ON THE GROUP DEFINED FOR ANY GIVEN FIELD BY THE MULTIPLICATION TABLE OF ANY GIVEN FINITE GROUP*

BY

LEONARD EUGENE DICKSON

Introduction.

In two papers,† each having the title "On the Continuous Group that is defined by any given Group of Finite Order," BURNSIDE establishes certain results of decided interest and importance, among them being the theorems‡ of FROBENIUS on the irreducible factors of group-determinants. The object of this paper is the development of the theory of analogous groups in any arbitrary field or domain of rationality. In particular, when the field is the general Galois field of order p^n, we obtain a doubly-infinite system of finite groups corresponding to each given finite group. An exceptional case not treated here is that of a field having a modulus which is a factor of the order of the given finite group.§

BURNSIDE bases his work upon several theorems proved by means of the LIE theory of continuous groups. The corresponding theorems for an arbitrary field are here derived by simple rational processes (§§ 2, 3). The auxiliary theorems on invariant-factors (the "Elementartheiler" of WEIERSTRASS) are established in § 4 by means of the canonical form of a linear transformation in any field. The later developments (§§ 5–7) run parallel to the corresponding parts of BURNSIDE's treatment, but include essential modifications.

The results find application in the problem of the representation of a given finite group as a group of linear transformations in a given field upon the smallest number of variables. That the introduction of the concept of a field gives rise to a generalization of KLEIN's normal problem may be illustrated by the fact that a given group may be represented as a modular group upon a smaller number of variables than is possible for a representation as an algebraic linear group.

* Presented to the Society (Chicago) March 29, 1902. Received for publication March 14, 1902.

† Proceedings of the London Mathematical Society, vol. 29 (1898), pp. 207–224, 546–565.

‡ *Über die Primfactoren der Gruppendeterminante*, Berliner Sitzungsberichte, 1896, pp. 1343–1382.

§ In a paper to be presented to the London Mathematical Society, I propose to consider this case, at least for certain classes of groups, and to give additional examples of the general theory.

§ 1. *Definition of the group* G.

Let the operators of a given finite group g be s_1 (identity), $s_2, \cdots, s_n$. The (left-hand) multiplication table of the group is derived from the array

$$
(1)\qquad \begin{array}{ccccccc}
s_1^{-1} & s_2^{-1} & \cdots & s_k^{-1} & \cdots & s_n^{-1} \\
s_2 s_1^{-1} & s_2 s_2^{-1} & \cdots & s_2 s_k^{-1} & \cdots & s_2 s_n^{-1} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
s_n s_1^{-1} & s_n s_2^{-1} & \cdots & s_n s_k^{-1} & \cdots & s_n s_n^{-1}
\end{array}
$$

by replacing each product by the equivalent operator of the group. We consider n arbitrary elements of the field F and assign to them the single-index notation x_{s_i} or x_i and also the double-index notations $x_{s_i s_j}$ or x_{ij}, $x_{s_k s_j^{-1}}$ or $x_{kj^{-1}}$, with the understanding that

$$
(2)\qquad x_{ij} = x_k, \quad x_{kj^{-1}} = x_i \qquad (\text{if } s_i s_j = s_k, \text{ whence } s_k s_j^{-1} = s_i).
$$

Consider the following matrix defined by the table (1):

$$
(3)\qquad \begin{vmatrix}
x_{11^{-1}} & x_{12^{-1}} & \cdots & x_{1k^{-1}} & \cdots & x_{1n^{-1}} \\
x_{21^{-1}} & x_{22^{-1}} & \cdots & x_{2k^{-1}} & \cdots & x_{2n^{-1}} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
x_{n1^{-1}} & x_{n2^{-1}} & \cdots & x_{nk^{-1}} & \cdots & x_{nn^{-1}}
\end{vmatrix}.
$$

Each variable x_i occurs once and but once in each row (or column). Hence any variable x_i occurs in exactly n places in the matrix. For all n places, the adjoint (first minor with proper sign) of x_i is the same. * In proof, denote by $A_{j,k}$ the adjoint of $x_{jk^{-1}}$. Consider first the adjoint

$$
A_{j,j} \equiv |x_{ik^{-1}}| \qquad (i, k = 1, \cdots, j-1, j+1, \cdots, n).
$$

Set $s_i = s_u s_j$, $s_k = s_v s_j$, so that $x_{ik^{-1}} = x_{ujj^{-1}v^{-1}} = x_{uv^{-1}}$. Then

$$
A_{j,j} = |x_{uv^{-1}}| \equiv A_{1,1} \qquad (u, v = 2, 3, \cdots, n).
$$

To show next that $A_{j,k} = A_{c,1}$, where $c = jk^{-1}$, we set

$$
x_{cit^{-1}} = x'_{it^{-1}} \qquad (i, t = 1, \cdots, n).
$$

Since ci and i run simultaneously through the series of n operators,

$$
\pm |x_{it^{-1}}| = |x_{cit^{-1}}| \equiv |x'_{it^{-1}}|.
$$

* FROBENIUS, *Über Gruppencharaktere*, Berliner Sitzungsberichte, 1896, pp. 985–1021, § 6.

To obtain $x_{jk^{-1}} \equiv x_c$ in $|x_{cit^{-1}}|$, we must take $i = t$; the corresponding term of $|x'_{it^{-1}}|$ is therefore in the main diagonal. But $A'_{1,1} = A'_{2,2} = \cdots = A'_{n,n}$.

