THE PRIMITIVE GROUPS OF CLASS $2p$ WHICH CONTAIN A SUBSTITUTION OF ORDER p AND DEGREE $2p$[*]

BY

W. A. MANNING

If a group contains substitutions displacing just N letters, and none besides the identity displacing fewer than N letters, it is of class N.[†] All the substitutions of class N are regular. If N is a composite number, it may be assumed that the group of class N contains a substitution A composed of l cycles of prime order p.[‡]

JORDAN determined all the primitive groups of class p.[§] He also published without proof a list of the primitive groups of class less than 14.[||] Among these are some of the primitive groups of class $2p$, namely, those of the classes 4, 6, and 10. Proofs of his results for class 4 have since been published.[¶] There are six of these groups: the metacyclic G^5_{20}, the semimetacyclic G^5_{10}, the G^6_{120} simply isomorphic to the symmetric group of degree 5, the icosaedral G^6_{60}, the simple G^7_{168}, and the G^8_{1344}. Since these results are well established and offer exceptions to the general theory, it will be assumed in what follows that p is an odd prime.

THEOREM I. *If an intransitive or imprimitive group of degree $lp + 1$ and class lp contains a substitution of order p, then must $l \geqq p + 2$.*

First let the group be intransitive. It must be a simple isomorphism between its $e + 1$ systems of intransitivity. One transitive constituent is of degree

[*] Presented to the Society (San Francisco) December 20, 1902. Received for publication February 27, 1903.

[†] C. JORDAN, Comptes Rendus, vol. 72 (1871), p. 384.

[‡] C. JORDAN, Liouville's Journal, ser. 2, vol. 16 (1871), p. 390.

[§] C. JORDAN, Liouville's Journal, ser. 2, vol. 17 (1872), p. 363.

In addition to the cyclic group of degree p there exists a primitive group of degree $p + 1$ and order $p(p + 1)$, and one of degree $p + 2$ and order $p(p + 1)(p + 2)$, if, and only if, $p + 1$ is a power of 2.

[||] Comptes Rendus, vol. 73 (1871), p. 385.

[¶] NETTO, *Theory of Substitutions*, Cole's translation (1892), p. 133.

MILLER, American Mathematical Monthly, vol. 9 (1902), p. 63.

$rp + 1$, class rp, and order $(rp+1)r'p$, where r' divides r.[*] The remaining e constituents are regular and of degree $(rp+1)r'p$, so that

$$lp + 1 = er'p(rp+1) + rp + 1;$$

whence

$$l = er'(rp+1) + r; \qquad e \geqq 1,\ r \geqq r' \geqq 1.$$

Suppose next that the group is imprimitive. The substitution A of order p leaves one letter u fixed. The system of imprimitivity to which u belongs is transformed into itself by A. If two letters of a cycle of A belong to the same system, all the letters of that cycle belong to the system. Then the number of letters in each system is $rp+1$. The other $l-r$ cycles of A must permute the remaining systems. The number of systems of imprimitivity in the group is therefore $ep+1$. Hence we have $lp+1 = (ep+1)(rp+1)$; from which follows $l = e(rp+1)+r$, where $e \geqq 1$, $r \geqq 1$.

In both cases the minimum value of l is $p+2$.

THEOREM II. *Two similar substitutions of prime order and of lowest class in a group, which are not powers the one of the other, and such that the number of letters in a cycle exceeds the number of cycles in each substitution, cannot displace exactly the same letters.*

Let S and T be two similar substitutions of lowest class N which displace the same N letters. Since the number of letters in a cycle exceeds the number of cycles, one of the substitutions contains in one of its cycles two letters a_1 and a_2 which occur in a certain cycle of the other. Then two numbers σ and τ can be so chosen that $S^\sigma T^\tau$ leaves a_1 fixed. But the group containing S and T is of class N and therefore $S^\sigma T^\tau = 1$, which proves the theorem.

THEOREM III. *A primitive group containing a substitution of order p on $2p$ letters includes a transitive subgroup of degree $\leqq 2p+2$ generated by two similar substitutions of order p and degree $2p$.*

The proof of this proposition is contained in a memoir of JORDAN, to which the reader is referred.[†] An outline of the proof is, however, necessary to make clear the application of the reasoning there employed to this special case.

