ON MULTIPLY TRANSITIVE GROUPS*

BY

W. A. MANNING

The properties of primitive groups that contain transitive subgroups of lower degree were first investigated by JORDAN.† In the *Traité des Substitutions* he proved that if a primitive group of degree n contains a circular substitution of prime degree (p) it is at least $n-p+1$ times transitive. The capital importance of this theorem led him to examine the general and much more difficult case, that in which the subgroup of lower degree is merely transitive. He obtained the remarkable theorem: ‡

"If a primitive group G of degree n contains a group Γ, the substitutions of which displace only p letters and permute them transitively (p being any integer), it is at least $n-p-2q+3$ times transitive, q being the greatest divisor of p such that we can arrange the letters of Γ in two different ways in systems of q letters which have the property that each substitution of Γ replaces the letters of each system by those of a single system. If none of the divisors of p have this property (which will happen notably if Γ is primitive, or formed of the powers of the same circular substitution) G is $n-p+1$ times transitive."

NETTO § and RUDIO ‖ later gave proofs for that special case in which Γ is primitive. The only other contribution to this theory was made by MARGGRAFF.¶ He proved that if q is the greatest divisor of p such that the letters of Γ may be arranged in systems of imprimitivity in at least *three* different ways, and if p is divisible by some number r such that Γ admits $r+1$ systems of imprimitivity with one letter in common and no two of which have more than one letter in common, G is at least $n-p-2q+3$ times transitive. If these two conditions are not fulfilled, G is $n-p+1$ times transitive. In MARGGRAFF's

* Presented to the Society (San Francisco), February 24, 1906. Received for publication June 19, 1906.

† C. JORDAN, *Traité des Substitutions*, 1870, p. 664.

‡ C. JORDAN, Journal de Mathématiques, ser. 2, vol. 16 (1871), pp. 383–408.

§ NETTO, Journal für Mathematik, vol. 83 (1877), pp. 43–56.

‖ RUDIO, Journal für Mathematik, vol. 102 (1888), pp. 1–9.

¶ 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.

second paper are given some interesting relations between n and p, for example, $p \geqq \frac{1}{2} n$.

The word "two" in JORDAN's theorem, and "three" in MARGGRAFF's may in all cases be replaced by "$q + 1$."

Let it be assumed that G is a doubly (and not triply) transitive group of degree $\sum_{x=1}^{r+1} q_x$ $(q_{r+1} = 1)$, in which are found transitive subgroups H^i $(i = 1, 2, \cdots, r)$ of degrees $\sum_{x=1}^{i} q_x$ respectively. It is also assumed that the degree of any transitive subgroup of G which displaces more than q_1 and less than $\sum_{x=1}^{r} q_x$ letters is one of the numbers $\sum_{x=1}^{i} q_x$ $(i = 2, 3, \cdots, r-1)$. This does not say that there is not a transitive subgroup of degree less than q_1. Let $a_{1,k}^i$ $(k = 1, 2, \cdots, q_i)$ be the letters displaced by H^i but not by H^{i-1}, and let Γ_1^i be the largest subgroup of G on the letters of H^i; Γ_1^i includes all the preceding subgroups and is transitive.

If $q_r = 1$, G is triply transitive contrary to hypothesis: hence $q_r > 1$. If for those values of i corresponding to which $q_i > 1$, the letters $a_{1,k}^i$ $(k = 1, 2, \cdots, q_i)$ do not form a system of imprimitivity in Γ_1^i, some substitution S of Γ_1^i will give a group $S^{-1} \Gamma_1^{i-1} S$ displacing some of the letters $a_{1,k}^i$ $(k = 1, 2, \cdots, q_i)$ and leaving fixed at least one of them. Then $\{ \Gamma_1^{i-1}, S^{-1} \Gamma_1^{i-1} S \}$ is a transitive group of degree greater than $\sum_{x=1}^{i-1} q_x$ and less than $\sum_{x=1}^{i} q_x$, contrary to hypothesis. By the definition of imprimitivity all the subgroups of Γ_1^i, notably $\Gamma_1^1, \Gamma_1^2, \cdots, \Gamma_1^{i-1}$, admit these systems. It should also be remarked that the letters $a_{1,k}^x$ $(k = 1, 2, \cdots, q_x)$ fall into sets of imprimitivity q_i by q_i, for $x = 1, 2, \cdots, i-1$. Since $q_r > 1$, then $q_i > 1$ $(i = 1, 2, \cdots, r-1)$.

Let $a_{2,1}^r$ represent the system $a_{1,k}^r$ $(k = 1, 2, \cdots, q_r)$ of Γ_1^r, and let $a_{2,k}^i$ $(i = 1, 2, \cdots, r-1;\ k = 1, 2, \cdots, q_i/q_r)$ be the remaining systems into which $a_{2,1}^r$ goes under the substitutions of Γ_1^r. We define Γ_2^i as the group in the systems $a_{2,k}^x$ $(x = 1, 2, \cdots, i;\ k = 1, 2, \cdots, q_x/q_r)$ of Γ_1^i. Obviously Γ_2^r is at least doubly transitive.

