ON THE ORDER OF PRIMITIVE GROUPS*

BY

W. A. MANNING

At the end of a memoir on primitive groups in the first volume of the Bulletin of the Mathematical Society of France,† JORDAN announced the following theorem:

Let q be a positive integer less than 6, p any prime number greater than q; the degree of a primitive group G that contains a substitution of order p on q cycles (without including the alternating group) cannot exceed $pq + q + 1$.

The proof of this theorem for $q = 1$ JORDAN published,‡ as well as that for the case of $q = 2$;† but for the values 3, 4, and 5 of q, no proofs have yet been published.

It is here shown to be possible to replace the above theorem by the following, which gives in part a closer limit:

Let q be an integer greater than unity and less than 5; p any prime greater than $q + 1$; then the degree of a primitive group which contains a substitution of order p that displaces pq letters (not including the alternating group) cannot exceed $pq + q$. When p is equal to $q + 1$, the degree cannot exceed $pq + q + 1$.

Before taking up the proof of this theorem, a series of general theorems on transitive groups must be established.

THEOREM I.§ *Let $s_1, s_2, \cdots$, be certain substitutions of order p (p an odd prime number) and of degree not greater than pq (q any number less than p) which generate a transitive group G. A number (λ) of these substitutions generate an intransitive subgroup I_1. A substitution s of order p and of degree not greater than pq can always be found in G, which connects letters of any given transitive constituent of I_1 with letters of some other transitive constituent of I_1.*

Suppose that the theorem is not true. Take a particular transitive con-

* Presented to the Society (San Francisco), September 29, 1906.

† C. JORDAN, Bulletin de la Société mathématique de France, vol. 1 (1873), pp. 175–221.

‡ C. JORDAN, ibid., vol. 1 (1873), pp. 40–71.

§ Cf. a related theorem in the writer's paper, *On the Primitive Groups of Class Ten*, American Journal of Mathematics, vol. 28 (1904), pp. 226–236.

stituent of $I_1 = \{ s_1, s_2, \cdots, s_\lambda \}$ in the letters $a_1, a_2, \cdots$. From all the powers of all the conjugates under G of $s_1, s_2, \cdots$, choose a substitution $s_{\lambda+1}$ which connects one of the letters $a_1, a_2, \cdots$ with a new letter, and which, of all the substitutions of this totality that connect letters $a_1, a_2, \cdots$ with new letters $\alpha_1, \alpha_2, \cdots$, has the fewest new letters in the cycles with letters $a_1, a_2, \cdots$. There may be a number of such substitutions. Now consider the group $I_2 = \{ I_1, s_{\lambda+1} \}$. If no substitution of the series $s_1, s_2, \cdots$ connects the extended set $a_1, a_2, \cdots$ with another transitive set of I_2, we take $s_{\lambda+2}$ as we did $s_{\lambda+1}$, and continue in this way until we have an intransitive subgroup I_{e-1} and a substitution s_e which connects the extended set $a_1, a_2, \cdots$ with some other set of I_{e-1}. It is now essential to consider closely the substitution s_{e-1} by which we pass from I_{e-2} to I_{e-1}. Let the letters of the first set of I_{e-2} be $a_1, a_2, \cdots, a_\kappa$, and let the remaining letters of I_{e-2}, which may or may not form a single transitive set, be denoted by $b_1, b_2, \cdots$; we shall speak of the letters a and the letters b.

