"Bulletin de la Société Mathématique de France," Tome xxi., No. 9 ; Paris.

"Bulletin de la Société Mathématique de France," Table des 20 Premiers Volumes ; Paris, 1894.

Gram, J. P.—"Essai sur la Restitution du Calcul de Léonard de Pise sur l'équation $x^3+2x^2+10x = 20$," pamphlet.

Gram, J. P.—"Rapport sur quelques Calculs entrepris par M. Bertelsen et concernant les Nombres Premiers," 4to pamphlet.

Zeuthen, H. G.—"Note sur l'Histoire des Mathématiques," pamphlet.

Barrett, T. S.—"Magic Squares," second edition, 8vo ; Berkhamsted, 1894.

"Beiblätter zu den Annalen der Physik und Chemie," Bd. xvii., St. 12, 1893 ; Bd. xviii., St. 1, 1894 ; Leipzig.

"Atti della Reale Accademia dei Lincei," Serie 5, Rendiconti, Vol. iii., Fasc. 1, 1 Sem. ; Vol. ii., Fasc. 12, 2 Sem. ; Roma, 1894.

"Indian Engineering," Vol. xiv., Nos. 26, 27 ; Vol. xv., Nos. 1 and 2.

"Educational Times," February, 1894.

"Rendiconti dell' Accademia delle Scienze Fisiche e Matematiche," Serie 2, Vol. vii., Fasc. 8-12 ; Napoli, 1894.

"Annales de la Faculté des Sciences de Toulouse," Tome vii., Année 1893, 4ème Fasc. ; Paris.

On a Class of Groups defined by Congruences. By Prof. W. Burnside. Received February 7th, 1894. Read February 8th, 1894.

1. *Introductory.*

Most of the groups of finite order which occur in connexion with problems of higher analysis can be defined by means of congruences. This is true, for example, of the group of the modular equation, and of the groups on which the division of the periods of the hyperelliptic functions depends. In his standard treatise (*Traité des Substitutions et des Equations Algébriques*) M. Camille Jordan has investigated at length the more important properties of the general linear group, defined by sets of congruences of the form

$$\left.\begin{array}{l} x_1' \equiv a_1x_1+b_1x_2+\ldots+c_1x_n \\ x_2' \equiv a_2x_1+b_2x_2+\ldots+c_2x_n \\ \ldots \quad \ldots \quad \ldots \quad \ldots \\ x_n' \equiv a_nx_1+b_nx_2+\ldots+c_nx_n \end{array}\right\} \pmod{p},$$

where the coefficients are ordinary integers.

The group of the modular equation, which is isomorphous with the general linear group when the number of variables is two, has formed the subject of a large number of memoirs; but it was first exhaustively analysed in a paper by Herr J. Gierster (*Math. Ann.*, Vol. XVIII.), in which the order and type of all possible sub-groups contained in the modular group for a prime transformation are completely determined. Though the congruences defining the groups dealt with in these investigations involve only real coefficients, both the authors mentioned find it of great advantage to introduce in their discussions the imaginaries which Galois* first used in analysis.

If these imaginaries are introduced in the congruences defining the groups, a new class of groups arises, altogether distinct from those defined by congruences whose coefficients are real integers; that is to say, the simple groups occurring in the composition-series (*Reihe der Zusammensetzung*) of these new groups are new simple groups. In the present paper some of the more important properties of the fractional linear group to a prime modulus, *i.e.*, the group defined by

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

when a, β, γ, δ are any rational functions of the roots of an irreducible congruence of the n^{th} degree (mod p), are investigated. It is shown that in this way new simple groups of orders $2^n(2^{2n}-1)$ and $\frac{1}{2}p^n(p^{2n}-1)$, p an odd prime and n any integer, are defined; the latter being in many respects closely analogous to the group of the modular equation. The orders of the separate operations of the groups and their distribution in conjugate sets are determined, and the order and type of some of the simpler sub-groups. For the case of $p=2$, a complete discussion is given of all possible types of sub-group; to carry this out, for p an odd prime, would probably necessitate the separate treatment of each value of n.

In two memoirs in Liouville's *Journal*, 1860-1, M. E. Mathieu has shown the existence of the triply-transitive group, called G in this paper, of which the simple group of order $\frac{1}{2}p^n(p^{2n}-1)$ is a self-conjugate sub-group. These memoirs deal, however, in the main, with the formation of functions which are unaltered by the operations of transitive groups, and the nature and properties of the groups themselves are not entered upon.

* *Cf.* Liouville's *Journal*, 1846, p. 381. Galois' papers have also been printed separately in a German translation by J. Springer, Berlin, 1889. *Cf.*, also, Serret, *Cours d'Algèbre Sup.*, Vol. II., p. 179, and Jordan's work mentioned above, p. 14.

In a subsequent paper the author hopes to deal with the simple groups that arise in connexion with systems of congruences involving n variables when the coefficients are imaginaries.

2. *Definition and Order of the Groups.*

Let x be a primitive root of the congruence

$$x^{p^n-1}-1 \equiv 0 \pmod{p},$$

so that x satisfies an irreducible congruence of the the form

$$x^n+a_1x^{n-1}+\ldots+a_n \equiv 0 \pmod{p},$$

where $a_1, \ldots a_n$ are real integers.

Then the p^n quantities

$$a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(A),$$

where $a_1, a_2, \ldots a_n$ may have any of the values $0, 1, 2, \ldots p-1$, are all incongruent, and it is known that in a proper order they are the same as the series of quantities

$$0, x, x^2, \ldots x^{p^n-1}.$$

If, now, $\alpha, \beta, \gamma, \delta$ are any four of these quantities, such that

$$\alpha\delta-\beta\gamma \not\equiv 0,$$

the system of congruences $\quad z' \equiv \dfrac{\alpha z+\beta}{\gamma z+\delta}$

form a group; for the result of combining any two congruences of this form is a third congruence of the same form.

The congruences

$$z' \equiv \frac{\alpha z+\beta}{\gamma z+\delta} \quad \text{and} \quad z' = \frac{m\alpha z+m\beta}{m\gamma z+m\delta}$$

are identical, and it may therefore be assumed that the determinant

$$\alpha\delta-\beta\gamma$$

of the substitution is either unity or a determinate quadratic non-residue, which may conveniently be taken as x.

Since $\quad z' \equiv \dfrac{\alpha z+\beta}{\gamma z+\delta} \quad$ and $\quad z' \equiv \dfrac{-\alpha z-\beta}{-\gamma z-\delta}$

are not distinct substitutions, the order of the group will be one half of the sum of the number of distinct solutions of the two separate congruences

$$\alpha\delta-\beta\gamma\equiv 1$$

and

$$\alpha\delta-\beta\gamma\equiv x.$$

In the first of these congruences, if α is zero, δ may have any one of the p^n possible values, and β and γ satisfy

$$\beta\gamma\equiv -1.$$

This congruence has clearly p^n-1 distinct solutions, and hence the number of solutions when α is zero is $p^n(p^n-1)$.

If α is different from zero, and δ such that

$$\alpha\delta\equiv 1,$$

then β, γ have $2p^n-1$ sets of values; while, if

$$\alpha\delta\not\equiv 1,$$

β, γ have p^n-1 sets of values, as in the first case.

Hence for each finite value of α there are

$$2p^n-1+(p^n-1)^2=p^{2n}$$

solutions of the congruence.

