ON THE ORDER OF PRIMITIVE GROUPS, II*

BY

W. A. MANNING

As early as 1873 Jordan proved that *a non-alternating primitive group cannot contain a substitution of degree and order p (p a prime) if its degree exceeds* $p+2$. On page 176 of the first volume of the Bulletin of the Mathematical Society of France he explicitly stated this theorem, as having been proved on page 42 of the same volume. There one finds, "*Let p be an odd prime; a group of degree $p+k$ cannot be more than k times transitive unless it contains the alternating group.*" This of course is seen to cover the theorem stated, if one has in mind (from page 664 of the *Traité des Substitutions*, 1870) "*If a group contains a circular substitution of prime order p it is $n-p+1$ times transitive.*" It is easy to infer that the order of a non-alternating primitive group of degree n cannot exceed $n!/(2\cdot 3\cdots p)$, where $2, 3, \cdots, p$ are the distinct primes less than $n-2$. For if p^α is the highest power of p in $n!$ a group of order p^α and of degree not greater than n certainly contains substitutions of degree and order p. Even so we have a great improvement on the theorem that asserts a limit of the same form but imposes upon p the greater restriction $p < 2n/3$.†

In the paper‡ bearing the same title as the present one, and of which this is a continuation, was proved

THEOREM X. *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 $pq+q+1$.*

By means of this theorem and our knowledge of the primitive groups of class less than 14§ it is possible to further limit the order of a primitive group of given degree. The desired connection is established by means of

THEOREM XI. *Let p^α, p^β be the highest powers of p that divide n and*

* Presented to the Society (San Francisco Section), Feb. 27, 1909.

† Burnside, *Theory of Groups*, 1st edition, p. 199; 2d edition, p. 207.

‡ These Transactions, vol. 10 (1909), p. 247.

§ *The Primitive Groups of Class Twelve*, American Journal of Mathematics, vol. 35 (1913), p. 229.

pq respectively, $n > pq$. Let G be a group of degree n that contains no substitution of order p on so few as q cycles. Then the Sylow subgroup of G corresponding to the prime p is not of higher order than $p^{\alpha-\beta}$.

Suppose the order of the Sylow subgroup of G is $p^{\alpha-\beta+k}$. The Sylow subgroup of the symmetric group of degree n which includes this group of order $p^{\alpha-\beta+k}$ contains also a subgroup of order p^{β}, the Sylow subgroup of the symmetric group of degree pq. Since these two subgroups, of orders $p^{\alpha-\beta+k}$ and p^{β}, have no substitution in common, k is necessarily zero.

Then if the order of a primitive group G of degree n does not divide $n!/(2^{10}\,3^5)$ its class is less than 13, and by theorem X, the order of G (of class greater than 12) must divide $n!/(5^4 \cdot 7^4 \cdots p_4^4 \cdots p_3^3 \cdots p_2^2 \cdots p_1)$, where $5, 7, \cdots p_1$ are all the distinct primes greater than 3 and less than $n - 2$, where those primes less than $n/2 - 1$ are squared, those less than $n/3 - 1$ are cubed, those less than $n/4 - 1$ are raised to the fourth power, unless G is of degree 25 and contains a transitive Sylow subgroup of order 125.*

Jordan also proved that *if a primitive group G contains a substitution of prime order p on 5 cycles, $p > 5$, and does not include the alternating group, its degree cannot exceed $5p + 6$.* If this theorem is used, and a proof of it will presently be given, we may formulate the inclusive theorem:

THEOREM XII. *The order of a primitive group (G) of degree n and of class greater than 12 divides $n!/(2^{10} P_1 P_2 P_3 P_4 P_5)$, where P_1 is the product of all the odd primes less than $n - 2$, P_2 the product of those less than $n/2 - 1$, P_3 the product of those less than $n/3 - 1$, P_4 the product of those less than $n/4 - 1$, and P_5 the product of those less than $(n - 1)/5 - 1$, unless* (1) *G, of degree 25, contains a substitution of order 5 on 4 cycles, or* (2) *G, of degree not greater than 45,*† *contains a substitution of order 5 on 5 cycles.*

The exact determination of these exceptions is not here attempted. The author prefers to leave the question open until he has had opportunity to complete the examination of the groups of classes 14 and 15. The remainder of this paper will be devoted to a proof of that part of Jordan's theorem that remains as yet without a published proof,—that relating to *the primitive groups which contain a substitution of prime order p $(p > 5)$ on 5 cycles.*

From theorem IV of the preceding paper it follows that the primitive group G in question contains a transitive subgroup H generated by substitutions of order p and of degree pq. These generators $A, B, \cdots$ are of such a nature that if an intransitive subgroup I_1 generated by a certain number of them taken in order be fixed upon, then the next substitution in the series connects at least two sets of intransitivity of I_1 and has in no cycle more than

* *On the Order of Primitive Groups,* these Transactions, vol. 10 (1909), pp. 255 and 256.

