MODULAR INVARIANTS OF A GENERAL SYSTEM OF LINEAR FORMS

By L. E. DICKSON.

[Received February 2nd, 1909.—Read February 11th, 1909.]

1. After giving an outline of a method of marked simplicity for the investigation of modular invariants, we state the main results of the present self-contained treatment of linear forms.

In the simplest case, the coefficients of the forms discussed are integers reduced modulo p, where p is a prime. In the general case, the coefficients are Galois' imaginaries $c_0+c_1\rho+\ldots+c_{n-1}\rho^{n-1}$, in which the c's are integers reduced modulo p, while ρ is a root of a congruence of degree n, irreducible modulo p. These p^n imaginaries constitute the Galois field $GF[p^n]$.

We consider the system L of q linear forms,

$$l_i = a_{i1}x_1+\ldots+a_{im}x_m \quad (i = 1, \ldots, q), \tag{1}$$

whose coefficients are arbitrary elements of the $GF[p^n]$. Let G be any given group of linear homogeneous transformations on $x_1, \ldots, x_m$ with coefficients in the field. The p^{qmn} particular systems $L', L'', \ldots$, obtained by assigning to the a's particular values, can be separated into certain classes $C_0, C_1, \ldots, C_{f-1}$ under the group G, such that two systems are transformable into each other by transformations of G if, and only if, the systems belong to the same class.

By a general theorem on interpolation, there exists one, and but one, polynomial $I(a)$ in $a_{11}, a_{12}, \ldots, a_{qm}$, with each exponent $\leqslant p^n-1$ and coefficients in the $GF[p^n]$, such that $I(a)$ takes a prescribed value v_a for each set of elements a in the field. In particular, if v_a is the same for all sets a leading to a class C, so that $I(a)$ takes prescribed values $v_0, v_1, \ldots, v_{f-1}$ for the respective classes $C_0, C_1, \ldots, C_{f-1}$, then $I(a)$ is obviously an invariant of the system of forms (1) under the group G. Thus $I(a) = \Sigma v_k I_k$, where I_k is the uniquely determined invariant which has the value unity for the class C_k and the value zero for every class C_i $(i \neq k)$; I_k is called the *characteristic* invariant for the class C_k. If $\Sigma d_k I_k = 0$, each $d_k = 0$. Although there is no linear homogeneous relation between the I's, we have $\Sigma I_k = 1$. In the former sense, we

shall say that $I_0, \ldots, I_{f-1}$ are linearly independent. Hence the total number of linearly independent invariants under G equals the number of classes under G.

When G is the total linear group on the m variables, the invariants just discussed are the *absolute* invariants of the system L. When the group is the group G_1 of all transformations of determinant unity, those invariants of G_1 which are multiplied by Δ^w under every transformation of determinant Δ are the *relative* invariants of weight w (absolute when w is a multiple of p^n-1). The number N of linearly independent invariants, relative and absolute, of the system L obviously does not exceed the number of the linearly independent invariants of G_1, the latter being the number f of the classes under G_1. As a matter of fact, $N = f$, as I have shown by a rather technical proof.* This result, however, is not presupposed in the present paper. Indeed, we here exhibit explicitly f linearly independent invariants of the general system L of linear forms. Hence $N \geqslant f$. But $N \leqslant f$, by the above simple discussion; whence $N = f$.

In the algebraic theory, q linear forms in m variables have no rational integral invariants if $q < m$, while, if $q \geqslant m$, the invariants are functions of the determinants of sets of m forms. If, for $h < m$, $l_1, \ldots, l_h$ are linearly independent, and

$$l_{h+1} = c_1 l_1 + \ldots + c_h l_h,$$

the c's are obviously invariant under linear transformation; in the modular theory (in contrast to the algebraic theory), the c's may be expressed by rational integral invariants (§ 8). In spite of the greater variety of invariants in the modular theory, we establish the following fundamental theorem: *Every invariant of a system of $q > m$ linear forms in m variables is a rational integral function of the invariants of systems of m forms in m variables.*

2. When there is a single variable, G_1 contains only the identity transformation, so that each system of forms $a_{i1}x_1$ constitutes a class. As a complete system of linearly independent invariants we may take the p^{qn} products of the powers of the a_{i1} with exponents $0, 1, \ldots, p^n-1$. Henceforth we take $m > 1$.

For a single form l_i there are two classes under G_1, one class containing only $l_i \equiv 0$, the other class containing the forms in which not every

* "General Theory of Modular Invariants," *Transactions of the American Mathematical Society*, Vol. x., April, 1909.

a_{iv} is zero and hence conjugate with x_1. For the respective classes the characteristic invariants are A_i and $1-A_i$, where

$$A_i = \prod_{v=1}^{m} (1-a_{iv}^{\mu}) \quad (\mu = p^n-1). \tag{2}$$

3. Two forms l_i, l_j may be linearly independent, or dependent with $l_i \neq 0$, &c. Hence they can be transformed within G_1 into one of the four pairs in the following table, which also gives the values of certain invariants :—

l_i	l_j	A_i	A_j	A_iA_j	V_{ij}
x_1	dx_2	0	0	0	0
x_1	cx_1	0	$1-c^{\mu}$	0	c
0	x_1	1	0	0	0
0	0	1	1	1	0

