ON THE ORDER OF PRIMITIVE GROUPS* (IV)

BY

W. A. MANNING

1. The last result under the above title was to the effect that a primitive group G of class greater than 3 which contains a substitution of prime order p and of degree qp, $p > 2q - 2$, and $q > 1$, is of degree less than or equal to $qp + 4q - 4$, and that p^2 does not divide its order.† Of course it is probable that this limit is higher than need be. For one thing, it depends on Bochert's theorem and there is good reason for supposing that Bochert's limits for the class of multiply transitive groups in terms of their degree are too low. I now propose to set limits to the degree of G when q is 6 and p is greater than q, and then to interpret this result in terms of the order of primitive groups of given degree. Some preliminary details will be disposed of before going on with the case $q = 6$. A theorem of which repeated use will be made is the following:

2. THEOREM XVI. *A simply transitive primitive group in whose sub-group that leaves one letter fixed there is one and only one doubly transitive constituent of degree m must have in this maximal subgroup at least one transitive constituent the degree of which is a divisor* $(> m)$ of $m(m-1)$.

Let G be the simply transitive primitive group and let g be its order and n its degree. Let $G(x)$ be its subgroup that leaves one letter x fixed. Let $a_1, \cdots, a_m$ be the letters of the given doubly transitive constituent (A) of degree m of $G(x)$. The order of $G(x)$ is g/n, that of $G(x)(a_1)$ (fixing first x and then a_1) is g/nm, and that of $G(x)(a_1)(a_2)$ is $g/nm(m-1)$. Obviously $G(x)(a_1) = G(a_1)(x)$.

The subgroup $G(x)(a_1)$ has a transitive constituent of degree $m - 1$ in the letters $a_2, a_3, \cdots, a_m$. In the subgroup $G(a_1)$, x is a letter of a transitive constituent of degree m. If in $G(a_1)$ the letters $a_2, \cdots, a_m$ form a transitive constituent of degree $m - 1$, or if they form with x a transitive constituent of degree m, $G(x)$ is not maximal. If the transitive constituent $a_2, \cdots$ of $G(a_1)$ is of degree m the order of $G(a_1)(a_2)$ is g/nm, and it follows that x is in a transitive constituent of degree $m - 1$ of $G(a_1)(a_2)$ and therefore is

* Presented to the Society October 29, 1917.

† These Transactions, *The order of primitive groups* (III), vol. 19 (1918), p. 127. This paper is referred to by the Roman numeral "III."

in a doubly transitive constituent of $G(a_1)$ of degree m. But the transitive constituent $a_2, \cdots$ of $G(a_1)$, being of degree m, is also doubly transitive. If now $G(a_1)$ is transformed into $G(x)$, $G(x)$ is seen to have two doubly transitive constituents of degree m, contrary to hypothesis. Hence in $G(a_1)$ the letters $a_2, \cdots$ form a part of a transitive constituent of degree $M > m$. Then $G(a_1)(a_2)$ is of order g/nM, and if x is one of y letters transitively connected by $G(a_1)(a_2)$, $g/nMy = g/nm(m-1)$, and $My = m(m-1)$. A substitution of G that transforms $G(x)$ into $G(a_1)$ transforms some transitive constituent $b_1, b_2, \cdots, b_M$ into the set $a_2, a_3, \cdots, a_m, \cdots$, and in particular some subgroup of that constituent has a transitive set of degree $m-1$, conjugate to the transitive constituent $a_2, \cdots, a_m$ in $G(a_1)(x)$.

3. It will be of advantage to study rather closely certain imprimitive groups of degree $mp + 2m$ that are generated by two or three similar substitutions of order p and of degree mp, and in which systems of m letters each are permuted according to a triply transitive group of degree $p+2$. Let E be such a group and let m be less than p. It follows that the order of E is not divisible by p^2. Set up for E the series of generators $A_1, A_2, \cdots$. A_2 connects cycles of A_1 and has at most one new letter in any cycle. Then H_2 (III, § 11) is of degree $mp + m$ at most. A_3 connects at least two constituents of H_2 and has at most one new letter in any cycle, and so on. The first transitive group in the series we call H_{r+1}, and it is an imprimitive group of degree mp, $mp + m$, or $mp + 2m$. If H_{r+1} is of degree mp, we may take a substitution A_{r+2} with at least one, and with at most m new letters, which with H_{r+1} generates a transitive group of degree $mp + m$. If H_{r+1} of degree $mp + 2m$ is the first transitive group in the series $H_1, H_2, \cdots$, we see that there is a subgroup $H_i (i = 2, 3, \cdots, r)$ with fewer than m sets of intransitivity and of degree $mp + m$, thereby insuring the existence in the group J_1 of H_{r+1} (III, § 19) of a substitution of degree not greater than m and on letters of one only of the two systems of imprimitivity of m letters each of J_1. The head of J (the J-group of E) of index 2, is then either a direct product of two conjugate transitive subgroups of J of degree m each, or is an (n, n) isomorphism $(n > 1)$ between two similar transitive groups of degree m. This J of E always contains its invariant intransitive direct product of order n^2.

