# THE $\phi$-SUBGROUP OF A GROUP*

BY

G. A. MILLER

## 1. INTRODUCTION

Any set of operators belonging to any group $G$ of finite order is called a set of independent generators of $G$ provided that these operators generate $G$ and that none of them is contained in the group generated by the rest of them. All the operators of $G$ can be divided into two categories, having no common operator, by putting into one category all those which occur in at least one of the possible sets of independent generators of $G$, and into the other category those which do not have this property. The operators of the second category constitute a characteristic subgroup of $G$, which has been called† by G. Frattini the *$\phi$-subgroup of $G$*.

If $H$ is any maximal subgroup of $G$ it is evidently always possible to select at least one set of independent generators of $G$ in such a manner that it includes any arbitrary one of the operators of $G$ which are not contained in $H$ while the remaining operators of the set belong to $H$. Moreover, there is at least one maximal subgroup of $G$ which does not include any given one of the independent generators of a particular set of independent generators of $G$. Hence it results that the $\phi$-subgroup of $G$ is the cross-cut of all the maximal subgroups of $G$. This useful second definition of the $\phi$-subgroup is also due to Frattini.

As every maximal subgroup of a group of order $p^m$, $p$ being a prime number, is of order $p^{m-1}$, it results directly from this second definition that *the $\phi$-subgroup of any group of order $p^m$ is the cross-cut of all its subgroups of index $p$*. It results from this that the $\phi$-subgroup of a group of order $p^m$ may also be defined as its smallest invariant subgroup which gives rise to an abelian quotient group of type $(1, 1, 1, \cdots)$.‡ If the order of this quotient group is $p^\alpha$, it results that $\alpha$ is the number of independent generators in every possible set of independent generators of this group of order $p^m$. In particular, *if the*

* Presented to the Society, September 8, 1914.

† G. Frattini, Atti della Reale Accademia dei Lincei, Rendiconti, ser. 4, vol. 1 (1885), p. 281.

‡ M. Bauer, Nouvelles Annales de Mathématiques, ser. 3, vol. 19 (1900), p. 509.

*order of $G$ is $p^m$, $p$ being any prime number, every possible set of independent generators of $G$ involves the same number of operators.* That is, the number of operators in each of the possible sets of independent generators of any Sylow group is an *invariant* of the group.

From the preceding paragraph it results directly that a necessary and sufficient condition that the $\phi$-subgroup of a given group of order $p^m$ be the identity is that this group be the abelian group of type $(1, 1, 1, \cdots)$. Hence there is one and only one group of order $p^m$, $p$ being any prime number and $m$ being any positive integer, which has the identity for its $\phi$-subgroup. The number of operators in every set of independent generators of this group is $m$. In every other group of order $p^m$ the number of these independent generators is less than $m$, and there is at least one group of order $p^m$ in which this number is any arbitrary positive integer from 1 to $m$.

If a $\phi$-subgroup of the group $G$ involves a non-invariant subgroup or a non-invariant operator this subgroup or operator cannot be transformed into all its conjugates under $G$ by the operators of the $\phi$-subgroup. That is, every complete set of conjugates of the $\phi$-subgroup is an incomplete set of conjugates under $G$ whenever the former set involves more than one element. If this were not the case all the operators of $G$ which would transform one of these elements into itself would form a subgroup which would not involve all the operators of the $\phi$-subgroup of $G$. This subgroup could not be maximal since it does not involve the $\phi$-subgroup. As any maximal subgroup obtained by extending this subgroup by means of operators of $G$ could also not involve the $\phi$-subgroup we have proved the theorem: *If the $\phi$-subgroup of a group $G$ involves a non-invariant operator or subgroup, the number of conjugates under $G$ of this operator or subgroup is greater than the number of the corresponding conjugates under the $\phi$-subgroup.*

An important special case of this theorem was noted by Frattini who observed that the $\phi$-subgroup of any group involves only one Sylow subgroup for every prime which divides the order of the $\phi$-subgroup. In other words, every $\phi$-subgroup is the direct product of its Sylow subgroups, and hence we can always reach the identity by forming successive $\phi$-subgroups, starting with any given group. If a group can be represented as a non-regular primitive substitution group of degree $n$, its $n$ subgroups of degree $n - 1$, composed of all its substitutions which omit a letter, are maximal and have only the identity in common. Hence it results that *the $\phi$-subgroup of every primitive substitution group is the identity.*