Letters α, new to I_{e-2}, are connected with letters a by s_{e-1}. Since s_{e-1} is of prime order, any power of s_{e-1} connects a's and α's. If s_{e-1} has two α's in any one cycle, a number x may be chosen so that in s_{e-1}^x these two new letters are adjacent. Then unless s_{e-1}^x replaces all the k letters a by α's, one of the generators of the group $s_{e-1}^{-x} I_{e-2} s_{e-1}^x$ will connect a's and α's and displace fewer α's than does s_{e-1}, contrary to hypothesis. Suppose that s_{e-1}^x replaces every a by an α, but has two a's in the same cycle:

$$s_{e-1}^x = (a_1 \alpha_1 \cdots a_2 \alpha_2 \cdots) \cdots .$$

We may choose y so that

$$s_{e-1}^{xy} = (a_1 a_2 \cdots \alpha_1 \alpha_2 \cdots) \cdots ,$$

and proceed as before. Finally, if in s_{e-1} all the cycles containing a letter a displace $p-1$ α's, then s_{e-1} must have at least p cycles, contrary to hypothesis. Hence s_{e-1} has not two letters α in any cycle. We may write

$$s_e = (a_\mu \beta \cdots) \cdots ;$$

where β is a new letter followed by a b in some power, s_{e-1}^z say, of s_{e-1}, and μ is arbitrary. Now s_{e-1}^z has two letters a, as $a_\mu a_{\mu+1}$, adjacent in one of its cycles, so that

$$s_{e-1}^{-z} s_e s_{e-1}^z = (a_{\mu+1} b \cdots) \cdots .$$

Hence the theorem as stated is true.

THEOREM II.* *If the group $\{ I_1, s \}$ is transitive, there is in it a substitution*

* Theorems II and IV were added by the author in March, 1908, after the presentation of the paper to the Society.

s' of order p which connects letters of the given set a of I_1 with other letters of I_1, and which is not of higher degree than that one of the substitutions $s_1, s_2, \cdots, s_\lambda$ which is of highest degree; nor does s' displace more new letters α than does s.

The generators of I_1 are $s_1, s_2, \cdots, s_\lambda$. Let the degree of s_λ be not lower than that of $s_1, s_2, \cdots$, or $s_{\lambda-1}$. Suppose $\{I_1, s\}$ transitive and $s = (a_1 b_1 \cdots)\cdots$ of higher degree than s_λ. Now the totality of substitutions conjugate to $s_1, s_2, \cdots, s_\lambda$ generate an invariant subgroup H of $\{I_1, s\}$. If H is intransitive its transitive sets form systems of imprimitivity in $\{I_1, s\}$, and each is of degree p at least. But $\{I_1, s\}$ is generated by substitutions of order p and degree less than p^2, which cannot permute systems with so many as p letters in each of them. Then H is transitive, includes I_1, and consequently contains a substitution, of order p and of degree not greater than the degree of s_λ, which replaces one of the letters a by a letter b. Since this new s is found in $\{I_1, s\}$ it does not displace more new letters α than the former substitution s.

THEOREM III. *Let s be a substitution of the series $s_1, s_2, \cdots$ which connects transitively a given set a of I_1 (as before defined) with some other set of I_1. Let s be one of the substitutions which connect with the letters a the minimum number of new letters α. Moreover let it be assumed that no power of s replaces every letter of the set a by letters not belonging to the set. When these conditions are satisfied, s has not more than one new letter α to a cycle.*

We first remark that s may not have two new letters α adjacent in any cycle. For we may apply theorem I to that transitive constituent of $\{I_1, s^{-1} I_1 s\}$ which includes the letters a and letters b and infer that some generator of order p and of degree not greater than pq of the transformed group $s^{-1} I_1 s$ would have a letter a and a letter b in the same cycle and would displace fewer letters α than does s.

In the next place s may not have two letters α in the cycle $(a_1 b_1 \cdots)$. A certain power s^x certainly has two α's adjacent, and hence by the preceding paragraph it is impossible that any a should be followed by a b. Also no b is followed by an a, for then we should have $s^{-x} = (a'b' \cdots \alpha_2 \alpha_1 \cdots)$. Hence $s^x = (a'\alpha' \cdots b'\alpha'' \cdots)\cdots$ and $s^{xy} = (a'b' \cdots \alpha'\alpha'' \cdots)\cdots$, again in contradiction with the preceding result. Hence in any power of s a b either precedes or follows an a.

