Balbin, V.—"Tratado de Geometría Analítica," 8vo; Buenos Ayres, 1888. "Tratado de Estereometría Genética," 8vo; Buenos Ayres, 1894. "Método de los Cuadrados Mínimos," 8vo; Buenos Ayres, 1889. "Elementos de Calculo de los Cuaterniones," 8vo; Buenos Ayres, 1887. "Geometría Plana Moderna," 8vo; Buenos Ayres, 1894.

D'Ocagne, M.—"Mémoire sur les Suites Récurrentes," 4to pamphlet.

"Annales de l'Ecole Polytechnique de Delft," Tome VIII., Livr. 1–2; Leide, 1894.

"Annales de la Faculté des Sciences de Toulouse," Tome VIII., Fasc. 4; Paris, 1894.

"Journal für die reine und angewandte Mathematik," Bd. CXIV., Heft 2; Berlin, 1894.

"Transactions of the Royal Irish Academy," Vol. XXX., Parts 13 and 14; Dublin, 1894.

"Indian Engineering," Vol. XVI., Nos. 16–20; Oct. 20th–Nov. 17th.

On a Class of Groups defined by Congruences. (*Second Paper.*) *By* W. Burnside. Received December 7th, 1894. Read December 13th, 1894.

1. *Introduction.*

In a paper printed in Vol. XXV of the Society's *Proceedings*, I have discussed the groups defined by a congruence of the form

$$z' \equiv \frac{\alpha z+\beta}{\gamma z+\delta} \qquad (\text{mod } p),$$

where p is prime, and α, β, γ, δ are rational integral functions of the roots of an irreducible congruence of the n^{th} degree to the same prime modulus.

This discussion was greatly facilitated by the fact that the groups defined by a congruence of the same form in which the coefficients are ordinary integers had been already exhaustively analysed.

Now the corresponding group in two non-homogeneous variables, namely, the group defined by the congruences

$$x' \equiv \frac{\alpha x+\beta y+\gamma}{\alpha'' x+\beta'' y+\gamma''}, \quad y' \equiv \frac{\alpha' x+\beta' y+\gamma'}{\alpha'' x+\beta'' y+\gamma''} \qquad (\text{mod } p),$$

has not hitherto been the subject of any similar discussion. If the determinants of all the substitutions be unity, it is known to be a simple group of order

$$(p^2+p+1)p^3(p+1)(p-1)^2 \quad\text{or}\quad \tfrac{1}{3}(p^2+p+1)p^3(p+1)(p-1)^2,$$

according as p is congruent to -1 or 1, mod 3; but beyond this nothing is known of the type and number of the cyclical and other sub-groups contained in it.

The present paper is intended, to some extent at least, to fill this gap; and it is an almost necessary preliminary to the discussion, which I hope to undertake later, of the similar groups in which the coefficients are rational integral functions of the roots of an irreducible congruence.

The last paragraph of the paper deals shortly with the two exceptional cases of $p = 2$ and $p = 3$. Passing over these, it is clear that, since the number giving the order of the group in terms of p depends on whether p is of the form $3m+1$ or $3m-1$, these two cases require separate treatment.

The greater part of the paper is occupied with a detailed discussion of the case in which p is of the form $3m-1$. On passing on to the case in which p is of the form $3m+1$, it is found that, though the results are different in form from those of the former case, they are closely analogous to them, while the process of arriving at them is practically the same in the two cases. I have, therefore, not thought it necessary to repeat in detail all the steps of the reasoning in this second case, which would have considerably increased the length of the paper, but have simply pointed out the necessary modifications of the processes employed, and stated the results.

A limitation on the generality of the results, which is not essential, and is more apparent than real, as the subjoined footnote will show, has been introduced, in the assumption that p^2+p+1 in the one case, and $\frac{1}{3}(p^2+p+1)$ in the other, is the product of not more than two prime factors.*

p	p^2+p+1	
5	31	= prime
11	133	= 7.19
17	307	= prime
23	553	= 7.79
29	871	= 13.67
41	1723	= prime
47	2257	= 37.61
53	2863	= 7.409
59	3581	= prime
71	5113	= prime
83	6973	= 19.367
89	8011	= prime

p	$\frac{1}{3}(p^2+p+1)$	
7	19	= prime
13	61	= prime
19	107	= prime
31	331	= prime
37	469	= 7.67
43	631	= prime
61	1261	= 13.97
67	1519	= 7^2.31
73	1801	= prime
79	2107	= 7^2.43
97	3169	= prime

The results obtained may be summarized as follows.

Case 1. $p \equiv -1$ (*mod* 3).

The orders of the highest cyclical sub-groups are p^2+p+1, p^2-1, p^2-p, p, and $p-1$, and every substitution of the group occurs in some cyclical sub-group whose order is one of these numbers.

The order and type of the sub-groups within which these cyclical sub-groups are contained self-conjugately is then determined. For each cyclical sub-group of order p^2+p+1, this is a group of order $3(p^2+p+1)$, and it is shown that every sub-group containing substitutions whose orders are equal to or factors of p^2+p+1 must be contained within a sub-group of order $3(p^2+p+1)$.

Finally, every sub-group which contains no substitutions whose order is equal to or a factor of p^2+p+1 is shown to be contained either within one of two sub-groups whose orders are $p^3(p+1)(p-1)^2$ or within a sub-group of order $6(p-1)^2$. The first two of these three general types are both isomorphous with the general linear homogeneous group in two variables, while the third is isomorphous with the permutation-group of three symbols. In this third case, the form of the sub-group is limited to a few easily recognised types, and in the two former the problem of determining all possible types is not essentially distinct from the corresponding problem for the general linear group in two homogeneous variables.

Case 2. $p \equiv 1$ (*mod* 3).

The orders of the highest cyclical sub-groups are $\frac{1}{3}(p^2+p+1)$, $\frac{1}{3}(p^2-1)$, $\frac{1}{3}(p^2-p)$, p, $p-1$, and $\frac{1}{3}(p-1)$, and every substitution of the group occurs in some cyclical sub-group whose order is one of these numbers.

The other results in this case are exactly the same as in the former case if the orders of all the sub-groups there mentioned be divided by 3.

In the first case, the non-homogeneous group is holohedrically isomorphous with the homogeneous group given by

$$\left.\begin{aligned} x' &\equiv \alpha x+\beta y+\gamma z \\ y' &\equiv \alpha' x+\beta' y+\gamma' z \\ z' &\equiv \alpha'' x+\beta'' y+\gamma'' z \end{aligned}\right\} \pmod{p},$$

and advantage is taken of this to avoid entirely working with the non-homogeneous form. To give completeness to the paper I have ventured to deal at length with the reduction of a homogeneous substitution in three variables to its canonical form, although this problem has been completely treated for the general case of n variables by M. C. Jordan, in his *Traité des Substitutions.* It would, in fact, be at least as lengthy to quote M. Jordan's general results and apply them to the particular case of $n=3$, as it is to obtain the results for the particular case *ab initio.* The group which is the subject of investigation is referred to sometimes as the main group, and sometimes as the group G.

2. *On the Representation of G as a Permutation Group.*

Consider the p^3-1 quantities $Ax+By+Cz$ formed by giving A, B, C any integral values from 0 to $p-1$, with the exception of simultaneous zero values. They may be arranged in p^2+p+1 sets of $p-1$ each, according to the following scheme

$$nx, \quad n(y+kx), \quad n(z+ky+k'x),$$

$$n=1, 2, \dots p-1; \quad k, k'=0, 1, 2, \dots p-1.$$

Now any substitution of the homogeneous group which changes $Ax+By+Cz$ into $A'x+B'y+C'z$ also changes $k(Ax+By+Cz)$ into $k(A'x+B'y+C'z)$. Hence, if one member of any one of the above p^2+p+1 sets is changed by the substitution into a member of a second set, then all the members of the first are changed into the various members of the second set. If, then, each set is regarded as a single entity, and is represented by the symbol $\{Ax+By+Cz\}$, the group is isomorphous with a permutation group of the p^2+p+1 symbols

$$\{x\}, \quad \{y+kx\}, \quad \{z+ky+k'x\},$$

$$k, k'=0, 1, 2, \dots p-1.$$

Now from the enumeration of all possible types of substitution given in the succeeding section, it follows that no substitution can keep more than $p+2$ of these symbols unchanged, this maximum number occurring in the case of substitutions of the type

$$x' \equiv ax, \quad y' \equiv ay, \quad z' \equiv \beta z,$$

which leaves unchanged the symbols

$$\{x\}, \quad \{y+kx\}, \quad \{z\}, \qquad k=0, 1, 2, \dots p-1.$$

Hence the permutation-group of the p^2+p+1 symbols is holohedrically isomorphous, *i.e.*, abstractly considered, identical with the group defined by the congruences.

If now $Ax+By+Cz$, $A_1x+B_1y+C_1z$ are any two linear functions, one of which is not a multiple of the other, and if $A'x+B'y+C'z$, $A_1'x+B_1'y+C_1'z$ are any other pair satisfying the same condition, the coefficients being, as is always supposed, unless otherwise stated, real integers, it is easy to see that six other constants P, Q, R, P', Q', R' may be determined in a variety of ways, so that the congruences

$$A'x'+B'y'+C'z' \equiv Ax+By+Cz,$$

$$A_1'x'+B_1'y'+C_1'z' \equiv A_1x+B_1y+C_1z,$$

$$P'x'+Q'y'+R'z' \equiv Px+Qy+Rz,$$

give, on solution for x', y', z', a substitution of determinant unity. Hence the permutation-group is doubly-transitive, and therefore its order must be $(p^2+p+1)(p^2+p)\,m$, where m is the order of the sub-group obtained by keeping any two symbols unchanged. The type of this sub-group may be obtained at once, for, if $\{y\}$ and $\{z\}$ are the two unchanged symbols, two of the defining congruences of every one of its substitutions must be of the form

$$y' \equiv \beta y, \quad z' \equiv \gamma z.$$

The most general substitution satisfying this condition is

$$x' \equiv ax+a'y+a''z, \quad y' \equiv \beta y, \quad z' \equiv \gamma z,$$

where $$a\beta\gamma \equiv 1,$$

and conversely the totality of substitutions of this type form a group.

Now the congruence $$a\beta\gamma \equiv 1$$

has $(p-1)^2$ distinct solutions; for to a and β any values from 1 to $p-1$ may be assigned, and then γ is determinate; while a' and a'' may each have any value from 0 to $p-1$.

The number of distinct sets of defining congruences of the above type is therefore $p^2(p-1)^2$. If now the congruence

$$z^3-1 \equiv 0$$

has no real solution except unity, that is $p \equiv -1 \pmod 3$, each set of defining congruences gives a different substitution, and the order of the sub-group is $p^2(p-1)^2$.

If, however, $$z^3-1 \equiv 0$$

has three different real roots, 1, ϵ, ϵ^2, or if $p \equiv 1 \pmod 3$, the three sets of congruences

$$\begin{array}{lll} x' \equiv ax + a'y + a''z, & y' \equiv \beta y, & z' \equiv \gamma z, \\ x' \equiv \epsilon ax + \epsilon a'y + \epsilon a''z, & y' \equiv \epsilon\beta y, & z' \equiv \epsilon\gamma z, \\ x' \equiv \epsilon^2 ax + \epsilon^2 a'y + \epsilon^2 a''z, & y' \equiv \epsilon^2\beta y, & z' \equiv \epsilon^2\gamma z \end{array}$$

give the same substitution, and the order of the sub-group is $\frac{1}{3}p^2(p-1)^2$.

Hence, when p is an odd prime greater than 3, the order of the main group is

$$(p^2+p+1)(p^2+p)\,p^2(p-1)^2 \quad\text{or}\quad \tfrac{1}{3}(p^2+p+1)(p^2+p)\,p^2(p-1)^2,$$

according as p is of the form $3m-1$ or $3m+1$. When p is 2 or 3, the order of the group is given by the former of these two expressions. These two special cases are, however, exceptional, and will be considered later.

When the characteristic congruence, as defined in the next section, is irreducible, no linear function of x, y, z with real coefficients is altered into a multiple of itself; and when it is the product of a linear factor and an irreducible quadratic factor there is one such function. An inspection of the other types of substitution, which are given explicitly in the next section, shows that in other cases there may be 3, $p+1$ or $p+2$ linear functions which are changed into multiples of themselves. The substitutions of the group, therefore, when expressed as a doubly-transitive permutation group of p^2+p+1 symbols, must either permute all the symbols or must keep 1, 3, $p+1$ or $p+2$ symbols unchanged.

Case I. $p \equiv -1 \pmod 3$.

3. *On the Typical Forms of the Substitutions of G.*

Let

$$\left.\begin{aligned} x' &\equiv ax + by + cz \\ y' &\equiv a'x + b'y + c'z \\ z' &\equiv a''x + b''y + c''z \end{aligned}\right\} \pmod p,$$

be any substitution S, of determinant unity. Then

$$Ax' + By' + Cz'$$
$$= (Aa + Ba' + Ca'')\,x + (Ab + Bb' + Cb'')\,y + (Ac + Bc' + Cc'')\,z.$$

Hence $Ax+By+Cz$ is transformed into a multiple λ, of itself, if

$$\begin{aligned} A(a-\lambda)+ \quad Ba' \quad + \quad Ca'' \quad &\equiv 0, \\ Ab \quad +B(b'-\lambda)+ \quad Cb'' \quad &\equiv 0, \\ Ac \quad + \quad Bc' \quad +C(c''-\lambda) &\equiv 0, \end{aligned}$$

so that λ is given by

$$\begin{vmatrix} a-\lambda, & a', & a'' \\ b, & b'-\lambda, & b'' \\ c, & c', & c''-\lambda \end{vmatrix} \equiv 0.$$

This congruence is known as the characteristic congruence of the substitution, and it is well known that if T is any other substitution of the same form as S, then $T^{-1}ST$ has the same characteristic congruence as S;* which is the same as saying that all conjugate substitutions within the group have the same characteristic congruences. The converse of this theorem is not generally true.