On the other hand, if I, the largest subgroup of E in which $\{A_1\}$ is invariant, contains no substitutions which fix every letter of A_1, then J, a transitive group of degree $2m$, is the direct product of a cyclic group of order d (d divides $p-1$) and of a quotient-group K that occurs among the groups of degree less than m. We construct J by writing K as a transitive group of degree $2m/d$ in d different sets of letters, and simply isomorphic to itself in such a way that the substitution of order d permutes these d sets and transforms every substitution of K into itself. If $d = 2$, the two sets of letters of K are cer-

tainly not systems of imprimitivity of J as determined by E. All substitutions of J not in K are of degree $2m$. Then there must be in K a subgroup of order $kk'/2$ which with t (of order d) generates in J the required intransitive head of index 2. This subgroup of order $kk'/2$ of K must therefore contain an invariant subgroup that is a direct product of square order. The same is true of K if d is greater than 2, or if $d = 1$. It is at once clear that m is not 2, 3, or 5. When $m = 4$, the octic group may be used for K, but the octic group is the only group of degree 4 that can be so used. Since J is not the regular octic, $d = 2$ and J is of order 16. Thus J may be generated by $ab\cdot ef$, $ac\cdot bd\cdot eg\cdot fh$. and $ae\cdot bf\cdot cg\cdot dh$. Here $abef$ and $cdgh$ are two systems of imprimitivity of E.

Then if $m = 2$, J is octic; if $m = 3$, J is of order 18, 36, or 72; if $m = 4$, the order of J is 16, 32, $\cdots$, $2\cdot 24^2$; if $m = 5$, the least value of the order of J is 50; and if $m = 6$, the least order of J is 24, when J is

$$\{ab\cdot cd\cdot ef,\ gh\cdot ij\cdot kl,\ acebdf\cdot gikhjl,\ ag\cdot bh\cdot ci\cdot dj\cdot ek\cdot fl\}.$$

As an example we may write the group of order 960:

$$\{abc\cdot ghi,\ ahd\cdot gbj,\ abe\cdot ghk\}$$
$$= \{ag\cdot ek,\ bh\cdot ek,\ ci\cdot ek,\ dj\cdot ek,\ abc\cdot ghi,\ abd\cdot ghj,\ abe\cdot ghk\}.$$

There are 40 subgroups of order 3, each of which is invariant in such a subgroup as

$$\{abc\cdot ghi,\ dj\cdot ek,\ ag\cdot bh\cdot ci\cdot dj,\ ab\cdot gh\cdot de\cdot jk\}.$$

Similarly when $p > 3$ and $m = 2$, there occurs an Abelian subgroup of order 2^{p+1} generated by such substitutions as $dj\cdot ek$. Now that subgroup of I which fixes every letter of A_1 is invariant in J and when not merely the identity (sometimes when $m = 4, 6, \cdots$) certainly includes substitutions from the head of J which involve letters of both systems of imprimitivity. Then the conjugates of this subgroup in E generate an invariant intransitive subgroup of E which does not permute any systems of imprimitivity of m letters each.

4. An intransitive group H_{ij} (III, § 10) may be regarded as an isomorphism between two constituents, one of which is transitive. We impose on H_{ij} the conditions that its order is divisible by p but not by p^2 and that the order of every transitive constituent is divisible by p. These two constituents we are using have a common quotient group of order $sp = n(kp + 1)p$, that is, the quotient group has just $kp + 1$ subgroups of order p. The head of the transitive constituent is of order $r' = l'(h'p + 1)$; the subgroup of order $r'p$ formed by adjoining a substitution of order p to the head of order r' has just $h'p + 1$ conjugate subgroups of order p, and in it each subgroup of order p is invariant in a subgroup of order $l'p$ in which there is an invariant

subgroup of order l', that is, is invariant in a group which is a direct product of two groups, one of order l' and one of order p. Then in this transitive constituent each subgroup of order p is invariant in a subgroup I' of order $l'np$ and there are in it just $(h'p+1)(kp+1)$ subgroups of order p. In the other constituent, perhaps intransitive, a subgroup of order $r''p$ has $h''p+1$ subgroups of order p and the entire constituent of order rsp has $(h''p+1)(kp+1)$ subgroups of order p, each of which is invariant in a subgroup I'' of order $l''np$. Now H_{ij} is of order $r'r''sp$ and has $(h'p+1)(h''p+1)(kp+1)$ conjugate subgroups of order $l'l''np$. Now I is intransitive and has two invariant subgroups of the orders l' and l'' in different sets of letters which have nothing but the identity in common, so that I is an (l', l'') isomorphism between two groups of order $l'np$ and $l''np$ which have a common quotient group of order np. No substitutions of the subgroup of I of order $l'l''$ transform the substitution A_1 of order p into a power other than the first. From this result we infer that the group J', which is a transitive constituent of I', is also a transitive constituent of the (l', l'') isomorphism between I' and I'', that is, *the transitive constituents of the J-group of H_{ij} are the J-groups of the transitive constituents of H_{ij}.* This answers a question raised in III, § 21.

5. THEOREM XVII. *The degree of a primitive group G of class greater than 3 which contains a substitution of order p and of degree $6p$, p a prime number greater than 6, is not greater than $6p+10$.*

This theorem will first be proved on the assumption that p is greater than 7, and in § 8 we shall examine the case of $p=7$.

If H_{r+1} (III, § 11) is imprimitive, H_{r+s} (III, § 18) has systems of imprimitivity of 2, 3, or 6 letters permuted according to a primitive group that is not triply transitive, that is, according to a primitive group of degree $3p+3$, $2p+2$, or $p+1$ at most in each case, so that the degree of H_{r+s} is at most $6p+6$. Clearly the order of H_{r+s} is not divisible by p^2 and therefore a multiply transitive group G of degree $6p+7$ that includes H_{r+s} does not exist.

Let H_{r+1} be a primitive group. Its subgroup F (III, § 36) is an intransitive group in which no constituent is alternating and in which no imprimitive constituent has systems permuted according to an alternating group. Then the degree of F does not exceed $6p+12$. The order of F is not divisible by p^2 (III, § 27) nor is the order of the subgroup of H_{r+1} that leaves one letter fixed divisible by p^2. The degree of F is not $6p+13$ because, in H_{r+1}, J_1 can not be of degree 13 (III, § 19 and § 23).