Consider the set of transformations, defined by the matrix (3),

$$X: \qquad \xi'_s = \sum_{i=1}^{n} x_{si^{-1}} \xi_i \qquad (s = 1, \cdots, n),$$

in which $x_1, \cdots, x_n$ take all sets of values in the field F such that $\Theta(x) \neq 0$, where $\Theta(x)$ denotes the determinant of the matrix (3). Then $\Theta(x)$ is called the *group-determinant of g*. In view of the preceding proof, the inverse of every such transformation X belongs to the set. Let

$$Y: \qquad \xi'_s = \sum_{i=1}^{n} y_{si^{-1}} \xi_i \qquad (s = 1, \cdots, n)$$

be a second transformation of the set. Then

$$(2') \qquad y_{ij} \equiv y_k \qquad (\text{if } s_i s_j = s_k).$$

Applying first X and then Y, we obtain the transformation

$$Z \equiv XY: \qquad \xi'_s = \sum_{i=1}^{n} z_{si^{-1}} \xi_i \qquad (s = 1, \cdots, n),$$

where

$$(4) \qquad z_{si^{-1}} \equiv \sum_{j=1}^{n} y_{sj^{-1}} x_{ji^{-1}} \qquad (s, i = 1, \cdots, n).$$

In view of the properties (2) and (2′), it follows that *

$$(2'') \qquad z_{ij} = z_k \qquad (\text{if } s_i s_j = s_k).$$

Hence the set of transformations X forms a group G.

§ 2. *Determination of the group G', reciprocal to G.*

Denote by X_k the particular transformation X given by the values

$$x_k = 1, \quad x_j = 0 \qquad (j = 1, \cdots, n;\ j \neq k).$$

Then $x_{si^{-1}}$ is zero unless $s_i = s_k^{-1} s_s$, so that we have

$$X_k: \qquad \xi'_s = \xi_{k^{-1}s} \qquad (s = 1, \cdots, n),$$

where $\xi_{k^{-1}s} \equiv \xi_i$ if $s_k^{-1} s_s = s_i$. If s_k is of period κ, the transformation X_k corresponds to a *regular* substitution X'_k on n letters, the general cycle being

$$(\xi_j \xi_{k^{-1}j} \xi_{k^{-2}j} \cdots \xi_{k^{-(\kappa-1)}j}).$$

* Hence relations (4) may be written in either of the forms:

$$z_l = \sum_{r=1}^{n} y_r x_{r^{-1}l}, \quad z_{st} = \sum_{r=1}^{n} y_r x_t.$$

The regular substitution group composed of the substitutions $X'_1, \cdots, X'_n$ is simply isomorphic with the group g in such a way that X'_k corresponds to s_k^{-1}.

Consider an arbitrary linear homogeneous transformation

$$(5) \qquad \xi'_i = \sum_{j=1}^{n} a_{i,j}\xi_j \qquad (i=1, \cdots, n).$$

If $\sigma_1, \sigma_2, \cdots, \sigma_n$ form a permutation of $1, 2, \cdots, n$, the linear transformation

$$\xi'_i = \xi_{\sigma_i} \qquad (i=1, \cdots, n)$$

transforms (5) into the following transformation:

$$\xi'_i = \sum_{j=1}^{n} a_{\sigma_i, \sigma_j}\xi_j \qquad (i=1, \cdots, n).$$

The latter is identical with the transformation (5) if, and only if,

$$a_{i,j} = a_{\sigma_i, \sigma_j} \qquad (i, j=1, \cdots, n)$$

Hence the conditions that the n transformations X_k shall be commutative with the transformation (5) are

$$(6) \qquad a_{i,j} = a_{k^{-1}i, k^{-1}j} \qquad (i, j, k=1, \cdots, n).$$

For $i = 1, \cdots, n$, we set $w_{t^{-1}} = a_{1,t}$, and set $w_{ab} = w_c$ if $s_a s_b = s_c$. Then by (6)

$$a_{i,j} = a_{1, i^{-1}j} = w_{j^{-1}i}.$$

Hence the transformation (5) may be written in the form

$$W: \qquad \xi'_s = \sum_{i=1}^{n} w_{i^{-1}s}\xi_i \qquad (s=1, \cdots, n).$$

Every transformation W is commutative with every transformation X. Indeed, the product XW replaces ξ_s by a linear function in which the coefficient of ξ_i is

$$\lambda_{si} \equiv \sum_{j=1}^{n} w_{j^{-1}s}x_{ji^{-1}}.$$

For s and i fixed, the operators s_j and $s_s s_j^{-1} s_i$ run simultaneously through the set of n operators of g. Replacing j by $sj^{-1}i$, we get

$$\lambda_{si} = \sum_{j=1}^{n} w_{i^{-1}j}x_{sj^{-1}}.$$

But this expression is the coefficient of ξ_i in the linear function by which the product WX replaces ξ_s.

It follows that the group G' of all the transformations W is the largest n-ary linear homogeneous group in the field F, each of whose transformations is commutative with every transformation X of G. Evidently the group G' may be defined by the right-hand multiplication table for the group g precisely as G was defined by its left-hand multiplication table. Hence G is the largest group of n-ary linear transformations in F which are commutative with every transformation of G'. Hence the groups G and G' are *reciprocal* to each other.

§ 3. *The commutative subgroup H.*

To obtain the transformations common to G and G', we must set

$$x_{si^{-1}} = w_{i^{-1}s} \qquad (i,\ s = 1, \cdots, n).$$

Setting $s_i^{-1} s_s = s_r$, so that $s_s s_i^{-1} = s_i s_r s_i^{-1}$, we get

$$x_{iri^{-1}} = w_r \qquad (i,\ r = 1, \cdots, n).$$

Hence the necessary and sufficient conditions that a transformation X of G shall belong to the group G' are that the variables $x_1, \cdots, x_n$ whose subscripts correspond to conjugate operators are all equal. Hence the transformations

$$E: \qquad \xi'_s = \sum_{i=1}^{n} e_{si^{-1}} \xi_i \qquad (s = 1, \cdots, n),$$

in which $e_1, \cdots, e_n$ run through every set of elements of F such that $e_j = e_k$ if s_j and s_k are conjugate in g and such that the determinant D_e of E is not zero, form a commutative group H. It is composed of all the self-conjugate transformations of G. This determinant D_e is called the *special group-determinant of* g. If r be the number of distinct sets of conjugate operators in g, exactly r of the e's are distinct and will be designated $\epsilon_1 = e_1, \epsilon_2, \cdots, \epsilon_r$. Since the inverse of the general transformation E belongs to the group H, the adjoint ϵ'_k of ϵ_k, in whatever position it occurs in D_e, is always the same. Let n_k denote the number of operators in the kth set of conjugates in the group g of order n. Then ϵ_k occurs exactly n_k times in each row of D_e, and altogether $n n_k$ times in the determinant. We derive therefore the *algebraic* identity

$$(7) \qquad \epsilon'_k \equiv \frac{1}{n n_k} \frac{\partial D_e}{\partial \epsilon_k}.$$

The division of $\partial D_e / \partial \epsilon_k$ by $n n_k$ must first be performed if we are to apply (7) in the case of a field F having a modulus which divides n.