Finally s may not have two α's in any cycle. If in $s^{\pm x}$ two α's are adjacent, from $s^{\pm x} I_1 s^{\mp x}$ we may take a substitution of order p and of degree not greater than pq which connects letters a and b and displaces fewer than the minimum number of new letters α.

THEOREM IV. *A substitution s of order p and of degree not greater than pq (q less than p) can always be found in $\{s_1, s_2, \cdots\}$, which connects some two transitive sets of I_1 and which introduces at most q new letters.*

Let $s_1, s_2, \cdots$ and I_1 be defined as before and let the transitive constituents of I_1 displace the letters

$$\begin{aligned} a: &\quad a_1, a_2, \cdots, a_\kappa; \\ b': &\quad b'_1, b'_2, \cdots, b'_{\kappa'}; \\ &\cdots\cdots\cdots \\ b^\nu: &\quad b^\nu_1, b^\nu_2, \cdots, b^\nu_{\kappa^\nu}; \end{aligned}$$

respectively. We know that in the group generated by $s_1, s_2, \cdots$, there are substitutions of order p and of degree not greater than pq which have in the same cycle letters from two or more of the sets $a, b', \cdots, b^\nu$ of I_1. From all such substitutions let us select those which displace the least possible number (μ) of letters α new to I_1, and call them $\sigma_1, \sigma_2, \cdots$. We wish to prove that the number μ is not greater than q.

Let s be any one of the substitutions $\sigma_1, \sigma_2, \cdots$, and let $s = (a_1 b'_1 \cdots) \cdots$, say. The theorem has already been proved if no power of s replaces every a by a letter not an a. Then it may be assumed that some power of each of the substitutions $\sigma_1, \sigma_2, \cdots$, has this property for each pair of transitive sets of I_1 that are joined in any cycle. Now suppose that s connects transitively the $\rho + 1$ sets $a, b', b'', \cdots, b^\rho$. Each of the sets $b', b'', \cdots, b^\rho$ has this property as well as a. For if it were not true for b^i, say, let b^i be taken for a and then apply theorem IV, according to which some substitution of order p and of degree not greater than pq connects b^i with some other set of I_1 and introduces at most q new letters. Then all the letters of these $\rho + 1$ sets are displaced by s; from which it follows, if we apply theorem II to this first transitive constituent of $\{I_1, s\}$, that no new letters α are present in the cycles of s which involve $a, b', \cdots, b^\rho$.

Suppose that s^x has two new letters adjacent in some cycle:

$$s^x = (a_1 b'_1 \cdots) \cdots (\alpha_1 \alpha_2 \cdots) \cdots.$$

Now from the transformed groups $s^{\pm x} I_1 s^{\mp x}$ we may infer that letters a can be followed in s^x only by letters b' and the letters b' can be preceded only by letters a, or in other words a b' never follows a b'. Again, if one b' is followed by an a, every b' is followed by an a. Then no b' is followed by an a, since p by hypothesis is an odd prime. It should be remarked that ρ is less than q, since each set of I_1 involves at least p letters, and the letters $a, b', \cdots, b^\rho$ fill up at most $q - 1$ cycles of s, and in consequence $\rho + 1$ is less than p. Now if letters b'' follow the b''s, every b' is followed by a b'', no b'' may follow a b'', no b' may follow a b'', and if an a follows a b'', p is necessarily a multiple of 3. Then must the b'''s be followed by letters b''', while b''' may not be followed by letters b''', b'' or b', nor may it be followed by a's without making p a multiple of 4; and

so on. Finally p would be equal to $\rho + 1$, but we have seen that $\rho + 1$ is less than p. Hence no cycle of s displaces two letters α.