The total number of solutions is therefore

$$p^n(p^n-1)+p^{2n}(p^n-1)\equiv p^n(p^{2n}-1).$$

It is easy to show that the second congruence

$$\alpha\delta-\beta\gamma\equiv x$$

has an equal number of solutions, and therefore

$$p^n(p^{2n}-1)$$

is the order of the group.

The order of the group may also be simply determined as follows. The substitutions of the group permute the p^n+1 symbols consisting of the set (A) with ∞ among themselves. If x_1, x_2, x_3, x_1', x_2', x_3' are any six of these symbols, the substitution

$$\frac{z'-x_1'}{z'-x_2'}\,\frac{x_3'-x_2'}{x_3'-x_1'}\equiv\frac{z-x_1}{z-x_2}\,\frac{x_3-x_2}{x_3-x_1}$$

is evidently a substitution of the group, and it replaces the three symbols x_1, x_2, x_3 by x_1', x_2', x_3' respectively. The group is therefore triply-transitive in the p^n+1 symbols, and its order is therefore divisible by $(p^n+1)p^n(p^n-1)$; while, since it clearly contains no substitution, except identity, which keeps more than two symbols fixed, the order must be equal to this number.

3. *The Generating Operations.*

It will now be shown that the group can be generated by the combination and repetition of the three substitutions

$$z' \equiv \frac{-1}{z}, \quad z' \equiv z+1, \quad z' \equiv xz,$$

which may be conveniently represented by the symbols T, S, X.

If S be transformed by X^i, the resulting substitution $X^{-i}SX^i$ is given by the congruence $$z' \equiv z+x^i.$$

Let now Σ or $$z' \equiv \frac{az+\beta}{\gamma z+\delta}$$

be any substitution of the group; then i may be so chosen that $\Sigma X^{-i}SX^i$ or

$$z' \equiv \frac{az+\beta}{\gamma z+\delta}+x^i$$

is of the form $$z' \equiv \frac{\beta'}{\gamma z+\delta}.$$

It follows that $\Sigma X^{-i}SX^iT$ is given by

$$z' \equiv \frac{\gamma z+\delta}{-\beta'},$$

and j may then be so chosen that $\Sigma X^{-i}SX_iTX^{-j}SX^j$ or

$$z' \equiv \frac{\gamma z+\delta}{-\beta'}+x^j$$

is the same as $$z' \equiv \frac{\gamma z}{-\beta'} \equiv x^kz.$$

Hence any substitution of the group can be expressed in the form

$$X^{\alpha}SX^{\beta}TX^{\gamma}SX^{-\gamma},$$

and the three substitutions T, S, X are therefore, as stated above, generating operations of the group.

It has been seen that one half of the substitutions of the group have unity, or a quadratic residue, for their determinant. These evidently form a self-conjugate sub-group, and it may be shown that the generating substitutions of this sub-group are T, S, and X^2;

indeed, the previous proof will hold, as it stands, so soon as it is shown that

$$z' \equiv z + x'$$

can be formed from these operations, whatever x' may be. Now, every operation of this form in which x' is a quadratic residue may be formed by transforming S by the powers of X^2; and, by combining these operations, every operation of the above form in which x' is the sum of any number of quadratic residues may be formed. But among these quantities non-residues must occur, for, if unity be added in turn to every quadratic residue, the sums are all different, and unity does not occur among them.

When $p = 2$, there are no quadratic non-residues, for the two solutions of the congruence

$$x^2 \equiv x'^2 \pmod{2}$$

are congruent with each other, and therefore every one of the 2^n quantities (A) is in this case a quadratic residue.

In calculating the order of the group in this case the congruence

$$\alpha\delta - \beta\gamma \equiv x \pmod{2}$$

does not occur. On the other hand, α, β, γ, δ and $-\alpha$, $-\beta$, $-\gamma$, $-\delta$ are not now different solutions of the congruence

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{2},$$

so that the order of the group is the total number of solutions of this congruence, viz., $2^n(2^{2n}-1)$. In this case also there is evidently no self-conjugate sub-group of index 2, corresponding to the one just referred to when p is an odd prime.

It will be convenient, to avoid repetition, to deal with the case $p = 2$ by itself, after considering the general case of p any odd prime. In what follows the triply-transitive group of order $p^n(p^{2n}-1)$ will be referred to as the group G, and the sub-group of order $\frac{1}{2}p^n(p^{2n}-1)$ as the group H. It will also be a useful abbreviation to speak of the substitution defined by the congruence

$$z' \equiv \frac{\alpha z + \beta}{\gamma z + \delta}$$

as the substitution $\dfrac{\alpha z + \beta}{\gamma z + \delta}$.

4. *On the Orders of the Operations of G, and their Distribution in Conjugate Sets.*

When G is regarded as a triply-transitive group in p^n+1 symbols, its operations either change all the symbols, all but one or all but two. Those that keep either one or two symbols fixed are necessarily regular, as otherwise their powers would keep more than two symbols fixed. On the other hand, some of those that change all the symbols may be such that their squares keep two symbols fixed; otherwise they also must be regular. Since the group is triply-transitive, there must occur among the substitutions conjugate to a substitution which contains a given transposition substitutions containing any other chosen transposition. If now the substitution $\dfrac{\alpha z+\beta}{\gamma z+\delta}$ transposes 0 and ∞, then $\alpha\equiv\delta\equiv 0$, and the substitution is therefore necessarily of order 2. Hence irregular substitutions, such as those suggested, cannot occur, and all the substitutions of G are regular.

The sub-groups which keep each one of the p^n+1 symbols successively unchanged are all conjugate, and that which keeps ∞ unchanged may be taken as their type.

This is clearly the group of order $p^n(p^n-1)$ which is generated by

$$z'\equiv z+1 \quad\text{and}\quad z'\equiv xz.$$

It is evident that this group contains the group of order p^n,

$$z'\equiv z,\quad z'\equiv z+1,\quad z'\equiv z+x,\ \dots\ z'\equiv z+x^{p^n-1},$$

self-conjugately. Hence this is the type of the single conjugate set of groups of order p^n, which according to Sylow's theorem is contained in G; and their number is p^n+1. This sub-group is such that all its operations, except identity, are of order p, and are permutable with each other.

Since $X^{-i}SX^i$ is the substitution $z+x^i$, the p^n-1 operations of order p form a single conjugate set within the sub-group which keeps ∞ unchanged, and therefore the $(p^n+1)(p^n-1)$ operations of order p contained in the group G form a single conjugate set. The remaining operations of the sub-group keeping ∞ unchanged (which all keep one other symbol fixed) consist of operations conjugate to xz and its powers, and therefore m can always be chosen so that any operation of the group which keeps two symbols unchanged is conjugate to $x^m z$. Since the first power of x which is congruent to unity is the $(p^n-1)^{\text{th}}$, the order of xz or X is p^n-1; and therefore the order of every operation which keeps two symbols fixed is a submultiple of p^n-1, while every such operation is a power of an operation of order p^n-1.

Since the operations which change all the symbols are regular, their orders must be sub-multiples of p^n+1; and, in close analogy with the operations which keep two symbols fixed, it may be shown that among the operations changing all the symbols there are operations of order p^n+1, while every operation changing all the symbols is the power of an operation of order p^n+1.

