ON THE PRIMITIVE GROUPS OF CLASS $3p$*

BY

W. A. MANNING

In this paper are considered only those groups which contain a substitution of order p and degree $3p$, p an odd prime. Two general theorems are first established and then class 9 is disposed of before the general problem is considered.

THEOREM I. *Let A be a substitution of degree pq and order p in a group of class pq, $q \leqq p$. No substitution similar to and non-commutative with A can be free from all the letters of any one cycle of A. An exception may occur when $q = p$ and the group contains a transitive subgroup of order p^2.*

Let B be a substitution similar to A, non-commutative with A, and free from all the letters of r cycles of A. If $q < p$, no two substitutions similar to A can displace exactly the same letters unless one is a power of the other,† and we may assume this to be true in the groups of class p^2 here considered, since the knowledge that G contains a transitive subgroup of degree p^2 makes its consideration and determination relatively simple.

If B does not connect old and new letters transitively in its cycles, $A^{-1}B^{-1}AB$ is of degree not greater than $(q-r)p$, and is not the identity. We can now assume that B and all its powers connect old and new letters transitively.

It will be shown that a substitution F can always be found among the substitutions similar to A, which transforms into themselves the r cycles of A left fixed by B and which displaces not more than $q-r$ letters new to A. The existence of F depends only upon the existence of B and leads to a substitution, not the identity, which displaces at most $(q-r)p+q-r$ letters. If B displaces not more than q new letters and $q \neq p$, we have at once a substitution $A^{-1}B^{-1}AB$ of degree less than pq. If $q = p$, an apparent exception arises when $r = 1$, and B displaces just p new letters. But here $A^{-1}BA$ is not a power of B and displaces the same p^2 letters as B.

It is now assumed that B displaces more than q new letters, so that some cycle contains at least two new letters. In $B^{-\rho}AB^{\rho} = C$, suppose ρ so chosen that two new letters which occur in the same cycle of B are adjacent in B^{ρ}.

* Presented to the Society (San Francisco) April 25, 1903. Received for publication June 2, 1904.

† Transactions of the American Mathematical Society, vol. 4 (1903), p. 351.

The substitution C does not displace as many new letters as B and in it r cycles of A occur unchanged. C certainly contains one or more new letters. We now wish to show that the new letters which are in C cannot merely fill up isolated cycles of C, but that C also must connect old and new letters in its cycles. Let $C = C_1 SR$, where C_1 contains only old letters, S only new ones, and R is made up of the r unchanged cycles of A. Let S have s cycles. Break A up into two parts, $A = A_1 R$, where $A_1 = c_1 c_2 \cdots c_{q-r}$. The substitution $A^{-1}C = (A_1^{-1} C_1) S$ contains not more than $(q - r + s)p$ letters. Unless $s \geqq r$, G is of class less than pq. Again $A^{-1} C^{-1} A C = A_1^{-1} C_1^{-1} A_1 C_1$ lowers the class of G to $(q - r)p$ or less unless we have $A_1^{-1} C_1 A_1 = C_1$. This condition can be satisfied only if $C_1 = c_1^{x_1} c_2^{x_2} \cdots c_{q-r-s}^{x_{q-r-s}}$, since C_1 has at most $p - 2$ cycles. From this form of C it follows that if a letter of any cycle of A is left fixed by B^ρ, no letter of that cycle occurs in B. But by hypothesis B is free from just r complete cycles of A. Then B^ρ contains just $(q - r)p$ old letters. The number of new letters in B^ρ is $sp = rp$, and since these rp new letters are all found in C, each one of them is in B^ρ preceded by an old letter. But ρ was chosen so that two new letters would be adjacent in B^ρ. We conclude that C connects old and new letters transitively.

Suppose that in some cycle of C two or more new letters are found. Again we choose ρ so that two new letters are adjacent in C^ρ. Then $D = C^{-\rho} A C^\rho$ displaces fewer new letters than does C, retains unchanged the r cycles of A left fixed by B, and furthermore connects old and new letters. The last statement requires proof.

In case D does not connect old and new letters, $D = D_1 SR$, where D_1 contains old letters only; S, sp new letters only; and R repeats r cycles of A without change. The degree of $A^{-1}D = (A_1^{-1} D_1) S$ is not greater than $(q - r + s)p$; hence $s \geqq r$. Again $A^{-1} D^{-1} A D = A_1^{-1} D_1^{-1} A_1 D_1 = 1$, since this substitution cannot displace more than $(q - r)p$ letters. Hence $D_1 = c_1^{x_1} \cdots c_{q-r-s}^{x_{q-r-s}}$. Now $C^{-\rho} A C^\rho = D = c_1^{x_1} \cdots c_{q-r-s}^{x_{q-r-s}} SR$. It follows that if a letter of any cycle of A is missing from C^ρ, no letter of that cycle occurs in C. Therefore C leaves fixed all the letters of at least s cycles of A. But we have seen that $s \geqq r$. The same reasoning can now be applied to C as was applied to B. Then D has the properties stated. Applying the same method to D we obtain another substitution E similar to A, connecting old and new letters transitively, containing unchanged at least r cycles of A, and displacing fewer new letters than D. This process can be continued until a substitution F is reached which has at least r cycles of A unchanged, is similar to A, and introduces k $(q - r \geqq k \geqq 1)$ new letters with no two new letters in the same cycle. The substitution $A^{-1}F$ displaces not more than $(q - r)p + q - r$ letters, which is contrary to the hypothesis that $r \geqq 1$.