THEOREM V. *Let P be a cyclic group of degree pq and of order p. The largest group G on the same letters that transforms P into itself and that contains no operator of order p with less than q cycles is of order $p(p-1)(q!)$.*

The largest possible group on these letters, of which G is a subgroup, is of order $p^q(p-1)(q!)$. If G contains a substitution of order p which is not a power of a substitution of P, it certainly contains substitutions of order p and of degree less than pq. Hence the order of G is not greater than $p(p-1)(q!)$. Since we can in all cases construct a group of this order that shall transform G into itself by setting up a simple isomorphism between q metacyclic groups and adjoining substitutions which permute the q sets of intransitivity in every possible way, G is exactly of this order.

THEOREM VI. *The quotient group G/P is the direct product of a cyclic group of order $p-1$ and the symmetric group on q symbols.*

Since s, a generator of P, belongs to a set of $p-1$ conjugate substitutions, s is invariant in a subgroup I of order $p(q!)$. The quotient group I/P is symmetric. Again, s is transformed into all its powers by the substitutions of the metacyclic subgroup M of G. Let t be a substitution of I, and let u be a substitution of M that transforms s into s^x, x not congruent to unity, modulo p. Then $(t^{-1}ut)^{-1}s(t^{-1}ut) = s^x$ also. Since $\{I/P, M/P\} = G/P$, every operator of M/P is invariant in G/P. Hence the group G/P is a direct product.

COROLLARY. *When q is less than p, the substitutions of order p in the largest group G' of order $p^q(p-1)(q!)$ in which P is invariant generate an abelian group.*

THEOREM VII. *A primitive group of degree $2p+k$ $(p > k > 2)$, which does not include the alternating group, cannot contain a substitution of order p and of degree $2p$.*

Let there be given a primitive group G which contains a substitution

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

Since p is greater than 3, G can contain no substitution of order and of degree p.* There is a second substitution B, similar to A, in the transitive (because invariant) subgroup generated by the conjugates of A, which connects the two cycles of A, and displaces at most two new letters. Hence G *contains a transitive subgroup $H = \{A, B\}$ of degree not greater than $2p+2$.*

*C. JORDAN, Bulletin de la Société mathématique de France, vol. 1 (1873), pp. 40–71.

It may now be shown that if H is included in a primitive group of degree greater than $2p+2$, it is included in a group of degree $2p+3$ which is at least doubly transitive. If H is primitive this is certainly the case.* If H is of degree $2p$ and imprimitive, it cannot have two systems of p letters each, because it is generated by two substitutions of order p. If it has p systems of two letters each, it is contained in a doubly transitive group of degree $2p+3$, if not in one of degree $2p+1$. If H is of degree $2p+1$ it is certainly primitive. Finally let H be of degree $2p+2$. If the two letters left fixed by A belong to two different systems of imprimitivity, each system is of degree $p+1$, but that is not possible in $\{A, B\}$. Then the two letters left fixed belong to the same system and H has $p+1$ systems of two letters each. Since A determines this system by the two letters left fixed, the choice of systems can be effected in only one way, in other words, H is simply imprimitive with respect to a system of two letters. Hence *this group H must lead to a doubly transitive group of degree* $2p+3$. Then in G^{2p+3}, the subgroup $P=\{A\}$ is invariant in a subgroup I† which has the symmetric group of degree 3 as one constituent, which constituent we may call the group J.‡ For suppose P is transformed into itself by kp substitutions in the subgroup of G^{2p+3} which leaves two letters fixed. These kp substitutions involve only the letters of A. In the subgroup of G which leaves one letter fixed, since it is a transitive group of degree $2p+2$, P is invariant in a subgroup I_1 of order $2kp$ which has one constituent of order 2 on the two letters not displaced by A. Finally in G itself P is transformed into itself by $6kp$ substitutions and J is a transitive group of degree 3 and of order 6, a non-abelian group; while the quotient group of the largest group in which P may be invariant, involving only the letters of A, and containing no substitutions of order p and lower degree, is abelian.

It is well known that if $p=3$, the degree of G cannot exceed 9 and that there exists a primitive group G^9_{1512} of class 6 containing the substitution $(a_1a_2a_3)(b_1b_2b_3)$.