The group I_1 that occurs in H_{r+1} has no substitutions on letters of J_1 only, for then G would be of class less than 13 and therefore of degree less than 36. Then J_1 is a transitive representation of the direct product of a cyclic group of order d and of a group of degree less than 7. Any quotient group of a

group of degree less than 7 is to be found as a group on less than 7 letters. Let a group K of order kk' and of degree less than 7 be multiplied into a cyclic group of order d. The direct product of order $kk'd$ can be represented as a transitive group on dk letters if and only if the group K of order kk' has a subgroup K' of order k' no subgroup of which (identity excluded) is invariant in K. Call the subgroup of J_1 that leaves one letter fixed J_1'. It should be noticed that J_1' is certainly not the identity if the degree of H_{r+1} exceeds $qp + q$. When $d > 1$, J_1 may be constructed by first writing down the transitive representation of K on k letters with respect to its subgroup of order k' and then making it simply isomorphic to itself in d different sets of letters and in such a way that the subgroup of order d permutes these d transitive constituents cyclically and is commutative with each substitution of K. The subgroup J_1' is of order k'.

6. Let F be of degree $6p + 11$. Since F includes H_3, the possible partitions of the degree of F are $5p + 10$, $p + 1$; $4p + 8$, $p + 2$, $p + 1$; $3p + 6$, $p + 2$, $p + 2$, $p + 1$; $2p + 4$, $2p + 4$, $p + 2$, $p + 1$; $4p + 8$, $p + 2$, $p + 1$. But all these partitions may be rejected at once if we apply to them the test of Theorem XVI.

The next step in order will be that of showing that H_{r+1} is not a primitive group of degree $6p + 8$. Obviously it is not of degree $6p + 7$. Now when H_{r+1} is of degree $6p + 8$ the possible partitions of the degree of F are $5p + 6$, $p + 1$; $5p + 5$, $p + 2$; $4p + 4$, $p + 2$, $p + 1$; $4p + 3$, $2p + 4$; $4p + 3$, $p + 2$, $p + 2$; $3p + 6$, $3p + 1$; $3p + 6$, $2p + 1$, p; $3p + 6$, $2p$, $p + 1$; $3p + 6$, $p + 1$, p, p; $3p + 3$, $2p + 4$, p; $3p + 3$, $2p + 2$, $p + 2$; $3p + 3$, $p + 2$, $p + 2$, p; $3p + 3$, $p + 2$, $p + 1$, $p + 1$; $3p + 2$, $2p + 4$, $p + 1$; $3p + 2$, $p + 2$, $p + 2$, $p + 1$; $3p + 1$, $2p + 4$, $p + 2$; $3p + 1$, $p + 2$, $p + 2$, $p + 2$; $2p + 4$, $2p + 2$, $2p + 1$; $2p + 4$, $2p + 2$, $p + 1$, p; $2p + 4$, $2p + 1$, $p + 2$, p; $2p + 4$, $2p + 1$, $p + 1$, $p + 1$; $2p + 4$, $2p$, $p + 2$, $p + 1$. The partitions $5p + 6$, $p + 1$; $4p + 4$, $p + 2$, $p + 1$; $3p + 6$, $p + 1$, p, p; $3p + 2$, $p + 2$, $p + 2$, $p + 1$; $3p + 2$, $2p + 4$, $p + 1$; are not permitted by Theorem XVI. All the remaining partitions require that H_{r+1} be simply transitive. Then J_1 is an imprimitive group of degree 8. The next partition, $5p + 5$, $p + 2$, is impossible. The partitions $4p + 3$, $2p + 4$; $4p + 3$, $p + 2$, $p + 2$; $3p + 3$, $2p + 4$, p; $3p + 3$, $2p + 2$, $p + 2$; $3p + 3$, $p + 2$, $p + 2$, p; $3p + 3$, $p + 2$, $p + 1$, $p + 1$; $3p + 6$, $3p + 1$; $3p + 6$, $2p + 1$, p; $3p + 6$, $2p$, $p + 1$; require that J_1 contain a circular substitution of order 3 (see § 3). When $dk = 8$, $d = 1$ or 2, and d is not 2 when there is this substitution of order 3 in J_1'. If $d = 1$, J_1 is imprimitive of order 288, 576, or 1152. All groups of degree 8 and of these orders occur for the first time on 8 letters. Let us now prepare a list of suitable groups J_1 from the known groups of degree less than 7. Let $d = 2$,

$k = 4$. The group K may be octic. J_1 is of class 4. Since the order of J_1' is even, K is not tetraedral, but the group of the cube may be used, $dkk' = 48$. In K' there are two substitutions of order 3 and of degree 6 and three substitutions of order 2 and of degree 4. If $d = 1$, there is only one group of degree less than 7 that may be written as a non-regular transitive group of degree 8, and in which the subgroup that leaves one letter fixed is of even order, the group $\{1234, 56\}$ which however gives us the group first mentioned over again. In fact we need never consider a second time the representation of a direct product, one factor of which is cyclic. Without more ado we reject the partitions that contain $2p + 4$. This leaves the partition $3p + 1, p + 2, p + 2, p + 2$. In this case it is not possible that all the substitutions of order 2 in J_1' should be of degree 4. *Hence H_{r+1} is not of degree $6p + 7$ or $6p + 8$ when p is greater than 7.*

Now when H_{r+1} is of degree $6p + 9$, the partitions of the degree of F are apparently $4p + 8, 2p$; $4p + 8, p, p$; $4p + 4, 2p + 4$; $4p + 4, p + 2, p + 2$; $3p + 6, 3p + 2$; $3p + 6, 2p, p + 2$; $3p + 6, p + 2, p, p$; $3p + 2, 2p + 4, p + 2$; $3p + 2, p + 2, p + 2, p + 2$; $2p + 4, 2p + 4, 2p$; $2p + 4, 2p + 4, p, p$; $2p + 4, 2p + 2, 2p + 2$; $2p + 4, 2p + 2, p + 1, p + 1$; $2p + 4, 2p, p + 2, p + 2$; $2p + 2, 2p + 2, p + 2, p + 2$. Eight others, $5p + 6, p + 2$; $\cdots$ are thrown out by Theorem XVI.

