GROUPS POSSESSING A SMALL NUMBER OF SETS OF CONJUGATE OPERATORS*

BY

G. A. MILLER

1. INTRODUCTION

Some properties of a group G can perhaps be most clearly presented by representing G as a kind of independent government. From this point of view every abstract group presents a distinct type of government so that there are as many forms of group governments as there are different abstract groups. The notion of regarding a group as a kind of government is not entirely new. Sophus Lie once divided all continuous transformation groups into two classes which he called *democratic* and *aristocratic* groups respectively,† and Felix Klein called conjugate operators of a group *equal rights* operators.‡

A common property of all finite groups is that every such group has one and only one identity. As a group operator this identity is a kind of figurehead having no effect on the operators with which it is combined. The uniqueness of the identity and the fact that as an operator it has no effect on the operators of G may suggest the appropriateness of regarding it as the king of G, and hence every finite group represents a type of a monarchy. Although the identity is a kind of figurehead it is the most prominent member of G and it is sometimes spoken of as the principal element of G. All the other elements of G are potentially equivalent to this king since some power of every element of a finite group is equal to the identity, but the other elements of G have normally properties which differ widely from those possessed by the identity.

The main objects of the present article are to establish a few general theorems relating to the possible number of sets of conjugate operators in a group of a given order, or the number of different classes of equal rights members of a group government, and to determine all the possible groups having a small number of complete sets of conjugate operators. In particular we shall determine an upper limit for the order of a discontinuous group having a given number of sets of conjugate operators so that every discontinuous

* Presented to the Society, December 27, 1918.

† S. Lie, Berichte der Gesellschaft der Wissenschaften zu Leipzig, vol. 47 (1895), p. 271.

‡ F. Klein, Mathematische Annalen, vol. 14 (1879), p. 430.

group which has a larger order must involve also a larger number of sets of conjugate operators. A striking difference between continuous and discontinuous is thus made clear since the former have always a non-denumerable set* of infinitesimal operators but these operators may appear in a small number of sets of conjugate. In particular, in the democratic groups noted above they appear in a single set.

2. General theorems

Let g represent the order of the group G. The number of operators in any one of the various complete sets of conjugate operators of G is equal to g divided by the order of the subgroup composed of all the operators of G which transform an arbitrary operator of the set into itself. In particular, the number of operators in any one of the complete sets of conjugate operators of G is a divisor of g, and a necessary and sufficient condition that a complete set of conjugate operators consists of a single operator is that this operator is invariant under G. When G is abelian the number of its complete sets of conjugate operators is equal to g and vice versa.

If $g_1, g_2, \cdots, g_k$ are the orders of the subgroups of G which have the property that each subgroup is composed of all the operators of G which transform into itself an operator of a complete set of conjugates and that there is one and only one such subgroup for each complete set of conjugate operators in G, then it results directly that

$$\frac{1}{g_1}+\frac{1}{g_2}+\cdots+\frac{1}{g_k}=1.$$

At least one of these denominators is equal to g since the identity constitutes a complete set of conjugate operators. When g is large the corresponding fraction must be small, and hence k must exceed a certain number. For instance, when $g = 100$ the value of k must exceed 4 since three unit fractions whose sum is as large as 99/100 can not have 100 for their least common denominator.

A maximum value of $g = g_k$ for a given value of k can readily be found as follows: If we assign a number to one of the symbols $g_1, g_2, \cdots, g_{k-1}$ the remaining symbols can assume their largest possible values when the value assigned to the first symbol is as small as possible, since the sum of the reciprocals of these numbers is fixed. Hence the largest possible value of g cannot exceed the number obtained for g_k by assigning to $g_1, g_2, \cdots, g_{k-1}$ in order, the values of the corresponding terms of the following series

$$2, 3, 7, 43, 1807, \cdots,$$

* *Encyclopédie des sciences mathématiques*, tome II, vol. 4, p. 176.

where each term after the first is obtained by multiplying together all the preceding terms and increasing by unity the product thus obtained, since $(n-1)/n + 1/(n+1)$ is of the form $(m-1)/m$. This series increases very rapidly as the number of its terms increases, but it is finite whenever this number is finite. In particular, we have proved the following

