ON THE LIMIT OF THE DEGREE OF PRIMITIVE GROUPS*

BY

W. A. MANNING

To the theory of multiply transitive groups BOCHERT has contributed formulæ for the upper limit of the degree of a group when the number of letters displaced by a substitution in it is known.† But for simply transitive primitive groups a corresponding theorem of such elegance does not exist.‡ However, in the present paper is offered a theorem with some claims to simplicity. It may be stated thus:

If a simply transitive primitive group contains a substitution of prime order p and of degree pq (q less than $2p+3$), its degree is not greater than the larger of the two numbers $qp+q^2-q$, $2q^2-p^2$.

Also when the given substitution of prime order has more than $2p+2$ and less than p^2 cycles or when p is 2 or 3, our results are capable of fairly concise expression; but when q exceeds p^2-1 and p is greater than 3 the corresponding upper limit is unfortunately a more complicated function of p and q.

The subject matter of this study is not restricted to the simply transitive primitive groups, but it is proposed to find an upper limit for the degree of some transitive subgroup of a primitive group known to contain a substitution of order p on qp letters. It seems unnecessary to state that a simply transitive primitive group has no transitive subgroup of a lower degree.

A property of transitive groups generated by substitutions of prime order.

1. Let $s_1, s_2, \cdots$ be certain substitutions of prime order that generate a transitive group G.§ For the sake of brevity of statement we may assume that all substitutions of G which are similar to $s_1, s_2, \cdots$ have been added to and

* Presented to the Society, Chicago, December 31, 1909.

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

‡ JORDAN, Bulletin de la Société Mathématique de France, vol. 1 (1873), pp. 175–221; Crelle's Journal, vol. 79 (1874), 248–258. The latter should be read in connection with the present paper. See also MANNING, Bulletin of the American Mathematical Society, vol. 13 (1907), p. 373.

§ In the American Journal of Mathematics, vol. 28 (1906), p. 226, the author imposed the condition that G is invariant in a primitive group. In these Transactions, vol. 10 (1909), p. 247, that condition was removed, but it was assumed that no substitution $s_1, s_2, \cdots$ has more than $p-1$ cycles. In the present investigation both these restrictions are removed. Note that the substitutions $s_1, s_2, \cdots$ are not said to be similar or yet of the *same* prime order.

are included in the series $s_1, s_2, \cdots$. Of these substitutions let $s_1, s_2, \cdots, s_i$, say, generate an intransitive subgroup H_i of G. If an arbitrary choice is made of a transitive constituent of H_i, it will ordinarily be possible to find among the substitutions of the series $s_1, s_2, \cdots$ a substitution s_{i+1} which replaces one of the letters of the arbitrarily chosen constituent by a letter of some other set of H_i. We seek the conditions under which it is impossible to affirm the existence of such a substitution.

Let the selected set of letters of H_i be $a_1, a_2, \cdots, a_{n_i}$. By hypothesis there is no substitution in the series $s_1, s_2, \cdots$ which replaces a letter a by a letter b, where b represents any letter displaced by H_i but not belonging to the set a. However, there must be at least one substitution in the series $s_1, s_2, \cdots$ that replaces an a by a letter α new to H_i, since G is transitive, and otherwise one of these generators would replace an a by a b. It is conceivable that there are a number of substitutions s_{i+1} that replace an a by an α. Let us select from $s_1, s_2, \cdots$ one that adds the least possible number of new letters to the set a. We may impose a second independent condition that s_{i+1} shall displace, in the cycles which do not involve letters α, as small a number of new letters β as possible. If no substitution s_{i+2} unites the extended set a of H_{i+1} to some other set of H_{i+1}, we select s_{i+2} in the same way. We may continue thus until we can find a substitution s_{k+2} which replaces a letter of the extended set $a_1, a_2, \cdots$ of H_{k+1} by a letter of some other transitive constituent of H_{k+1}. Let $a_1, a_2, \cdots, a_{n_k}$ be the letters of the set $a_1, \cdots$ of H_k, which we shall call the set a.