§ 4. *Invariant-factors of a linear transformation.*

By the *characteristic determinant* (with parameter ρ) of the transformation (5) is meant the determinant

$$D(\rho) \equiv \begin{vmatrix} a_{11}-\rho & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22}-\rho & a_{23} & \cdots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn}-\rho \end{vmatrix}.$$

Then $D(0)$ is the determinant of the transformation; it is assumed to be different from zero in the field F. The rth minors of $D(\rho)$ are polynomials in ρ with coefficients in F not all zero. The unique polynomial of highest degree in ρ which divides all of these minors and in which the coefficient of the highest power of ρ is $(-1)^n$ will be designated $D_r(\rho)$. It may be determined by EUCLID's algorithm for finding the greatest common divisor. Hence $D_r(\rho)$ has its coefficients in F. Now any $(r-1)$-th minor of $D(\rho)$ is the sum of certain rth minors each multiplied by an element of $D(\rho)$. Hence $D_r(\rho)$ divides $D_{r-1}(\rho)$ in the field F. The polynomials, with coefficients in F, defined by the quotients

$$\frac{D(\rho)}{D_1(\rho)}, \quad \frac{D_1(\rho)}{D_2(\rho)}, \quad \frac{D_2(\rho)}{D_3(\rho)}, \quad \cdots \tag{8}$$

are called the *invariant-factors* * of the characteristic determinant $D(\rho)$.

The importance of the invariant-factors is shown by the

THEOREM.—*The necessary and sufficient conditions that two n-ary linear homogeneous transformations A and A′ with coefficients in F shall be conjugate within the n-ary linear homogeneous group in the field F are that the invariant-factors of the characteristic determinant of A shall be identical with the invariant-factors of that of A′.*

For the case in which F is the continuous field of all numbers, the theorem merely states the existence of a transformation T such that

$$T^{-1}AT = A',$$

without requiring that T shall belong to a *special* field. In this case, the theorem follows from a general result due to WEIERSTRASS. †

The proof that the conditions are necessary is very simple. If $T^{-1}AT = A'$, then the polynomials giving the expansions of the characteristic determinants of

* They are to be distinguished from the WEIERSTRASS "Elementartheiler," called the "einfachen Elementartheiler" by FROBENIUS, the latter being polynomials in ρ with coefficients involving the roots of $D(\rho) = 0$. But, if two determinants have the same "einfachen Elementartheiler," they have the same invariant-factors, and inversely.

† *Zur Theorie der bilinearen und quadratischen Formen, Werke*, II, pp. 19–44.

A and A' are identical. Let C and C' denote the unexpanded characteristic determinants of A and A' respectively. Any r-th minor of C' may be expressed as a sum of products of three factors, the first an r-th minor of $|T^{-1}|$, the second an r-th minor of C, the third an r-th minor of $|T|$. Let the coefficients of T belong to the field F. Then every common divisor of all the r-th minors of C is a divisor (with coefficients in F) of all the r-th minors of C'. Since $TA'T^{-1} = A$, the inverse is true. Hence $D_r(\rho) = D'_r(\rho)$.

To prove that the conditions are sufficient,* apply to A a linear transformation (not belonging to F, in general) to reduce it to its canonical form A_1:

$$(9)\qquad \begin{aligned} &\eta'_{ia} = K_i\eta_{ia}, \quad \eta'_{i\alpha} = K_i\eta_{i\alpha} + K_i\eta_{i\alpha-1} \qquad (i=1,\cdots,k);\\ &\zeta'_{ib} = L_i\zeta_{ib}, \quad \zeta'_{i\beta} = L_i\zeta_{i\beta} + L_i\zeta_{i\beta-1} \qquad (i=1,\cdots,l);\\ &\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \end{aligned}$$

in which the following notations have been employed.† Let

$$(-1)^n D(\rho) \equiv [F_k(\rho)]^{\kappa}[F_l(\rho)]^{\lambda}\cdots \qquad (n = k\kappa + l\lambda + \cdots),$$

$F_k(\rho)$, $F_l(\rho)$, $\cdots$ being distinct functions belonging to and irreducible in the field F, and having unity as coefficient of the highest power of ρ. The roots of $F_k(\rho) = 0$ are designated $K_1, \cdots, K_k$; the roots of $F_l(\rho) = 0$ are designated $L_1, \cdots, L_l$; etc. Then κ, λ, $\cdots$ are partitioned into positive integers

$$\kappa = a_1 + a_2 + \cdots + a_{r+1}, \quad \lambda = b_1 + b_2 + \cdots + b_{s+1}, \quad \cdots$$
$$(a_1 \geqq a_2 \geqq a_3\cdots, \ b_1 \geqq b_2 \geqq b_3\cdots, \ \cdots).$$

Then a, b, $\cdots$, denote integers selected arbitrarily from the respective sets

$$(a)\qquad 1, \quad a_1+1, \quad a_1+a_2+1, \quad \cdots, \quad a_1+a_2+\cdots+a_r+1;$$
$$(b)\qquad 1, \quad b_1+1, \quad b_1+b_2+1, \quad \cdots, \quad b_1+b_2+\cdots+b_r+1;$$
$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$

Then α is any integer $\overline{\gtrless}\,\kappa$ and not an a; β is any integer $\overline{\gtrless}\,\lambda$ and not a b; and so on. Each η_{ij} is the same function of K_i that η_{1j} is of K_1. A similar statement may be made for the functions ζ_{ij} of L_i.

