THE ORDER OF PRIMITIVE GROUPS* (III)

BY

W. A. MANNING

1. The theorem which I now propose to prove is

THEOREM XIII. *Let q be any positive integer greater than 5, and let p be any prime greater than $2q-2$; then the degree of any primitive group G that contains a substitution of order p and degree qp but none of order p and of degree less than qp does not exceed $qp+4q-4$; if G is not triply (doubly) transitive its degree does not exceed $qp+4q-6$ ($qp+4q-7$); the order of G is not divisible by p^2.*

2. In the two former papers in these Transactions† under this same title, and to which references are indicated by the Roman numerals I and II in parenthesis, a proof and a slight extension were given (for q greater than unity) of the theorem which Jordan stated in the *Memoir on Primitive Groups* in the first volume of the Bulletin of the Mathematical Society of France, page 175:

Let q be a positive integer less than 6; p any prime 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) can not exceed $qp+q+1$.

To this one may add that when p is greater than $q+1$, the order of G is not divisible by p^2.

3. The memoir at the end of which this theorem is given is devoted to the larger question of the corresponding limit for the degree of G when q is not confined to numbers less than 6. Jordan's general result may be stated thus:

Let q be any positive integer, p any prime greater than $2q\log_2 q+q+1$; the degree of a primitive group G that contains a substitution of order p on q cycles (without including the alternating group) can not exceed $qp+2q\log_2 2q$.

4. This is supplemented in certain directions by the theorem:‡

If a primitive group of class greater than 3 contains a substitution of prime order p and of degree qp (q less than $2p+3$), it includes a transitive subgroup of degree not greater than the larger of the two numbers $qp+q^2-q$, $2q^2-p^2$. In particular, if q is less than $p+2$, the degree of G, when it is simply transitive, is not greater than $qp+q^2-q$.

* Presented to the Society, April 7, 1917.

† These Transactions, vol. 10 (1909), pp. 247–258; vol. 16 (1915), pp. 139–147. Theorem X asserts that the upper limit of the degree is $qp+q$ when p is greater than $q+1$, and q is greater than 1 and less than 5.

‡ These Transactions, vol. 12 (1911), pp. 375–386.

5. Simply transitive primitive groups are known which contain a substitution of prime order p and of degree qp $(q < p)$ and whose degree is $qp + q(q-2)/8$. For example, if the alternating group of degree n is represented as a transitive group on the $n(n-1)/2$ binary products ab, ac, $\cdots$, the number of these products left fixed by a circular substitution of prime order p is exactly $(n-p)(n-p-1)/2$. Then the given substitution of order p in the new representation of the alternating group is of degree $[n-(p+1)/2]p$; the condition that the number of cycles in this substitution is less than p, $n-(p+1)/2 < p$, may be written $n < 3p/2$. The number of letters left fixed by the given substitution of order p has therefore its maximum value when $n = (3p-1)/2$, viz., $(p-1)(p-3)/8$, when $n-(p+1)/2 = p-1$. Now

$$n(n-1)/2 = (p-1)p + (p-1)(p-3)/8 = qp + q(q-2)/8.$$

If

$$n = 3p/2 - (2k-1)/2, \qquad n-(p+1)/2 = p-k,$$

$$(n-p)(n-p-1)/2 = (p-2k+1)(p-2k-1)/8,$$

and we have

$$n(n-1)/2 = (p-k)p + (p-2k+1)(p-2k-1)/8,$$

$k = 1, 2, \cdots, (p-3)/2$, as the degree of a simply transitive primitive group which contains a substitution of order p and degree qp, $q < p$.

It is not improbable that the true limit $(q < p)$ is $qp + q(q-2)/8$ instead of $qp + q^2 - q$ but we know so few primitive groups that an induction from those known has not much value. At any rate we need not expect to extend the formula $qp + q + 1$ to all primitive groups in which q is less than p.

6. Another related theorem is that of Bochert:*

The class (> 3) *of a substitution group of degree* n *exceeds* $n/3 - 2\sqrt{n}/3$ *if it is doubly,* $n/3 - 1$ *if triply,* $n/2 - 2$ *if quadruply, transitive.*

7. This theorem, with that of Sylow,† is indispensable in the proof of Theorem XIII. Another theorem which has been of constant use in the two preceding numbers, and without which the present development would be well-nigh, probably quite, impossible, is

THEOREM XIV. *The largest subgroup of a transitive group* G *of degree* n, *in which a subgroup* H *that leaves fixed* m $(0 < m < n)$ *letters is invariant, has as many transitive constituents in these* m *letters as there are different conjugate sets in* G_1 *(a subgroup of* G *that leaves one of the* m *letters fixed) which, under the substitutions of* G, *enter into the complete set of conjugates to which* H *belongs. Moreover, the degree of each of these constituents is proportional to the number of subgroups in the several conjugate sets of* G_1 *in question.*

* Bochert, Mathematische Annalen, vol. 40 (1892), pp. 176–193; vol. 49 (1897), pp. 133–144.

† Sylow, Mathematische Annalen, vol. 5 (1873), pp. 584–594.

A clear comprehension of this theorem is so necessary to the reader that I venture to insert here a proof of it, considerably fuller than the brief indication given in the Bulletin of the American Mathematical Society.*