The primitive group G contains a transitive subgroup H generated by the similar substitutions $A = (a_1 a_2 \cdots a_p)(b_1 b_2 \cdots b_p)$, A', A'', $\cdots$. Since H is transitive, among the substitutions A', A'', $\cdots$ there will exist at least one A_1 which permutes letters of the first cycle of A with other letters. Now A_1 cannot replace each of the p letters a by b's and new letters c, for then A_1 must contain

[*] BURNSIDE, *Theory of Groups* (1897), p. 141.

FROBENIUS, Berliner Sitzungsberichte (1902), p. 455.

[†] Crelle's Journal, vol. 79 (1874), pp. 249-253. Cf. JORDAN, *Memoire sur les groupes primitifs*, Bulletin de la Société Mathématique de France, vol. 1 (1873), p. 175.

all the a's and must not have more than $(p-1)/2$ of them in each cycle, which is impossible since there are but two cycles. It is next shown that the substitution A_1 can be chosen in such a way that it replaces an a by a b. It may happen that among the substitutions A', A'', $\cdots$ there exist several which replace an a by a b. Choose for A_1 the one that displaces the fewest new letters c. Finally JORDAN proves that A_1 cannot contain more than one c in each of its cycles. The group generated by A and A_1 is transitive and of degree $\overline{\gtrless} 2p+2$.

We notice that this subgroup is positive since it is generated by two positive substitutions. It does not contain a substitution of order 2 on $2p$ letters. If the condition that the primitive group G under consideration is of class $2p$ is introduced, theorem II limits the degree of this subgroup K to $2p+1$ and $2p+2$. Then there are two cases to be considered. We shall take them up separately.

CASE I. The group G contains a transitive subgroup K of degree $2p+1$ and class $2p$. From theorem I it follows that K is primitive. Since it is positive, the subgroups of degree $2p$ are of order p and hence K is of order $(2p+1)p$. There is in K a selfconjugate subgroup F of degree and order $2p+1$.* Moreover $2p+1$ must be a power of a prime,† as q^α, and since

$$2p=(q-1)(q^{\alpha-1}+q^{\alpha-2}+\cdots+q+1),$$

it follows that $q=3$, or $\alpha=1$. When $2p+1$ is a prime, K is the semimetacyclic group. Since no substitution of degree $2p+1$ can be commutative with one of the substitutions of order p, and since no operator of odd order can transform a substitution of order 3 into its inverse, it follows that when $q=3$, F contains p subgroups of order 3, all conjugate in K. Hence F is Abelian and of type $(1, 1, \cdots 1)$, and K is a subgroup of the holomorph of this Abelian group F. The order of this holomorph is $3^\alpha(3^\alpha-1)(3^\alpha-3)\cdots(3^\alpha-3^{\alpha-1})$, and it is divisible by $p=(3^\alpha-1)/2$ but not by p^2. Then all the subgroups of order p in the holomorph are conjugate. Therefore all the subgroups of order $(2p+1)p$ are also conjugate. The above reasoning applies to any positive primitive group G of degree $2p+1$ and class $2p$ as no other conditions were imposed upon K. There is then only one positive primitive group of degree $2p+1$ and class $2p$ when $2p+1$ is a power of 3 as well as when $2p+1$ is a prime.

If a positive $G^{(2p+2)}$ (on $2p+2$ letters) of class $2p$ exists, the subgroup leaving one letter fixed is the $G^{(2p+1)}$ just determined, so that $G^{(2p+2)}$ is doubly transitive and of order $(2p+2)(2p+1)p$. Each subgroup of order p is self-

* FROBENIUS, Berliner Sitzungsberichte (1901), p. 1220.

† FROBENIUS, Berliner Sitzungsberichte (1902), p. 458; BURNSIDE, *Theory of Groups* (1897), p. 143.

conjugate in a subgroup of order $2p$, in which the substitutions that are not of order p are of degree $2p+2$. It will now be shown that $G^{(2p+2)}$ cannot exist if the subgroup of order $2p$ is cyclic and $p > 3$. Such a group is known to exist if $p = 3$, namely, the compound G^{8}_{168}.