† For this limit 45, see these Transactions, vol. 12 (1911), p. 375.

one letter not already displaced by I_1. Hence the degree of H does not exceed $pq + (q - 1)q$.

When H is an imprimitive group, generated by substitutions of order p and degree pq, the systems of imprimitivity are permuted by these substitutions of order p, so that *the number of letters in any system divides* q. In the present case q is 5, so that imprimitive systems of 5 letters each are permuted according to a primitive group of degree $p + k$, $0 \leqq k \leqq 4$. The new letters introduced by B, or by C, $\cdots$ form a system of imprimitivity. Then if $\{A, B\}$ is not of degree $5p$, it is of degree $5p + 5$ and causes the group* J to be of class 5 or less. Now the head of H, when it is not the identity, has transitive constituents of degree 5. Then the order of H divides $(5!)^{p+k}((p+k)!)$. This number is not divisible by p^2. Hence all subgroups of H of order p are Sylow subgroups. Then J is a transitive group, and must have imprimitive systems of 5 letters each. When k is greater than unity there are substitutions of class less than 5 in J and they can permute no systems of 5 letters; therefore $J(k > 1)$ has an intransitive subgroup leaving fixed each of the k systems. Each constituent of this head is of degree 5 and of order greater than 5. If the letters of a substitution in J of degree 4 or less all belong to the same system, the head is a direct product. If they belong to different systems, each constituent is a symmetric group of degree 5. But we recall that J is a transitive representation on $5k\,(k = 2, 3, 4)$ letters of the direct product of a cyclic group and a subgroup of the symmetric group on 5 symbols. The symmetric group is included among its own subgroups. Then J can only be of class 4 with $k = 2$, when it is a simple isomorphism between two symmetric groups permuted by an invariant substitution of order 2. Since systems of imprimitivity of H may be chosen in but one way, $H(k = 2)$ must be found in a primitive group of degree $5p + 10$ or $5p + 11$. However J cannot be written as a non-regular group of degree 11. After having studied the simply transitive primitive groups of degree $5p + 10$ we shall return to the imprimitive group H of that degree and show that it cannot be contained in a primitive group of degree $5p + 10$.

In case H is a multiply transitive group of degree greater than $5p$, H_1, the subgroup leaving one letter fixed, cannot be primitive, for then the subgroups of order p and degree $5p$ in H_1 would generate a transitive group. H$_1$ is therefore imprimitive and the substitutions of order p and degree $5p$ generate an intransitive group with the same number $p + k$ of letters in each constituent. Then H_1 does not involve the subgroup $\{A, B\}$, which it certainly would, were its degree as great as $5p + 5$. Then H_1 is of degree $5p$, and H, when doubly transitive, is of degree not greater than $5p + 1$.

* I is the largest subgroup of the transitive group under discussion in which $\{A\}$ is invariant, and J is the constituent (or constituents) of I in the letters left fixed by A.

Let us now assume that H is a simply transitive primitive group. The subgroup H_1 that leaves one letter fixed is intransitive and displaces all but one of the letters permuted by the group H. Another theorem for which we are indebted to Jordan is that if a given prime p divides the order of one transitive constituent of the subgroup leaving fixed one letter of a simply transitive primitive group, then does p divide the order of every constituent of that subgroup. Hence *H_1 has no transitive constituent of degree less than p.*

LEMMA I. *If a constituent of H_1 is alternating or symmetric, the degree of H is at most $5p + 6$ and p is 7. In no case is H of higher degree than $5p + 10$, nor does H contain a subgroup of order p^2.*

If a substitution of order 3 on 15 letters is present in H, it has elsewhere been proved that the upper limit of the degree of H is 41.* This is possible only when p is 7, and then $41 = 5 \cdot 7 + 6$.

Let us make the assumption, to be removed later, that there is no substitution of order 5 and degree 25 in H.

If a constituent of maximum degree is alternating the remaining constituents are simply isomorphic to it. Now when n is greater than 6 the symmetric group of degree n is the holomorph of the alternating group of degree n, so that here, where the degree of any constituent of H_1 is at least 7, H_1 contains substitutions of order 3 on as many cycles as it has constituents. Hence a constituent of maximum degree cannot be an alternating or symmetric group. Let us see if any constituent of H_1 can include the alternating group of its degree.