THEOREM. *If the number k of complete sets of conjugate operators contained in a group is given then it is always possible to determine another number such that none of the possible discontinuous groups whose operators occur in exactly k complete sets of conjugates can have an order which exceeds this number.* As a special case of this theorem it may be noted that a necessary and sufficient condition that a discontinuous group is of finite order is that the number of its complete sets of conjugate operators is finite.*

In the following section it will be noted that the upper limit for the value of g resulting from the above theorem is usually much too large. When $k = 2$ or 3 the theorem gives the exact value of g, but when $k = 4$ it fixes 42 for an upper limit of the value of g while the actually largest value of $g = 12$, and when $k = 5$ the largest actual value of g is 60 while the upper limit obtained from the theorem is 1806.

A necessary and sufficient condition that G is solvable is that the identity can be attained by forming successive commutator subgroups of G. Let

$$C_1, C_2, \cdots, C_l = 1$$

represent such a successive set of commutator subgroups of a solvable group G and consider the corresponding quotient groups

$$G/C_1, G/C_2, \cdots, G/C_l \equiv G.$$

The number of complete sets of conjugate operators in each of these quotient groups, after the first, must be at least one larger than in the preceding quotient group since each of the successive commutator subgroups includes all those which follow it. In particular, if a solvable group contains a non-abelian commutator subgroup it must involve at least two more complete sets of conjugate operators than its commutator quotient group does.

As C_{l-1} is abelian the number of operators in one of its sets of conjugates under G cannot exceed the order of G/C_{l-1}. If the number of these sets in addition to the identity is α, the order of C_{l-1} cannot exceed 1 plus α times the order of G/C_{l-1}. For solvable groups this furnishes another proof of the

* Cf. E. Landau, Mathematische Annalen, vol. 56 (1903), p. 674. It may be noted that the statement of this theorem as given on p. 199 of vol. 1, second edition, Pascal's *Repertorium der höheren Mathematik*, 1910, is meaningless since the number of the distinct abstract groups of finite order may be regarded as finite irrespective of the number of conjugate sets of operators contained in such groups. The theorem established by Landau does not give a definite upper limit for the order of a group having a fixed number of sets of conjugate operators while such a limit is here established.

fact that a discontinuous group must be of finite order whenever the number of its complete sets of conjugate operators is finite. Some of these results may be stated in the form of a theorem, as follows:

THEOREM. *If the solvable group G has k complete sets of conjugate operators and if the largest solvable group which has $k - \alpha$, $\alpha \geqq 1$, complete sets of conjugate operators is of order q then the order of G cannot exceed $q(\alpha q + 1)$.* In particular, when all the operators besides the identity of any of the successive commutator subgroups are conjugate under G then this commutator subgroup must be C_{l-1} and its order is a power of a prime number.

3. DETERMINATION OF ALL THE GROUPS WHICH INVOLVE NO MORE THAN FIVE SETS OF CONJUGATE OPERATORS

The only finite group which possesses only two sets of conjugate operators, one in addition to the identity, is the group of order 2. In fact, each operator in the second set of conjugates of such a group must be transformed into itself by its powers and hence the number of conjugates in this set cannot exceed $g/2$. As this number must also be $g - 1$ it results that $g = 2$.

If a non-abelian group involves only three complete sets of conjugate operators its order cannot be a power of a prime since the commutator quotient group of a prime power group is always non-cyclic* and hence its order cannot be less than 4. The order of this non-abelian group must therefore be of the form $p^\alpha q^\beta$, p and q being prime numbers. As there are only two sets of conjugate operators besides the identity one of these sets must be composed of operators of order p while the other is composed of operators of order q. The former set contains at most $1/p$ of the operators of G while the latter contains at most $1/q$ of them. Hence it follows that g could not exceed 6 since

$$\frac{1}{g} + \frac{1}{p} + \frac{1}{q} = 1$$

is satisfied only when $g = 6$. It therefore results that *the non-cyclic group of order 6 is the only non-abelian group which involves three and only three complete sets of conjugate operators.*

When the non-abelian group G involves four and only four complete sets of conjugate operators its order cannot be a power of a prime for the reasons stated in the preceding paragraph. This order could not be divisible by three distinct prime numbers since this would imply that the operators in each of the sets of conjugates would be prime and that all the operators of the same prime order would be conjugate. As at least one of these primes p would exceed 3 there would have to be operators in G whose orders would be

*G. A. Miller, Annals of Mathematics, vol. 3 (1902), p. 180; H. Hilton, *Finite Groups*, 1908, p. 146.

divisible by $p-1$, viz., the operators which would transform an operator of order p into a power whose index is a primitive root of p. As these operators would be of composite order we have proved that if the operators of the non-abelian group G appear in exactly four complete sets of conjugates then g is of the form $p^\alpha q^\beta$, p and q being prime numbers. In particular, G must be solvable.