THEOREM VIII. *A primitive group of degree $3p+k$ ($p>k>3$), which does not include the alternating group, cannot contain a substitution of order p and of degree $3p$.*

In the first place G has no substitution of order p and of degree p or $2p$.

If theorem IV be twice applied, it is seen that G contains a transitive group H of degree not higher than $3p+6$ generated either by two (when the degree

* *On Multiply Transitive Groups*, these Transactions, vol. 7 (1906), pp. 499-508. This article will be used freely in what follows without further citation.

† *A Note on Transitive Groups*, Bulletin of the American Mathematical Society, vol. 13 (1906), p. 20.

‡ This notation, I for the largest subgroup of G in which $P=\{A\}$ is invariant, and J for the constituent on the letters left fixed by A, will be used throughout the remainder of this paper.

does not exceed $3p+3$) or by three similar substitutions of order p. In case the degree of H does not exceed $3p+3$ it will next be shown that G includes a doubly transitive subgroup of degree $3p+4$ whenever the degree of G exceeds $3p+3$. This is obviously true if the degree of H is $3p$, $3p+1$, or $3p+2$. If H is of degree $3p+3$, consider the three letters left fixed by $A=(a_1a_2\cdots a_p)(b_1b_2\cdots b_p)(c_1c_2\cdots c_p)$; one of them cannot belong to different systems of imprimitivity from the other two, and moreover a system of three letters may be chosen in but one way. Hence, in this case also, H leads to a doubly transitive group G^{3p+4}. Consider now the subgroup of G^{3p+4} which leaves two letters fixed. It is of order kp, say, and has perhaps one constituent of degree 2. Going back to G^{3p+4}, in it $P=\{A\}$ is invariant in a subgroup of order $12kp$ or $6kp$ which has a constituent on 4 letters which is doubly or triply transitive, that is, includes the tetraedral group. But the tetraedral group is not a subgroup of the quotient group with respect to P of the group of theorem V. Hence if the degree of G is greater than $3p+3$, the degree of H is also greater than $3p+3$.

Let H be of degree $3p+4$. It may not be imprimitive because A can only permute systems of three letters. Now if H is primitive, we know that it is simply transitive, and that the subgroup leaving one letter fixed is of degree $3p+3$, with two constituents.* One constituent cannot be of degree $2p+3$, nor can the other be of degree $p+3$ without making J tetraedral. If the larger constituent is of degree $2p+2$, or if the smaller is of degree $p+2$ (the only cases that remain) then in this intransitive subgroup of G the subgroup in which P is invariant has certainly a constituent of degree 2, so that in G itself I has a constituent of order 8 on 4 letters which involves a transposition, and hence is the octic group. But in the direct product of the symmetric group of order 6 and a cyclic group of order $p-1$ there is no octic subgroup.

Again H may be assumed to be of degree $3p+5$. It is primitive. If G^{3p+5} is doubly transitive, the subgroup leaving one letter fixed is transitive and is in turn primitive, for A in case of imprimitivity either permutes systems of three letters or leaves fixed systems of p or more letters. Just as before, this primitive group of degree $3p+4$ cannot exist. Now assume that G^{3p+5} is a simply transitive primitive group. The subgroup leaving one letter fixed has just two constituents, since $\{A, B\}$ has already a constituent of degree $2p+2$ at least. One constituent may be of degree $2p+2$, so that there will have to be a constituent of degree 5 and order 10 in I. This is impossible unless G contains a subgroup of order p^2, and $p=5$. In this case the two constituents are of degree 12 and 7. But a primitive group of degree 20 cannot contain a substitution of order 7 without including the alternating group. If there is a

*C. JORDAN, *Traité des Substitutions* (1870), p. 284; G. A. MILLER, Proceedings of the London Mathematical Society, vol. 28 (1897), p. 533.

constituent of degree $2p+3$ or $p+3$, that constituent is alternating or symmetric, and in the first case G certainly contains substitutions of order p of degree p or $2p$. In the second case, when p is greater than 5, the largest subgroup of G in which P is invariant has a transitive constituent of degree 5 which involves a cyclic substitution of order 3, that is, includes the alternating group of order 60; but this is impossible. When $p=5$, G contains a substitution of order 11, and hence must be alternating. This completes the consideration of H if it is of degree $3p+5$.

