On Transitive Groups of degree n and class n—1. *By* W. BURNSIDE. Received June 6th, 1900, and communicated June 14th, 1900.

A transitive group of degree n and class $n-1$ contains just $n-1$ substitutions which displace all the n symbols. This property is characteristic; for, if the class be less than $n-1$, the number of substitutions which displace all the n symbols is greater than $n-1$. It is natural to seek to determine whether for such a group the $n-1$ substitutions which are regular in the n symbols, with the identical substitution, constitute a sub-group. No general answer to this question has yet been given. M. E. Maillet, in his thesis, *Récherches sur les Substitutions* (1892), and in subsequent memoirs in the *Bulletin of the French Mathematical Society*, has obtained in this connexion a number of interesting results; and, from quite a different point of view, I have obtained (*Theory of Groups*, pp. 141–144) limitations on the order of the group when the degree is given. In the present communication I show that, unless n is greater than the square of the least odd number which is the order of a simple group, a transitive group of degree n and class $n-1$ necessarily contains a transitive self-conjugate sub-group of order and degree n, consisting of the n substitutions in question. The problem is thus directly connected with another, at present unsolved, question in the theory of groups, viz., that of the possible existence of a simple group of odd order. No detailed investigation of a lower limit for the possible order of a simple group, if odd, has hitherto been undertaken; but I have shown (*loc. cit.*, p. 371) that such a limit must exceed 2835, and it is easy to verify that it certainly cannot be less than 9000. Hence, unless n exceeds 81,000,000, a transitive group of degree n and class $n-1$ is here shown to have a self-conjugate sub-group of order and degree n.

1. Let G be a transitive substitution group of degree n and order N, such that the n sub-groups of G each of which leaves one symbol unchanged are all distinct. Let G_0 be the sub-group of G which leaves the symbol a_0 unchanged, and let

$$a_{01}, a_{02}, \ldots, a_{0m}$$

be a set of the symbols which are interchanged transitively by G_0. Any substitution of G which changes a_0 into a_r must change the set

$$a_{01}, a_{02}, \ldots, a_{0m}, \text{ or } A_0$$

into the set

$$a_{r1}, a_{r2}, \ldots, a_{rm}, \text{ or } A_r,$$

this latter set being one, the symbols of which are interchanged transitively by the operations of the sub-group G_r which leaves a_r unchanged. Every substitution of G which changes a_0 into a_r must change the set A_0 into the set A_r; for otherwise A_r could not be a set of symbols which are interchanged transitively by G_r. Suppose now, further, that a linear function of the symbols of the set A_0 exists, other than their sum, which is changed into a multiple of itself by every operation of G_0. The necessary and sufficient conditions for this are that G_0, so far as it affects the symbols of the set A_0, shall be imprimitive in such a way that the imprimitive systems are merely interchanged cyclically by G_0. When these conditions are satisfied, the linear function of $a_{01}, a_{02}, \ldots, a_{0m}$ can, by taking the symbols in a suitable sequence, be written in the form

$$a_{01}+\epsilon a_{02}+\ldots+\epsilon^{m-1}a_{0m} \quad \text{or} \quad \alpha_0,$$

where ϵ is an mth root of unity, not necessarily a primitive root. If

$$\epsilon^{m'}=1,$$

where m' is equal to or is a factor of m, then $\alpha_0^{m'}$ is invariant for all the substitutions of G_0. If

$$a_{r1}+\epsilon a_{r2}+\ldots+\epsilon^{m-1}a_{rm}=\alpha_r,$$

where again the symbols are taken in a suitable sequence, then every substitution of G which changes a_0 into a_r must change $\alpha_0^{m'}$ into $\alpha_r^{m'}$, and α_0 into $\epsilon'\alpha_r$, where ϵ' is some integral power of ϵ.