8. Let g be the order of G, and let those conjugates of H, which are found in G_1, lie in k different sets, in so far as they are permuted by the substitutions of G_1 only, with r conjugates in the set that includes H, r_1 in a second set, and so on. In G_1, H is invariant in a subgroup of order g/nr, while H_1, a subgroup in the second set, is invariant in a group of order g/nr_1. The largest subgroup I of G in which H is invariant is of order gm/ns, $s = r + r_1 + \cdots + r_{k-1}$. Now I does not connect transitively the $n - m$ letters displaced by H and the m letters it leaves fixed. Since the largest subgroup of G_1 in which H is invariant is of order g/nr, I has one transitive constituent of degree $(gm/ns)/(g/nr) = mr/s$ in letters left fixed by H. Let $a_1, a_2, \cdots, b_1, b_2, \cdots$ be the letters of G left fixed by H. The letter fixed by G_1 is a_1. Consider a substitution $S = a_1 b_1 \cdots$ of G. Since there are substitutions of G which transform H_1 into H we may assume that S transforms H_1 into H. Then $SHS^{-1} = H_1$, $(G_1 S) H (G_1 S)^{-1} = G_1 H_1 G_1^{-1} = H_1'$, that is, every substitution $G_1 S = a_1 b_1 \cdots$ of G transforms some subgroup H_1' (conjugate to H_1 under substitutions of G_1) into H: $(G_1 S)^{-1} H_1' (G_1 S) = H$. Then no matter by which of the substitutions $a_1 b_1 \cdots$ of G we transform G_1 we get a group G_2 that fixes b_1 and in which H is a member of that set of r_1 conjugate subgroups by which every substitution $G_1 S = a_1 b_1 \cdots$ replaces the set $H_1, \cdots$ of G_1. Then b_1 is one of the letters of a transitive constituent of degree mr_1/s in I. Since no substitution $a_1 b_1 \cdots$ transforms H into itself, the letter a_1 is not an element of this transitive constituent in the mr_1/s letters $b_1, b_2, \cdots$. If mr_1/s is not unity, there is a substitution $T_2 = b_1 b_2 \cdots$ in I, and the product $ST_2 = a_1 b_2 \cdots$ transforms H_1 into H, as do also the products $ST_3 = a_1 b_3 \cdots, \cdots$, where $T_3 = b_1 b_3 \cdots, \cdots$. Every substitution $G_1 ST_i$, $i = 2, 3, \cdots$, transforms some subgroup H_1' (conjugate of H_1 in G_1) into H. Suppose that a substitution $S_1 = a_1 c_1 \cdots$ transforms H_1 into H. Then $S^{-1} = b_1 a_1 \cdots$ transforms H into H_1, so that $S^{-1} S_1 = b_1 c_1 \cdots$ transforms H into itself, thereby showing that c_1 is one of the letters $b_1, b_2, \cdots$. If S_1 had transformed H_1' (some other member of the set H_1 of G_1) into H, a properly chosen substitution $G_1 S_1 = a_1 c_1 \cdots$ would have transformed H_1 into H, and that substitution could have been called S_1. Then no substitution $a_1 c_1 \cdots$ (c_1 not one of the letters $b_1, \cdots$) can transform any member of the set H_1 into H. Next, there must be a substitution in G to transform H_2 into H: call it $U = a_1 c_1 \cdots$. We know that c_1 does not belong to the same transitive constituent in I as a_1 or b_1. Then just as before I has a transitive constituent in the mr_2/s letters $c_1, c_2, \cdots$ associated with the conjugate set $H_2, \cdots$ of G_1.

* Vol. 13 (1906), p. 20.

Thus we find $k-1$ transitive constituents in $r_1 m/s$ letters $b_1, b_2, \cdots$, in $r_2 m/s$ letters $c_1, c_2, \cdots$, in $r_3 m/s$ letters $d_1, d_2, \cdots$, and so on, associated with the $k-1$ conjugate sets $H_1, \cdots, H_2, \cdots, H_3, \cdots, \cdots$ of G_1 in addition to the constituent of degree rm/s in the letters $a_1, a_2, \cdots$. Every substitution $a_1 a_2 \cdots, a_1 a_3 \cdots, \cdots$ transforms some subgroup H' (of the set $H, \cdots$ of G_1) into H.

We now pass to the consideration of Theorem XIII, which will be proved after the necessary preparation by a complete induction. The reader would do well to have freshly in mind the arguments of the two preceding numbers of this series on *the Order of Primitive Groups* and is recommended also to fortify himself by a perusal of the first twenty or thirty pages of Jordan's great *Memoir on Primitive Groups*. It will be seen that in setting up the subgroups H_{ij} in § 10 I have effected a combination of Jordan's method with that of my two earlier papers.

The subgroups H_{ij}

9. The group G is by hypothesis a primitive group in which there is a substitution of order p and degree qp but no substitution of the same order and of lower degree. From the beginning we assume that q is less than p, and ultimately we shall introduce the condition that p is greater than $2q-3$, but not before it seems unavoidable.

10. Let H_i be a subgroup of G that is generated by the similar substitutions $A_1, A_2, \cdots, A_i, A_1', A_2', \cdots, A_i', A_1'', A_2'', \cdots, A_i'', \cdots$, of order p and degree qp. It is to be understood as a part of the definition of H_i that all the substitutions of G of order p and degree qp and which are not in H_i displace one or more letters new to H_i.

If H_i is intransitive there exists in G a substitution A_{i+1}, similar to A_1, that unites two or more of the transitive sets of H_i (I, Theorem I). It is legitimate to assume that no other substitution similar to A_1 that joins two of the transitive sets of H_i displaces fewer new letters than does A_{i+1}. This being granted, A_{i+1} has at most one new letter in any cycle (I, Theorem IV). To $\{H_i, A_{i+1}\}$ are now to be adjoined all the other substitutions of G on the same letters that are similar to A_1. Call the resulting group H_{i+1}. It may be that there are in H_{i+1} and not in H_i certain substitutions of order p and degree qp which displace fewer letters new to H_i than A_{i+1} does. If so, no one of them connects sets of H_i. Let then $H_{ij}, j = 1, 2, \cdots (H_{i0} = H_i)$, be a subgroup of H_{i+1} that includes $H_i, H_{i1}, H_{i2}, \cdots, H_{i,\, j-1}$, and which is generated by $H_{i,\, j-1}$, a substitution B_{ij}, similar to A_1, which displaces a minimum number of letters new to $H_{i,\, j-1}$, hence at most one to any cycle, and all other substitutions of G of order p and degree qp on letters of $\{H_{i,\, j-1}, B_{ij}\}$ only. Let H_{ik_i} be the last of these groups before H_{i+1}. Let $x_1, x_2, \cdots,$