Let H be of degree $3p+6$. It cannot be doubly transitive, for then its transitive subgroup of degree $3p+5$ yields to the preceding analysis. If it is a simply transitive primitive group, its intransitive subgroup of degree $3p+5$ has just two constituents. Since $\{A, B\}$ has one constituent of degree $2p+2$ and the other of degree $p+1$, the largest subgroup of H in which P is invariant involves a transposition. But if p is greater than 5 this group has a transitive constituent of degree 6, whereas no subgroup of the direct product of the symmetric group of order 6 and a cyclic group of order $p-1$ can be written as a transitive group on 6 letters which involves a transposition. This remark holds as well when H is imprimitive. If $p=5$, and if H is primitive, H contains a substitution of order 7 involving not more than two cycles. If H is imprimitive, the subgroup leaving one letter fixed may contain no substitution of order 5 and degree 20, for such a substitution would not permute in the proper manner systems of three letters each. Then P is a Sylow subgroup, and again the subgroup of H in which it is invariant would have a constituent of degree 6 involving a transposition. This completes the proof of theorem VIII.

THEOREM IX. *A primitive group of degree* $4p+k(p>k>4)$, *which does not include the alternating group, cannot contain a substitution of order* p *and degree* $4p$.

By theorem IV, G contains a transitive subgroup H of degree not greater than $4p+12$ generated by two, three or four substitutions similar to A.

If H is an imprimitive group, its degree is $4p+2n$, where $n=0, 1, \cdots,$ or 6. If n is 3 or 5 the $2p+n$ systems of two letters each are permuted according to an alternating group, so that G is of class 6 at most. The primitive groups of class 6 are known and none is of higher degree than 10. For the same reason systems of two letters, when $n=4$ or 6, may not be permuted according to a primitive group. Now H cannot be of degree $4p+12$, because $\{A, B, C\}$ has a transitive constituent of degree $3p+6$ in which the group J is transitive and contains a transposition while having the quotient group with respect to an invariant operator a subgroup of the symmetric group on three symbols. This is true even for $p=5$. If H is of degree $4p+8$ it can have no subgroup of order p^2, for then H would include substitutions of order p hav-

ing 5 cycles, by which systems of 4 letters can neither be permuted nor left fixed. It follows that if H is contained in a doubly transitive group of degree $4p+9$, J is of degree 9 and doubly transitive. But no quotient group of the group of theorem V is simply isomorphic to a doubly transitive group of degree 9. An imprimitive group of degree $4p+10$ or $4p+14$ would be of class 10.* In the imprimitive group of degree $4p+12$ the systems of 4 letters each are permuted according to the alternating group of degree $p+3$. Since systems of two letters each are not possible, and the systems certainly contain 4 letters each, it is impossible for this group of degree $4p+12$ to have a subgroup of order p^2, even when $p=5$. Then its group J is transitive of degree 12 and of order $96m$, where m is greater than unity. Since the order of J is greater than 4! it contains an invariant operator which is regular, of degree 12, and is transformed into itself by the transitive subgroup of degree 8, so that this operator can only be of order 2 or 4, making J of order 96 at most. But we have seen that the order of J is greater than 96. Let H be of degree $4p+4$. Systems of 4 letters can be chosen in one way only. If H does not lead to a doubly transitive group of degree $4p+5$, it must lead to an imprimitive group of degree $4p+6$ with systems of two letters, which is in consequence of class 6 or less. If p is greater than 5, the doubly transitive group of degree $4p+5$ which we are led to consider can have no subgroup of order p^2, and hence J would necessarily be a doubly transitive group of degree 5, and that is impossible. Let $p=5$. Now $4p+5=25$, so that the order of G is a multiple of 125. Since P is a Sylow subgroup of the subgroup G_1 of G which leaves one letter fixed, P is invariant in a subgroup I whose constituent J is doubly transitive of order $20m$. Since the subgroup of order 5 in J is invariant, J is metacyclic. Such a group G^{25} is known to exist. It is the holomorph of the group of order 25 and type (1, 1). Its order is $25\cdot 24\cdot 20=12000$. However G^{25} is not a subgroup of a triply transitive group of degree 26, since our constituent J in such a group cannot be triply transitive of order $6\cdot 5\cdot 4=120$.