If, however, the characteristic congruence has three unequal roots, whether real or imaginary, then all substitutions which have such a common characteristic congruence are conjugate substitutions. This theorem is of so great importance for what follows that I give a formal proof of it.

Suppose, then, that $\lambda_1, \lambda_2, \lambda_3$ are the three unequal roots of the above congruence. Corresponding to λ_1, the ratios $A : B : C$ are given by

$$A_1 : B_1 : C_1$$

$$:: \lambda_1^2-\lambda_1(b'+c'')+b'c''-b''c' : b\lambda_1+b''c-bc'' : c\lambda_1+bc'-b'c.$$

If, then, $\xi = x,$

$$\eta = -(b'+c'')x+by+cz,$$

$$\zeta = (b'c''-b''c')x+(c'a''-c''a')y+(a'b''-a''b')z,$$

the substitution S may be written in the form

$$\begin{aligned} \lambda_1^2\xi'+\lambda_1\eta'+\zeta' &= \lambda_1(\lambda_1^2\xi+\lambda_1\eta+\zeta), \\ \lambda_2^2\xi'+\lambda_2\eta'+\zeta' &= \lambda_2(\lambda_2^3\xi+\lambda_2\eta+\zeta), \\ \lambda_3^2\xi'+\lambda_3\eta'+\zeta' &= \lambda_3(\lambda_3^2\xi+\lambda_3\eta+\zeta), \end{aligned}$$

* Jordan, *Traité des Substitutions*, p. 98.

while every other substitution with the same characteristic equation can be represented in this form when ξ, η, ζ are replaced by three other independent linear functions of x, y, z with real integral coefficients. In particular, the above form, when ξ, η, ζ are replaced by x, y, z, may be taken as the type of all substitutions whose characteristic congruences have the three unequal roots λ_1, λ_2, λ_3.

If, now, in this form x, y, z be replaced by

$$\begin{gathered} \alpha x \;+\beta y \;+\gamma z, \\ \alpha' x \;+\beta' y \;+\gamma' z, \\ \alpha'' x+\beta'' y+\gamma'' z, \end{gathered}$$

and a corresponding change be made in the accented symbols, the resulting substitution is that represented by TST^{-1}, where T is the substitution

$$\begin{aligned} x' &\equiv \alpha x \;+\beta y \;+\gamma z, \\ y' &\equiv \alpha' x+\beta' y+\gamma' z, \\ z' &\equiv \alpha'' x+\beta'' y+\gamma'' z. \end{aligned}$$

This will not generally be a substitution of determinant unity, so that TST^{-1} is not necessarily conjugate to S within the group considered. It remains to be shown that T can be expressed in the form T_1T_2, where T_1 is a substitution of determinant unity, where T_2 is permutable with S. Writing the substitution S, for a moment, in the abbreviated form

$$X' \equiv \lambda_1 X, \quad Y' \equiv \lambda_2 Y, \quad Z' \equiv \lambda_3 Z,$$

it is evidently permutable with every substitution of the form

$$X' = \kappa_1 X, \quad Y' = \kappa_2 Y, \quad Z' = \kappa_3 Z,$$

and this latter will certainly be a substitution with real coefficients if

$$\kappa_1 = f(\lambda_1), \quad \kappa_2 = f(\lambda_2), \quad \kappa_3 = f(\lambda_3),$$

where $f(\lambda)$ is any rational function of λ with real coefficients. The determinant of this substitution is $f(\lambda_1)\, f(\lambda_2)\, f(\lambda_3)$, which may be given any value from 1 to $p-1$, by suitably choosing $f(\lambda)$. Hence, whatever the determinant n of T may be, a substitution of determinant n may be found which is permutable with S; and, since the complete set of substitutions of determinant n arise by combining any one of them with the group of substitutions of determinant unity, it follows that T can be expressed in the required form T_1T_2.

It may be pointed out that the theorem thus proved, and the proof itself, hold equally well whatever the number of variables involved may be.

The characteristic congruence may be (i) irreducible, (ii) the product of an irreducible quadratic factor and a linear factor, or (iii) the product of three linear factors; and it is clearly only in the last case that it can have equal roots. A typical form of any substitution for which the three roots are all unequal has already been found.

Suppose, now, that the congruence has two equal roots, so that the roots may be taken as α, β, β; these being real numbers. Exactly as before, two independent linear functions of x, y, z may be found (here necessarily with real coefficients) which the substitution multiplies by α and β, so that taking these to replace x and y, the substitution may be written

$$\xi' \equiv \alpha\xi,$$
$$\eta' \equiv \beta\eta,$$
$$z' \equiv \alpha''\xi + \beta''\eta + \beta z.$$

Hence $$z' + P\xi' + Q\eta' \equiv \beta z + (\alpha'' + P\alpha)\,\xi + (\beta'' + Q\beta)\,\eta.$$

If $$\beta'' \equiv 0,$$

and P is chosen so that $$P(\beta - \alpha) \equiv \alpha'',$$

then $$z' + P\xi' + Q\eta' \equiv \beta\,(z + P\xi + Q\eta);$$

so that, writing $$\zeta = z + P\xi + Q\eta,$$

the substitution takes the form

$$\xi' = \alpha\xi,$$
$$\eta' = \beta\eta,$$
$$\zeta' = \beta\zeta.$$

If, however, $\beta'' \not\equiv 0$, it is impossible to reduce the substitution to this form. In this case, if

$$P(\beta - \alpha) \equiv \alpha'',$$
$$Q \equiv 0,$$

and $$\zeta \equiv z + P\xi,$$

the substitution may be written

$$\xi' \equiv \alpha\xi, \quad \eta' = \beta\eta, \quad \zeta' \equiv \beta\left(\zeta + \frac{\beta''}{\beta}\eta\right),$$

and if, further, η be written for $\frac{\beta''}{\beta}\eta$, the form will be

$$\xi' \equiv \alpha\xi, \quad \eta' \equiv \beta\eta, \quad \zeta' \equiv \beta(\zeta+\eta).$$

Every substitution whose characteristic congruence has two equal roots must come under one of these two types, but it is immediately evident that a substitution of the one type cannot be conjugate to one of the other type. On the other hand, a repetition of the previous reasoning will show that all substitutions of the first of these two types with a common characteristic congruence are conjugate.

If the characteristic congruence has three equal roots, each must be unity. In this case one linear function of x, y, z with real coefficients can be found which is unaltered by the substitution, and, if this be denoted by ξ, the substitution can be expressed in the form

$$\begin{aligned} \xi' &\equiv \xi, \\ y' &\equiv \alpha'\xi + \beta' y + \gamma' z, \\ z' &\equiv \alpha''\xi + \beta'' y + \gamma'' z, \end{aligned}$$

where
$$\begin{vmatrix} \beta'-\lambda & \gamma' \\ \beta'' & \gamma''-\lambda \end{vmatrix} \equiv (1-\lambda)^2.$$

Now, $Py'+Qz' \equiv (P\beta'+Q\beta'')\,y+(P\gamma'+Q\gamma'')\,z+(P\alpha'+Q\alpha'')\,\xi$,

and the congruences
$$\begin{aligned} P &\equiv P\beta'+Q\beta'', \\ Q &\equiv P\gamma'+Q\gamma'' \end{aligned}$$

are, from the above equation of condition, equivalent to each other. Hence, if P and Q are determined from

$$\begin{aligned} P(\beta'-1)+Q\beta'' &\equiv 0, \\ P\alpha' \qquad + Q\alpha'' &\equiv 1, \end{aligned}$$

then
$$Py'+Qz' = Py+Qz+\xi;$$

and, when η is written for $Py+Qz$, the substitution takes the form

$$\begin{aligned} \xi' &= \xi, \\ \eta' &= \xi+\eta, \\ z' &= a''\xi+b''\eta+z. \end{aligned}$$

Here again

$$Lz'+M\xi'+N\eta' \equiv Lz+(La''+M+N)\,\xi+(Lb''+N)\,\eta,$$

and if
$$La''+N \equiv 0,$$
$$Lb'' \equiv 1,$$
$$Lz'+M\xi'+N\eta' \equiv Lz+M\xi+N\eta+\eta;$$
hence, writing
$$\zeta = Lz+M\xi+N\eta,$$
the substitution becomes
$$\xi' \equiv \xi,$$
$$\eta' \equiv \xi+\eta,$$
$$\zeta' \equiv \eta+\zeta.$$
It has been assumed that b'' is different from zero; if, however, b'' were zero, the corresponding typical form would be
$$\xi' \equiv \xi,$$
$$\eta' \equiv \xi+\eta,$$
$$\zeta' \equiv \zeta,$$
so that again, when the characteristic equation has three equal roots, there are two distinct types.

4. *On the Orders of the Substitutions of G, and on their Distribution in Cyclical Sub-Groups.*

When the characteristic congruence
$$\lambda^3-\alpha\lambda^2+\beta\lambda-1 \equiv 0$$
of a substitution is irreducible, the roots are, according to Galois' theory, of the form λ, λ^p, λ^{p^2}, where
$$\lambda^{p^2+p+1}-1 \equiv 0.$$
Now, if the real form of the substitution is
$$x' \equiv ax+by+cz,$$
$$y' \equiv a'x+b'y+c'z,$$
$$z' \equiv a''x+b''y+c''z,$$
then
$$\alpha \equiv a+b'+c'',$$
$$\beta \equiv b''c'-b'c''+ca''-c''a+a'b-ab',$$
and α and β can evidently, by suitably choosing the substitution, take all possible values. Hence all cubic congruences in which the coefficient of the leading term is unity, while the constant term is

negative unity, must occur among the characteristic congruences. Among those that are irreducible must therefore occur congruences satisfied by a primitive root of

$$\lambda^{p^2+p+1}-1 \equiv 0.$$

If $$X' \equiv \lambda X, \quad Y' \equiv \lambda^p Y, \quad Z' \equiv \lambda^{p^2} Z$$

is a substitution in its typical form corresponding to such a congruence, its order m is the least integer which satisfies

$$\lambda^m \equiv \lambda^{mp} \equiv \lambda^{mp^2},$$

and, since in the case considered $p-1$ has no factor in common with p^2+p+1, this least value of m is p^2+p+1.

Moreover, the roots of any other irreducible characteristic congruence can be clearly expressed in the form λ^r, λ^{rp}, λ^{rp^2}, so that the corresponding substitutions are r^{th} powers of substitutions of orders p^2+p+1. The orders of all substitutions, therefore, whose characteristic congruences are irreducible are either p^2+p+1 or a factor of this number.

When the characteristic congruence is resolvable into a linear factor and an irreducible quadratic factor, so that

$$\lambda^3-a\lambda^2+\beta\lambda-1 \equiv (\lambda-n)(\lambda^2-a'\lambda+\beta'),$$

where n, a', β' are real, the quadratic congruence

$$\lambda^2-a'\lambda+\beta' \equiv 0$$

may be any whatever, since a and β can take all possible values, and among such congruences must occur those satisfied by a primitive root μ of

$$\mu^{p^2-1}-1 \equiv 0.$$

The typical form of the corresponding substitution is

$$X' \equiv \mu X, \quad Y' \equiv \mu^p Y, \quad Z' \equiv \mu^{-(p+1)} Z,$$

and its order, which is the least integer m satisfying

$$\mu^m \equiv \mu^{mp} \equiv \mu^{-m(p+1)},$$

is p^2-1. The roots of every other irreducible quadratic congruence can be expressed in the form μ^r, μ^{rp}, where r is not a multiple of $p+1$; and therefore the order of every substitution whose characteristic congruence has an irreducible quadratic factor is either p^2-1 or some factor of this number which is not at the same time a factor of $p-1$.

It has been seen that all other substitutions can be reduced, without the use of imaginaries, to one of the five following typical forms:—

$$\begin{array}{lllll} \text{(i)} & x' \equiv \alpha x, & y' \equiv \beta y, & z' \equiv \gamma z, & \alpha\beta\gamma \equiv 1; \\ \text{(ii)} & x' \equiv \alpha x, & y' \equiv \beta y, & z' \equiv \beta z, & \alpha\beta^2 \equiv 1; \\ \text{(iii)} & x' \equiv \alpha x, & y' \equiv \beta y, & z' \equiv \beta (z+y), & \alpha\beta^2 \equiv 1; \\ \text{(iv)} & x' \equiv x, & y' \equiv y+z, & z' \equiv z; & \\ \text{(v)} & x' \equiv x, & y' \equiv y+x, & z' \equiv z+y. & \end{array}$$

The orders of these types can be determined by inspection. For (i) or (ii) the order is $p-1$, or a factor of $p-1$; for (iii) it is $p(p-1)$, or a factor of this number which itself contains p as a factor; for (iv) and (v) the order is p.

The result of this discussion is to show that the main group contains cyclical sub-groups whose orders are p^2+p+1, p^2-1, p^2-p, $p-1$, p, or factors of these numbers, and that every substitution of the group, except identity, is contained in some such sub-group.

