# NUMBER OF CYCLES OF THE SAME ORDER IN ANY GIVEN SUBSTITUTION GROUP*

BY G. A. MILLER

1. *Introduction.* If $G$ is a transitive substitution group and if the subgroup composed of all the substitutions of $G$ which omit a given letter is of degree $n-\alpha$, then there are exactly $\alpha$ substitutions involving no letters except possibly those of $G$ which are commutative with every substitution of $G$. These $\alpha$ substitutions include the identity. If $\alpha > 1$ the remaining $\alpha-1$ substitutions may or may not appear in $G$. From this well known theorem, it follows directly that $G$ involves exactly $\alpha-1$ sets of conjugate cycles which are such that no two distinct cycles of the set have a common letter. Each of these cycles appears in $g/n$ different substitutions of $G$, where $g$ denotes the order of $G$. A necessary and sufficient condition that a transitive substitution group be regular is that no two of its sets of conjugate cycles have a common letter.

When no two conjugate cycles of $G$ have a letter in common it is evident that every pair of cycles in a set of conjugates must be commutative, but these cycles may also be commutative when $G$ is non-regular. When $G$ involves at least one set of conjugate cycles which has the property that every pair of cycles in the set is composed of commutative cycles, $G$ must be imprimitive unless all these cycles involve the same letters and are also of prime order. In this special case, $G$ is evidently always primitive. From the fact that a cycle of prime degree $p$ is transformed into each of its various powers which are incongruent to 1 (mod $p$) only by substitutions of degree $p-1$ on the letters of this cycle it results directly that such substitutions involve cycles

* Presented to the Society, December 29, 1923.

that are not commutative for every such power. Hence we have the following theorem.

THEOREM I. *If every set of conjugate cycles of a transitive substitution group is composed of relatively commutative cycles, then the subgroups composed separately of all the substitutions of the group which omit a letter must omit a number of letters which is divisible by the product of the prime factors of the order of the group.*

In particular, it results from this theorem that a transitive group which has the property that all of its sets of conjugate cycles are composed of cycles that are relatively commutative must also involve at least one set of conjugate cycles that is composed of cycles such that no two of them have a common letter.

Suppose that $G$ is intransitive and involves $\lambda$ transitive constituents of orders $g_1, g_2, \ldots, g_\lambda$, respectively. Let $k$ represent the order of an arbitary cycle of some substitution of $G$. From the fact that the number of the letters contained in every set of conjugate cycles of any substitution group is equal to the order of the group, whenever each cycle is counted for every substitution in which it appears, it results directly that the numbers of the cycles of order $k$ in the transitive constituents of $G$ are, respectively,

$$\frac{m_1 g_1}{k}, \quad \frac{m_2 g_2}{k}, \quad \ldots, \quad \frac{m_\lambda g_\lambda}{k},$$

where $m_1, m_2, \ldots, m_\lambda$ are positive integers or zero, and that the number of cycles of order $k$ contained in $G$ is $mg/k$, where $g$ is the order of $G$ and $m = m_1 + m_2 + \cdots + m_\lambda$. It should be noted that this theorem is independent of the way in which $G$ is constructed by means of its transitive constituents, and that there are an infinite number of possible groups for every arbitrary pair of values of $m$ and $k$, since all of the cycles of the same order contained in the symmetric group of degree $n$ are conjugate under this group.

In particular, it results from the theorem noted above that if at least two of the transitive constituents of $G$ in-

volve cycles of the same order, the number of letters found in all of the cycles of this order contained in $G$ must always exceed the order of $G$, each cycle being counted for every substitution in which it appears. It is evident that the numbers $m_1, m_2, \ldots, m_\lambda$, cannot exceed the degrees of the corresponding transitive constituents diminished by one, and when they attain these maximal values $k$ must be a prime number $p$ and all the cycles of the corresponding constituents must be of order $p$. In particular, the order of such a constituent must be of the form $p^m$. It should also be noted that all the substitutions of a given order $k$ may be conjugate under the group while the cycles of this order do not constitute a single set of conjugates, and that conversely all the cycles of order $k$ contained in a group may constitute a single set of conjugates while the substitutions of this order do not have this property.

2. *Smallest Number of Cycles of Order $p$ in a Substitution Group of Order $p^m$.* If $G$ is a substitution group of order $p^m$, where $p$ is a prime number, it results directly from the theorems noted above that the number of cycles of order $p$ contained in $G$ cannot be less than $g/p$, and this minimum can be attained only when $G$ is transitive. It is also evident that this minimum cannot be attained unless $p = 2$, since all the cycles of order $p$ must be conjugate under $G$ when it is attained. Hence we shall assume in the rest of this section, unless the contrary is stated, that $p = 2$, and that the number of the transpositions contained in the substitutions of $G$ is exactly $g/2$.