Since G is solvable and involves four complete sets of conjugate operators its commutator quotient group is either of order 2 or of order 3. In the latter case, the commutator subgroup is evidently abelian and its order cannot exceed 4. Hence G must be the tetrahedral group in this case. When the order of the commutator quotient group of G is 2 the commutator subgroup of G must again be abelian; for, if it were non-abelian the quotient group of G with respect to the second commutator subgroup would be non-abelian and it would involve three sets of conjugate operators. Hence it would be the non-cyclic group of order 6, and the order of G could not exceed 42. This order could clearly not be 42 since the group of isomorphisms of the group of order 7 is cyclic. It could not be 24 or 12 as can be readily verified. When the commutator subgroup of G is abelian and the commutator quotient group is of order 2 G must be the dihedral group of order 10 so that *the tetrahedral group and the dihedral group of order* 10 *are the only two non-abelian groups involving exactly four complete sets of conjugate operators.*

When all the operators of the non-abelian group G occur in five complete sets of conjugates G is not necessarily solvable as results directly from the icosahedral group, which involves exactly five complete sets of conjugate operators. We proceed to prove that no other simple group of composite order has this property, and hence we shall assume for the present that G is a simple group. The order of G cannot be divisible by four distinct prime numbers for the reasons given above in connection with the case when all the operators of G appear in four complete sets of conjugates. Hence we may assume that $g = p^\alpha q^\beta r^\gamma$, where p, q, and r represent distinct prime numbers.

It is easy to prove that these prime numbers must be 2, 3, and 5. In fact, one of them must be 2 since at least one of the sets of conjugates is necessarily composed of all the operators of G having the same odd prime order. Moreover, g must be divisible by 4 since every group whose order is the double of an odd number is composite. The number of the operators of order 2 in G can therefore not exceed $g/4$. If both of the other prime factors were greater than 3 G would involve operators of more than four different orders besides the identity. The order of G must therefore be of the form $2^\alpha 3^\beta p^\gamma$, p being a prime number greater than 3.

If all the operators of order $p > 5$ were conjugate the number of operators of each of the orders 2 and $p-1$ contained in G could not exceed $g/(p-1)$

while the operators of orders 3 and p could not exceed $g/3$ and g/p respectively. Since

$$\frac{2}{p-1}+\frac{1}{3}+\frac{1}{p}+\frac{1}{g}<1$$

for $g \geqq 60$ this is impossible. If all the operators of order p were conjugate when $p = 5$ the operators of order 4 contained in G would be transformed into their inverses by operators of order 2 and therefore each of the latter operators would be transformed into itself by at least 8 operators of G. Hence the number of operators of orders 2, 4, 3, and 5 contained in G could not exceed

$$g/8,\ g/4,\ g/3, \text{ and } g/5$$

respectively. As

$$\frac{1}{8}+\frac{1}{4}+\frac{1}{3}+\frac{1}{5}+\frac{1}{g}<1$$

when $g \geqq 60$, the group is impossible.

All the operators of order p contained in G are therefore found in two complete sets of conjugates, and the following equation

$$\frac{1}{4}+\frac{1}{3}+\frac{2}{p}+\frac{1}{g}=1$$

must be satisfied for some value of $g \geqq 60$. This is clearly only possible when $p = 5$ and $g = 60$. That is, *there is one and only one simple group of composite order which has the property that all of its operators appear in five complete sets of conjugates; viz., the icosahedral group.* From this theorem it results directly that no composite insolvable group involves exactly five complete sets of conjugate operators.