If $d = 3$, $k = 3$, there is a group J_1 of degree 9 and of order 18 in which there are substitutions of order 2 and of degree 6 which fit in with none of the above partitions. Then d equals 1 only. When $\{abc, ab\cdot de, def\}$ is put on nine letters its nine conjugate substitutions of order 2 are of degree 8. The next group to go on nine letters is $\{123, 12, 456, 45\}$, with respect to $\{12\cdot 45\}$. Its subgroup of degree 8 is then $1, 47\cdot 58\cdot 69, 23\cdot 56\cdot 89, 23\cdot 47\cdot 59\cdot 68$, with three transitive constituents, 23, 47, and 5689. Then there is the cyclic subgroup $\{aebd\cdot cf\}$ in $\{abc, def, ab\cdot de, aebd\cdot cf\}$ by means of which we get the primitive G_{36}^{9}. The group $\{ace, bdf, ac, bd, ab\cdot cd\cdot ef\}$ of order 72 has a set of nine conjugate octic subgroups, one of which, when the group is put on nine letters is $1, 2437\cdot 5698, 2734\cdot 5896, 23\cdot 47\cdot 59\cdot 68, 47\cdot 58\cdot 69, 27\cdot 34\cdot 59, 24\cdot 37\cdot 68, 23\cdot 56\cdot 89$. This is the only J_1 of degree 9 and of order 72, and there are no higher orders. Then we are concerned only with the partitions $4p + 4, 2p + 4$; $3p + 2, p + 2, p + 2, p + 2$; $2p + 4, 2p + 4, 2p$; $2p + 4, 2p + 4, p, p$; $2p + 2, 2p + 2, p + 2, p + 2$. Now we recall that in the transitive constituent of degree $2p + 4$ the group J is octic and in the group I the invariant substitution of order 2 of the octic J-group fixes all the $2p$ letters of the substitution A_1. Hence when the partition is $2p + 4, 2p + 4, p, p$, F contains a substitution of degree 8. If the partition is $2p + 4, 2p + 4, 2p$, there is either a substitution of degree 8 or a substitution of degree $8 + 2p$ of order 2 in F. But in this case we have re-

course to the group H_2 whose degree is broken according to the partitions $2p+2, 2p+2, p, p$; $2p+2, 2p, p+1, p+1$; $2p+2, p+1, p+1, p$; or $2p, p+1, p+1, p+1, p+1$. But in J_1' of order 8 all the substitutions of order 2 are of degree 6 or 8. If the partition is $3p+2$, $p+2$, $p+2$, $p+2$, the constituent of degree $3p+2$ is not imprimitive, nor by Theorem XVI is it multiply transitive. The maximal subgroup of a simply transitive primitive constituent of degree $3p+2$ has three possible partitions: $2p, p+2$; $2p+1, p+1$; $2p+2, p$; none of which agree with Theorem XVI. So we are up in the air with two partitions: $2p+4, 4p+4$; $2p+2$, $2p+2$, $p+2$, $p+2$. These are however impossible if $p+2$ is a prime number (e. g., $p=11$) for then the degree of G is not greater than $3p+9$ (I, Th. VII).

Let F be of degree $6p+9$. The partitions, exclusive of five which are not in agreement with Theorem XVI, are $4p+8$, $2p+1$; $3p+6$, $3p+3$; $3p+6$, $2p+1$, $p+2$; $3p+6$, $p+1$, $p+1$, $p+1$; $3p+3$, $2p+4$, $p+2$; $3p+3$, $p+2$, $p+2$, $p+2$; $2p+4$, $2p+4$, $2p+1$; $2p+4$, $2p+1, p+2, p+2$.

The groups J_1 of degree 10 for which $d=2$, $k=5$, are an icosaedral K and the symmetric-5 K. Then the groups in which $d=1$ are the symmetric-5 represented with respect to the alternating-4 group, an imprimitive representation in which the subgroup leaving one letter fixed has its substitutions of order 3 of degree 6 and its substitutions of order 2 of degree 8, and the transitive representation of the same group with respect to $\{abc, ab, de\}$. The latter is a primitive representation in which the given maximal subgroup has substitutions of order 6 and degree 9, a substitution of order 2 and degree 6, and substitutions of order 3 and degree 6. The group $\{abc, def, ab\cdot de, aebd\cdot cf\}$ of order 36 is a subgroup of the alternating-6 group, and with respect to it the latter is a (doubly transitive) modular group. With respect to $\{abc, def, ab, de, ad\cdot be\cdot cf\}$ of order 72 the symmetric-6 is a doubly transitive group of class 6.

