is any set of characteristics, and

$$\chi_1^k,\ \chi_2^k,\ \ldots,\ \chi_r^k$$

a set for which χ_1^k is unity, then

$$\chi_1^k\chi_1^i,\ \chi_2^k\chi_2^i,\ \ldots,\ \chi_r^k\chi_r^i$$

is a set of characteristics.

Returning to the irreducible representation of the group in the form

$$x_s' = \Sigma a_{stm} x_t,$$

the $\frac{1}{2}\chi_1^i(\chi_1^i+1)$ homogeneous products of the second degree of the x's are transformed linearly among themselves by every operation of the group; and, for this representation, the sum of the multipliers of any operation is equal to the sum of the homogeneous products two together of the multipliers in the above irreducible form. Hence, by similar reasoning to that employed above, there must be positive integers e_{is}, such that

$$\psi_k^i = \Sigma_s e_{is}\chi_k^s \quad (k, i = 1, 2, \ldots, r), \qquad \text{(ii)}$$

where ψ_k^i is the sum of the homogeneous products two together of the multipliers whose sum is χ_k^i. In this way it may be shown that, if any symmetric function be formed of χ_1^i symbols, a system of equations of the form (ii), in which the e's are positive integers, must hold when ψ_k^i is the symmetric function formed from the multipliers whose sum is χ_k^i. In particular, the products of the multipliers for each set of conjugate operations in any representation of the group constitutes a set of characteristics for which χ_1 is unity.

On some Properties of Groups of Odd Order. *By* W. Burnside.

Received and communicated November 8th, 1900.

This paper consists mainly of applications of the theory of group-characteristics given in the preceding paper to groups of odd order. It is shown in the first section that a group of odd order has no self-inverse set of characteristics. From this it follows at once that such a group when represented as an irreducible group of linear substitutions must contain substitutions whose coefficients are not all

real. In other words, a group of linear substitutions of odd order the coefficients in which are all real is necessarily reducible. Another consequence is that the order of such a group and the number of sets of conjugate operations which it contains are congruent to each other (mod. 16).

The chief result of the second section is that a group of prime degree which is not doubly transitive must be metacyclical. It follows that there are no simple groups of odd composite order and prime degree.

In the third section I have extended from degrees not exceeding 50 to degrees not exceeding 100 the result obtained by Dr. Miller,* viz., that corresponding to such degrees there are no simple groups of odd composite order. The method used is such that in only four cases, namely, for degrees 57, 81, 91, and 99, is any detailed discussion necessary; and I have no doubt that by it the lower limit for the degree of possible simple groups of odd composite order might, without much labour, be carried considerably beyond 100.

The results obtained in this paper, partial as they necessarily are, appear to me to indicate that an answer to the interesting question as to the existence or non-existence of simple groups of odd composite order may be arrived at by a further study of the theory of group-characteristics.

I.

1. A doubly transitive permutation group has obviously only two quadratic invariants, viz., the sum of the squares of its symbols and the sum of their products two together.

Let G be a simply transitive group in the symbols

$$x_1, x_2, \ldots, x_n,$$

and let G_s be the sub-group of G which leaves x_s unchanged. G_s will interchange the remaining $n-1$ symbols in $m(\geq 2)$ transitive sets. For each suffix s these sets will be denoted by

$$\begin{array}{llll} x_{s1,1}, & x_{s1,2}, & \ldots, & x_{s1,k_1}, \\ x_{s2,1}, & x_{s2,2}, & \ldots, & x_{s2,k_2}, \\ \ldots & \ldots & \ldots & \ldots \\ x_{sm,1}, & x_{sm,} & \ldots, & x_{sm;k_m}, \end{array}$$

where one or more of the k's may be unity.

* *Proc. Lond. Math. Soc.*, Vol. XXXIII., pp. 6-10.

Suppose that S and S' are any two substitutions each of which changes x_1 into x_s, so that

$$S^{-1}G_1S = S'^{-1}G_1S' = G_s.$$

The set of symbols $x_{11,1},\ x_{11,2},\ \ldots,\ x_{11,k_1}$

which are interchanged transitively by G_1 must be changed by S into a set, equal in number, which are interchanged transitively by G_s. Hence it may be assumed that

$$S\,(x_{11,1},\ x_{11,2},\ \ldots,\ x_{11,k_1}) = (x_{s1,1},\ x_{s1,2},\ \ldots,\ x_{s1,k_1}).$$

Suppose, if possible, that

$$S'\,(x_{11,1},\ x_{11,2},\ \ldots,\ x_{11,k_1}) = (y_1,\ y_2,\ \ldots,\ y_{k_1}),$$

where the y's constitute some other set which are interchanged transitively by G_s. Then $S^{-1}S'$ changes the set

$$x_{s1,1},\ x_{s1,2},\ \ldots,\ x_{s1,k_1}$$

into the set $y_1,\ y_2,\ \ldots,\ y_{k_1}$.

But $S^{-1}S'$, leaving x_s unchanged, belongs to G_s; and the former set are interchanged transitively among themselves by G_s. Hence

$$S'\,(x_{1,11},\ x_{11,2},\ \ldots,\ x_{11,k_1}) = (x_{s1,1},\ x_{s1,2},\ \ldots,\ x_{s1,k_1}).$$

It follows that a correspondence may be established among the transitive sets in which the different sub-groups G_s interchange the symbols such that for all values of the suffixes s and t every operation of G which changes x_s into x_t also changes the set

$$x_{sp,1},\ x_{sp,2},\ \ldots,\ x_{sp,k_p}$$

into the set $x_{tp,1},\ x_{tp,2},\ \ldots,\ x_{tp,k_p}$

$$(p = 1, 2, \ldots, m).$$

Consider now the quadratic function

$$f = \sum_{s=1}^{s=n} x_s\,(x_{s1,1} + x_{s1,2} + \ldots + x_{s1,k_1}).$$

It is clearly invariant for every operation of G; and, apart from a possible numerical factor, it is the smallest quadratic invariant of G which contains $x_s x_{s1,1}$. No one of the n brackets contains a repeated symbol, and every one of the n symbols must enter in the brackets the same number of times, viz., k_1. Hence, gathering together those

products which have the same second symbol,

$$f = \sum_{s=1}^{s=n} (y_{s1} + y_{s2} + \dots + y_{sk_1})\, x_s,$$

and every operation of G_s must interchange among themselves the symbols in the bracket multiplying x_s. These symbols must, therefore, constitute one or more complete transitive sets for G_s; and, since, from the first form of f, there are substitutions in G which change any one product $x_s x_{s1,1}$ of f into any other, the y's must constitute a single transitive set of G_s. Suppose, first, that

$$(y_{s1}, y_{s2}, \dots, y_{sk_1}) = (x_{s1,1}, x_{s1,2}, \dots, x_{s1,k_1}).$$

Then every product of two symbols must occur twice in f, and therefore nk_1 must be even. If G is a group of odd order, this is impossible, and the two sets must be distinct. Hence, for a group of odd order the k's are equal in pairs and m is even. Further, m is clearly congruent to 0 or 2 (mod. 4), according as n is congruent to 1 or 3 (mod. 4); and the number of independent quadratic invariants is $1+\frac{m}{2}$. For a group of even order

$$(y_{s1}, y_{s2}, \dots, y_{sk_1}) = (x_{s1,1}, x_{s1,2}, \dots, x_{s1,k_1}),$$

if the group contains a substitution of order 2 which transposes x_s and $x_{s1,1}$. In this case no statement can be made as regards the parity of m, and the number of independent quadratic invariants is greater than $1+\frac{m}{2}$.