In what follows it will be assumed that G is solvable and that it involves five and only five complete sets of conjugate operators. The order of the commutator quotient group of G is therefore one of the three numbers 2, 3, 4. When this order is 4, the commutator subgroup of G must be abelian and have an order which cannot exceed $4 + 1 = 5$. When this order is 5 G is the metacyclic group of order 20. When this order is 2 G is either the octic group or the quaternion group. There are therefore *three and only three non-abelian groups whose operators appear in exactly five complete sets of conjugates and whose commutator quotient group is of order* 4, *viz., the octic group, the quaternion group, and the metacyclic group of order* 20.

When the commutator quotient group of G is of order 3 its commutator subgroup must again be abelian, for if this commutator subgroup were non-abelian the quotient group of G with respect to its second commutator subgroup would be non-abelian and would involve four complete sets of conjugate operators. As its commutator quotient group would be of order 3 it would

be the tetrahedral group. Moreover, the second commutator subgroup of G would be abelian since all of its operators besides the identity would be conjugate under G. The order of this subgroup could therefore not exceed 13. It could not be 13 since the group of isomorphisms of the group of order 13 is cyclic. For a similar reason it could not be 7 or 5. If it were 4, G would be of order 48 and its subgroup of order 16 would be non-abelian, contain 12 operators of order 4 which would be conjugate under G, and have three invariant commutators of order 2. As this is impossible the second commutator subgroup of G could not be of order 4. As this order could clearly not be 2 or 3 it results that the commutator subgroup of G must be abelian and that *the non-cyclic group of order* 21 *is the only group whose operators appear in exactly five complete sets of conjugates and whose commutator quotient group is of order* 3.

It remains to consider the case when the solvable non-abelian group G involves exactly five complete sets of conjugate operators and when the commutator quotient group of G is of order 2. The special case when the commutator subgroup of G is abelian is easily disposed of since G could then not exceed 14 and the dihedral group of order 14 is evidently the only one that satisfies these conditions. Hence we shall assume in what follows that the commutator subgroup H of G is non-abelian. We proceed to prove that the commutator subgroup of H, or the second commutator subgroup of G, must be abelian.

If the commutator subgroup of H were non-abelian the quotient group of G with respect to the commutator subgroup of this commutator subgroup would involve four complete sets of conjugates and have an $(\alpha, 1)$ isomorphism with the non-cyclic group of order 6. As neither of the two non-abelian groups involving exactly four complete sets of conjugate operators has the latter property the commutator subgroup of H must be abelian. Moreover, the quotient group of G with respect to this abelian subgroup must be non-abelian and cannot involve more than four complete sets of conjugate operators. As this quotient group involves a subgroup of index 2 it is either the non-cyclic group of order 6 or the non-cyclic group of order 10.

It could not be the non-abelian group of order 10 since all the operators of G corresponding to the same non-identity operator of this quotient group would be conjugate under G and the subgroup of G corresponding to the identity in this quotient group would have an order which could not exceed 11. Hence it remains only to consider the case when the quotient group of G with respect to its second commutator subgroup is the non-abelian group of order 6. Since this commutator subgroup is abelian and its order could clearly not be 7 its order must be 4 and G must be the group of the cube. *There are therefore exactly seven non-abelian groups whose operators occur in five and only five complete sets of conjugates.* One of these is insolvable and

the remaining six are solvable. Three of the latter have a commutator quotient group of order 4, in two of them this quotient group is of order 2, and in the remaining one it is of order 3.

4. Complete sets of conjugate operators under the group of isomorphisms

A group G may contain operators which are not conjugate under G but are conjugate under the group of isomorphisms of G. These operators may be said to be implicitly equal rights operators while those which are conjugate under G are explicitly equal rights operators. In the present section we shall call operators of G conjugate if they are conjugate under the group of isomorphisms of G, and shall especially consider those groups which do not involve more than three complete sets of such conjugate operators. The identity clearly constitutes a complete set under the group of isomorphisms of G as well as under G itself.

A necessary and sufficient condition that G contains only one complete set of conjugate operators besides the identity is that it is an abelian group of prime power order and of type $(1, 1, 1, \cdots)$, and a necessary and sufficient condition that an abelian group has exactly two complete sets of conjugate operators besides the identity is that it is a prime power group and of type $(2, 2, 2, \cdots)$. Hence we shall assume in what follows that G is non-abelian and that it has exactly two complete sets of conjugate operators besides the identity.