Let H be doubly transitive. Its degree is $4p+\lambda$, where we may assume that λ is greater than 5. The subgroup H_1 of H that leaves one letter fixed is imprimitive, for otherwise the substitutions of order p and degree $4p$ in it would generate a transitive group of degree $4p+\lambda-1$. H_1 has two systems of imprimitivity. The order of H_1 (when p is greater than 5) is not divisible by p^2, for then the substitutions of order p and of degree $5p$ in H_1 are incompatible with the systems of imprimitivity. If $p=5$, and 25 divides the order of H_1, each constituent of the group generated by the substitutions in H_1 of order p and degree $4p$ is of degree 15. The presence in a constituent of degree 15 of substitutions of degree 10 and also of degree 15, both of order 5, requires that it be primitive and alternating, thereby lowering the class of H to 6. Hence

*American Journal of Mathematics, vol. 28 (1904), p. 226.

the order of H_1 is not divisible by p^2. Then J, of degree λ is doubly transitive and hence has no invariant operators. But no subgroup of the octaedral group is doubly transitive on more than 4 letters, so that H cannot be doubly transitive.

It may be that H is a simply transitive primitive group. If H is of degree less than $4p+5$ it may lead to a doubly transitive group of degree $4p+5$, if our theorem is not true; but that, except for $p=5$, has been seen to be impossible. We now take up the various groups H in order.

H is of degree $4p+5$. The cyclic group P is now a Sylow subgroup of H_1, so that J is transitive of degree 5. Since H_1 is intransitive and has either two or three constituents, J is of order 10. This is certainly not possible unless $p=5$. Our theorem is still true unless H now leads to a doubly transitive group of degree $4p+6$ in which the group J (here of degree 6) is doubly transitive. But the substitutions of order p in this last group must generate an abelian group, and this is not true for a doubly transitive group of degree 6.

H is of degree $4p+6$. The order of H is not divisible by p^2 unless perhaps when $p=5$. But a substitution of order 5 and of degree 25 in H_1 requires that one transitive constituent of H_1 (of degree $5r+s$) have substitutions of order 5 both of degree $5r$ and $5(r-1)$ and hence be alternating. Then the class of H would not exceed 6. It follows that P is a Sylow subgroup of H_1 and J is a transitive group of degree 6. The transitive constituents of H_1 correspond to the 4 partitions of $4p+5$, thus:

$$3p+3, p+2;\ 2p+4, 2p+1;\ 2p+4, p+1, p;\ 2p+2, p+2, p+1.$$

The first partition requires that J be the symmetric group of degree 6, as is clearly impossible.

Now the non-regular transitive groups of degree 6 in which the quotient group with respect to an invariant substitution is a subgroup of the octaedral group may be readily set up. If there is an invariant substitution of order 3, there is one group:

(*a*) G^6_{18}, in which the quotient group is the non-abelian group of order 6.

If there is an invariant substitution of order 2 there are three groups:

(*b*) G^6_{48}, of class 2, with an octaedral quotient group. The subgroup leaving one letter fixed is octic.

(*c*) G^6_{24}, a subgroup of (*b*) corresponding to the tetraedral subgroup of its quotient group. The subgroup that leaves one letter fixed is the non-regular axial group.