By the direct calculation of NETTO,‡ the invariant-factors of (9) are

$$\prod_{i=1}^{k}(\rho - K_i)^{a_1}\prod_{i=1}^{l}(\rho - L_i)^{b_1}\cdots, \quad \prod_{i=1}^{k}(\rho - K_i)^{a_2}\prod_{i=1}^{l}(\rho - L_i)^{b_2}\cdots, \quad \cdots .$$

These invariant-factors may evidently be written in the simple form

$$(10)\quad [F_k(\rho)]^{a_1}[F_l(\rho)]^{b_1}\cdots, \ [F_k(\rho)]^{a_2}[F_l(\rho)]^{b_2}\cdots, \ [F_k(\rho)]^{a_3}[F_l(\rho)]^{b_3}\cdots, \ \cdots.$$

* The method of WEIERSTRASS does not seem adapted to prove the generalized theorem.

† Transactions, vol. 2 (1901), p. 393. The proof of the theorem quoted is given in the American Journal of Mathematics, vol. 24 (1902), pp. 101–108.

‡ *Zur Theorie der linearen Substitutionen*, Acta Mathematica, vol. 17 (1893), pp. 265–280

Upon expansion these expressions become polynomials in ρ with coefficients in F. But A_1 is the transform of A by a linear transformation. Hence the expressions (10) are the invariant-factors of the characteristic determinant of A. It follows that the canonical form is uniquely determined by the invariant-factors.

If, therefore, the invariant-factors of the characteristic determinants of A and A' are identical, A' is reducible to the same canonical form (9) as A. Hence, by the theorem concerning the canonical form, there exists a linear homogeneous transformation T on n variables with coefficients in F which transforms A into A'.

§ 5. *Factors of the special group-determinant D_e.*

Let A be one of the transformations E of the commutative group H and let B be a transformation such that $B^{-1}AB \equiv A_1$ is the canonical form (9) of A. Since $K_1, K_2, \cdots, K_k, L_1, \cdots, L_l, \cdots$ are all distinct, any transformation which is commutative with A_1 replaces each η_{ij} by a linear function of $\eta_{i1}, \cdots, \eta_{i\kappa}$ only, and replaces each ζ_{ij} by a linear function of $\zeta_{i1}, \cdots, \zeta_{i\lambda}$ only, etc. Hence every transformation of the commutative group $B^{-1}HB$ has these properties. Attending only to the variables $\eta_{i1}, \cdots, \eta_{i\kappa}$ (i being a fixed integer), we obtain a commutative group on κ variables. Unless the roots of the characteristic equation of each transformation of this group are all equal, we select one having at least two distinct roots and reduce it to its canonical form. Proceeding in this way, we obtain a transformation B_1 and a number of sets of variables such that every transformation of $B_1^{-1}HB_1$ replaces any variable of one set by a linear function of the variables of that set, thereby defining a partial group for each set; and such that the characteristic equation of every transformation of each partial group has all its roots equal.

Now the characteristic determinant $D_e(\rho)$ of the general transformation E of the group H is a homogeneous integral rational function of $\epsilon_1, \epsilon_2, \cdots, \epsilon_r, \rho$ of degree n. Also $D_e(\rho)$ is invariant under linear transformation. Hence $D_e(\rho)$ equals the product of the characteristic determinants of the partial transformations derived from E by the above process. Each of the latter determinants is therefore a homogeneous integral rational function of $\epsilon_1, \epsilon_2, \cdots, \epsilon_r, \rho$, and at the same time a power of a linear function of ρ. It is consequently a power of a linear homogeneous function of $\epsilon_1, \epsilon_2, \cdots, \epsilon_r, \rho$. Since $\epsilon_1 \equiv e_1$ occurs only in the combination $\epsilon_1 - \rho$, we may write

$$(11) \qquad (-1)^n D_e(\rho) = \prod_{i=1}^{s} (\rho - \epsilon_1 - a_{i2}\epsilon_2 - a_{i3}\epsilon_3 - \cdots - a_{ir}\epsilon_r)^{m_i} \quad \left(\sum_{i=1}^{s} m_i = n\right),$$

the s linear factors being distinct, each corresponding to a partial group. In case a factor f_1 involves quantities irrational with respect to F, the functions conjugate to f_1 with respect to F must occur as factors in (11). Since $D_e(0) = D_e$, it follows that the special group-determinant of g decomposes into linear homogeneous functions of $\epsilon_1, \epsilon_2, \cdots, \epsilon_r$, a result due to FROBENIUS.

§ 6. *Canonical forms of the groups H and G.*

Consider the adjoints of the elements $\epsilon_1 - \rho, \epsilon_2, \cdots, \epsilon_r$ in the determinant $D_e(\rho)$. In view of (7), the k-th adjoint is identical, aside from the factor $1/nn_k$, with the partial derivative of $D_e(\rho)$ with respect to ϵ_k. Suppose that, in case the field F has a modulus p, the latter divides none of the numbers * $n, m_1, \cdots, m_s$. Then

$$\rho - \epsilon_1 - a_{i2}\epsilon_2 - \cdots - a_{ir}\epsilon_r \equiv \rho - \tau_i,$$

which occurs in $D_e(\rho)$ exactly to the power m_i, occurs exactly to the power $m_i - 1$ in the factor of highest degree in ρ which divides all the first minors of $D_e(\rho)$. Hence the first invariant-factor of $D_e(\rho)$ is $(\rho - \tau_1) \cdots (\rho - \tau_s)$. Since the characteristic determinant of the i-th partial group H_i is $(\tau_i - \rho)^{m_i}$, and its first invariant-factor in the field $F(\tau_i)$ is $\rho - \tau_i$, it follows that each invariant-factor is $\rho - \tau_i$. Indeed, each is of degree $\gtreqless 1$ and their product is of degree m_i. Hence the canonical form of the general transformation of H_i is

$$\xi'_{ij} = \tau_i \xi_{ij} \qquad (j = 1, \cdots, m_i). \tag{12}$$

Let a particular transformation, for which τ_i has the value τ'_i, be reduced to its canonical form of type (12). Without altering the latter, a second particular transformation, for which $\tau_i = \tau''_i$, can be reduced to its canonical form of type (12). Proceeding thus, we find that all the transformations of H_i can be reduced simultaneously to the form (12). Hence there exists a linear transformation which transforms the group H into the group H of the transformations

$$\xi'_{ij} = \tau_i \xi_{ij} \qquad (j = 1, \cdots, m_i;\ i = 1, \cdots, s). \tag{13}$$