Here $d = 1$, if $m > 2$; while, for $m = 2$, d is the non-vanishing determinant D_{ij} of a pair of independent forms l_i, l_j. For the construction of an invariant V_{ij} taking the assigned values for the various classes, we may proceed as in § 8 or as follows. If, in (2), we replace a_{iv} by $a_{iv}-\kappa a_{jv}$ and apply

$$\kappa^{p^n} = \kappa, \tag{3}$$

we obtain a polynomial in κ of degree $\mu = p^n-1$; the coefficient of each power of κ is an absolute invariant of l_i, l_j. It will be seen to be convenient to separate the terms involving κ^{μ} and write

$$\prod_{v=1}^{m} [1-(a_{iv}-\kappa a_{jv})^{\mu}] \equiv A_i + A_i(A_j-1)\kappa^{\mu} - \sum_{t=1}^{\mu} S_{ijt}\kappa^t \tag{4}$$

for every root of (3). For x_1, cx_1, the non-vanishing a's are $a_{i1} = 1$, $a_{j1} = c$. Hence in (4) the factors with $v > 1$ equal unity, while the factor with $v = 1$ is $1-(1-\rho c)^{\mu}$. But

$$(\alpha-\beta)^{\mu} \equiv \sum_{t=0}^{\mu} \alpha^{\mu-t}\beta^t \pmod{p}. \tag{5}$$

Hence, for the pair x_1, cx_1, (4) becomes

$$-\sum_{t=1}^{\mu} c^t\kappa^t = -\sum_{t=1}^{\mu} S_{ijt}\kappa^t.$$

For the remaining pairs in the table, we find immediately that $S_{ijt}=0$. Hence $V_{ij}=S_{ij1}$, $S_{ijt}=S_{ij1}$. Thus V_{ij} is the sum of the coefficients of κ, $\kappa^{\mu+1}$, $\kappa^{2\mu+1}$, ... in the expansion of the left member of (4). Applying (5), get

$$V_{ij}=\Sigma F_{1t_1}F_{2t_2}\dots F_{mt_m} \tag{6}$$

$$[t_1+\dots+t_m\equiv 1 \pmod{\mu};\ t_1,\dots,t_m=0,1,\dots,\mu],$$

$$F_{vt}=-a_{iv}^{\mu-t}a_{jv}^{t}\ (t>0),\qquad F_{v0}=1-a_{iv}^{\mu}. \tag{7}$$

In particular, for $m=2$,

$$V_{ij}=(a_{i1}^{\mu}-1)a_{i2}^{\mu-1}a_{j2}+(a_{i2}^{\mu}-1)a_{i1}^{\mu-1}a_{j1}+\sum_{t=1}^{\mu}a_{i1}^{\mu-t}a_{j1}^{t}a_{i2}^{t-1}a_{j2}^{\mu+1-t}. \tag{6'}$$

By undetermined coefficients it follows, from the above table (or by the more instructive method of § 4), that the absolute invariants

$$1,\ A_i,\ A_j,\ A_iA_j,\ V_{ij}^{t}\quad (t=1,\dots,\mu) \tag{8}$$

are linearly independent; also, that, for $m=2$, the only linear relation between the invariants (8) and D_{ij}^{k} $(k=1,\dots,\mu)$ is

$$D_{ij}^{\mu}+V_{ij}^{\mu}=(1-A_i)(1-A_j). \tag{9}$$

The number of classes is p^n+3 if $m>2$, $2p^n+1$ if $m=2$.

THEOREM.—*As a complete set of linearly independent invariants of two linear forms l_i and l_j in the $GF[p^n]$ on m variables, we may take the p^n+3 absolute invariants* (8) *if $m>2$, and, if $m=2$, the $2p^n+1$ invariants*

$$A_i,\ A_j,\ A_iA_j,\ V_{ij}^{t},\ D_{ij}^{t}\quad (t=1,\dots,p^n-1). \tag{10}$$

4. We readily derive the characteristic invariants for the various classes of two linear forms in m variables. For x_1, 0; 0, x_1; 0, 0, these are

$$A_j-A_iA_j,\quad A_i-A_iA_j,\quad A_iA_j. \tag{11}$$

For x_1, cx_1, where $c\neq 0$, the characteristic invariant is

$$-\sum_{k=1}^{\mu}c^{-k}V_{ij}. \tag{12}$$

Indeed, for $V=c$, this sum is $-\mu\equiv 1 \pmod{p}$, for $V=\gamma\neq c$; it equals a fraction with the numerator $(c^{-1}\gamma)^{\mu+1}-c^{-1}\gamma$, which vanishes in the field. For $m=2$, the characteristic invariant of x_1, dx_2 $(d\neq 0)$ is likewise

$$-\sum_{k=1}^{\mu}d^{-k}D_{ij}^{k}. \tag{13}$$

The linear independence of invariants (10) thus follows from that of the characteristic invariants (11), (12), (13), where c and d range over the μ elements $\neq 0$ of the field. The sum of the μ functions (12) is V_{ij}^{μ}, since* the sum of the k-th powers of the elements of the field is zero for $0 < k < \mu$, and -1 for $k = \mu$. But the sum of all the characteristic invariants is 1 (§ 1). Hence relation (9) follows.

For $m > 2$, the characteristic invariant of x_1, x_2 is

$$(14) \qquad (1-A_i)(1-A_j) - V_{ij}^{\mu},$$

determined so that the sum of all shall be unity, or directly from the table of § 3. Since the linearly independent characteristic invariants (11), (12), (14) are linear functions of invariants (8), the latter are linearly independent.

5. For a given set of elements E, we shall say that

$$(15) \qquad E_{rst\ldots} \text{ precedes } E_{\rho\sigma\tau\ldots}, \qquad E_{\rho\sigma\ldots} \text{ follows } E_{rs\ldots},$$

if $r < \rho$; or, if $r = \rho$, $s < \sigma$; or, if $r = \rho$, $s = \sigma$, $t < \tau$; &c.

6. Every invariant of q binary linear forms will be shown to equal a rational integral function of A_i, V_{ij}, D_{ij} $(i, j = 1, \ldots, q)$. We employ a canonical type for each system of q forms with given coefficients in the field.