2. If p, the order of s_{k+1}, is an odd prime, and if s_{k+1} may be so chosen that it has not more than one letter new to H_k in any cycle, then we can show as follows that there is a substitution s in the series $s_1, s_2, \cdots$ which replaces a letter of the set a of H_k by a letter of another set of H_k, contrary to the hypothesis on which the group H_{k+1} was set up. Thus of course we may not have $s_{k+2} = (a_1 b_1 \cdots)\cdots$, where b_1 is one of the letters (b) of H_k not included in the set a. If $s_{k+2} = (\alpha_1 \beta_1 \cdots)\cdots$, where α_1 is a part of the set $a_1, a_2, \cdots$ of H_{k+1}, and β_1 is a letter of H_{k+1} but not in the set $a_1, a_2, \cdots$ nor yet in H_k, then $s_{k+1}^{-1} s_{k+2} s_{k+1}$ replaces an a of H_k by a b of H_k. If $s_{k+2} = (a_1 \beta_1 \cdots)\cdots$ or $(\alpha_1 b_1 \cdots)\cdots$, the same is true of $s_{k+1}^{-1} s_{k+2} s_{k+1}$ or else of $s_{k+1} s_{k+2} s_{k+1}^{-1}$. If $p = 2$ and s_{k+1} replaces an a by an α, the same result follows. For let $s_{k+2} = (a_1' \beta \cdots$ and $s_{k+1} = (a' a'')(b' \beta)\cdots$, where perhaps $a' = a''$. Some substitution H_k transforms s_{k+2} into $(a'' \beta \cdots$ and $s_{k+1}^{-1}(a'' \beta \cdots) s_{k+1} = (a' b' \cdots)$.

3. Now consider the substitution s_{k+1}. It bears the same relation to H_k as s_{i+1} does to H_i. We first note that every power of s_{k+1} replaces an a by an α. If there are two letters α in a cycle of s_{k+1}, in a certain power s_{k+1}^x these two letters α_1 and α_2 are adjacent. Now one of the generators of $s_{k+1}^{-x} H_k s_{k+1}^x$ will replace a letter a by an α unless s_{k+1}^x replaces each one of the n_k letters $a_1, a_2, \cdots, a_{n_k}$ by a letter α, new to H_k; if every a is followed by an α and if

there are two letters a in the same cycle, $s_{k+1}^{x} = (a_1 \alpha' \cdots a_2 \alpha'' \cdots) \cdots$ and $s_{k+1}^{xy} = (a_1 a_2 \cdots \alpha' \alpha'' \cdots) \cdots$. *Hence* s_{k+1} *either has at most one* α *in any cycle, and also at most one* β *in any one of the other cycles, or* s_{k+1} *is of the type*

$$(A) \quad (a_1 \alpha_1' \alpha_1'' \cdots \alpha_1^{(p-1)})(a_2 \alpha_2' \alpha_2' \cdots \alpha_2^{(p-1)}) \cdots (a_{n_k} \alpha_{n_k}' \alpha_{n_k}'' \cdots \alpha_{n_k}^{(p-1)}) \cdots ;$$

and in this second case we should note that the minimum number of new letters displaced in cycles with $a_1, a_2, \cdots, a_{n_k}$ by any substitution of the series $s_1, s_2, \cdots$, which connects letters of the set a of H_k with other letters, is equal to the maximum number of such new letters.

4. It may be possible to find a substitution t that replaces an a by an a and an a by some letter ω not one of the letters $a_1, a_2, \cdots, a_{n_k}$, and such that *both* $t^{-1}H_k t$ *and* $tH_k t^{-1}$ *are subgroups of* G. Consider the group $t^{-1}H_k t$. One of the generators σ (a member of the series $s_1, s_2, \cdots$) of $t^{-1}H_k t$ replaces an a by a letter not belonging to the set a. This is clear since the set of letters in $t^{-1}H_k t$ which takes the place of the n_k letters a of H_k is now composed of two classes of letters, letters a and *not-a*. Then σ is of the type (A) with the n_k letters a involved in exactly n_k cycles, and the remaining places in these cycles are filled by letters new to H_k. Hence

$$t = (aa' \cdots a'' \alpha \cdots b\alpha' \cdots),$$

that is, t replaces an a by an a, an a by a new letter α, and some letter b of H_k by a letter new to H_k, so that tHt^{-1} leaves fixed the letter a'', and one of its generators (belonging to $s_1, s_2, \cdots$) replaces an a by a *not-a*. This *not-a* cannot, by hypothesis, be a b from H_k, and is therefore an α. But since $tH_k t^{-1}$ leaves one a fixed, this generator is not of the type (A). *Hence, whenever a substitution* t *can be set up satisfying the conditions stated, the substitution* s_{k+1} *of prime order* p *has at most one new letter in any cycle.*

This is trivial when $p = 2$, for then the maximum number of new letters α in a cycle is one. But suppose that s_{k+1} is of type (A):

$$s_{k+1} = (a_1 \alpha_1)(a_2 \alpha_2) \cdots (a_{n_k} \alpha_{n_k}) \cdots,$$

and let us consider the group $t^{-1}H_k t$. From this it follows that t has the form displayed above. The transform of H_k by t^{-1} gives a substitution belonging to the series $s_1, s_2, \cdots$ which leaves fixed one of the letters a, and replaces at least one of them by a letter α. Thus when $p = 2$ the minimum number of new letters α is not in excess of $n_k - 1$. If there are two letters new to H_k in any cycle of s_{k+1} (of order 2), $s_{k+1}^{-1} H_k s_{k+1}$ leaves those two new letters fixed and one of its generators replaces an a by an a and an a by an α, since $s_{k+1}^{-1} H_k s_{k+1}$ has not more new letters in the set which takes the place of a than the number of new letters that s_{k+1} connects with the a's, that is, than $n_k - 1$.