Suppose that H_1 has just two constituents. If one constituent is alternating it is of lower degree than the other. Again, if the isomorphism is simple, the alternating group can only be of degree 7 or 8 ($p = 7$) and the other constituent is of degree $4 \cdot 7 + 2 = 30$ or $4 \cdot 7 = 28$ respectively, so that H_1 is of degree $5p + 2$ or $5p + 1$, cases which occasion no difficulty. Let the smaller constituent be alternating with the second constituent in an $(m, 1)$ isomorphism to it. The subgroup of order m cannot be transitive, since H is simply transitive. Then the larger constituent is imprimitive. If one substitution of order p in the larger constituent permutes systems, all the substitutions of order p permute systems and there are in this case no substitutions of order p in the intransitive head. Then the tail, isomorphic to an alternating group, permutes the systems accordingly. There are not more than four letters in a system, so that there is a substitution of order 5 and degree 25 in H_1. Now one substitution of order p in the larger constituent certainly permutes systems because at least one such substitution is in the tail of that constituent. The above applies *a fortiori* if the smaller constituent is symmetric. The conclusion is that neither of *two* constituents

* These Transactions, vol. 12 (1911), p. 375.

can be alternating or symmetric. It follows that the degree of H_1 is not in excess of $5p + 10$.

If p^2 divides the order of H_1, p can only be 7 and one of the two constituents is of degree $4p + 8$, an imprimitive group with $p + 2$ systems of 4 letters each. Such a group however does not admit the factor 49 in its order.

Let H_1 have three constituents, and suppose that one of them, not of maximum degree, is alternating. If a second constituent is of the same degree, it is also alternating. Since the larger constituent cannot be in simple isomorphism ($p \overset{=}{>} 7$) to these groups, it would have an intransitive head, be imprimitive, and require a substitution of order 5 and degree 25 in H_1. Then both the remaining constituents are of higher degree than the alternating constituent and neither can be of degree less than $2p$. The alternating group is of degree $p + k$. In neither of the two groups of higher degree is the invariant subgroup the identity. Nor can both these constituents be imprimitive. For consider an imprimitive group of degree $2p + k_1$. If no substitution of order p permutes systems, two alternating groups in simple isomorphism are permuted by a substitution of order 2, which after all means that substitutions of order p permute systems of two letters each in all cases. Then H_1 contains a substitution of order 3 and of degree 15. Hence at least one of the larger constituents is primitive. It is evident that in this event p^2 does not divide the order of H_1 even when p is 7, because the order of a non-alternating primitive constituent of degree at most $2p + 2$ is not divisible by $p^2 = 49$. If the latter were divisible by p^2 it would contain a cycle of p letters. Now consider a non-alternating primitive constituent of degree $2p + k_1$. If the subgroup leaving one letter fixed is imprimitive, it either contains invariantly a simple isomorphism between two alternating groups each of degree greater than 6, or else permutes systems of two letters each according to an alternating group. But this constituent cannot be of so low a class as 6. Again, if the subgroup leaving one letter fixed is primitive, it is in a multiple isomorphism to an alternating group, and by applying the same analysis we must at last come to a subgroup that is a simple isomorphism between two alternating groups and is of class 6, or to an imprimitive subgroup that has systems of two letters permuted by an alternating group, also of class 6. Finally if the constituent in question is simply transitive its subgroup leaving one letter fixed is a simple isomorphism between two alternating groups, giving class 6 again. Hence when there are just three constituents in H_1 no one of them can be alternating (or symmetric). This again reduces the degree of H_1 to $5p + 10$ at most. The order of H_1 is not divisible by p^2.

Let there be four constituents in H_1. Now H_1 does not include the group $\{A, B, C\}$ and its degree is at most $5p + 9$. Three constituents are alternating groups of equal degree $p + k$. Except for $p = 7$, with one constituent of degree 15 and the others of degree 8, and H_1 of degree $5p + 4$, the constituent of degree $2p + k_1$ cannot be in simple isomorphism to these alternating groups, nor can it have an invariant transitive head. If it is imprimitive with $p + k$ systems of two letters each, H_1 includes a substitution of degree 15 and order 3.

If there are five constituents, H_1 is of degree less than $5p + 5$.

Let us now remove the restriction upon H, that it contain no substitution of order 5 and degree 25. If such a substitution is present, H is not of higher degree than 45, and consequently $p = 7$. We return to the cases in the preceding paragraphs in which use was made of the presence of a substitution of order 5 in H.

Case when H_1 has just two constituents. The larger is imprimitive and in an $(m, 1)$ isomorphism to an alternating or symmetric group. Substitutions of order 11 in the imprimitive group cannot permute systems at the same time with substitutions of order 7. Then the alternating constituent is at most of degree 10. Hence the constituents of H_1 are of the degrees 7, 28 or 8, 32.