I go on next to discuss the number of cyclical sub-groups of each type, and their distribution into conjugate sets.

Order p^2+p+1. The type of substitution S which will generate a cyclical sub-group of order p^2+p+1 is

$$X' \equiv \lambda X, \quad Y' \equiv \lambda^p Y, \quad Z' \equiv \lambda^{p^2} Z,$$

where

$$\begin{aligned} X &\equiv \lambda^2 x + \lambda y + z, \\ Y &\equiv \lambda^{2p} x + \lambda^p y + z, \\ Z &\equiv \lambda^{2p^2} x + \lambda^{p^2} y + z. \end{aligned}$$

If a substitution T is permutable with S, it must keep the same three (imaginary) elements unchanged, and must therefore be of the form

$$X' \equiv \kappa_1 X, \quad Y' \equiv \kappa_2 Y, \quad Z' \equiv \kappa_3 Z.$$

If, now, $\kappa_1 \equiv f(\lambda), \quad \kappa_2 \equiv f(\lambda^p), \quad \kappa_3 \equiv f(\lambda^{p^2}),$

this is a real substitution, since when expressed in terms of x, y, z the coefficients are symmetric functions of λ, λ^p, λ^{p^2}, and therefore real. But, if the κ's are not of the above form, the coefficients are unsymmetric functions of λ, λ^p, λ^{p^2} are therefore necessarily imaginary.

Now, any rational function of λ with real coefficients is some power of λ_1, a primitive root of

$$\lambda_1^{p^3-1}-1 \equiv 0$$

and if
$$\lambda_1^{r} \equiv f(\lambda),$$
$$\lambda_1^{rp} \equiv \left[f(\lambda)\right]^p \equiv f(\lambda^p),$$
and
$$\lambda_1^{rp^2} \equiv f(\lambda^{p^2}).$$

The determinant of

$$X' \equiv f(\lambda)\, X, \quad Y' \equiv f(\lambda^p)\, Y, \quad Z' \equiv f(\lambda^{p^2})\, Z$$

is then only unity when

$$\lambda_1^{r(p^2+p+1)}-1 \equiv 0,$$

or when r is a multiple of $p-1$.

But in this case $\qquad f(\lambda) \equiv \lambda_1^{\kappa(p-1)} \equiv \lambda^{\kappa},$

and therefore the only substitutions with which S is permutable are its own powers.

The substitution S, therefore, forms one of a set of $\dfrac{N}{p^2+p+1}$ conjugate substitutions, the symbol N denoting the order of the main group. Now, the only powers of S which have the same multipliers (*i.e.*, the same characteristic congruence) as S are clearly S^p and S^{p^2}, and to each set of three substitutions such as S^r, S^{rp}, S^{rp^2} contained in the cyclical sub-group generated by S, which belong to the same characteristic congruence, there corresponds such a set of $\dfrac{N}{p^2+p+1}$ conjugate substitutions. There are, therefore, in all $\frac{1}{3}(p^2+p)\dfrac{N}{p^2+p+1}$ substitutions whose orders are p^2+p+1 or one of its factors, and these form $\frac{1}{3}\dfrac{N}{p^2+p+1}$ conjugate cyclical sub-groups of order p^2+p+1, each of which must therefore be contained self-conjugately in a sub-group of order $3(p^2+p+1)$.

Order p^2-1. The type of substitution S which will generate a cyclical sub-group of order p^2-1 is

$$X' \equiv \mu X, \quad Y' \equiv \mu^p Y, \quad Z' \equiv \mu^{-(p+1)} Z,$$

where μ is a primitive root of

$$\mu^{p^2-1}-1 \equiv 0.$$

By reasoning almost identical with that used in the previous case, it may be shown that this substitution is permutable only with its own powers, so that S is one of a set of $\dfrac{N}{p^2-1}$ conjugate substitutions.

The only power of S which has the same multipliers as S is S^p, and therefore this set of conjugate substitutions consists of $\frac{1}{2}\dfrac{N}{p^2-1}$, no one of which is a power of any other, and their p^{th} powers. These $\frac{1}{2}\dfrac{N}{p^2-1}$ substitutions generate as many conjugate cyclical sub-groups of order p^2-1, each of which is therefore contained self-conjugately in a sub-group of order $2\,(p^2-1)$.

That the substitutions contained in these cyclical sub-groups, whose orders are not $p-1$ or a factor of $p-1$, are all different, may be verified by noticing that they form $\frac{1}{2}\,(p^2-p)$ different sets, each set having the same multipliers; while each set with common multipliers are shown above to contain $\dfrac{N}{p^2-1}$ conjugate substitutions. The total number of substitutions contained in the main group, then, whose orders are equal to or factors of p^2-1, without being equal to or factors of $p-1$, is $\frac{1}{2}\dfrac{Np}{p+1}$.

Order p^2-p. The type of substitution which generates a cyclical sub-group of order p^2-p is

$$x' \equiv a\,(x+y), \quad y' \equiv ay, \quad z' \equiv a^{-2}z,$$

where a is a primitive root, mod. p.

Considered as an operation of the permutation group, this is an operation belonging to the sub-group which keeps the two symbols $\{y\}$ and $\{z\}$ fixed. The general type of such sub-group is

$$x' \equiv ax+a'y+a''z, \quad y' \equiv \beta y, \quad z' \equiv \gamma z, \quad a\beta\gamma \equiv 1,$$

and, since the permutation group is doubly transitive, there are $\frac{1}{2}\,(p^2+p+1)(p^2+p)$ such sub-groups all conjugate to each other. I shall then first consider the number of cyclical sub-groups of order p^2-p contained in the sub-group that keeps $\{y\}$ and $\{z\}$ fixed, and their relation to each other. It will then be easy to extend the results to the totality of such cyclical sub-groups.

The necessary and sufficient conditions that the typical substitution of the sub-group, above written, should be of order $p(p-1)$ are that (i) α should be a primitive root, mod. p; (ii) either $\beta \equiv \alpha$ and $\alpha' \not\equiv 0$, or $\gamma \equiv \alpha$ and $\alpha'' \not\equiv 0$. Taking first $\beta \equiv \alpha$ and $\alpha' \not\equiv 0$, the n^{th} power of the substitution

$$x' \equiv ax + \alpha' y + \alpha'' z, \quad y' \equiv ay, \quad z' \equiv \alpha^{-2} z$$

is $$x' \equiv \alpha^n x + n\alpha'\alpha^{n-1} y + n\alpha''\alpha^{2-2n} z, \quad y' \equiv \alpha^n y, \quad z' \equiv \alpha^{-2n} z.$$

Hence neither of the substitutions

$$x' \equiv ax + y + Az, \quad y' \equiv ay, \quad z' \equiv \alpha^{-2} z,$$

$$x' \equiv ax + y + Bz, \quad y' \equiv ay, \quad z' \equiv \alpha^{-2} z,$$

can be a power of the other, when A and B are different; and therefore the p substitutions obtained from either of these by writing for A or B all values from 0 to $p-1$ generate p different cyclical sub-groups of order p^2-p. Moreover, every substitution of the sub-group that keeps $\{y\}$ and $\{z\}$ fixed, whose order is a factor of p^2-p without at the same time being p or a factor of $p-1$, and for which $\alpha \equiv \beta$, is contained in one of these cyclical sub-groups. For let

$$x' \equiv \alpha^s x + \alpha' y + \alpha'' z, \quad y' \equiv \alpha^s y, \quad z' \equiv \beta^{-2s} z$$

be such a substitution.

The $[s+\kappa(p-1)]^{\text{th}}$ power of

$$x' \equiv ax + y + Az, \quad y' \equiv ay, \quad z' \equiv \alpha^{-2} z$$

is $$x' \equiv \alpha^s x + [s+\kappa(p-1)]\,\alpha^{s-1} y + [s+\kappa(p-1)]\,A\alpha^{2-2s} z,$$

$$y' \equiv \alpha^s y, \quad z' \equiv \alpha^{-2s} z,$$

and κ, A can be chosen in one way so that this is the same as the given substitution.

There are, therefore, within the sub-group which keeps $\{y\}$ and $\{z\}$ fixed, p cyclical sub-groups of order p^2-p for which $\alpha \equiv \beta$, and there are therefore p more for which $\alpha \equiv \gamma$. Moreover, these cyclical sub-groups are all conjugate with the larger sub-group considered.

For it may be verified by actual calculation that the substitution

$$\left(x+\frac{B-A}{\alpha^{-2}-\alpha}z,\ y,\ z\right)^{*}$$

transforms $$(\alpha x+y+Az,\ \alpha y,\ \alpha^{-2}z)$$

into $$(\alpha x+y+Bz,\ \alpha y,\ \alpha^{-2}z)\,;$$

while $$(x,\ -z,\ y)$$

transforms $$(\alpha x+y,\ \alpha y,\ \beta z)$$

into $$(\alpha x+z,\ \beta y,\ \alpha z).$$

The sub-group which keeps $\{y\}$ and $\{z\}$ fixed contains, then, $2p$ conjugate cyclical sub-groups of order p^2-p, and the substitutions of these cyclical groups whose orders are not p or factors of $p-1$ are all different.

The $\frac{1}{2}(p^2+p+1)(p^2+p)$ conjugate sub-groups each of which keeps two symbols fixed contain in all $(p^2+p+1)(p^2+p)\,p$ conjugate cyclical sub-groups of order p^2-p. This number is equal to $\dfrac{N}{p\,(p-1)^2}$, and therefore each such cyclical sub-group is contained self-conjugately in a group of order $p\,(p-1)^2$. The type of this group is given by

$$x' \equiv \alpha x+\alpha' y,\quad y' \equiv \beta y,\quad z' \equiv \gamma z,\quad \alpha\beta\gamma \equiv 1.$$

Each of the cyclical sub-groups contains $(p-1)(p-2)$ substitutions, whose orders are neither p nor $p-1$ or one of its factors, and the main group therefore contains $\dfrac{N\,(p-2)}{p\,(p-1)}$ substitutions whose orders are factors of p^2-p, which are different from p and from $p-1$ and its factors.

Order p. There are two types of sub-group of order p, and of these I first consider those of the form

$$(x+z,\ y,\ z).$$

* Where there is no risk of confusion, the substitution

$$x' \equiv ax+by+cz,\quad y' \equiv a'x+b'y+c'z,\quad z' \equiv a''x+b''y+c''z$$

will in future be written in the abbreviated form

$$(ax+by+cz,\ a'x+b'y+c'z,\ a''x+b''y+c''z).$$

The sub-group which keeps $\{y\}$ and $\{z\}$ fixed contains p^2-1 substitutions of this type, which are given generally by

$$(x+\alpha y+\beta z,\ y,\ z),$$

where α and β take all possible values. Now, the substitution

$$(ax,\ by,\ cz)$$

will transform $\qquad (x+\alpha y+\beta z,\ y,\ z)$

into $\qquad (x+\alpha' y+\beta' y,\ y,\ z),$

if $\qquad a\alpha \equiv b\alpha',\quad a\beta \equiv c\beta'.$

Since $\qquad abc \equiv 1,$

these congruences give $\qquad a^3 \equiv \dfrac{\alpha'\beta'}{\alpha\beta},$

which, when α, β, α', β' are finite, always has a real solution, in the case $p \equiv -1$ (mod. 3), which is under consideration. On the other hand,

$$(x,\ z,\ -y)$$

transforms $\qquad (x-y,\ y,\ z)$

into $\qquad (x+z,\ y,\ z),$

and therefore the whole set of p^2-1 substitutions are conjugate within the main group. The p^2 substitutions give $p+1$ cyclical sub-groups contained in the sub-group which keeps $\{y\}$ and $\{z\}$ fixed. Every sub-group keeping two symbols fixed similarly contains $p+1$ such cyclical sub-groups; but these are not all distinct, for the cyclical sub-groups occurring in the groups keeping any two of the $p+1$ symbols $\{y\}$, $\{z\}$, $\{y+nz\}$, $n = 1, 2, \dots p-1$, are evidently all the same. Hence the main group contains $\dfrac{\frac{1}{2}(p^2+p+1)(p^2+p)}{\frac{1}{2}(p+1)p}(p+1)$ such cyclical sub-groups, which are all conjugate to each other, as also are all their substitutions. This number, expressed as before, is $\dfrac{N}{p^3(p-1)^2}$, so that each such sub-group is contained self-conjugately in a sub-group of order $p^3(p-1)^2$. Thus the cyclical sub-group generated by

$$(x,\ y+z,\ z)$$

is self-conjugate within the group given by

$$(ax+by+cz,\ b'y+c'z,\ c''z),\quad ab'c'' \equiv 1.$$

The total number of substitutions of order p and of this first type contained in the main group is $\dfrac{N}{p^3(p-1)}$.

The second type of substitution of order p is

$$(x+y,\ y+z,\ z).$$

The n^{th} power of this substitution is

$$\left(x+ny+\tfrac{1}{2}n(n-1)z,\ y+nz,\ z\right),$$

and the conditions that the substitution should be transformed into its n^{th} power by

$$(ax+by+cz,\ a'x+b'y+c'z,\ a''x+b''y+c''z)$$

are easily found to be

$$a' \equiv a'' \equiv b'' \equiv 0, \quad an \equiv b', \quad b'n = c'', \quad c' \equiv bn+\tfrac{1}{2}an(n-1).$$

These give

$$a \equiv \frac{1}{n}, \quad b' \equiv 1, \quad c'' = n, \quad c' \equiv bn+\tfrac{1}{2}(n-1).$$

Hence the sub-group given by all substitutions of the form

$$\left(\frac{1}{n}x+by+cz,\quad y+\left[bn+\tfrac{1}{2}(n-1)\right]z,\quad nz\right)$$

is the sub-group of greatest order which contains the cyclical sub-group generated by

$$(x+y,\ y+z,\ z)$$

self-conjugately. Since b, c may take all possible values, and n all values except zero, the order of this sub-group is $(p-1)p^2$. Hence the cyclical sub-group is one of a conjugate set of $\dfrac{N}{(p-1)p^2}$ contained in the main group.