Thus, if the substitution

$$z' \equiv \frac{\alpha z+\beta}{\gamma z+\delta}$$

is thrown into the form

$$\frac{z'-\mu}{z'-\nu} \equiv \lambda\frac{z-\mu}{z-\nu},$$

λ is given by $$\lambda^2+\left(2-\frac{(\alpha+\delta)^2}{\alpha\delta-\beta\gamma}\right)\lambda+1 \equiv 0.$$

Now the coefficient of λ in this congruence can take all possible values, for, when

$$\alpha\delta-\beta\gamma \equiv 1,$$

$\dfrac{(\alpha+\delta)^2}{\alpha\delta-\beta\gamma}$ may be any quadratic residue, and, when

$$\alpha\delta-\beta\gamma \equiv x,$$

it may be any quadratic non-residue.

Now the congruence $\quad \lambda^2-x^i\lambda+1 \equiv 0$

is reducible when j can be found such that

$$x^i \equiv x^j+x^{-j},$$

and, if this congruence can be satisfied at all, it can only be satisfied in one way, for

$$x^j+x^{-j} \equiv x^k+x^{-k}$$

gives at once $\quad x^j \equiv x^k$ or x^{-k}.

For all other values of x^i the congruence is irreducible. But

$$\prod_{0}^{p^n-1} (\lambda^2 - z^i\lambda + 1)$$

$$= \lambda^{p^n}\left(\lambda+\frac{1}{\lambda}\right)\prod_{1}^{p^n-1}\left(\lambda+\frac{1}{\lambda}-x^i\right)$$

$$= \lambda^{p^n}\left(\lambda+\frac{1}{\lambda}\right)\left[\left(\lambda+\frac{1}{\lambda}\right)^{p^n-1}-1\right]$$

$$\equiv \lambda^{p^n}\left(\lambda^{p^n}+\frac{1}{\lambda^{p^n}}-\lambda-\frac{1}{\lambda}\right)$$

$$\equiv (\lambda^{p^n+1}-1)(\lambda^{p^n-1}-1).$$

Those quadratic congruences which are reducible give the quadratic factors of $\lambda^{p^n-1}-1$, and the factors $\lambda-1$ and $\lambda+1$ of $\lambda^{p^n+1}-1$; and therefore the irreducible quadratic congruences give the remaining factors of $\lambda^{p^n+1}-1$.

Now, since $$\lambda^{p^{2n}-1}-1 \equiv 0$$

has primitive roots, $$\lambda^{p^n+1}-1 \equiv 0$$

must also have primitive roots.

Hence among the quantities λ, defined by the irreducible congruences
$$\lambda^2 - x^i\lambda + 1 \equiv 0,$$

there must be some for which the first power of λ which is congruent to unity is the $(p^n+1)^{\text{th}}$. There are therefore operations $\dfrac{\alpha z+\beta}{\gamma z+\delta}$, whose order is p^n+1, since the order of the operation is equal to the index to which the corresponding λ belongs.

If $\dfrac{\alpha z+\beta}{\gamma z+\delta}$ is transformed into $\dfrac{\alpha' z+\beta'}{\gamma' z+\delta'}$ by any substitution of determinant unity, it is well known that

$$\alpha'+\delta' \equiv \alpha+\delta \quad\text{and}\quad \alpha'\delta'-\beta'\gamma' \equiv \alpha\delta-\beta\gamma,$$

and this result is still true when the transforming substitution has determinant x, if the transformed substitution $\dfrac{\alpha' z+\beta'}{\gamma' z+\delta'}$ be brought into its standard form so as to have unity or x for its determinant.

It may, however, be further shown that for the group G all the substitutions for which $\alpha+\delta$ and $\alpha\delta-\beta\gamma$ have given values form a single conjugate set. Thus, if $\frac{Az+B}{Cz+D}$ be the transforming substitution, α', β', γ', δ' are given by

$$A\alpha+B\gamma \equiv \alpha'A+\beta'C, \quad A\beta+B\delta \equiv \alpha'B+\beta'D,$$

$$C\alpha+D\gamma \equiv \gamma'A+\delta'C, \quad C\beta+D\delta \equiv \gamma'B+\delta'D,$$

and, since here $AD-BC$ may be either 1 or x, it is clear that, except when $\alpha\equiv\delta\equiv 1$ and $\beta\equiv\gamma\equiv 0$, α' and β' may be chosen arbitrarily, and therefore that every substitution $\frac{\alpha'z+\beta'}{\gamma'z+\delta'}$, for which

$$\alpha'+\delta'\equiv\alpha+\delta \quad\text{and}\quad \alpha'\delta'-\beta'\gamma'\equiv\alpha\delta-\beta\gamma,$$

is conjugate to $\frac{\alpha z+\beta}{\gamma z+\delta}$.

Now, the multiplier λ of a substitution Σ of order p^n+1 has been shown to satisfy an irreducible quadratic congruence of the form

$$\lambda^2-x^i\lambda+1\equiv 0,$$

and the multipliers λ^2, λ^3, &c., of its successive powers satisfy similar congruences. If λ^r satisfied the same congruence as λ^s, then

$$\lambda^{r+s}\equiv 1;$$

and hence, since λ is a primitive root of the congruence

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

$$r+s=p^n+1.$$

The multipliers of successive powers of Σ, with the exception of the $\frac{1}{2}(p^n+1)^{\text{th}}$, therefore satisfy $\frac{p^n-1}{2}$ different irreducible quadratic congruences of the above form. But this is the total number of such congruences, and therefore among the powers of Σ all possible values of $\frac{(\alpha+\delta)^2}{\alpha\delta-\beta\gamma}$, for substitutions whose orders are submultiples of p^n+1, occur. Combining this with the previous result, it follows that every operation changing all the symbols is conjugate with a power of an operation of order p^n+1, and is therefore itself a power of an operation of order p^n+1.

The operations $\frac{\alpha z+\beta}{\gamma z+\delta}$ and $\frac{-\alpha z-\beta}{-\gamma z-\delta}$ being identical, the result just proved may be stated in the form that all operations for which

$(\alpha+\delta)^2$ and $\alpha\delta-\beta\gamma$ have given values constitute a single conjugate set of operations.

Since $(\alpha+\delta)^2$ may be zero, or any one of the $\frac{p^n-1}{2}$ quadratic residues, while $\alpha\delta-\beta\gamma$ may be either 1 or x, there must be p^n+1 conjugate sets of operations, exclusive of identity.

This discussion of the orders of the operations of G, and their distribution into conjugate sets, may be applied to simplify considerably the corresponding investigation for the group H.

5. *On the Distribution of the Operations of H in Conjugate Sets.*

The cyclical substitutions of p^n+1 and p^n-1 symbols that G contains are odd substitutions, *i.e.*, substitutions that are equivalent to an odd number of transpositions. Hence the self-conjugate subgroup H of index 2 consists of the even substitutions of G.

It follows at once that all the substitutions of order p contained in G belong to H, and that operations of G of orders $\frac{p^n+1}{\mu}$ and $\frac{p^n-1}{\nu}$ will belong to H when μ and ν are even.

Hence the operations of H which keep no symbols fixed have for their orders sub-multiples of $\frac{p^n+1}{2}$, and every such operation is the power of an operation of order $\frac{p^n+1}{2}$; while the operations which keep two symbols fixed are powers of operations of order $\frac{p^n-1}{2}$.

It is not, however, now the case that all the operations for which $(\alpha+\delta)^2$ is the same form a single conjugate set. For, if the substitution $z+1$ is transformed into $z+x^i$ by $\frac{\alpha z+\beta}{\gamma z+\delta}$,

$$\alpha\equiv\delta x^i \quad \text{and} \quad \gamma\equiv 0;$$

but
$$\alpha\delta\equiv 1;$$

and therefore x^i must be a quadratic residue.