Case when H_1 has three constituents. The largest is imprimitive and there are two alternating constituents of equal degree less than 11 as before. Hence the degrees are 7, 7, 21 or 8, 8, 24 respectively.

In no case does 49 divide the order of H. This completes the proof of Lemma I.

We shall now prepare a list of the groups J of degree $6, \cdots, 10$ inclusive that are non-regular and with its aid prove

LEMMA II. *The transitive group* $H = \{A, B, \cdots\}$ *is in no case of higher degree than* $5p + 5$.

The principle employed in the construction of this list is that J is the direct product of a cyclic group and a subgroup of the symmetric group of order 120, the product being represented transitively on n letters, $n = 6, 7, \cdots, 10$.

Let h be the order of the cyclic group and kk' the order of the subgroup of the symmetric-5 group. The necessary and sufficient condition for the representation is that the subgroup (K) of the symmetric-5 have a subgroup (K') of order k' such that no subgroup of K' is invariant in K and that $kh = n$. Since $k' \mp 1$, the least value of k is 3, so that h is one of the numbers 1, 2, or 3. We arrange these groups in the descending order of their degrees.

There are 8 groups J of degree 10. In the first four $h = 1$.

(1) The symmetric G_{120}^{5} gives an imprimitive J_{120}^{10}, in which J_1 (the subgroup leaving one letter fixed) is the G_{12}^{4}, here intransitive on two sets of letters. Each constituent of J_1 is doubly transitive. The class is 6.

(2) The G_{120}^{5} has an intransitive subgroup of order 12 with respect to which we have a primitive J_{120}^{10}. The J_1 is intransitive. One constituent is of order 12 and the other of order 6. This J is the group of the permutations of the ten products ab, ac, $\cdots$. It contains negative substitutions and is of class 6.

(3) The positive subgroup J_{60}^{10} is primitive and of class 8. J_1 is a $(1, 1)$ isomorphism between a regular and a non-regular symmetric-3 group.

(4) The metacyclic G_{20}^{5} is an imprimitive J_{20}^{10} of class 8.

In the remaining four groups of degree 10, $h = 2$.

(5) The direct product of the symmetric-5 and the cyclic-2 gives us an imprimitive $\pm J_{240}^{10}$. The J_1 is G_{24}^{4} on two sets of four letters each. The class is 4.

(6) The direct product of the alternating-5 and the cyclic-2 is an imprimitive $\pm J_{120}^{10}$. J_1 is G_{12}^{4} on two sets of four letters each. The class is 6.

(7) The direct product of the metacyclic G_{20}^{5} and a cyclic-2 is an imprimitive $\pm J_{40}^{10}$. The J_1 is the cyclic-4 on two sets of letters. The class is 8.

(8) The direct product of the semi-metacyclic G_{10}^{5} and the cyclic-2 is an imprimitive $\pm J_{20}^{10}$. It is of class 8.

The H_1 of a primitive group H of degree $5p + 10$ is an intransitive group of degree $5p + 9$, and has not more than four constituents since it contains $\{A, B\}$. No constituent is alternating. There cannot be just two constituents, for one of them would necessarily be of degree $4p + 8$, from which it would follow that J_1 is transitive. But on consulting the above list this is seen to be impossible. If there are three constituents of the degrees $3p + n$, $p + n'$, $p + n''$, we must have $n = 6$, $n' = 2$, so that J_1 has a constituent of degree 6 along with one of degree 2. This our list forbids. If the partition of the degree of H_1 corresponding to its transitive sets is $2p + n$, $2p + n'$, $p + n''$, then must $n = n' = 4$. The first two constituents are each imprimitive with $p + 2$ systems of two letters each. J is transitive of degree 10, J_1 is intransitive of degree 8, with two sets of four letters each. These constituents of J_1 are imprimitive, since J_1 must respect the systems of H_1. Furthermore each constituent of J_1 involves a transposition. But in none of the groups J^{10} as listed does J_1 involve an octic constituent. Finally let there be four constituents in H_1. Their degrees can only be $2p + 4$, $p + 2$, $p + 2$, $p + 1$, always bearing in mind that no constituent is alternating. Now if $\{A, B\}$ has constituents of degrees $2p + 2$, $p + 1$, $p + 1$, $p + 1$, J involves a transposition, which we know is not possible, consequently the degree of the large constituent of $\{A, B\}$ is not greater than $2p + 1$. This leads to the contradiction that H_1 includes $\{A, B, C\}$.