The group G, being doubly transitive, contains a substitution $T_{i_1} = (a_{1,1}^{r+1} a_{1,i_1}^r) \cdots$. Let it be granted for the moment that T_{i_1} transforms $\Gamma_1^{i+1}, \Gamma_1^{i+2}, \cdots, \Gamma_1^{r-1}$ each into itself and leaves fixed the letters $a_{1,1}^{i+1}, a_{1,1}^{i+2}, \cdots, a_{1,1}^{r-1}$. Then $\{ T_{i_1}^{-1} \Gamma_1^i T_{i_1}, \Gamma_1^i \} = \Gamma_1^i$; for, its degree is less than $\sum_{x=1}^{i+1} q_x$ and must consequently be $\sum_{x=1}^{i} q_x$, that of Γ_1^i. If T_{i_1} displaces $a_{1,1}^i$ there is a substitution S in Γ_1^i which replaces $a_{1,1}^i$ by the same letter as does T_{i_1}. Then $S^{-1} T_{i_1}$ leaves fixed $a_{1,1}^i$ as well as $a_{1,1}^{i-1}, \cdots, a_{1,1}^r$ and may be used for T_{i_1}. But it is clear that $T_{i_1} = (a_{1,1}^{r+1} a_{1,i_1}^r) \cdots$ transforms Γ_1^{r-1} into itself, and by multiplication by a substitution of Γ_1^{r-1} a like substitution may be obtained which leaves $a_{1,1}^{r-1}$ fixed. Then by a complete induction G contains a substitution

$$T_{i_1} = (a_{1,1}^1)(a_{1,1}^2) \cdots (a_{1,1}^{r-1})(a_{1,1}^{r+1} a_{1,i_1}^r) \cdots$$

for $i_1 = 1, 2, \cdots, q_r$, which transforms each group $\Gamma_1^1, \Gamma_1^2, \cdots, \Gamma_1^{r-1}$ into itself.

Each system of letters $a^i_{1,k}$ $(k = 1, 2, \cdots, q_i)$ is transformed into itself. The symbol $a^{r-1}_{3,1}$ will be introduced later for the system $a^{r-1}_{1,k}$ $(k = 1, 2, \cdots, q_{r-1})$, and other properties of T_{i_1} pointed out.

Now $T^{-1}_{i_1}\Gamma^{r-1}_1 T_{i_1} = \Gamma^{r-1}_1$ $(i_1 = 1, 2, \cdots, q_r)$, but the system $a^{r-1}_{2,1}$ is replaced by q_r other systems which have at least the letter $a^{r-1}_{1,1}$ in common with $a^{r-1}_{2,1}$. Let these q_r new systems of imprimitivity of Γ^{r-1}_1 be represented by $a^{r-1}_{2,1,i_1}$. If it is assumed that $a^{r-1}_{2,1,i_1}$ has a second letter $a^{r-1}_{1,2}$ in common with $a^{r-1}_{2,1}$, T_{i_1} has the sequence $a^{r-1}_{1,k}a^{r-1}_{1,2}$, where $a^{r-1}_{1,k}$ is some letter of the system $a^{r-1}_{2,1}$. In Γ^r_2 there is a substitution $S = (a^{r-1}_{2,1}a^r_{2,1})\cdots$. Now $U = S^{-1}T_{i_1}S$ leaves fixed the letter of $a^{r-1}_{2,1}$ which follows $a^{r-1}_{1,1}$ in S, replaces the letter which follows $a^{r-1}_{1,k}$ in S by the one which follows $a^{r-1}_{1,2}$, and certainly replaces a letter of $a^{r-1}_{2,1}$ by $a^{r+1}_{1,1}$. Hence one sees that the degree of $\{U^{-1}\Gamma^{r-1}_1 U, \Gamma^{r-1}_1\}$ is greater than $\sum^{r-1}_{x=1} q_x$ and less than $\sum^r_{x=1} q_x$, contrary to hypothesis. *The q_r systems $a^{r-1}_{2,1,i_1}$ have one and only one letter in common with $a^{r-1}_{2,1}$.*

Suppose it possible to find in G a substitution T that transforms Γ^{r-1}_1 into itself, and which replaces the system $a^{r-1}_{2,1,i_1}$ by a system α' distinct from any system resulting from the $q_r + 1$ arrangements obtained above. If α' does not include the letter $a^{r-1}_{1,1}$, some substitution S'' of Γ^{r-1}_1 will replace α' by a system α which does include $a^{r-1}_{1,1}$. Now $T_{i_1}TS''$ replaces the system $a^{r-1}_{2,1}$ by α and the letter $a^{r-1}_{1,1}$ by $a^{r-1}_{1,k}$ say. We take from Γ^{r-1}_1 a substitution S' which replaces $a^{r-1}_{1,k}$ by $a^{r-1}_{1,1}$, and in consequence leaves α fixed; the product $U = T_{i_1}TS''S'$ leaves $a^{r-1}_{1,1}$ fixed and replaces $a^{r-1}_{2,1}$ by α, so that $U = (a^{r-1}_{1,1})(a^{r+1}_{1,1}a^r_{1,k}\cdots)\cdots$. Now $UT^{-1}_k = (a^{r-1}_{1,1})(a^{r+1}_{1,1})\cdots = S$, a substitution of Γ^r_1, and therefore $U = ST_k$, $k \leqq q_r$. Hence α, the result of transforming Γ^{r-1}_1 first by S and then by T_k, is merely one of the systems $a^{r-1}_{2,1,i_1}$.