While the number of the possible independent generators of a group whose order is a power of a prime is an invariant of the group, this number is not always an invariant as regards other groups. For instance, it is evident that if we use transpositions as independent generators of the symmetric group

of degree $n$ the number of these generators is always $n - 1$. On the other hand, this number is always two if we use a cyclic substitution of degree $n - 1$ and a transposition involving the remaining letter as the independent generators of this symmetric group. Hence it results that it is possible to select a set of independent generators of the symmetric group of degree $n$ so that the number of operators in the set is an arbitrary integer from 2 to $n - 1$.

## 2. The $\phi$-subgroup of an abelian group

If $G$ is an abelian group of order $p^m$, $p$ being any prime number, the $\phi$-subgroup of $G$ is the subgroup composed of the distinct operators obtained by raising every operator of $G$ to its $p$th power. As a *reduced set of independent generators** of this $\phi$-subgroup we may therefore take the $p$th powers of each operator whose order exceeds $p$ in any reduced set of independent generators of $G$. The order of the $\phi$-subgroup of $G$ is therefore $p^{m-\alpha}$, $\alpha$ being the number of the invariants of $G$. In other words, $p^\alpha$ is the order of the subgroup of $G$ generated by all of its operators of order $p$.

If any group (abelian or non-abelian) is the direct product of two groups it results that the direct product of one of these two factor groups and a maximal subgroup of the other is a maximal subgroup of the original group. Since the $\phi$-subgroup of any group is both invariant and occurs in every maximal subgroup it results, as was observed by G. Frattini, that *every maximal invariant subgroup of any group (abelian or non-abelian) involves the $\phi$-subgroup of this group.* By combining these two results we have a proof of the following useful theorem.

Theorem. *The $\phi$-subgroup of the direct product of any two groups (abelian or non-abelian) is the direct product of the $\phi$-subgroups of these two groups.*

As every abelian group whose order is not a power of a prime number is the direct product of its Sylow subgroups it results directly from the preceding theorem that the $\phi$-subgroup of any abelian group is the direct product of the $\phi$-subgroups of its Sylow subgroups. A necessary and sufficient condition that the $\phi$-subgroup of an abelian group be the identity is that each of its Sylow subgroups be of type $(1, 1, 1, \cdots)$. There is therefore one and only one abelian group of every possible order which has the identity for its $\phi$-subgroup.

If $s_1, s_2, \cdots, s_\lambda$ is any set of independent generators of an abelian group $G$ of order $p^m$, it is easy to derive a *reduced* set of $\lambda$ independent generators from the given set. In fact, any operator of highest order in this set may be selected

* A reduced set of independent generators is characterized by the fact that the group generated by all except one of these generators has only the identity in common with the group generated by the remaining generators irrespective of the choice of this remaining generator.

for the first operator in the required reduced set. To find a second operator of the reduced set we select one of the remaining operators of the given set such that it must be raised to the highest possible power to be contained in the group generated by the determined operator of the required reduced set. The index of this highest power is clearly the order of a second independent generator of the group generated by the two selected operators, if the first of these operators is selected as one of its two independent generators. This second independent generator may then be used as the second operator of the required reduced set. This process is clearly similar to a well-known process to find a set of independent generators of an abelian group of order $p^m$, and can be continued until the $\lambda$ operators of the required reduced set have been determined.

When the order of an abelian group is not a power of a prime number, the number of operators in a set of independent generators (reduced or non-reduced) may vary from the rank of the group to the sum of the ranks of its Sylow subgroups. By repeating the process explained in the preceding paragraph as many times as there are different prime divisors of the order of this abelian group, it results that we can find a reduced set of $\lambda$ independent generators of any abelian group from any given set of $\lambda$ independent generators. In speaking of abelian groups it is customary to use the term set of independent generators for *reduced* set of independent generators. The fact that non-abelian groups do not always possess a reduced set of independent generators may be illustrated by means of the Hamiltonian groups. It is evident that none of these groups has a reduced set of independent generators.