First, let not every D_{ij} vanish. Let $D_{rs} \neq 0$ $(r < s)$, but let every preceding D_{ij} $(i < j)$ vanish, viz.,

$$(16) \qquad D_{ij} = 0 \ (i < r), \qquad D_{rk} = 0 \ (r < k < s), \qquad D_{rs} \neq 0.$$

After applying an obvious transformation of G_1, we have

$$l_r = x_1, \qquad l_s = cx_2, \qquad c = D_{rs}.$$

By $D_{ir} = D_{is} = 0$ $(i < r)$, l_i is free of x_2 and x_1. By $D_{rk} = 0$, l_k is free of x_2. Hence the canonical type is

$$(17) \qquad l_i = 0, \quad l_r = x_1, \quad l_k = c_k x_1, \quad l_s = cx_2, \quad l_t = -d_t x_1 + e_t x_2$$
$$(i < r < k < s < t \leqslant q; \ c \neq 0).$$

Next, let every $D_{ij} = 0$, but not every l_i, vanish identically. Let l_f be the first non-vanishing l. Applying a transformation of G_1, we get

$$(18) \qquad l_i = 0, \qquad l_f = x_1, \qquad l_j = m_j x_1 \quad (i < f < j \leqslant q).$$

* Dickson, *Linear Groups*, Leipzig, 1901, p. 54.

Finally, there remains the system

$$l_i = 0 \quad (i = 1, \ldots, q). \tag{19}$$

A system of forms (17) defines a class A_{rs}^{cde}; a system (18) defines a class B_f^m; the system (19) the class C_0. In addition to the definition in § 5, we shall say that any class A precedes a class B or C_0, and that any B precedes C_0. No two classes are equivalent under G_1. As to the A's, this follows from the invariance of the D_{ij}; for (17), we have relations (16) and

$$D_{rs} = c, \quad D_{rt} = e_t, \quad D_{ks} = cc_k, \quad D_{st} = cd_t \quad (r < k < s < t), \tag{20}$$

so that the c, d, e may be expressed in terms of invariants. For (18),

$$V_{ff} = mj \quad (f < j \leqq q), \tag{21}$$

where V is the invariant of § 3. Since the c_k, d_t, e_t may take any values in the field and c any values $\neq 0$, it follows from (20) that the products

$$\prod_{k=r+1, \ldots, s-1;\ t=s+1, \ldots, q} D_{rs}^{\gamma} D_{ks}^{\gamma_k} D_{rt}^{\epsilon_t} D_{st}^{\delta_t} \quad (\gamma = 1, \ldots, \mu;\ \gamma_k, \epsilon_t, \delta_t = 0, 1, \ldots, \mu) \tag{22}$$

are linearly independent in the field, and that the number of these invariants (22) is the number of classes A_{rs}^{cde}. In view of the factor D_{rs}, (22) vanishes for the classes B, C_0, and those classes $A_{\rho\sigma}$ which follow the A_{rs}. Similarly,

$$1 - A_f, \qquad \prod_{j=f+1}^{q} V_{ff}^{\mu_j} \quad (\mu_j = 0, 1, \ldots, \mu;\ \text{not every } \mu_j = 0) \tag{23}$$

are linearly independent, of the same number as the classes B_f^m, and vanish for the classes C_0, B_ϕ $(\phi > f)$ which follow the B_f. Finally, with the class C_0 we associate the invariant 1. We deduce at once the linear independence of the specified invariants whose number equals that of the classes.

THEOREM—*Every invariant of q binary linear forms is expressible in terms of invariants of pairs of forms. A complete set of the*

$$(p^{mq}-1)(p^{n(q-1)}-1)/(p^{2n}-1)+(p^{mq}-1)/(p^{n}-1)+1$$

linearly independent invariants of q binary linear forms in the $GF[p^n]$ is given by unity, (22) and (23) for $r, s, f = 1, \ldots, q$; $r < s$.*

7. For $q = 3$, the $p^{3n}+p^{2n}+p^{n}+1$ linearly independent variants are

$$D_{12}^{\alpha} D_{13}^{\beta} D_{23}^{\gamma} \ (\alpha, \beta, \gamma = 0, 1, \ldots, \mu), \qquad A_1, A_2, A_3,$$
$$V_{12}^{\rho}, \ V_{13}^{\rho}, \ V_{23}^{\rho}, \ V_{12}^{\rho} V_{13}^{\sigma} \quad (\rho, \sigma = 1, \ldots, \mu).$$

* We may introduce $A_1 A_2$ instead of 1 by (9). Then, if $q = 2$, the set becomes (10).

Other products can be expressed in terms of these by (9) and

$$A_1 D_{12} = 0, \qquad A_1 D_{23} = (D_{12}^{\mu}-1)(D_{13}^{\mu}-1)D_{23},$$

$$A_1 V_{12} = 0, \qquad A_1 V_{23}^{t} = (D_{23}^{\mu}-1)D_{12}^{2\mu-t}D_{13}^{t} - V_{12}^{2\mu-t}V_{13}^{t} + V_{23}^{t},$$

$$D_{12}V_{12} = 0, \qquad D_{12}^{\lambda}V_{13}^{t} = (-1)^{\lambda}D_{12}^{\mu+\lambda-t}D_{23}^{t}(1-D_{13}^{\mu}),$$

$$V_{ij}^{t}V_{jk}^{e} = V_{ij}^{\mu+t-e}V_{ik}^{e}, \qquad V_{ik}^{t}V_{jk}^{e} = V_{ij}^{2\mu-e}V_{ik}^{t+e},$$

$$(1-A_1)(1-A_2)(1-A_3) = V_{12}^{\mu}V_{13}^{\mu}+D_{12}^{\mu}D_{13}^{\mu}+D_{12}^{\mu}D_{23}^{\mu}+D_{13}^{\mu}D_{23}^{\mu}-2D_{12}^{\mu}D_{13}^{\mu}D_{23}^{\mu}.$$