A cyclic group of order $2p$ has only one substitution of order 2. No other substitution of order 2 in $G^{(2p+2)}$ can transform the same subgroup of order p into itself, for then the latter would be selfconjugate in a subgroup of higher order than $2p$. To each of the $p+1$ cycles of such a substitution of order 2 there corresponds a subgroup of order p leaving the two letters of that cycle fixed, and with which it is commutative. Therefore $G^{(2p+2)}$ contains just $2p+1$ substitutions of order 2. Now $G^{(2p+2)}$ contains $2(2p+2)p$ substitutions of degree $2p+1$, $(2p+1)(p^2-1)$ of order p and degree $2p$, at least $(2p+1)(p^2-1)$ of order $2p$ and degree $2p+2$, and $2p+1$ of order 2, making with the identity a total of at least $2p(2p+1)(p+1)$ substitutions. But this is the order of the group. No substitutions of prime order other than those enumerated occur. Then $p+1$ must be a power of 2 when $2p+1$ is a prime greater than 3. But $p+1$ is divisible by 3 since neither $2p$ nor $2p+1$ is divisible by 3. If $2p+1 = 3^{\beta}$, $p+1$ is not divisible by 3 and must again be a power of 2. But both $2^{\alpha}-1 = p$ and $2^{\alpha+1}-1 = 3^{\beta}$ cannot hold. Then $G^{(2p+2)}$ does not exist if the subgroup of order $2p$ is cyclic and $p > 3$.

There is one other form which the subgroup of order $2p$ may have. It may be a p, 1 isomorphism between a regular diedral rotation group and the group in the remaining two letters. All the substitutions of a regular diedral rotation group are completely determined by the subgroup of order p. Then $G^{(2p+2)}$, if it exists, is completely determined by the subgroup leaving one letter fixed and is therefore unique. When $2p+1$ is a prime, the modular group on $2p+2$ letters is a positive doubly transitive group of class $2p$. When $2p+1 = 3^{\beta}$, a group satisfying our conditions is defined by the congruences

$$y \equiv \frac{ax+b}{cx+d}, \quad \text{mod. } 3, \qquad ad - bc \equiv 1, \quad \text{mod. } 3,$$

in which a, b, c, and d are marks of the $GF[3^{\beta}]$.* The reasoning of this paragraph clearly holds when $p = 3$. The group in question is the simple G^{8}_{168} of class 6.

It is known that there is just one positive primitive group of degree 9 and class 6. Its order is 1512 and it contains the compound G^{8}_{168}. This G^{9}_{1512} is not, however, in turn contained in a primitive group of degree 10.†

*Mathieu, Liouville's Journal, ser. 2, vol. 5 (1860), p. 9; vol. 6 (1861), p. 241.

†Cole, Bulletin of the New York Mathematical Society, vol. 2 (1892), p. 250. Miller, Quarterly Journal, vol. 31 (1899), p. 228.

‡Burnside, *Theory of Groups* (1897), p. 202. Cf. ib., exercise, p. 204.

Assuming that $p > 3$ we have next to determine whether a positive triply transitive group containing $G^{(2p+2)}$ exist on $2p + 3$ letters.[‡] In such a group each subgroup of order p would be selfconjugate in a subgroup I of order $6p$. Evidently I has a transitive constituent of degree 3 and order 6, permuting the letters left fixed by the subgroup of order p. This is the symmetric group of degree 3. Then this symmetric group must be found in the quotient group of the largest group on the same letters that transforms a given group of degree $2p$ and order p into itself. But in this quotient group the operators of order 2 generate a subgroup in which there is no operator of order 3. The subgroup I of order $6p$ can therefore not exist. Then when $p > 3$, the chain of primitive groups comes to an end with the degree $2p + 2$.

Under this case are still to be considered those groups in which occurs a negative substitution. The primitive group G contains a selfconjugate subgroup of half its order composed of the totality of its positive substitutions, which must be one of the primitive groups just determined.

Of the primitive groups of class 6 neither the compound G^{3}_{168} nor the G^{9}_{1512} is contained in a positive and negative group of the same degree.

The group G is of order $(2p + 1)2p$ or $(2p + 2)(2p + 1)2p$ as its degree is $2p + 1$ or $2p + 2$. Since the subgroup of degree $2p$ is also of order $2p$, these groups are doubly and triply transitive respectively.