The system $a^{r-1}_{2,1,i_1}$ bears the same relation to Γ^{r-1}_1, $T^{-1}_{i_1}\Gamma^r_1 T_{i_1}$, and G, that $a^{r-1}_{2,1}$ does to Γ^{r-1}_1, Γ^r_1, and G. From $a^{r-1}_{2,1,i_1}$ then can be obtained, by means of substitutions that leave $a^{r-1}_{1,1}$ fixed and Γ^{r-1}_1 invariant, q_r other systems with but one letter in common with $a^{r-1}_{2,1}$. But we have just seen that these q_r systems will coincide with systems already obtained. Hence *the letters of Γ^{r-1}_1 may be arranged in systems of imprimitivity of q_r letters each in at least $q_r + 1$ ways with one letter common to the $q_r + 1$ systems and with no other letter common to any two of them.* This theorem holds *à fortiori* for all transitive subgroups of Γ^{r-1}_1, in particular for H^1. It was first proved by MARGGRAFF, loc. cit.

Since T_{i_1} permutes the letters $a^{r-1}_{1,k}$ $(k = 1, 2, \cdots, q_{r-1})$ among themselves, *the letters (q^2_r in number) involved in the systems $a^{r-1}_{2,1}$, $a^{r-1}_{2,1,1}$, $a^{r-1}_{2,1,2}$, $\cdots$, $a^{r-1}_{2,1,q_r}$, are all found in the larger system $a^{r-1}_{1,k}$ above. Hence we have the important relation $q_{r-1} \geqq q^2_r$.*

It will now be shown that Γ^r_2 is not in general triply transitive. An exception arises only when $r = 2$. Suppose Γ^r_2 triply transitive. To each of the $q_r + 1$ distinct arrangements of the letters of Γ^{r-1}_1 in systems of imprimitivity of

q_r letters each, corresponds a doubly transitive group according to which systems are permuted.* Let $\Gamma_1^{r-1}(a_{1,1}^{r-1})$ be the subgroup of Γ_1^{r-1} that leaves fixed the letter $a_{1,1}^{r-1}$. The remaining $q_r - 1$ letters of each system of imprimitivity to which $a_{1,1}^{r-1}$ belongs may be permuted only among themselves by the substitutions of $\Gamma_1^{r-1}(a_{1,1}^{r-1})$. Now $\Gamma_2^{r-1}(a_{2,1}^{r-1})$ is transitive of degree $(1/q_r)\sum_{x=1}^{r-1} q_x - 1$, while the number of systems transitively connected by it cannot exceed $q_r - 1$. Hence $\sum_{x=1}^{r-1} q_x \leqq q_r^2$, and (since $q_{r-1} \geqq q_r^2$), $q_{r-1} = q_r^2$ and $r = 2$, unless Γ_1^{r-1} is a regular group, in which case also $r = 2$. It will be shown later that an imprimitive group of degree q^2 in which $q + 1$ systems of q letters each with one letter in common, and such that no two of these systems have more than one letter in common, is either regular or of class $q^2 - 1$. However, the proof of the theorem we are going to establish is already complete for $r = 2$, whether Γ_2^r is triply transitive or not. In completing the proof we assume then that $r > 2$, so that Γ_2^r *is doubly but not triply transitive.* It is such a group as G itself and to it may be applied all preceding results for G.

Is it possible for Γ_2^r to have a transitive subgroup of degree greater than q_1/q_r and not equal to one of the numbers $(1/q_r)\sum_{x=1}^{i} q_x\,(i = 2, 3, \cdots, r)$? Let, if possible, $\Gamma_2^{i,k}$ be a transitive subgroup of Γ_2^{i+1} which displaces besides the letters of Γ_2^i the k letters $a_{2,1}^{i+1}, a_{2,2}^{i+1}, \cdots, a_{2,k}^{i+1}\,(1 \leqq k < q_{i+1}/q_r)$. Then between Γ_1^i and Γ_1^{i+1} there is a corresponding subgroup $\Gamma_1^{i,k}$, which includes Γ_1^i and is transitive in the systems $a_{2,1}^1, \cdots$, so that $\Gamma_1^{i,k}$ certainly has a transitive constituent of degree $\sum_{x=1}^{i} q_x + kq_r$. Now transform Γ_1^i by all the substitutions of $\Gamma_1^{i,k}$. If the group generated by Γ_1^i and all these transforms is not transitive of degree $\sum_{x=1}^{i} q_x + kq_r$, it is because $kq_r \geqq \sum_{x=i}^{i} q_x$, an absurdity since $kq_r < q_{i+1}$, $q_{i+1} \leqq q_i$, that is, $kq_r < q_i$. This holds for $i = 1, 2, \cdots, r-2$. Nothing is said about possible transitive subgroups of various degrees in Γ_2^1.