The operations of order p therefore fall into two conjugate sets, each containing $\frac{1}{2}(p^{2n}-1)$.

If, now, $\frac{\alpha z+\beta}{\gamma z+\delta}$ be any substitution whose order is a sub-multiple of

$\frac{p^n+1}{2}$, and if this be transformed into $\frac{\alpha' z+\beta'}{\gamma' z+\delta'}$ by $\frac{Az+B}{Cz+D}$, by combining the first two of the equations for the transformed coefficients already given with

$$AD-BC\equiv 1,$$

it is easily shown that

$$\beta'\left[C^2\beta+CD\,(\delta-\alpha)-D^2\gamma\right]\equiv \alpha'^2-(\alpha+\delta)\,\alpha'+1.$$

Now, $\beta+\frac{D}{C}(\delta-\alpha)-\frac{D^2}{C^2}\gamma$ cannot vanish for any value of $\frac{D}{C}$, for, when equated to zero, it would give the fixed elements of the operation, and no elements remain fixed; and, when the p^n different possible values of $\frac{D}{C}$ are successively substituted for it, this expression will take $\frac{p^n+1}{2}$ different values, since the congruence

$$\beta+\frac{D}{C}(\delta-\alpha)-\frac{D^2}{C^2}\gamma\equiv\beta+x'(\delta-\alpha)-x'^2\gamma$$

will always have two and only two roots, and for one value of x' these will be equal. Moreover, there are only $\frac{p^n-1}{2}$ quadratic residues, so that the expression in question can, by suitably choosing $\frac{D}{C}$, be made either a residue or a non-residue.

It follows that, when all possible values are given to C and D,

$$C^2\beta+CD\,(\delta-\alpha)-D^2\gamma$$

can take every possible value except zero.

Hence, when α' is chosen arbitrarily, β' may have every possible value except zero. But since

$$\alpha'\delta'-\beta'\gamma'\equiv 1 \quad\text{and}\quad \alpha'+\delta'\equiv x',$$

where

$$\lambda^2-x'\lambda+1\equiv 0$$

is irreducible, the value $\beta=0$ is in any case inadmissible.

It follows from this discussion that all the operations which keep no symbols fixed, and for which $(\alpha+\delta)^2$ has the same value, form a single conjugate set.

A closely similar discussion of the congruence connecting α', β', C, D leads to the same result for operations whose orders are sub-multiples of $\frac{p^n-1}{2}$.

There are, therefore, two conjugate sets of substitutions for which

$$(\alpha+\delta)^2 = 4,$$

and one set of every other possible value. The total number of conjugate sets, exclusive of identity, is $\frac{p^n+3}{2}$.

6. *Proof that H is a Simple Group.*

The proof which Herr Weber gives in his *Elliptische Functionen und Algebraische Zahlen* that the group of the modular equation is simple may be applied directly, with suitable modifications, to show that the analogous group H is simple. The following proof of this property, founded on the discussion just given of the distribution of the operations in conjugate sets, is, however, considerably shorter.

Let K be a self-conjugate sub-group of H, and suppose first that K contains an operation of order p. It must then contain the whole of one of the two conjugate sets of operations of order p, and therefore the whole of both sets, since by a previous remark a sub-group which contains all the operations $z+x^i$ where x^i is a quadratic residue must also contain those where x^i is a non-residue. The group K therefore contains the two operations $\frac{\alpha z+\beta}{\gamma z+2-\alpha}$ and $z+x^i$, where α, γ and x^i may be chosen arbitrarily. The result of combining these two is

$$\frac{(\alpha+\gamma x^i)\,z+\beta+(2-\alpha)\,x^i}{\gamma z+2-\alpha},$$

and the sum of the first and last coefficients in this substitution, namely, $2+\gamma x^i$, may be made anything whatever.

Hence, in this case, K coincides with H.

Suppose now that K contains a substitution keeping two symbols fixed, say $\frac{x^i z}{x^{-i}}$. It will then contain $\frac{\alpha z+\beta}{\gamma z+\delta}$, where

$$\alpha+\delta = x^i+x^{-i}.$$

These combined give $$\frac{\alpha x^i z+\beta x^{-i}}{\gamma x^i z+\delta x^{-i}},$$

and, if now $\alpha \equiv x^{-i}, \quad \delta \equiv x^i, \quad \gamma \equiv 0, \quad \beta \not\equiv 0,$

this substitution is $z+\beta x^{-i}$,

which is of order p. Hence, again, K coincides with H.

Suppose, lastly, that K contains an operation, displacing all the symbols, for which

$$\alpha+\delta\equiv x^i;$$

then K contains $\frac{x^iz+1}{-z}$ and $\frac{1}{-z+x^i}$, and these combined give $z-2x^i$, an operation of order p. Hence, once again, K coincides with H.

It follows, therefore, that, since H contains no self-conjugate sub-group different from itself, it is a simple group.

7. *On H_n regarded as a Sub-Group of H_m.*

If a suffix be now used to denote the degree of the irreducible congruence on which the coefficients of the substitutions of G or H depend, it is immediately clear that H_N will contain H_n, if p^n-1 is a factor of p^N-1. For, if

$$p^N-1=\lambda\,(p^n-1),$$

and if y is a primitive root of the congruence

$$y^{p^N-1}-1\equiv 0,$$

then y^λ is a primitive root of

$$x^{p^n-1}-1\equiv 0,$$

and the group H_n is derived from

$$z'\equiv\frac{-1}{z},\quad z'\equiv z+1,\quad z'\equiv\frac{y^\lambda z}{y^{-\lambda}}.$$

The sub-group of H_N with which H_n is permutable may be determined as follows. If $\frac{\alpha z+\beta}{\gamma z+\delta}$ a substitution of H_n is transformed into $\frac{\alpha' z+\beta'}{\gamma' z+\delta'}$ by any substitution $\frac{Az+B}{Cz+D}$ of H_N, then

$$\begin{aligned}
\alpha' &\equiv AD\alpha-AC\beta+BD\gamma-BC\delta,\\
\beta' &\equiv -AB\alpha+A^2\beta\;-B^2\gamma\;+AB\delta,\\
\gamma' &\equiv CD\alpha-C^2\beta\;+D^2\gamma\;-CD\delta,\\
\delta' &\equiv -BC\alpha+AC\beta-BD\gamma+AD\delta.
\end{aligned}$$

Now $\frac{Az+B}{Cz+D}$, where $AD-BC\equiv 1$, is permutable with H_n, if, when these congruences are applied to the three generating substitutions of H_n, the values of α', β', γ', δ' obtained are all powers of y^{λ}.