2. The result thus obtained for groups of odd order will now be applied to a particular case. Let g be a group of odd order n, represented as a regular permutation group in n symbols; and let g' be the simply isomorphic permutation group* in the n symbols, each of whose substitutions is permutable with every substitution of g. The group $\{g, g'\}$, whose order is n^2/n', where n' is the number of self-conjugate operations of g, is such that its sub-groups which leave one symbol unchanged interchange the remaining $n-1$ in $r-1$ sets (*loc. cit.*), where r is the number of conjugate sets in g. Since n is odd, r is odd, and the number of independent quadratic invariants of $\{g, g'\}$ is $\frac{1}{2}(r+1)$.

The group $\{g, g'\}$, being a permutation group, is reducible, and it is

* *Theory of Groups*, p. 146.

shown in my paper "On the Continuous Group defined by any given Group of Finite Order" (*Proc. Lond. Math. Soc.*, Vol. XXIX., pp. 558, 559) that the r sets of linear functions of the original variables, there denoted by

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i} \quad (i = 1, 2, \ldots, r),$$

are each transformed among themselves by the operations of $\{g, g'\}$. The total number of these linear functions is n; they are shown (*loc. cit.*) to be linearly independent. Since the original form of $\{g, g'\}$ is real, it follows that, if

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i}$$

are transformed among themselves, so also are

$$\bar{\xi}_{i1}, \bar{\xi}_{i2}, \ldots, \bar{\xi}_{im_i},$$

where ξ and $\bar{\xi}$ are conjugate imaginaries.

Moreover, these $2m_i$ functions either must be linearly independent or each of one set must be linearly expressible in terms of the other set. In fact, if $m' (< m_i)$ linear functions of the second set were expressible in terms of the first set, these m' functions would be transformed among themselves by all the operations of $\{g, g'\}$, and therefore also by all operations of the continuous group $\{G, G'\}$; and this is shown (*loc. cit.*, p. 558) not to be the case.

Now, for every group of linear substitutions of finite order in m variables, at least one Hermitian form,

$$\Sigma a_{ij} x_i \bar{x}_j \quad (a_{ij} = \bar{a}_{ji}),$$

exists which is invariant for the group.* Let such a Hermitian form be constructed for each of the r sets of variables in which $\{g, g'\}$ has been expressed. If

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i}$$

and

$$\bar{\xi}_{i1}, \bar{\xi}_{i2}, \ldots, \bar{\xi}_{im_i}$$

are linearly independent, the Hermitian forms for these two sets are identical, and the two sets so give rise to a single real quadratic invariant for $\{g, g'\}$. If, on the other hand,

$$\bar{\xi}_{i1}, \bar{\xi}_{i2}, \ldots, \bar{\xi}_{im_i}$$

are expressible in terms of

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i},$$

* This theorem was given independently by Prof. A. Loewy (*Comptes Rendus*, Vol. CXXIII., pp. 168–171), and by Prof. E. H. Moore (*Math. Ann.*, Vol. L., pp. 213–219).

then this single set gives rise to a real quadratic invariant for $\{g, g'\}$. Since, in any case,

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i}, \quad \bar{\xi}_{i1}, \ldots, \bar{\xi}_{im_i}$$

are linearly independent of the variables

$$\xi_{j1}, \xi_{j2}, \ldots, \xi_{jm_j}$$

belonging to any other distinct set, the quadratic invariant of $\{g, g'\}$ which arises from this latter set is essentially distinct from that which arises from

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i}.$$

Now, when i is unity m_i is unity, and the corresponding ξ_{11} is real, viz., the sum of the original variables. This set by itself gives rise to one quadratic invariant, and therefore, unless the remaining $r-1$ sets occur in pairs, such as

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i}$$

and

$$\bar{\xi}_{i1}, \bar{\xi}_{i2}, \ldots, \bar{\xi}_{im_i},$$

so that each pair gives rise to a single real quadratic invariant, the number of independent quadratic invariants would exceed $\frac{1}{2}(r+1)$. But $\frac{1}{2}(r+1)$ has been shown to be the number of such invariants. Hence for each value of i except unity

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i},$$

$$\bar{\xi}_{i1}, \bar{\xi}_{i2}, \ldots, \bar{\xi}_{im_i}$$

are linearly independent; and therefore, with the same limitation,

$$\frac{1}{\chi_1^i} \sum_s h_s \chi_s^i e_s \quad \text{and} \quad \frac{1}{\chi_1^i} \sum h_s \bar{\chi}_s^i \epsilon_s,$$

the multipliers of these two sets of functions in H, are distinct.

In other words, a group of odd order has no self-inverse set of group-characteristics except the first; and therefore in each such set some at least of the characteristics must be imaginary.

This involves that when a group of odd order is represented as an irreducible group of linear substitutions some of the coefficients must be imaginary; or, that a group of odd order cannot be expressed in a form which is at once real and irreducible.

3. This result appears to me of such importance for the theory of groups of odd order that I give a second independent proof of it. Suppose, if possible, that every characteristic of a set, other than the

first, is real; and let the characteristic of an operation S of order m be

$$\chi_1 = a_0 + a_1(\omega + \omega^{-1}) + a_2(\omega^2 + \omega^{-2}) + \dots,$$

where ω is a primitive m-th root of unity, and a_0, a_1, a_2, ... are positive integers or zeroes. Then χ_1 is also the characteristic of S^{-1}, which belongs to the inverse set to that containing S. Moreover, if S^x (x prime relatively to m) does not belong to the same set as either S or S^{-1}, no more does S^{-x}; and, if the set containing S^x has χ_1 for its characteristic, so also has the set containing S^{-x}. Hence, of the conjugate sets containing powers of S whose indices are relatively prime to m, an even number 2μ must have χ_1 for characteristic. Suppose, now, that when ω is replaced by each primitive m-th root in turn χ_1 takes the s distinct values

$$\chi_1, \chi_2, \dots, \chi_s.$$

Then for each of these as characteristic there are 2μ conjugate sets containing powers of S whose indices are relatively prime to m; and the conjugate sets which contain such powers of S are thus exhausted. Moreover, the number of operations in each such set is the same. Hence $\Sigma h\chi$ for these sets is an even multiple of

$$\chi_1 + \chi_2 + \dots + \chi_s,$$

and this latter quantity is a rational positive or negative integer (or zero). Hence, for this system of conjugate sets $\Sigma h\chi$ is even. Now all the sets except the first may be arranged in such systems, and therefore $\Sigma h\chi$ for all conjugate sets except the first is even. Since the group is of odd order, the characteristic of the identical operation is necessarily odd; and the equation

$$\sum_{k=1}^{k=r} h_k \chi_k = 0^*$$

would involve that the sum of an even and an odd number is zero. This contradiction shows therefore that the supposition that all the characteristics of the set were real was incorrect; and hence that a group of odd order can have no self-inverse set of characteristics except the first.