Let the N operations T_s $(s=1, 2, \ldots, N)$ of G be

$$a_r'=a_{r_s} \quad (r=0, 1, \ldots, n-1),$$

where $0_s, 1_s, \ldots, (n-1)_s$ are $0, 1, \ldots, (n-1)$, in some new sequence. The effect of these substitutions on the α's is to give N linear substitutions T_s' $(s=1, 2, \ldots, N)$

$$\alpha_r'=\epsilon_{r,s}\alpha_{r_s} \quad (r=0, 1, \ldots, n-1).$$

These linear substitutions constitute a group G' which is simply isomorphic with G, so that T_s and T_s' are corresponding operations.

The quantities $\epsilon_{r,s}$ are m'th roots of unity, and some of them are certainly distinct from unity.

Let T'_s be an operation of G whose order is relatively prime to m'. If it permutes the symbols cyclically in sets of $m_1, m_2, \ldots, m_t$, its multiplier equation will be

$$(\lambda^{m_1}-1)(\lambda^{m_2}-1)\ldots(\lambda^{m_t}-1)=0,$$

where $m_1, m_2, \ldots, m_t$ are relatively prime to m'. The multiplier equation of T'_s will be

$$(\lambda^{m_1}-\epsilon_1)(\lambda^{m_2}-\epsilon_2)\ldots(\lambda^{m_t}-\epsilon_t)=0,$$

where $\epsilon_1, \epsilon_2, \ldots, \epsilon_t$ represent products of the n quantities $\epsilon_{r,s}$ in sets of $m_1, m_2, \ldots, m_t$. Hence, as T'_s is of the same order as T_s, $\epsilon_1, \epsilon_2, \ldots, \epsilon_t$ must all be unity, and therefore

$$\prod_{r=0}^{r=n-1} \epsilon_{r,s} = 1.$$

The product of two operations of G' for which this last equation holds is obviously another operation of G' for which it holds. Now the totality of the operations of G, whose orders are relatively prime to m' generate a self-conjugate sub-group, and, unless the equation

$$\prod_{r=0}^{r=n-1} \epsilon_{r,s} = 1$$

holds for all the operations of G', this sub-group cannot coincide with G itself. Hence, unless the product $\prod_{r=0}^{r=n-1} \epsilon_{r,s}$ is unity for all the operations of G', the group G is composite and has a self-conjugate sub-group constituted of the totality of the operations for which this product is unity.*

2. The result thus obtained is now to be applied to transitive groups of degree n and class $n-1$. The order of such a group is $n\nu$, where ν is a factor of $n-1$, and a sub-group of order ν which leaves one symbol unchanged permutes the remainder regularly in $\frac{n-1}{\nu}$

* [*Sept. 4th*, 1900.—This result is immediately obvious by considering the effect of the substitutions of G' on the product $a_0 a_1 \ldots a_{n-1}$. Unless $\prod_{n=0}^{r=n-1} \epsilon_{r,s} = 1$ for each substitution, a cyclical group thus arises with which G' and G are multiply isomorphic.]

transitive sets of ν each. Hence, if G_0 is not a perfect group, the conditions are satisfied for the existence of a linear invariant a_0 of G_0. With the notation of § 1 m' is a factor of ν; and the order of an operation S' of G', which changes a_0 in ϵa_0, must be some multiple $m'p$ of m'. If S is the corresponding operation of G, then S must leave a_0 unchanged and permute the remaining $n-1$ symbols cyclically in sets of $m'p$ each. Let

$$a_1' = a_2, \quad a_2' = a_3, \quad \ldots, \quad a_{m'p}' = a_1$$

be a cycle of S. Then

$$a_1' = \epsilon_1 a_2, \quad a_2' = \epsilon_2 a_3, \quad \ldots, \quad a_{m'p}' = \epsilon_{m'p} a_1$$

is the corresponding part of S'; and, since $m'p$ is the order of S',

$$\epsilon_1 \epsilon_2 \ldots \epsilon_{m'p} = 1.$$

Hence, for S',
$$\prod_{r=0}^{r=n-1} \epsilon_{r,s} = \epsilon,$$

and therefore G has a self-conjugate sub-group which does not contain S. The order of any operation of G which displaces all the symbols is prime relatively to ν, and therefore to m'. Hence the self-conjugate sub-group for which