We may now form the doubly transitive group in the systems of Γ_2^{r-1}. The system $a_{2,k}^{r-1}$ $(k = 1, 2, \cdots, q_{r-1}/q_r)$ will be represented by $a_{3,1}^{r-1}$. The large system $a_{2,k}^i$ $(k = 1, 2, \cdots, q_i/q_r)$ breaks up into the smaller systems $a_{3,k}^i$ $(k = 1, 2, \cdots, q_i/q_{r-1})$. This group on the letters $a_{3,k}^i$ $(i = 1, 2, \cdots, r-1)$ will be indicated by Γ_3^{r-1}, and the subgroup of it which corresponds to Γ_2^i is Γ_3^i. In the same way we proceed to form the successive groups Γ_j^i in the sys-

*Cf. C. JORDAN, Journal de Mathématiques, ser. 2, vol. 16 (1871), third paragraph of article 7 on page 388. From the fact that "I" is doubly transitive with respect to the systems of q letters $s, s_1, \cdots$ which it contains, it does not follow that if its letters can be grouped in different ways in systems of imprimitivity, each of the new systems will be contained completely within one of the systems $s, s_1, \cdots$. For example it is not true in the regular non-cyclic group of order 6. In it systems of two letters each are permuted according to a doubly transitive group, while there are three distinct ways of arranging the letters of the group in systems of imprimitivity of two letters each. But the argument is valid if use is made of the fact that "I" contains substitutions leaving fixed at least two letters. To see how the subgroup "H" of "I" should be brought in to complete the proof, see MARGGRAFF, l. c., theorem X (1889), p. 20, and (1895), p. 16.

tems $a^i_{j,k}$ ($k = 1, 2, \cdots, q_i/q_{r-j+2}$; $i, j = 1, 2, \cdots, r$, provided $i + j \leqq r + 2$; and $q_{r+1} = 1$). The groups Γ^i_j for which $i + j = r + 2$ are all doubly and not triply transitive except perhaps Γ^2_r. *From* Γ^{i+1}_{r-i+1} *we have*

$$\frac{q_{i-1}}{q_{i+1}} \geqq \left(\frac{q_i}{q_{i+1}}\right)^2, \quad \text{or} \quad q_{i-1} \geqq \frac{q_i^2}{q_{i+1}} \qquad (i=2, 3, \cdots, r),$$

so that

$$q_i \geqq q_{i+1} \sqrt[r-i]{q_{i+1}}, \quad \text{or} \quad q_i \geqq q_r^{r-i+1}, \quad \text{or} \quad q_i \leqq q_1^{(r-i+1)/r}.$$

The operator $T_{i_1} = (a^{r+1}_{1,1} a^r_{1,i_1}) \cdots$, we have seen, leaves fixed the letters $a^1_{1,1}$, $a^2_{1,1}, \cdots, a^{r-1}_{1,1}$, and the systems $a^{r-1}_{3,1}, a^{r-2}_{4,1}, a^{r-3}_{5,1}, \cdots, a^2_{r,1}, a^1_{r+1,1}$. Since T_{i_1} leaves fixed the system $a^{r-j+2}_{j,1}$ of Γ^{r-j+2}_j ($j = 3, 4, \cdots, r$), it permutes the systems $a^i_{j,k}$ ($k = 1, 2, \cdots, q_i/q_{r-j+2}$; $i = 1, 2, \cdots, r - j + 2$) among themselves, without a change to an arrangement essentially distinct. Then T_{i_1} leaves fixed all the systems $a^i_{j,1}$ ($j = 1, 2, \cdots, r + 1$; $i = 1, 2, \cdots, r - 1$, provided $i + j \leqq r + 2$, and, when $j = 2$, $i \neq r - 1$). In exactly the same way we get a substitution $T_{i_j} = (a^{r-j+2}_{j,1} a^{r-j+1}_{j,i_j}) \cdots$ which leaves fixed all those elements which bear to Γ^{r-j+2}_j the same relation as the elements left fixed by T_{i_1} bear to G. If we consider the group Γ^x_y it is clear that a substitution S can always be found in it that replaces a certain letter $a^x_{y,z}$ by $a^x_{y,1}$ and that has the property of leaving fixed each of the letters $a^1_{y,1}, a^2_{y,1}, a^{x-1}_{y,1}$, and hence also the systems $a^1_{y+1,1}, a^2_{y+1,1}, \cdots, a^{r-1}_{y+1,1}, a^1_{y+2,1}, \cdots$. With the aid of such substitutions we may choose T_{i_j} so that it leaves fixed all the elements $a^i_{y,1}$ ($y = 1, 2, \cdots, r + 1$; $i = 1, 2, \cdots, r - j$, provided $y + i \leqq r + 2$, and $i \neq r - j$ when $y = j$). It is clear that T_{i_j} transforms Γ^i_1 ($i = 1, 2, \cdots, r - j$) and Γ^{r-j+2}_1 each into itself. We should bear in mind that T_{i_j} may also be regarded as a substitution of Γ^{r-j+2}_1 and leaves fixed all the letters $a^i_{1,k}$ ($k = 1, 2, \cdots, q_i$; $i = r - j + 3, \cdots, r + 1$).

