primitive or imprimitive. In the latter case it will be isomorphic with some primitive group P.[†] The subgroup of G which corresponds to identity in P is abelian and every subgroup of P is abelian. The group G is solvable whenever P is solvable. Hence it remains to prove that a non-abelian primitive group P in which every subgroup is abelian is always solvable. Let P_1 be the subgroup of P which is composed of all the substitutions omitting a given letter. Since P is non-regular,[‡] P_1 includes at least one substitution besides the identity. If two conjugates of P_1 had a common substitution besides the identity, this substitution would be invariant under P, since P_1 is a maximal subgroup of P. Hence P must be of class $n-1$, n being the degree of$P$. Therefore P contains an invariant subgroup of order n,[§] with respect to which the quotient group is simply isomorphic with P_1. As

[*] Presented to the Society (San Francisco) May 3, 1902 and April 25, 1903. Received for publication, May 5, 1903.

[†] JORDAN, *Traité des substitutions* (1870), p. 399.

[‡] JORDAN, *Traité des substitutions* (1870), p. 60.

[§] FROBENIUS, Berliner Sitzungsberichte (1902), p. 455.

both this invariant subgroup and P_1 are abelian, P is solvable and hence *G is solvable.*

It will be convenient to consider all the groups in question under two headings according as the order (g) of G is divisible by more than one prime, or is a power of a single prime.

§ 1. *The order of G is divisible by more than one prime number.*

Let $g = p^\alpha q^\beta r^\gamma \cdots (p, q, r, \cdots$ being distinct primes). Since G is solvable it must contain a subgroup G_1 of prime index p. The order G_1 is $g_1 = p^{\alpha-1} q^\beta r^\gamma \cdots$. Since G_1 is abelian, it is the direct product of the subgroups $P_{\alpha-1}$, Q_β, R_γ, $\cdots$, of orders $p^{\alpha-1}$, q^β, r^γ, $\cdots$ respectively. The orders of each of the operators of G which are not in G_1 is divisible by p, and hence G contains only one subgroup of each of the orders q^β, r^γ, $\cdots$. If it contained only one subgroup P_α of order p^α, it would be the direct product of the abelian groups, P_α, Q_β, R_γ. As this is impossible, *G contains only one subgroup of each of the orders q^β, r^γ, $\cdots$, but it contains more than one subgroup of order p^α.*

Any two of the abelian subgroups of order p^α must generate G and hence each of the operators of $P_{\alpha-1}$ is invariant under G. Let s be any operator of P_α which is not contained in $P_{\alpha-1}$. If s were commutative with each operator in the subgroups Q_β, R_γ, $\cdots$, then G would be abelian. Hence s transforms one of these subgroups, Q_β say, into itself without being commutative with each of its operators. As $\{Q_\beta, s\}$ is non-abelian it follows that *g cannot be divisible by more than two distinct primes.* We may therefore assume that $g = p^\alpha q^\beta$, and that G contains only one subgroup Q_β of order q^β, but that it contains more than one subgroup of order p^α.

Since $\{Q_\beta, s\}$ is non-abelian it is identical with G. The order of $\{Q_\beta, s\}$ is the product of q^β and the order of s. Hence s must generate P_α; i. e., *P_α is cyclic.*

We shall next prove that Q_β is of type $(1, 1, 1, \cdots)$. Let t_1 be any operator of highest order in Q_β and suppose that $t_1^q \neq 1$. The operator s is commutative with all the operators of Q_β whose orders are less than the order of t_1, otherwise these operators and s would generate a non-abelian group which would not include t_1. Let t be any operator of Q_β such that $t^q = t_1^q$. Then $t = t' t_1$, where t' is some operator of order q in Q_β. From this it follows that t has q^n values, n being the number of invariants of Q_β. As s transforms these q^n operators among themselves, it must transform at least one of them into itself. It also transforms into themselves each of the operators represented by t'. Hence s would be commutative with each operator of highest order in Q_β, if this order were supposed to exceed q; i. e., *Q_β contains no overator whose order exceeds q.*

When Q_β is cyclic G is of order $p^\alpha q$. Since each of the operators of $P_{\alpha-1}$ is invariant under G it follows that the group of cogredient isomorphisms of G is non-abelian and of order pq. Hence $q-1$ must be divisible by p. Moreover, when this condition is satisfied, we can construct one G for every value of α by establishing a $(p^{\alpha-1}, q)$ isomorphism between the cyclic group of order p^α and the non-abelian group of order pq. Since every possible G of order $p^\alpha q$ is simply isomorphic with one of these groups it follows that *there is one and only one G of order $p^\alpha q$ for every value of α, whenever $q-1$ is divisible by p. When this condition is not satisfied there is no such group.* Each of. these groups contains $p^{\alpha-1}q(p-1)$ operators of order p^α in addition to the cyclic invariant subgroup of order $p^{\alpha-1}q$.