By transforming $(x+y, y+z, z)$ with a substitution which keeps $\{z\}$ fixed, it may be seen at once that all possible sub-groups of the type considered may be obtained for which $\{z\}$ is unchanged; and hence the conjugate set of sub-groups just obtained contains all sub-groups of the order p and of the second type.

The substitutions of these groups are necessarily all different, and all conjugate with each other; and the number of such substitutions contained in the main group is $\dfrac{N}{p^2}$.

Order $p-1$. The cyclical sub-groups of order $p-1$, unlike the sub-groups of other orders, do not form a single conjugate set. If a is any primitive root, mod. p, a^r, a^s, $a^{-(r+s)}$ will be the multipliers of a substitution of order $p-1$, if and only if the greatest common factor of r and s is prime relatively to $p-1$. The cyclical sub-group generated by $(a^r x, a^s y, a^{-(r+s)} z)$ will contain $\phi(p-1)$ substitutions of order $p-1$, where $\phi(n)$ is the symbol used in the theory of numbers for the number of integers less than and prime to n. Two of these substitutions will have the same multipliers if the set of quantities a^{mr}, a^{ms}, $a^{-m(r+s)}$ is identical with the set a^r, a^s, $a^{-\,r+s)}$ for some value of m different from unity; and it may be at once verified that the only values of r, s, and m for which this can be the case are given by

$$r+s \equiv 0, \quad m \equiv p-2 \quad (\text{mod. } p-1).$$

Hence in a cyclical substitution arising from a substitution with the multipliers, a, a^{-1}, 1, the sets of multipliers of the substitutions of order $p-1$ are the same in pairs, and the sub-group contains only $\tfrac{1}{2}\phi(p-1)$ such sets of multipliers; whereas in every cyclical sub-group of order $p-1$ which arises from a substitution with multipliers no one of which is unity the sets of multipliers of the $\phi(p-1)$ substitutions of order $p-1$ are all different.

Now, the number of ways in which two distinct symbols r, s, less than $p-1$, may be chosen so that their highest common factor is prime relatively to $p-1$, excluding simultaneous zero values, is

$$\phi(p-1)\,\psi(p-1),\text{*}$$

where
$$\psi(p-1) = (p-1)\left(1+\frac{1}{q_1}\right)\left(1+\frac{1}{q_2}\right)\ldots,$$

$q_1, q_2, \ldots$ being the different prime factors of $p-1$.

If $r, s, -(r+s)$, the indices of a set of multipliers of a substitution of order $p-1$, are all different, then

$$\begin{array}{lll} r,\, s\,; & r,\, -(r+s)\,; & s,\, -(r+s)\,; \\ s,\, r\,; & -(r+s),\, r\,; & -(r+s),\, s \end{array}$$

will appear in the above solution as six distinct ways of choosing r and s, which, however, all lead to the same set of multipliers.

If, on the other hand, r, r, $-2r$ are the multipliers of a substitution of order $p-1$, then

$$r,\, r\,; \quad r,\, -2r\,; \quad -2r,\, r$$

* *Cf.* Jordan, *Traité des Substitutions*, p. 96.

will appear as three distinct ways of choosing r and s, which again all lead to the same set of multipliers.

In this latter case, r must be prime to $p-1$, and may therefore have $\phi(p-1)$ values. There are, then, $3\phi(p-1)$ such solutions of the problem of choosing r and s, leading to $\phi(p-1)$ sets of multipliers. Subtracting these $3\phi(p-1)$ solutions from the total number, there remain

$$\phi(p-1)\left[\psi(p-1)-3\right]$$

solutions, leading to $\frac{1}{6}\phi(p-1)\left[\psi(p-1)-3\right]$

further sets of multipliers; and the number of distinct sets of multipliers is therefore in all

$$\tfrac{1}{6}\phi(p-1)\left[\psi(p-1)+3\right].$$

Of these sets of multipliers $\frac{1}{2}\phi(p-1)$ occur in a cyclical sub-group arising from a substitution whose multipliers are a, a^{-1}, 1; while it has been seen that the sets of multipliers of the substitutions of order $p-1$ in any other cyclical sub-group of this order are all distinct. Hence there are $\frac{1}{6}\psi(p-1)$ further types of cyclical sub-group of order $p-1$, each type containing an entirely distinct collection of sets of multipliers of the substitutions of order $p-1$ from all the others. The total number of types of cyclical sub-group of order $p-1$ is therefore $\frac{1}{6}\psi(p-1)+1$.

The cyclical sub-group arising from the substitution

$$(ax,\ a^{-1}y,\ z)$$

is transformed into itself by an operation which transforms the substitution itself into its $(p-2)^{\text{th}}$ power, that is, into

$$(a^{-1}x,\ ay,\ z).$$

The general form of an operation which will effect this transformation is

$$(ay,\ bx,\ cz)\quad abc\equiv -1,$$

and the group that arises by combining together these substitutions in all possible ways, containing all substitutions of the above forms together with those of the form

$$(a'x,\ b'y,\ c'z)\quad a'b'c'\equiv 1,$$

is of order $2(p-1)^2$. Hence this type of cyclical sub-group of order

$p-1$ is self-conjugate in a group of order $2(p-1)^2$, and therefore forms one of a set of $\frac{N}{2(p-1)^2}$ conjugate sub-groups. The remaining types contain no substitutions which can be transformed into powers of themselves, and hence, to find the sub-groups within which they are self-conjugate, it is only necessary to find the substitutions permutable with them. When the multipliers of the generating substitution $(a^r x, a^s y, a^{-(r+s)} z)$, so that $r \pm s \not\equiv 0$, it is seen at once that the only substitutions with which the cyclical sub-group is permutable are those of the form

$$(ax,\ by,\ cz) \quad abc \equiv 1,$$

forming a group of order $(p-1)^2$. Each of the $\frac{1}{6}\psi(p-1)-1$ types, coming under this head, is therefore self-conjugate in a group of order $(p-1)^2$, and each forms one of a set of $\frac{N}{(p-1)^2}$ conjugate sub-groups.

The remaining type of cyclical sub-group arises from a substitution of the form

$$(ax,\ ay,\ a^{-2}z).$$

The conditions that this substitution should be permutable with

$$(ax+by+cz,\quad a'x+b'y+c'z,\quad a''x+b''y+c''z)$$

are $$c \equiv c' \equiv a'' \equiv b''' \equiv 0,$$

and the order of the sub-group so defined is $p(p+1)(p-1)^2$. This remaining type therefore forms one of a set of $\frac{N}{p(p+1)(p-1)^2}$ conjugate sub-groups.

It would not be easy to determine, from the above enumeration of the sets of conjugate groups of order $p-1$, the total number of substitutions contained in the main group whose orders are equal to or factors of $p-1$, but the number in question may be obtained independently in the following manner.

The sub-group of order $(p-1)^2$ whose type is

$$(ax,\ by,\ cz) \quad abc \equiv 1$$

is self-conjugate within a group of order $6(p-1)^2$ obtained by combining the group itself with all those substitutions which permute $\{x\}$, $\{y\}$, $\{z\}$ among themselves. It forms therefore one of

$\frac{N}{6(p-1)^2}$ conjugate sub-groups. Any one of the $(p-1)^2$ substitutions belonging to the original group which keeps three symbols only fixed appears in that group only; but a substitution of the form (ax, ay, cz) appears in each of the $\frac{1}{2}(p+1)p$ conjugate groups which keeps $\{z\}$ and any pair of the symbols $\{x\}$, $\{y\}$, $\{x+\kappa y\}$, $\kappa = 1, 2, \dots p-1$ fixed. Now, of the $(p-1)^2-1$ substitutions in the original group, other than identity, $3(p-2)$ keep $p+2$ symbols fixed. Hence the total number of substitutions in the main group whose orders are equal to or factors of $p-1$ is

$$\frac{N}{6(p-1)^2}\left[(p-1)^2 \quad 1-3(p-2)+\frac{3(p-2)}{\frac{1}{2}p(p+1)}\right],$$

or
$$\frac{N(p-2)}{6(p-1)^2}\left[p-3+\frac{6}{p(p+1)}\right].$$

As a partial verification of the accuracy of the enumeration that has now been completed of the number of substitutions of each different order that are contained in the main group, it may be observed that the sum of

$\frac{N(p^2+p)}{3(p^2+p+1)}$, the number of substitutions whose orders are equal to or factors of p^2+p+1,

$+ \frac{Np}{2(p+1)}$, the number whose orders are equal to or factors of p^2-1, without being factors of $p-1$,

$+ \frac{N(p-2)}{p(p-1)}$, the number whose orders are equal to or factors of p^2-p, while different from p, $p-1$, or its factors,

$+ \frac{N}{p^3(p-1)}$, the number whose orders are p, and which are of the type $(x+z, y, z)$,

$+ \frac{N}{p^2}$, the number whose orders are p, and which are of the type $(x+y, y+z, z)$,

$+ \frac{N(p-2)}{6(p-1)^2}\left[p-3+\frac{6}{p(p+1)}\right]$, the number whose orders are equal to or factors of $p-1$,

$+ 1$, the identical substitution,

is N, as it should be.

5. *On the Sub-Groups of G which contain Substitutions of Order p.*

Before going on to a general discussion of the various types of sub-group contained in the group of substitutions considered, it will be convenient to begin by obtaining certain results relative to sub-groups whose order is divisible by p, as these will materially shorten certain portions of the subsequent discussion.

Suppose first that a sub-group g of order m contains a substitution of the type
$$(x+y,\ y+z,\ z).$$

If g contains the cyclical sub-group arising from this substitution self-conjugately, m must be equal to or a factor of $(p-1)\,p^2$. If this is not the case, and if at the same time m is not divisible by p^2, g must contain either $\frac{m}{p}$ or $\frac{m}{(p-1)\,p}$ conjugate sub-groups of order p. In the latter case, each will be self-conjugate within a sub-group formed by all substitutions of the type (p, 76)
$$\left\{\frac{1}{n}x+by,\ y+\left[bn+\tfrac{1}{2}(n-1)\right]z,\ nz\right\},$$
and no two sub-groups of this type have a common substitution except identity. Hence, in this case, g will contain only $\frac{m}{(p-1)\,p}$ substitutions other than those contained in the $\frac{m}{(p-1)\,p}$ sub-groups of order $(p-1)\,p$; while in the former case g contains only $\frac{m}{p}$ substitutions whose orders are different from p. It follows that in either case g can contain no substitutions whose orders are factors of p^2+p+1 or $p+1$; and therefore that m is a factor of $(p-1)^2p$. But from this it is easily seen that g must contain the sub-group of order p self-conjugately. Hence, when the sub-group of order p is not contained self-conjugately in g, m must be divisible by p^2.

Suppose next that the sub-group contains a substitution of the type
$$(x+y,\ y,\ z).$$

If the cyclical sub-group arising from this substitution is contained self-conjugately in g, then m must be equal to or a factor of $p^3\,(p-1)^2$. If this is not the case, g contains substitutions conjugate to the given one. Any such substitution has among the $p+1$ symbols unchanged by it at least one in common with those unchanged by the given substitution; for, if
$$\{ax+by+cz\}\quad\text{and}\quad\{a'x+b'y+c'z\}$$

are two of the unchanged symbols, then

$$\{(a'b-ab')\,y+(a'c-ac')\,z\}$$

is unchanged by both cyclical sub-groups.

If now the notation be changed so that $\{z\}$ is a common unchanged symbol for the two groups, while the first is generated by

$$(x+Ay+Bz,\ y,\ z),$$

which involves no loss of generality, three different cases may occur.

Firstly, all $p+1$ unchanged symbols may be the same for the two groups, so that the second is generated by

$$(x+A'y+B'z,\ y,\ z).$$

The two then generate a group of order p^2, given by all substitutions which are of the type

$$(x+\alpha y+\beta z,\ y,\ z)\ ;$$

and this, moreover, interchanges p^2 symbols transitively.

When this is not the case, the second cyclical sub-group must be generated by a substitution of the form

$$\begin{aligned} z' &\equiv z, \\ x'+\alpha y' &\equiv x+\alpha y, \\ x'+\beta y' &\equiv x+\beta y+z, \end{aligned}$$

or by one of the form

$$\begin{aligned} z' &\equiv z, \\ x'+\alpha y' &\equiv x+\alpha y, \\ x'+\beta y' &\equiv x+\beta y+x+\alpha y. \end{aligned}$$

In the first of these alternative cases, the second substitution may be written in the form

$$(x+\gamma z,\ y+\delta z,\ z),$$

where

$$(\beta-\alpha)\,\gamma\equiv-\alpha,\quad(\beta-\alpha)\,\delta\equiv1.$$

The two substitutions then generate a sub-group of order p^2 or p^8, according as A is or is not zero.

