

A THEOREM CONCERNING THE INVARIANTS OF LINEAR HOMOGENEOUS GROUPS, WITH SOME APPLICATIONS TO SUBSTITUTION-GROUPS*

BY

H. F. BLICHFELDT

1. Consider a group G of order N , written in linear homogeneous form in terms of the variables x_1, x_2, \dots, x_n . Let the multipliers of S_i , any substitution of G , be $\theta_1, \theta_2, \dots, \theta_n$, and designate by χ_i the "characteristic"† $\theta_1 + \theta_2 + \dots + \theta_n$ of S_i . We shall now prove the

LEMMA. *If*

$$\sum_{i=1}^N \chi_i \neq 0,$$

then will G have an absolute invariant, linear in x_1, x_2, \dots, x_n .‡

Let t_1, t_2, \dots, t_n be arbitrary constants. The expression

$$(S_1 + S_2 + \dots + S_N)(t_1 x_1 + t_2 x_2 + \dots + t_n x_n) \equiv I$$

will be an absolute invariant of G of degree 1, if it does not vanish identically. If it does, then must the coefficients of the terms $t_1 x_1, t_2 x_2, \dots, t_n x_n$ of I each be $= 0$. Accordingly, if the *sum* of these coefficients is $\neq 0$, then $I \neq 0$. But this sum is readily found to be

$$\sum_{i=1}^N \chi_i.$$

Hence the lemma.

We shall now prove the following

THEOREM. *The number of linearly independent absolute invariants of G of the first degree in x_1, x_2, \dots, x_n is equal to*

$$\frac{1}{N} \sum_{i=1}^N \chi_i.$$

* Presented to the Society at the San Francisco meeting, April 30, 1904. Received for publication July 12, 1904.

† BURNSIDE, *On the Representation of a Group of Finite Order as an Irreducible Group of Linear Substitutions*, etc., Proceedings of the London Mathematical Society, November, 1903, pp. 117-123. The quantities χ_i have been called *weights* by the author in two papers published in these Transactions, vol. 4 (1903), p. 387, and vol. 5 (1904), p. 310.

‡ Cf. equation (true for transitive groups) given by BURNSIDE, Proceedings of the London Mathematical Society, March, 1903, p. 122, bottom.

According to the preceding lemma, G possesses an invariant $I = z_1$ if $\sum \chi_i \neq 0$. Then, by a theorem concerning the reducibility of linear groups,* G is intransitive, its systems being z_1 and (say) z_2, z_3, \dots, z_n . Let the group in the variables z_2, z_3, \dots, z_n be denoted by G' , and its characteristics by χ'_i . The multipliers of z_1 all being $= 1$, we have $\sum \chi_i = N + \sum \chi'_i$.

Conversely, if G possesses an invariant $I = z_1$, then $\sum \chi_i \neq 0$. For, writing G as an intransitive group in terms of $z_1, z_2, z_3, \dots, z_n$, we have $\sum \chi_i = N + \sum \chi'_i$. Now, if $\sum \chi'_i \neq 0$, we have an absolute invariant of degree 1 in z_2, z_3, \dots, z_n , and G' must be intransitive, its variables breaking up into two systems containing, respectively, 1 and $n - 2$ variables. We would find that $\sum \chi'_i = N + \sum \chi''_i$. Continuing thus, we see the truth of the theorem stated.

COROLLARY 1. *The number of linearly independent absolute invariants of G of degree m in x_1, x_2, \dots, x_n is equal to*

$$\frac{1}{N} \sum_{i=1}^N \chi_i^{(m)},$$

where $\chi_i^{(m)}$ represents the sum of the homogeneous products of $\theta_1, \theta_2, \dots, \theta_n$ of degree m .

We prove the corollary by constructing from G the group whose variables are all the different terms of degree m in the letters x_1, x_2, \dots, x_n , and then applying the theorem given. In case the group constructed (which is isomorphic with G) is of order N/k , we write each of its substitutions k times before applying the theorem, regarding the entire set of N substitutions as forming a group.