The partitions show that H_{r+1} is not doubly transitive and that therefore the last two groups above are not here applicable. We may also scratch the first two after glancing over the partitions. In fact the only partitions which allow J_1' to have two transitive constituents of degree 4 each are the last two, and they require in case J_1 is the third group above that an octic group be invariant in the group of the cube. So we reject the third and fourth groups above as well as the second. There is then but one group J_1, the primitive group of order 120, the fifth. A constituent of degree $3p+6$ asks for a constituent in J_1' of order 18 or more. Thus we have only to consider the two partitions: $3p+3$, $p+2$, $p+2$, $p+2$; and $3p+3$, $2p+4$, $p+2$. But both of them assert the presence in J_1' of a circular substitution of order 3.

Hence H_{r+1} is not of degree $6p+10$, but when H_{r+1} of degree $6p+9$ exists, H_{r+2} of degree $6p+10$ is doubly transitive and J_2 is doubly transitive, one of the two doubly transitive groups above. But J_2 is not the modular group for that group is simple, and in consequence every substitution of I_2 is commutative with A_1, while in the group I_1 of H_{r+1} there are substitutions that transform A_1 into A_1^{-1}. For the same reason when I_2 is of order $720p$, it is constructed by multiplying a substitution of order 2, that transforms every cycle of A_1 into its inverse, into all the operators of the tail of the group of order $720p$ and of degree $6p$ in which every operator is commutative with A_1. We note that if a group G of degree $6p+9$ or $6p+10$ exists, it contains a substitution of order 3 and degree $3p+9$. *No G of degree greater than $6p+6$ exists if $p+2$ is a prime number.*

7. Before examining this reasoning with special reference to the prime number 7, we have to show that if a primitive group contains a substitution s_1 of order 3 and of degree 18, it contains a transitive subgroup of degree not greater than 48 generated by substitutions similar to s_1. Let $s_1 = a_1\, a_2\, a_3 \cdot b_1\, b_2\, b_3 \cdot c_1\, c_2\, c_3 \cdot d_1\, d_2\, d_3 \cdot e_1\, e_2\, e_3 \cdot f_1 f_2 f_3$. We assume first that every substitution of order 3 and degree 18 in G that unites two or more cycles of s_1 (or of any substitution of order 3 and degree 18) has at least one cycle in which all the letters are new to s_1. Let s_2 be such a substitution of order 3. The transform $s_1^2\, s_2\, s_1$ has not two cycles new to s_2. For if $s_2 = a_1\, b_1\, c_1 \cdot d_1\, e_1 f_1 \cdots (a_2) \cdots$, $s_2^2\, s_1\, s_2$ unites cycles of s_1, has no cycle new to s_1, and has at most four letters new to s_1. From two such substitutions s_1, s_2, we can build up a transitive subgroup of G of degree not greater than 48. If $s_1^2\, s_2\, s_1$ connects two cycles of s_2,

$$s_2 = (a_1\, b_1\, c_1)\,(d_1\, x_1\, -)\,(d_2\, x_2\, -)\,(d_3\, x_3\, -)\,(y_1\, y_2\, y_3)\,(---)\,(a_2)\,(b_2)\,(c_2),$$

and $\{s_2, s_1^2\, s_2\, s_1\}$ is of degree at most 24 and has at most five transitive constituents. Then there is a transitive subgroup of degree not greater than 48. Our assumption now is that the structure of s_2 is such that $s_1^2\, s_2\, s_1$ does not unite two cycles of s_2. If s_2 has a new letter in a cycle with a letter of s_1, s_2 fixes the other two letters of that cycle of s_1. If $s_2 = (a_1\, b_1\, -) \cdots$, it does not replace an a by an a nor a b by a b. The substitution $s_2^2\, s_1\, s_2$ has no cycle new to s_1 and therefore does not unite cycles of s_1. Hence $s_2 = (a_1\, b_1\, c_1)\,(a_2\, bc)\,(a_3\, bc) \cdots$. There can be no alternating constituent of degree 5 in $\{s_1, s_2\}$ on account of the simplicity of the alternating-5 group. If there is an alternating constituent of degree 4, then in $\{s_2, s_1^2\, s_2 s_1\}$ the head has substitutions of order 3 and degree 9 or contains substitutions of degree 4 or 8 and of order 2. Then every substitution that is similar to s_1 and unites two cycles of s_1 is commutative with s_1 and has one, two, or three cycles new to s_1:

$$s_2 = a_1\, b_1\, c_1 \cdot a_2\, b_2\, c_2 \cdot a_3\, b_3\, c_3 \cdot d_1\, d_2\, d_3 \cdot e_1\, e_2\, e_3 \cdot x_1\, x_2\, x_3\,,$$
$$= a_1\, b_1\, c_1 \cdot a_2\, b_2\, c_2 \cdot a_3\, b_3\, c_3 \cdot d_1\, d_2\, d_3 \cdot x_1\, x_2\, x_3 \cdot y_1\, y_2\, y_3\,,$$

or

$$= a_1\, b_1\, c_1 \cdot a_2\, b_2\, c_2 \cdot a_3\, b_3\, c_3 \cdot x_1\, x_2\, x_3 \cdot y_1\, y_2\, y_3 \cdot z_1\, z_2\, z_3\,.$$