5. It will be convenient to have a summary of the preceding results. We recall that $s_1, s_2, \cdots$ are substitutions of prime order that generate a transitive group G, and that $s_1, s_2, \cdots, s_i$ generate an intransitive subgroup H_i of G. The letters $a_1, a_2, \cdots, a_{n_i}$ compose a given set of intransitivity of H_i. If it is impossible to find a substitution in $s_1, s_2, \cdots$ that connects another set of H_i with the set a, we pass to the study of the group H_k. Now H_k coincides with or includes H_i and while the set $a_1, a_2, \cdots, a_{n_k}$ may contain more letters than the set $a_1, a_2, \cdots, a_{n_i}$ of H_i, it includes no letter of any other set of H_i. *But if there is no substitutiion among $s_1, s_2, \cdots$ possessing the required property (of connecting the set $a_1, a_2, \cdots$ of H_k with another set of H_k), all the substitutions of the series $s_1, s_2, \cdots$ that replace one of the letters $a_1, a_2, \cdots, a_{n_k}$ by a letter not a member of this set must be of the type*

$$(A) \quad (a_1, \alpha_1', \alpha_1'', \cdots, \alpha_1^{(p-1)})(a_2\alpha_2'\alpha_2'' \cdots \alpha_2^{(p-1)}) \cdots (a_{n_k}\alpha_{n_k}'\alpha_{n_k}'' \cdots \alpha_{n_k}^{(p-1)}) \cdots .$$

None of the letters α in (A) are displaced by H_k, or *à fortiori*, by H_i.

But we have another condition. Among $s_1, s_2, \cdots$ there certainly exists a substitution that replaces an a of H_k by a letter of another set of H_k, provided a substitution t can be set up that replaces an a by an a, and an a by a *not-a*, and having in addition the property that the two transformed groups $t^{-1}H_kt$ and tH_kt^{-1} are both subgroups of G. In particular G itself contains such a substitution t whenever $a_1, a_2, \cdots, a_{n_k}$ do not form a system of imprimitivity of G.

This is only a partial solution of the problem proposed, but it is sufficient for our present purpose.

Other properties of the prime generators of a transitive group.

6. Suppose that there is in the series $s_1, s_2, \cdots$ a substitution s_{i+1} that replaces a letter of any given set of H_i by a letter of H_i not belonging to that set. From all the substitutions of the series $s_1, s_2, \cdots$ which replace an a by a b, let us select those which displace the minimum number of new letters. Now suppose that one of these substitutions thus selected is such that every power replaces an a by an a. *From this hypothesis we shall conclude that s_{i+1} has at most one new letter in any cycle.* Let new letters be denoted by α, whether they are transitively connected with $a_1, a_2, \cdots$ or not. If s_{i+1} has two letters adjacent in any cycle, $s_{i+1}^{-1}H_is_{i+1}$ leaves fixed the second of them, so that by hypothesis $H' = \{H_i, s_{i+1}^{-1}H_is_{i+1}\}$ can have no generator (belonging to $s_1, s_2, \cdots$) which replaces an a by a b. But H' has letters a and letters b in the same constituent, and all that we can affirm of this constituent is that it is a transitive group generated by certain substitutions of prime order. Bearing in mind the results of § 5, we know that there must be a set of letters $a_1, a_2, \cdots, a_{n_k}$ including the set $a_1, a_2, \cdots, a_{n_i} (n_i \leqq n_k)$, such that all the generators of H' which replace a letter of the set $a_1, a_2, \cdots, a_{n_k}$ by a letter