x_m $(m > 0)$ be the letters of H_{i+1} that are not displaced by H_{ik_i}. Any substitution of H_{i+1} that replaces one of the m letters $x_1, x_2, \cdots, x_m$ by one of the same letters permutes these m letters only among themselves. This holds true of any two successive groups, as H_{ij} and $H_{i,\, j-1}$. Those of the letters $x_1, x_2, \cdots, x_m$ of H_{i+1} that belong to a transitive constituent of H_{i+1} form a system of imprimitivity of that constituent if their number exceeds unity. Since the number of letters in any system of imprimitivity of a group generated by substitutions of order p and degree less than p^2 is less than p, no letter x_1, say, can be associated in a system of imprimitivity with any letter of H_{ik_i}. It follows that a transitive constituent of H_{i+1} with just one new letter in it is primitive. This holds not only for H_{i+1} but for any group of the series, as H_{ij}.

11. For some value of i not greater than q, H_i is a transitive group. Let H_{r+1} be the first transitive group in the series. The group H_{r+2} is formed by the adjunction of a substitution A_{r+2} which displaces a minimum number of letters new to H_{r+1} and then all the substitutions of order p and degree qp in G on the letters of $\{H_{r+1}, A_{r+2}\}$. Of course A_{r+2} displaces at least one new letter if H_{r+1} is not the last group in the series $H_1, H_2, \cdots$. All the groups H_{r+1}, $H_{r+2}, \cdots$ are transitive. Finally a group H_{r+i} will be reached which is invariant in G.

12. When the degree of H_{r+1}, the first transitive group in the series, does not exceed $qp + q$, no great difficulty is involved in finding a limit for the degree of G within the limits of our theorem. For the present it is assumed that the degree of H_{r+1} exceeds $qp + q$. We shall return to this case later (§ 25).

13. Now H_{r+1} displaces m letters $x_1, x_2, \cdots, x_m$ which H_{rk_r} leaves fixed. These letters form one of several systems of imprimitivity of H_{r+1} which are permuted according to a primitive group. If $m = 1$, H_{r+1} is primitive. In like manner, if H_{r+i+1} displaces several letters new to H_{r+i} those letters form a system of imprimitivity, permuted with other systems according to a primitive group.

14. Let G be of the same degree, if possible, as H_{r+i}, $i = 1, 2, \cdots$. A subgroup G_1 of G displaces all but one of the letters of G and the invariant subgroup F of G_1, generated by all the substitutions of order p and degree qp in G_1, is of the same degree as G_1. Hence when H_{r+i} is contained in a primitive group of the same degree, H_{r+i} is itself primitive. F coincides with H_{r+i-1}, $i = 2, 3, \cdots$, and with H_{rk_r} when $i = 1$.

15. Consider the group in the systems of imprimitivity of m letters each $(m > 1)$ of H_{r+1}. It is a primitive group and it can be shown that *it is not triply transitive*. One system, which we call s, is composed of the letters x_1, $x_2, \cdots, x_m$ and these systems of m letters can be chosen in but one way.

Now H_{rk_r} (call it F) permutes all the other systems of m letters of H_{r+1}: $t, u, \cdots$. The letters which F displaces but H_{r,k_r-1} or $H_{r-1,k_{r-1}}$ (call this group F') leaves fixed form one or several of the systems $t, u, v, \cdots$. Suppose that the group in the systems $s, t, \cdots$ of H_{r+1} is triply transitive. Then the subgroup of H_{r+1} that leaves one letter fixed is doubly transitive in the remaining systems and has an invariant subgroup generated by all its substitutions of order p and degree qp which coincides with F. Since F is an invariant subgroup of a doubly transitive group (in the systems $t, u, \cdots$), it is primitive, or an imprimitive group in which every substitution displaces all or all but one of the systems $t, u, \cdots$.* The degree of F by hypothesis exceeds qp, so that it is not regular in the systems $t, u, \cdots$. Then the subgroup of F that leaves one system fixed displaces all the systems $u, v, \cdots$, that is, all the systems of H_{r+1} except s and t; and N, the subgroup of M generated by all its substitutions of order p and degree qp, also displaces the same systems $u, v, \cdots$ as M. This is true when F is primitive in the systems in question; and when F is imprimitive, every substitution of M displaces all the systems $u, v, \cdots$, and N does not reduce to the identity because the degree of F (in the systems $t, u, \cdots$) is then the power of some prime other than p. Now F' and N coincide. For any substitution of N fixes all the letters of F that are not in F', and no other letters of F are fixed by N. It now follows since F' displaces all the letters of F except those in the systems t, that there is only the one way of dividing the letters of F into systems of m letters each.

16. Consider now the group H_{r+2} that displaces just m' letters $y_1, y_2, \cdots, y_{m'}$ new to H_{r+1}. We have seen that m' divides m and we know from the theory of primitive groups with transitive subgroups of lower degree† that m/m' is greater than 1. Call this new system of m' letters y and call the m/m' systems of H_{r+2} in the letters $x_1, x_2, \cdots, x_m$: $x', x'', \cdots$. H_{r+2} is at least doubly transitive in its systems of m' letters and contains a substitution $S = (yx')\cdots$, which certainly transforms F into itself, because $S^{-1}FS$ fixes y and x', and therefore also $x'', \cdots, x^{m/m'}$. It follows too that S permutes the systems $t, u, \cdots$ of F as units. Now consider $S^{-1}H_{r+1}S$. Its systems are $t, u, v, \cdots$, and a system s' composed of $y, x'', x''', \cdots, x^{m/m'}$. If we admit that H_{r+1} is doubly transitive in the systems, $S^{-1}H_{r+1}S$ contains a substitution $U = (s't)\cdots$. The group $H' = U^{-1}FU$ fixes all the m letters of t and the letters of x' but displaces the letters of y. Also H_{r+1} contains a substitution $V = (st)\cdots$. The group $H'' = V^{-1}H'V$ fixes all the letters of s, but displaces y. From H'' we take a substitution C of order p and degree qp that displaces y. The transitive group $S^{-1}H_{r+1}S$ contains a

*Bulletin of the American Mathematical Society, vol. 13 (1906), pp. 20–23, Theorem IV.