From this result a relation between n, the order of the group, and r, the number of sets of conjugate operations, may be at once deduced.

---

* This relation is the particular case of the relation

$$\Sigma h_k \chi_k^i \chi_k^j = 0,$$

which results from taking $j = 1$.

In fact, for two inverse sets

$$\chi_1^i = \chi_1^{i'} = 2k+1, \text{ an odd number.}$$

Hence $$(\chi_1^i)^2 + (\chi_1^{i'})^2 = 2(2k+1)^2 \equiv 2, \mod 16;$$

and therefore, since $\chi_1^1 = 1$,

$$n = \sum_i (\chi_1^i)^2 \equiv r, \mod 16.$$

Similarly, it may be shown that, if every factor of n is of the form $2km+1$, where m is an assigned odd integer, then

$$n \equiv r, \mod 16m.*$$

4. The relation $$\sum_i \chi_k^i \chi_l^i = 0, \quad l \neq k',$$

becomes for a group of odd order, by taking k for l,

$$\sum_i (\chi_k^i)^2 = 0,$$

and, combining this with $\sum_i \chi_k^i \chi_{k'}^i = \frac{n}{h_k}$,

$$-\sum_i (\chi_k^i - \chi_{k'}^i)^2 = \sum_i (\chi_k^i + \chi_{k'}^i)^2 = \frac{2n}{h_k}.$$

As an application of these formulæ, I consider a group whose order is divisible by 3, and I suppose the order of the operations of the k-th set to be 3. Then

$$\chi_k^i = a_0^i + a_1^i \omega + a_2^i \omega^2,$$

where ω is a primitive cube root of unity and a_0^i, a_1^i, a_2^i are positive integers or zeroes,

$$\chi_k^i - \chi_{k'} = (a_1^i - a_2^i)\sqrt{-3},$$

and therefore $$3\Sigma (a_1^i - a_2^i)^2 = \frac{2n}{h_k} = 2m_k,$$

---

* For the smaller values of r the determination of all groups of odd order with a given number of conjugate sets presents no difficulty. Thus for values of r less than 16 the only groups of odd order which have no self-conjugate operations are the following:—For $r = 5$, $n = 7 \cdot 3$; $r = 7$, $n = 11 \cdot 5, 13 \cdot 3$; $r = 9$, $n = 19 \cdot 3$; $r = 11$, $n = 5^2 \cdot 3, 31 \cdot 5, 29 \cdot 7, 19 \cdot 9$; $r = 13$, $n = 31 \cdot 3, 41 \cdot 5, 43 \cdot 7, 37 \cdot 9, 23 \cdot 11, 3^4 \cdot 13$; $r = 15$, $n = 37 \cdot 3, 3^3 \cdot 13$. These groups are all metacyclical with the exception of those of orders $5^2 \cdot 3$, $3^3 \cdot 13$, and $3^4 \cdot 13$. This list is in marked contrast to the corresponding one for groups of even order. Again, omitting groups with self-conjugate operations, the latter is:—for $r = 3$, $n = 3 \cdot 2$; $r = 4$, $n = 5 \cdot 2$, $2^2 \cdot 3$; $r = 5$, $n = 7 \cdot 2$, $5 \cdot 2^2$, $2^3 \cdot 3$, $2^2 \cdot 3 \cdot 5$; $r = 6$, $n = 3^2 \cdot 2$, two types, $3^2 \cdot 2^2$, $2^3 \cdot 3 \cdot 7$. In this list two simple groups appear, though the number of conjugate sets does not exceed 6.

where m_k is the order of the greatest sub-group which contains one of the operations of the k-th set self-conjugately. Hence, unless m_k is a multiple of 27, there must be at least one pair of inverse sets of characteristics for which $a_1^i - a_2^i$ is not a multiple of 3. The product of the multipliers for such a set would be $\omega^{a_1^i - a_2^i}$, that is ω or ω^2; and the group therefore would have a self-conjugate sub-group of index 3, formed by those operations for which the product of the multipliers is unity. In particular a group of order $3m$ or 3^2m, where m is odd and prime relatively to 3, has a self-conjugate sub-group of order m. Suppose now that 5 is a factor of the order, and that the k-th set is of order 5. Then

$$\chi_k^i = a_0^i + a_1^i \epsilon + a_2^i \epsilon^2 + a_3^i \epsilon^3 + a_4^i \epsilon^4,$$

where ϵ is a primitive fifth root of unity and

$$\chi_k - \chi_{k'}^i = (a_1^i - a_4^i)(\epsilon - \epsilon^4) + (a_2^i - a_3^i)(\epsilon^2 - \epsilon^3).$$

If this is not zero, there must be a second set for which

$$\chi_k^j - \chi_{k'}^j = (a_1^i - a_4^i)(\epsilon^2 - \epsilon^3) + (a_2^i - a_3^i)(\epsilon^4 - \epsilon),$$

and
$$(\chi_k^i - \chi_{k'}^i)^2 + (\chi_k^j - \chi_{k'}^j)^2 = -5\left\{(a_1^i - a_4^i)^2 + (a_2^i - a_3^i)^2\right\}.$$

Hence
$$5\Sigma\left\{(a_1^i - a_4^i)^2 + (a_2^i - a_3^i)^2\right\} = 2m_k,$$

where the summation is extended to all pairs of sets such as the i-th and j-th. If m_k is not divisible by 5^2, there must be at least one set for which

$$(a_1^i - a_4^i)^2 + (a_2^i - a_3^i)^2 \not\equiv 0, \quad \text{mod. } 5;$$

and therefore
$$a_1^i - a_2^i + 2(a_2^i - a_2^i) \not\equiv 0, \quad \text{mod. } 5.$$

For such a set the product of the multipliers of an operation of the k-th set is a primitive fifth root of unity. Moreover, if 5 is an unrepeated factor of the order, m_k cannot be divisible by 25. Hence, a group of order $5m$, where m is odd and prime relatively to 5, has a self-conjugate sub-group of order m.

II.