not in that set are of the type (A). Now s_{i+1} replaces an a by an a and an a by a b, that is by a letter not in the set $a_1, a_2, \cdots, a_{n_k}$. By hypothesis s_{i+1} has the three sequences $a_1 a_2$, $a_3 b_1$, $\alpha_1 \alpha_2$. Since $s_{i+1}^{-1} H_i s_{i+1}$ has at least one substitution of type (A), s_{i+1} must also have the two other sequences $a_4 \alpha_3$ and $b_2 a_5$. Now consider the group $H'' = \{ H_i, s_{i+1} H_i s_{i+1}^{-1} \}$. Since H'' does not displace α_1, no substitution (belonging to $s_1, s_2, \cdots$) of H'' replaces an a by a b. But $s_{i+1} H_i s_{i+1}^{-1}$ leaves fixed a_4 as well as α_1 and a generator certainly replaces an a by a *not-a*, no matter how far we have extended the original set $a_1, a_2, \cdots, a_{n_i}$ of H_i by new letters. That is to say, when we have formed the extended set $a_1, a_2, \cdots, a_{n_k}$ in the constituent $a_1, a_2, \cdots$ of H'', among the generators of $s_{i+1} H_i s_{i+1}^{-1}$ there is a substitution connecting other letters with the letters $a_1, a_2, \cdots, a_{n_k}$ and which is not of the type (A), inasmuch as it leaves fixed one of the letters a. Therefore, s_{i+1} has not two new letters adjacent in any cycle. If there are two new letters in one cycle of s_{i+1}, some power s_{i+1}^x brings them together. From what has just been said it follows that in s_{i+1}^x no a is followed by or preceded by a b, but $s_{i+1}^x = (a_2 \alpha_1 \cdots b_2 \alpha_2 \cdots) \cdots$, and $s_{i+1}^{xy} = (a_2 b_2 \cdots \alpha_1 \alpha_2 \cdots) \cdots$, which again is the case fully discussed. We have proved that *if one of the substitutions $s_1, s_2, \cdots$, which replaces an a by a b and displaces the minimum number of new letters, has the property that no power of it replaces every a by a not-a, then there is at most one new letter in any one of its cycles.*

7. If $b', b'', \cdots, b^{(\rho)}$ are sets b of H_i which have at least one letter in the same cycle of s_{i+1} with a letter a (a arbitrarily chosen), and unless s_{i+1} has a power which replaces every b' by a *not-b'* for at least one of the sets $b', b'', \cdots, b^{(\rho)}$, then s_{i+1} has at most one new letter to a cycle. This is an easy inference from the preceding section.

8. Let s_{i+1}, one of the substitutions $s_1, s_2, \cdots$, be chosen subject to the conditions:

(1) It unites at least two sets of H_i;

(2) it displaces as few new letters as any substitution that satisfies (1);

(3) it unites as few sets as any of the substitutions satisfying (1) and (2); then if s_{i+1} does not displace all the letters of all the sets united it has at most one new letter to a cycle. This follows from § 6.

9. We again select from $s_1, s_2, \cdots$ those substitutions which replace a letter of the set a of H_i by a letter of some other set, and which displace the minimum number of letters α, new to H_i (assuming that at least one such substitution exists). What follows if one of these substitutions (s_{i+1}) has a cycle composed entirely of new letters? As a matter of notation let $\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_{i+1}, \overline{H}_i$, etc., be the substitutions and groups remaining after the erasure of the letters of $\{ H_i, s_{i+1} \}$ that do not form a part of the set $a_1, a_2, \cdots$. The group K_{i+1} generated by the conjugates of H_i is invariant in H_{i+1}, and the constituent $\overline{K}_{i+1}$

is invariant in $\bar{H}_{i+1}$. If $\bar{K}_{i+1}$ is intransitive its sets of intransitivity are systems of imprimitivity of $\bar{H}_{i+1}$ and these systems are permuted by s_{i+1}. If $\bar{K}_{i+1}$ is transitive, we note that, since $\bar{K}_{i+1}$ leaves fixed certain letters α, no generator (belonging to $\bar{s}_1, \bar{s}_2, \cdots$) can replace an a of H_i by a b. Then $\bar{K}_{i+1}$ has a subgroup $\bar{H}_k$, the set $a_1, a_2, \cdots, a_{n_i}, \alpha_1, \cdots, \alpha_{n_k-n_i}$ of which is a system of imprimitivity of $\bar{H}_{i+1}$. Since $\bar{s}_{i+1}$ replaces an a by a b, $\bar{s}_{i+1}$ replaces the system $a_1, \cdots, \alpha_1, \cdots$ by another system. Hence the result:

If s_{i+1} connects transitively a given set a of H_i and another set, and displaces the minimum number of new letters, it cannot contain a cycle composed entirely of new letters unless it actually displaces the n_i letters a and has not more than one letter a in any cycle.

Applications to primitive groups.