In the second alternative case, the second substitution is

$$(ax+by,\quad cx+dy,\quad z),$$

where

$$a\equiv\frac{\beta-2\alpha}{\beta-\alpha},\quad b\equiv\frac{-\alpha^2}{\beta-\alpha},\quad c\equiv\frac{1}{\beta-\alpha},\quad d\equiv\frac{\beta}{\beta-\alpha},$$

so that

$$a+d\equiv2.$$

The two substitutions $(x+Ay+Bz,\ y,\ z)$

and $$(ax+by,\ cx+dy,\ z),\qquad a+d\equiv 2,\quad ad-bc\equiv 1,$$

then generate either the general linear group in two homogeneous variables of determinant unity, or a group within which it is contained.

Hence, again, in this case, with a single exception, the order m of the sub-group must be divisible by p^2; while, in the exceptional case, the sub-group g must itself contain, as a sub-group, a group of order $p(p^2-1)$, isomorphous with the general linear group in two homogeneous variables. This latter sub-group, keeping one symbol fixed, interchanges the remainder in two transitive sets of p^2-1 and $p+1$.

Returning now to the first case, and putting on one side those groups which contain a sub-group of order p self-conjugately, it has been seen that the order m of a group g, containing a substitution of the type

$$(x+y,\ y+z,\ z),$$

that is, a substitution of order p that keeps only one symbol fixed, must be divisible by p^2. The sub-group of order p^2 contained in g is of the type that contains

$$(x+y,\ y+z,\ z)$$

self-conjugately; and this is given by all substitutions of the form

$$(x+\alpha y+\beta z,\ y+\alpha z,\ z).$$

The group therefore contains substitutions of the type

$$(x+z,\ y,\ z),$$

and, unless the cyclical sub-group arising from this is contained self-conjugately (which cannot be the case when a factor of p^2+p+1 or an odd factor of $p+1$ divides m), the preceding investigation again applies here.

It follows, therefore, that if a sub-group contains, not self-conjugately, a sub-group of order p which keeps only one symbol fixed, its order must be divisible either by p^3 or by $p^2(p^2-1)$; for either it must contain two distinct types of sub-group of order p^2, or it must contain sub-groups of orders p^2 and $p(p^2-1)$.

Suppose now that the sub-group g contains operations displacing all the symbols. Then, (i) if it contain a sub-group of type

$$(x+\alpha y+\beta z,\ y,\ z)$$

which displaces the symbols in two transitive sets of p^2 and $p+1$, it must contain a sub-group conjugate to this, displacing the symbols in two other sets. Hence g must be transitive in the p^2+p+1 symbols. Also the conjugate sub-group of order p^3 must have one undisplaced symbol in common with the given sub-group of order p^2, and, if, again changing the notation, this be taken for z, the two sub-groups are of the forms

$$(x+\alpha y+\beta z,\ \ y,\ \ z)$$

and

$$z' \equiv z,$$

$$x'+Ay' \equiv x+Ay,$$

$$x'+By' \equiv x+By+\alpha\,(x+Ay)+\beta z.$$

The latter contains the operation

$$(x-z,\ \ y+z,\ \ z),$$

and this, taken with the former sub-group, generates a sub-group of order p^3.

Again, (ii) if g contain a sub-group, order p^2, of the type

$$(x+\alpha z,\ \ y+\beta z,\ \ z),$$

it will contain a conjugate sub-group with a different undisplaced symbol. Now, the given sub-group may be written in the form

$$ax' +by' +cz' \equiv ax +by +cz +\alpha' z,$$

$$a'x'+b'y'+c'z' \equiv a'x+b'y+c'z+\beta' z,$$

$$z' \equiv z\,;$$

and, therefore, the conjugate sub-group may be taken without loss of generality in the form

$$(x,\ \ y+\alpha x,\ \ z+\beta x).$$

The two conjugate sub-groups therefore contain the two substitutions

$$(x+z,\ \ y,\ \ z\ ),$$

$$(\ x,\ \ y,\ \ z+x),$$

which, as has been seen, generate a sub-group of order $p\,(p^2-1)$, and also the two substitutions

$$(x+z,\ \ y,\ \ z),$$

$$(\ x,\ \ y+x,\ \ z),$$

which generate a sub-group, order p^2, of different type from

$$(x+\alpha z,\ \ y+\beta z,\ \ z).$$

Hence g, containing two sub-groups of order p^2 of different types, must contain sub-groups of order p^3, and its order must be divisible by $p^3(p^2-1)$. It is also again necessarily transitive in the p^2+p+1 symbols.

Lastly, (iii) if g contain the sub-group of order $p(p^2-1)$ arising from

$$(x+y,\quad y,\quad z)$$

and

$$(\ x,\quad x+y,\quad z),$$

which displaces the symbols in two transitive sets of p^2-1 and $p+1$, keeping one fixed, it contains a conjugate sub-group, displacing the symbols in two other sets, and it is therefore transitive in all the symbols.

The order of the group is therefore at least $(p^2+p+1)\,p\,(p^2-1)$. Now, no operation displacing all the symbols is permutable with an operation of order p, and hence the sub-group g would contain at least $(p^2+p+1)(p+1)$ conjugate sub-groups of order p. But the sub-group arising from

$$\begin{array}{ccc}(x+y, & y, & z), \\ (\ x, & y+x, & z)\end{array}$$

contains only $p+1$ sub-groups of order p, and each of these is common to $p+1$ of the p^2+p+1 such conjugate sub-groups. Hence each sub-group of g which keeps one symbol fixed must contain further substitutions of order p, beyond those contained in the sub-group of order $p(p^2-1)$ of the above type. Among the substitutions keeping $\{z\}$ fixed, there must therefore be, besides the simultaneous types

$$\begin{array}{ccc}(x+y, & y, & z), \\ (\ x, & x+y, & z),\end{array}$$

simultaneous types either of the form

$$\begin{array}{ccc}(x+y, & y, & z), \\ (x+z, & y, & z),\end{array}$$

or of the form

$$\begin{array}{ccc}(x+y, & y, & z), \\ (\ x, & y+z, & z).\end{array}$$

In either case the order of the sub-group must be divisible by p^3; since, as in former cases, there will be two distinct types of sub-group of order p^2.

The final result of this discussion of sub-groups containing operations of order p may be stated as follows:—

If a sub-group contains substitutions displacing all the symbols (*i.e.*, substitutions whose orders divide p^2+p+1), and if it also contain substitutions of order p, the sub-group must be transitive in all the p^2+p+1 symbols, and its order must be divisible by p^3.

In the proof of this result it is first shown that, if the sub-group g contain a cyclical sub-group of order p, not self-conjugate, it must contain sub-groups of one of the three types,

$$\text{(i)}\ (x+\alpha y+\beta z,\quad y,\quad z),$$
$$\text{(ii)}\ (x+\alpha z,\quad y+\beta z,\quad z),$$
$$\text{(iii)}\ \left\{\begin{array}{lll}(x+y, & y, & z)\\ (\ x, & x+y, & z)\end{array}\right\}.$$

Now, if the substitutions of g do not all keep $\{z\}$ fixed, there must, when the sub-group contained in g is of types (ii) and (iii), be conjugate sub-groups, and then the reasoning already given shows that g must be transitive, and of order divisible by p^3, independently of the additional supposition that it contains substitutions displacing all the symbols.

The same is true when g contains a sub-group of type (i), unless the symbols $\{y\}$, $\{z\}$, $\{y+\kappa z\}$, $\kappa = 1, 2, \dots p-1$, form a single transitive set of symbols for the group g.

Hence the result may also be stated in the following form:—

If the substitutions of a sub-group g do not all keep some one symbol fixed, and if the order of g is divisible by p, then g must be transitive in the complete set of p^2+p+1 symbols, and its order must be divisible by p^3, unless it interchanges the symbols in two transitive sets of p^2 and $p+1$.

The most general group of this latter type is evidently one of order $p^3(p-1)^2(p+1)$, whose substitutions are of the type

$$(ax+by+cz,\quad b'y+c'z,\quad b''y+c''z),$$
$$a\,(b'c''-b''c')\equiv 1,$$

which contains as a self-conjugate sub-group

$$(x+\alpha y+\beta z,\quad y,\quad z).$$

6. *On the Transitive Sub-Groups of G.*

I go on now to consider the sub-groups which contain cyclical sub-groups of order p^2+p+1. Such sub-groups are necessarily transitive.

Let g denote one of them, and let $(p^2+p+1)\,m$ be its order. Then, if the cyclical sub-group of order p^2+p+1 is contained self-conjugately in g, it has been seen that m must be 3.

If not, g contains either $(p^2+p)\,m$ or $(p^2+p)\,\frac{m}{3}$ operations displacing all the symbols. In the former case there are only m substitutions left over, and therefore the sub-group of order m keeping one symbol fixed is contained self-conjugately in g, and must consist of the identical substitution only, so that m is 1.

If m is not unity, it must be divisible by 3, and the number of substitutions in g which do not displace all the symbols is

$$(p^2+p+1)\,m-\tfrac{1}{3}p\,(p+1)\,m.$$

Now, with the exception of identity, no substitution is permutable with a substitution of order p^2+p+1, so that each of the remaining operations, except identity, forms one of a conjugate set, whose number is a multiple of p^2+p+1. It follows that

$$\frac{m}{3}\equiv 1 \quad (\text{mod. } p^2+p+1),$$

or

$$m=3\left[1+\lambda\,(p^2+p+1)\right],$$

where λ is an integer.

Now, m is a factor of $p^3\,(p-1)^2\,(p+1)$, and it has been seen that, if m contains p as a factor, it must contain p^3.

Hence (i), if m is not a multiple of p,

$$3\left[1+\lambda\,(p^2+p+1)\right]$$

is a factor of

$$(p-1)^2\,(p+1),$$

i.e., of

$$3\left[1+\frac{p-2}{3}\,(p^2+p+1)\right];$$

and therefore of

$$3\left(\frac{p-2}{3}-\lambda\right),$$

which is impossible unless this last expression is zero.

In this case, then,

$$\lambda=\frac{p-2}{3},$$

and

$$m=(p-1)^2\,(p+1).$$

If (ii) m is a multiple of p^3, it follows at once that

$$\lambda=p-1,$$

and

$$m=3p^3.$$

Hence the only possible orders for groups containing substitutions of order p^2+p+1, not self-conjugately, are

$$(p^2+p+1)(p-1)^2\,(p+1),$$

and

$$(p^2+p+1)\,3p^3$$

It is immediately obvious that no sub-group of the latter order can exist. For its sub-groups that keep one symbol fixed would be of order $3p^3$, and these would necessarily contain groups of order p^3 as self-conjugate sub-groups. But a group of order p^3 is self-conjugate only within one of order $p^3\,(p-1)^2$, and 3 is not a factor of $p-1$.

If a transitive sub-group of order $(p^2+p+1)(p-1)^2\,(p+1)$ exists, its sub-group keeping one symbol fixed is of order $(p-1)^2\,(p+1)$. Suppose that this sub-group contains m_1, m_3, m_{p+2} substitutions keeping respectively just 1, 3, and $p+2$ symbols fixed. Now, each substitution keeping r symbols fixed belongs to r different sub-groups keeping one symbol fixed. Hence the total number of different substitutions belonging to the p^2+p+1 conjugate sub-groups which each keep one symbol fixed is

$$1+(p^2+p+1)\left(m_1+\frac{m_3}{3}+\frac{m_{p+2}}{p+2}\right).$$

Neither 3 nor $p+2$ can be a factor of p^2+p+1, and therefore $\frac{m_3}{3}$ and $\frac{m_{p+2}}{p+2}$ must be integers. Writing n_3 and n_{p+2} for them, and n_1 for m_1,

$$(p-1)^2\,(p+1) = 1+n_1+3n_3+(p+2)\,n_{p+2},$$

and

$$(p^2+p+1)(p-1)^2\,(p+1)-\tfrac{1}{3}\,(p^2+p)(p-1)^2\,(p+1)$$
$$= 1+(p^2+p+1)(n_1+n_3+n_{p+2}),$$

the two sides of the latter equation representing two ways of counting all the substitutions in the sub-groups which do not displace all the symbols. Combining these equations, there results

$$2n_3+(p+1)\,n_{p+2} = \tfrac{1}{3}p\,(p+1)(p-2),$$

whence

$$(p-1)\,n_3 = (p+1)\left[(p-1)(\tfrac{2}{3}p^2+p)-n_1\right],$$

$$(p-1)\,n_{p+2} = 2n_1-p^2\,(p-1).$$

Now, it is, on the other hand, easy to show that the sub-group can contain no substitution that keeps $p+2$ symbols fixed.

For any such substitution

$$S,\quad\text{or}\quad(\alpha x,\ \alpha y,\ \beta z),$$

cannot be contained self-conjugately, and a substitution Σ conjugate to S and keeping $\{z\}$ fixed is necessarily of the form

$$(\alpha x+\gamma z,\quad \alpha y+\gamma' z,\quad \beta z),$$

so that $S\Sigma^{-1}$ would be of order p, contrary to supposition.