5. In his memoir "Über die Darstellung der endlichen Gruppen durch lineare Substitutionen" (*Berliner Sitzungsberichte*, 1897, pp. 994–1015) Herr Frobenius has proved the theorem that, if two groups of linear substitutions in the same number of variables are simply isomorphic, and if the sums of the multipliers of corresponding operations in the two groups are the same, then the one group is

the result of transforming the other by some substitution of non-vanishing determinant. This theorem is clearly of fundamental importance in dealing with groups of finite order. In any representation of a group as a group of linear substitutions the sum of the multipliers for every operation of the k-th conjugate set is of the form $\Sigma a_i \chi_k^i$, where a_i is a positive integer (or zero) which is the same for all the sets, and $\Sigma a_i \chi_1^i$ is the number of variables (*Proc. Lond. Math. Soc.*, Vol. XXIX., pp. 564, 565). Hence, by taking a_i sets of χ_1^i variables for each suffix i, and forming in each set the irreducible group which has the characteristics $\chi_1^i, \chi_2^i, \ldots, \chi_r^i$, a group of linear substitutions is set up simply isomorphic with the given group, and having the same total number of variables and the same sum of the multipliers for each operation that the given group has. The theorem therefore shows the possibility of transforming any group of linear substitutions of finite order in such a way as to represent it as the result of an isomorphism established among a number of irreducible groups in independent sets of variables. These irreducible groups will here be spoken of as the irreducible *components* of the given group of linear substitutions. Apart from transformations of the irreducible components themselves, this reduction will be a unique process if no one of the irreducible components is repeated, but not otherwise.

A permutation group is never irreducible. In fact, the sum of the variables is unaltered by every operation of the group. If

$$x_1, x_2, \ldots, x_n$$

are the variables of a permutation group g, and if

$$\xi_1, \xi_2, \ldots, \xi_m$$

are a set of linear functions of the x's which are transformed among themselves by an irreducible component of g of which

$$\chi_1, \chi_2, \ldots, \chi_r$$

are the characteristics, then

$$\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_m$$

must be linearly transformed among themselves by an irreducible component whose characteristics are

$$\bar{\chi}_1, \bar{\chi}_2, \ldots, \bar{\chi}_r.$$

For a group of even order this may be the same component as the previous one, but for a group of odd order it is necessarily distinct. For a transitive group of odd order the number of irreducible com-

ponents is therefore odd and congruent (mod. 4) to the degree of the group. Moreover, since the coefficients of a permutation group are all rational, it follows that, if it has an irreducible component for which the characteristics are

$$\chi_1, \chi_2, \ldots, \chi_r,$$

it must have irreducible components whose characteristics,

$$\chi_1', \chi_2', \ldots, \chi_r',$$

are derived from the previous set by replacing any irrationality that occurs in them by one of its conjugate values.

6. Let g be a transitive permutation group in the n symbols

$$x_1, x_2, \ldots, x_n.$$

When the reduction of g is completely effected, let

$$\begin{aligned} &\xi_{11} \qquad (= x_1 + x_2 + \ldots + x_n);\\ &\xi_{21}, \xi_{22}, \ldots, \xi_{2m_2};\\ &\ldots \quad \ldots \quad \ldots \quad \ldots\\ &\xi_{k1}, \xi_{k2}, \ldots, \xi_{km_k} \end{aligned}$$

be the sets of symbols which are transformed, each among themselves, by irreducible components of g; so that the ξ's form a set of n independent linear functions of the x's. Every operation of the continuous Abelian group H,

$$\begin{aligned} &\xi_{si}' = a_s \xi_{si}\\ &(i = 1, 2, \ldots, m_s),\\ &(s = 1, 2, \ldots, k), \end{aligned}$$

is permutable with every operation of g. This continuous group H is not, however, necessarily the most extensive group every one of whose operations is permutable with every operation of g. In fact, if two (or more) sets of the ξ's, such as

$$\xi_{i1}, \xi_{i2}, \ldots, \xi_{im_i}$$

and

$$\xi_{j1}, \xi_{j2}, \ldots, \xi_{jm_j},$$

contain the same number of symbols (so that $m_i = m_j$), and if these two sets undergo identical transformations corresponding to the same substitution of g, then

$$\begin{aligned} &\xi_{st}' = \xi_{st} \quad (s \neq i, j),\\ &\left.\begin{aligned} \xi_{it}' &= a\xi_{it} + \beta\xi_{jt}\\ \xi_{jt}' &= \gamma\xi_{it} + \delta\xi_{jt} \end{aligned}\right\} \quad (t = 1, 2, \ldots\ m_i) \end{aligned}$$

is a linear substitution not contained in H, and permutable with every operation of g. No such linear substitution, however, is permutable with every operation of H; and therefore, if such substitutions exist, the most general continuous group G each of whose operations is permutable with every operation of g is not Abelian.

Conversely, if the most general continuous group G whose operations are permutable with every operation of g is Abelian, it must be the group H; and each set of functions which occur in connexion with the same multiplier in H are transformed among themselves by an irreducible component of g.

The form of G, in terms of the x's, may be obtained as follows. Let

$$x_r' = x_{r'} \quad (r = 1, 2, \ldots, n)$$

be any operation of g. The linear substitution

$$x_r' = \sum_{s=1}^{s=n} a_{rs} x_s \quad (r = 1, 2, \ldots, n)$$

will be permutable with this operation if

$$\left.\begin{aligned} x_r' &= \sum_{s=1}^{s=n} a_{rs} x_{s'} \\ \text{and} \qquad x_r' &= \sum_{s=1}^{s=n} a_{r's} x_s \end{aligned}\right\} \quad (r = 1, 2, \ldots, n)$$

are the same substitution; that is, if

$$a_{rs} = a_{r's'} \quad (r, s = 1, 2, \ldots, n),$$

$x_{r'}$ and $x_{s'}$ being the symbols in which x_r and x_s are changed by the operation of g considered. Hence the necessary and sufficient condition that

$$x_r' = \sum_{s=1}^{s=n} a_{rs} x_s \quad (r = 1, 2, \ldots, n)$$

should be permutable with every operation of g is that the coefficients a_{rs} should be equal in sets; any two a_{rs} and a_{pq} being equal if g contains a substitution which changes x_r and x_s into x_p and x_q respectively.

Since g is transitive, $a_{11} = a_{22} = \ldots = a_{nn}$,

and no one of these symbols is equal to a_{rs}, if r and s are different. If g is doubly transitive,

$$a_{rs} = a_{pq},$$

where r, s and p, q are any two pairs of distinct symbols; and the general operation of G takes the form

$$x_r' = (a-b)\, x_r + b \sum_{1}^{n} x_s \quad (r = 1, 2, \ldots, n).$$

If g is not doubly transitive, the general operation of G, with the notation of p. 163, will be

$$x_s' = a_0 x_s + \sum_{t=1}^{t=m} a_t (x_{st,1} + x_{st,2} + \ldots + x_{st,k_t})$$
$$(s = 1, 2, \ldots, n).$$

The order of G is, therefore, $m+1$, where m is the number of transitive sets in which a sub-group of g that leaves one symbol unchanged interchanges the remaining $n-1$, and the number of irreducible components of g is equal to or is less than $1+m$, according as G is or is not Abelian. It may be noticed that the necessary and sufficient condition that G should contain a permutation is that at least one of the numbers $k_1, k_2, \ldots, k_m$ should be unity; *i.e.*, that a sub-group of g which leaves one symbol unchanged leaves more than one. If G is not Abelian, g must have at least three irreducible components; and, if G is Abelian, the number of irreducible components of g is equal to the order of G. Hence, g must have more than two irreducible components, unless it is doubly transitive; and, if g is doubly transitive, it has just two irreducible components. One of these is the component of order unity corresponding to the sum of the variables, and the other may be represented as a group of linear substitutions in the $n-1$ differences

$$x_1 - x_n, \; x_2 - x_n, \; \ldots, \; x_{n-1} - x_n.$$

It is not difficult to show that, if g is primitive, then G must be Abelian.