The order g of G can clearly not be divisible by more than two distinct prime numbers and hence G must be solvable. If g is of the form $p^\alpha q^\beta$, p and q being distinct primes and $\alpha, \beta \geqq 1$, the commutator subgroup C of G must be abelian and of type $(1, 1, 1, \cdots)$ and must be a Sylow subgroup of G. Hence we may assume that the order of C is p^α and that the order of the commutator quotient group is q^β. The latter group is evidently also abelian and of type $(1, 1, 1, \cdots)$. It results therefore that G contains only one Sylow subgroup of order p^α and that its Sylow subgroups of order q^γ are abelian and of type $(1, 1, 1, \cdots)$.

As none of the operators of C, except the identity, can be transformed into itself by an operator of order q contained in G it results that $p^\alpha - 1$ is divisible by q^β. A subgroup of order q^β cannot be transformed into itself by any operator besides the identity of the subgroup of order p^α. In fact, if a subgroup of order q^β were transformed into itself by a group of order p^γ, $\gamma > 0$, G would contain a subgroup of order $p^\gamma q^\beta$ which would involve only $p^\gamma - 1$ operators whose orders are divisible by p. Hence this subgroup would involve an invariant subgroup of each of the orders p^α and q^β. As these subgroups have only the identity in common every operator of the one

would be commutative with every operator of the other. This is impossible since G involves no operator whose order is pq. Hence G contains p^α subgroups of order q^β.

That the value of β must be 1 may be proved as follows: The group of isomorphisms of the abelian group of order p^α and of type $(1, 1, 1, \cdots)$ contains at least one cyclic group of order $p^\alpha - 1$. In fact, when $\alpha > 1$ it is well known that this group of isomorphisms contains more than one such cyclic group. As the order of this group of isomorphisms is

$$(p^\alpha - 1)(p^\alpha - p)(p^\alpha - p^2)\cdots(p^\alpha - p^{\alpha-1})$$

it is clear that its subgroup of order q^β is cyclic unless $p^\gamma - 1$, $\gamma < \alpha$, is divisible by q. When this subgroup is non-cyclic it must involve operators which are commutative with some of the operators of order p in the group of order p^α. Since the group of order q^β in the present case is known to be non-cyclic whenever $\beta > 1$ we have established the following

THEOREM. *If all the operators besides the identity of a non-abelian group belong to two sets of conjugates under its group of isomorphisms the order of this group is either of the form p^α or of the form $p^\alpha q$, p and q being prime numbers.*

As an illustration of an infinite system composed entirely of groups having separately only two systems of conjugate operators besides the identity under their respective groups of isomorphisms we may cite the groups of order $2p^\alpha$, $p > 2$, obtained by extending every abelian group of order p^α and of type $(1, 1, 1, \cdots)$ by means of an operator of order 2 which transforms each of the operators of this abelian group into its inverse. On the other hand, it is easy to construct groups of order $p^\alpha q$ involving only operators of order p and q besides the identity but having more than three systems of conjugate operators under their groups of isomorphisms.

To obtain such a group we may assume $p = 2$ and q any prime number of the form $2^\alpha - 1$, $\alpha > 2$. It is known that the group of isomorphisms of the abelian group of order 2^α and of type $(1, 1, 1, \cdots)$ is simple and hence it cannot involve negative substitutions. This group of order $2^\alpha q$ can be represented as a substitution group of degree $2^\alpha - 1$. As it contains no negative substitutions it cannot contain any substitutions which transform the cycles of order q into their inverses. Hence the groups of order $2^\alpha q$, where $q = 2^\alpha - 1$ and $\alpha > 2$, which involve only operators of orders 2 and q in addition to the identity, do not permit isomorphisms in which each operator of order q is made to correspond with every other operator of this order. The smallest group coming under this theorem is of order 56.

When a non-abelian group G of order p^α is such that all of its operators appear in three sets of conjugates under its group of isomorphisms all of its commutators besides the identity must constitute one such set. Since at least

one non-identity commutator of every non-abelian prime power group is invariant under the group all the commutators of G must be invariant operators under G. Hence the commutator subgroup of G must coincide with its central and all the operators of G besides the identity must be of order p or of order p^2. When $p = 2$ operators of the latter order must occur in G but this is not necessarily true when $p > 2$.