† These Transactions, vol. 7 (1906), pp. 499–508.

substitution W that replaces y by x'', fixes all the letters of x', and which therefore permutes the m/m' systems $y, x'', x''', \cdots, x^{m/m'}$ only among themselves. Hence $W^{-1}CW$ is a substitution similar to A_1 that fixes the letters of $y, x', x''', \cdots, x^{m/m'}$ and displaces the letters of x''. This is contrary to the hypothesis that F is the last group of the series before H_{r+1}.

17. Thus it is proved that H_{r+1} $(r > 1, m > 1)$ is not so much as triply transitive in its systems of imprimitivity of m letters each. The primitive group in the systems is simply or doubly transitive.* As we run back through the groups $F, F', \cdots$ we see that the number of new letters introduced at any step is divisible by m, and that q therefore is divisible by m; and since H_{r+1} $(r > 1)$ is not triply transitive in the systems, m is less than q.

18. Now H_{r+s} is the last imprimitive group in the series before the doubly transitive group H_{r+s+1}. Its degree is $qp + k + m + m' + \cdots + n$, where $n = m^{s-1}$, and where $qp + k$ is the degree of $F = H_{rk_r}$. We are now in position to state that *the primitive group in the systems of n letters each of H_{r+s} $(r > 1)$ is never more than doubly transitive.* It has just been proved when $m' = 1$. If m' is greater than 1, and $m'' = 1$, it is doubly and not triply transitive, because H_{r+1} is neither regular nor of class $qp + k + m - 1$.† If m'' is greater than 1, it is doubly but not triply transitive by the general theory of primitive groups with transitive subgroups of lower degree.

The J-group

19. If all the subgroups of order p and degree qp in $F = H_{rk_r}$ form a complete set of conjugates under the substitutions of F, then the largest subgroup (I_1) of H_{r+1} in which $\{A_1\}$ is invariant has a transitive constituent in the $k + m$ letters of H_{r+1} that are left fixed by A_1 (Theorem XIV). A further consequence is that all the subgroups of order p and degree qp in H_{r+1} are conjugate under the substitutions of H_{r+1}, so that in H_{r+2} the largest subgroup I_2 of H_{r+2} in which $\{A_1\}$ is invariant has a transitive constituent on the $k + m + m'$ letters of H_{r+2} that A_1 leaves fixed, and so on. Finally in H_{r+s+1}, I_{s+1} has a doubly transitive constituent of degree $k + m + m' + \cdots + n + 1$. For a transitive group is doubly transitive if it has a subgroup transitive in all but one of its letters. Let us call these transitive constituents of $I_1, I_2, \cdots, J_1, J_2, \cdots$, respectively. Then J_{s+2} is triply transitive, J_{s+3} is quadruply

* Cf. Jordan, Bulletin de la Société mathématique de France, vol. 1 (1873), pp. 185–188, where under similar conditions it is proved that the group in the systems is not quadruply transitive. It there appears to have been tacitly assumed that the group in the systems is not a simply transitive group. This is indeed the case in a corresponding passage of the discussion of primitive groups with transitive subgroups of lower degree, but in this more general problem I fail to see any valid arguments for the exclusion of those imprimitive groups whose systems of imprimitivity are permuted according to a simply transitive primitive group.

† These Transactions, loc. cit.

transitive, and so on. Similarly when $m = 1$, and H_{r+1} is a simply transitive primitive group, if all the subgroups of order p and degree qp in F are conjugate under the substitutions of F, J_1 is transitive, J_2 is at least doubly transitive, J_3 is at least triply transitive, and so on. Then if F has the required property, we can be sure that G has the same property, and that the constituent J of I, the largest subgroup of G in which $\{A_1\}$ is invariant, is transitive on all the letters of G that are left fixed by A_1.

20. If the transitive group J is of degree greater than q as at present and is alternating or symmetric, the class of G is not greater than 3, contrary to hypothesis. For if I has a substitution which displaces only letters of J, the totality of all such substitutions of I form an invariant subgroup of I, and if J is alternating or symmetric, this subgroup (assumed not to be the identity) is the alternating group. And since the largest group on the same letters in which A_1 is invariant is of order $p^q(p-1)(q!)$ (I, page 251) $\{A_1\}$ is certainly transformed into itself by substitutions leaving fixed all the letters of A_1 when J is alternating or symmetric. Hence we could apply Bochert's theorem (§ 6) to J whenever it is multiply transitive did we but know its class.

21. It is not difficult to show that the class of J is not greater than $2q - 3$. *Then if J is quadruply transitive it does not displace so many as $4q - 3$ letters.* While we are about it we shall prove that the class of J is not greater than $2q - 4$ although this result will not be used in the proof of Theorem XIII.

Since two commutative substitutions of order p and degree qp, $q < p$, on the same letters are powers one of the other, the order of H_1 is not divisible by p^2. Then if H_2 has a transitive constituent of degree $rp + s$, $s > 1$, the class of J is at most q. Let H_{i+1} be the first among the groups $H_1, H_2, \cdots$ in which any transitive constituent is of degree $rp + s$, $s > 1$. Then the transitive constituents of H_i, $i > 1$, are of the degrees $rp + 1, r'p + 1, \cdots, tp, t'p, \cdots$ ($r > 1$ or $t > 1$), and the order of H_i is not divisible by p^2 because its degree is less than $qp + p$. In consequence the J-group of each transitive constituent of degree $up + v$, $v > 1$, in H_{i+1} is transitive of degree v, and these v letters constitute a transitive constituent of the J-group of H_{i+1}. We do not however assert that this transitive constituent of the J-group of H_{i+1} coincides with the J-group of the transitive constituent of degree $up + v$. The degree of H_{i+1} is $qp + 2q - 1$, $qp + 2q - 2$, or $qp + 2q - 3$, if it is argued that the class of J exceeds $2q - 4$. If H_{i+1} is of degree $qp + 2q - 1$, H_{i+1} has a transitive constituent of degree $kp + 2k - 1$, k a positive integer greater than unity, and transitive constituents of degree $mp + 2m$, m a positive integer or zero. The transitive constituent of degree $kp + 2k - 1$ is primitive and is not alternating. No such group exists if k is less than 6 (§ 2). It can be shown that the subgroup (L) of H_{i+1} that leaves one letter of the primitive constituent of degree $kp + 2k - 1$ fixed and which includes