Since all of these transpositions are conjugate under $G$, they must appear in an invariant substitution of $G$. In fact, in every substitution group of order $p^m$, where $p$ is any prime number, all the cycles of order $p$ that appear in an invariant substitution of order $p$ constitute a complete set of conjugates and must therefore appear in more than one substitution whenever the group is non-regular. In the particular case under consideration, $G$ involves only

one set of conjugate cycles of order 2, and hence the substitutions of order 2 contained in $G$, if there is more than one such substitution, generate an abelian invariant sub-group.

Except in the trivial case when $g = 2$ there must be a substitution $s$ of order 4 in $G$ which permutes all the transpositions of the invariant substitution of order 2 contained in $G$, since the transitive group according to which these transpositions are transformed contains an invariant substitution of order 2. The group generated by $s$ and the substitutions contained in $G$ whose orders divide 2, is composed of substitutions of order 4 and of degree $n$, where $n$ is the degree of $G$, in addition to the subgroup composed of the substitutions whose orders divide 2. Hence all of the substitutions of order 4 have a common square and the group generated by them is abelian.

If $G$ involves no substitutions whose orders exceed 4, the cycles of the invariant substitution of order 2 contained in the transitive group $G$ must be transformed under $G$ according to a regular group, since this group is transitive and involves only substitutions of order 2 besides the identity. Hence all of the substitutions of order 4 must have a common square and $G$ can involve only one substitution of order 2, as otherwise all of the subgroups corresponding to subgroups of order 2 in the regular group according to which the cycles of order 2 are permuted could not be abelian. The order of this regular group cannot exceed 4, since a substitution of order 4 must transform into its inverse every substitution of this order which is not generated by it. This proves the following theorem.

THEOREM II. *If a transitive substitution group of order $p^m$, where $p$ is a prime number, involves no substitution of order $p^3$, and if the number of its cycles of order $p$ is $p^{m-1}$, then it must be regular and simply isomorphic with one of the following three groups: the quaternion group, the cyclic group of order 4, or the group of order 2.*

When $m = n-2$ for the cycles of a given order $k$ found in the transitive group $G$ of degree $n$, $m$ must be unity for

the cycles of the other possible order and the latter cycles must constitute a single set of conjugates under $G$. It was noted above that $k$ is either 2 or 4 when the order of $G$ is a power of a prime number. From the theorem at the end of § 1, it results that when $k = 2$, $G$ must be one of three groups. The fact that $G$ must be the octic group when $k = 4$ will be proved in the following section.

3. *Minimum Number of Cycles of Order* 4. When the cycles of order 4 in the transitive group $G$ constitute a single set of conjugates, the subgroup composed of all the substitutions of $G$ which omit a letter must involve at least one substitution besides the identity which omits at least two letters, since $G$ cannot be regular and each of the cycles of the invariant substitution of order 2 contained in $G$ is of order 2. It will first be proved that the cycles of order 2 found in the squares of the cycles of order 4 contained in $G$ may be assumed to appear in the invariant substitution of order 2.

If this were not the case none of these squares could be commutative with all the cycles of this invariant substitution, and hence these cycles would be transformed according to cycles of order 4 by the cycles of order 4 contained in $G$. The transitive group according to which these cycles are transformed has a degree which is one-half the degree of $G$, and hence two cycles of order 4 in $G$ would correspond to one cycle of this order in this transitive group. The cycles of order 4 in $G$ would therefore be transformed under $G$ according to an imprimitive group having two letters in each of these systems of imprimitivity. In the transitive group according to which these cycles would be transformed, there would therefore be again a single set of conjugate cycles of order 4, while each of the remaining cycles would be of order 2. Since this transitive group would have a lower order than the original group, we may assume for the time being that $G$ is a transitive group of lowest order having the properties

in question, and hence the squares of its cycles of order 4 are found in the invariant substitution of order 2.

Since the substitutions of $G$ transform the cycles of the invariant substitution of order 2 according to a group which contains only operators of order 2, this group must be abelian; and since it is transitive, it must also be regular. If it is of order 2, $G$ must be the octic group. If its order exceeds 2, the cycles of order 4 can appear in only one of the co-sets of $G$ which correspond to the various substitutions of order 2 according to which the cycles in the invariant substitutions are transformed under $G$, since all of these cycles of order 4 would have to appear in such a co-set if one such cycle appears there, and all the substitutions of these co-sets must involve all the letters found in $G$.