$$\prod_{r=0}^{r=n-1} \epsilon_{r,s} = 1$$

contains all the operations of G which displace all the symbols. This self-conjugate sub-group then appears as a transitive group of degree n, class $n-1$, and order $n\nu'$, where $\nu' = \nu/m'$. If the sub-groups of degree ν' are not perfect, the same process may be repeated. Hence, finally, if the sub-group of order ν is soluble, the $n-1$ operations which displace all the symbols form, with the identical operation, a self-conjugate sub-group.

If ν is even, I have shown (*loc. cit.*) that this self-conjugate sub-group always exists, and that it is then Abelian. It is also proved in the same place that, if ν is not less than $\sqrt{n}$, the degree n must be the power of a prime, so that again, in this case, the self-conjugate sub-group of order and degree n necessarily exists. If l is the smallest odd number which is the order of a simple group, every group of odd order less than l is necessarily soluble. Hence, finally, unless n is greater than l^2, a transitive group of degree n and class $n-1$ necessarily contains a self-conjugate sub-group of order and degree n.

3. It has been shown in the preceding section that, if the sub-groups of order ν of a transitive group G of degree n, order $n\nu$, and class $n-1$ are soluble, then G has a transitive self-conjugate sub-group of order n. I proceed now to prove that, if G has such a self-conjugate sub-group, then the sub-groups of order ν are soluble, with a single possible exception.

Let H be the transitive self-conjugate sub-group of order n of G now assumed to exist; and, $p^{\alpha'}$ being the highest power of a prime p which divides n, let P' be a sub-group of H of order $p^{\alpha'}$. There must be a sub-group K of G of order ν each of whose operations transforms P' into itself; as otherwise G would contain more sub-groups of order $p^{\alpha'}$ than H contains. Hence $\{P', K\}$ is a group of order $p^{\alpha'}\nu$ which contains P' self-conjugately. Let P, of order p^{α}, be that characteristic sub-group of P' which consists of all the self-conjugate operations of P' whose orders are p. Then every operation of K transforms P into itself, and therefore $\{P, K\}$ is a group of order $p^{\alpha}\nu$ which contains P self-conjugately. Moreover, no operation of K is permutable with any operation of P. Hence K can be represented as a group of isomorphisms of P; and no one of these isomorphisms leaves any operation of P, except identity, unchanged.

Let q be any prime factor of ν, and suppose, if possible, that K contains two permutable operations of order q which are not powers of each other. These will generate a group of isomorphisms of P of order q^2. If

$$T_{r,s} \quad (r = 1, 2, \ldots, q;\ s = 1, 2, \ldots, q)$$

be a set of q^2 operations of P which are interchanged transitively by this group of isomorphisms, the two generating operations of the group (so far as it affects this set of symbols) may be taken to be

$$(T_{1,1}T_{1,2}\ldots T_{1,q}) \ \ldots\ (T_{q,1}T_{q,2}\ldots T_{q,q})$$

and

$$(T_{1,1}T_{2,1}\ldots T_{q,1}) \ \ldots\ (T_{1,q}T_{2,q}\ldots T_{q,q}),$$

and from these the remaining operations may be at once written down. The product of the T's contained in any one cycle of any of these isomorphisms is an operation of P which is changed into itself. It must therefore be the identical operation. Now in the $q+1$ products thus formed which contain $T_{1,1}$ each of the other T's occurs just once. Hence

$$T_{1,1}^{q+1}T_{1,2}\ \ldots\ T_{q,q} = 1.$$

But

$$T_{1,1}T_{1,2}\ \ldots\ T_{q,q} = 1,$$

since the left-hand side is the product of the T's in the q cycles of any one isomorphism. Hence