For $q = 4$, we use also $D_{12}D_{34}-D_{13}D_{24}+D_{14}D_{23} = 0$ and its products by

$$D_{12}^{\mu}, \quad 1-D_{12}^{\mu}, \quad (1-D_{12}^{\mu})(1-D_{13}^{\mu}).$$

8. We employ a general function-theoretic process to construct an invariant* $V = V_{i_1, \ldots, i_{h+1}}$ of $h+1$ (not necessarily linear forms $l_{i_1}, \ldots, l_{i_{h+1}}$) in m' variables ($m' > h$), such that V shall have the value c_1 when $l_{i_1}, \ldots, l_{i_h}$ are linearly independent, but $l_{i_1}, \ldots, l_{i_{h+1}}$ dependent and

$$l_{i_{h+1}} = c_1 l_{i_1} + \ldots + c_h l_{i_h}, \tag{24}$$

while V shall have the value zero for all systems of $h+1$ forms not having the preceding two properties. Let $a_{11}, \ldots, a_{1m}$ be the coefficients of l_1 in any order; $a_{i1}, \ldots, a_{im}$ the corresponding coefficients of l_i. Since V shall vanish if the $h+1$ forms are linearly independent, we may set

$$V = v\Pi(1-M^{\mu}) \quad (\mu = p^n-1), \tag{25}$$

M ranging over the determinants of order $h+1$ in the matrix of the l's. It suffices to consider henceforth only sets of coefficients for which every $M = 0$; for such a set $V = v$. Of these sets, consider one for which

$$D = |a_{ij}| \quad (i = i_1, \ldots, i_h; \; j = j_1, \ldots, j_h) \tag{26}$$

is not zero, $j_1, \ldots, j_h$ being distinct integers $\leqslant m$. Thus there holds a relation of type (24), so that

$$a_{i_{h+1}r} = \sum_{s=1}^{h} c_s a_{i_s r} \quad (v = 1, \ldots, m).$$

Taking $v = j_1, \ldots, j_h$, we have h equations in which the determinant of the coefficients of $c_1, \ldots, c_h$ equals (26) with rows and columns interchanged. Let d denote the determinant derived from (26) by replacing (in the first row) each $a_{i_1 j}$ by $a_{i_{h+1} j}$. Then $Dc_1 = d$. Thus $c_1 = dD^{\mu-1}$.

Let $D_1, \ldots, D_r$ denote the determinants (26), taken in any sequence, which are defined by the $r = \binom{m}{h}$ combinations $j_1, \ldots, j_h$ of h integers

* The order of the intermediate subscripts $i_2, \ldots, i_h$ is immaterial.

$\leqslant m$. Let $d_1, \ldots, d_r$ denote the corresponding determinants d in the same sequence. We have

$$v = d_k D_k^{\mu-1} \quad (\text{when } D_k \neq 0).$$

From $v = d_1 D_1^{\mu-1}$, when $D_1 \neq 0$, we get

$$v \equiv d_1 D_1^{\mu-1} + \lambda_1 (1 - D_1^{\mu}).$$

To determine λ_1, we consider a set making $D_1 = 0$, $D_2 \neq 0$. For such a set

$$d_2 D_2^{\mu-1} = v = \lambda_1,$$

so that for every set with $D_1 = 0$

$$\lambda_1 = d_2 D_2^{\mu-1} + \lambda_2 (1 - D_2^{\mu}).$$

The product of the two members by $1 - D_1^{\mu}$ are equal for every D_1. Thus

$$v \equiv d_1 D_1^{\mu-1} + (1 - D_1^{\mu})\, d_2 D_2^{\mu-1} + \lambda_2 (1 - D_1^{\mu})(1 - D_2^{\mu})$$

for all sets. Proceeding similarly, we find by induction that

$$(27) \quad v = d_1 D_1^{\mu-1} + (1 - D_1^{\mu})\, d_2 D_2^{\mu-1} + (1 - D_1^{\mu})(1 - D_2^{\mu})\, d_3 D_3^{\mu-1} + \ldots + (1 - D_1^{\mu}) \ldots (1 - D_{r-1}^{\mu})\, d_r D_r^{\mu-1}$$

with initially the additional term

$$\lambda_r (1 - D_1^{\mu}) \ldots (1 - D_r^{\mu}).$$

But for a set for which $D_1, \ldots, D_r$ all vanish, (27) becomes $v = \lambda_r$, while by hypothesis $V = 0$, so that, by (25), $v = 0$. The invariance of V, given by (25) and (27), follows from the fact that it takes the same value for any two systems of $h+1$ forms equivalent under the total group.

For $h = 1$ we set $i_1 = i$, $i_2 = j$, and obtain

$$V_{ij} = \{a_{j1} a_{i1}^{\mu-1} + (1 - a_{i1}^{\mu})\, a_{j2} a_{i2}^{\mu-1} + \ldots + (1 - a_{i1}^{\mu}) \ldots (1 - a_{im-1}^{\mu})\, a_{jm} a_{im}^{\mu-1}\} \Pi (1 - M^{\mu}),$$

where M ranges over the determinants $a_{ir} a_{js} - a_{is} a_{jr}$ $(r, s = 1, \ldots, m)$.

9. We proceed to exhibit a complete set of linearly independent invariants of the system of $q \geqslant m$ linear forms l_i on m variables with arbitrary coefficients in the $GF[p^n]$. We shall employ a canonical type for each system with given coefficients.