Hence $$n_{p+2}=0;$$
and therefore $$n_1=\tfrac{1}{2}p^2(p-1).$$

But, if the greatest cyclical sub-group, whose order is a factor of p^2-1, contained in the sub-group considered, is of order $\frac{p+1}{q_1}\frac{p-1}{q_2}$, where $\frac{p-1}{q_2}$ is the greatest factor of $p-1$ dividing this number, it contains $\left(\frac{p+1}{q_1}-1\right)\frac{p-1}{q_2}$ substitutions that keep only one symbol fixed, and, together with its conjugate sub-groups, it must contain $\epsilon(p-1)^2(p+1-q_1)$ such substitutions, where ϵ is 1 or $\frac{1}{2}$. The total number of such substitutions contained in the sub-group is the sum of a number of such terms as this, and is therefore divisible by $\frac{1}{2}(p-1)^2$. Hence the above found value for n_1 is impossible, and a sub-group of the type supposed does not exist. The only sub-groups, therefore, which contain substitutions of order p^2+p+1 are those already found of order $3(p^2+p+1)$.

Before going on to the intransitive sub-groups, there is one other type of transitive sub-group, the possibility of which it is necessary to consider. There might be a sub-group g, of order $(p^2+p+1)m$, containing no substitutions of order p^2+p+1. Here, and in dealing with the intransitive sub-groups, I make the limitation, already referred to in the introduction, that p^2+p+1 is the product of not more than two prime factors, which will be represented by p_1 and p_2. If, now, g contains no substitutions of order p_1p_2, it must contain $\epsilon p_2 m$ and $\epsilon' p_1 m$ conjugate sub-groups of orders p_1 and p_2 respectively, where ϵ, ϵ' are either 1 or $\frac{1}{3}$. If they are not both $\frac{1}{3}$, there would be a number of substitutions in g, displacing all the symbols, greater than the order of the group, and this is impossible.

Hence, since all the substitutions of these [sub-groups are distinct, the group contains $\frac{1}{3}(p_1-1)p_2m+\frac{1}{3}(p_2-1)p_1m$ substitutions displacing all the symbols, leaving over

$$\tfrac{1}{3}(p_1p_2+p_1+p_2)$$

substitutions.

Suppose, now, first that m is not divisible by p; and, if possible, let the sub-group contain a substitution S of the type

$$(-x,\ -y,\ z).$$

If S is transformed into S' by any substitution which keeps $\{z\}$

unchanged, $S'S^{-1}$ would be a substitution of order p. Hence the sub-group either contains no substitutions of this type, or else such a substitution must be permutable with all the substitutions of the sub-group which keep $\{z\}$ unchanged. Now, it is substitutions of the type S which transform substitutions of order p^2-1 into their own p^{th} powers.

Hence, g must contain at least $\frac{2}{3}p_1 p_2 m$ substitutions that keep one symbol only fixed, or else that sub-group of g which keeps $\{z\}$ unchanged must contain a substitution of type S self-conjugately. On the former supposition the number of substitutions of g which keep either one or no symbols unchanged would exceed the order of g; and this is impossible. Passing to the latter supposition, the general type of substitution which is permutable with S is

$$(ax+by,\ a'x+b'y,\ c''z), \qquad (ab'-a'b)\,c'' \equiv 1,$$

and that sub-group of g which keeps $\{z\}$ unchanged must be contained within this group. Now, this group is identical with the general linear group in the homogeneous variables, and therefore any sub-group of it which contains distinct cyclical sub-groups whose orders are factors of $p+1$ must also contain substitutions of order p. Hence that sub-group of g which keeps one symbol unchanged must contain a substitution of order 3 self-conjugately. It will, therefore, be a sub-group of dihedral type, and m will be of the form

$$2\,\frac{p+1}{q_1}\,\frac{p-1}{q_2}.$$

Of the substitutions of this sub-group exclusive of identity, $\left(\frac{p+1}{q_1}-1\right)\frac{p-1}{q_2}$ keep one symbol unchanged, and $\left(\frac{p+1}{q_1}+1\right)\frac{p-1}{q_2}-1$ keep $p+1$ symbols unchanged.

Hence the $p_1 p_2$ conjugate sub-groups contain

$$1+p_1p_2\left(\frac{p+1}{q_1}-1\right)\frac{p-1}{q_2}+\frac{p_1p_2}{p+1}\left(\left[\frac{p+1}{q_1}+1\right]\frac{p-1}{q_2}-1\right)$$

distinct substitutions.

Now, if $\frac{p+1}{q_1}$ is greater than 3, this quantity is greater than

$$\tfrac{1}{3}\,(p_1p_2+p_1+p_2)\,m\,;$$

and, if $\frac{p+1}{q_1}$ is equal to 3, $\frac{1}{p+1}\left(\left[\frac{p+1}{q_1}+1\right]\frac{p-1}{q_2}-1\right)$ cannot be an integer, and therefore in any case the second supposition is inadmissible.

If, now, p is a factor of m, then $3p^3$ must be a factor of m, and the sub-group of g that keeps one symbol unchanged cannot contain the group of order p^3 self-conjugately. It must therefore contain at least $p+1$ conjugate sub-groups of order p^3. But this is the number that is contained in the most general sub-group that keeps one symbol unchanged, and it is easy to see that any sub-group containing these $p+1$ groups of order p^3 is at least as extensive as this most general sub-group. The sub-group g would therefore, in this case, coincide with the main group.

Hence, finally, no transitive sub-group of the type in question can exist.

7. *On the Intransitive Sub-Groups of G.*

Among the intransitive sub-groups contained in the main group there are two classes the discussion of which is practically involved in the known results obtained by former writers in connexion with the general homogeneous integral group in two variables. These are (i) the sub-groups contained in the sub-group of order

$$p^3(p-1)^2\,(p+1)$$

which keeps one symbol fixed, and (ii) the sub-group contained in the group of the same order which interchanges the symbols in two transitive sets of p^2 and $p+1$.

It has already been seen incidentally that there is an intransitive sub-group of order $6\,(p-1)^2$, namely, (iii) the group of type

$$\left\{\begin{matrix}(\;\;y, & z, & x) \\ (-y, & x, & z) \\ (\;ax, & by, & cz)\end{matrix}\right\}, \qquad abc\equiv 1,$$

which either leaves the three symbols $\{x\}$, $\{y\}$, $\{z\}$ unchanged or interchanges them among themselves.

I shall first show that any intransitive sub-group not belonging to the first two classes is necessarily either contained in a sub-group of the type just given, or is a sub-group of the transitive group of order $3\,(p^2+p+1)$.

Suppose that N is the order of such a sub-group g, and n the order of the highest sub-group contained at once in g and in one of class (iii). Then g must contain $\dfrac{N}{n}$ conjugate sub-groups of order n.

Now, two such conjugate sub-groups can only have substitutions in common if the symbols which they interchange are of the forms

$$\{x\},\quad \{y\},\quad \{z\}$$

and

$$\{x+Ay\},\quad \{x+By\},\quad \{z\};$$

so that the sub-groups contain conjugate substitutions

$$(\alpha x,\quad \beta y,\quad \gamma z)$$

and

$$x'+Ay' \equiv \alpha\,(x+Ay),\quad x'+By' \equiv \beta\,(x+By),\quad z' \equiv \gamma z.$$

Moreover, the multipliers α and β cannot be equal for all the substitutions of the two sub-groups, as in that case the sub-groups would not be distinct. But, if α and β are unequal, it is easy to verify that the two substitutions just written will generate the sub-group formed by all substitutions of the type

$$(ax+by,\quad a'x+b'y,\quad \gamma z),\qquad (ab'-a'b)\,\gamma \equiv 1,$$

and the order of this sub-group is equal to or a multiple of $p\,(p^2-1)$. Now, by supposition, the substitutions of g do not all keep $\{z\}$ unchanged. Hence (p. 86, bottom) the group, if not transitive in all the p^2+p+1 symbols, must interchange the symbols in two transitive sets of p^2 and $p+1$. But, by supposition, the latter is not the case, and therefore, finally, the $\frac{N}{n}$ conjugate sub-groups of order n contained in g have no common substitutions except identity. The $N\left(1-\frac{1}{n}\right)$ distinct substitutions thus accounted for must contain all the substitutions of g whose orders are equal to or factors of $p-1$, as otherwise there would be a second set of $N\left(1-\frac{1}{n'}\right)$ substitutions, which with the previous set would give a number greater than the order of the group. The remaining substitutions of the sub-group, if any, must either displace all the symbols or must keep one symbol unchanged; and in the latter case their orders must divide p^2-1, since the group can contain no substitutions of order p. If there are substitutions displacing all the symbols, their number must be $\epsilon N\left(1-\frac{1}{p_1}\right)$, where p_1 is a factor of p^2+p+1, and ϵ is either 1 or $\frac{1}{3}$. If there are substitutions which keep one symbol unchanged, and if $\frac{p+1}{q_1}\,\frac{p-1}{q_2}$ is the highest order of any such substitution, there will be a set of $\eta N\left(1-\frac{q_1}{p+1}\right)$ substitutions, conjugate to this substitution, and to those of its powers which keep only one symbol unchanged, where η is 1 or $\frac{1}{2}$; and, if this does not exhaust all the substitutions of the group, there must be further sets similar to the last. Hence, finally,

$$N = 1+N\left(1-\frac{1}{n}\right)+\epsilon N\left(1-\frac{1}{p_1}\right)+\Sigma\eta N\left(1-\frac{q_1}{p+1}\right),$$

where ϵ is 0, 1, or $\frac{1}{8}$, and each η is 0, 1, or $\frac{1}{2}$. This equation cannot clearly be satisfied if ϵ is unity. If $\epsilon = \frac{1}{3}$, there cannot be more than one term under the sign of summation, and, if there is such a term, η must be $\frac{1}{2}$, so that either

$$N = 1+N\left(1-\frac{1}{n}\right)+\tfrac{1}{3}N\left(1-\frac{1}{p_1}\right)+\tfrac{1}{2}N\left(1-\frac{q_1}{p+1}\right)$$

or $$N = 1+N\left(1-\frac{1}{n}\right)+\tfrac{1}{3}N\left(1-\frac{1}{p_1}\right).$$

The least possible values of $1-\frac{1}{n}$, $1-\frac{1}{p_1}$, and $1-\frac{q_1}{p+1}$ are $\frac{1}{2}$, $\frac{6}{7}$, and $\frac{2}{3}$, and therefore the first equation is impossible. The second equation gives

$$\tfrac{1}{3}+\frac{1}{N} = \frac{1}{3p_1}+\frac{1}{n},$$

and can only be satisfied by

$$N = 3p_1, \quad n = 3.$$

Corresponding to this solution there are the intransitive sub-groups of the sub-groups of order $3(p^2+p+1)$.

Finally, if $\epsilon = 0$, so that

$$N = 1+N\left(1-\frac{1}{n}\right)+\Sigma\eta N\left(1-\frac{q_1}{p+1}\right),$$

there can be only one term again under the sign of summation $\left(\text{the least value of } 1-\frac{q_1}{p+1} \text{ is } \frac{2}{3}\right)$, and η must be $\frac{1}{2}$. Hence

$$N = 1+N\left(1-\frac{1}{n}\right)+\tfrac{1}{2}N\left(1-\frac{q_1}{p+1}\right)$$

or $$\tfrac{1}{2}+\frac{1}{N} = \frac{1}{n}+\frac{q_1}{2(p+1)},$$

and the only solution of this equation is

$$n = 2, \quad N = 2\frac{p+1}{q_1},$$

The corresponding type of sub-group belongs to the first class, all of its substitutions keeping one symbol unchanged.

The only other possibility is represented by the equation

$$N = 1+N\left(1-\frac{1}{n}\right),$$

so that

$$n = N,$$

and the sub-group g is contained within the above considered sub-group of order $6\,(p-1)^2$.

The intransitive sub-groups of the sub-group of order $3\,(p^2+p+1)$, which exist when p^2+p+1 is not a prime, are of simple type and need not be explicitly dealt with, so that it is now only necessary to consider the various sub-groups of the three general types of intransitive sub-groups specified at the beginning of this section. The first two types, though obviously not conjugate to each other within the main group, are holohedrically isomorphous, and therefore, when the various types of sub-group contained in the one have been investigated, those contained in the other may be immediately written down. This isomorphism may be established in the following manner:—

Type (ii) contains the group of order p^2,

$$(x+ay+bz,\ \ y,\ \ z),$$

self-conjugately, and is generated by combining this group with the group generated by

$$\begin{array}{llll}(x, & y+z, & z &), \\ (x, & y, & y+z &), \\ (ax, & a^ry, & a^{-(r+1)}z), & \end{array}$$

a a primitive root mod. p.

If these three substitutions are denoted by A, B, C, and if the substitution

$$(x+ay+bz,\ \ y,\ \ z)$$

is denoted by $S_{a,b}$ a simple calculation gives

$$AS_{a,b}A^{-1} = S_{a,\,a+b},$$

$$BS_{a,b}B^{-1} = S_{a+b,\,b},$$

$$CS_{a,b}C^{-1} = S_{aa^{r-1},\ ba^{-r-2}}.$$

Type (i) contains the sub-group of which $S'_{a,b}$ or

$$(x+az,\quad y+bz,\quad z)$$

is the type self-conjugately; and is generated by combining this group with the group arising from

$$\begin{aligned} A' &\text{ or } (x-y, & y, && z\ ), \\ B' &\text{ or } (\ x, & y-x, && z\ ), \\ C' &\text{ or } (\alpha^{-r}x, & \alpha^{r+1}y, && \alpha^{-1}z); \end{aligned}$$

moreover,

$$\begin{aligned} A'S'_{a,b}A'^{-1} &= S'_{a,a+b}, \\ B'S'_{a,b}B'^{-1} &= S'_{a+b,a}, \\ C'S'_{a,b}C'^{-1} &= S'_{a\alpha^{r-1},\ b\alpha^{-r-2}}. \end{aligned}$$

Now, except as regards the symbols in terms of which they are written, A', B', C' are identical with the inverses of A, B, C; and it is well known that, among the various ways in which a group can be isomorphously connected with itself, that in which two inverse operations are taken as corresponding operations always occurs. Hence an isomorphous correspondence is established between the two types by taking A, B, C, $S_{a,b}$ as corresponding substitutions to A', B', C' and $S'_{a,b}$. It is, therefore, only necessary to deal in detail with one of the two types, and the first will be chosen, as lending itself rather more readily to calculation. This may, for shortness, be referred to as the sub-group H.