If τ_1, for example, does not belong to the field F, its conjugates $\tau_1, \tau_2, \cdots, \tau_l$, with respect to F, must occur as multipliers in (13). By the canonical form theory, each ξ_{1j} is a linear function of the initial indices with coefficients involving only the elements of F and the irrationalities occurring in τ_1, while

$$\xi_{1j}, \quad \xi_{2j}, \quad \cdots, \quad \xi_{lj}$$

are conjugate with respect to F. Among the s multipliers τ_i, exactly r are in-

* Since $m_1, \cdots, m_s$ are divisors of n (FROBENIUS), only divisors p of n are excluded.

dependent with respect to F. It is shown later that $s = r$, so that the distinct multipliers τ_i in (11) are all independent.*

Let the groups G, G' become Γ, Γ' when expressed in terms of the new variables ξ_{ij}. Since every transformation of Γ (or Γ') is commutative with every transformation of H, every transformation of Γ (or Γ') must replace ξ_{ij} by a function of $\xi_{i1}, \cdots, \xi_{im_i}$ only. Let Γ_i and Γ'_i denote the partial groups on the latter variables. Every transformation of Γ_i is commutative with every one of Γ'_i. Since G (or G') involves linearly and homogeneously n parameters which are independent in F, Γ_i (or Γ'_i) must involve linearly and homogeneously m_i parameters which are independent with respect to F. In fact, G is simply transitive in its n variables, so that Γ contains a transformation which replaces any given set of values of ξ_{ij} obeying the prescribed conjugacies with respect to F by any second set of values ξ_{ij} obeying the same conjugacies. Hence the general transformation of Γ_i may be written

$$(14) \qquad \xi'_{ij} = \sum_{l,k}^{1,\cdots,m_i} a_{jkl}\tau_{ik}\xi_{il} \qquad (j = 1, \cdots, m_i),$$

where $\tau_{i1}, \cdots, \tau_{im_i}$ are linear functions of the n parameters of G, the functions being independent with respect to F. Moreover, the n parameters

$$\tau_{ik} \qquad (k = 1, \cdots, m_i;\ i = 1, \cdots, s)$$

are independent with respect to F, since otherwise the group in its initial form G would depend upon less than n independent parameters of F. Hence each partial group Γ_i is a subgroup of Γ.

Likewise Γ' contains as a subgroup the partial group Γ'_i, whose transformations are of type (14), the variables ξ_{ij} being the same as before. Since every transformation (13), in which τ_i has for the coefficients of the irrationalities entering $\xi_{i1}, \cdots, \xi_{im_i}$ *arbitrary* elements in F, is commutative with every transformation of Γ', and leads to a transformation on the initial variables having its coefficients in F, it belongs to the group Γ (see end of § 2). Hence the self conjugate transformations of Γ form a group with s parameters independent with respect to F. By § 3 this number is r. Hence $s = r$.

§ 7. *Structure of G. Properties of the group-determinant.*

The group Γ is the direct product of the groups $\Gamma_1, \Gamma_2, \cdots, \Gamma_r$ which affect different variables. If τ_1 does not belong to F, the complete set of conjugates $\tau_1, \tau_2, \cdots, \tau_l$, with respect to F, defines a larger field F_l. To the latter belong the coefficients of the groups $\Gamma_1, \Gamma_2, \cdots, \Gamma_l$, which may be said to be

---

* This seems to be assumed by BURNSIDE (l. c., p. 557) in showing at this point that $s = r$.

conjugate with respect to the field F; their direct product is simply isomorphic with a group J_1 on m_1 variables and involving m_1 arbitrary parameters of F_l. By a suitable choice of notation, we may therefore express Γ as the direct product of certain groups $J_1, J_2, \cdots, J_\rho$ on different variables, J_i being a group on m_i variables and involving m_i arbitrary parameters of a field F_{l_i}, so that

$$m_1 l_1 + m_2 l_2 + \cdots + m_\rho l_\rho = n, \quad l_1 + l_2 + \cdots + l_\rho = r.$$

From the transformations (14) of the group J_i, we form the determinant

$$D_{\xi_i} \equiv \left| \sum_{l=1}^{m_i} a_{jkl}\,\xi_{il} \right| \qquad (j,\, k = 1, \cdots, m_i). \tag{15}$$

It is (relatively) invariant under every transformation W of the group J_i and hence is absolutely invariant under every transformation $W_1^{-1} W_2^{-1} W_1 W_2$ of the commutator group of J_i. A like result holds for every factor of D_{ξ_i} belonging to and irreducible in the field F_{l_i} (compare BURNSIDE, l. c., § 3, pp. 549, 550). Hence these irreducible factors are all invariants of the commutator group of Γ. Now the commutator group of G is the quotient-group of G by the subgroup H and hence is a group on n variables with $n - r$ parameters in F, and consequently has at most r independent invariants in F. Consider the $r = l_1 + l_2 + \cdots + l_\rho$ groups $J_1, \cdots, J_\rho$ and their conjugates with respect to F. Their determinants give r independent invariants of Γ and hence give rise to r independent functions in F which are invariants of G. Hence, for each value of i, the determinant (15) must be a power of an irreducible factor in F_{l_i}. The self-conjugate transformations of J_i form a group with one arbitrary parameter in F_{l_i}. It follows that the irreducible factor of (15) is linear only when $m_i = 1$ (compare BURNSIDE,* l. c., § 5). For $m_i > 1$, it must be a perfect square, $m_i = \mu_i^2$, and J_i is simply isomorphic with a linear homogeneous group on μ_i variables with coefficients in F_{l_i} (compare BURNSIDE, l. c., § 6). Since it involves μ_i^2 independent parameters, this group must be the general linear homogeneous group in F_{l_i} on μ_i variables. The transformations of J_i may therefore be given the form