First, let m of the forms be linearly independent. Let $l_{r_1}, \ldots, l_{r_m}$ $(r_1 < r_2 \ldots < r_m)$ be independent, but every preceding (§ 5) set of m forms dependent. Applying a transformation of G_1, we have

$$(28_a) \qquad l_r = x_k \quad (k < m), \qquad l_{r_m} = c x_m \quad (c \neq 0).$$

For $i_1 < r_1$, l_{i_1} and any $m-1$ of the forms $l_{r_1}, \ldots, l_{r_m}$ are dependent by hypothesis; whence $l_{i_1} = 0$. For $r_1 < i_2 < r_2$, l_{r_1}, l_{i_2} and any $m-2$ of the forms $l_{r_2}, \ldots, l_{r_m}$ are dependent; whence l_{i_2} is a multiple of x_1. Proceeding similarly, we get

$$(28_b) \qquad l_{i_1} = 0, \qquad l_{i_t} = \sum_{j=1}^{t-1} b_{i_t j} x_j \quad (t = 2, \ldots, m+1),$$

$$(i_1 < r_1 < i_2 < r_2 < i_3 \ldots < r_{m-1} < i_m < r_m < i_{m+1} \leqq q).$$

Conversely, the q forms (28_a) and (28_b) obviously have the properties that $l_{r_1}, \ldots, l_{r_m}$ are independent, while every preceding set of m forms give dependent forms. We employ the determinants of order m:

$$(29) \qquad D_{r_1 \ldots r_m} = c, \quad D_{r_1 \ldots r_{j-1} i_t r_{j+1} \ldots r_m} = \begin{Bmatrix} c b_{i_t j} & (j < m) \\ b_{i_t j} & (j = m) \end{Bmatrix}$$

$$(t = 2, \ldots, m+1\,;\ j < t).$$

The parameters c, b are uniquely determined by these determinants, which are invariant. Hence no two of the classes* $A^{bc}_{r_1 \ldots r_m}$ defined by (28) are equivalent under the group G_1. For given values of the r's, the number of these classes equals the number of products

$$(30) \qquad \Pi D^{\gamma}_{r_1 \ldots r_m} D^{\beta_{i_t j}}_{r_1 \ldots r_{j-1} i_t r_{j+1} \ldots r_m},$$

where a particular product is obtained by taking all sets

$$t = 2, \ldots, m+1\,;\ j = 1, \ldots, t-1,$$

and then allowing $i_2, \ldots, i_{m+1}$ to range over all sets of integers $1, \ldots, q$ satisfying the inequalities (28_b); while the various products are obtained by taking

$$\gamma = 1, \ldots, \mu\,;\ \beta_{i_t j} = 0, 1, \ldots, \mu \quad (\mu = p^n - 1).$$

Since the b's are arbitrary in the field, while c has any value $\neq 0$, it follows from (29) that the various products (30) are linearly independent in the field. Allowing the r's to vary, we obtain as many linearly independent invariants (30) as there are classes $A^{bc}_{r_1 \ldots r_m}$. Indeed, in view of the first factor, the product (30) vanishes for any class $A^{b'c'}_{r'_1 \ldots r'_m}$ which follows $A^{bc}_{r_1 \ldots r_m}$.

Next, for $h < m$, let h of the q forms be linearly independent, but every set of $h+1$ of the forms be dependent. Let

$$l_{r_1}, \ldots, l_{r_h} \quad (r_1 < r_2 \ldots < r_h)$$

be independent, but every preceding set of h forms dependent. Apply-

* We employ b to denote the ordered aggregate of the coefficients in (28_a).

ing a transformation of G_1, we have $l_{r_1} = x_1, \ldots, l_{r_h} = x_h$. We derive (28_b), with m replaced by h. For the invariants determined in § 8, we have

$$V_{r_j r_1 \ldots r_{j-1} r_{j+1} \ldots r_h i_t} = b_{i_t j} \quad (t = 2, \ldots, h+1\,;\ j < t). \tag{31}$$

Hence no two of the present classes $B^b_{r_1 \ldots r_h}$ are equivalent under G_1. Each invariant (31) vanishes for every subsequent class $B^{b'}_{r'_1 \ldots r'_{h'}}$ $(h' \leqslant h)$ and for the class C_0 composed of the system (19). For given r's, consider the products

$$\Pi V^{\beta_{i_t j}}_{r_j r_1 \ldots r_{j-1} r_{j+1} \ldots r_h i_t} \quad \text{(exponents not all zero)}, \tag{32}$$

a particular product being obtained by taking all sets $t = 2, \ldots, h+1$; $j = 1, \ldots, t-1$ and allowing $i_2, \ldots, i_{h+1}$ to range over all sets of h of the integers $1, \ldots, q$ for which

$$r_1 < i_2 < r_2 < i_3 < \ldots < r_h < i_{h+1}\,;$$

while the various products are obtained by taking each $\beta = 0, 1, \ldots, \mu$, but not all zero. In place of unity, excluded in (32), we desire an invariant E which has the value 1 for each class $B^b_{r_1 \ldots r_h}$ and the value 0 for the subsequent classes. Thus E may be taken to be that invariant of the forms $l_{r_1}, \ldots, l_{r_h}$ alone which is characteristic for the class containing $x_1, \ldots, x_h$. Hence

$$E_{r_1 \ldots r_h} = 1 - \Pi(1 - D^\mu), \tag{33}$$

where D ranges over the determinants of order h in the matrix of the hm coefficients of the h forms on $m > h$ variables. Indeed, $E = 1$ if any $D \neq 0$, $E = 0$ if every $D = 0$. Since the invariants (32) and (33) vanish for all classes following $B^b_{r_1 \ldots r_h}$, they are linearly independent. Varying h and the r's we obtain as many linearly independent invariants (32) and (33) as there are classes B. With the class C_0 of vanishing forms we associate the invariant * 1.

