POSSIBLE ORDERS OF TWO GENERATORS OF THE ALTERNATING AND OF THE SYMMETRIC GROUP*

BY

G. A. MILLER

It is well known that every alternating and every symmetric group can be generated by two of its substitutions, and that two such generating substitutions can usually be selected in a large number of different ways. Since two operators of order 2 must always generate a dihedral group it is evident that no alternating group can be generated by two of its substitutions of order 2, and that the only symmetric group which can be thus generated is the symmetric group of order 6. On the other hand, it is known that with very few exceptions, relating to groups whose degrees do not exceed 8, every alternating group and every symmetric group can be generated by two of its substitutions of orders 2 and 3 respectively.† In the present article we shall prove that whenever an alternating group involves a substitution of order $l>3$ then it contains two substitutions of orders 2 and l respectively which generate the entire group. We shall also determine the degrees of all the symmetric groups to which a similar theorem does not apply.

Before proving this general theorem, it may be desirable to consider the more elementary question of generating an alternating or a symmetric group by two of its substitutions which are separately composed of a single cycle. When neither of the two numbers l_1, l_2 exceeds n but their sum exceeds n it is obvious that two substitutions s_1, s_2 which are separately composed of a single cycle, and whose orders are l_1, l_2 respectively, can be so selected that they generate a transitive group of degree n, and that half the substitutions of this transitive group are negative whenever at least one of the two numbers l_1, l_2 is even. If s_1 and s_2 do not have all their letters in common we may suppose that the common letters are arranged in the same order in both of these substitutions and hence their commutator is either of the form abc or of the form $ab \cdot cd$. If both of them are of degree n we may suppose that all their letters are arranged in the same order with the exception that two adjacent letters are interchanged. Hence their commutator is of the form abc in this case. The group generated by s_1, s_2 is obviously multiply transitive

* Presented to the Society, December 31, 1926; received by the editors, December 20, 1926.

† G. A. Miller, Bulletin of the American Mathematical Society, vol. 7 (1901), p. 424.

whenever $n>3$ and hence it must be alternating or symmetric, at least when $n>8$, since the class of a primitive group which is neither alternating nor symmetric must exceed 4 whenever its degree exceeds 8. When n does not exceed 8 it is easy to verify directly that two such substitutions can be so selected as to generate the alternating groups when both of the numbers l_1, l_2 are odd, and the symmetric group when at least one of these numbers is even. These results may be stated in the form of a theorem as follows: *If l_1, l_2 represent a pair of numbers, each being greater than unity, such that neither exceeds n but their sum exceeds n, then it is always possible to find two cycles of orders l_1 and l_2 respectively such that they generate the alternating group of degree n whenever both l_1 and l_2 are odd. When at least one of these two numbers is even they generate the symmetric group of the same degree.*

From this theorem it results directly that if l_1, l_2 represents any pair of positive integers such that each exceeds unity then it is always possible to find two cycles s_1, s_2 of orders l_1, l_2 respectively such that the group generated by s_1, s_2 is either alternating or symmetric and has an arbitrary one of l_1, $l_1 \leqq l_2$, different degrees. For instance, pairs of cycles of order 9 can be selected such that each pair generates an arbitrary one of nine different alternating groups, viz., the alternating groups whose degrees vary from 9 to 17 inclusive, while an arbitrary one of the nine different symmetric groups of the degrees 10 to 18 can be generated by a cycle of order 9 and a cycle of order 10. This constitutes a complete solution of the elementary problemof generating alternating or symmetric groups by means of twocycles on their letters.

For the proof of the general theorem noted in the first paragraph it will often be convenient to use the following obvious theorem: *If a transitive group of degree n contains a cycle of prime order p, where p satisfies the condition $n/2<p\leqq n-3$, it must be either alternating or symmetric.* It is known that whenever $n>7$ it is always possible to find such a prime number.*

It will also frequently be desirable to use the following theorem:

If a transitive group is generated by two substitutions s_1, s_2 and if one of these substitutions s_2 involves one and only one cycle of a given prime degree while the other does not transform all the letters of this cycle into letters which do not occur in it, then the transitive group generated by s_1, s_2 is either alternating or symmetric whenever its degree exceeds the degree of this cycle by more than 2.