The following theorem will now be proved by a complete induction:

The letters of Γ^{i-1}_1 *may be grouped* q_i *by* q_i *in systems of imprimitivity which have an arbitrary letter* $a^{i-1}_{1,1}$ *in common in at least* $q_i \sum_{x=i}^{r+1} 1/q_x$ *distinct ways. Furthermore,* (1) *Any two of these systems have exactly* q_{i+1} *letters in common.* (2) *The letters involved in these systems are all included in the larger system* $a^{i-1}_{r-i+3,1}$. (3) *No substitution of* G *which leaves* Γ^{i-1}_1 *invariant can replace one of these systems by a system of imprimitivity not included among those into which one of them goes by a substitution of* Γ^{i-1}_1 *itself.* (4) *Those systems which have* $a^{i-1}_{2,1}$ *in common preserve the original systems* $a^i_{2,k}$. (5) *The* q_i *systems of* q_i *letters which have* $a^{i-1}_{1,1}$ *but not* $a^{i-1}_{2,1}$ *in common contain no letter of the system* $a^{i-1}_{2,1}$ *except* $a^{i-1}_{1,1}$.

We assume the truth of the above theorem for the subgroup Γ^i_1 and its systems of q_{i+1} letters, and shall show that it must then hold as stated for Γ^{i-1}_1. Now if it holds for Γ^i_1 it holds also for Γ^{i-1}_2. Hence systems of q_i/q_r letters with $a_{2,1}^{i-1}$ in common may be chosen in $q_i\sum_{x=i}^{r}1/q_x$ distinct ways, $q_i\sum_{x=i}^{r-1}1/q_x$ of which have the system $a_{3,1}^{i-1}$ in common. Now transform Γ_1^{i-1} by T_{i_1} $(i_1=1, 2, \cdots, q_r)$. Since T_{i_1} does not replace the systems $a_{3,k}^{i}$ of Γ_2^{i-1} by other systems essentially distinct, the $q_i\sum_{x=i}^{r-1}1/q_x$ systems with $a_{3,1}^{i-1}$ in common undergo no change. But since T_{i_1} leaves fixed $a_{3,1}^{i-1}$ and may replace letters of $a_{2,1}^{i-1}$ only by letters of $a_{3,1}^{i-1}$, and since $a_{1,1}^{i-1}$ is the only letter of $a_{3,1}^{i-1}$ in the remaining q_i/q_r systems, no two of the block of $(q_i/q_r)(1+q_r)$ systems obtained by this transformation are the same. Since T_{i_1} leaves fixed the system $a_{r-i+2,1}^{i-1}$ (the system of q_i letters from which we start), each system of the total number, $q_i\sum_{x=i}^{r-1}1/q_x+q_i(1+q_r)/q_r=q_i\sum_{x=i}^{r+1}1/q_x$, has just q_{i+1} letters in common with $a_{r-i+2,1}^{i-1}$. Obviously all the letters of all these systems are included in $a_{r-i+3,1}^{i-1}$. The next point to establish is that no substitution of G under which Γ_1^{i-1} is invariant can replace any of the $q_i\sum_{x=i}^{r+1}1/q_x$ systems with $a_{1,1}^{i-1}$ in common (the system a say) by a system (α'') not found among the $\sum_{x=1}^{i-1}q_x\cdot\sum_{x=i}^{r+1}1/q_x$ systems of Γ_1^{i-1} resulting from the above systems which have $a_{1,1}^{i-1}$ in common, after transformation by all the substitutions of Γ_1^{i-1}. By hypothesis all substitutions of Γ_2^{r} under which Γ_2^{i-1} is invariant give rise to no new systems. Let T be a substitution of G which replaces the system a by α'', and let $T^{-1}\Gamma_1^{i-1}T=\Gamma_1^{i-1}$. Let T_{i_1} be that substitution (defined as before) which replaces one of the systems of q_i letters which include $a_{2,1}^{i-1}$, by a. Since $T_{i_1}T$ cannot be a substitution of Γ_2^{r}, it must replace $a_{1,1}^{r+1}$ by some letter $a_{1,k}^{i}$ $(i<r+1)$, The group $\{T_{i_2}, T_{i_3}, \cdots, T_{i_{r-i+1}}\}$ leaves Γ_1^{i-1} invariant, $a_{1,1}^{i-1}$ and $a_{2,1}^{i-1}$ fixed, and has a constituent which is transitive in the letters $a_{1,k}^{x}$ $(k=1, 2, \cdots, q_i;$ $x=i, i+1, \cdots, r)$, so that from it we may take a substitution S''' which replaces the letter $a_{1,k}^{i}$ that follows $a_{1,1}^{r+1}$ in $T_{i_1}T$ by a letter $a_{1,i_1'}^{r}$. Now $T_{i_1}TS'''$ replaces $a_{1,1}^{r+1}$ by $a_{1,i_1'}^{r}$; let α' be the system into which S''' changes α''. Since S''' is a substitution of Γ_1^{r}, α' satisfies the condition imposed on α''. Let S'' be a substitution of Γ_1^{i-1} that replaces the system α' by another (α) which includes the letter $a_{1,1}^{i-1}$. Finally let S' be a substitution of Γ_1^{i-1} the inverse of which replaces $a_{1,1}^{i-1}$ by the same letter as does $T_{i_1}TS'''S''$; S' leaves fixed the system α. Then $U=T_{i_1}TS'''S''S'$ leaves Γ_1^{i-1} invariant, $a_{1,1}^{i-1}$ fixed, replaces $a_{1,1}^{r+1}$ by $a_{1,i_1'}^{r}$, and changes one of the systems which have $a_{2,1}^{i-1}$ in common directly into α. Now $UT_{i_1'}^{-1}=(a_{1,1}^{i-1})(a_{1,1}^{r+1})\cdots=S$, a substitution of Γ_2^{r}, which leaves the element $a_{2,1}^{i-1}$ fixed since $a_{1,1}^{i-1}$, one of the letters of $a_{2,1}^{i-1}$, is fixed. From $U=ST_{i_1'}$ it is clear that α must be one of the set of systems obtained from those of Γ_2^{i-1} by means of T_{i_1}.