Since we have exhibited as many linearly independent invariants as there are classes under the group G_1, we have proved the

THEOREM.—*For $q > m$, every invariant of q linear forms in the $GF[p^n]$ on m variables is a rational integral function of the invariants of m forms on m variables. A complete set of linearly independent invariants of $q \geqslant m$ forms is given by* (30), (32), (33) *and unity, each being a polynomial in the determinants of orders $\leqslant m$ of the matrix of the coefficients of the forms.*

* We may take any invariant, as (35), which does not vanish for C_0.

10. For $q < m$, the first case of § 9 does not occur. If the q forms are linearly independent, they may be transformed into $x_1, \ldots, x_q$. For the resulting class $B^0_{1 \ldots q}$ the characteristic invariant $E_{1 \ldots q}$ is given by (33) for $h = q$. If, for $h < q$, h of the forms are linearly independent, but every set of $h+1$ dependent, we proceed as in § 9.

THEOREM.—*For $q < m$, a complete set of linearly independent invariants of q linear forms on m variables is given by* (32) *for $h < q$,* (33) *for $h \leqslant q$, and unity.*

11. Instead of introducing the new invariants E, we may make use of products of the invariants A_i of single forms (§ 2). In place of (33), we use

$$J_{r_1 \ldots r_h} = \Pi A_i \quad (i = 1, \ldots, q\,; \; i \neq r_1, \ldots, i \neq r_h). \tag{34}$$

For the class C_0 the characteristic invariant is

$$A_1 A_2 \ldots A_q. \tag{35}$$

For $q \geqslant m$, there are as many invariants (30), (32), (34), (35) as classes under G_1. Suppose there is a linear (homogeneous) relation between these invariants. For the class $B^0_{r_1 \ldots r_h}$, the D's and V's vanish, while

$$A_{r_1} = 0, \; \ldots, \; A_{r_h} = 0, \; A_i = 1 \quad (i \neq r_1, \ldots, i \neq r_h).$$

Taking $h = m-1$, we see that the only non-vanishing invariant of the set (34), (35) is $J_{r_1 \ldots r_{m-1}}$, whose coefficient in the relation therefore vanishes. We take in turn the various sets of $m-1$ subscripts r. Proceeding similarly with $h = m-2, \ldots, h = 1$, we conclude that no invariant (34) occurs in the relations. Taking every $l_i = 0$, we see that the coefficient of $A_1 \ldots A_q$ vanishes. The relation now involves only the D's and V's; but these were shown in § 9 to be linearly independent.

For $q < m$, we replace $E_{1 \ldots q}$ of § 10 by unity, which takes the place of (34) for $h = q$. For the independence proof we employ in succession the classes $B^0_{r_1 \ldots r_h}$ for $h = q, q-1, \ldots, 1$ and C_0. The case $h = q$ shows that the relation lacks the invariant unity.

THEOREM.—*A complete set of linearly independent invariants of q linear forms on m variables is given by* (30), (32), (34), (35) *if $q \geqslant m$; and by* (32), (34), (35) *and unity if $q < m$, viz., by* (32) *and the 2^q products $A_1^{\alpha_1} \ldots A_q^{\alpha_q}$ (each $\alpha = 0$ or 1).*

12. It now follows that the invariant E of h forms on m variables, $m > h$, is expressible in terms of the A's and V's. Since E is the

characteristic invariant for the class containing $x_1, \ldots, x_h$, formula (14) gives

$$E_{ij} = (1-A_i)(1-A_j) - V_{ij}^{\mu}, \tag{36}$$

while, by § 2, $E_i = 1-A_i$. A comparison of (36) with (9) reveals a fact which is true for any h. If, in the expression for $E_{r_1 \ldots r_h}$ in terms of the invariants A and V of h forms on $m > h$ variables, we replace E by $D^{\mu}_{r_1 \ldots r_h}$, we obtain a true relation between the invariants of h forms on h variables, where D is the determinant of the latter forms. The converse is true if we employ the non-homogeneous linear relation $D^{\mu} + \ldots = 1$ which hold between the invariants of § 11 for h forms in h variables. Such a relation exists, since the sum of the characteristic invariants is unity (§ 1) and since the sum of those for the classes $x_1, \ldots, x_{h-1}, dx_h$ (d taking all values $\neq 0$) is D^{μ} (§ 4). This relation not not only gives at once the desired expression for E, but is of considerable importance in the general theory. We shall derive it by certain devices for $h = 3$ and $h = 4$.

13. For three forms in $m \geqslant 3$ variables, we have

			V_{123}	V_{213}	V_{132}	V_{12}	V_{13}	V_{23}	A_1	A_2	A_3
x_1	x_2	bx_3	0	0	0	0	0	0	0	0	0
x_1	x_2	$cx_1 + dx_2$	c	d	$-cd^{\mu-1}$	0	$c(1-d^{\mu})$	$d(1-c^{\mu})$	0	0	$(1-c^{\mu})(1-d^{\mu})$
x_1	ex_1	x_2	0	0	e	e	0	0	0	$1-e^{\mu}$	0
0	x_1	x_2	0	0	0	0	0	0	1	0	0
x_1	fx_1	gx_1	0	0	0	f	g	$gf^{\mu-1}$	0	$1-f^{\mu}$	$1-g^{\mu}$
0	x_1	hx_1	0	0	0	0	0	h	1	0	$1-h^{\mu}$
0	0	x_1	0	0	0	0	0	0	1	1	0
0	0	0	0	0	0	0	0	0	1	1	1

In the first type, $b = 1$ if $m > 3$; while, if $m = 3$, b may have any value $\neq 0$. The remaining parameters $c, \ldots, h$ are arbitrary in the field. By § 11 a complete set of linearly independent invariants is given, for $m > 3$, by $A_1^{a_1} A_2^{a_2} A_3^{a_3}$ (each $a = 0$ or 1), the powers of V_{132} and V_{23}, the products of the powers of V_{123} and V_{213}, and those for V_{12} and V_{13}, the exponents being $\leqslant \mu$. For $m = 3$, unity is to be deleted and the powers of the determinant $D = D_{123}$ inserted.