Now assume that every substitution similar to s_1 that joins cycles of s_1 has just three cycles new to s_1. Since $H_2 = \{s_1, s_2\}$ is invariant under transformation by $a_2\, b_1 \cdot a_3\, c_1 \cdot b_3\, c_2 \cdot d_1\, x_1 \cdot d_2\, x_2 \cdot d_3\, x_3 \cdot e_1\, y_1 \cdot \cdots \cdot f_3\, z_3$, we have only to consider for the next step in the formation of a transitive subgroup of G the substitution $(a_1\, d_1\, -) \cdots$. If $s_3 = (a_1\, d_1\, e_1) \cdots$, $s_3^2\, s_2\, s_3 = (d_1\, b_1\, c_1) \cdots$, and $s_2^2\, s_3^2\, s_2\, s_3\, s_2 = (a_1\, d_1\, c_1) \cdots$: Now H_2 is invariant under

$$\{b_1\, c_1 \cdot b_2\, c_2 \cdot b_3\, c_3 \cdot x_2\, x_3 \cdot y_2\, y_3 \cdot z_2\, z_3\,, \quad x_1\, x_2\, x_3\,, \quad y_1\, y_2\, y_3\,, \quad z_1\, z_2\, z_3\}$$

so that finally we may put

$$s_3 = (a_1\, d_1\, b_1)\,(a_2\, d_2\, b_2)\,(a_3\, d_3\, b_3)\,(x_1\, - -)\,(y_1\, - -)\,(z_1\, - -)\,.$$

This substitution has no cycle with two letters new to s_2. Note that $H_3 \equiv \{H_2, s_3\}$ contains the substitution

$$s_2^2\, s_3\, s_2 = (b_1\, d_1\, c_1)\,(b_2\, d_2\, c_2)\,(b_3\, d_3\, c_3) \cdots,$$

and that H_3 is invariant under $\{e_1\, e_2\, e_3, f_1 f_2 f_3\}$. As for s_4 there are but three distinct replacements of a_1 that need be considered with a given s_3: $(a_1\, e_1\, -) \cdots$, $(a_1\, x_2\, -) \cdots$, and either $(a_1\, x_1\, -) \cdots$ or $(a_1\, x_3\, -) \cdots$, not both with a given s_3; that is, after the complete determination of the fourth cycle of s_3, since one of these two substitutions is conjugate to $(a_1\, x_2\, -) \cdots$ under $s_2^2\, s_3\, s_2$. The second, $(a_1\, x_2\, -) \cdots$, is to be rejected, for from s_2, s_4 is $(a_1\, x_2\, -)\,(b_1\, x_3\, -)\,(c_1\, x_1\, -) \cdots$, and since s_3 displaces x_1 and either x_2 or x_3, and fixes c_1, this substitution can not exist alongside s_3. A consequence of this fact is that G is not doubly transitive. Another consequence is that s_3 certainly displaces a letter x_4 in the cycle $(x_1\, - -)$. Also any substitution $(a_1\, x_4\, -) \cdots$ of order 3 and degree 18 is impossible. Then s_4, s_5, s_6, $\cdots$ replace a_1 by letters of H_2. In fact we can set up uniquely the generators

$$s_1\,, s_2\,,$$

$$s_3 = a_1\, d_1\, b_1 \cdot a_2\, d_2\, b_2 \cdot a_3\, d_3\, b_3 \cdot x_1\, x_4\, x_2 \cdot y_1\, y_4\, y_2 \cdot z_1\, z_4\, z_2\,,$$

$$s_4 = a_1\, e_1\, b_1 \cdot a_2\, e_2\, b_2 \cdot a_3\, e_3\, b_3 \cdot x_1\, x_5\, x_2 \cdot y_1\, y_5\, y_2 \cdot z_1\, z_5\, z_2\,,$$

$$s_5 = a_1\, f_1\, b_1 \cdot a_2\, f_2\, b_2 \cdot a_3\, f_3\, b_3 \cdot x_1\, x_6\, x_2 \cdot y_1\, y_6\, y_2 \cdot z_1\, z_6\, z_2\,,$$

$$s_6 = a_1\, x_1\, a_2 \cdot b_1\, x_2\, b_2 \cdot c_1\, x_3\, c_2 \cdot d_1\, x_4\, d_2 \cdot e_1\, x_5\, e_2 \cdot f_1\, x_6 f_2\,,$$

$$s_7 = a_1\, y_1\, a_2 \cdot b_1\, y_2\, b_2 \cdot c_1\, y_3\, c_2 \cdot d_1\, y_4\, d_2 \cdot e_1\, y_5\, e_2 \cdot f_1\, y_6 f_2\,,$$

$$s_8 = a_1\, z_1\, a_2 \cdot b_1\, z_2\, b_2 \cdot c_1\, z_3\, c_2 \cdot d_1\, z_4\, d_2 \cdot e_1\, z_5\, e_2 \cdot f_1\, z_6 f_2\,,$$

of H_8. The primitive group G contains no other substitutions of order 3 and degree 18 than those of H_8. Hence the degree of G is not greater than 36 in this case. We must now assume that every substitution s_2 that connects two or more cycles of another substitution has at least two cycles entirely new to s_1. At once we notice that there is no substitution $(a_1 d_1 -) \cdots$ in the series $s_1, s_2, \cdots$. Then we have uniquely

$$s_3 = (a_1 e_1 b_1)(a_2 e_2 b_2)(a_3 e_3 b_3)(x_1 - - -) \cdots .$$

Note that s_3 displaces x_2 also. Since $s_2^2 s_3 s_2 = (a_1)(b_1 e_1 c_1) \cdots$, s_4 need not replace a_1 by a letter new to H_3. A substitution $(a_1 x_2 -) \cdots$ or $(a_1 x_3) \cdots$ is impossible. Then the substitutions $s_4, s_5, \cdots$ have the property that each of them replaces a_1 by a letter of subscript unity from s_1 or s_2. But since $(a_1 d_1 -) \cdots$ is impossible, this case leads to no transitive subgroup of G. We reach the same conclusion if we remove the condition that every substitution s_2 has more than one cycle new to s_1.