7. Let g be a simply transitive substitution group of prime degree p containing the operation P or

$$(x_0 x_1 \ldots x_{p-1}),$$

and let g be resolved into its irreducible components in such a way that in each of them P appears in canonical form. In the first component corresponding to the sum of the variables the multiplier of P is unity. Hence, in any other component the multipliers of P must be distinct primitive p-th roots of unity. Let

$$\xi_{it}' = \omega_{it} \xi_{it} \quad (t = 1, 2, \ldots, m_i)$$

be the operation corresponding to P in the $(i+1)$-th irreducible component $(i = 1, 2, \ldots, s)$. There is only one linear function of the variables which P replaces by ω_{it} times itself, viz.,

$$x_0 + \omega_{it}^{-1} x_1 + \omega_{it}^{-2} x_2 + \ldots + \omega_{it}^{-p+1} x_{p-1}.$$

This therefore must be ξ_{it}, and the $p-1$ ξ's of this form, corresponding to the $p-1$ primitive p-th roots of unity, are transformed linearly among themselves in s distinct sets by the irreducible components, other than the first. The coefficients in these linear substitutions are rational functions of any assigned p-th root of unity ω. If ω is replaced by any other primitive root ω', the sets of linear substitutions giving g in its reduced form is unaltered as a whole, but individual components may be interchanged.

Consider now the characteristic of P (*i.e.*, the sum of its multipliers) in one of the components, viz.,

$$\omega_{i1}+\omega_{i2}+\ldots+\omega_{im_i}.$$

When ω' is written for ω this is either unchanged or it becomes another characteristic of P. Hence, since P has no repeated multipliers, this expression must be a "period" in the cyclotomic sense; and m_i must have the same value r for each of the irreducible components, where

$$rs = p-1.$$

Also, if q is a primitive root of the congruence

$$q^r \equiv 1 \pmod{p},$$

and if $$\xi_i = x_0+\omega^i x_1+\omega^{2i}x_2+\ldots+\omega^{(p-1)i}x_{p-1},$$

the form which any operation of g takes when expressed in terms of the ξ's is

$$\xi' = c^t_{11}\xi_t + c_{12}\xi_{tq}+\ldots+c^t_{1r}\xi_{tq^{r-1}},$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$\xi_{tq^{r-1}} = c^t_{r1}\xi_t + c^t_{r2}\xi_{tq}+\ldots+c^t_{rr}\xi_{tq^{r-1}},$$

$$(t = 1, 2, \ldots, s).*$$

Since the ξ's are linear functions of the x's with powers of ω as coefficients, the coefficients c^t_{ij} in this substitution are rational functions of ω. Moreover, since by writing ω^t for ω,

$$\xi_1,\ \xi_q,\ \ldots,\ \xi_{q^{r-1}}$$

become $$\xi_t,\ \xi_{tq},\ \ldots,\ \xi_{tq^{r-1}},$$

c^t_{ij} must be the same function of ω^t as c^1_{ij} is of ω.

* The t in c^t_{ij} is not an index, but merely an affix.

Consider now any operation of g whose order, q, is different from and necessarily prime to p. Its characteristic in the t-th component,

$$c_{11}^t + c_{22}^t + \ldots + c_{rr}^t,$$

is the sum of r q-th roots of unity. But this sum is also a rational function of ω. Hence it must be a rational number, and therefore independent of t. Moreover, this sum, being a characteristic, is an algebraical integer; and therefore, being a rational number, it is a rational integer. Represent it by χ. Then $1+s\chi$ is the sum of the multipliers (*i.e.*, the number of unchanged symbols) of the operation in g. If this were zero, χ could not be integral; if it is unity, χ is zero; and, if it is greater than unity, χ is a positive integer. Hence, the only operations of g which displace all the symbols are the operations of order p, and every other operation of g leaves $1+s\chi$ symbols unchanged, where χ is zero or a positive integer. In each of the s irreducible components, other than the first, that arise from the reduction of g the characteristic of any conjugate set whose order is prime to p is then the same positive integer; and the characteristics of a conjugate set whose order is p are the s values of

$$\omega + \omega^q + \ldots + \omega^{q^{r-1}},$$

when for ω each p-th root is put in turn. Let x be the number of conjugate sets whose characteristic in any one irreducible component is

$$\omega + \omega^q + \ldots + \omega^{q^{r-1}},$$

and ν the number of operations in each set. Also, let ν_t be the number of operations of g which leave just t symbols unchanged, so that ν_t is zero, unless t is of the form $1+s\chi$. Then the equation

$$\sum_k h_k \chi_k^i = 0,$$

connecting a set of characteristics becomes

$$0 = -x\nu + \nu_{1+s} + 2\nu_{1+2s} + \ldots + r\nu_{1+rs}.$$

Also the equation $\quad \sum_k h_k \chi_k^i \chi_{k'}^j = 0 \quad (i \neq j),$

becomes

$$0 = x\nu\Sigma\,(\omega + \omega^q + \ldots + \omega^{q^{r-1}})(\omega^{-t} + \omega^{-tq} + \ldots + \omega^{-tq^{r-1}}) + \nu_{1+s} + 2^2\nu_{1+2s} + \ldots + r^2\nu_{1+rs},$$

where the sum is extended to the s different values of the product.

To the condition $i \neq j$ corresponds the condition that the "periods"

$$\omega + \omega^q + \ldots + \omega^{q^{r-1}}$$

and

$$\omega^t + \omega^{tq} + \ldots + \omega^{tq^{r-1}}$$

are distinct; and with this limitation the sum is easily shown to be equal to $-r$. Hence, eliminating $x\nu$ between the two equations,

$$r(\nu_{1+s} + 2\nu_{1+2s} + 3\nu_{1+3s} + \ldots + r\nu_{1+rs}) = \nu_{1+s} + 2^2\nu_{1+2s} + 3^2\nu_{1+3s} + \ldots + r^2\nu_{1+rs}.$$

This relation can only be satisfied by

$$\nu_{1+s} = \nu_{1+2s} = \ldots = \nu_{1+(r-1)s} = 0;$$

or, in words, the substitution group g has no operations, except identity, which leave more than one symbol unchanged. The order of such a group must be pr, where r is a factor of $p-1$, and it contains a single sub-group of order p.

A transitive group of prime degree must therefore be either doubly transitive or metacyclical.

In particular, a group of odd order and prime degree is metacyclical.