We shall first consider the case when operators of order p^2 occur in G. If p^β and p^γ represent respectively the orders of the commutator subgroup and of the commutator quotient group of G it is easy to prove that $\beta = \gamma$ when $p > 2$, and that β is a divisor of γ when $p = 2$. In fact, when $p > 2$ the pth power of the product of any two operators of order p^2 contained in G is the product of the pth powers of these operators since their commutator is invariant and of order p.* Hence all the operators of G which have the same pth power must appear in the same coset with respect to the central of G. Moreover, all the operators of order p contained in the central of G must be pth powers of operators of order p^2 contained in G since the operators of order p are conjugate under the group of isomorphisms of G. These conditions imply the following

THEOREM. *If a non-abelian group of order p^α, $p > 2$ involves operators of order p^2 and has the property that all of its operators occur in three complete sets of conjugates under its group of isomorphisms then its commutator subgroup is of order $p^{\alpha/2}$.*

When $p = 2$ it is not necessarily true that $\beta = \gamma$ as results directly from the quaternion group. The squares of the operators in the same coset with respect to the commutator subgroup are evidently equal to each other and the number of such different cosets whose operators have the same square is clearly the same for the various operators of order 2 contained in G since all of the latter are conjugate under the group of isomorphisms of G. This implies that

$$\frac{2^\gamma - 1}{2^\beta - 1}$$

is an integer, which is possible only when γ is a multiple of β.

It is not difficult to prove that α is necessarily odd whenever G involves operators of order p^2 and $p > 2$. In fact, the independent generators of the commutator subgroup of G are the commutators of pairs of operators corresponding to independent generators of the quotient group of G. Hence the number of the pairs of the latter generators must be divisible by the number of the former generators since the latter number is equal to the number of the independent generators in the quotient group of G. As the first of these numbers is divisible by the second only when β is odd there results the

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

THEOREM. *If a non-abelian group of order p^α, $p > 2$, involves operators of order p^2 and has the property that all of its operators appear in three sets of conjugates under its group of isomorphisms then α is the double of an odd number.*

The preceding considerations establish the fact that the number of the independent generators of the commutator subgroup of G is always a divisor of the number of the pairs of independent generators in the commutator quotient group of G, but when G does not involve operators of order p^2 or when $p = 2$ the order of the commutator subgroup of G need not be equal to the order of its commutator quotient group as results directly from the fact that there is one and only one group of order p^3, p any prime number, which has the property that all of its operators appear in three sets of conjugates under its group of isomorphisms. When $p = 2$ this is the quaternion group and when $p > 2$ it is the non-abelian group which involves no operator of order p^2. There is also one and only one group of order p^4 for every value of p which has the given properties but this group is necessarily abelian.

When the commutator subgroup of G is of order $p > 2$ the independent generators of the commutator quotient group of G can be so selected that the operators of G which correspond to any one of them are commutative with those corresponding to each of the others save one. Hence the commutator quotient group of G must be of even order while α is an odd number. Moreover α can evidently be an arbitrary odd number > 1 for a G having a commutator subgroup of order p.* All of these groups involve only operators of order p besides the identity since all the non-invariant operators of G are conjugate under its group of isomorphisms. It results therefore that *there is at least one group of order p^α, $\alpha > 1$ and $p > 2$, which has the property that all of its operators appear in three sets of conjugates under its group of isomorphisms.*

When $p = 2$ and 2^β is the order of the commutator subgroup of G while 2^γ is the order of its commutator quotient group it was noted above that γ is divisible by β and that β must also be a divisor of the number of pairs that can be formed with γ objects whenever G is non-abelian. As $\alpha = \beta + \gamma$ it results directly that α cannot be equal to 5 since γ cannot excel 2 when $\beta = 1$.† That is, the smallest order of the form 2^α, $\alpha > 1$, for which there is no group whose operators appear in three sets of conjugates under the group of isomorphisms is 32.

* J. W. A. Young, American Journal of Mathematics, vol. 15 (1893), p. 171.

† Miller, Blichfeldt, Dickson, *Finite Groups*, 1916, p. 127.