The respective values of α, β, γ, δ are

$$\begin{array}{cccc} 0, & -1, & 1, & 0, \\ 1, & 1, & 0, & 1, \\ y^{\lambda}, & 0, & 0, & y^{-\lambda}; \end{array}$$

and therefore $AC+BD$, A^2+B^2, C^2+D^2, $1-AC$, A^2, C^2, $ADy^{\lambda}-BCy^{-\lambda}$, $AB\,(y^{\lambda}-y^{-\lambda})$, $CD\,(y^{\lambda}-y^{-\lambda})$, and $ADy^{-\lambda}-BCy^{\lambda}$ are powers of y^{λ}. Hence, since the sum of any number of powers of y^{λ} is again a power of y^{λ}, it follows that A^2, B^2, C^2, D^2, AB, AC, AD, BC, BD, CD must all of them be powers of y^{λ}. If, then, λ be odd, A, B, C, D must themselves be powers of y^{λ}, and the group H_n is only permutable with itself; if, however, λ be even, the coefficients may also be of the form $y^{(m+\frac{1}{2})\lambda}$. Now, if $\frac{\alpha z+\beta}{\gamma z+\delta}$ is any substitution of H_n, $\frac{\alpha y^{\frac{1}{2}\lambda}z+\beta y^{\frac{1}{2}\lambda}}{\gamma y^{-\frac{1}{2}\lambda}z+\delta y^{-\frac{1}{2}\lambda}}$ is a substitution of the second kind which transforms H_n into itself, and in this way each such substitution is obtained once and once only. It follows that, when λ is even, the order of the group with which H_n is permutable is twice the order of H_n. This group is evidently G_n.

Now p^n-1 will only divide p^N-1, when n divides N and λ is odd or even according as $\frac{N}{n}$ is odd or even. The group H_n is therefore one of a conjugate set of sub-groups of H_{ns} whose number is

$$p^{n(s-1)}\,(p^{2n(s-1)}+p^{2n(s-2)}+\ldots+p^{2n}+1),$$

or one half of this number according as s is odd or even. In particular H_1 the group of the modular equation is always contained as a sub-group in H_n.

Consider now the case of $s=2$, and H_n as a sub-group of H_{2n}. Since p^n+1 is not a factor of $p^{2n}+1$, none of the operations of H_n displace all the symbols of H_{2n}; and therefore any operation of H_n of the order $\frac{p^n+1}{2}$ occurs as the p^n-1 power of some operation of H_{2n} of order $\frac{p^{2n}-1}{2}$ which keeps two symbols fixed. But the cyclical sub-groups of H_{2n} of order $\frac{p^{2n}-1}{2}$ are all conjugate to the sub-group arising from $\frac{yz}{y^{-1}}$; and therefore H_n must contain operations of order $\frac{p^n+1}{2}$ which are conjugate, within H_{2n}, to $\frac{y^{p^n-1}z}{y^{-p^n+1}}$. It follows that among the groups conjugate to H_n, within H_{2n}, which are all isomorphous with H_n, there must be one at least containing the operation $\frac{y^{p^n-1}z}{y^{-p^n+1}}$.

A group H'_n, contained in H_{2n}, which is isomorphous with H_n, and which contains the operation $\frac{y^{p^n-1}z}{y^{-p^n+1}}$, consists of all operations of the form

$$\frac{\alpha'z+\beta'}{\gamma'z+\delta'},\ (\alpha'\delta'-\beta'\gamma'\equiv 1),$$

for which α', β', γ', δ' are given in form by

$$\alpha'\equiv r+s\,(y^{p^n-1}-y^{-p^n+1}),\qquad \beta'\equiv u+v\,(y^{p^n-1}-y^{-p^n+1}),$$
$$\delta'\equiv r-s\,(y^{p^n-1}-y^{-p^n+1}),\qquad \gamma'\equiv -u+v\,(y^{p^n-1}-y^{-p^n+1}),$$

where r, s, u, v are powers of y^{p^n+1}.

That these operations actually form a group may be verified at once by forming the operation which is compounded of any two operations of the above form, when it will be found that the coefficients in the resulting operation are again of the same form. That the group thus defined may be obtained by transforming H_n by an operation $\frac{Az+B}{Cz+D}$ may be proved as follows.

If the formulæ given at the foot of the last page but one for α', β', γ', δ' are equivalent to the above-written forms, the quantities r, u, $s\,(y^{p^n-1}-y^{-p^n+1})$ and $v\,(y^{p^n-1}-y^{-p^n-1})$ must be given by

$$r\equiv \alpha+\delta,$$
$$u\equiv (CD+AB)(\delta-\alpha)+(A^2+C^2)\,\beta-(B^2+D^2)\,\gamma,$$
$$s\,(y^{p^n-1}-y^{-p^n+1})\equiv (AD+BC)(\alpha-\delta)-2AC\beta+2BD\gamma,$$
$$v\,(y^{v^n-1}-y^{-p^n+1})\equiv (AB-CD)(\delta-\alpha)+(A^2-C^2)\,\beta+(D^2-B^2)\,\gamma.$$

It has therefore to be shown that an operation $\frac{Az+B}{Cz+D}$ can be found, such that, when r, u, s, v are given powers of x satisfying

$$r^2+u^2-(s^2+v^2)(y^{p^n-1}-y^{-p^n+1})^2\equiv 1,$$

the above congruences determine α, β, γ, δ as powers of x or y^{p^n+1}.

Now it has been shown above that, since y^{p^n-1} is a primitive root of the congruence

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

it must satisfy an irreducible quadratic congruence

$$x'^2 - x^{\prime}x' + 1 \equiv 0,$$

where
$$x = y^{p^n+1}$$

is a primitive root of
$$\lambda^{p^n-1}-1 \equiv 0.$$

It follows that $y^{p^n-1}+y^{-p^n+1}$ is a power of x, and therefore so also is $(y^{p^n-1}-y^{-p^n+1})^2$, which will be called ξ^2. On the other hand, ξ is clearly not expressible rationally in terms of x.

If, now, m and n are any powers of x, the expression

$$m+n\xi$$

includes, with zero, p^{2n} incongruous values; and therefore every integral power of y can be expressed in this form.

Since ξ^2 is a power of x, so also is $(m+n\xi)(m-n\xi)$, and $m+n\xi$, $m-n\xi$ are therefore either both even or both odd powers of y.

Suppose then that

$$A^2 \equiv m+n\xi, \qquad B^2 = m'+n'\xi,$$

$$C^2 \equiv m-n\xi, \qquad D^2 = m'-n'\xi,$$

where $m+n\xi$, $m'+n'\xi$ are odd powers of y, and $m^2-n^2\xi^2$, $m'^2-n'^2\xi^2$ are odd powers of x. They can obviously be chosen so in a variety of ways satisfying

$$A^2D^2+B^2C^2-2ABCD \equiv (AD-BC)^2 \equiv 1.$$

From these forms it at once follows that A^2+C^2 and B^2+D^2 are powers of x, while A^2-C^2, B^2-D^2, AC and BD are, each of them, powers of x multiplied by ξ.

Also
$$AD+BC = A^2D^2-B^2C^2 \equiv 2\,(m'n-mn')\,\xi,$$

and
$$(CD-AB)(CD+AB) \equiv -2\,(m'n+mn')\,\xi,$$

while
$$(CD-AB)(AD-BC) = AC\,(B^2+D^2)-BD\,(A^2+C^2)$$

is also a power of x multiplied by ξ; and therefore $CD-AB$ is a power of x multiplied by ξ, while $CD+AB$ is a power of x. The values assumed for A, B, C, D satisfy therefore all the conditions given at the beginning of this investigation, and the group whose operations are of the form

$$\frac{(r+s\xi)\,z+u+v\xi}{(-u+v\xi)\,z+r-s\xi}$$

is obtained from the transformation of H_n by $\dfrac{Az+B}{Cz+D}$.

The operation $\dfrac{Az+B}{Cz+D}$ does not belong to H_{2n}, since A, B, C, D are not rationally expressible in terms of y; it will, however, evidently be an operation of the group H_{4n}; and the group H'_n is therefore conjugate with H_n within H_{4n}, but not within H_{2n}. It necessarily follows that H_{2n} contains at least two different conjugate sets of sub-groups, each isomorphous with H_n.