2. Let it be proposed to find an upper limit to the least order of existing absolute invariants of a given group G . We shall take as an illustration a group in 3 variables. The quantity $\chi^{(m)}$ is here represented by

$$(1) \quad \begin{vmatrix} 1 & 1 & 1 \\ \theta_1 & \theta_2 & \theta_3 \\ \theta_1^{2+m} & \theta_2^{2+m} & \theta_3^{2+m} \end{vmatrix} \div \begin{vmatrix} 1 & 1 & 1 \\ \theta_1 & \theta_2 & \theta_3 \\ \theta_1^2 & \theta_2^2 & \theta_3^2 \end{vmatrix} \equiv A_0 \theta_1^m + B_0 \theta_2^m + C_0 \theta_3^m,$$

if θ_1, θ_2 and θ_3 are all different; in the case $\theta_1 = \theta_2 \neq \theta_3$ we get (by treating (1) as an indeterminate form)

$$\chi^{(m)} = A_1 \theta_1^m + B_1 m \theta_1^{m-1} + C_1 \theta_3^m,$$

and, if $\theta_1 = \theta_2 = \theta_3$, we obtain

$$\chi^{(m)} = A_2 \theta_1^m + B_2 m \theta_1^{m-1} + C_2 m(m-1) \theta_1^{m-2};$$

the quantities A_i, B_i and C_i being independent of m .

* MASCHKE, *Mathematische Annalen*, vol. 52 (1899), p. 363; LOEWY, *these Transactions*, vol. 4 (1903), p. 44.

Substituting in $N^{-1} \sum \chi_i^{(m)} = k$ we obtain an equation, the right-hand member of which is an integer representing the number of invariants of degree m of G . Collecting, in the left-hand member, all the terms having the same factors θ_i^m , $m\theta_i^m$ or $m(m-1)\theta_i^m$, this member takes the form

$$(2) \quad \sum_i \theta_i^m K_i + m \sum_i \theta_i^m L_i + m(m-1) \sum_i \theta_i^m M_i,$$

where the coefficients K_i , L_i and M_i are independent of m .

A root θ , occurring never more than once among the multipliers of the different substitutions of the group, will appear in only one term ($\theta^m K$) in (2); a root θ , occurring twice as a multiplier in some one of the substitutions of G , will appear as a term $\theta^m K$ and as a term $m\theta^m L$ in the expression (2); etc. Accordingly, there are as many terms in (2) as there are different multipliers in G , each multiplier counted once, twice or three times, according as it occurs once, twice or three times in some one or other of the substitutions of G (e. g., the root 1 must be counted three times, occurring three times in the identical substitution). Let us designate this number by I' .

Taking now in turn $m = 1, 2, 3, \dots, I'$, we have I' equations, the right-hand members of which cannot all be zero unless the determinant obtained by eliminating the quantities K_i , L_i and M_i is zero (the quantities K_i , L_i and M_i are not all zero, as their sum $= N$, as shown by putting $m = 0$). Now, this determinant is readily found to be the product of the first, second, or third powers of the differences of the various roots θ and does, therefore, not vanish. Accordingly, there must be at least one absolute invariant of G whose order is not greater than I' . Again, it is evident that $I' \leq 3$ times the number of conjugate sets of substitutions of G . Hence, generalizing our results we see that *a linear homogeneous group G in n variables must have at least one absolute invariant whose order is not greater than n times the number of conjugate sets of substitutions of G .*

3. Having given two isomorphic groups, we may construct an intransitive group and employ the corollary to show the existence or not of invariant bilinear functions of the two sets of variables. Thus, let the two isomorphic groups be G and \bar{G} in the variables x_1, x_2, \dots, x_n and $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n$, \bar{G} being obtained from G by replacing in the latter every variable and coefficient by its conjugate imaginary expression. Then will

$$\frac{1}{N} \{ \sum \chi_i^{(2)} + \sum \chi_i \bar{\chi}_i + \sum \bar{\chi}_i^{(2)} \}$$

be the total number of absolute invariants of degree 2 of the intransitive group exhibited by