THEOREM II. *Among the substitutions similar to A in a primitive group of class pq $(1 < q \leqq p)$, p odd, a substitution B can be found connecting transitively two cycles of A and having not more than one new letter in any cycle.*

Since G is primitive the similar substitutions $A, \cdots$ generate a transitive group. If no one of the set replaces all the letters $a_1, a_2, \cdots, a_p$ by other letters, one of them connects two cycles of A and has not more than one new letter α in any cycle.* But if A_1 replaces all the letters $a_1, \cdots$ by other letters, these p letters a are found in at least three of the q cycles of A_1, so that by the theorem just proved some cycle of A_1 contains letters from different cycles of A. Therefore there always is in the set $A, \cdots$ a substitution $B = (a_1 b_1 \cdots) \cdots$.

Among all the substitutions $A, \cdots$ which connect cycles of A, there is one which displaces a minimum number λ of the new letters α. It is immaterial which two cycles of A are connected. Let B be a substitution of the form $(ab \cdots) \cdots$ displacing λ new letters. Also let B leave fixed one of the letters a. It cannot have two new letters α consecutive, for then $B^{-1}AB$ would connect letters a and b in one of its cycles and would displace fewer than λ new letters. Suppose that B has two or more new letters in its first cycle. A convenient power B^ρ makes these two new letters consecutive. In B^ρ letters a can only be followed (or preceded) by other letters a and new letters α. Hence in the first cycle of B^ρ there are the sequences $a'\alpha'$ and $b'\alpha''$, where a' is one of the letters $a_1, \cdots, a_p$, and b' is one of the remaining $(q-1)p$ letters of A. Now choose σ so that $B^{\rho\sigma} = (a'b' \cdots \alpha'\alpha'' \cdots) \cdots$. Since by hypothesis B leaves an a fixed, $B^{-\rho\sigma}AB^{\rho\sigma}$ connects cycles of A and has fewer than λ letters α. Then B has just one α in its first cycle. It is clear that any power of B has a letter a followed (or preceded) in its first cycle by a letter from another cycle of A. Hence B cannot have two new letters in any cycle.

We shall now show that it may always be assumed that B leaves a letter a fixed. Suppose that B displaces all the $a_1, \cdots, a_p$. Evidently the same is true of $b_1, b_2, \cdots, b_p$. If the $2p$ letters $a_1, \cdots, b_i, \cdots$ occupy just two cycles of B, any power of B replaces some a by an a and some other a by a b, and, as before, B has not more than one new letter α to a cycle. If the $2p$ letters $a_1, \cdots, b_1, \cdots$ are found in more than two cycles of B, two cases arise. First, let no letter $c, d, \cdots$ be in the same cycle with an a or b. Some power B^x of B now connects c and d, say, because of Theorem I. Then B must displace the $2p$ letters $c_1, \cdots, d_1, \cdots$, and these letters again are found in at least two cycles of B. Now if no e is in a cycle of B with c or d, we have a B^y connecting e and f, with the same conditions. Proceeding thus we finally find that either B connects two cycles k and l of A, leaving fixed some of the letters $k_1, \cdots, k_p$, or else B connects three or more cycles of A. So we have the second case,

*JORDAN, Journal für Mathematik, vol. 79 (1874), pp. 249-253.

a letter c is in a cycle with a and b. Here B displaces the $3p$ letters $a_1, \cdots, b_1, \cdots, c_1, \cdots$. These $3p$ letters cannot occupy just 3 cycles of B, for then any power of B would transform A into a new substitution connecting cycles of A. In fact B cannot have kp letters of k cycles of A in k cycles by themselves for the same reason. Hence $a_1, \cdots, b_1, \cdots, c_1, \cdots$ are to be found in at least 4 cycles of B. Continuing thus it is evident that B either displaces all the qp letters of A or connects two cycles of A without displacing all the letters of one of the two cycles.

Class 9.

Let there be a transitive subgroup (F) of degree 9 in G. This subgroup cannot be cyclic for it would then be contained in a doubly transitive G^{10},* which does not exist. If F is non-cyclic it leads to a doubly transitive $G^{13}_{13.12.9}$, also impossible.

We can now say that there is a substitution B similar to A which connects transitively two cycles of A and displaces one, two, or three new letters.

Suppose that $I_1 = \{A, B\}$ is intransitive. It is a simple isomorphism between two transitive constituents, one of which is of degree 4 and order 12. Now the other constituent can only be of degree 6, and class 4, lowering the class of G to 8.

Then I_1 is transitive. It is of degree 12 and order 36. The 4 systems of imprimitivity of three letters each can be chosen in only one way. Hence I_1 must be maximal in a doubly transitive $G^{13}_{13.12.3}$, an absurdity. No primitive group of class 9 exists.