10. Now let $s_1, s_2, \cdots$ be a complete set of conjugate substitutions of prime order p and of degree pq in a primitive group. The subgroup $\{s_1, s_2, \cdots\}$, because invariant in a primitive group, is transitive. As before let all the substitutions of $\{s_1, s_2, \cdots\}$ that are similar to s_1 be associated with the original set of generators $s_1, s_2, \cdots$. Since we have to do with a primitive group in which $\{s_1, s_2, \cdots\}$ is invariant, there exists a substitution t satisfying the conditions of § 5, and in consequence there is in the series $s_1, s_2, \cdots$ a substitution s_{i+1} that replaces a letter of any given set of H_i by a letter of H_i not belonging to that set (an a by a b if we continue the former notation). Let N_i be the degree of H_i, c_i the number of its transitive constituents, and as before let n_i be the degree of the constituent a. We shall make use of a number θ which represents $2p/(p-1)$ when p is odd, but is equal to 2 when p is 2. Again suppose that we have before us all the substitutions of the series $s_1, s_2, \cdots$ that (1) connect the given system a with other letters of H_i, and (2) displace the minimum number of new letters. If all these substitutions have a power that replaces every a by a *not-a*, if each one of them displaces all the letters of one of the sets $b', b'', \cdots$ whose letters are found in cycles with a, and if more than one new letter is in some cycle, we have two cases to consider. Each of these substitutions may have at least one cycle entirely new to H_i, in which case the following inequalities hold true:

$$(B)\quad N_{i+1} \leqq N_i + pq - n_i - p, \qquad c_{i+1} \leqq c_i - 1 + q - n_i, \qquad n_{i+1} \geqq pn_i.$$

On the other hand if even one substitution has no cycle of new letters only, the three conditions just stated being satisfied, we conclude that

$$(C)\qquad N_{i+1} \leqq N_i + pq - n_i - p, \qquad c_{i+1} \leqq c_i - 1, \qquad n_{i+1} \geqq \theta n_i.$$

The inequality $n_{i+1} \geqq \theta n_i$ requires explanation. If $n_{i+1} < \theta n_i$, every power of s_{i+1} replaces one letter a at least by an a. Then the number of new letters is

q at most, with not more than one in any cycle. In fact, if there is one of the substitutions that satisfy (1) and (2) for which any one of the three conditions under which (B) and (C) were formed fails, that substitution s_{i+1} has not more than one new letter in any cycle. Hence

$$(D) \qquad N_{i+1} \leqq N_i + q, \qquad c_{i+1} \leqq c_i - 1, \qquad n_{i+1} \geqq n_i + p.$$

11. In the formation of the groups $H_2, H_3, \cdots$ there is another point of view which is of value. We no longer base our reasoning upon an arbitrarily chosen set a of H_i, but impose upon s_{i+1} the conditions of § 8, which we need not repeat, and in addition the condition (4) that no substitution of $s_1, s_2, \cdots$ which satisfies (1), (2) and (3) has fewer cycles in the letters of the extended set formed by the union of sets of H_i by s_{i+1}. Let $\bar{H}_i$, $\bar{H}_{i+1}$, $\bar{K}_{i+1}$, have the same meaning as before, that is, $\bar{H}_{i+1}$ is transitive in the letters of the sets $a, b, \cdots$ of H_i and certain new letters which s_{i+1} joins to these sets. If $\bar{s}_{i+1}$ is of higher degree than any of the substitutions $\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_i$, then by condition (4), no substitution of $\bar{K}_{i+1}$, similar to one of the substitutions $\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_i$, can connect in its cycles two of the sets of $a, b, \cdots$. Then if two of the sets $a, b, \cdots$ are in one transitive constituent of $\bar{K}_{i+1}$, there are substitutions in $\bar{K}_{i+1}$ that displace all the letters of one of the sets, as a, and such that all powers of these substitutions replace every a by a new letter:

$$r = (a_1 \alpha_1' \cdots \alpha_1^{(p-1)}) \cdots (a_{n_i} \alpha_{n_i}' \cdots \alpha_{n_i}^{(p-1)}) \cdots.$$

The transforms of r by substitutions of H_i generate a group with a transitive constituent of degree pn_i in the letters $a_1, a_2, \cdots, \alpha_1', \cdots, \alpha_{n_i}^{(p-1)}$. If $\bar{K}_{i+1}$ does not unite transitively two sets of H_i, the sets of intransitivity of $\bar{K}_{i+1}$ are systems of imprimitivity of $\bar{H}_{i+1}$ which $\bar{s}_{i+1}$ must permute. Then the degree of $\bar{H}_{i+1}$ is pn_i or more. If one system is made up entirely of new letters, the transforms of $\bar{s}_{i+1}$ by substitutions of $\bar{H}_i$ generate a transitive group. If no system is made up entirely of new letters, exactly p distinct sets of $a, b, \cdots$ of H_i are united by $\bar{s}_{i+1}$. Consider in particular a substitution $\bar{s} = (a_1 a_2 \cdots a_p) \cdots$ of $\bar{H}_i$. The group $\{ r, s^{-1} rs \}$ has a constituent of degree p^2, and for it

$$(E) \qquad N_2 \leqq 2pq - p^2, \qquad c_2 \leqq 1 + 2(q-p), \qquad n_2 \geqq p^2.$$

Likewise, when $\bar{K}_{i+1}$ has p sets, if a power of $\bar{s}_{i+1}$ replaces each of the letters $a_1, a_2, \cdots a_p$ by a new letter α, the same inequalities are satisfied by the group $\{ s_{i+1}, s^{-1} s_{i+1} s \}$. If no power of s_{i+1} replaces each of the letters $a_1, a_2, \cdots, a_p$ by letters new to H_i, s_{i+1} involves all the letters of p cycles of s, so that the inequalities hold for $\{ s, s_{i+1} \}$.