From the first paragraph of this section it is easy to derive a method to obtain the $\phi$-subgroup of any abelian group of order $g$. In fact, it is only necessary to raise each operator of this abelian group to a power whose index involves all the prime factors of $g$ but is not divisible by the square of one of these prime factors. To obtain a set of independent generators of the $\phi$-subgroup of any abelian group of order $g$ it is only necessary to raise each operator of a set of independent generators of the group to the given power and to reject those operators which reduce to the identity when they are raised to this power. *The order of the $\phi$-subgroup of any abelian group of order $g$ is therefore equal to $g$ divided by the order of the subgroup generated by all the operators of prime orders contained in this abelian group.**

## 3. The $\phi$-subgroups of the Sylow subgroups of the symmetric group

We shall begin with the case when $G$ is a Sylow subgroup of order $p^m$ contained in the symmetric group of degree $p^\alpha$. Hence $G$ is a transitive substi-

* Cf. G. Frattini, Atti della Reale Accademia dei Lincei, Rendiconti, ser. 4, vol. 2 (1886), p. 18.

tution group. In the special case when $\alpha = 2$ the value of $m$ is clearly $p + 1$, and the order of the commutator subgroup of $G$ is $p^{p-1}$, since a cyclic substitution of degree $p$ is transformed under $G$ into itself multiplied by a substitution consisting of two cycles of degree $p$. As the $\phi$-subgroup of every group of order $p^m$ includes the commutator subgroup of this group, it results directly that each of the Sylow subgroups of order $p^m$ contained in the symmetric group of degree $p^2$ has exactly two independent generators.

It is well known that a Sylow subgroup of order $p^m$, contained in the symmetric group of degree $p^\alpha$, may be constructed by forming the direct product of $p$ Sylow subgroups of symmetric groups of degree $p^{\alpha-1}$ written on distinct sets of letters and extending this direct product by a substitution of order $p$ which interchanges its $p$ systems of intransitivity and transforms it into itself.* Hence it results directly that the index of the commutator subgroup of a Sylow subgroup of order $p^m$ contained in the symmetric group of degree $p^\alpha$ is $p$ times the index of the commutator subgroup of a Sylow subgroup of the symmetric group of degree $p^{\alpha-1}$. As the commutator subgroup of such a Sylow subgroup involves the $p$th power of every substitution of the group it results that the number of operators in a set of independent generators of a Sylow subgroup of order $p^m$ contained in the symmetric group of degree $p^\alpha$ is always $\alpha$.

It is now easy to determine the number of the operators in a set of independent generators of any Sylow subgroup of the symmetric group of degree $n$. In fact, if we write $n$ in the form

$$n = a_1 p^{\alpha_1} + a_2 p^{\alpha_2} + \cdots + a_l$$

where $\alpha_1, \alpha_2, \cdots$ are positive integers in descending order of magnitude, and all of the coefficients $a_1, a_2, \cdots, a_l$ are positive integers which are less than $p$, then the Sylow subgroup of order $p^m$ contained in the symmetric group of degree $n$ is the direct product of $a_1$ transitive constituents of degree $p^{\alpha_1}$, $a_2$ transitive constituents of degree $p^{\alpha_2}$, etc. As the commutator subgroup of a direct product is the direct product of the commutator subgroups of the factors, it results from the preceding paragraphs that *the Sylow subgroup of order $p^m$ contained in the symmetric group of degree*

$$n = a_1 p^{\alpha_1} + a_2 p^{\alpha_1-1} + \cdots + a_{\alpha_1} p + a_{\alpha_1+1}$$

*has $m' = a_1 \alpha_1 + a_2(\alpha_1 - 1) + \cdots + a_{\alpha_1}$ independent generators, where the coefficients $a_1, a_2, \cdots, a_{\alpha_1}$ are either 0 or positive integers less than $p$, and $\alpha_1$ is a positive integer.* The order of the $\phi$-subgroup of a Sylow subgroup of order $p^m$ contained in the symmetric group of degree $n$ is therefore $p^{m-m'}$.

It results directly from what precedes that the $\phi$-subgroup of an intransitive

* G. A. Miller, American Journal of Mathematics, vol. 23 (1901), p. 173.