H_i has just the same transitive constituents as F $(= H_{ik_i})$: $2p + 2$, $p + 2$, $\cdots$, $p + 2$. For in the J-group of L the substitution of order 2 from F is invariant and has one invariant cycle that belongs to the constituent of F of degree $2p + 2$, so that if L has a transitive constituent of degree $mp + 2m$, $m > 1$, the class of J is at most $2q - 4$. Then the transitive constituent of degree $kp + 2k - 1$ in H_{i+1} is a simply transitive primitive group and in its subgroup that leaves one letter fixed the constituent of degree $2p + 2$ should be simply transitive in accordance with the theorem:*

If the degree of a transitive constituent of the subgroup leaving one letter fixed in a simply transitive primitive group exceeds by two (or more) units the degree of any other transitive constituent of that subgroup, then the transitive constituent of highest degree is a simply transitive group.

But because it includes a transitive subgroup of degree $2p + 1$, that constituent is doubly transitive. Let H_{i+1} be of degree $qp + 2q - 2$. If H_{i+1} has a primitive constituent of degree $kp + 2k - 2$, $k > 2$, F supplies to J a substitution of degree less than $2q - 2$ and of order 2. If a constituent of degree $kp + 2k - 2$, $k > 2$, is imprimitive, systems of two letters each are permuted by that constituent according to a non-alternating primitive group, so that k is greater than 10, and F again contains substitutions which throw substitutions of order 2 and degree less than $2q - 2$ into J. If H_{i+1} has one constituent of degree $2p + 2$, it must have a transitive constituent of degree $mp + 2m$, $m > 1$, generated by similar substitutions of order p and degree mp, an imprimitive group with systems permuted according to a triply transitive group of degree $p + 2$. In H_{i+1} a substitution conjugate to A_1 can be found that unites two cycles of A_1 (in letters of our imprimitive constituent) and introduces in m of its cycles exactly m new letters that form one of the $p + 2$ systems of imprimitivity of the constituent in question, and that fixes the m letters of another system. Thus the class of J is something less than $2q - 3$ when the degree of H_{i+1} is $qp + 2q - 2$. Let H_{i+1} be of degree $qp + 2q - 3$. Since now the J-group of H_{i+1} is of odd order, H_{i+1} has no transitive constituent of degree $mp + 2m$, $m = 1, 2, \cdots$, or of degree $kp + 2k - 2$, $k > 1$. Nor has it a primitive constituent. Then H_{i+1} is an imprimitive group with systems of three letters each permuted according to a primitive group of degree $(qp + 2q - 3)/3$ which is not triply transitive, and which therefore does not exist if q is less than 18. The subgroup F of H_{i+1} is of degree $qp + 2q - 6$ and certainly has a transitive constituent of degree $rp + s$, $s > 1$. Hence J is of class less than $2q - 3$.

22. From this point on we confine our attention to those primitive groups G whose J-groups (whether transitive or not) contain substitutions of degree not greater than $2q - 3$.

* American Journal of Mathematics, vol. 39 (1917), pp. 281–310.

Let G be of degree $qp + p$. The order of G_1, leaving one letter fixed, is not divisible by p^2 because its degree is $qp + p - 1$. It follows that the constituent J of the largest subgroup I in which $\{A_1\}$ is invariant is a transitive group of degree p. Any invariant subgroup (not identity) of J is also a transitive group of degree p. So that if I includes substitutions that leave fixed all the letters of A_1, they constitute an invariant subgroup of I and G contains a substitution of order p and degree p contrary to hypothesis. The largest group on the same letters in which $\{A_1\}$ is invariant is a subgroup of a group of order $p^q(p-1)(q!)$ in which there is just one subgroup of order p^q, generated by q cycles of order p in q $(q < p)$ different sets of letters. Now J, being of degree p, can not have an invariant subgroup of order p^2. Then J, whose order is not divisible by p^2, has an invariant subgroup of degree and order p, and is of class $p - 1$. To verify the statement that the class of J is $p - 1$ and not p, it is only necessary to notice that F of degree $qp + p - 1$ has not so many as q constituents and therefore has at least one transitive constituent of degree $rp + s$, $s > 1$. Hence $p - 1$ is less than $2q - 3$.

23. This primitive group G of degree $qp + p$ does not exist unless p is less than $2q - 2$, and then is not a subgroup of another group G' of higher degree. For if we grant that I', the largest subgroup of G' in which $\{A_1\}$ is invariant, has no substitutions on the letters of J' alone, as we must unless G' contains a transitive subgroup of degree $p + 1$, J' becomes impossible because the substitutions of order p in it should generate an invariant abelian subgroup of J' (I, Theorem VI, Corollary). But if G' contains a transitive subgroup of degree $p + 1$ the degree of G' does not exceed $2p + 2$.*

24. Let G be of degree $qp + 2p$. If the J-group of G is primitive and of degree $2p$, every invariant subgroup of J contains substitutions of order p, and I has no substitutions which fix all the letters of A_1. Therefore all the substitutions of order p in J generate an invariant abelian subgroup of J, an impossibility in a primitive group of degree $2p$.