$$z'_{tj} = u_{j1} z_{t1} + u_{j2} z_{t2} + \cdots + u_{j\mu_i} z_{t\mu_i} \qquad (t, j = 1, 2, \cdots, \mu_i),$$

the number of parameters u_{jk} being μ_i^2. The determinant corresponding to (15) is therefore the power μ_i of the determinant

$$|z_{tk}| \qquad (t,\, k = 1, 2, \cdots, \mu_i). \tag{16}$$

We may therefore state the following

THEOREM.—*Excluding the case in which the given field F has a modulus which divides the order n of the given finite group g, let the r linear factors*

* In a note offered to the Bulletin, I correct an error made by BURNSIDE in § 5.

of the special group-determinant be separated into sets of conjugates with respect to F, *the sets containing* $l_1, l_2, \cdots, l_\rho$ *factors, respectively. Denote by* $F_{l_1}, F_{l_2}, \cdots, F_{l_\rho}$ *the respective enlarged fields. The group* G *defined in* F *by the multiplication table of* g *is the direct product of* ρ *groups simply isomorphic with the general linear homogeneous groups in the fields* $F_{l_1}, F_{l_2}, \cdots, F_{l_\rho}$ *on* $\mu_1 = 1, \mu_2, \cdots, \mu_\rho$ *variables, respectively, where* $l_1\mu_1^2 + l_2\mu_2^2 + \cdots + l_\rho\mu_\rho^2 = n$. *For each* $i = 1, \cdots, \rho$, *the general group-determinant contains* l_i *distinct factors of degree* μ_i *belonging to and irreducible in the field* F_{l_i}, *and conjugate with respect to* F; *each of these factors occurs exactly to the power* μ_i *in the group-determinant. The general factor may be expressed as a determinant* (16) *on* μ_i^2 *independent linear functions of the* n *elements of the group-matrix.*

§ 8. *Two illustrative examples.*

Consider first the symmetric group g_6 on three letters, with the substitutions

$$s_1 = \text{identity},\quad s_2 = (132),\quad s_3 = (123),\quad s_4 = (12),\quad s_5 = (13),\quad s_6 = (23).$$

Denote by X, T and C the respective matrices *

$$\begin{bmatrix} x_1 & x_3 & x_2 & x_4 & x_5 & x_6 \\ x_2 & x_1 & x_3 & x_5 & x_6 & x_4 \\ x_3 & x_2 & x_1 & x_6 & x_4 & x_5 \\ x_4 & x_5 & x_6 & x_1 & x_3 & x_2 \\ x_5 & x_6 & x_4 & x_2 & x_1 & x_3 \\ x_6 & x_4 & x_5 & x_3 & x_2 & x_1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -2 & 2 & -1 & -1 \\ -2 & 1 & 1 & -1 & 2 & -1 \\ 1 & -2 & 1 & -1 & 2 & -1 \\ 1 & 1 & -2 & -1 & -1 & 2 \end{bmatrix}, \quad \begin{bmatrix} \lambda & 0 & 0 & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 & 0 & 0 \\ 0 & 0 & a & b & 0 & 0 \\ 0 & 0 & d & c & 0 & 0 \\ 0 & 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & 0 & d & c \end{bmatrix}.$$

The first matrix X is the group-matrix of g_6. The determinant of the second matrix T equals -2.3^5. If the field F has a modulus p, we assume that $p > 3$. Then † T defines a transformation which transforms that defined by X into that defined by C, where

$$\lambda = x_1 + x_2 + x_3 + x_4 + x_5 + x_6,\quad a = x_1 - x_2 + x_5 - x_6,\quad b = x_3 - x_2 + x_5 - x_4,$$

$$\mu = x_1 + x_2 + x_3 - x_4 - x_5 - x_6,\quad c = x_1 - x_3 - x_5 + x_6,\quad d = x_2 - x_3 + x_6 - x_4.$$

---

* For a simple and natural determination of the matrix T, from which follows incidentally the evaluation of its determinant, see the final reference in the introduction. For the case of a field containing an imaginary cube root of unity, DEDEKIND found a transformation having the desired property (Berliner Sitzungsberichte, 1897, p. 1007).

† Between the *matrices* the following relations therefore hold:

$$TXT^{-1} = C,\quad TX = CT.$$

Now λ, μ, a, b, c, d are independent functions of $x_1, \cdots, x_6$. Hence the group G of the transformations (x_i) is simply isomorphic with a group which is the direct product of two general unary linear groups in F and a general binary linear group in F.

The second example was chosen to illustrate the theory when the factors of the special group-determinant involve irrationalities. Aside from the cyclic groups, the dihedron group of order 10 is the simplest case in which irrationalities enter. A more difficult example is the simple group of order 60, the irrationality being $\sqrt{5}$. But no irrationality enters for a symmetric group (FROBENIUS).