8. Let g be a group of odd order and degree p^2, where p is a prime, and suppose that g contains an operation P of order p^2. If ω is a p^2-th root of unity, the characteristic χ of P in an irreducible component of g, other than the first, is a sum of powers of ω, none being repeated. Suppose, if possible, that χ contains both ω and ω^{ν}. Since ω^{ν} is unaltered by writing ω^{1+p} for ω, χ must also contain $\omega^{1+p\nu}$, $\omega^{1+2p\nu}$, ..., $\omega^{1+(p-1)p\nu}$. If this does not exhaust all the p^2-th roots entering in χ, and if χ contains ω^t, then it must also contain $\omega^{t(1+p\nu)}$, $\omega^{t(1+2p\nu)}$, ..., $\omega^{t[1+(p-1)p\nu]}$, and $\omega^{tp\nu}$. The total number of roots of unity entering in χ would, therefore, be a multiple of $p+1$, which is impossible, since this number must be odd. Hence, that characteristic which contains ω cannot contain ω^{ν}. There must, therefore, be a characteristic in which all the multipliers are p-th roots of unity. The group therefore must be composite and isomorphic with a group in which P is represented by an operation of order p; in other words, g is imprimitive, and therefore, by the foregoing result, soluble.

A similar result may be proved for a group of odd order and degree pq, where p and q are primes, which contains a regular substitution S of order pq. Let ω and ω' be primitive p-th and q-th roots of unity. Then, if χ is the characteristic of S in one of the irreducible components of the group, ω and ω' cannot both occur in χ. For, if they did, since ω is unaltered on replacing ω' by any other primitive

q-th root, ω', ω'^2, ..., ω'^{q-1} would all occur; and this is impossible, since the roots composing $\bar{\chi}$, the inverse characteristic, must all be distinct from those composing χ. If $\omega\omega'$ and ω occur in χ, then in the characteristics derived from χ on replacing ω' by any other primitive q-th root every primitive pq-th root and every primitive p-th root occur. Hence there must then be other characteristics which consist solely of q-th roots. So also, if $\omega\omega'$ and ω' occur in χ, there must be characteristics which consist solely of p-th roots. The group is therefore composite, and isomorphic with a group in which S is represented by an operation of prime order; in other words, g is imprimitive, and therefore soluble. Hence:—

A transitive group of odd order, and degree p^2 or pq where p and q are primes, which contains a regular substitution of order equal to the degree is imprimitive and soluble.

It appears highly probable that this result may be extended to any group of odd order which contains a regular substitution of order equal to the degree of the group; but I have not yet succeeded in proving this.

III.

9. In conclusion, I propose to determine all the primitive groups of odd order and degree not exceeding 100. Dr. Miller sent me a paper four months ago for communication to the Society, in which an investigation, almost equivalent to this, was carried out for degrees not exceeding 50. The method I follow is, to a considerable extent, distinct from Dr. Miller's, and I have therefore allowed myself to repeat the investigation already given by him for degrees less than 50. This occupies but a small space, and serves to make the nature of the process clear.

In consequence of the theorem proved above for groups of prime degree, it is only necessary to consider those groups whose degrees are not primes. The method of the enumeration is as follows:—It is assumed that corresponding to a given odd number n as degree a primitive group g exists. Then a sub-group, g_0, which leaves one symbol unchanged must (p. 165) interchange the remaining $n-1$ symbols in $2m$ transitive sets, the numbers in which are equal in pairs. These numbers are represented by

$$k_1, k_2, \ldots, k_{2m}.$$

Moreover, $$2m \equiv n-1 \pmod 4.$$

Corresponding to each available value of m there will be a number of sets of values of the k's which may be written down. No k can be

unity, for the group would then be imprimitive. Now Jordan has shown (" Traité des Substitutions," p. 284) that every prime which divides the order of one of the transitive constituents of g_0 must divide the order of each transitive constituent. On this ground, a large number of the sets of values of the k's may be put aside at once as impossible, including all those cases in which two k's are equal to different primes. Moreover, the earlier determinations increase the number of cases that may be so put aside in the later ones. For instance, it is found at once that there is no transitive group of odd order, and degree 9 or 15, whose order is divisible by 7; so that 7 and 9, or 7 and 15, are incompatible values for two k's. If each k is the same prime, every transitive constituent of g_0 is a metacyclical group. In this case, g_0 is metacyclical and simply isomorphic with each of its transitive constituents. This is an immediate consequence of a theorem due to Dr. Miller (*Proc. Lond. Math. Soc.*, Vol. XXVIII., p. 534, Theorem I.). When all impossible sets of values of the k's have been put aside, the orders of possible groups g corresponding to the remainder are of known form. These are separately discussed, with a view to showing that they are soluble. If n is not the power of a prime, a primitive group of degree n is not soluble. Hence, if it is shown that a group corresponding to a given possible order is soluble, the group is non-existent when n is not the power of a prime.

The number of cases which have to be thus dealt with is not considerable, but some of the more troublesome ones may be avoided by the following considerations:—If $m = 1$, the number of irreducible components of the group is 3 (p. 174). Suppose, now, that the group contains an operation of prime order p ($\equiv 1$, mod. 4) which displaces all the symbols. If χ is its characteristic in one of the irreducible components (other than that corresponding to the sum of the symbols, for which the characteristic is unity), then χ', the conjugate of χ, is its characteristic in the other irreducible component; and $\chi+\chi'+1$, the sum of the multipliers of the operation, is zero, since the operation displaces all the symbols. Hence, χ cannot be real. But, if χ is imaginary, it must be at least a four-valued function of the p-th roots of unity; and the four corresponding irreducible representations of the group would necessarily appear among the irreducible components of g. This is impossible; and, therefore, for a group which contains a substitution, regular in all the symbols and of prime order p ($\equiv 1$, mod. 4), m cannot be unity.

I now procced to the actual enumeration. This is given in some

detail for the smaller values of n; but for the larger ones, except when special discussion is necessary, the results are merely stated.

10. $n = 9$. There is no available value of m; so that the group must be imprimitive. Its order is 3^3, 3^3, or 3^4.

$n = 15$. The only available value of m is 1, and the k's are 7, 7. The order therefore would be 15.7 or $15.7.3$, containing less than 6 prime factors. The group, therefore, would be soluble,* which is impossible. Hence the group must be imprimitive. The possible orders are 3.5, 3.5^2, 3.5^3, $3^4.5$, or $3^5.5$.

$n = 21$. Then $m = 2$, and the k's are 5, 5, 5, 5 or 3, 3, 7, 7. The second case is impossible. In the first the order would be 21.5, and, for the same reason as in the previous case, such a group cannot exist. The group is therefore imprimitive.

$n = 25$. If $m = 2$, the k's would be 5, 5, 7, 7 or 3, 3, 9, 9, each of which is impossible. If $m = 4$, the k's are all 3, and the order is 25.3. There is such a primitive group. All other groups of this degree must be imprimitive, their orders being powers of 5.

