ON MODULAR GROUPS ISOMORPHIC WITH A GIVEN LINEAR GROUP

BY

H. F. BLICHFELDT

Theorem. Given a group $G$ of linear homogeneous substitutions in $n$ variables, transitive (irreducible) and of finite order. Then there exists an infinitude of prime numbers $p$ for each of which we can construct a simply isomorphic transitive group $G'$ of linear homogeneous substitutions in $n$ variables, the elements of whose matrices are integers taken modulo $p$.

Let the operators of the abstract group $G''$ simply isomorphic with $G$ be $S'_i, i = 1, 2, \ldots, N$. Write down $N$ matrices in $n$ variables with undetermined coefficients

$$S'_i = |a'_{jk}|,$$

and form the $N^2$ products $S'_i S'_j$. Writing $S'_i S'_j = S'_k$ whenever $S''_i S''_j = S''_k$, we obtain $n^2 N^2$ equations in the elements $a'_{jk}$. This system of equations shall be denoted by $A$. Any system of elements $a'_{jk}$ satisfying $A$ will furnish a linear group $G_1$ isomorphic with $G''$. That this group may be transitive in $n$ variables we must, furthermore, have no equation of the form $\sum_{j, k} b_{jk} a'_{jk} = 0$ (i = 1, 2, \ldots, N),

the coefficients $b_{jk}$ being independent of $i$. In other words, zero cannot be the value of every determinant of $(n^2)^2$ elements of the matrix of $n^2$ columns and $N$ rows, the $i$th row of which is formed of the $n^2$ elements $a'_{jk}$. We shall denote by $B'$ the system of equations obtained by equating to zero all the determinants mentioned. Furthermore, in order that $G_1$ may not contain two transformations that are identical, we must exclude all possible sets of solutions of $A$ for which two rows of the matrix of $n^2 N$ elements just mentioned are identical. This condition expressed in analytical form is as follows: the expression

*Presented to the Society (Chicago), April 14, 1906. Received for publication February 13, 1906.

must not vanish for a set of \( n^2 \) arbitrary parameters \( \lambda_{jk} \). We shall modify the system \( B' \) by multiplying each of its equations by \( P \), and we shall denote the resulting set of equations by \( B \).

Now, because the transitive group \( G \) exists, the system \( A \) can be solved, and solutions exist which will not satisfy all the equations of \( B \). To solve \( A \) we may, by a well known process, form a normal equation of the system, an algebraic equation whose coefficients are integers and which has no double roots. Let this equation be

\[
F = a_0 x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0.
\]

Denoting by \( x \) any one of the roots of this equation, we can write every corresponding value of \( a_{jk} \) as an integral function of \( x \), the coefficients of which are definitely given rational numbers (the same for any root \( x \) of \( F \)) considered. Substituting in the system \( B \) we have a series of equations in \( x \) with rational coefficients, known functions of the parameters \( \lambda_{jk} \), which equations could not all be satisfied for every root \( x \) of \( F \). Hence \( F' = 0 \) has at least one root not found in one (say \( C = 0 \)) of the equations \( B \). Let us suppose \( F = F_1 F_2 \), where \( F_1 = 0 \) has no root in common with \( C = 0 \). Then we can construct an identity of the form

\[
a F_1 + b C = K_1 = 0,
\]

where \( a, b \) and \( b C \) are integral functions of \( x \) whose coefficients, as well as \( K_1 \), are integral functions of the parameters \( \lambda_{jk} \) with integral coefficients. To every root \( x \) of \( F_1 = 0 \) will correspond a transitive group \( G_x \) simply isomorphic with \( G' \).

The question whether or not there exists a transitive linear group in \( n \) variables simply isomorphic with \( G'' \) with coefficients modulo \( p \) can now be solved. We start as above with the \( N \) matrices

\[
S_i' = \left| a_{jk} \right|
\]

and write down all the congruences (mod \( p \)) following from the equations \( S_i' S_j' = S_k' \). The system \( A \) above will merely be replaced by congruences, and instead of \( F' = F_1 F_2 = 0 \) we will have \( F' = F_1 F_2 \equiv 0 \) (mod \( p \)). We remark that the coefficients of \( F, F_1 \) and \( F_2 \) are all known integers, although \( p \) is, as yet, not known. The elements \( a_{jk} \) are, as above, expressed as integral functions of a root \( x \) of \( F_1 \equiv 0 \) (mod \( p \)), the coefficients of which functions are known fractions. Let the least common multiple of all the denominators entering in these functions be denoted by \( M \). We shall replace the parameters \( \lambda_{jk} \) by such a system of integers that \( \overline{K} \) does not vanish. The resulting value of \( \overline{K} \) (an integer) will be denoted by \( \overline{K} \).
Suppose that $F_1 = b_n x^n + \ldots + b_0$. We may assume that $b_0 \neq 0$, as we may replace $x$ by $x + h$. Let us substitute for $x$ in $F_1 \equiv 0 \pmod{p}$ the quantity $MK b_0 y$. We obtain

$$b_0 \{MK(c_n y^n + \ldots + c_1 y) + 1\} \equiv 0 \pmod{p},$$

the coefficients of the left-hand member being known integers evidently not all zero.

If we substitute any integer $y'$ for $y$ such that

$$MK(c_n y'^n + \ldots + c_1 y') + 1 = L \equiv 1 \text{ or } 0,$$

and choose for $p$ any prime factor $> 1$ of $L$, we have a modulus $p$ fulfilling the conditions of the problem. For, $p$ is prime to $MK$, and $F_1 \equiv 0 \pmod{p}$ has a solution $x = MK b_0 y'$. Accordingly, the system of congruences $A$ is satisfied, but not the system $B$ (by virtue of the identity $\alpha F_1 + \beta C \equiv K$).

Because $A$ is satisfied, we have a modular group $H$ isomorphic with $G''$. If this group is intransitive modulo $p$, it may be transformed into a group of type

$$\begin{array}{c|c}
H_1 & 0 \\
0 & H_2
\end{array},$$

from which it follows that the elements of $H$ satisfy at least one system of congruences corresponding to (1), from which again would follow the system $B$, and therefore also $C \equiv 0 \pmod{p}$. Again, if $H$ were not simply isomorphic with $G$, the factor $P$ would vanish $\pmod{p}$, and therefore also every equation of $B$. But this is not the case, according to our procedure.

Berlin,

January, 1906.