To prove that any two of the $q_i\sum_{x=i}^{r+1}1/q_x$ systems with one letter in common have q_{i+1} and only q_{i+1} in common, we have only to note that the series of transitive subgroups Γ_1^{x} $(x=i, i+1, \cdots, r)$ may be so chosen that any one of the systems involving the letter $a_{1,1}^{i-1}$ may be made to take the place of $a_{r-i+2,1}^{i-1}$. In fact $\{T_{i_1}, T_{i_2}, \cdots, T_{i_{r-i+1}}\}$ contains a substitution T which replaces any one of the $q_i \sum_{x=i}^{r+1} 1/q_x$ systems which include $a_{1,1}^{i-1}$ by any other and permutes them only among themselves. Such a series of subgroups is $\Gamma_1^1, \Gamma_1^2, \cdots, \Gamma_1^{i-1}$, $T^{-1}\Gamma_1^i T, \cdots, T^{-1}\Gamma_1^r T$, G, and in it an arbitrary system plays the part of $a_{r-i+2,1}^{i-1}$.

It remains to be shown that the q_i systems which have $a_{1,1}^{i-1}$ but not $a_{2,1}^{i-1}$ in common contain no letter of the system $a_{2,1}^{i-1}$ except $a_{1,1}^{i-1}$. These q_i systems are those by which the q_i/q_r systems in the letters of Γ_2^{i-1}, which do not have $a_{3,1}^{i-1}$ in common, are replaced by $T_{i_1}(i_1 = 1, 2, \cdots, q_r)$. By hypothesis these q_i/q_r systems contain no letter of the system $a_{3,1}^{i-1}$, except $a_{2,1}^{i-1}$, and T_{i_1} permutes the letters $a_{1,1}^{i-1}, \cdots$, of $a_{3,1}^{i-1}$, among themselves, giving in place of the system $a_{2,1}^{i-1}$, q_r systems which have no letter in common with it except $a_{1,1}^{i-1}$. Hence none of these $(q_i/q_r)q_r = q_i$ systems have, besides $a_{1,1}^{i-1}$ any letter in common with $a_{2,1}^{i-1}$.

This theorem has been proved for the systems of q_r letters in Γ_1^{r-1}, and in consequence holds for the systems of q_{r-1} letters in Γ_1^{r-2}, and so on. In regard to H^1 we may now say that *systems of imprimitivity of q_i letters may be chosen in $q_i \sum_{x=i}^{r+1} 1/q_x$ distinct ways, for $i = 2, 3, \cdots, r-1, r$.*

If G is contained in a larger primitive group G' of degree n, G' is $n - \sum_{x=1}^{r} q_x + 1$ times transitive. Now

$$\sum_1^r q_x \leqq q_1\left(1 + \tfrac{1}{2} + \tfrac{1}{4} + \cdots + \frac{1}{2^{r-1}}\right) \leqq 2q_1\left(1 - \frac{1}{2^r}\right) \leqq 2q_1\left(1 - \frac{1}{q_1}\right).$$

Hence the theorem:

A primitive group of degree n which contains a transitive subgroup of degree q_1 is at least $n - 2q_1 + 3$ times transitive.

We may give another incomplete but useful statement of our theorem:

If a primitive group G of degree n contains a transitive subgroup H of degree q_1, G is at least $n - q_1 - q_r(q_2 - 1)/(q_r - 1) + 1$ times transitive, q_2 being the greatest divisor of q_1 such that H has at least $q_2 + 1$ distinct arrangements of its letters in systems of imprimitivity of q_2 each, and q_r being the least divisor of q_1 such that H has at least $q_r + 1$ systems of q_r letters each with one letter in common, and not more than the one letter common to any two of them.

If both these conditions are not satisfied by the given group H, G is at least $n - q_1 + 1$ times transitive.

From $q_{i-1} \geqq q_i^2/q_{i+1}$, it follows that $q_r^{r-i+1} \leqq q_i \leqq q_2^{(r-i+1)(r-1)}$. Then

$$q_3 + q_4 + \cdots + q_r \leqq q_2^{\frac{r-2}{r-1}} + q_2^{\frac{r-3}{r-1}} + \cdots + q_2^{\frac{1}{r-1}} \leqq \frac{q_2 - 1}{q_2^{1/(r-1)} - 1} - 1 \leqq \frac{q_2 - 1}{q_r - 1} - 1.$$

Hence G, which is $n - \sum_{x=1}^{r+1} q_x$ times transitive, is at least

$$n - q_1 - q_2 - \frac{q_2 - 1}{q_r - 1} + 2 = n - q_1 - q_r\frac{q_2 - 1}{q_r - 1} + 1$$

times transitive.