$n = 27$. If $m = 1$, the k's are 13, 13. The order, then, is 27.13 or $27.13.3$. Primitive groups of these orders exist, containing self-conjugate sub-groups of order 27. If $m = 3$, the k's are 3, 3, 3, 3, 7, 7 or 3, 3, 5, 5, 5, 5, both of which are impossible. All other groups of this order, then, are imprimitive and have powers of 3 for their order.

$n = 33$. If $m = 2$, the k's are 7, 7, 9, 9; 5, 5, 11, 11; or 3, 3, 13, 13, all of which are impossible. If $m = 4$, two k's at least are 3, which is, again, impossible. The group is therefore imprimitive.

$n = 35$. If $m = 1$, the k's are 17, 17, and the order 35.17, the product of 3 primes. There can be no such group. If m is 3 or 5, two k's must either be 3 or 5, leading, again, to impossibilities. The group is therefore imprimitive.

$n = 39$. If $m = 1$, the k's are 19, 19, and the order 39.19, $39.19.3$, or $39.19.9$; in each case the product of fewer than 6 primes. There can be no such groups. The values 3 or 5 of m lead to the same impossibilities as in the previous case. The group is, then, imprimitive.

$n = 45$. If $m = 2$, the k's are 11, 11, 11, 11; 9, 9, 13, 13; 7, 7, 15, 15;

* *Theory of Groups*, p. 367.

5, 5, 17, 17; or 3, 3, 19, 19. All of these are impossible except the first case. In that the order would be 45.11 or 45.11.5; and the group again therefore is non-existent. If m were 4 or 6, two k's would again be 3 or 5, leading to impossibilities. The group is imprimitive.

$n = 49$. If $m = 2$, the k's are 11, 11, 13, 13; 9, 9, 15, 15; 7, 7, 17, 17; 5, 5, 19, 19; or 3, 3, 21, 21; all of which are impossible. If m is 4 or 6, two k's at least must be 3 or 5, leading to impossibilities. If $m = 8$, the k's are all 3. No primitive group of order 49.3 can exist; for a non-cyclical group of order 49 has 8 sub-groups of order 7, two at least of which must be transformed into themselves by an operation of order 3. The group is therefore necessarily imprimitive.

$n = 51$. If $m = 1$, the k's are 25, 25. The order of the sub-group that keeps one symbol fixed is of the form $3^{\alpha}.5^{\beta}$, and the group must contain an operation of order 17 which displaces all the symbols. It has been shown (p. 179) that this is inconsistent with the condition $m = 1$. If $m = 3$, the k's are 7, 7, 7, 7, 11, 11; 7, 7, 9, 9, 9, 9; which are impossible, or two k's are 3 or 5, leading to impossibilities. If $m = 5$, the k's are all 5, or two at least are 3, and, if $m = 7$, two k's at least are 3. All these cases are clearly impossible. The group is therefore imprimitive.

$n = 55$. If $m = 1$, the k's are 27, 27, and the order of the sub-group that keeps one symbol fixed is of the form $3^{\alpha}.13^{\beta}$. Tho group therefore has operations of order 5 which displace all the symbols, and this is inconsistent with the condition $m = 1$. If $m = 3$, the k's are 9, 9, 9, 9, 9, 9; 7, 7, 7, 7, 13, 13; 7, 7, 9, 9, 11, 11; or two k's at least are 3 or 5. The only possibility is the first, in which case the order of the group is $3^{\alpha}.5.11$. Such a group contains a self-conjugate sub-group of order $3^{\alpha-1}$ or $3^{\alpha-2}$, and could not be expressed as of degree 55. If m is 5, 7, or 9, two k's at least are 3 or 5, leading to impossibilities. Hence the group is imprimitive.

$n = 57$. If $m = 2$, the k's are 13, 13, 15, 15; 11, 11, 17, 17; 9, 9, 19, 19; 7, 7, 21, 21; 5, 5, 23, 23; or 3, 3, 25, 25; of which 7, 7, 21, 21 is the only set giving a possible group. The order of the sub-group that keeps one symbol fixed is of the form $3^{\alpha}.7^{\beta}$, and the order of the group itself is $3^{\alpha+1}.7^{\beta}.19$. If β is unity, there must be 7.19 sub-groups of order $3^{\alpha+1}$. Any two of these must have a common sub-group of order 3^{α}, and this must be self-conjugate in a sub-group of order $3^{\alpha+1}.7$, $3^{\alpha+1}.19$, or $3^{\alpha+1}.7.19$. In either case the

group would be soluble, and it is therefore non-existent. Next suppose $\beta > 1$. The sub-groups of order 7^β are Abelian, and of degree 56. The greatest sub-group, g, common to two of them must keep $1+7x$ symbols fixed. Each of the corresponding sub-groups that keep one symbol fixed, and no others, has at least one sub-group of order 7^β which contains g. Hence, the order of the sub-group which contains g self-conjugately is divisible by $1+7x$. Now the only number of this form which is a factor of the order and not greater than the degree of the group is the degree itself; so that g is self-conjugate. Hence, again, in this case the group is non-existent. If m is 4, each k is 7, or two k's at least are 3 or 5; if $m > 4$, two k's at least are 3 or 5; and in all these cases the group is clearly non-existent. Hence the group must be imprimitive.

$n = 63$. If $m = 1$, the k's are 31, 31, and the order of the group 63.31, 63.31.3, 63.31.5, or 63.31.15. The last is the only one in which the order has 6 prime factors. Now, a group of order $3^3.5.7.31$ must contain a sub-group of order $3^3.5$, and in this a sub-group of order 5 must be self-conjugate. The group then would contain 1 or 31 sub-groups of order 5 and would be soluble. If $m = 3$, all sets of values of the k's lead to impossibilities. If m is 5, or greater, two k's at least must be 5 or 3. Hence the group must be imprimitive.

$n = 65$. Whatever m is, all sets of k's are found to lead to impossibilities. The group is imprimitive.

$n = 69$. If $m = 2$, the only possible set of values of the k's is 17, 17, 17, 17. The order of the corresponding group would be 3.17.23, containing only 3 prime factors, and therefore necessarily soluble. All other values of m lead to impossible sets of values of the k's. The group is, then, imprimitive.

$n = 75$. If $m = 1$, the k's are 37, 37, and the order is 75.37, 75.7.3, or 75.37.9. The last alone contains 6 prime factors. A group of order $3^3.5^2.37$ must have a self-conjugate sub-group of order 5 or 5^2, and is therefore soluble. This case, then, cannot occur. All other values of m lead to impossible sets of values for the k's. The group is therefore imprimitive.

$n = 77$. If $m = 2$, the only possible values of the k's are 19, 19, 19, 19. The order is, then, 77.19, 77.19.3, or 77.19.9, in each case containing less than 6 prime factors. This case cannot occur, and all

other values of m lead to impossibilities. The group, then, is imprimitive.