Since it is well known that a primitive group of degree n which does not include the alternating group of this degree can not involve a substitution

* G. A. Miller, School Science and Mathematics, vol. 21 (1921), p. 874.

composed of a single cycle of prime degree less than $n-2$, it is only necessary to show that s_1 and s_2 generate a primitive group. To do this we may transform by s_1 a power of s_2 which is equal to this prime cycle and thus obtain a prime cycle which has not all its letters in common with the former but has at least one letter in common therewith. Hence the group G generated by s_1, s_2 involves two such prime cycles which generate a doubly transitive group whose degree is just one larger than the degree of one of these cycles. Since a transitive group which contains a primitive subgroup of lower degree is itself primitive unless all the letters of this primitive subgroup appear in one of the sets of every one of its possible systems of imprimitivity, it results almost directly that G must be primitive and hence the theorem in question has been established.

To exhibit the nature of the limitations imposed in this theorem and at the same time prove a somewhat striking theorem it may be noted here that *if s_2 represents a substitution of composite order k_1k_2 and is composed of two cycles of orders k_1k_2 and k_1 respectively, and if s_1 is a transposition which involves one letter from each of these two cycles, then the group generated by s_1, s_2 is imprimitive and contains invariantly the direct product of k_1 symmetric groups which are separately of degree k_2+1.* A proof of this theorem results from the following consideration. The commutator of s_1 and $s_2^{k_1}$ is a cycle of order 3. The symmetric group of degree 3 generated by this commutator and s_1 has two letters in common with a cycle of $s_2^{k_1}$ and these two letters are adjacent in this cycle. Hence G involves the symmetric group of degree k_2+1 in view of the theorem noted near the close of the preceding paragraph. This symmetric group is transformed by s_2 into k_1 symmetric groups such that no two of them have a letter in common. The order of G is k_1 times that of the direct product of these symmetric groups. The simplest illustration of such a group is the transitive group of degree 6 and of order 72. In this case $k_1=k_2=2$.

Another elementary theorem which will be very useful in the solution of our general problem may be stated as follows:

If s_1, s_2 generate a transitive group and if s_1 has only one letter in common with some power of s_2 and if the letter by which this common letter is replaced in s_1 does not appear in a cycle of s_2 whose order is a multiple of the number of cycles in the given power of s_2, then this transitive group includes the alternating group of its degree.

The proof of this theorem is similar to that noted in the preceding paragraph. The commutator of the given power of s_2 and s_1 is again a cycle of order 3 and hence G involves the alternating group on a number of letters which is at least one larger than the order of a cycle in the said power of s_2. This alternating group involves letters from at most two cycles of s_2. Hence s_2 would have to transform it into alternating groups on sets of distinct letters if the theorem were not true. As this is impossible from the conditions noted in the theorem it results that the theorem is established. When the given power of s_2 is a single cycle it is clear that the condition as regards the letter by which the common letter is replaced in it may be omitted in the theorem.

In what follows s_2 will represent a substitution of order $l>3$ while s_1 will represent a substitution of order 2. The smallest possible degree of s_2 is the sum of the highest powers of the prime power factors of l, and when l is even, s_2 must be negative both for this smallest degree and also for the next larger degree of the symmetric group in which it appears. In every larger symmetric group there is a positive as well as a negative substitution of order l. It will be assumed that s_1 and s_2 have been so constructed that they generate a transitive group of degree n, and it results directly from the theorems noted above that when l is a given even number, s_1, s_2 can be so chosen that they generate the symmetric group when n has the smallest possible value or the next larger value. In what follows we may therefore always assume that n has a larger value. When l is odd, s_2 must be positive, and when l is even it will be assumed that s_2 is positive unless the contrary is stated, and that the degree of s_2 is not less than $n-p_1+1$, where p_1 is the smallest prime factor of l when l is either odd or divisible by 3. When neither of these two conditions is satisfied then the degree of s_2 may be assumed to be at least $n-3$. Moreover, it will generally be assumed that the cycles of s_2 appear in descending order of magnitude in case there is a difference in their orders.