Sylow subgroup of a symmetric group is the direct product of the $\phi$-subgroups of its transitive constituents, and that the $\phi$-subgroup of one of these transitive constituents of degree $p^\alpha$, $\alpha > 1$, is an intransitive group with $p$ transitive constituents which may be constructed as follows: Write a Sylow subgroup of the symmetric group of degree $p^{\alpha-1}$ on $p$ distinct sets of letters, and construct an isomorphism between one of these $p$ groups and each of the others in such a way that the $p - 1$ resulting groups of degree $2p^{\alpha-1}$ involve the direct products of the commutator subgroups of their transitive constituents, while the operators of their commutator quotient groups correspond to their inverses. The $\phi$-subgroup of the given transitive group of degree $p^\alpha$ is the direct product of the $p - 1$ intransitive groups constructed in this manner.

## 4. Various sets of independent generators of any group

The number of ways of choosing a set of independent generators of a given group is generally very large. As regards an abelian group of order $p^m$, $p$ being a prime number, it is well known that the number of possible choices of a reduced set of independent generators is equal to the order of the group of isomorphisms of this abelian group.* As regards non-abelian groups, in general, the matter becomes much more complex. In fact, the number of operators in the various possible reduced sets of independent generators is not necessarily the same since this number may evidently vary from 2 to $n - 1$ in the symmetric group of degree $n$, as was observed in the Introduction.

If a set of independent generators is so selected that the number of these generators is as large as possible it may be assumed that the order of each of these generators is a power of a prime number. That is, there is always at least one set of independent generators, involving the largest possible number of distinct operators, such that the order of each of these generators is a power of some prime number. In fact, if $s_1, s_2, \cdots, s_\lambda$ is a set of independent generators of $G$ such that $\lambda$ is a maximum, and if the order of $s_\alpha$, $1 \leqq \alpha \leqq \lambda$, is not a power of a prime, it results that $s_\alpha = s'_\alpha \cdot s''_\alpha$ where it may be assumed that $s'_\alpha$ has an order which is a power of a prime and that the order of $s''_\alpha$ is prime to that of $s'_\alpha$.

When at least one of the two groups generated by the two sets of $\lambda$ operators, obtained by replacing successively $s_\alpha$, in the given set, by $s'_\alpha$ and $s''_\alpha$ coincides with $G$ the number of prime factors of the order of one of the independent generators in a set of $\lambda$ independent generators of $G$ has been reduced. If neither of these two groups would coincide with $G$ we could replace $s_\alpha$ in the first set by the two operators $s'_\alpha$ and $s''_\alpha$. Hence the given set would not have

*Cf. Bulletin of the American Mathematical Society, vol. 20 (1914), p. 360.

contained a maximum number of independent generators. The main result just proved may be embodied in a theorem as follows: *Among the possible sets of independent generators which involve a maximal number of operators there is at least one set in which the order of every operator is a power of some prime number.*

Let $G$ be an intransitive substitution group and consider a set of independent generators of $G$ such that this set involves the largest possible number of substitutions. If $H$ is any transitive constituent of $G$, and if we select from the given set of generators of $G$ any sub-set of operators which involve as their constituents from $H$ a set of independent generators of $H$, then it is evident that all the other independent generators of $G$ can be selected so as not to involve any letter from $H$. Moreover, this selection can always be so made as to preserve the number of operators in the sets of independent generators under consideration. Hence it results that *the number of operators in a set of independent generators of an intransitive substitution group cannot exceed the largest sum which can be obtained by adding the numbers of the operators in some one set of possible independent generators of each transitive constituent.*

It has been observed that the number of the operators in a set of independent generators of a group of order $p^m$ is an invariant of the group. When this number is $m$ the group is abelian and of type $(1, 1, \cdots)$. The other extreme case is when this number is unity and the group is cyclic. In each of these extreme cases there is only one possible group, but there exists clearly more than one possible group in every other case. In fact, there is at least one abelian and at least one non-abelian group in every other case. In the particular case when the number of these independent generators is $m - 1$ the possible abelian group has one invariant which is equal to $p^2$ while each of the other invariants is equal to $p$. The number of the possible non-abelian groups of order $p^m$ which have $m - 1$ independent generators increases without limit as $m$ increases.