The order of the greatest possible sub-group of H which contains no substitutions whose orders are factors of $p+1$ is $p^3(p-1)^2$. Such a sub-group, if it exists, must, by Sylow's theorem, contain either a single self-conjugate sub-group of order p^3, or $(p-1)^2$ conjugate sub-groups of this order, since $(p-1)^2$ contains no factor of the form $\kappa p+1$ except itself and unity. Now, every group of order p^3 is of the type

$$(x+\alpha y+\beta z,\quad y+\gamma z,\quad z),$$

and is obviously self-conjugate within the group of type

$$(ax+by+cz,\quad b'y+c'z,\quad c''z),$$

whose order is $p^3(p-1)^3$. Hence H only contains $p+1$ conjugate sub-groups of order p^3, and therefore the supposition that a sub-group of H of order $p^3(p-1)^2$ contains $(p-1)^2$ conjugate sub-groups of order p^3 is impossible.

Hence any sub-group of H which contains no substitutions whose orders are $p+1$ or one of its factors must be contained as a sub-group within a group of the type

$$(ax+by+cz,\quad b'x+c'z,\quad c''z).$$

Consider now sub-groups of H which contain substitutions whose orders are factors of $p+1$. If such a sub-group contains the operation

$$(x+z,\quad y,\quad z),$$

it must contain a conjugate substitution in which $\{y\}$ is not an unchanged symbol, and it must therefore contain the whole of the self-conjugate sub-group

$$(x+\alpha z,\quad y+\beta z,\quad z).$$

Every sub-group of H containing substitutions whose orders are factors of $p+1$ must therefore either contain this self-conjugate sub-group of order p^2, or, containing none of the operations of this sub-group, it must be a sub-group of one of the p^2 sub-groups of H whose type is

$$\left\{\begin{matrix} (x+y, & y, & z\,) \\ (\;x, & x+y, & z\,) \\ (\;a^r x, & a^{-r-1}y, & az) \end{matrix}\right\}.$$

Moreover, if it contains the sub-group of order p^2, it must be merihedrically isomorphous with some sub-group of the group of type just written, and, therefore, must be generated by some sub-group of the group just written, combined with the group of order p^2 given by

$$(x+\alpha z,\quad y+\beta z,\quad z).$$

Again, every sub-group of the group given by

$$\left\{\begin{matrix} (x+y, & y, & z\,) \\ (\;x, & x+y, & z\,) \\ (\;a^r x, & a^{-r-1}y, & az) \end{matrix}\right\}$$

contains as a self-conjugate sub-group those substitutions which multiply z by unity; and any such sub-group is a sub-group of the group

$$\left\{\begin{matrix} (x+y, & y, & z) \\ (\;x, & x+y, & z) \end{matrix}\right\},$$

of which all possible types of sub-group are known.

Hence, by starting from the known sub-groups of this last sub-group, all the sub-groups of H which contain substitutions that keep only one symbol fixed may be constructed. They will consist (i) of these sub-groups themselves, (ii) of those obtained by combining them with substitutions of the form

$$(\alpha x,\ \beta y,\ \gamma z),$$

and (iii) of those obtained by combining the sub-groups of type (ii) with the group

$$(x+az,\ y+bz,\ z).$$

To every type of sub-group of H thus obtained will correspond an isomorphous sub-group of

$$(x+by+cz,\ b'y+c'z,\ b''y+c''z);$$

which may or may not be conjugate within the main group to the sub-group of H with which it corresponds.

The other intransitive sub-groups that require consideration are, as has been seen, the sub-groups of a group I, of type

$$\left\{\begin{matrix}(\ y, & z, & x\ ) \\ (-y, & x, & z\ ) \\ (\ ax, & by, & cz)\end{matrix}\right\},$$

and they must contain substitutions of order 3, since the sub-group

$$\left\{\begin{matrix}(-y, & x, & z\ ) \\ (\ ax, & by, & cz)\end{matrix}\right\}$$

is contained within H.

Now the sub-group $(ax,\ by,\ cz),\ abc\equiv 1,$

is contained self-conjugately within I, and is generated by the two permutable operations of order $p-1$,

$$(a^{-1}x,\ ay,\ z)\ \text{ and }\ (a^{-1}x,\ y,\ az).$$

Every possible sub-group of this Abelian group may now be written down, and combined either with

$$(\ y,\ z,\ x),$$

$$(-y,\ x,\ z),$$

or with the former of these two substitutions alone.

The sub-groups thus obtained will evidently not be all distinct from I; but in this way all possible sub-groups of I are obtained.

The actual enumeration of all possible types of intransitive sub-group would be excessively laborious, and it is doubtful whether it would serve any useful purpose; but the preceding analysis supplies the means for determining directly whether a sub-group of any given type actually exists or not.

8. *Case II.* $p \equiv 1 \pmod{3}$.

I now go on to the case in which $p \equiv 1 \pmod{3}$, in which the congruence

$$z^3 \equiv 1 \pmod{p}$$

will have three different real roots. These will be denoted by $1, \theta, \theta^2$.

The homogeneous group of determinant unity

$$(ax+by+cz,\quad a'x+b'y+c'z,\quad a''x+b''y+c''z)$$

is no longer holohedrically isomorphous to the non-homogeneous group

$$x' \equiv \frac{ax+by+c}{a''x+b''y+c''},\quad y' \equiv \frac{a'x+b'y+c'}{a''x+b''y+z''},$$

for the three different homogeneous substitutions

$$\left[\theta^r(ax+by+cz),\ \theta^r(a'x+b'y+c'z),\ \theta^r(a''x+b''y+c''z)\right],\quad r = 1, 2, 3,$$

correspond to one and the same non-homogeneous substitution.

The sub-group $\qquad (\theta^r x,\ \theta^r y,\ \theta^r z), \qquad r = 1, 2, 3,$

of the homogeneous group, being permutable with every one of its substitutions, is a self-conjugate sub-group, and the homogeneous group is merihedrically isomorphous to the non-homogeneous group, in such a way that to the identical substitution of the latter corresponds the above self-conjugate sub-group of order 3 of the former. The homogeneous group, moreover, contains no sub-group which is holohedrically isomorphous to the non-homogeneous group. For, if it did, of the three substitutions

$$\begin{array}{lll}(\ x, & \theta y, & \theta^2 z),\\ (\theta x, & \theta^2 y, & z\ ),\\ (\theta^2 x, & y, & \theta z\ ),\end{array}$$

one only would belong to the sub-group; but the two latter are obtained from the former by transforming it by (y, z, x) and (z, x, y).

It would, however, be most inconvenient to use the non-homogeneous forms throughout the following discussions, and there will be no difficulty or confusion in still using the homogeneous form with the understanding that the substitutions

$$\left[\theta^r(ax+by+cz),\ \theta^r(a'x+b'y+c'z),\ \theta^r(a''x+b''y+c''z)\right],\quad r=1,2,3,$$

are not to be regarded as distinct.

This is the same as regarding the three sets of multipliers

$$\lambda_1,\ \lambda_2,\ \lambda_3;\quad \theta\lambda_1,\ \theta\lambda_2,\ \theta\lambda_3;\quad \theta^2\lambda_1,\ \theta^2\lambda_2,\ \theta^2\lambda_3$$

as equivalent; or, in other words, the three characteristic congruences

$$f(\lambda)\equiv 0,\quad f(\theta\lambda)\equiv 0,\quad f(\theta^2\lambda)\equiv 0$$

as equivalent.

It may be shown at once, precisely as in the former case, that any two substitutions which have equivalent characteristic congruences with unequal roots are conjugate to each other, and the reduction of any substitution to a typical form may be carried out exactly as in the former case.

If, now, the characteristic congruence has for its roots λ, λ^p, λ^{p^2}, where λ is a primitive root of

$$\lambda^{p^2+p+1}-1\equiv 0,$$

which again will always be the case for some suitably chosen substitution, this substitution in its typical form will be

$$\xi'\equiv\lambda\xi,\quad \eta'\equiv\lambda^p\eta,\quad \zeta'\equiv\lambda^{p^2}\zeta,$$

and its order m will be the least integer for which

$$\lambda^m=\lambda^{mp}\equiv\lambda^{mp^2}.$$

In this case 3 is the only common factor of $p-1$ and p^2+p+1, and therefore the order of this substitution is $\frac{1}{3}(p^2+p+1)$. The order, then, of every substitution whose characteristic congruence is irreducible is $\frac{1}{3}(p^2+p+1)$ or a factor of this number.

If, again, μ is a primitive root of the congruence

$$\mu^{p^3-1}-1\equiv 0,$$

there must be substitutions, whose characteristic congruences have an irreducible quadratic factor, of the type

$$\xi' \equiv \mu\xi, \quad \eta' \equiv \mu^p\eta, \quad z' \equiv \mu^{-(p+1)}z.$$

The order n of such a substitution is the least integer for which

$$\mu^n \equiv \mu^{np} \equiv \mu^{-n(p+1)},$$

and this is $\frac{1}{3}(p^2-1)$. Every substitution, then, whose characteristic congruence contains an irreducible quadratic factor has for its order $\frac{1}{3}(p^2-1)$ or a factor of this number.

Of the remaining types

$$\begin{array}{llll}
\text{(i)} & x' \equiv \alpha x, & y' \equiv \alpha^r y, & z' \equiv \alpha^{-(r+1)}z, \\
\text{(ii)} & x' \equiv \alpha x, & y' \equiv \alpha y, & z' \equiv \alpha^{-2}z, \\
\text{(iii)} & x' \equiv \alpha^{-2}x, & y' \equiv \alpha y, & z' \equiv \alpha(y+z), \\
\text{(iv)} & x' \equiv x, & y' \equiv y+z, & z' \equiv z, \\
\text{(v)} & x' \equiv x, & y' \equiv y+x, & z' \equiv z+y,
\end{array}$$

where the coefficients are real, the orders may be determined at once by inspection. Thus in (i) the order is equal to or a factor of $p-1$; in (ii) equal to or a factor of $\frac{1}{3}(p-1)$; in (iii) equal to or a factor of $\frac{1}{3}p(p-1)$; in (iv) and (v) equal to p.

Hence the order of every substitution contained in the group must be equal to or a factor of one of the numbers $\frac{1}{3}(p^2+p+1)$, $\frac{1}{3}(p^2-1)$, $\frac{1}{3}p(p-1)$, p, $p-1$, while, on the other hand, the group contains substitutions whose orders are actually equal to each one of these numbers. Also every substitution whose order is a factor of $\frac{1}{3}(p^2+p+1)$ must be a power of a substitution whose order is $\frac{1}{3}(p^2+p+1)$, and a similar property holds for a substitution whose order is a factor of $\frac{1}{3}(p^2-1)$ other than $p-1$ or its factors.

The number of cyclical sub-groups of each type and their distribution in conjugate sets may now be investigated.

Order $\frac{1}{3}(p^2+p+1)$. Exactly as in the corresponding order of the former case, it may be shown that a substitution S of order $\frac{1}{3}(p^2+p+1)$ is permutable only with its own powers, and therefore forms one of a set of $\dfrac{N}{\frac{1}{3}(p^2+p+1)}$ conjugate substitutions, where N is the order of the main group.

Now, the only powers of S which have equivalent multipliers with S are S^p and S^{p^2}, and hence to each set of substitutions such as S^r, S^{rp}, S^{rp^2}, there corresponds such another set of $\frac{N}{\frac{1}{3}(p^2+p+1)}$ conjugate substitutions.

There are, therefore, in all $\frac{\frac{1}{3}(p^2+p+1)-1}{p^2+p+1}N$ such substitutions, whose orders are $\frac{1}{3}(p^2+p+1)$ or one of its factors, and these form $\frac{N}{p^2+p+1}$ conjugate cyclical sub-groups of order $\frac{1}{3}(p^2+p+1)$, each of which must therefore be contained self-conjugately in a sub-group of order p^2+p+1.

Order $\frac{1}{3}(p^2-1)$. Exactly as in the corresponding order of the previous case, it may again be shown here that there are $\frac{N}{\frac{2}{3}(p^2-1)}$ conjugate cyclical sub-groups of order $\frac{1}{3}(p^2-1)$, each being self-conjugate in a group of order $\frac{2}{3}(p^2-1)$; and that these sub-groups contain in all $\frac{Np}{2(p+1)}$ different substitutions whose orders are equal to or factors of $\frac{1}{3}(p^2-1)$ without at the same time being factors of $\frac{1}{3}(p-1)$.

Order $\frac{1}{3}(p^2-p)$. By similar reasoning to that used in the former case, it may be shown that there are $\frac{N}{\frac{1}{3}p(p-1)^2}$ conjugate cyclical sub-groups of order $\frac{1}{3}(p^2-p)$, so that each is contained self-conjugately in a sub-group of order $\frac{1}{3}p(p-1)^2$; also that these sub-groups contain $\frac{p-4}{p(p-1)}N$ different substitutions, whose orders are neither p nor $\frac{1}{3}(p-1)$ nor one of its factors.