First, let the degree of G be $2p + 1$. If this number is a prime, G is metacyclic. If $2p + 1 = 3^{\beta}$, G contains a regular Abelian selfconjugate subgroup F of order 3^{β}, which contains p cyclic subgroups of order 3. The substitution $A = (a_1 a_2 \cdots a_p)(b_1 b_2 \cdots b_p)$ permutes these p subgroups cyclically. The subgroup G_1 of G that leaves one letter fixed and contains A is either cyclic or of diedral type. If G_1 is cyclic of order $2p$, it contains just one operator of order 2. A substitution of order 2 which with A generates a transitive cyclic group can be chosen in p ways. This substitution must, however, transform at least one subgroup of order 3 in F into itself. Only one of these p substitutions of order 2 can have this property, and it transforms every substitution of F into its inverse. This gives us the well known doubly transitive group of degree 3^{β} defined by

$$y \equiv ax + b, \quad \text{mod. } 3.$$

where a and b are marks of $GF[3^{\beta}]$, $a \neq 0$.

There remains the possibility that G_1 is a regular diedral rotation group. In this case all the negative substitutions of G are of order 2, and if we select any one of them and multiply it into all the negative substitutions of G in turn, all the positive substitutions of G are obtained. Now any two operators of order 2 generate a group in which the cyclic subgroup generated by their product is selfconjugate. Hence every substitution of order 2 in G transforms every subgroup of order p into itself. This is absurd. Then there is only the one positive and negative primitive group of degree $2p+1$ and class $2p$, which contains a substitution of order p.

It follows at once that there is not more than one positive and negative triply transitive group of degree $2p+2$; for such a group is determined by its positive subgroup of order $(2p+2)(2p+1)p$ and any negative substitution found in the subgroup leaving one letter fixed. The group exists and is the linear fractional group written on $2p+1$ letters, defined by

$$y \equiv \frac{ax+b}{cx+d},$$

$$ad - bc \not\equiv 0,$$

mod. $2p+1$, when $2p+1$ is a prime; and mod. 3, when $2p+1 = 3^\beta$, with the additional condition in the latter case that a, b, c, and d run through the marks of the $GF[3^\beta]$.

Case II. Suppose next that G is positive and contains a transitive subgroup K of degree $2p+2$ generated by two similar substitutions of order p. We may assume that K is imprimitive and that it is not contained in a primitive group of the same degree. For a primitive group of degree $2p+2$ contains a subgroup of degree $2p+1$ and class $2p$, which we have seen (theorem I) must be primitive, and this gives case I again. In fact K can contain no substitution displacing $2p+1$ letters. Now one of the generators,

$$A = (a_1 a_2 \cdots a_p)(b_1 b_2 \cdots b_p)$$

say, must interchange systems of imprimitivity of K. If two letters of a cycle of A belong to the same system of imprimitivity, all the letters of that cycle belong to the system. Therefore K has $p+1$ systems of two letters each. Every substitution of order p in K determines a system by the two letters which it leaves fixed, and hence the elements of the $p+1$ systems can be chosen in but one way. The subgroup of K that leaves one letter fixed leaves two fixed and is of order p. Then the order of K is $(2p+2)p$. If k is contained in a primitive group of degree n, that group is $n-(2p+2)+1 = n-2p-1$ times transitive,* and must in consequence contain a doubly transitive G of degree $2p+3$. The order of G is clearly $(2p+3)(2p+2)p$. When $p>3$, a subgroup of order p in G is transformed into itself by a subgroup of order $6p$, which, as we have already seen, is impossible in a primitive group of this degree.

In case $p=3$, G is of degree 9 and order 216. It is not contained in a primitive group of degree 10, but does lead to a $\pm G^9_{432}$, which is the holomorph of the regular non-cyclic group of order 9.†

*Jordan, Liouville's Journal, ser. 2, vol. 16 (1871), p. 383.

Marggraff, *Dissertation, Ueber primitive Gruppen mit transitiven Untergruppen geringeren Grades*, Giessen (1892).

†Cole, Bulletin of the New York Mathematical Society, vol. 2 (1892), p. 250.

Summing up our results, we find that there are five positive and three positive and negative primitive groups of class 6 which contain a substitution of order 3 on two cycles. They are the $\pm G^7_{42}$, the $\pm G^8_{336}$, the compound G^8_{168}, the G^9_{1512}, the $\pm G^9_{432}$ and their positive subgroups. When $p > 3$, primitive groups of class $2p$ containing a substitution of order p and degree $2p$ exist only when $2p + 1$ is a prime or a power of 3. There are just four groups when one or the other of these conditions is satisfied. All four are included in the triply transitive Mathieu group.

The determination of the primitive groups of class $2p$ which contain no substitution of order p on $2p$ letters seems to present greater difficulties than the case here considered.

STANFORD UNIVERSITY,
December, 1902.