It remains to consider the case in which Q_β is non-cyclic. In this case Q_β cannot contain just q operators which are invariant under G. For, as s cannot transform any subgroup of Q_β into itself without transforming each of its operators into itself, the number of subgroups of order q in Q_β would have to be $lp+1$. Since the number of subgroups of order $q^{\beta-1}$ would also have to be $lp+1$*, s would transform at least one of these $(Q_{\beta-1})$ into itself. If $\beta > 2$, $Q_{\beta-1}$ would contain operators which are not commutative with s, and if $\beta = 2$ the number of subgroups of order $q^{\beta-1}$ could not be of the form $lp+1$. As each of these results is impossible, it follows that Q_β cannot contain just q operators which are invariant under G.

Suppose that Q_β contains just q^e invariant operators, $1 < e < \beta$. With respect to q^{e-1} of these G would be isomorphic with a group containing at least $q-1$ invariant operators of order q. If it contained more invariant operators of this order, G would contain a non-abelian subgroup. As it has been proved above that all the subgroups of this quotient group (which contains just $q-1$ invariants operators of order q) cannot be abelian, the proof is complete. Hence $P_{\alpha-1}$ is composed of all the invariant operators of G.

The group of cogredient isomorphisms (I_0) of G is therefore non-abelian and of order pq^β, $\beta > 1$. Since Q_β is abelian, contains no invariant operators or invariant subgroup, and leads to an abelian quotient group, it must be the commutator subgroup of G and each of its operators must be a commutator.† From these facts it follows that G contains just q^β cyclic subgroups of order p^α. In other words, all the operators of G which are not contained in G_1 are of order p^α, while G_1 is the direct product of Q_β and $P_{\alpha-1}$.

The group G can therefore be constructed only when $q^\beta \equiv 1 \bmod p$ and when Q_β is generated by any one of its sets of p conjugate operators. As the continued product of these p operators must be invariant and hence equal to the identity, β must be less than p. From FERMAT's theorem it follows that β is

* Cf. BURNSIDE, *Theory of Groups of Finite Order* (1897), p. 60.

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

a divisor of $p-1$. Moreover G can be constructed only when I_0 can be constructed. By establishing a $(q^\beta, p^{\alpha-1})$ isomorphism between I_0 and a cyclic group of order p^α we obtain one and only one G for every value of $\alpha > 0$. As each possible G is isomorphic with such a group the construction of these groups is reduced to the construction of such groups as I_0.

Since each one of the subgroups of order p in I_0 is maximal and non-invariant, I_0 may be represented as a primitive substitution group (S) of degree q^β. Conversely every primitive group of degree q^β and order pq^β is such an I_0. The necessary and sufficient condition that S is doubly transitive is that $q^\beta - 1 = p$. In this case $q = 2$ and I_0 can always be constructed and hence the infinite system which depends upon it can also be constructed. The alternating group of degree 4 and G_{56}^{8} are the first two instances of this kind. In all other cases S is simply transitive and it will be proved that it can be constructed for one and only one value of β when p and q are given. The first two instances of this kind are G_{80}^{16} and G_{75}^{25}.

It is easy to prove that I_0 cannot be constructed when $q \equiv 1 \bmod p$. The number of subgroups of every order in Q_β is evidently $\equiv 0 \bmod p$. The number of subgroups of order q is $q^{\beta-1} + q^{\beta-2} + \cdots + q + 1$, and we may write this number $(q^{\beta-1} - 1) + (q^{\beta-2} - 1) + \cdots + (q-1) + \beta \not\equiv 0 \bmod p$, since $1 < \beta < p$. That is, G can be constructed only for $\beta = 1$ when $q \equiv 1 \bmod p$, and there is only one group when α, p and q are given.