$n = 81$. If $m = 2$, the only possible values for the k's are 15, 15, 25, 25, and the order of the group is $3^{4+\alpha}.5^{\beta}$ $(\beta \geq 2)$. The sub-groups of order 5^{β} are Abelian and of degree 80. The greatest sub-group, g, common to two of them must keep $1+5x$ symbols fixed. Each of the corresponding sub-groups which keep one symbol fixed must contain at least one sub-group of order 5^{β} in which g is self-conjugate; and the order of the greatest sub-group containing g self-conjugately is therefore divisible by $1+5x$. The only factor of the order of the group of this form which is not greater than 81 is 81. Hence g is self-conjugate, and the group non-existent. All values of m greater than 2 lead to impossibilities except $m = 8$ and all the k's 5. There is, in fact, a primitive group of order 81.5, degree 81, and class 80. All other groups of this order are imprimitive.

$n = 85$. The only sets of values of the k's which do not lead to impossibilities are 21, 21, 21, 21; 7, 7, 7, 7, 7, 7, 21, 21; and twelve 7's. In none of these cases is the order of the group divisible by 5^2. Hence (p. 170) the group contains a self-conjugate sub-group of index 5, which is intransitive. For a primitive group this is impossible. The group is therefore imprimitive.

$n = 87$. If $m = 1$, the k's are 43, 43, and the order is 87.43; 87.43.3; 87.43.7; or 87.43.21, in each case containing less than 6 prime factors. All other values of m lead to impossible sets of values for the k's. The group, then, is imprimitive.

$n = 91$. If $m = 1$, the k's are 45, 45. The order of a transitive constituent of degree 45 cannot be divisible by 13; and the group contains operations of order 13 which displace all the symbols. This has been shown (p. 179) to be inconsistent with the condition $m = 1$. If $m = 3$, the only possible values of the k's are 15, 15, 15, 15, 15, 15 and 9, 9, 9, 9, 27, 27. If m is 5, the only possible values for the k's are ten 9's. In the two latter cases the order of the group is $3^{\alpha}.7.13$. Two sub-groups of order 3^{α} would have a common sub-group of order $3^{\alpha-2}$ at least, and this would be one of 1, 7, 13, 21, or 39 conjugate groups. Groups of degree 21 and 39 have been shown to be imprimitive. Hence this case cannot occur. In the first case the order of the group is

$3^{\alpha}.5^{\beta}.7.13$. The groups of order 5^{β} are Abelian and of degree 90. If β is unity, the group may be shown, as in the previous case, to be non-existent. If β is greater than unity, the greatest sub-group, g, common to two groups of order 5^{β} must keep $1+5x$ symbols fixed, and the greatest sub-group which contains g self-conjugately must interchange the $1+5x$ symbols transitively. The only possible value of $1+5x$ is 81; and the group can contain no sub-group with a transitive constituent of degree 81. Hence this case cannot occur. No value of m greater than 5 gives a possibility. The group, then, is imprimitive.

$n=93$. The only possible values for a set of k's are 23, 23, 23, 23. The order of the group is then 93.23 or $93.23.11$; in either case containing less than 6 primes. This case, then, is impossible, and the group is imprimitive.

$n=95$. If $m=1$, the k's are 47, 47, and the order contains less than 6 prime factors. No other value of m leads to possible values for a set of k's. The group, then, is imprimitive.

$n=99$. If $m=1$, the k's are 49, 49, and the order of the group is $3^{2+\alpha}.7^{\beta}.11$, where β is equal to or greater than 2. If β were 2, the group would contain 7 or 49 sub-groups of order $3^{2+\alpha}.11$, and would be soluble. If $\beta>2$, let g be a greatest sub-group of a group of order 7^{β} which leaves more than one symbol unchanged. Then g must leave $1+7x$ symbols unchanged; and the greatest sub-group, h, in which g is self-conjugate must interchange the $1+7x$ symbols among themselves. Moreover, the order of the constituent of h which affects these $1+7x$ symbols is divisible by 7, and no one of them is left unchanged by every operation of h. Hence, for some value of x' equal to or less than x, $1+7x'$ must be a factor of the order of the group. No such factor exists other than 99, and this case therefore is impossible. The only other possible values of a set of k's are two 7's and four 21's; eight 7's and two 21's; or fourteen 7's. In each case the order of the group is of the form $3^{2+\alpha}.7^{\beta}.11$; while the sub-groups of order 7^{β} are Abelian and of degree 98. If $\beta=1$, the group would obviously be soluble; and, if $\beta>1$, the method used for degrees 81 and 91 will show that the group cannot exist. The group is therefore imprimitive.

To sum up, the result of this enumeration shows that:—

Apart from metacyclical groups of prime degree, the only primitive groups of odd order whose degree is less than 100 are (i.) a group of degree 25 and order 25.3; (ii.) two groups of degree 27 and orders

27.13 and 27.13.3; and (iii.) a group of degree 81 and order 81.5. All groups of odd order whose degree is less than 100 are soluble.

[*Note, January 15th*, 1901.—Since the above enumeration was made, I have succeeded in showing that a group of odd order and degree $3p$, where p is an odd prime, is necessarily imprimitive. This result, of which I hope to give the proof in a subsequent paper, would materially lessen the number of cases that have to be considered.]

Conformal Space Transformations. *By* T. J. I'A. Bromwich.

Received November 6th, 1900. Read November 8th, 1900.

The basis of the following note is a very suggestive method given by the late Prof. Sophus Lie,* by which he found the expression for a rigid-body displacement, assuming only that the distance between consecutive points of the body remains constant in the displacement. A slight extension of the same method is applied here to find the conformal transformations of space; and we are led to Liouville's theorem that the most general conformal transformation is due to an inversion, a uniform magnification, and a rigid-body displacement (combined in various ways).†

Liouville's theorem was extended by Lie (in 1871) to space of any number of dimensions and to non-Euclidian spaces; Lie's methods differ entirely from Liouville's and from what follows.‡ Lie has also given a determination of the infinitesimal conformal transformations of ordinary space, by connecting points in space with circles in a

---

* *Geometrie der Berührungstransformationen*, Kap. vi., § 3, p. 206. A similar method was used by Beltrami for finding rigid-body displacements in a space of constant curvature; my authority is an abstract given in Darboux's *Bulletin* (t. xi., 1876), where it is stated that the original paper was presented to the Roman Academy (*dei Lincei*); but I have not been able to find it.

† Liouville, *Journal de Mathématiques*, t. xv., 1850, p. 103, where the theorem appears without proof; which will be found in his notes to Monge's *Applications de l'analyse à la géometrie* (Paris, 1850, p. 609). Another form of the proof is given by J. N. Haton de Goupillière (*Journal de l'Ecole Polytechnique*, t. xxv., 1867, p. 188). The theorem was rediscovered in 1872 by Clerk Maxwell (*Proc. Lond. Math. Soc.*, Vol. iv., p. 117; *Works*, Vol. ii., p. 297), whose method differs but little from Liouville's.

‡ *Math. Annalen*, Bd. v.; and *Gött. Nach.*, May, 1871.