Now we assume that $\bar{s}_{i+1}$ is not of higher degree than the substitutions of highest degree among $\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_i$, and that s_{i+1} has two new letters in some one of its cycles. We know (§ 8) that $\bar{s}_{i+1}$ displaces all the letters of $\bar{H}_i$ so that

$\bar{s}_{i+1}$ displaces no new letter. From this it follows that every power of s_{i+1} replaces a letter of one set of $\bar{H}_i$ by a letter of another set of $\bar{H}_i$. Let s^x_{i+1} have two new letters adjacent. Because of condition (2) no generator of $\{\bar{H}_i, \bar{s}^{-x}_{i+1}\bar{H}_i\bar{s}^x_{i+1}\}$ has letters of two sets of H_i in one of its cycles. But since there are no new letters α in this group, $\bar{s}_{i+1}$ permutes cyclically p sets $a, b, \cdots$ of $\bar{H}_i$. Again if $\bar{s}$ is a generator of $\bar{H}_i$, the group $\{s, s_{i+1}\}$ satisfies inequalities (E) provided $\bar{s}$ displaces letters of all the p sets $a, b, \cdots$; but if $\bar{s}$ leaves fixed all the letters of one of the sets $a, b, \cdots$, the group $\{s, s^{-1}s_{i+1}s\}$ satisfies inequalities (E). The result which we are going to use is this:

If we have before us a group H_i we may be able to find in $s_{i+1}, s_{i+2}, \cdots$ a substitution which unites two or more sets of H_i and has at most one new letter in any cycle, thus satisfying the inequalities:

$$(F) \qquad N_{i+1} \leqq N_i + q, \qquad c_{i+1} \leqq c_i - 1.$$

A third inequality $n_{i+1} \leqq n_i$ is irrelevant since the largest set of H_i is not taken into account and may not be enlarged by s_{i+1}. But if $s_{i+1}, s_{i+2}, \cdots$ do not include such a substitution, we can say that there are two substitutions in the series $s_1, s_2, \cdots$ which we are at liberty to use for s_1 and s_2 which generate a group satisfying (E). The constituent of degree p^2 or more is imprimitive.

12. Should it be possible to find for all the groups $H_i (i = 1, 2, \cdots)$ up to the transitive group H_λ a substitution s_{i+1} with at most one new letter to a cycle, then the degree of H_λ is not greater than $pq + (q-1)q$. This is certainly true if q is less than or equal to p. But if at any point in the formation of this chain of groups, there is no substitution s_{i+1} with at most one new letter in a cycle, we begin our series $H_1, H_2, \cdots$ with the H_2 satisfying (E). Let us first impose upon q the condition $p < q < 2p + 3$, and suppose p odd. If then the upper limit of the degree of H_λ is not given by $pq + q^2 - q$, we begin with inequalities (E). In the next step we cannot have inequalities (D) since then the p^2 (or more) letters of a set a of H_2 would have to be present in at least $\theta p = 2p + 2 + 2/(p-1)$ cycles of s_3. Then the degree of H_λ is not greater than $N_2 + (c_2 - 1)q = 2q^2 - p^2$. Note that if $q = p + 1$, $pq + q^2 - q > 2q^2 - p^2$, and if $q = 2p$, $pq + q^2 - q < 2q^2 - p^2$; it is sufficiently precise to state that *a primitive group that contains a substitution of order p and degree pq (p an odd prime, $p < q < 2p + 3$), contains a transitive subgroup the degree of which is not greater than the larger of the two numbers $pq + q^2 - q$ and $2q^2 - p^2$.*

13. Let us now suppose that q is subject to the inequality $2p + 3 \leqq q < p^2$, and that p is odd. Let H_2 satisfy (E). If we have before us a group H_i, the question arises: What comparison exists between the degree of H_λ when H_{i+1} satisfies (C) and H_{i+2} satisfies (E) and the degree when H_{i+1} is subject to (E) while H_{i+2} obeys (C)? A simple calculation shows that there is no difference in the degrees. But to have H_{i+1} satisfy (C) and H_{i+2} (D) is more unfavor-

able than the reverse. Then let $H_3, H_4, \cdots, H_x$ obey (C), so that

$$N_3 \leqq N_2 + pq - n_2 - p, \qquad c_3 \leqq c_2 - 1, \qquad n_3 \leqq \theta p^2,$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$N_x \leqq N_{x-1} + pq - n_{x-1} - p, \qquad c_x \leqq c_{x-1} - 1, \qquad n_x \leqq \theta^{x-2} p^2.$$