Invariant E_{12}, defined by (36), equals 1 for the first two types and 0 for the other types. Hence $A_3 E_{12}$ is the characteristic invariant for

the class $x_1, x_2, 0$. To obtain its expression as a linear function of the above invariants, we need $A_3 V_{12}^{\mu}$. Now

$$V_{132}^{\mu} - V_{123}^{\mu} V_{213}^{\mu} = V_{12}^{\mu}(1 - A_3 - V_{13}^{\mu}), \tag{37}$$

since each member vanishes except for the third type and equals e^{μ} for the latter. Hence

$$A_3 E_{12} = A_3(1-A_1)(1-A_2) + V_{132}^{\mu} - V_{123}^{\mu} V_{213}^{\mu} - V_{12}^{\mu} + V_{12}^{\mu} V_{13}^{\mu}. \tag{38}$$

For $m = 3$, $E_{12} - D^{\mu}$ equals 1 for the second type, 0 for the other types. Hence the characteristic invariant for $x_1, x_2, 0$ is given by

$$E_{12} - D^{\mu} + (1 - V_{123}^{\mu})(1 - V_{213}^{\mu}) - 1. \tag{39}$$

Inserting the value (36) of E_{12} and equating the result to (38), we obtain the desired non-homogeneous linear relation between our invariants for $m = 3$:

$$D^{\mu} = 2V_{123}^{\mu} V_{213}^{\mu} - V_{123}^{\mu} - V_{213}^{\mu} - V_{132}^{\mu} - V_{12}^{\mu} V_{13}^{\mu} + (1-A_1)(1-A_2)(1-A_3). \tag{40}$$

The right member is thus the expression for the invariant E_{123} of three forms in m variables for $m > 3$.

We note in passing that it is not difficult to exhibit the characteristic invariant $I_{c,d}$ of the general class $A_{c,d}$ of the second type. As in § 4, we employ

$$\kappa_c = -\sum_{k=1}^{\mu} c^{-k} V_{123}^{k}, \qquad \lambda_d = -\sum_{k=1}^{\mu} d^{-k} V_{213}^{k}. \tag{41}$$

If $c \neq 0$, $\kappa_c = 1$ for $A_{c,d}$, 0 for $A_{\gamma,\delta}$, for every d, γ, δ, $\gamma \neq c$. If $d \neq 0$, $\lambda_d = 1$ for $A_{c,d}$, 0 for $A_{\gamma,\delta}$, for every c, γ, δ, $\delta \neq d$. Hence

$$I_{c,d} = \kappa_c \lambda_d \quad (cd \neq 0), \qquad I_{c,0} = \kappa_c(1 - V_{213}^{\mu}) \quad (c \neq 0), \tag{42}$$

$$I_{0,d} = \lambda_d(1 - V_{123}^{\mu}) \quad (d \neq 0), \quad I_{0,0} \text{ in (38) or (39)}.$$

As a check, the sum of these p^{2n} characteristic invariants was verified to be $E_{12} - D^{\mu}$ by means of $\Sigma c^{-k} d^{-t} = (\Sigma c^{-k})(\Sigma d^{-t}) = 1$ if $\kappa = t = \mu$, otherwise $= 0$, where the sums range over all elements $c \neq 0$, $d \neq 0$.

14. For 4 forms in 4 variables, we obtain two determinations of the characteristic invariant I for the class $x_1, x_2, x_3, 0$. As in (39),

$$I = E_{123} - D^{\mu} + (1 - V_{1234}^{\mu})(1 - V_{2134}^{\mu})(1 - V_{3124}^{\mu}) - 1, \tag{43}$$

where E_{123} is the right member of (40). Again, $I = A_4 E_{123}$. As in (37),

$$V_{1243}^{\mu} - V_{1234}^{\mu} V_{3124}^{\mu} = V_{123}^{\mu}(1 - A_4 - V_{124}^{\mu} - V_{214}^{\mu} + V_{124}^{\mu} V_{214}^{\mu}). \tag{44}$$

Hence $A_4 V_{123}^{\mu}$ is expressed linearly in terms of our system of invariants (§ 11). Interchanging subscripts 1, 2 or 2, 3, we get $A_4 V_{213}^{\mu}$, $A_4 V_{132}^{\mu}$.

Multiplying (44) by V^{μ}_{213} and applying

$$V_{213}\,V_{3124}=0, \qquad V^{\mu}_{213}\,V^{\mu}_{1243}=V^{\mu}_{1243}\,V^{\mu}_{2143}-V^{\mu}_{1234}\,V^{\mu}_{2134}\,V^{\mu}_{3124},$$

we obtain $A_4\,V^{\mu}_{123}\,V^{\mu}_{213}$ linearly in terms of the system. It remains to find $A_4\,V^{\mu}_{12}\,V^{\mu}_{13}$. Interchanging 3 and 4 in (37), we have

$$A_4\,V^{\mu}_{12}=V^{\mu}_{12}-V^{\mu}_{12}\,V^{\mu}_{14}+W, \qquad W\equiv V^{\mu}_{124}\,V^{\mu}_{214}-V^{\mu}_{142}.$$

To find $V^{\mu}_{13}W$, we note that $V^{\mu}_{13}W+V^{\mu}_{142}\,V^{\mu}_{143}$ vanishes for every class except that containing x_1, x_2, ax_1+bx_2, cx_1+dx_2; and for it has the value $c^{\mu}d^{\mu}\Delta^{\mu}$, where $\Delta=bc-ad$. But

$$P=V_{213}\,V_{124}-V_{123}\,V_{214}$$

vanishes except for the same class, and for it has the value Δ. Thus

$$V^{\mu}_{13}\,W=P^{\mu}V^{\mu}_{124}\,V^{\mu}_{214}-V^{\mu}_{142}\,V^{\mu}_{143}.$$