Class $3p$, $p > 3$.

If a primitive group contains a cyclic subgroup F on $3p$ letters, it also contains a doubly transitive $G^{3p+1}_{(3p+1)3p}$. Then $3p = 2^{2m} - 1$, and $p = 5$. We have here a $G^{16}_{16.15}$† which is maximal in turn in a G^{17}, but is not contained in a 4-ply transitive group of degree 18.‡

In case F is non-Abelian only the doubly transitive G^{3p+4} need be examined. Here the subgroup transforming F into itself has a tetrahedral subgroup in its quotient group. But such a subgroup is not to be found in the group of isomorphisms of F.

Let $I_1 = \{A, B\}$, of degree greater than $3p$, be intransitive, and let I_1' and I_1'' be the two simply isomorphic transitive constituents of degrees $2p + k'$,

* JORDAN, Journal de Mathématiques, ser. 2, vol. 16 (1871), p. 383; MARGGRAFF, *Ueber primitive Gruppen mit transitiven Untergruppen geringeren Grades*, Dissertation, Giessen, 1889.

† MILLER, *The primitive groups of degree* 16, American Journal of Mathematics, vol. 20 (1898), p. 229; *The transitive groups of degree* 17, Quarterly Journal of Mathematics, vol. 31 (1899), p. 49.

‡ JORDAN, Journal de Mathématiques, ser. 2, vol. 17 (1872), p. 351.

$p+k''$, respectively; where $k', k''=0, 1; k'=k''\neq 0$. Suppose I_1'' of degree p. It is then of class $p-2$, and hence* is the simple triply transitive $G_{p.p-1.p-2}$. To all the substitutions not of order p in I_1'' must correspond substitutions of degree $2p+2$ in I_1'. Hence $(p-1)(p-2)=2p+2$, from which $p=5$. The group I_1 is icosaedral of degree 17. Next suppose that I_1'' is of degree $p+1$. It can only be of class $p-1$ and hence is of order $(p+1)p\cdot 2$. Now I_1'' has $(p+1)p/2$ subgroups of order 2 on $p-1$ letters, and each is invariant in a subgroup of order 4. But the substitutions of order 2 involve all possible transpositions of $p+1$ letters, so that a given transposition is found in $(p-1)/2$ distinct substitutions. These $(p-1)/2$ substitutions generate an Abelian group since the product of any two of them is of order 2. Hence $(p-1)/2=2$, $p=5$.†

Since the degree of I_1' exceeds $(3p-1)/2$ a substitution C similar to A can be found in G which connects I_1' and I_1'', and introduces at most three letters new to I_1.

We take up I_{60}^{17} first. A transitive group of degree 17 and class 15 is triply transitive and has already been considered. It may be remarked that I_{60}^{17} cannot be included in a larger intransitive group of the same degree. Then $I_2=\{A, B, C\}$, if of degree 18, is of order $18\cdot 60$. This group cannot be primitive, as may be shown as follows. There are in I_2 36 conjugate subgroups of order 5, each of which is invariant in a subgroup of order 30. By considering the transitive representation of I_2 on 36 letters it is seen that I_2 has one conjugate set of 6 subgroups of order 3, and since no operator of order 5 can be permutable with each of the 6 subgroups of order 3, I_2 is isomorphic to a multiply transitive group on 6 letters. Then I_2 has either an invariant intransitive subgroup or a regular invariant subgroup of order 18 containing negative substitutions. But I_2 is a positive primitive group by hypothesis. Since I_2 is generated by I_1^{17} and C, it cannot be imprimitive. Continuing in much the same way the examination of the limited number of cases to which I_{60}^{17} and I_{60}^{18} lead, we reach the conclusion that the subgroup I_1 of G is never intransitive.

If the transitive group I_1 is of degree $3p+1$ it is primitive of order $(3p+1)p$. Here again $p=5$, because of the condition $3p+1=2^\alpha$. This well-known G_{80}^{16} is not maximal in a group of degree 17. If I_1 is of degree $3p+2$, the number of subgroups of order p in it is $(3p+2)/2$, an absurdity. Let $I_1=\{A, B\}$ be of degree $3p+3$. Since any substitution of I_1 which replaces one new letter by another must merely permute the new letters among themselves, I_1 is imprimitive. There are $p+1$ systems of 3 letters each. Since a system of three letters can be chosen in only one way, I_1 leads to a

*Cf. MAILLET, *Recherches sur les Substitutions*, etc., Dissertation, Paris, 1892, p. 78.

†Cf. DE SÉGUIER, Comptes Rendus de l'Académie des Sciences de Paris, vol. 137 (1903), p. 37.

doubly transitive G^{3p+4} of order $(3p+4)(3p+3)p$ or $(3p+4)(3p+3)2p$. In G the Sylow subgroup of order p is invariant in a group in which the quotient-group is tetrahedral or octahedral. This is impossible.

There exist then only three primitive groups of class $3p$, p odd, containing a substitution of order p and class $3p$. These groups are of class 15 and order 80, 240 and 4080.