That I_0 can be constructed for only one value of β when $q \not\equiv 1 \bmod p$ may be proved as follows: Let β_0 be the smallest value of x such that $q^x \equiv 1 \bmod p$, and let $\beta < p$ be any other possible value of x. It is well known that $\beta = l\beta_0$, l being an integer. If p^m is the highest power of p which divides the order of the group of isomorphisms (I_0') of Q_{β_0}, we shall prove that p^{ml} is the highest power of p which divides the order of the group of isomorphisms (I') of Q_β. From FERMAT's theorem and from the condition $q \not\equiv 1 \bmod p$, it follows that

$$q^{\beta_0-1} + q^{\beta_0-2} + \cdots + q + 1 \equiv q^{\beta-1} + q^{\beta-2} + \cdots + q + 1 \equiv 0 \bmod p.$$

As $\beta = l\beta_0$ the second member may be written

$$[1 + q^{\beta_0} + \cdots + q^{(l-1)\beta_0}] \cdot [1 + q + \cdots + q^{\beta_0-2} + q^{\beta_0-1}].$$

To see that the first factor is not divisible by p, it may be written in the form $l + (q^{\beta_0} - 1) + \cdots + (q^{(l-1)\beta_0} - 1)$, where each term except the first is divisible by p. Let (I'') be a subgroup of I' which transforms each of just q^r operators of Q_β into itself. The order of I'' is $q^{r(\beta-r)}$ times the order of the group of isomorphisms of the quotient group of Q_β with respect to these invariant operators. By letting $r = (l-1)\beta_0, (l-2)\beta_0, \cdots, \beta_0$, in succession, it is easy to see that p^{ml} is the highest power of p which divides the order of I'. Hence I' contains a subgroup P_{ml} of order p^{ml} and it remains to prove that each operator of this subgroup transforms into itself at least one subgroup of order q^{β_0} in Q_β. It is clear that P_{ml} contains a subgroup of order $p^{m(l-1)}$ which transforms each of just q^{β_0} operators of Q_β into itself. As there is a substitution of order p^m which permutes these $q^{\beta_0}-1$ operators among themselves,* the proof is complete. Hence *there is always one and only one value of β such that there exists a primitive group of order pq^β and degree q^β. When $q^\beta-1>p$, this primitive group is simply transitive.*

§2. *The order of G is a power of a prime.*

We shall first construct two triply infinite systems of such groups and then prove that every possible group (with the exception of a few known ones) is simply isomorphic with a group in one of these systems. Let (P_m) represent any non-abelian group of order p^m, $m>2$, which contains an operator (t) of order p^{m-1} but no non-abelian subgroup of this order.† It is well known that there is just one such group for every value of m except when $p=2$ and $m=3$. In this special case there are two groups: viz., the quaternion and the octic groups. In every case the commutator subgroup is generated by an operator (t_0) of order p.

Consider the groups obtained by establishing an isomorphism between P_m, with respect to the group generated by t, and the cyclic groups of order p^{m_1}, $m_1>2$. All the subgroups of every one of these groups are abelian, and in each of them t_0 is a power of operators of order p^{m-1} but not of an operator of higher order. Hence no two of the triply infinite systems of groups, obtained by assigning to p, m and m_1 all possible values can be simply isomorphic, with the possible exception of those in which P_m is the octic or the quaternion group. All the groups obtained when P_m is the octic group are evidently simply isomorphic with those obtained when P_m is the quaternion. Hence we need to use only one of these groups for P_m so that we consider only one group for every value of m and p. If this is done, all the groups obtained in this manner are distinct.

The second triply infinite system may be constructed in a somewhat similar manner. Let t' and t_0 represent two independent operators of orders p^{m-2} and p, respectively $(m>3)$ and let s_0 be an operator of order p which satisfies the conditions

$$s_0^{-1}t_0s_0=t_0, \qquad s_0^{-1}t's_0=t_0t_0'.$$

The group $\{t', t_0, s_0\}$ is of order p^m and each of its subgroups is abelian since all the subgroups of order p^{m-1} must include $\{t_0, t'^p\}$. By establishing an isomorphism between the cyclic group of order $p^{m'}$, $m'>m-3$, and $\{t', t_0, s_0\}$

*Cf. MATHIEU, Journal de Liouville (1861), p. 241.