To P^{μ} we apply (5). By additions we obtain A_4E_{123} expressed linearly in the system. Comparing the result with (43), we obtain

$$\begin{aligned}(45)\quad D^{\mu}=&(1-A_1)(1-A_2)(1-A_3)(1-A_4)-3\,V^{\mu}_{1234}\,V^{\mu}_{2134}\,V^{\mu}_{3124}\\
&+2(V^{\mu}_{1234}\,V^{\mu}_{2134}+V^{\mu}_{1234}\,V^{\mu}_{3124}+V^{\mu}_{2134}\,V^{\mu}_{3124})+2\,V^{\mu}_{1243}\,V^{\mu}_{2143}-V^{\mu}_{1243}\\
&-V^{\mu}_{2143}-V^{\mu}_{1284}-V^{\mu}_{2184}-V^{\mu}_{3124}-V^{\mu}_{1342}-2\,V^{\mu}_{123}\,V^{\mu}_{213}\,V^{\mu}_{124}\,V^{\mu}_{214}\\
&-V^{\mu}_{12}\,V^{\mu}_{13}\,V^{\mu}_{14}-(V^{\mu}_{123}\,V^{\mu}_{124}+V^{\mu}_{123}\,V^{\mu}_{214}+V^{\mu}_{213}\,V^{\mu}_{124}+V^{\mu}_{213}\,V^{\mu}_{214})\\
&-(V^{\mu}_{132}\,V^{\mu}_{134}+V^{\mu}_{132}\,V^{\mu}_{314})-V^{\mu}_{142}\,V^{\mu}_{143}+V^{\mu}_{132}\,V^{\mu}_{134}\,V^{\mu}_{314}\\
&+2\,V^{\mu}_{122}\,V^{\mu}_{213}(V^{\mu}_{124}+V^{\mu}_{214})+2\,V^{\mu}_{124}\,V^{\mu}_{214}(V^{\mu}_{123}+V^{\mu}_{213})\\
&+\sum_{r=1}^{\mu}(V_{123}\,V_{214})^{r}(V_{213}\,V_{124})^{\mu-r},\end{aligned}$$

the terms in any parenthesis being related under the classification in § 9. The second member of (45) defines E_{1231} for $m>4$ variables.

15. In addition to the general method in § 8 of constructing the invariants V, a second method was employed in § 3 for the case of two forms. As the latter method, apart from details, is that commonly used in the algebraic theory, it will prove interesting to give the results obtained similarly for three forms. In (2) we replace a_{iv} by $a_{iv}-\kappa a_{jv}-\lambda a_{kv}$ and, in view of (3), express the result in the form

$$\Pi=A_i[1+(A_j-1)\kappa^{\mu}][1+(A_k-1)\lambda^{\mu}]-\sum_{t=1}^{\mu}V^{t}_{ij}\kappa^{t}-\sum_{t=1}^{\mu}V^{t}_{ik}\lambda^{t}+\sum_{r,s=1}^{\mu}T_{rs}\kappa^{r}\lambda^{s},$$

which, for $\lambda=0$, reduces to (4). We obtain the value of T_{rs} for each canonical set of the three forms (§ 13). Most of the cases may be treated

by inspection. But for the second type

$$\Pi = [1-(1-c\lambda)^\mu][1-(-\kappa-d\lambda)^\mu]$$
$$\equiv \Big[\sum_{t=1}^{\mu} c^t\lambda^t\Big]\Big[d^\mu\lambda^\mu - 1 + \sum_{r=1}^{\mu}(-1)^r\kappa^r(d\lambda)^{\mu-r}\Big] \pmod p,$$

by (5). For the fourth type

$$\Pi = 1-(1-f\kappa-g\lambda)^\mu \equiv -\sum_{l=1}^{\mu}(f\kappa+g\lambda)^l$$
$$= -\Sigma\binom{r+s}{r} f^r g^s \kappa^r\lambda^s \quad (r, s = 0, 1, \ldots, \mu;\ r+s = 1, \ldots, \mu).$$

We find that $T_{rs} = 0$ for types 1, 4, 7, 8; $(-1)^r c^{r+s} d^{\mu-r}$ for 2; e^r $(s = \mu)$, 0 $(s < \mu)$ for type 3; $-\binom{r+s}{r} f^r g^s$ $(r+s \leqslant \mu)$, 0 $(r+s > \mu)$ for 5; $(-1)^{s-1} h^s$ $(r+s = \mu$ or $r = s = \mu)$, otherwise 0 for type 6. Hence $T_{\mu 1} = V_{ijk}$, $T_{1\mu} = V_{ikj}$. Permuting the forms l_i and l_j, we see that the new function $T_{\mu 1}$ is V_{jik}. Conversely, each T_{rs} may easily be expressed in terms of the V's and A's. As a complete set of linearly independent invariants we may take

$$(46) \qquad T_{rs},\ V^r_{ij},\ V^r_{ik},\ V^r_{jk},\ V^r_{ij}V^s_{ik},\ A_iV^r_{jk},\ A_jV^r_{ik},\ A_kV^r_{ij},\ A_i^{\alpha_i}A_j^{\alpha_j}A_k^{\alpha_k}$$
$$(r, s = 1, \ldots, \mu;\ \alpha\text{'s} = 0, 1),$$

if $m > 3$; the same with unity deleted and D^r inserted, if $m = 3$. The only non-homogeneous linear relation between the invariants for $m = 3$ is

$$(47) \qquad D^\mu + T_{\mu\mu} + V^\mu_{jk} = (1-A_i)(1-A_j)(1-A_k).$$