This limit is attained by the holomorph of the Abelian group of degree 2^a and type $(1, 1, \cdots)$, which is triply transitive and has a transitive subgroup of degree 2^{a-1}, for which $q_2 = 2^{a-2}$ and $q_r = 2$.

Other useful conditions which Γ_1^{i-1} must satisfy may be obtained by considering the meaning of the multiple imprimitivity it exhibits.

Let J be an imprimitive group of degree n and order nm; let $a_1, a_2, \cdots, a_q$ be the letters of a certain system of imprimitivity of J. The substitutions, qm in number, that replace a_1 by $a_1, a_2, \cdots, a_q$ respectively, leave the system $a_1, \cdots, a_q$ fixed. The product of any two of them also has this property. No other substitution of J permutes the letters $a_1, \cdots, a_q$ among themselves. Then these qm substitutions form a group (H). Let there be another system of q letters in J which has the letters $a_1, a_2, \cdots, a_\alpha$ in common with the first, and the remaining letters $a'_{\alpha+1}, a'_{\alpha+2}, \cdots, a'_q$ distinct. The group H' which corresponds to this system has exactly $q\alpha$ substitutions in common with H: those which replace a_1 by $a_1, a_2, \cdots, a_\alpha$. These αm common substitutions form by themselves a group (F).

Now if a substitution T transforms J into itself, permutes the letters $a_2, a_3, \cdots, a_\alpha$ among themselves, leaves a_1 fixed, and replaces $a_{\alpha+1}, \cdots, a_q$ by $a'_{\alpha+1}, \cdots, a'_q$, it transforms F into itself and H into H'. We conclude that *Γ_1^{i-1} has a set of $q_i \sum_{x=i}^{r+1} 1/q_x$ subgroups of order $q_i m_{i-1}$ which have in common the subgroup (of order m_{i-1}) of Γ_1^{i-1} that leaves one letter fixed. Any two of these subgroups have in common also a subgroup of order $q_{i+1} m_{i-1}$.* This set of $q_i \sum_{x=i}^{r+1} 1/q_x$ subgroups of order $q_i m_{i-1}$ must be such that some isomorphism of Γ_1^{i-1} to itself brings any two we please into a $1, 1$ correspondence. In particular, no one of them can be a characteristic subgroup of Γ_1^{i-1}. If one is invariant in Γ_1^{i-1}, all are invariant.

We recall that Γ_1^{r-1} admits $q_r + 1$ arrangements of its letters in systems of imprimitivity of q_r each such that $q_r + 1$ systems may be taken with one common letter and no two of which have more than this one letter in common. If $a_{1,1}^{r-1}$ be taken as the leading letter, the $q_r^2 - 1$ letters thus associated with it are all found in the larger system $a_{3,1}^{r-1}$. It may happen, as when $q_{r-1} = q_r^2$, that the q_r^2 letters in question form a system (A) of imprimitivity of Γ_1^{r-1}. The subgroup Δ' which leaves this system A fixed has a transitive constituent on the q_r^2 letters of A. We call this constituent group Δ and suppose all the other letters of Δ' erased. Now Δ has the properties of Γ_1^{r-1} in so far as systems of imprimitivity are concerned — even more extensive properties perhaps. Consider a substitution S of Δ which leaves fixed two letters $a_{1,1}^{r-1}$ and $a_{1,k}^{r-1}$. Let $S = (a_{1,\rho}^{r-1} a_{1,\sigma}^{r-1} \cdots) \cdots$. Since S can only permute among themselves the letters of each of the systems to which $a_{1,1}^{r-1}$ belongs—and similarly for $a_{1,k}^{k-1}$—the letters $a_{1,\rho}^{r-1}$ and $a_{1,\sigma}^{r-1}$ belong to that system which contains both $a_{1,1}^{r-1}$ and $a_{1,k}^{r-1}$. Then S displaces at most most $q_r - 2$ letters, from which it readily follows that S is the identity. We conclude that when Δ is not regular, it is of class $q_r^2 - 1$ and has a characteristic transitive subgroup (Θ) which is regular.* This regular subgroup of order q_r^2 occurs in both cases, and Δ, when regular, may be called Θ for the sake of uniformity. This group Θ admits a $(q_r + 1)$ fold division into systems of imprimitivity, no two systems having more than one letter in common, hence its substitutions are distributed among $q_r + 1$ subgroups of order q_r, no two of which have an operator in common other than the identity.