† All the subgroups of such a group must be abelian when $p>2$.

with respect to $\{t_0, t'\}$, we clearly obtain a triply infinite system of non-abelian groups in which every subgroup is abelian by assigning to p, m and m' all possible values. No two of these can be simply isomorphic since t' is a non-invariant operator of lowest order in the simply infinite system for which m and p have given values. No group of this triply infinite system can be simply isomorphic with a group of the triply infinite system considered in the preceding paragraph, because every subgroup of order $p^{m+m'-2}$ in the present system includes $\{t'^p, t_0, s_1^p\}$, where s_1 involves a constituent of the highest order from the cyclic group of order of p, and hence it has three invariants, while there are just two invariants in some subgroup of index p in the preceding system.

Having proved the existence of two triply infinite systems of non-abelian groups in which every subgroup is abelian, and also that no two groups contained in these two systems can be simply isomorphic, it remains to show that (with the exception of a few known ones) every possible group (G) is simply isomorphic with a group in one of these systems. The order of G will be represented by p^a. It will first be proved that G contains just $p+1$ subgroups of order p^{a-1} and that such a subgroup cannot involve more than three invariants.

Let G_1 be any subgroup of order p^{a-1} and let s be one of the smallest operators of G which are not in G_1. Since the order of s is a power of p it must transform some invariant subgroup of order p^β ($\beta = 1, 2, \cdots a-2$) in G_1 into itself. Moreover, it transforms the operators of one of these invariant subgroups into themselves multiplied by just p invariant operators.* As this subgroup and s must generate G, it follows that *the commutator subgroup of G is of order p*. Hence the group of cogredient isomorphisms of G is of order p^2. Since a group of cogredient isomorphisms cannot be cyclic it follows that the pth power of every operator in G is invariant.

As every subgroup of order p^{a-1} is abelian it must include all the invariant operators of G. Hence *G contains just $p+1$ subgroups of order p^{a-1}*. Let t be any non-invariant operator of lowest order in G_1 and let t_0 be one of the $p-1$ commutators of order p. Every subgroup of G which includes t_0 is invariant. Since $\{t, s^p, t_0\}$ and s generate G, it is clear that $\{t, s^p, t_0\} \equiv G_1$. Hence *a subgroup of order p^{a-1} contains at most three invariants.* If there are three, at least one of them is of order p and t_0 may be taken as one of its independent generators.

In case G_1 is cyclic the possible groups are well known and have been noted above. When G_1 has just two invariants it may be assumed that the order of each of them exceeds p, for the groups of order p^m containing an abelian subgroup of order p^{m-1} and type $(m-2, 1)$ are known.* We proceed to consider the other possible groups, when G_1 has just two invariants. From the

* Annals of Mathematics, vol. 3 (1902), p. 180.

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

way in which s and t have been selected, and from the fact that the order of each of the invariants of G_1 exceeds p, it follows that s and t have only identity in common. Hence $G_1 \equiv \{t, s^p\}$. Since t_0 is in G_1, it must be of the form $t_0 = t^m s^{np}$. Hence we may suppose that t and s were so selected that t_0 is a power of one of them.

If t_0 is a power of t it is clear that G is simply isomorphic with one of the groups in the first triply infinite system mentioned above. If t_0 is a power of s we may select a group of order p^{m-1} so as to include s. Since this is abelian it will not include t, and G must again be simply isomorphic with a group of the first system. It remains to prove that every possible group when G_1 has three invariants is simply isomorphic with a group of the second triply infinite system.

We shall hereafter suppose that G_1 has three invariants and includes a non-invariant operater t of lowest order, so that the order of s is equal to or greater than the order of t. Since t and s are independent, it may be assumed that t, s^p, t_0 are the three independent generators of G_1. Hence each of these groups is simply isomorphic with one of the groups of the second triply infinite system. We can evidently establish such a simple isomorphism by choosing the order of t' equal to that of t and the order of the isomorphic cyclic group equal to that of s, and letting t' correspond to t, t_0 to t_0 and a generator of the isomorphic cyclic group to s. Every non-abelian group of order p^α, in which every subgroup is abelian is therefore contained in one or the other of the two triply infinite systems, or else among the groups which contain either an operator of order $p^{\alpha-1}$ or an abelian group of type $(\alpha - 2, 1)$.

STANFORD UNIVERSITY,
April, 1903.