25. Suppose now that the degree of H_{r+1} is not greater than $qp + q$. Its order therefore is not divisible by p^2 and its J_1-group is in consequence transitive. If H_{r+1} is imprimitive the degree of H_{r+s}, the last imprimitive group before the doubly transitive group H_{r+s+1}, is certainly less than $qp + q + q(1/2 + 1/4 + 1/8 + \cdots)$,† which in turn is less than $qp + 2q$. If H_{r+1} is primitive and if it permits of a quadruply transitive group H_{r+4}, the J_4 of H_{r+4} is of class not greater than q, so that by no possibility can the degree of a primitive group G which contains this primitive H_{r+1} of degree

* Marggraff, Dissertation, *Ueber primitive Gruppen mit transitiven Untergruppen geringeren Grades*, Giessen, 1889; and also, Wissenschaftliche Beilage zum Jahresberichte des Sophien-Gymnasiums zu Berlin, 1895, Programm nr. 65.

† These Transactions, vol. 7 (1906), pp. 499–508.

not greater than $qp + q$ exceed $qp + 2q + 2$. So too the class of the doubly transitive group J_1 in H_{r+s+1} (H_{r+1} imprimitive) is not greater than q, and G in that case can not be of degree greater than $qp + 2q + 2$. If p is greater than $q + 1$ none of these groups is of degree $qp + p$ or $qp + 2p$. *Then the order of none of the primitive groups G in which H_{r+1} is of degree not greater than $qp + q$ is divisible by p^2, provided q is less than $p - 1$.*

26. We have seen that if H_{r+1} is imprimitive, the last group H_{r+s}, just before H_{r+s+1}, has systems of n letters permuted according to a primitive group which is not triply transitive. Then if we assume the truth of Theorem XIII for primitive groups which contain a substitution of order p on less than q cycles, the degree of H_{r+s} is not greater than $(qp/n + 4q/n - 6)n = qp + 4q - 6n$, and the degree of the doubly transitive group H_{r+s+1} is not greater than $qp + 4q - 11$. This appears to fail when $n = q$, in which case the degree of the group in the systems is at most $p + 1$, and hence the degree of H_{r+s} is at most $qp + q$. The order of H_{r+s} is not divisible by p^2. If the degree of one of the following groups H_{r+s+t} $(t = 1, 2, \cdots)$ is $qp + 2p$, the corresponding J_{s+t}-group is multiply transitive and therefore impossible. If that degree is $qp + p$, $s = t = 1$, and the group J_2 of H_{r+2} is of order $p(p - 1)$. Since J_1 is regular, the degree of H_{r+1} is at most $qp + q$ and therefore $p = q + 1$.

In the remainder of this paper H_{r+1}, wherever mentioned, is understood to be a primitive group.

27. This question must now be answered: If the order of no transitive constituent of H_{ij} is divisible by p^2, can the order of H_{ij} be divisible by p^2? Look at H_{ij} as an isomorphism between one of its transitive constituents and one other (in general intransitive) constituent. The isomorphism in question is not a direct product, for substitutions of order p must be of degree not less than qp, while there are substitutions like A_1 in H_{ij} that involve letters of both constituents and which are of degree qp. Every transitive constituent of H_{ij} is generated by its complete set of conjugate subgroups of order p. Then H_{ij} is an (m, n) isomorphism between the two constituents, and m is not divisible by p. Suppose n is divisible by p. The common quotient group is of order kp, where k is prime to p. If in the constituent of order nkp, a transitive constituent has one subgroup of order p in the subgroup of order n, every subgroup of order p of the transitive constituent, and hence every substitution of that constituent is in the subgroup of order n. But this means that all those substitutions of H_{ij} which are of order p and involve letters of the first transitive constituent of order mkp displace no letters of a certain other transitive constituent. But A_1 involves letters of all the transitive constituents. Then in the subgroup of order n of the second constituent there is no substitution of order p of any one of the transitive constituents of H_{ij}. Then n is not divisible by p, nor is the order of H_{ij} divisible by p^2.

Alternating constituents of H_{ij}

28. Let us now see if H_{ij} can have an alternating constituent.

Suppose that an alternating constituent involves letters of two or more cycles of A_1. Then we may transform A_1 by the substitution $(a_1\, a_2\, a_3) \cdots$ of H_{ij} into a substitution C which has $(a_2\, a_3\, a_1\, a_4\, a_5 \cdots a_p)$ for its first cycle, $(b_1\, b_2\, b_3 \cdots b_p)$ for its second cycle. If C has two letters new to

$$A_1 = (a_1\, a_2\, a_3 \cdots a_p)(b_1\, b_2\, b_3 \cdots b_p) \cdots$$

in any cycle, in some power C^n, $n = 1, 2, \cdots$, or $(p-1)/2$, these two new letters are adjacent and in $C^{-n} A_1 C^n$ the second of the two new letters is omitted. Now if $\{A_1, C^{-n} A_1 C^n\}$ is again an alternating group in the constituent on the letters $a_1, a_2, \cdots, a_p$ the process may be repeated until we have C_1, similar to A_1, with $(a_2\, a_3\, a_1\, a_4 \cdots a_p)$ and $(b_1\, b_2\, b_3 \cdots b_p)$ for its first two cycles. Write $A = (123 \cdots p)$, and $B = (132) A (123)$. Then

$$\begin{aligned}
B^{-n} AB^n &= (132) A^{-n} (123) A (132) A^n (123) \\
&= (132) A^{-n} A (234) (132) A^n (123) \\
&= A (243) A^{-n} (134) A^n (123) \\
&= A (243) (1+n,\ 3+n,\ 4+n) (123) \\
&= A (12534) && (\text{for } n = 1), \\
&= A (12456) && (\text{for } n = 2), \\
&= A (12674) && (\text{for } n = 3),
\end{aligned}$$

and

$$= A (124) (1+n,\ 3+n,\ 4+n) \quad (3 < n \leqq (p-1)/2.)$$

Now the group $\{A, B^{-n} AB^n\}$ is a primitive group of degree p and of class at most 6, and hence is alternating. It is now evident that $\{A_1, C_1\}$ of degree less than $qp + q$ has two simple constituents of degree p each, one alternating and one cyclic, so that G certainly contains a substitution of order p and of degree less than qp. Then no alternating constituent of H_{ij} involves letters of two or more cycles of A_1.