Therefore the order of the regular group in question cannot exceed 4, since at least one-fourth of the substitutions of $G$ must have orders which exceed 2. Hence each substitution of order 4 contained in $G$, even when the squares of the cycles of order 4 contained in $G$ are not found in the invariant substitution of order 2, is regular, and hence only one-fourth of the substitutions of $G$ have an order greater than 2. It follows that $G$ is either the octic group or the direct product of this group and an abelian group of type (1, 1, 1, . . .). Hence the degree of $G$ cannot be less than half its order, and $G$ must be the octic group if all its cycles of order 4 are conjugate.

4. *Non-Prime Power Transitive Groups in which* $m = n-2$. When the order of the transitive group $G$ is not a power of a prime number and the number of the cycles of order $k$ contained in $G$ is $(n-2)g/k$, where $n$ is the degree of $G$, it results directly that all the cycles of $G$ are of prime order. When $n = 3$, $G$ is the symmetric group of order 6; and when $n = 4$, $G$ is the alternating group of order 12. We shall therefore assume in what follows that $n > 4$ unless the contrary is stated.

It will be convenient to use the following general theorem.

THEOREM III. *If a transitive substitution group which contains only one set of conjugate cycles of order $k$ involves an invariant subgroup $H$ such that $H$ and each of the corresponding co-sets involves all these conjugate cycles, then $H$ must be transitive and must contain only one set of conjugate cycles of order $k$.*

Since each of these cycles appears in $H$ and in every co-set of $G$ with respect to $H$, it results directly that it has as many distinct conjugates under $H$ as it has under $G$. That is, all these cycles form a single set of conjugates under $H$. If $H$ were intransitive, all of these cycles would therefore appear in one and in only one of its transitive constituents. This is impossible since the transitive constituents of $H$ are transformed transitively under $G$.

It is now easy to prove that cycles of $G$ which constitute a single set of conjugates must be of order 2. In fact, if these cycles were of prime order $p > 3$, the substitutions which would transform one such cycle into all its different powers less than $p$ would involve cycles of composite order. It remains therefore only to consider the case when these cycles are assumed to be of order 3. In this case there would also be cycles of order 2 in $G$, and hence the order of $G$ would be of the form $2^\alpha 3^\beta$. In particular, $G$ would be solvable.

If $G$ contains an invariant subgroup $H$ of index 3 and all the cycles of order 3 are conjugate, each of the co-sets corresponding to the operators of order 3 in this quotient group involves all the different cycles of order 3 contained in $G$, and these cycles are also found in $H$. Hence it follows from Theorem II that $H$ would be transitive and would involve only one set of conjugate cycles of order 3, while all of its other cycles would be of order 2. This subgroup being of the same degree as $G$ could therefore be used in place of $G$.

By repeating this process we finally would arrive at a transitive group which would be of the same degree as $G$ and could be used for $G$, and which would have no in-

variant subgroup of index 3. This group would therefore contain a subgroup of index 2 involving all of its cycles of order 3. If not all the remaining substitutions were of order 2, all the cycles of order 3 would again be conjugate under this invariant subgroup, and hence this subgroup would again be transitive and involve cycles of order 2. Since it may be assumed that all of the remaining substitutions would be of order 2, this subgroup would have the property that each of its substitutions could correspond to its inverse in an automorphism, and hence it would be abelian. Since it would also be transitive, it would be regular. This is clearly impossible since it has been assumed that $n > 4$. We have therefore proved the following theorem.

THEOREM IV. *The symmetric group of degree* 3 *is the only non-prime power transitive group which has the properties that it involves cycles of only two different orders and that all the different cycles of the larger order are conjugate.*

When all of the different cycles of order 2 contained in $G$ form a single set of conjugates, it may be assumed that $G$ involves no subgroups of index 2. In fact, if there were such a subgroup each of the remaining substitutions would have to be of even order, and hence each of them would involve one and only one cycle of order 2, while the subgroup of index 2 would involve no cycle of order 2, and hence it would be of odd order. Since this is impossible, and since $G$ is solvable, it follows that $G$ involves an invariant subgroup of index $p$, where $p$ is an odd prime number. The order of $G$ is therefore $2^{\alpha}p^{\beta}$.

THE UNIVERSITY OF ILLINOIS