The values

$$r \equiv \tfrac{1}{2}\,(y^{p^n-1}+y^{-p^n+1}), \quad s \equiv \tfrac{1}{2}, \quad u \equiv v \equiv 0,$$

of which the first has been shown to be a power of x, give the operation $\dfrac{y^{p^n-1}z}{y^{-p^n+1}}$ contained in H'_n.

This transformed form of the group may be used to bring out the analogy between the cyclical sub-groups of orders $\tfrac{1}{2}(p^n-1)$ and $\tfrac{1}{2}(p^n+1)$. Thus in the original form of the group a typical cyclical sub-group of order $\tfrac{1}{2}(p^n-1)$ is that arising from $\dfrac{xz}{x^{-1}}$. This keeps the symbols 0, ∞ unchanged, and can therefore only be transformed into itself by operations which either keep 0, ∞ unchanged, or by operations which interchange them. The former are the operations of the sub-group itself, and the latter are the $\tfrac{1}{2}(p^n-1)$ operations of order 2 of the form $\dfrac{-x^i}{x^{-i}z}$ contained in H_n. Each of the latter transforms any operation of the cyclical sub-group into its own inverse; and the $\tfrac{1}{2}(p^n-1)$ operations of order 2, taken with the operations of the cyclical sub-group, form a sub-group of dihedral type of order p^n-1.

In the transformed group H'_n a typical cyclical sub-group of order $\tfrac{1}{2}(p^n+1)$ is that arising from $\dfrac{y^{p^n-1}z}{y^{-p^n+1}}$. Considered as an operation in the group H_{2n}, this keeps the symbols 0, ∞ unchanged, and therefore is only transformed into itself by the operations $\frac{y^i z}{y^{-i}}$ and $\frac{-y^i}{y^{-i} z}$ of H_{2n}. Those of the former type which belong to H_n are the operations of the cyclical sub-group itself, while those of the latter type are the operations included under the form

$$\frac{u+v\,(y^{p^n-1}-y^{-p^n+1})}{\{-u+v\,(y^{p^n-1}-y^{-p^n+1})\}\,z},$$

where $$u^2-v^2\,(y^{p^n-1}-y^{-p^n+1})^2 \equiv 1.$$

This congruence has for its solutions

$$u = \pm\tfrac{1}{2}\,(y^{m\,(p^n-1)}+y^{-m\,(p^n-1)}),$$

$$v = \pm\tfrac{1}{2}\,\frac{y^{m\,(p^n-1)}-y^{-m\,(p^n-1)}}{y^{p^n-1}-y^{-p^n+1}},$$

$$m = 0,\ 1,\ \dots\ p^n$$

and these correspond to the $\frac{1}{2}\,(p^n+1)$ operations

$$\frac{y^{m\,(p^n-1)}}{-y^{-m\,(p^n-1)}\,z},\quad \left[m = 0,\ 1,\ \dots\ \tfrac{1}{2}\,(p^n-1)\right].$$

Finally, these $\frac{1}{2}\,(p^n+1)$ operations of order 2, taken with the cyclical sub-group arising from $\frac{y^{p^n-1}z}{y^{-p^n+1}}$, give a dihedral group of order p^n+1.

The sub-groups of tetrahedral type, and those of octahedral and icosahedral types for the cases of $p^n \equiv \pm 1$ (mod 8 and mod 5, respectively), the existence of which Herr Gierster demonstrates in his memoir for the case $n = 1$, may also be shown to exist in the general case.

The complete discussion which is given in the following paragraph of all possible sub-groups for the case $p = 2$ indicates the lines on which a similar discussion may be carried out for the case of p an odd prime; and suggests that the types of sub-group which have been shown to exist, including those mentioned in the last sentence probably exhaust all types that actually exist.

8. *On the Group G, when $p = 2$.*

The necessary modifications of the foregoing theorems with respect to the omitted case of $p = 2$ are now very readily made, and it seems hardly necessary to repeat proofs which are almost identical with those already given.

As was shown in § 3, when $n = 2$, there are no quadratic non-residues, and therefore all the operations of the group G of order $2^n (2^{2n}-1)$ may be brought to the standard form in which the determinant is unity. Considered as a permutation group of 2^n+1 symbols, the operations which displace all the symbols are all powers of operations of order 2^n+1, those which keep one symbol fixed are all of order 2, and those which keep two symbols fixed are powers of operations of order 2^n-1.

The operations of order 2 form a single conjugate set, as also do all the operations for which $(\alpha+\delta)^2$ has a given value; but here $(\alpha+\delta)^2$, including the value zero which gives the operations of order 2, may have any one of 2^n values, and there are, therefore, 2^n different conjugate sets of operations, exclusive of identity.

The proof that H, for p an odd prime, is a simple group will apply exactly to show that G is simple, when $p = 2$.

It may also be shown, exactly as in the corresponding case for H, that corresponding to each cyclical sub-group of order 2^n+1 or 2^n-1 there is a sub-group of dihedral type of order $2(2^n+1)$ or $2(2^n-1)$ containing the cyclical group as a self-conjugate sub-group, and that no cyclical sub-group is contained self-conjugately in any sub-group of higher order than these dihedral groups. As regards sub-groups of tetrahedral, octahedral, and icosahedral types, there can clearly be none of octahedral type, since the groups contain no operations of order 4. If n is odd, 5 divides neither 2^n+1 nor 2^n-1, and hence, for an odd n, G cannot contain an icosahedral sub-group. If, however, n is even, G_n contains G_2 as a sub-group, and this, being of order 60, is necessarily an icosahedral group. Since the icosahedral group contains tetrahedral sub-groups, G_n, when n is even, will have sub-groups of tetrahedral type. Finally, when n is odd, 2^n+1 is divisible by 3 and not 2^n-1, and, since a sub-group of order 4 cannot be transformed into itself by an operation changing all the symbols, a tetrahedral sub-group, which must contain a group of order 4 self-conjugately, cannot exist in this case.

It will now be shown that the sub-groups already enunciated, together with the sub-group that keeps one symbol fixed, and *its* sub-groups, and the sub-group of type $G_{n'}$, where n' is a factor of n, exhaust all existing types. This will be proved by a modification and extension of the process used by Herr Gierster in his often referred to memoir in discussing the corresponding question for the modular group.

Let Γ be any sub-group of G_n of order $2^m g' = g$, where g' is a factor of $2^{2n}-1$, and let Σ be an operation of odd order p_1 contained in Γ, there being no operations in Γ of higher order than p_1. Then the sub-group arising from Σ is permutable within Γ, either with itself or with a dihedral group of order $2p_1$, and it therefore forms one of a set of either $\frac{g}{p_1}$ or $\frac{g}{2p_1}$ conjugate sub-groups. No two of these sub-groups contain a common operation, for, if they did, all their operations would be common. Hence, omitting identity from each such sub-group, they contain in all $\frac{(p_1-1)g}{p_1}$ or $\frac{(p_1-1)g}{2p_1}$ different operations. Let, now, Σ' be an operation of odd order p_2 contained among the remaining operations, there being no remaining operation of a higher order than p_2. Then, as before, the set of sub-groups conjugate with the cyclical sub-group arising from Σ' contain either $\frac{(p_2-1)g}{p_2}$ or $\frac{(p_2-1)g}{2p_2}$ different operations of odd order, and no one of these can coincide either with another of the same set or with one of the previous set. If this process is continued till the operations of odd order are exhausted, there remain only operations of order 2. Any one S of these is permutable with a sub-group of order 2^m, and therefore forms one of a set of $\frac{g}{2^m}$ or g' conjugate operations. If among these g' operations there occurs none of the group of order 2^m with which S is permutable, then each operation, except identity, of this group will give rise to a similar set, no two sets containing a common operation, and the number of operations of order 2 contained in Γ will be $(2^m-1)g'$. It is necessary therefore to determine in what cases the sub-group of order 2^m contains operations conjugate within Γ.