29. Suppose an imprimitive constituent of H_{ij} has systems of imprimitivity permuted according to an alternating group such that A_1 permutes more than p of these systems. Then we may read the preceding paragraph with the understanding that $a_1, a_2, \cdots, b_1, b_2, \cdots$, are not single letters but are systems of imprimitivity, and draw the conclusion that A_1 does not permute more than p of these systems.

30. Any alternating constituent of H_{ij} implies the existence of (1) a subgroup $\{A_1, C\}$, where C is the transform of A_1 by the substitution $(a_1\, a_2\, a_3)(a_4) \cdots$ of H_{ij}, and (2) a subgroup $E_1 = \{A_1, C_1\}$ of the latter in which C_1,

a transform of A_1, has at most one letter new to A_1 to a cycle, and generates with A_1 an alternating group in the p letters $a_1, a_2, \cdots, a_p$.

When the prime p is greater than 7 a transitive group simply isomorphic to an alternating group of degree p is, if of degree greater than p, of degree $(p-1)p/2$. Corresponding to values of p greater than 7 there is this one transitive representation of the alternating group and no other of degree less than $(q-1)p+q$. For the two largest intransitive subgroups of the alternating group of degree p are of the orders $(p-2)!$ and $3(p-3)!$; the largest imprimitive subgroup is of order $[(p-1)/2]!\,2!$; the two largest alternating subgroups of the alternating group of degree p are of the orders $(p-1)!/2$ and $(p-2)!/2$; the largest non-alternating primitive subgroup of the alternating p-group is of index greater than $p(p-1)$.

31. Now for the first time we shall use the condition that p is greater than $2q-5$.

Since p is greater now than $2q-5$ this transitive constituent of degree $(p-1)p/2$ simply isomorphic to the alternating group of degree p can occur only if E_1 has at most three transitive constituents and is of degree at most $qp+2$. Whence it follows that H_{r+1} is of degree not greater than $qp+2q+2$.

32. If all the transitive constituents of E_1 are alternating groups, E_1 contains a substitution of any odd prime order P less than p and of degree qP. In particular there is a prime P such that $(q+1)/2 < P \leqq q-1$;* hence one of the two numbers, $qP+q^2-q$ or $2q^2-P^2$, either of which is less than $qp+q$, can be used for the limit of the degree of H_{r+1}, at least if H_{r+1} is simply transitive.

If H_{r+1} is doubly transitive it can contain no transitive subgroup of lower degree generated by substitutions that have fewer than p cycles each. For if H_{r+1} had such a transitive subgroup, its subgroup that leaves one letter fixed, and in which F is invariant, would also be an imprimitive group with no systems of so many as p letters. But F is intransitive.

33. Let there be at least one transitive constituent of order greater than $p!/2$ in multiple isomorphism to the alternating constituent of degree p. From the manner of the derivation of C_1, we know that C_1 can be taken similar to A_1 in the two generators of any transitive constituent of E_1. In a primitive constituent of order greater than $p!/2$ the head that corresponds to the identity of the alternating constituent is of order $(mp+n)k$ $(n \leqq m < q)$. If $n=0$, E_1 contains a substitution of order p and of degree less than qp. Then let n be greater than zero. The subgroup of this constituent that leaves one letter fixed is of order $k(p!/2)$ and has an invariant subgroup of

* Tchebychef, Journal de mathématiques, vol. 17 (1852), pp. 366–390; *Oeuvres*, 1899, vol. 1, pp. 51–70.

order k (which may be unity), with respect to which the quotient group is an alternating group of order $p!/2$. The subgroup of E_1 that leaves this letter fixed has the same alternating constituent as before. Call it E'; if E' has a primitive constituent of order greater than $p!/2$, pass on to E''; we must at last reach a group without a primitive constituent of order greater than $p!/2$ or with such a constituent of degree mp. Hence we may as well assume in the first place that E_1 has no primitive constituent of order greater than $p!/2$.

34. Let there be an imprimitive constituent of order greater than $p!/2$. If the invariant subgroup that corresponds to the identity of the alternating constituent is transitive, we have the same condition as when it was assumed primitive. Then the head may be taken to be intransitive. The two similar generators of order p permute systems of less than q letters. The largest possible systems are permuted according to a primitive group. Now the transitive sets of the head are systems of imprimitivity. There is no larger head because the quotient group with respect to the first is alternating. The group according to which these systems are permuted is simply isomorphic to the alternating group, that is, is the alternating group of degree p or its transitive representation on $p(p-1)/2$ letters, which last is impossible when q is less than p and p is greater than 7. Then if there are m letters in each system of imprimitivity of a certain transitive constituent, the degree of this imprimitive constituent is mp. Let P be the largest prime less than $2q-6$ so that an imprimitive constituent of E_1 has a substitution of order P which permutes systems, and since m, less than $q-2$, is less than P, it displaces no other letter of that constituent. Hence E_1 has a substitution of order P and degree qP. The substitutions of order P and degree qP in E_1 generate an invariant subgroup of E_1 which is an alternating-p group or has an alternating group of degree p as a quotient group. But this subgroup coincides with E_1 because it contains all E_1's substitutions of order p, two of which generate E_1. Take, in one of the imprimitive constituents of E_1, a subgroup that leaves $p-P$ systems fixed. This subgroup (E) is an isomorphism between alternating groups of degree P and imprimitive groups (for it respects the systems of E_1) having alternating quotient groups. Its degree is qP. Not all the constituents are alternating groups (we have discussed such a possibility before). Since H_{r+1} is primitive the substitutions of order P and degree qP in H_{r+1} generate a transitive group. Imprimitive constituents of E are of the degrees M_1P, M_2P, $\cdots$, $(M_1 \geqq M_2 \geqq \cdots)$. If M_1 is greater than $P/2$, E has at most $q-M_1+1$ transitive constituents. Therefore H_{r+1} contains a transitive subgroup of degree not greater than