$$T_{1,1}^{q} = 1,$$

which is not true. The supposition that K contains two permutable operations of order q which are not powers of each other therefore leads to a contradiction. Hence, if q^{β} be the highest power of a prime q which divides ν, a sub-group of K of order q^{β} has only one sub-group of order q. It follows immediately* that, if q is odd, the sub-groups of K of order q^{β} are cyclical; while, if q is 2, they are either cyclical or of the type

$$S^{2^{\beta-1}} = 1, \quad \Sigma^2 = S^{2^{\beta-2}}, \quad \Sigma^{-1} S \Sigma = S^{-1}.$$

A group of order $p^{\alpha} q^{\beta} \ldots$ in which the sub-groups of order p^{α}, q^{β}, ... are cyclical, is always soluble;† and a group of order $2^{\alpha} q^{\beta}, \ldots$ in which the sub-groups of order 2^{α} are of the above type, while those of order q^{β}, ... are cyclical, is certainly soluble,‡ unless the order is divisible by 3. Hence in a transitive group of degree n, class $n-1$, and order $n\nu$, the sub-groups of order ν are, with a single possible exception, soluble if the group has a sub-group of order n.

4. The main results obtained in this note may be stated, apart from the phraseology of substitution groups, as follows:—

If a group of order nm, where n and m are relatively prime, contains n conjugate sub-groups of order m which have no common operations except identity, and if these sub-groups are soluble, then the group has a self-conjugate sub-group of order n.

If these conditions are satisfied, and m is the power of an odd prime (in which case the sub-groups of order m are necessarily soluble), then these sub-groups are cyclical.

If a group admits a group of isomorphisms whose order is a power of an odd prime, no one of which leaves any operation of the group except identity unchanged, the group of isomorphisms is cyclical.

If a group admits a group of isomorphisms whose order is a power of 2, no one of which leaves any operation of the group unchanged except identity, the group of isomorphisms is either cyclical or of the type defined above.

---

* *Theory of Groups*, pp. 72–75.
† *Ibid.*, p. 352.
‡ *Ibid.*, p. 364.

[*Note, July* 10*th*, 1900.—An odd number certainly cannot be the order of a simple group unless it has more than five prime factors. Moreover, it must not be of the forms p^a, p^aq, p^aq^2, p^aq^β, ..., r^γ, where, in the last form, each index is either 1 or 2. These results are proved in the last chapter of my *Theory of Groups*.

Now the only odd numbers less than 9000 which satisfy these conditions are :—

(i) $3^5.5.7$, (ii) $3^4.5.7$, (iii) $3^4.5.11$, (iv) $3^4.5.13$,
(v) $3^4.5.17$, (vi) $3^4.5.19$, (vii) $3^4.7.11$, (viii) $3^4.7.13$,
(ix) $3^3.5^3$, (x) $3^3.5^2.7$, (xi) $3^3.5^2.11$, (xii) $3^3.5^2.13$,
(xiii) $3^3.5.7^2$, (xiv) $3^2.5^3.7$.

Groups of orders (i), ..., (vii) may be shown immediately to have a self-conjugate sub-group whose order is a power of 3. A group of order (viii), if simple, could be represented as a substitution group of degree 27, and the sub-group of order 13.7.3, which keeps one symbol unchanged, could be expressed as a group of degree 13; it is known that no such group exists. A group of order (ix) must have a self-conjugate sub-group of order 5^3. A group of order (x) must have a self-conjugate sub-group whose order is a power of 5. A group of order (xi), if simple, could be expressed as a substitution group of degree 11 ; it is known that no such group exists. A group of order (xii) must have a self-conjugate sub-group whose order is a power of 5. A group of order (xiii), if simple, could be expressed as a substitution group of degree 15; no such group exists. A group of order (xiv) must have a self-conjugate sub-group whose order is a power of 5. No group whose order is odd and less than 9000 then can be simple; and every such group is, therefore, soluble. The statement in the introduction is thus justified.]