Order p. For cyclical sub-groups of order p arising from a substitution of the form

$$(x+z,\ y,\ z),$$

it may be shown by a slight modification of the former method of proof that the main group contains a single conjugate set of $\frac{N}{\frac{1}{3}(p-1)^2p^3}$ sub-groups, so that each such sub-group is self-conjugate in a group of order $\frac{1}{3}(p-1)^2p^3$. These conjugate cyclical sub-groups contain in all $\frac{3N}{p^3(p-1)}$ different substitutions of order p.

For cyclical sub-groups arising from a substitution of the form

$$(x+y,\ \ y+z,\ \ z),$$

it will be found again, as before, that there is a single conjugate set of $\frac{3N}{(p-1)p^2}$ in the main group, so that each is self-conjugate in a sub-group of order $\frac{1}{3}(p-1)p^2$, while the whole set contain $\frac{3N}{p^2}$ different substitutions of order p.

Order $p-1$. It is no longer the case here that every substitution whose order is a factor of $p-1$ is the power of substitution whose order is $p-1$. If, a being a primitive root mod. p, a^r, a^s, a^{-r-s} are the multipliers of a substitution, it is still a necessary condition in order that the order of the substitution may be $p-1$ that the highest common factor of r and s should be relatively prime to $p-1$. But this condition is not now sufficient, for, if the difference of r and s is a multiple of 3, the order of the substitution is only $\frac{p-1}{3}$, and it is easy to see that the substitution is not the third power of a substitution of order $p-1$.

It is not difficult to modify the result of the previous case for the number of conjugate sets of cyclical sub-groups of order $p-1$, so as to obtain the numbers of conjugate sets in this case of cyclical sub-groups of orders $p-1$ and $\frac{p-1}{3}$, but the result is rather complicated, and it will be replaced here by a determination of the number of conjugate sets of substitutions, and the number in each set.

For this purpose, consider the congruence

$$\alpha\beta\gamma \equiv 1 \quad (\text{mod. } p).$$

It has $(p-1)^2$ different solutions; in three of which α, β, γ are equal to each other, while in $3(p-4)$ of the remainder two only of the three quantities α, β, γ are equal. There are, therefore,

$$(p-1)^2-3(p-4)-3$$

solutions in which the three quantities are unequal, and therefore, allowing for the six permutations of α, β, γ among themselves, there are

$$\frac{(p-1)^2-3(p-4)-3}{6}$$

distinct sets of unequal multipliers of substitutions whose orders are factors of $p-1$ in the homogeneous group. Of these the set $1, \theta, \theta^2$ is the only one which is equivalent to itself; α, β, γ; $\theta\alpha, \theta\beta, \theta\gamma$; $\theta^2\alpha, \theta^2\beta, \theta^2\gamma$, being, as before defined, three equivalent sets of multipliers. The number of equivalent sets of unequal multipliers, *i.e.*, the number of sets of unequal multipliers, in the non-homogeneous group is therefore

$$1+\tfrac{1}{3}\left(\frac{(p-1)^2-3(p-4)-3}{6}-1\right),$$

or

$$1+\frac{(p-1)(p-4)}{18}.$$

Allowing for permutations among α, β, γ, the $3(p-4)$ solutions of the above congruence in which two of the three quantities are equal give $p-4$ sets of multipliers in the homogeneous group, and $\frac{p-4}{3}$ sets of multipliers in the non-homogeneous group. To each of these sets of multipliers corresponds a single conjugate set of substitutions. Now, a substitution

$$(x,\ \theta y,\ \theta^2 z)$$

is permutable with the group arising from

$$\begin{aligned} &(ax,\ by,\ cz), \qquad abc \equiv 1,\\ &(y,\ z,\ x),\\ &(-y,\ x,\ z), \end{aligned}$$

which generate in the homogeneous group a sub-group of order $6(p-1)^2$, to which corresponds a sub-group of order $2(p-1)^2$ in the non-homogeneous group. There is, therefore, a conjugate set of $\frac{N}{2(p-1)^2}$ substitutions with multipliers $1, \theta, \theta^2$. Every other substitution with 3 unequal multipliers is permutable only with the group

$$(ax,\ by,\ cz), \qquad abc \equiv 1;$$

and therefore gives rise to a conjugate set of $\frac{N}{\frac{1}{3}(p-1)^2}$ substitutions in the non-homogeneous group.

Finally, a substitution $(ax,\ ay,\ a^{-2}z)$

is permutable in the homogeneous group, as in the former case, with a sub-group of order $p(p+1)(p-1)^2$, and is therefore in the non-homogeneous group one of a set of $\frac{N}{\frac{1}{3}p(p+1)(p-1)^2}$ substitutions. Hence the total number of substitutions in the group whose orders are equal to or factors of $p-1$ is

$$\frac{N}{2(p-1)^2}+\frac{N(p-4)}{6(p-1)}+\frac{N(p-4)}{p(p+1)(p-1)^2}.$$

On adding together the numbers of substitutions of the different types that have thus been obtained with an additional unity for the identical substitution the sum will be found to be N, as it should be.

It is not necessary to go again through the discussion of sub-groups containing substitutions of order p.

The result, exactly as in the former case, is that a sub-group, containing operations of order p, and neither contained in the sub-group of order $\frac{1}{3}p^3(p-1)^2(p+1)$ which keeps one symbol fixed, nor in the isomorphous sub-group which interchanges the p^2+p+1 symbols in two transitive sets of p^2 and $p+1$, must be transitive, while its order must be divisible by p^3.

Now, it has been seen that every cyclical sub-group of order $\frac{1}{3}(p^2+p+1)$ is contained self-conjugately in a sub-group of order p^2+p+1. This sub-group is not, however, transitive in all the symbols, but interchanges them transitively in sets of $\frac{1}{3}(p^2+p+1)$ each. Suppose now that a transitive sub-group g exists of order $\frac{1}{3}(p^2+p+1)\,m$, containing cyclical sub-groups of order $\frac{1}{3}(p^2+p+1)$. Since the sub-group is transitive, m must be divisible by 3, and the group must contain either

$$\{\tfrac{1}{3}(p^2+p+1)-1\}\,m \quad\text{or}\quad \{\tfrac{1}{3}(p^2+p+1)-1\}\,\tfrac{1}{3}m$$

substitutions displacing all the symbols, leaving over either m or $m\,\{\frac{2}{3}(p^2+p+1)+\frac{1}{3}\}$ substitutions.

The first supposition is clearly impossible, and the latter gives, as in the former case,

$$\frac{m}{3}\equiv 1, \qquad \text{mod.}\,\tfrac{1}{3}(p^2+p+1).$$

This again leads, according as m is or is not divisible by p, either to

$$m = 3p^3$$

or

$$m = (p-1)^2(p+1),$$

and it may be again shown here that neither of the corresponding types of group exists.

The former reasoning may also be repeated to show that there can be no transitive sub-group which contains substitutions of the orders p_1 and p_2, where p_1, p_2 are the two different prime factors of $\frac{1}{3}(p^2+p+1)$, this number being supposed not to be a prime, without containing substitutions of the order $p_1 p_2$; so that, finally, the group contains in this case no transitive sub-groups. The possibility occurs in this case of an intransitive sub-group containing substitutions of order $\frac{1}{3}(p^2+p+1)$, but a consideration of the sets in which such a substitution would displace the symbols immediately shows that no such type can exist with the exception of the above mentioned sub-groups of order p^2+p+1. The previous reasoning applies to all other types of intransitive sub-group without modification, and leads to the same result, viz., that every intransitive sub-group, other than those whose orders are equal to or factors of p^2+p+1, is contained either in the sub-group of order $\frac{1}{3}p^3(p-1)^2(p+1)$ that keeps one symbol fixed, or in the isomorphous group that displaces the symbols in two transitive sets of p^2 and $p+1$, or, finally, in the sub-group of order $2(p-1)^2$, arising from

$$\big[(y,\ z,\ x),\quad (-y,\ x,\ z),\quad (ax,\ by,\ cz)\big].$$

It may be noticed that the intransitive sub-group of the homogeneous group which keeps one symbol fixed contains a sub-group of order $\frac{1}{3}p^3(p-1)^2(p+1)$, viz.,

$$(ax+by+cz,\ a'x+b'y+c'z,\ c''z),\quad (ab'-a'b)\,c''\equiv 1,\quad c''^{\frac{1}{3}(p-1)}\equiv 1,$$

which is holohedrically isomorphous with the corresponding sub-group of the non-homogeneous group.

9. *On the Group G for $p=2$ and $p=3$.*

When $p=2$, the order of the main group is 168. The only simple group of this order is the known group of the modular equation for transformation of the seventh order of elliptic functions; so that this case does not require separate discussion.

It may be noticed that the sub-group of order p^3 or 8 in this case contains substitutions of order p^2 or 4, whereas in all other cases the substitutions of the sub-groups of order p^3 are all of order p.

When $p=3$, the order of the main group is 5616 or $13 \,.\, 3^3 \,.\, 2^4$. A consideration of the multipliers of a substitution of order 13 shows, as before, that every cyclical sub-group of this order is contained self-conjugately in a sub-group of order 39. If, now, there were any other sub-groups containing substitutions of order 13, and therefore of order $13m$, either m or $\frac{m}{3}$ must, by Sylow's theorem, be congruent to unity mod. 13. But the only factors of $3^3 . 2^4$ which are congruent to unity mod. 13 are 3^3 and $3^2 . 2^4$. Now sub-groups of orders $13 . 3^3$ and $13 . 3^2 . 2^4$, if they existed, would be transitive in 13 symbols, and would at the same time contain $12 . 3^3$ and $12 . 3^2 . 2^4$ substitutions respectively of order 13; but this is impossible. The only transitive sub-groups, therefore, are those of orders 13 and 39.

The intransitive sub-groups, finally, will come under the same three heads as in the two general cases already discussed.

Thursday, January 10th, 1895.

Major MACMAHON, R.A., F.R.S., President, in the Chair.

Mr. Ernest Frederick John Love, M.A., Queen's College, Carlton, Melbourne, Victoria, was elected a member, and Mr. J. H. Hooker was admitted into the Society.

The Chairman gave a short obituary account of Mr. A. Cowper Ranyard's work and connexion with the Society.

The following communications were made:—

On Fundamental Systems for Algebraic Functions: Mr. H. F. Baker.

On the Expansion of Functions: Mr. E. T. Dixon.

Some Properties of a Generalized Brocard Circle: Mr. J. Griffiths.

Electrical Distribution on Two Intersecting Spheres: Mr. H. M. Macdonald.

The Dynamics of a Top: Prof. Greenhill.

The following presents were received:—

"Calendar of Queen's College, Cork," 1894–5; Cork, 1894.

"Journal of the Institute of Actuaries," Vol. XXXI., Pt. 5; October, 1894.

"Bulletin of the American Mathematical Society," 2nd Series, Vol. I., No. 3; New York, 1894.

Issaly, M. l'Abbé.—"Optique Géométrique," pamphlet, 8vo; Bordeaux.

"Berichte über die Verhandlungen der Koniglich Sächsischen Gesellschaft der Wissenschaften zu Leipzig," II., 1894.

"Memoirs and Proceedings of the Manchester Literary and Philosophical Society," Vol. VIII., No. 4.

"Bulletin des Sciences Mathématiques," Tome XVIII., December, 1894; Paris.

"Bulletin de la Société Mathématique de France," Tome XXII., No. 9.

"Rendiconti del Circolo Matematico di Palermo," Tomo VIII., Fasc. 6; Nov.-Dec., 1894.

"Atti della Reale Accademia dei Lincei—Rendiconti," 2 Sem., Vol. III., Fasc. 10; Roma, 1894.

"Educational Times," January, 1895.

"Annals of Mathematics," Vol. IX., No. 1; November, 1894, Virginia.

"Indian Engineering," Vol. XVI., Nos. 21-24; Nov. 24-Dec. 15, 1894.

A bound volume of letters from Prof. De Morgan and his son G. C. De Morgan, to A. C. Ranyard, bearing upon the foundation of The London Mathematical Society, and a letter from Mrs. De Morgan.

Tracts by Professor De Morgan:—

i. "On the Mode of using the Signs + and − in Plane Geometry."
ii. (i. *continued*) "and on the Interpretation of the Equation of a Curve."
iii. "On the word 'Αριθμός."
iv. "On a Property of Mr. Gompertz's Law of Mortality."
v. "Remark on Horner's Method of Solving Equations."
vi. "Contents of the Correspondence of Scientific Men of the Seventeenth Century."
vii. "On Ancient and Modern Usage in Reckoning."
viii. "On the Difficulty of Correct Description of Books."
ix. "On the Progress of the Doctrine of the Earth's Motion, between the times of Copernicus and Galileo."
x. "On the Early History of Infinitesimals in England."

These two volumes were left by will, by Mr. Ranyard, for the acceptance of the Council.

On Fundamental Systems for Algebraic Functions. *By* H. F. Baker.

Read January 10th, 1895. Received, in abbreviated form, 18th February, 1895.

In a note which has appeared in the *Math. Annal.*, Vol. XLV., p. 118, it is verified that certain forms for Riemann's integrals, given by Herr Hensel for integrals of the first kind, and deduced by him algebraically from quite fundamental considerations, can be very briefly obtained on the basis of Riemann's theory. But a desire to dispense with the homogeneous variables used by Herr Hensel has