$$qP + (q - M_1)q \leqq q^2 + qP/2 - q/2 < 2q^2 - 3q < qp.$$

If M_1 is less than $P/2$, there are in E substitutions of order P' and degree qP',

where P' is the largest prime less than P, and certain ones of which, just as before, generate a group E' with imprimitive constituents of degree $M_1' P'$, $M_2' P'$, $\cdots$ $(M_1' \geqq M_2' \geqq \cdots)$, each of which are alternating-P' groups in their systems of imprimitivity. Not all the transitive constituents are alternating groups of degree P', nor is M_1' greater than $P'/2$. Another subgroup E'' generated by substitutions of prime order P'' and of degree qP'', where P'' is the largest prime less than P', and with imprimitive constituents of degree $M_1'' P''$, $M_2'' P''$, $\cdots$ $(M_1'' \geqq M_2'' \geqq \cdots)$ can next be set up, and so on. Thus we can find a substitution of order p' and degree qp', $q - 1 \geqq p' > (q + 1)/2$, which insures that the degree of H_{r+1} is at most

$$qp' + q^2 - q < 2q^2 - 2q \leqq qp + q,$$

or else is at most

$$2q^2 - p'^2 < 2q^2 - (q + 1)^2/4 < qp + q.$$

With the next paragraph in view, it should be noticed that E_1 may be free from alternating constituents of degree p without affecting the above conclusion.

35. Any imprimitive constituent of H_{ij} is generated by substitutions of order p, one of which must permute systems, so that the number of letters in a system of imprimitivity is at most q and all these generators permute systems. There are at least p systems in such an imprimitive constituent. Suppose that the group in the systems is alternating. Then H_{ij} contains a substitution which in that constituent is a circular permutation of just three systems. Transform A_1 by it, and the transform C generates with A_1 a group with an imprimitive constituent of degree $m'p$, which is alternating in its systems. Continuing step by step we can find a group $E_1 = \{A_1, C_1\}$, in which C_1, similar to A_1, generates with A_1 an imprimitive constituent, alternating in the systems, and has not more than one new letter in a cycle. All the transitive constituents of E_1 are imprimitive groups with systems permuted according to alternating groups of degree p.

Hence H_{ij}, when p is greater than $2q - 5$, can have no transitive constituent which is alternating or permutes systems of imprimitivity according to an alternating group.

The degree of F

36. If H_{r+1} is a primitive group, its subgroup F $(= H_{rk_r})$, of degree lower by unity, is an isomorphism between groups generated by substitutions of order p, which are not alternating, nor, if imprimitive, are the groups in the systems alternating. Then if we assume the truth of our theorem for smaller values of q than the one actually under consideration, we may say that F is an isomorphism between x_i primitive constituents of degree at most $q_i p/x_i + 4q/x_i - 4$ (or by the same symbolism an imprimitive constituent of degree

$q_i(p+4) - 4x_i$ with systems of x_i letters each permuted according to a primitive group of degree $q_i p/x_i + 4q_i/x_i - 4)$, $i = 1, 2, \cdots$, and y constituents of degree p, y_1 of degree $p+1$, y_2 of degree $p+2$, including imprimitive groups with systems permuted according to groups of these degrees, making the degree of F at most

$$yp + y_1(p+1) + y_2(p+2) + \sum x_i(q_i p/x_i + 4q_i/x_i - 4)$$
$$= qp + 4q - 4y - 3y_1 - 2y_2 - 4\sum x_i.$$

Here $\sum x_i$ is not zero, so that the maximum degree of F is got by putting $\sum x_i = 1$, $y_2 = 1$, and $y = y_1 = 0$. This maximum degree is then $qp + 4q - 6$, so that the maximum degree of H_{r+1} appears to be $qp + 4q - 5$. The next highest degree of F is got by putting $\sum x_i = 1$, $y = 0$, $y_1 = 1$, and $y_2 = 0$, whence F is of degree $qp + 4q - 7$; and after this we have the degree $qp + 4q - 8$, by putting $\sum x_i = 2$, $y = y_1 = y_2 = 0$, or by putting $\sum x_i = 1$, $y = y_1 = 0$, $y_2 = 2$, etc. This last limit, $qp + 4q - 8$ we may accept, for when H_{r+1} is a simply transitive primitive group a constituent of F on more than half the letters of F is not more than simply transitive (by the theorem quoted in § 21). Then when there are just two transitive constituents in F, and one is of degree $p+1$ or $p+2$, the other constituent is of degree not greater than $(q-1)p + 4(q-1) - 7$, making the degree of F at most $qp + 4q - 8$. If the large constituent is imprimitive, we have $\sum x_i$ greater than unity. If H_{r+2}, H_{r+3}, H_{r+4} exist, their degrees are not greater than $qp + 4q - 6$, $qp + 4q - 5$, $qp + 4q - 4$, respectively. A group H_{r+5} of degree $qp + 4q - 3$ that contains the primitive group H_{r+1} we have seen to be impossible because its group J_5 is a quintuply transitive group of class less than $2q - 2$, the degree of which therefore can not be so great as $4q - 3$ (§ 21).

37. If p is greater than $2q - 5$, $2p$ is greater than $4q - 7$, so that the degree of H_{r+1} can not be $qp + 2p$. It was noted (§ 24) that no one of the groups H_{r+2}, H_{r+3}, $\cdots$ is of degree $qp + 2p$, and if at last we impose the strong condition, that p be greater than $2q - 3$, the degree of no one of our primitive groups is $qp + p$ (§ 23). Then the order of G is in no case divisible by p^2, and the proof of Theorem XIII by induction is complete.

38. The degrees of the primitive groups of class 4 and of class 6 do not exceed 8 and 10 respectively so that it is possible to formulate the clean-cut

THEOREM XV. *The degree of a primitive group of class greater than* 3 *which contains a substitution of prime order* p *on* q *cycles* $(p > 2q - 3,\ q > 1)$ *does not exceed* $qp + 4q - 4$.

STANFORD UNIVERSITY,
December, 1916