$$\frac{G}{0} \left| \begin{array}{c} 0 \\ \bar{G} \end{array} \right|,$$

and

$$(3) \quad \frac{1}{N} \sum \chi_i \bar{\chi}_i$$

will evidently be the number of invariants of the form

$$\sum_{i,j} a_{i,j} x_i \bar{x}_j.$$

There must be at least one such, as not all the terms of (3) are zero (e. g., that from S_1 (identity) $= n^2$), and none of them are negative. It is well known that there is always one such invariant, a positive-definite Hermitian form,* and BURNSIDE has shown that if G is transitive, there is only one invariant of the form

$$\sum_{i,j} a_{i,j} x_i \bar{x}_j. \dagger$$

Hence, for a transitive group G , $N^{-1} \sum \chi_i \bar{\chi}_i = 1$, whereas, for an intransitive group, $N^{-1} \sum \chi_i \bar{\chi}_i > 1. \ddagger$

4. COROLLARY 2. Let ϕ_i be any integral symmetric function with integral coefficients of the multipliers of the substitution S_i of the group G of order N . Then is

$$\sum_{i=1}^N \phi_i = kN,$$

where k is an integer.

We prove this corollary first for the case when ϕ_i is one of the elementary symmetric functions of the multipliers $\theta_1, \theta_2, \dots, \theta_n$. Suppose

$$\phi_i = \theta_1 \theta_2 + \theta_1 \theta_3 + \theta_2 \theta_3 + \dots$$

Let G' be obtained from G merely by replacing the variables x_1, x_2, \dots, x_n by y_1, y_2, \dots, y_n . Then the group H , whose variables are $x_i y_j - x_j y_i$ ($i, j = 1, 2, \dots, n; i \neq j$) will be isomorphic with G , and its characteristics are the quantities ϕ_i . If its order is N/k , we write each of its substitutions k times. Then

$$\sum_{i=1}^N \phi_i = k_1 N$$

by the theorem stated above. §

Next, by considering an intransitive group constructed from two such groups,

* FUCHS, *Berliner Sitzungsberichte* (1896), p. 753; MOORE, *Chicago University Record* (1896), *Mathematische Annalen*, vol. 50 (1898), p. 213; LOEWY, *Comptes Rendus* (1896), p. 168.

† *Proceedings of the London Mathematical Society*, November, 1903, p. 121.

‡ *Ibid.*, p. 123.

§ Cf. BURNSIDE, *Proceedings of the London Mathematical Society*, Nov., 1900, p. 162.

H_1 and H_2 , whose characteristics are elementary symmetric functions ϕ'_i and ϕ''_i (the substitutions of each being repeated such a number of times that the total number equals the order of the isomorphic group G), we prove that $\sum \phi'_i \phi''_i = k_2 N$. This process may be continued, and we prove finally that

$$\sum_{i=1}^N \sigma_i = kN,$$

where σ_i is any function of the elementary symmetric functions of the multipliers $\theta_1, \theta_2, \dots, \theta_n$.

Now, any integral symmetric function with integral coefficients of a certain number of quantities $\theta_1, \theta_2, \dots, \theta_n$ can be expressed as an integral function with integral coefficients of the elementary symmetric functions of the same quantities. The corollary follows.

5. A substitution-group G in n letters x_1, x_2, \dots, x_n may be written as a linear homogeneous group G' whose variables are the n letters given. The multipliers belonging to a substitution S of G can be written down immediately by the following rule: to each of the letters x_1, x_2, \dots, x_n left unchanged by S belongs a multiplier 1, to a cycle of S of order a belongs the a different a th roots of unity. The characteristic of S , i. e., the sum of the multipliers is therefore equal to the number of letters left unchanged by S . Accordingly, by the theorem of § 1, *the average number of letters which remain unchanged by a substitution of a group G is equal the number of linear invariants of G* ; i. e., is equal the number of transitive sets of G .* This theorem may be readily extended by Corollary 2 by taking for ϕ_i the sum of the 2d, 3d, \dots , powers of the multipliers of the corresponding substitution of G . We find immediately that *the total number of letters occurring in all of the cycles of a given order m is a multiple of the order of the group*.†

6. A number of theorems of like nature may evidently be proved by purely arithmetical means, and will be more or less different according to the mode in which the given group is represented. We shall here mention only two such, one by FROBENIUS and one by MAILLET.