There is then in G at least one substitution $s_2 = (a_1 b_1 -) \cdots$ which connects two cycles of s_1 and which has no cycle new to s_1. Now $\{s_1, s_2, \cdots\}$ is a transitive group of degree not greater than 48 unless s_2 unites only two cycles of s_1 and has more than six new letters. But in this event $s_1^2 s_2 s_1$ (and $s_1 s_2 s_1^2$ as well) has no cycle new to s_2 and does not displace more than six letters new to s_2. If in addition $s_1^2 s_2 s_1$ connects cycles of s_2, $\{s_2, s_1^2 s_2 s_1\}$ may be used instead of $\{s_1, s_2\}$ to begin a series that will generate a transitive group of degree not greater than 48. If $s_1^2 s_2 s_1$ does not connect cycles of s_2, s_2 does not replace the three letters of a cycle of s_1 by letters new to s_1, and therefore $s_2^2 s_1 s_2$ has no cycle new to s_1, s_2 replaces no a by an a and no b by a b, and no a or b is in a cycle of s_2 with a new letter. Then s_2 must unite more than three cycles of s_1.

It is proved then that *a primitive group G that contains a substitution of order* 3 *and of degree* 18 *includes a transitive subgroup of degree not greater than* 48.

8. Let us once more take up the proof of Theorem XVII for the special prime number 7.

If H_{r+1} is imprimitive, the degree of H_{r+s} is at most $6p + 6$ as before, and in H_{r+s} the subgroups of order 7 are Sylow subgroups. In the doubly transitive group H_{r+s+1} of degree $6p + 7$, the group J_{s+1} is doubly transitive of degree 7 and contains an invariant subgroup of order 7 (III, § 26), that is, it is the metacyclic group. If H_{r+s+2} exists, J_{s+2} must contain substitutions of degree 8 or less. Then if the degree of G exceeds $6p + 7$ ($p = 7$ of course), H_{r+1} is primitive.

Now let it be assumed that F has an alternating constituent. If the subgroup E_1 (III, § 30) is a simple isomorphism between six alternating groups, it contains a substitution of order 3 and of degree 18, so that H_{r+1} contains a

transitive subgroup of degree not greater than 48 (§ 6 and III, § 32, second paragraph). Then E_1 has at most five transitive constituents. An alternating constituent of H_r is on at most ten letters. If the degree of H_r does not exceed $6p + 1$, the degree of H_{r+1} is at most $6p + 7$. The transitive representations of the alternating-7, -8, -9, and -10 groups on not more than 40 letters are: for the alternating-7, of the degrees 15, 21, 35; for the alternating-8, 15, 28, 35; for the alternating-9, 36; for the alternating-10, none. Among the primitive groups of degree 14, 15, and 16 there are two which have alternating-7 and alternating-8 quotient groups with respect to an invariant subgroup of order 16. Then an imprimitive constituent of H_r has its systems of imprimitivity permuted according to an alternating group, or according to a primitive group of degree 15 or 16.

A simply transitive primitive group of degree 24 generated by substitutions of order 7 and degree 21, which has an alternating-7, -8, $\cdots$ quotient group can be shown not to exist. Let G_1 be the maximal subgroup of degree 23. If G_1 has three transitive constituents, they are all alternating and not all of the same degree, an absurdity. If G_1 has just two transitive constituents, their degrees run 7, 16; 8, 15; 9, 14. The constituent of degree 16 or 15 is doubly transitive, and no transitive group of degree 14 has an alternating quotient group.

Nor does there exist a simply transitive primitive group of degree 30 or 32 which has an alternating-7, -8, $\cdots$ quotient group. G_1 has not four transitive constituents. With three transitive constituents in G_1, there are the partitions 7, 7, 15; 7, 7, 17; 8, 8, 15; in all three of which the transitive constituent of highest degree is doubly transitive. If there are just two transitive constituents, the partitions are 7, 22; 8, 21; 14, 15; 14, 17; 15, 16; 7, 24; 8, 23; 9, 22; 10, 21. Here 7, 22; 14, 17; 8, 23; and 9, 22 go out by Jordan's theorem on simply transitive primitive groups.* In 8, 21 the second constituent is not imprimitive and G_1 is not a simple isomorphism. In 14, 15 the constituent of degree 14 is imprimitive of order greater than $7!/2$, is a positive group, and contains a substitution of order 2 of degree less than 14, that is, G_1 is of class 4 or 8 because the constituent of degree 15 is of order $7!/2$. G_1 contains a transitive subgroup of degree 16 if the partition is 15, 16. A transitive constituent of degree 21 or 24 is imprimitive.

If the transitive constituents of H_r which are not alternating are all imprimitive the partitions of the degree of H_r are $p + k$, $5p + 5k$ $(k = 1, 2, 3)$; $p + k$, $p + k$, $4p + 4k$ $(k = 1, 2)$; $p + k$, $2p + 2k$, $3p + 3k$ $(k = 1, 2)$; $p + 1$, $p + 1$, $2p + 2$, $2p + 2$; $p + 1$, $p + 1$, $p + 1$, $3p + 3$; $p + 1$, $p + 1$, $p + 1$, $p + 1$, $2p + 2$; $p + k$, $p + k$, $4p + 2$ $(k = 0, 1)$. There is also $p + k$, $p + k$, $4p + 4$, $k = 0, 1$, but then H_r contains a transitive

* Jordan, *Traite des substitutions* (1870), p. 284.

subgroup of degree 16. The subgroup F of H_{r+1} has the same number of transitive constituents as H_r, and since the degree of F is greater than the degree of H_r by at most five units, the degree of H_{r+1} is $6p + 6k + 1$, $(k = 1, 2, 3)$ or less. Bear in mind that F can have no doubly transitive constituent of degree $5p + 6$ and that a primitive constituent of that degree is doubly transitive.* The order of F is not divisible by p^2, and a transitive J_1 in H_{r+1} of degree 13 or 19 is impossible.