The general type of group of order 2^m contained in G is the group arising from the m permutable operations of order 2,

$$z+x^{a_1},\ z+x^{a_2},\ \dots\ z+x^{a_m},$$

where $a_1, a_2, \dots a_m$ are any m chosen integers from $1, 2, \dots 2^n-1$.

No operation of this sub-group can be transformed into another, except by the operations of the sub-group arising from

$$z+1 \text{ and } xz.$$

Hence Γ must contain the operation $x^{\nu}z$, or an operation conjugate to it within the sub-group which keeps ∞ fixed, if the sub-group of order 2^m contains conjugate operations. Now, the $\frac{2^n-1}{\nu}$ powers of $x^{\nu}z$ transform $z+x^{n_1}$ into a set of $\frac{2^n-1}{\nu}$ conjugate operations of the same form $z+x^t$, and these must all be contained in the sub-group of order 2^m, as otherwise 2^m would not be the highest power of 2 dividing g.

Hence, if a is the symbol that any sub-group of Γ of order 2^m keeps fixed, and if $\frac{2^n-1}{\nu}$ is the order of the highest operation of odd order contained both in Γ and in the sub-group keeping a fixed, the operations of the sub-group of order 2^m will be conjugate in sets of $\frac{2^n-1}{\nu}$. This involves that $\frac{2^n-1}{\nu}$ is a factor of 2^m-1, and is also one of the numbers $p_1, p_2, \ldots$. If, then,

$$\frac{2^n-1}{\nu}=p_r,$$

the number of operations of order 2 contained in Γ is $\frac{(2^m-1)g'}{p_r}$.

Adding together the numbers of different operations thus obtained, including the identical operation, there results

$$g=1+\Sigma\frac{(p_1-1)g}{s_1p_1}+\frac{(2^m-1)g}{2^mp_r},$$

where each s is either 1 or 2.

Hence $$g=\frac{1}{1-\Sigma\frac{p_1-1}{s_1p_1}-\frac{2^m-1}{2^mp_r}}.$$

If m is zero, so that Γ contains no operations of order 2, each s must be unity, and the relation becomes

$$g=\frac{1}{1-\Sigma\frac{p_1-1}{p_1}}.$$

Now g is a positive integer, and each p is an odd number. Hence in this case there can be only one term under the sign of summation, and

$$g = p_1.$$

It follows that the only sub-groups not containing operations of order 2 are the cyclical sub-groups.

Again
$$\frac{p_1-1}{s_1 p_1} \geqslant \tfrac{1}{3},$$

so that, when m is not zero, there can be at most two terms under the sign of summation; and, if there are two terms, $s_1 = s_2 = 2$; while, if there is one term only, s_1 may be either 1 or 2.

With one term only, if $s_1 = 1$,

$$\frac{1}{g} = \frac{1}{p_1} - \frac{2^m-1}{2^m p_r},$$

where p_r is either unity or p_1.

If $p_r = p_1$, $g = 2^m p_1$, and Γ is a sub-group of the sub-group that keeps one symbol fixed.

If $p_r = 1$, $\frac{2^m p_1}{2^m-(2^m-1)\,p_1}$ must be an integer, and this can only be so when $p_1 = 1$. Γ is then a sub-group of order 2^m.

With one term only, and $s_1 = 2$,

$$\frac{1}{g} = \frac{1}{2} + \frac{1}{2p_1} - \frac{2^m-1}{2^m p_r}.$$

If $p_r = p_1$,
$$\frac{1}{g} = \frac{2^{m-1}p_1-(2^{m-1}-1)}{2^m p_1},$$

and, since p_1 is a factor of 2^m-1, g can only be an integer when $p_1 = 1$; leading again to a sub-group of order 2^m.

If $p_r = 1$, m must be unity, and Γ is a dihedral group of order $2p_1$.

When there are two terms under the sign of summation, both s_1 and s_2 must be 2 that g may be a positive integer. Hence

$$\frac{1}{g} = \frac{1}{2p_1} + \frac{1}{2p_2} - \frac{2^m-1}{2^m p_r},$$

where p_r is either 1, p_1 or p_2.

Since p_1, p_2 are odd integers, g cannot be positive if p_r is unity, and therefore it may be taken as p_1. Then

$$\frac{1}{g} = \frac{2^{m-1}p_1-(2^{m-1}-1)p_2}{2^m p_1 p_2}.$$

If q is the G.C.M. of p_1 and p_2, so that

$$p_1 = qp_1', \quad p_2 = qp_2',$$

where p_1', p_2' are relatively prime, then

$$\frac{1}{g} = \frac{2^{m-1}p_1'-(2^{m-1}-1)p_2'}{2^m q p_1' p_2'}.$$

The numerator of this fraction is prime relatively to $2^m p_1' p_2'$, and hence, if g is an integer,

$$2^{m-1}p_1'-(2^{m-1}-1)p_2' = q',$$

a factor of q.

The general values of p_1' and p_2' which satisfy this equation are given by

$$p_1' = q'+k(2^{m-1}-1),$$

$$p_2' = q'+k\,2^{m-1};$$

and therefore

$$p_1 = qq'+kq(2^{m-1}-1),$$

$$p_2 = qq'+kq\,2^{m-1}.$$

Now p_1 is a factor of 2^m-1, so that kq cannot be greater than 2. Also q is odd and is therefore unity, as also must therefore be q'. Hence

$$p_1 = 1+k(2^{m-1}-1),$$

$$p_2 = 1+k\,2^{m-1},$$

where k can only be 1 or 2, and must be 2 since p_1 is odd. Then

$$p_1 = 2^m-1, \quad p_2 = 2^m+1.$$

Also, since p_1 is a factor of 2^n-1, m must be a factor of n. Hence this last possible case leads to the sub-groups of type $G_{n'}$, where n' is a factor of n.

9. *On certain Special Cases of the Groups G and H.*

There are three values of p^n for which the corresponding groups are already known. When

$$p^n = 2^2,$$

G is a simple group of order 60, and must therefore be a form of the icosahedral group. Thus a new and very simple specification is obtained for this group, as consisting of all substitutions of the form

$$\left.\begin{aligned} z' &\equiv \frac{\alpha z+\beta}{\gamma z+\delta} \\ \alpha\delta-\beta\gamma &\equiv 1 \end{aligned}\right\} \text{(mod 2)},$$

where the coefficients are either 0, 1, x, or x^2; x being such that

$$x^2+x+1 \equiv 0 \text{ (mod 2)}.$$

When $$p^n = 2^3,$$

G is a simple group of order 504. This group was first discovered by Dr. Cole (*American Journal of Mathematics*, Vol. xv.).

When $$p^n = 3^2,$$

H is a simple group of order 360, and must therefore be a form of the alternating group of 6 symbols. G is a triply-transitive group of 10 symbols, order 720, containing H self-conjugately.