If n is a factor of N , the number of substitutions of G satisfying the equation $S^n = 1$ is a multiple of n .‡

Write G as a regular group of degree N . If h_i represents the total number of substitutions of G of order i , then must, according to Corollary 2, every coefficient of t in

$$(1+t)^N + h_2(1-t^2)^{N/2} + h_3(1+t^3)^{N/3} + h_4(1-t^4)^{N/4} + \dots = P$$

* FROBENIUS, Journal für Mathematik, vol. 101 (1887), p. 288.

† NETTO, Journal für Mathematik, vol. 103 (1888), p. 321.

‡ FROBENIUS, Berliner Sitzungsberichte, 1895, pp. 984-985.

be a multiple of N . The coefficient of t^m in $(1 \pm t^k)^{N/k}$ is, namely, the elementary symmetric function of degree m of the multipliers of a substitution of order k of the group as written.

Noticing that, if $N = p^a m = kpl$, we have

$$(1 \pm t^k)^{N/k} \equiv (1 \pm t^{kp})^{N/kp} \pmod{p^a} \quad (p \text{ a prime})$$

and then also

$$\begin{aligned}
P \equiv & (1 \pm t^{p^a})^{N/p^a} (1 + h_p + h_{p^2} + \cdots + h_{p^a}) \\
& + (1 \pm t^{n_1 p^a})^{N/n_1 p^a} (h_{n_1} + h_{n_1 p} + \cdots + h_{n_1 p^a}) \\
& + (1 \pm t^{n_2 p^a})^{N/n_2 p^a} (h_{n_2} + h_{n_2 p} + \cdots + h_{n_2 p^a}) \\
& \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
& + (1 \pm t^{n_0 p^a})^{N/n_0 p^a} (h_{n_0} + h_{n_0 p} + \cdots + h_{n_0 p^a}) \\
& + h_b (1 \pm t^b)^{N/b} + h_c (1 \pm t^c)^{N/c} + \cdots \pmod{p^a},
\end{aligned}$$

where $n = p^a n_0$ (p prime to n_0) and is not divisible by b, c, \dots ; and where $1, n_1, n_2, \dots, n_0$ are all the different factors of n_0 , in ascending order of magnitude. By considering in turn the coefficients of $x^a, x^{n_1 a}, \dots, x^{n_0 a}$ we find that they are all $\equiv 0 \pmod{p^a}$. It follows that the number of substitutions satisfying $S^n = 1$ is $\equiv 0 \pmod{p^a}$ and is therefore also $\equiv 0 \pmod{n}$.

If G contains substitutions which leave unchanged $n_0 = n$ letters (identity), n_1 letters, \dots , n_r letters, this list containing all the substitutions, then is the order N of G a factor of $(n_0 - n_1)(n_0 - n_2) \dots (n_0 - n_r)$.*

Let the number of substitutions of each kind be respectively $h_0 = 1, h_1, h_2, \dots, h_r$. Then, by choosing for ϕ_i of Corollary 2 in turn $1, \chi_i, (\chi_i)^2, (\chi_i)^3, \dots$ we obtain the congruences

$$\begin{aligned} h_0 + h_1 + h_2 + \cdots + h_r &= N, \\ n_0 h_0 + n_1 h_1 + n_2 h_2 + \cdots + n_r h_r &\equiv 0, \\ n_0^2 h_0 + n_1^2 h_1 + n_2^2 h_2 + \cdots + n_r^2 h_r &\equiv 0 \pmod{N}, \\ \vdots & \end{aligned}$$

Hence,

$$h_i \prod_{\substack{j=0, 1, \dots, r; \\ j \neq i}} (n_i - n_j) \equiv 0 \pmod{N},$$

which includes the theorem stated.

STANFORD UNIVERSITY.

* MAILLET, Annales de la Faculté des Sciences de Toulouse, 1895, p. 8.