Let $s_1 = 1,\ s_2,\ \cdots,\ s_{q_r}$ be the substitutions of one of these subgroups, one of whose substitutions is conjugate to some substitution t_j not in it. Let $t_1 = 1,\ t_2,\ \cdots,\ t_j,\ \cdots,\ t_{q_r}$ be that one of the $q_r + 1$ subgroups in question which includes t_j. Now every substitution of the group Θ is given by $s_\alpha t_\beta\,(\alpha,\ \beta = 1,\ 2,\ \cdots,\ q_r)$. But clearly $t_\beta^{-1} s_\alpha^{-1} s_i s_\alpha t_\beta \neq t_j$. Then each of the $q_r + 1$ subgroups is invariant, and since no two have anything in common but the identity, every substitution of one of these subgroups is commutative with all the substitutions not in it. Then the group Θ is Abelian. Let $q_r = mp^\alpha$, where, if possible, m is prime to p (p being a prime number). The Sylow subgroup of Θ of order $p^{2\alpha}$ must have $mp^\alpha + 1$ subgroups of order p^α with nothing in common but the identity. Then

$$1 + (mp^\alpha + 1)(p^\alpha - 1) = p^{2\alpha},$$

so that $m = 1$. If now we take the two subgroups of order $q_r = p^\alpha$ in which the subgroups composed of the operators of order p are of the lowest possible orders p^{k_1} and p^{k_2}, $k_1 \geqq k_2$, we get the inequality $p^{k_1 + k_2 - \alpha} \geqq p^{k_1}$, whence $k_1 = k_2 = \alpha$. Then Θ is of type $(1, 1, \cdots)$.† The elementary group of order 16 has 5 subgroups of order 4, no two of which have anything but the identity in common. It is found in the quintuply transitive group of degree 24 of MATHIEU.‡

Another assumption we may make in regard to Γ_1^{r-1} is that there is in it an imprimitive system of $q_r^2 + q_r$ letters including $a_{1,1}^{r-1}$ and the $q_r^2 - 1$ letters associated with $a_{1,1}^{r-1}$ in imprimitive systems of q_r letters each. Just as in the preceding case there is a subgroup Δ' that has a transitive constituent Δ of degree $q_r^2 + q_r$, which we now investigate.

Let S be a substitution of Δ that leaves fixed two letters $a_{1,1}^{r-1}$ and $a_{1,k}^{r-1}$. By

* FROBENIUS, Berliner Sitzungsberichte, 1901, pp. 1216–1230, and 1902, pp. 455–459.

† Cf. MILLER, Bulletin of the American Mathematical Society, vol. 12 (1906), pp. 446–449. This is the proof Professor MILLER mentions in the note at the bottom of page 449.

‡ MATHIEU, Journal de Mathématiques, ser. 2, vol. 18 (1873), pp. 25–46.

MILLER, Bulletin de la Société mathématique de France, vol. 28 (1900), pp. 266–267.

the method used above we know that the only letters which S can displace are the $q_r - 2$ other letters of a system which includes both $a_{1,1}^{r-1}$ and $a_{1,k}^{r-1}$, the q_r letters not in a system with $a_{1,1}^{r-1}$ and the q_r not in a system with $a_{1,k}^{r-1}$, $3q_r - 2$ at most. But if $S = (a_{1,\rho}^{r-1} a_{1,\sigma}^{r-1} \cdots) \cdots$, it must replace every system of q_r letters in which $a_{1,\rho}^{r-1}$ is found by a system in which $a_{1,\sigma}^{r-1}$ is present. Then S displaces at least $q_r^2 - q_r + 2$ letters. Now $q_r^2 - q_r + 2 > 3q_r - 2$ when $q_r > 2$. It is obvious that when $q_r = 2$, Δ is regular. Then for all values of q_r, Δ is either regular or of class $q_r^2 + q_r - 1$. In the latter case Δ contains a regular characteristic subgroup. Then the regular subgroup Θ of order $q_r^2 + q_r$ is always found in the constituent Δ of Δ'. Let $\Lambda_1, \Lambda_2, \cdots, \Lambda_{q_r+1}$ be the subgroups with nothing in common but the identity which correspond to the $q_r + 1$ systems of imprimitivity of q_r letters each in question. In Θ systems of q_r letters each are permuted according to a transitive group of degree $q_r + 1$. All the substitutions which lie in the subgroups $\Lambda_1, \cdots$ leave fixed at least one of these systems of imprimitivity. This is seen by applying to Θ all the substitutions of its conjoin.* Then Θ has just q_r substitutions which displace all $q_r + 1$ systems. The group of degree $q_r + 1$ in the systems is of class q_r. For it is a characteristic property of groups of "class $n - 1$" that they have just $n - 1$ substitutions of degree n.† Hence Θ has a characteristic subgroup Π which leaves fixed none of the $(q_r + 1)^2$ possible systems. It is clear that $\Lambda_1, \cdots$ are conjugate under Π. Consequently the group in the systems is of order $(q_r + 1)q_r$ and doubly transitive. Hence Π is Abelian of type $(1, 1, \cdots)$.‡ If $q_{r-1} = q_r(q_r + 1)$, we have $q_{r-1} + q_r + 1 = p^{2a}$. The doubly transitive group of order 432, degree 9 and class 6 is a case in point. The transitive subgroup of degree 6 in it is non-cyclic.

STANFORD UNIVERSITY.

* JORDAN, *Traité des Substitutions*, 1870, p. 80.

† BURNSIDE, Proceedings of the London Mathematical Society, vol. 32 (1900), pp. 240-246.

‡ JORDAN, Journal de Mathématiques, ser. 2, vol. 17 (1872), pp. 351-367; FROBENIUS, l. c.