If all the non-alternating constituents of H_r are primitive, their degrees range from 15 to 40, inclusive. A single non-alternating primitive constituent is not of higher order than the alternating group beside it. The degree of a primitive constituent is not a multiple of 7 unless it is simple. Then the groups H_r of degree greater than $6p + 1$ that are simple isomorphisms between primitive groups are indicated by the partitions 9, 36; 8, 8, 28; 7, 7, 15, 15; 8, 8, 15, 15; 8, 8, 8, 8, 15; and if H_r is not a simple isomorphism, by 7, 7, 16, 16; 8, 8, 16, 16. Certainly in the five partitions in which the alternating constituent is of degree 8 or 9, the degree of F is the same as that of H_r, and therefore in all seven cases the degree of H_{r+1} is not greater than $6p + 7$.

Let H_r have an imprimitive constituent along with a non-alternating primitive constituent. The partitions of the degree $(> 6p + 1)$ of H_r are (the degree of the imprimitive constituent being written last): 8, 15, 24; 8, 16, 24; 8, 8, 15, 16; 8, 8, 16, 16; 7, 7, 16, 14. As before, the degree of H_{r+1} is at most $6p + 7$.

If the degree of G exceeds $6p + 7$ there is no alternating constituent in F, but perhaps there is an imprimitive constituent in which the systems are permuted according to an alternating-7, -8, $\cdots$, group. The imprimitive constituent that occurs in F is of the degree $mp + mk$, $(m = 2, 3, 4)$. E_1 has a constituent (most likely intransitive) in mp of these same letters which permutes p systems of m letters according to the alternating-p group. H_r permutes some or all of the $p + k$ systems according to an alternating group. E_1 has not six transitive constituents. Then an alternating constituent of H_r is of degree not greater than $p + 3 = 10$. We therefore use the preceding partitions of the degree of H_r and add to them the partitions that obtain when H_r has no alternating constituent but has an imprimitive constituent of degree $mp + mk$ $(m = 2, 3, 4, k = 0, 1, 2, 3)$. If H_r has no primitive constituent the partitions are $4p + 4k$, $2p + 2k$ $(k = 1, 2, 3)$; $3p + 3k$, $3p + 3k$ $(k = 1, 2, 3)$; $2p + 2k$, $2p + 2k$, $2p + 2k$ $(k = 1, 2)$; $2p + 2k$, $4p + 2$, $(k = 0, 1)$; $2p + 2k$, $4p + 4$ $(k = 0, 1)$. Here H_{r+1} is of degree $6p + 13$, $6p + 19$, or of degree less than $6p + 8$. If H_r has just one primitive constituent, the partitions are 28, 16; 32, 15; 32, 16; 14, 14, 16; 16, 16, 15;

* These Transactions, vol. 16 (1915), p. 147, last paragraph.

16, 16, 16; and if there are two or more primitive constituents, 14, 15, 15; 14, 15, 16; 14, 16, 16; 16, 15, 15; 16, 15, 16; 16, 16, 16. The degree of F is then not greater than $6p + 6$ and the degree of H_{r+1} is not greater than $6p + 7$.

Now F has no alternating constituent and no transitive constituent which permutes systems of imprimitivity according to an alternating group. The partitions of the degree of F are those given when p was assumed to be greater than 7. The order of F is not divisible by 49. Then we can show that the degree of G is not greater than $6p + 7$ $(p = 7)$ if we can dispose of F when its transitive constituents are of the degrees $2p + 4, 4p + 4$; $2p + 2, 2p + 2$, $p + 2$, $p + 2$. The transitive group of degree $2p + 4$ has nine systems of imprimitivity permuted according to a transitive group of degree 9 generated by substitutions of order 7, that is, according to the G_{504} or the alternating-9, both of which are simple. An imprimitive group of degree $4p + 4$ whose systems are permuted according to a primitive group of degree 8 or 16, generated by substitutions of order 7 and in isomorphism to the 504 group or alternating-9 group does not exist. If the constituent of degree $4p + 4$ is primitive, it is simply transitive. No transitive constituent of its maximal subgroup is of degree less than 9 and the partitions 9, 22; 14, 17; 15, 16 are impossible. The other partition of the degree of F is 16, 16, 9, 9. No transitive group of degree 16 has a simple group of degree 9 as a quotient group.

Of course the holomorph of the non-cyclic group of order p^2 (p an odd prime) is a doubly transitive group in which there are substitutions of order p and of degree $p^2 - p$, so that $6p + 7 = 49$ *is the true upper limit of the degree of a primitive group that contains a substitution of order* 7 *and of degree* 42.

9. By means of Theorem XI it is easy to give an interpretation of Theorems XIII and XVII in terms of the order of primitive groups.

THEOREM XVIII. *The order of a primitive group, not symmetric or alternating, divides*

$$n\,!\Big/\prod_{k=1}^{k=q} P_q,$$

where P_1 *is the product of all primes* $< n - 2$, P_k *is the product of all primes* $< n/k - 1$ *and* $> k + 1$ $(k = 2, 3, 4)$, P_5 *is the product of all primes* $< (n - 6)/5$ *and* > 5, P_6 *is the product of all primes* $< (n - 10)/6$ *and* > 5, P_q *is the product of all primes* $< (n - 4q + 4)/q$ *and* $> 2q - 2$ $(q = 7, 8 \cdots)$.

STANFORD UNIVERSITY, CAL.,
October, 1917.