The dihedron group g_{10} is generated by operators a, β such that

$$a^5 = I, \quad \beta^2 = I, \quad a\beta = \beta a^{-1}.$$

Its operators fall into four distinct sets of conjugate operators:

$$I; \quad a, \quad a^4; \quad a^2, \quad a^3; \quad \beta, \quad \beta a, \quad \beta a^2, \quad \beta a^3, \quad \beta a^4.$$

Denote a^i by a_i and βa^i by β_i for $i = 1, 2, 3, 4$. The group-matrix is

$$(17) \qquad \begin{array}{c|c} A & B \\ \hline B & A \end{array},$$

where

$$A \equiv \begin{vmatrix} I & a_1 & a_2 & a_3 & a_4 \\ a_4 & I & a_1 & a_2 & a_3 \\ a_3 & a_4 & I & a_1 & a_2 \\ a_2 & a_3 & a_4 & I & a_1 \\ a_1 & a_2 & a_3 & a_4 & I \end{vmatrix}, \qquad B \equiv \begin{vmatrix} \beta & \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta \\ \beta_2 & \beta_3 & \beta_4 & \beta & \beta_1 \\ \beta_3 & \beta_4 & \beta & \beta_1 & \beta_2 \\ \beta_4 & \beta & \beta_1 & \beta_2 & \beta_3 \end{vmatrix}.$$

By inspection, the group-determinant D is seen to have the factors

$$\delta \equiv I + a_1 + a_2 + a_3 + a_4 + \beta + \beta_1 + \beta_2 + \beta_3 + \beta_4,$$

$$\delta_1 \equiv I + a_1 + a_2 + a_3 + a_4 - \beta - \beta_1 - \beta_2 - \beta_3 - \beta_4.$$

If the field F has a modulus p, we assume that $p \neq 2, p \neq 5$. The transformation

$$\xi_1' = \sum_{j=1}^{10} \xi_j, \quad \xi_2' = \sum_{j=1}^{5} \xi_j - \sum_{j=6}^{10} \xi_j, \quad \xi_i' = \xi_i - \xi_1 \ (i = 3, 4, \cdots, 10)$$

has determinant 10. It transforms (17) into a matrix * having as first two rows

$$
\begin{matrix}
\delta & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \delta_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{matrix}
$$

and having zero as every element of the first column except that in the first row. New zero elements are introduced by transforming in succession by

$$[3, 6], \quad [5, 8], \quad [7, 4], \quad [4, 9], \quad [10, 5], \quad [10, 8], \quad [8, 3],$$

where $[i, j]$ is a transformation affecting only ξ_i which it replaces by $\xi_i - \xi_j$. The resulting matrix has zeros at the intersections of the third, fifth, seventh, ninth rows [columns] with the fourth, sixth, eighth, tenth columns [rows]. Applying next the transformation

$$[10, 8]^{-1} [4, 6] [6, 10] (\xi_4' = \xi_8, \xi_8' = \xi_{10}, \xi_{10}' = \xi_4, \xi_6' = -\xi_6),$$

we obtain a matrix in which the partial matrix on the variables $\xi_4, \xi_6, \xi_8, \xi_{10}$ is identical with that on $\xi_3, \xi_5, \xi_7, \xi_9$, viz., matrix M below. To make the elements of the second column, which lie in the third, $\cdots$, tenth rows, all zero, it suffices to transform by

$$
\begin{gathered}
\xi_3' = \xi_3 - \tfrac{1}{5}\xi_2, \quad \xi_5' = \xi_5 - \tfrac{1}{5}\xi_2, \quad \xi_7' = \xi_7 + \tfrac{1}{5}\xi_2, \quad \xi_9' = \xi_9 + \tfrac{1}{5}\xi_2, \\
\xi_4' = \xi_4 + \tfrac{2}{5}\xi_2, \quad \xi_6' = \xi_6 + \tfrac{2}{5}\xi_2, \quad \xi_8' = \xi_8 + \tfrac{3}{5}\xi_2, \quad \xi_{10}' = \xi_{10} - \tfrac{2}{5}\xi_2.
\end{gathered}
$$

Transforming by $(\xi_4 \xi_5 \xi_7)(\xi_6 \xi_9 \xi_8)$, we obtain the final matrix

$$
\left|\begin{array}{c|c|c}
\begin{smallmatrix}\delta & 0 \\ 0 & \delta_1\end{smallmatrix} & O & O \\
\hline
O & M & O \\
\hline
O & O & M
\end{array}\right|
$$

where each O denotes a matrix all of whose elements are zero, while M is the matrix

$$
\begin{bmatrix}
I - a_4 + \beta_1 - \beta_2 & a_2 - a_4 + \beta_1 - \beta_4 & -a_1 + a_4 - \beta_1 + \beta_3 & -a_3 + a_4 + \beta - \beta_1 \\
-a_2 + a_3 + \beta_3 - \beta_4 & I - a_2 - \beta_1 + \beta_3 & a_2 - a_4 + \beta - \beta_3 & -a_1 + a_2 + \beta_2 - \beta_3 \\
a_3 - a_4 - \beta_2 + \beta_3 & -a_1 + a_3 + \beta - \beta_2 & I - a_3 + \beta_2 - \beta_4 & a_2 - a_3 - \beta_1 + \beta_2 \\
a_1 - a_2 + \beta - \beta_4 & a_1 - a_4 + \beta_2 - \beta_4 & -a_1 + a_3 - \beta_1 + \beta_4 & I - a_1 - \beta_3 + \beta_4
\end{bmatrix}.
$$

* In this example, a matrix denotes the transformation defined by the matrix.

For a canonical form of still simpler type, we must resort to a transformation involving the irrationality $\sqrt{5}$. To obtain the special group-determinant, we must set $a_1 = a_4$, $a_2 = a_3$, $\beta = \beta_1 = \beta_2 = \beta_3 = \beta_4$. Then M becomes

$$M' \equiv \begin{vmatrix} I - a_1 & a_2 - a_1 & 0 & a_1 - a_2 \\ 0 & I - a_2 & a_2 - a_1 & a_2 - a_1 \\ a_2 - a_1 & a_2 - a_1 & I - a_2 & 0 \\ a_1 - a_2 & 0 & a_2 - a_1 & I - a_1 \end{vmatrix}.$$