When l is divisible by at least three distinct prime numbers it is obvious that s_1 can be so selected that it has only one letter in common with the firse cycle of s_2 and that all the other cycles may be assumed to be of lower primt power orders. Moreover, when it is desirable to add to s_1 another transposition in order to give it the suitable sign we may form this, in case the order of the first cycle is divisible by the square of a prime number, on letters of this first cycle in such a way that the commutator of this cycle and s_1 is composed of a cycle of ordet 3 and of two transpositions. The square of this commutator is therefore a cycle of order 3 and may be used just as the commutator was used in the preceding case. When the order of this first cycle is not divisible by the square of a prime number, a transposition on the letters of the first cycle of s_2 may be added arbitrarily. Hence s_2 and s_1 can always be so selected as to generate either the alternating group of degree n or the symmetric group of this degree, as may be desired, whenever l is divisible by at least three distinct prime numbers and the group concerned contains a substitution of order l. When l is divisible by two distinct odd prime numbers, or by one such number and 4, the remarks which have just been made still apply, and hence we may assume in what follows that l is either a power of a prime number or the double of a power of an odd prime number.

When $l=2p_1$, where $p_1>3$ is a prime number, it results again directly from the preceding theorems that s_1 and s_2 can be so selected as to generate either the symmetric or the alternating group, as may be desired, whenever the group in question involves a substitution of order l. When $l=2p_1^\alpha$, $\alpha>1$, and p_1 any odd prime number, it is easy to prove that s_1, s_2 can be so chosen that their product contains a cycle of order p, as defined above, and that another transposition can be added to s_1 so as to give it the proper sign without affecting this cycle of order p. A simple proof of this fact may be given as follows. First, select s_1 so as to connect the last letter of the first cycle of s_2 with the first letter of the second cycle, and the first letter of every other cycle with the second letter of the preceding cycle. When the degree s_2 is not n, we connect also the last letter of s_2 with a letter not found in s_2, and when n exceeds the degree of s_2 by more than 1 we may connect the additional letter or letters with the second or the second and third letter of the first cycle of s_2. It was noted above that there could not be more than two such additional letters. When s_1' is selected in this way it is obvious that $s_1's_2$ is a single cycle of order n. If the $(p+1)$th letter of this cycle, counting from the next to the last letter of the first cycle of s_2, is not in s_1', we add to s_1' the transposition composed of this letter and the next to the last letter of the first cycle in s_2. The product of s_2 and the s_1 thus obtained will then involve a cycle of order p and this cycle will not be affected by adding a properly chosen transposition to s_1 to give it the desired sign.

It remains to consider the case when the $(p+1)$th letter of the given cycle of order n appears in s_1'. If in this case the letter which precedes this $(p+1)$th letter does not appear in s_1' we start our cycle with the third letter from the end of the first cycle of s_2 and proceed as before. If both the $(p+1)$th letter and the preceding letter of the cycle of order n appear in s_1' and $p_1>3$ we start our cycle with the sixth letter from the end of the first cycle of s_2 and proceed as before. If $p_1=3$ we start with the fourth letter from the end of this cycle. If s_2 has been so chosen that it involves as small a number of transpositions as possible, no other case can present itself and hence it remains to consider only the cases when $l=6$, and when l is a power of a single prime number.