The remaining groups $H_{x+1}, \cdots, H_{2(q-p+1)}$ satisfy (D):

$$N_{x+1} \leqq N_x + q, \qquad c_{x+1} \leqq c_x - 1, \qquad n_{x+1} \leqq \theta^{x-2} p^2 + p,$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$N_{2(q-p+1)} \leqq N_{2(q-p)+1} + q, \qquad c_{2(q-p+1)} \leqq c_{2(q-p)+1},$$

whence

$$N_{2(q-p+1)} \leqq xpq - p^2 - (x-2)p - (p^2 + p^2\theta + \cdots p^2\theta^{x-3}) + (2q - 2p + 2 - x)q,$$

or

$$N_{2(q-p+1)} \leqq 2q^2 - p^2 + (pq - q - p)(x-2) - p^2\frac{\theta^{x-2} - 1}{\theta - 1}.$$

A condition which n_{x-1} must satisfy is

$$n_{x-1} \leqq q\frac{p-1}{2},$$

that is

$$\theta^{x-3} p^2 \leqq q\frac{p-1}{2}.$$

If H_{x-1} instead of H_x were the last group subject to inequality (C), then

$$N_{2(q-p+1)} \leqq 2q^2 - p^2 + (pq - q - p)(x-3) - p^2\frac{\theta^{x-3} - 1}{\theta - 1}.$$

This expression is always numerically less than the other. For the difference

$$(pq - q - p) - p^2\theta^{x-3} \geqq pq - q - p - q\frac{p-1}{2} \geqq \frac{p-1}{2}(q - \theta),$$

is positive. Hence the limiting value of the degree of H_λ is obtained by replacing x in the first formula by the largest integer which satisfies $\theta^{x-3}p^2 \leqq q(p-1)/2$, and this is the largest integer in $2 + \log_\theta(q/p)$.

If a primitive group contains a substitution of odd prime order p on more than $2p + 2$ and less than p^2 cycles, it contains a transitive subgroup of degree not greater than

$$2q^2 - p^2 + (pq - q - p)\mu - p^2\frac{\theta^\mu - 1}{\theta - 1},$$

where μ is the integral part of $\log_\theta(q/p)$ and $\theta = 2p/(p-1)$.

14. We finally take q so large $(q \geqq p^2)$ that the inequality (B) is possible. The case $p = 2$ is not excluded. As before it is evident that it is more unfavor-

able to have H_{i+1} subject to (B) and H_{i+2} to (D) than for H_{i+1} to satisfy (D) and H_{i+2} to satisfy (B). Now compare (B) and (C) in relation to H_{i+1} and H_{i+2}. If the inequalities are applied in the order (B), (C), we have

$$N_{i+2} \leqq N_i + 2p(q-1) - n_i - pn_i, \qquad c_{i+2} \leqq c_i - 2 + q - n_i, \qquad n_{i+2} \geqq \theta p n_i;$$

and if in the order (C), (B):

$$N'_{i+2} \leqq N_i + 2p(q-1) - n_i - \theta n_i, \qquad c'_{i+2} \leqq c_i - 2 + q - \theta n_i, \qquad n'_{i+2} \geqq p\theta n_i.$$

If p is 2 or 3, $\theta = p$, and then obviously the first arrangement is the more unfavorable. When p is greater than 3 the matter is not so simple. However we can show that the addition of one new set of intransitivity by s_{i+1} is equivalent in the end to the introduction of q or more new letters. For one more set means one more group H in the chain $H_1, H_2, \cdots$ before arrival at a transitive group H_λ. This is evidently true if the extra group gives rise to a repetition of the inequalities (D). There only remains the question whether $pq - n_i - p$ can be less than q. Now (B) and (C) are not necessary unless $n_i \leqq (p-1)/2q$. From

$$pq - n_i - p < q,$$

we have

$$(p-1)q - p < n_i \leqq \frac{p-1}{2} q,$$

whence

$$q < \theta,$$

which is false under the present assumptions. Hence, while N'_{i+2} exceeds N_{i+2} by $(p-\theta)n_i$, if we multiply $(\theta - 1)n_i$, the difference between c_{i+2} and c'_{i+2}, by q, it is apparent that the first order is the more unfavorable.