We return to the hypothesis that H is an *imprimitive* group of degree $5p + 10$. It was shown that J in this case is (5) of our list. Since there is a subgroup of degree $5p+5$, transitive in $p+1$ systems, the other five letters belong to one system, that is, systems of five letters can be chosen in only one way. Then H is included in a primitive group of degree $5p+10$ or $5p+11$. The latter is impossible since J cannot be of degree 11. Nor can a primitive group containing H be of degree $5p+10$. For if it is simply transitive we apply to it the reasoning employed in the case of a simply transitive primitive H of degree $5p+10$. Since J^{10} is in no case doubly transitive, this group cannot be doubly transitive. Hence H, if imprimitive, is not of higher degree than $5p+5$.

Next in order we have to consider the simply transitive primitive groups H of degree less than $5p+10$. In continuation of our list of possible groups J, we note that if $h=1$ or $h=2$, there is no transitive J, but if $h=3$ we have one group:

(9) The direct product of the symmetric group of order 6 and the cyclic-3 represented on 9 letters. This imprimitive $\pm J_{18}^{9}$ is of class 6.

In a simply transitive primitive group H of degree $5p+9$, H_1 is of degree $5p+8$ and has at most four constituents. No partition of $5p+8$ is consistent with a J_1 of order 2 and degree 6.

The groups J on 8 letters are:

(10) The G_{24}^{4} may be written as an imprimitive group of class 6.

(11) The direct product of the G_{24}^{4} and the cyclic-2 is an imprimitive J_{48}^{8} of class 4.

(12) The direct product of G_{12}^{4} and G_{2}^{2}. This J_{24}^{8} is of class 6.

(13) The direct product of G_{8}^{4} and G_{2}^{2}. This J_{16}^{8} is of class 4.

Consider the intransitive H_1 of degree $5p+7$. There are at most 4 constituents. The (10), (11), (12) are not possible as groups J because they call for two constituents of degree $lp+3$ in H_1. Neither is (13) possible because two constituents of degree $lp+2$ do not permit us to build up the degree $5p+7$.

Let J be of degree 6. We represent

(14) G_{120}^{5} as a triply transitive $\pm J_{120}^{6}$ of class 4.

(15) G_{60}^{5} as a doubly transitive J_{60}^{6} of class 4.

(16) G_{24}^{4} as an imprimitive J_{24}^{6}. J_1 is axial and transitive.

(17) G_{24}^{4} as an imprimitive J_{24}^{6}. J_1 is cyclic and transitive.

(18) G_{12}^{4} as an imprimitive J_{12}^{6} of class 4.

(19) $G_{6}^{3}\times G_{2}^{2}$ as an imprimitive J_{12}^{6} of class 4.

Now H is of degree $5p+6$. Since H_1 is intransitive the five letters of J_1 can not form a single transitive set. This bars (14) and (15). If in I (the largest subgroup of H in which $P=\{A\}$ is invariant) the five cycles of A were connected transitively, then would substitutions of order 5 certainly be found in it. Hence the cycles of A are not connected transitively by I. In (16), (17), and (18) the intransitive head of J is the axial group

$$1, \quad \alpha\beta \cdot \gamma\delta, \quad \alpha\beta \cdot \epsilon\zeta, \quad \gamma\delta \cdot \epsilon\zeta,$$

and when we adjoin $\alpha\beta \cdot \epsilon\zeta$ to the subgroup of J which leaves ϵ fixed we obtain an intransitive subgroup of J. Hence there is a substitution in I, not in H_1, which with H_1 generates an intransitive subgroup of H. But H_1 is maximal since H is primitive. This leaves only (19) to which the same reasoning applies, inasmuch as the invariant head of this diedral rotation group is $1, \alpha\beta \cdot \gamma\delta \cdot \epsilon\zeta$.

It has now been proved that G contains a transitive group $H = \{A, B, \cdots\}$ of degree not greater than $5p + 5$. If H is imprimitive its degree is $5p$ or $5p + 5$. Since in the latter case systems of five letters can be chosen in but one way, H, if contained in a primitive group of higher degree is found in a doubly transitive group of degree $5p + 6$. If H is primitive, it too may lead to a doubly transitive group of degree $5p + 6$. It is evident that the group of degree $5p + 6$, if it exists, is in neither case quadruply transitive nor is it a subgroup of a group of degree $5p + 7$. The possibility of the occurrence of the degree $5p + 6$ is due to the representation of the alternating and symmetric groups of degree 5 on six letters. It may be remarked that a substitution of order 3 and degree $3(p + 2)$ is present in this case.

STANFORD UNIVERSITY, CAL.