When $l=6$ and s_2 is positive, $n>6$. When $n=7$ or 8, it follows directly from the general theorems noted above that s_1, s_2 can be suitably selected. When $n>7$ it may be assumed that the first cycle in s_2 is of order 6 and that s_2 involves no more than one transposition. It may also be assumed that its degree is not less than $n-2$, since cycles of order 3 may be added to it if necessary to increase its degree. Hence it is obvious that s_1 and s_2 may be so selected that their product involves a cycle of order p and that s_1 is either positive or negative as may be desired. It remains to consider the case when l is a power of a single prime number and $l>3$.

The case when $l=p_1$, p_1 being a prime number, is especially interesting since there is an infinite number of values of n, one and only one for each such prime number, such that the symmetric group of degree n contains a substitution of order l but cannot be generated by two operators of orders 2 and l respectively. The fact that $2p_1-1$ is such a value of n is obvious since s_1 must then be of degree $2p_1-2$ and hence it must be positive. This substitution and s_2 generate the alternating group of degree n according to the general theorems noted above, and hence it remains to prove that for every other value of n it is possible to find two substitutions of orders 2 and l respectively which generate either the alternating group or the symmetric group of degree n as may be desired. When $n<2p_1$, this requires no further proof since it is included in a general theorem noted above. When $n\geqq 3p_1$ it is obvious that s_1, s_2 can be so chosen that their product involves a cycle of order p. When $n=2p_1+k$, $k<p_1$, we may first consider the case when $k=p_1-1$. If $p>n-p_1'$, it must be at least equal to $n-p_1+2$. Hence we may connect the letters of the second cycle of s_2 by means of s_1' with the k letters which do not appear in s_2 and add a suitable transposition to s_1 so as to obtain a cycle of order p in the product of s_1' and s_2. An additional transposition on the letters of the first cycle of s_2 may be added to s_1' so as to give it the desired sign without affecting this cycle of order p, since p cannot exceed $n-3$. When $p=n-p_1$, then we may connect one of the letters not found in s_2 with the first letter in the first cycle of s_1 and the other letters not found in s_2 with letters of the second cycle of s_2. When $p<n-p_1$ we can evidently proceed in a similar way. Finally, when $k<p_1-1$ we may again connect by s_1 the letters of the second cycle of s_2 with those not found in s_2 and thus obtain suitable forms for s_1 and s_2. Hence the following theorem. *If $l>3$ represents a prime number which divides the order of the symmetric group of degree $n\neq 2l-1$, then it is always possible to find two operators of orders l and 2 respectively which generate this symmetric group and also two such operators* *which generate the alternating group of this degree. When $n=2l-1$ it is possible to find two such generators of the alternating group of degree n but it is impossible to find two such generators of the symmetric group of this degree.*

When $l=p_1^\alpha$, where p_1 is any odd prime number and $\alpha>1$, the substitution s_2 may be assumed to be of degree $n-k$, $k<p_1$. If s_2 involves more than one cycle we may again suppose that s_1' connects the last letter of the first cycle of s_2 with the first letter of the second cycle and the first letter of every other cycle with the second letter of the preceding cycle. Moreover, s_1' connects letters of the last cycle in s_2 with the k letters which do not appear in s_2. The product s_2s_1 is a cycle of degree n, and if the $(p+1)$th letter of this cycle, counting from the next to the last letter of the first cycle of s_2, does not appear in s_1' we adjoin to s_1' a transposition composed of this letter and the next to the last letter in the first cycle of s_2. If the said $(p+1)$th letter appears in s_1', the preceding letter cannot have this property, and hence we begin our cycle with the third letter from the end of the first cycle and adjoin to s_1' the transposition composed of this letter and the pth letter in the said cycle of order n. In both cases we obtain a value of s_1' such that s_2s_1' involves a cycle of order p, and that we can add another transposition to s_1', in case we desire to change its sign, without affecting this cycle of order p. When s_2 involves only one cycle, the k letters which do not appear in s_2 may be connected with the first k letters of s_2 and we may begin our cycle of order n with the last letter of s_2. The $(p+1)$th letter of this cycle cannot now appear in s_1' and hence we may adjoin to s_1' the transposition composed of this letter and the last letter of s_2 in order to obtain a cycle of order p in the product of s_2s_1; and an additional transposition can be added to this s_1 without affecting this cycle. When l is a power of 2 which is divisible by 8, similar considerations obviously apply, and hence it remains only to consider the case where $l=4$.