We now form the successive inequalities in their most unfavorable order:

$$
\begin{array}{lll}
N_2 \leqq 2pq - p^2, & c_2 \leqq 1 + 2(q-p), & n_2 \geqq p^2, \\
N_3 \leqq N_2 + pq - n_2 - p, & c_3 \leqq c_2 + q - n_2 - 1, & n_3 \geqq p^3, \\
\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots \\
N_x \leqq N_{x-1} + pq - n_{x-1} - p, & c_x \leqq c_{x-1} + q - n_{x-1} - 1, & n_x \geqq p^x, \\
N_{x+1} \leqq N_x + pq - n_x - p, & c_{x+1} \leqq c_x - 1, & n_{x+1} \geqq p^x \theta, \\
\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots \\
N_{x+y} \leqq N_{x+y-1} + pq - n_{x+y-1} - p, & c_{x+y} \leqq c_{x+y-1} - 1, & n_{x+y} \geqq p^x \theta^y, \\
N_{x+y+1} \leqq N_{x+y} + q, & c_{x+y+1} \leqq c_{x+y} - 1, & \\
\cdots\cdots\cdots & \cdots\cdots\cdots & \\
N_\lambda \leqq N_{x+y} + (c_{x+y} - 1)q. & &
\end{array}
$$

From these inequalities we derive the following expression for the upper limit of the degree of H_λ, in which x and y remain to be determined:

$$N_\lambda \leqq \frac{p^2(q-p+2)}{p-1} + q^2x + (pq-q-p)(x+y-2) - \left(\frac{q+1}{p-1} - \frac{1}{\theta-1}\right)p^x - \frac{p^x\theta^y}{\theta-1}.$$

To cut short unprofitable refinements we now regard this expression, following Jordan's lead, as a continuous function of two independent variables x and y and equate to zero the partial derivatives

$$q^2 + pq - q - p - \left(\frac{q+1}{p-1} - \frac{1}{\theta-1}\right)p^x \log p - \frac{p^x\theta^y}{\theta-1}\log p = 0,$$

$$pq - q - p - \frac{p^x\theta^y}{\theta-1}\log\theta = 0.$$

We solve, substitute for N_λ, reduce, and have for the limit of the degree of the transitive subgroup H_λ

$$\frac{p^2(q-p+2)}{p-1} + (q-1)(q+p)\log_p\frac{ac}{e} + a\log_\theta\frac{c\theta^2\log\theta}{\theta-1},$$

in which

$$a = pq - q - p, \qquad b = \frac{q+1}{p-1} - \frac{1}{\theta-1}, \qquad abc = \frac{q^2+a}{\log p} - \frac{a}{\log\theta}.$$

15. When p is 2 or 3, the formula can be greatly simplified, for then $\theta = p$, and $y = 0$. For $p = 3$ it becomes

$$\tfrac{1}{2}(q+3) + (q+3)(q-1)\mu - \tfrac{1}{2}(q+1)3^\mu,$$

where μ is the integral part of $\log_3 3q$.

16. When $p = 2$ inequality (F) may be replaced by

$$(F') \qquad N_{i+1} \leqq N_i + q - 1,$$

whence

$$N_\lambda \leqq N_x + (c_x - 1)(q-1) \leqq 2(q+1) + (q^2-1)x - q\cdot 2^x.$$

If 2^{x-1} is less than q, the difference of N_λ with respect to x is

$$(q^2-1) - q2^{x-1}$$

and is positive. If 2^{x-1} is equal to q, this difference is negative, but the difference with respect to x of

$$2(q+1) + (q^2-1)(x-1) - q2^{x-1}$$

is positive. Hence when $p = 2$ $(q \geqq 4)$ the limit of the degree of a transitive subgroup H_λ of G is

$$2(q+1) + (q^2-1)\mu - q\cdot 2^\mu,$$

where μ is the largest whole number less than $\log_2 2q$.

17. A theorem was stated in the introduction which was proved in § 12 for p an odd prime. But if p is 2, we know from recent researches * on the class of primitive groups that the theorem is true except perhaps when the given substitution of order 2 has 6 cycles and the group in question is of class 12. But the limit of the preceding paragraph, obtained without any restriction on the class of the group, is 71, while the limit required for the theorem is 68. The inequalities of § 14 allow $H_3 (p = 2, q = 6)$ ten transitive constituents. A moment's consideration shows that, if the entire group is of class 12, H_3 cannot have so many constituents and that the limit of the degree of H_λ is 66.

URBANA, ILLINOIS,
December, 1909.

* C. JORDAN, Liouville's Journal, ser. 2, vol. 17 (1872), p. 363; NETTO, *Theory of Substitutions*, COLE'S translation (1892), p. 133; MILLER, American Mathematical Monthly, vol. 9 (1902), p. 63; MANNING, American Journal of Mathematics, vol. 32 (1910), pp. 235–257, and vol. 28 (1906), p. 226.