Now M' may be transformed into the canonical form M'', in which the first two variables are multiplied by $I + a_1 y_2 + a_2 y_1$ and the last two by $I + a_1 y_1 + a_2 y_2$, where $y_1 = \frac{1}{2}(\sqrt{5} - 1)$, $y_2 = \frac{1}{2}(-\sqrt{5} - 1)$ are the roots of $y^2 + y - 1 = 0$. A transformation T such that $T^{-1} M' T = M''$ is given by the first of the following matrices, T^{-1} by the second:

$$\begin{vmatrix} 1 & \frac{-y_2}{\sqrt{5}} & y_1 - \frac{1}{\sqrt{5}} & \frac{-1}{\sqrt{5}} \\ 0 & y_1 & 1 & 1 \\ 1 & \frac{y_1}{\sqrt{5}} & y_2 + \frac{1}{\sqrt{5}} & \frac{1}{\sqrt{5}} \\ 0 & y_2 & 1 & 1 \end{vmatrix}, \quad \begin{vmatrix} \frac{-y_2}{\sqrt{5}} & \frac{-y_1}{5} & \frac{y_1}{\sqrt{5}} & \frac{y_1}{5} \\ 0 & \frac{1}{\sqrt{5}} & 0 & \frac{-1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{1}{5} & \frac{-1}{\sqrt{5}} & \frac{-1}{5} \\ \frac{-1}{\sqrt{5}} & \frac{3+\sqrt{5}}{10} & \frac{1}{\sqrt{5}} & \frac{-3-\sqrt{5}}{10} \end{vmatrix}.$$

It follows from the conjugacy of the variables in T and from the commutativity of M and M' that $T^{-1} M T$ has the form

$$M_1 \equiv \begin{vmatrix} A & B & 0 & 0 \\ C & D & 0 & 0 \\ 0 & 0 & A_1 & B_1 \\ 0 & 0 & C_1 & D_1 \end{vmatrix},$$

where A and A_1 are of the respective forms $a + a'\sqrt{5}$ and $a - a'\sqrt{5}$, etc. That M_1 is of the specified form is also shown by direct computation; then

$$A = I - \tfrac{1}{5}\sqrt{5}\,a_1 - \tfrac{1}{5}(y_2+3)a_2 + \tfrac{2}{5}\sqrt{5}\,a_3 + \tfrac{1}{5}\sqrt{5}(y_2-1)a_4 - \tfrac{1}{5}\sqrt{5}\,\beta + \beta_1$$
$$- \tfrac{1}{10}(5+3\sqrt{5})\beta_2 + \tfrac{2}{5}\sqrt{5}\,\beta_3 - \tfrac{1}{5}\sqrt{5}\,y_1\beta_4,$$
$$B = -\tfrac{1}{10}(7-\sqrt{5})(a_1-a_4) + \tfrac{1}{10}(1+3\sqrt{5})(a_2-a_3) + \tfrac{4}{5}\beta$$
$$-\tfrac{1}{10}(5+\sqrt{5})\beta_1 + \tfrac{3}{10}(\sqrt{5}-1)\beta_2 + \tfrac{1}{10}(\sqrt{5}-1)\beta_3 + \tfrac{1}{10}(1-3\sqrt{5})\beta_4,$$
$$C = y_2(a_2+\beta_4-a_3-\beta_3) + a_1 + \beta - a_4 - \beta_2,$$
$$D = I + \tfrac{2}{5}\sqrt{5}\,a_2 + \tfrac{1}{10}(\sqrt{5}-5)a_3 - \tfrac{1}{5}\sqrt{5}\,a_4 - \tfrac{1}{10}(5+3\sqrt{5})(a_1-\beta_2)$$
$$+ \tfrac{1}{5}\sqrt{5}\,\beta - \beta_1 - \tfrac{2}{5}\sqrt{5}\,\beta_3 + \tfrac{1}{10}(5-\sqrt{5})\beta_4$$

For the determinant $\Delta \equiv AD - BC$ we obtain the value*

$$I^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 - \beta^2 - \beta_1^2 - \beta_2^2 - \beta_3^2 - \beta_4^2$$
$$+ y_1(Ia_2 + Ia_3 + a_1a_3 + a_1a_4 + a_2a_4)$$
$$+ y_2(Ia_1 + Ia_4 + a_1a_2 + a_2a_3 + a_3a_4)$$
$$- y_1(\beta\beta_2 + \beta_1\beta_3 + \beta_2\beta_4 + \beta_3\beta + \beta_4\beta_1)$$
$$- y_2(\beta\beta_1 + \beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_4 + \beta_4\beta).$$

The value of $A_1D_1 - B_1C_1$ is obtained from Δ by interchanging y_1 with y_2.

That δ, δ_1, A, B, C, D, A_1, B_1, C_1, D_1 are independent functions of $I, a_1, \cdots, \beta_4$ follows from the fact that the final canonical form may be transformed into the initial matrix (17), so that $I, a_1, \cdots, \beta_4$ are linear functions of $\delta, \delta_1, \cdots, D_1$. To give a direct proof, we note that from δ and δ_1 may be derived

$$I + a_1 + a_2 + a_3 + a_4, \quad \beta + \beta_1 + \beta_2 + \beta_3 + \beta_4;$$

from C and C_1 may be derived $a_2 + \beta_4 - a_3 - \beta_3$, $a_1 + \beta - a_4 - \beta_2$; also

$$A + A_1 = 2I - a_2 - 3a_4 + 2\beta_1 - \beta_2 - \beta_4,$$
$$\sqrt{5}(A_1 - A_2) = -2a_1 + a_2 + 4a_3 - 3a_4 - 2\beta - 3\beta_2 + 4\beta_3 + \beta_4.$$

---

* This result was also computed directly by FROBENIUS's method. The characteristics of g_{10} are given by the table

f	χ_I	χ_{a_1}	χ_{a_2}	χ_β
1	1	1	1	1
1	1	1	1	-1
2	2	y_1	y_2	0
2	2	y_2	y_1	0

From these and the analogous expressions for $B \pm B_1$, $D \pm D_1$, we may derive $I, a_1, \cdots, \beta_4$.

If $\sqrt{5}$ belongs to the field F, the group G defined by the matrix (17) is simply isomorphic with a group given by the direct product of the two general unary groups and two general binary groups, all belonging to F. If $\sqrt{5}$ serves to extend F to a larger field F_2, G is simply isomorphic with a group given by the direct product of two general unary groups in F (having the respective multipliers δ, δ_1) and a general binary group in F_2, viz.,

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

THE UNIVERSITY OF CHICAGO,
March 10, 1902.