It is curious to notice that, as is well known, the symmetric group of 6 symbols, order 720, which also contains the alternating group self-conjugately, can be expressed as a doubly-transitive group of 10 symbols; so that there are two distinct transitive groups of 10 symbols, one doubly and the other triply transitive, both of order 720, and both containing the same doubly-transitive simple group of order 360 as a self-conjugate sub-group.

10. *On a Property of certain Transitive Groups.*

The sub-group of G which keeps one symbol fixed is doubly transitive in p^n symbols while its order is $p^n(p^n-1)$. Now the order of a doubly-transitive group in m symbols is necessarily divisible by $m(m-1)$, and it may be shown that, when it is equal to this number, m is the power of a prime, and moreover that, as has been seen to be the case with G, the operations of the sub-group of order m must all be permutable with each other. Thus, assuming the existence of a doubly-transitive group in m symbols of order $m(m-1)$, its operations must displace all the symbols or all but one; and therefore the $m-2$ symbols into which a given symbol is changed, by the operations of a sub-group keeping one symbol fixed, are all different. Hence among the operations of the m sub-groups, each of which keeps one symbol unchanged, there must be $m-2$ operations which change a given symbol a into another given symbol

b; for each sub-group contains one such operation except those that keep a and b respectively unchanged.

Now the group contains $m-1$ operations changing a into b, and hence among the $m-1$ operations which change all the symbols there is one, and only one, which changes a into b. It follows, therefore, that these $m-1$ operations with identity form a sub-group of order m, since the product of any two of them necessarily changes all the symbols. This sub-group of order m is evidently self-conjugate.

If, now, P is any particular operation of this sub-group of order m, and if A is any operation of the sub-group that keeps a fixed, the operations

$$A^{-1}PA$$

are clearly all different, for the symbols into which they change a are all different. Hence the $m-1$ operations which change all the symbols form a single conjugate set within the main group, and they are therefore all of the same order. Since with identity these operations form a group, their common order must be a prime, and hence finally m must be the power of a prime.

Since P is one of a set of $m-1$ conjugate operations, the operations permutable with P form a sub-group whose order is

$$m(m-1) \div (m-1),$$

i.e., m. Hence every operation of the sub-group of order m is permutable with every other, and the sub-group is therefore Abelian.

The type of doubly-transitive group of order $p^n(p^n-1)$ which appears as that sub-group of G which keeps one symbol fixed is not, however, the only possible type. Thus Dr. Cole in his analysis of the transitive groups of 9 letters (*Bulletin of the New York Mathematical Society*, July, 1893) has shown that there are two such doubly-transitive groups of order 82. All possible types may be obtained by the following considerations. The sub-group of order p^n is generated by n permutable operations $P_1, P_2, \dots P_n$ of order p. Let Σ be any operation of the sub-group K that keeps one symbol fixed, and let

$$\Sigma^{-1}P_1\Sigma = P_1^{n_1}P_2^{n_2}\dots P_n^{a_n},$$

$$\dots \quad \dots \quad \dots \quad \dots$$

$$\Sigma^{-1}P_n\Sigma = P_1^{n_1}P_2^{n_2}\dots P_n^{n_n},$$

so that

$$\Sigma^{-1}P_1^xP_2^y\dots P_n^z\Sigma$$

$$= P_1^{a_1x+b_1y+\dots+n_1z}\,P_2^{a_2x+b_2y+\dots+n_2z}\dots P_n^{a_nx+b_ny+\dots+n_nz}.$$

Since no operation of the sub-group K is permutable with any operation of the sub-group of order p^n, it follows that, if the p^n-1 operations of this sub-group other than identity be transformed by all the operations of the sub-group K in succession, a permutation group is obtained which is holohedrically isomorphous with K. The operations of this sub-group are, as the last equation shows, defined by congruences of the form

$$\left.\begin{array}{l} x' \equiv a_1x+b_1y+\ldots+n_1z \\ y' \equiv a_2x+b_2y+\ldots+n_2z \\ \ldots \quad \ldots \quad \ldots \quad \ldots \\ z' \equiv a_nx+b_ny+\ldots+n_nz \end{array}\right\} \pmod{p};$$

and therefore the problem of determining all possible forms of the sub-group K is equivalent to that of finding all the sub-groups of the general homogeneous linear group in n variables which are of order p^n-1, and all of whose operations displace all the p^n-1 symbols in terms of which the group can be expressed transitively.

Thursday, March 8th, 1894.

Mr. A. B. KEMPE, F.R.S., President, in the Chair.

Mr. Adam Brand, M.A., Fellow of Pembroke College, Cambridge, was elected a member. Mr. F. W. Hill, M.A., and Major Hippisley, R.E., were admitted into the Society.

The following communications were made:—

Groups of Points on Curves: Mr. F. S. Macaulay.

On a Simple Contrivance for Compounding Elliptic Motions: Mr. G. H. Bryan.*

On the Buckling and Wrinkling of Plating supported on a Framework under the Influence of Oblique Stresses: Mr. G. H. Bryan.

On the Motion of Paired Vortices with a Common Axis: Mr. A. E. H. Love.

On the Existence of a Root of a Rational Integral Equation: Prof. E. B. Elliott.

* For an account of this contrivance, see *Nature*, March 22nd, 1894, p. 498.

The following presents to the Library were received :—

"Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich," 38$^{\text{er}}$ Jahrgang, Hefte 3, 4 ; Zurich, 1893.

"Beiblätter zu den Annalen der Physik und Chemie," Bd. xviii., St. 2 ; Leipzig, 1894.

"Proceedings of the Royal Society," Vol. liv., Nos. 330, 331.

"Jahrbuch über die Fortschritte der Mathematik," Bd. xxiii., Jahrgang 1891, Heft 1 ; Berlin, 1894.

"Proceedings of the Royal Society of Edinburgh," Vol. xix., Session 1891–2.

"Nyt Tidsskrift for Mathematik," A. Fjerde Aargang, Nos. 7, 8 ; B. Fjerde Aargang, No. 4 ; Copenhagen, 1893.

"Mittheilungen der Mathematischen Gesellschaft in Hamburg," Bd. iii., Heft 4.

D'Ocagne, M.—"Abaque général de la Trigonométrie Sphérique," pamphlet.

"Berichte über die Verhandlungen der Koniglich sächsischen Gesellschaft der Wissenschaften zu Leipzig, Math. Phys. Classe," 1893, 7–9.

"Jornal de Sciencias Mathematicas e Astronomicas," Vol. xi., No. 6 ; Coimbra, 1894.

"Bulletin des Sciences Mathématiques," Tome xviii., Janvier, 1894 ; Paris.

Macfarlane, A.—"On the Definitions of the Trigonometric Functions," 8vo ; Boston.

"Bulletin of the New York Mathematical Society," Vol. iii., No. 5 ; February, 1894.

"Rendiconti del Circolo Matematico di Palermo," Tomo vii., Fasc. 6 ; November, December, 1893.

"Atti della Reale Accademia dei Lincei—Rendiconti," Sem. 1, Vol. iii., Fasc. 2, 3 ; Roma.

"Journal de l'Ecole Polytechnique," 63$^{\text{ème}}$ Cahier ; Paris, 1893.

"Educational Times," March, 1894.

"Journal für die reine und angewandte Mathematik," Bd. cxiii., Heft 1 ; Berlin, 1894.

"Annals of Mathematics," Vol. viii., No. 2 ; University of Virginia.

"Indian Engineering," Vol. xv., Nos. 3–6.

"American Journal of Mathematics," Vol. xvi., No. 1 ; Baltimore.