(*d*) G^6_{12}, again a subgroup of (*b*), of class 4, in which the quotient group is of order 6.

If the identity is the invariant operator we have three groups:

(*e*) the octaedral group on 6 letters, written with respect to the cyclic group of order 4,

(f) with respect to an axial subgroup, and

(g) the tetraedral group put on 6 letters.

The last three groups are of class 4.

According to the second and third arrangements of the letters of H_1 in transitive sets, the constituent of degree $2p+4$ must be imprimitive, since it cannot be an alternating group. The group J belonging to it cannot be the octic group. This consideration bars these two partitions at once, since then J must contain a transposition. In the case of the last partition $(2p+2, p+2, p+1)$ there is in J_1 a substitution of order 2 and degree 4. Since this substitution is not invariant in J, it corresponds to operators in the tail of I which transpose systems. But only two systems may be transposed. Hence the entire operator of order 2 is a negative substitution, while H is a positive group.

H is of degree $4p+7$. A substitution of order 7 in J cannot be invariant and a subgroup of order 7 can be invariant only if $p=7$ and J is of class 6. There are only two possible partitions of $4p+6$ corresponding to the arrangements of the letters of H_1 in transitive sets which may permit J to be of class 6. One is $(3p+6, p)$ and since $\{A, B\}$ must have a constituent of degree $2p+2$, J is not of class 6. The other partition is $(2p+2, p+2, p+2)$. The group $\{A, B\}$ in this case has constituents of degrees $2p+1, p+1, p+1$. The constituent of degree $p+2=9$ in H_1 is triply transitive. The larger constituent is doubly transitive because of $\{A, B\}$ and hence the group of degree 9 is alternating. But a doubly transitive group of degree 16 may not have the alternating group of degree 9 as a quotient group. Or it is easy to see that the order of such a group may not be divisible by 81.

H is of degree $4p+8$. There are two possible partitions of $4p+7$, the degree of H_1: $3p+6, p+1$; and $2p+4, p+1, p+2$. If the order of H is a multiple of p^2, $p=5$ or 7, and hence a constituent of H_1 of degree $3p+6$ or $2p+4$ may not be imprimitive as none the less it must be. In the first place J is of class 2 or 3 and therefore not primitive. But an imprimitive group of degree 8 cannot have a substitution of degree and order 3 unless there are two systems of imprimitivity of 4 letters each. Two such systems however cannot be permuted by the transitive subgroup of degree 6. In case of the second partition the constituent of degree $2p+4$ must be imprimitive, and, since $\{A, B\}$ has a transitive constituent of degree $2p$ or $2p+2$, this constituent of degree $2p+4$ has a transitive subgroup of degree $2p+2$. Then in H the order of J is divisible by 64. But since the order of the quotient group of J taken with respect to the invariant substitution is a divisor of 24, the invariant operator is of order 8, an impossibility.

H is of degree $4p+9$. For the degree of H_1, the partition $(2p+4, 2p+4)$ is impossible inasmuch as each constituent is necessarily imprimitive, so that $\{A, B\}$ has one constituent of degree $2p+2$ and hence in $\{A, B, C\}$,

which is included in H_1, the substitution C may (by theorem III) be supposed to have been chosen in such a way that the last named group has one constituent of degree $3p + k$. Then the constituents of H_1 are of degrees $3p + 6$ and $p + 2$. The factor p^2 cannot enter the order of H. The order of J is a multiple of 27, but J cannot have an invariant operator of order 9.

If H is of degree $4p + 10$, $4p + 11$, or $4p + 12$, one constituent of H_1 certainly includes an alternating group, and in consequence H has substitutions of order p on less than 4 cycles.

We have now considered all possible cases that might lead to an exception to the theorem. It has been proved too that when $p = 5$, the degree of G may be as high as 25 but may not exceed 25 unless G includes the alternating group.

STANFORD UNIVERSITY,
July 26, 1908.