While an infinite number of exceptions presented themselves when $l>3$ was assumed to be an odd prime number, one for each such prime, there is only one exception when $l=4$, since every alternating group which involves substitutions of order 4 can be generated by two operations of orders 2 and 4 respectively, and every symmetric group, except the symmetric group of degree 6, can be generated by two such operators whenever its order is divisible by 4. To prove this theorem it may be assumed that s_2 is positive and that its degree is $n-k$, $k<2$, and that s_2 involves at most three transpositions. When $k=1$ the letter which is not found in s_2 is connected by s_1' with the last letter of s_2, while s_1' connects the other letters of s_2 as in the preceding cases so that s_2s_1' is again a single cycle of order n. When $n>19$, s_2 involves at least four cycles of order 4, and when $k=0$, s_1' is positive when the transposition is adjoined to give a cycle of order p in s_2s_1'. Hence when

$p=n-3$ it is not necessary to adjoin to s_1' an additional transposition to obtain generators of the alternating group. Generators of the symmetric group in this case may be obtained by replacing a cycle of order 4 in s_2 by two transpositions. When $p<n-3$ it is clearly possible to assume that s_2 is always positive and to adjoin a transposition to s_1' without affecting the cycle of order p. Hence two substitutions of orders 2 and 4 respectively can always be found so that they generate either the alternating or the symmetric group of degree n as may be desired whenever $n>19$.

When $7<n<20$ the value of p can be so selected as to make the determination of two possible generators s_1, s_2 very simple. The groups of degrees 6 and 7 are so well known that it seems unnecessary to give here two substitutions of orders 2 and 4 respectively which generate the alternating groups of these degrees or the symmetric group of degree 7 as may be desired. On the other hand, it may be of some interest to give an outline of a proof that the symmetric group of degree 6 cannot be thus generated. If it could be generated by two such substitutions we may assume that s_2 would be one of the following two substitutions, $abcd$, $abcd \cdot ef$. Since the separate groups generated by these substitutions are transformed into themselves by a group of order 16 on these letters we need to use for s_1 only one of each set of conjugates under this group. When s_2 is the former of the two given substitutions s_1 may therefore be assumed to be one of the following four substitutions:

$$ce \cdot df, \quad be \cdot df, \quad ab \cdot ce \cdot df, \quad ac \cdot be \cdot df.$$

In the first case the commutator of s_2 and s_1 would be $adcef$. This commutator and s_2^2 generate the simple group of order 60 since their product is of order 3. As this group is invariant under s_1 and s_2, these two substitutions generate the triply transitive group of order 120. The second and fourth substitutions to be used for s_1 evidently generate an imprimitive group with s_2, while the third and s_2 again generate the triply transitive group of order 120, since s_1s_2 in this case is $acedf$ and the square of this into s_2^2 is again of order 3. Hence these two substitutions generate the simple group of order 60 which is invariant under s_1 and s_2.

When $s_2=abcd \cdot ef$ it may be assumed that s_1 is one of the following three substitutions:

$$de, \quad ab \cdot cf \cdot de, \quad ac \cdot bf \cdot de.$$

In the first case it follows from a general theorem noted above the s_1 and s_2 generate a group of order 72. In the other two cases it is obvious that they must also generate an imprimitive group. Hence it has been proved that the symmetric group of degree 6 can not be generated by two of its substitutions of orders 2 and 4 respectively. That is, *Every symmetric group whose order is divisible by 4 except the symmetric group of degree 6 can be generated by two operators of orders 2 and 4 respectively, and every alternating group which involves operators of order 4 can be generated by two such operators.*

University of Illinois,
Urbana, Ill.