FORMAL MODULAR INVARIANTS WITH APPLICATION TO BINARY MODULAR COVARIANTS*

BY

MILDRED SANDERSON

§ 1. *Introduction.*

Consider a system of forms $f_1(x_1, \cdots, x_m), \cdots, f_k(x_1, \cdots, x_m)$, whose coefficients $a_1, \cdots, a_r$ (arranged in a definite order) are independent variables. Let $b_1, \cdots, b_r$ be the coefficients (taken in the same order) of the forms derived from $f_1, \cdots, f_k$ by applying a given linear transformation T with integral coefficients. Let $F(a_1, \cdots, a_r)$ be a polynomial with integral coefficients and

$$D(a_1, \cdots, a_r) = F(b_1, \cdots, b_r) - F(a_1, \cdots, a_r)$$

be the polynomial in $a_1, \cdots, a_r$ with integral coefficients which is obtained from $F(b) - F(a)$ upon replacing $b_1, \cdots, b_r$ by their expressions in terms of $a_1, \cdots, a_r$ and the coefficients of T. In case two or more of the terms in the initial expression for D had the same literal part $a_1^{r_1} \cdots a_r^{r_r}$, such terms are assumed to have been combined additively into a single term. Let p be a prime. According to the definition by HURWITZ† (stated for a single form in two variables), $F(a_1, \cdots, a_r)$ is an invariant of $f_1, \cdots, f_k$ modulo p with respect to the transformation T if $D(a_1, \cdots, a_r) \equiv 0 \pmod{p}$, identically in $a_1, \cdots, a_r$, viz., if the coefficient of each term of D is divisible by p. He gave an interesting example of such an invariant with respect to all of the transformations T with integral coefficients whose determinant is not divisible by p, but did not construct a theory of invariants modulo p.

As a generalization we may employ transformations T with coefficients in the Galois field $GF[p^n]$ composed of the p^n elements

$$c_0 + c_1 j + c_2 j^2 + \cdots + c_{n-1} j^{n-1} \quad (c_0, \cdots, c_{n-1} = 0, 1, \cdots, p-1),$$

where j is a root of a congruence of degree n irreducible modulo p. A polynomial $F(a_1, \cdots, a_r)$ with integral coefficients is a *formal* invariant of $f_1, \cdots, f_k$, in the field, under transformation T if‡ $D(a_1, \cdots, a_r)$ is identi-

* Presented to the Society (Chicago), March 21, 1913, under different title.

† Archiv der Mathematik und Physik, ser. 3, vol. 5 (1903), p. 22.

‡ In the spirit of KRONECKER's use of polynomials in indeterminates $a_1, \cdots, a_r$ with coefficients in any domain of rationality, we use polynomials with coefficients in the $GF[p^n]$. Cf. J. KÖNIG, *Theorie der algebraischen Grössen*, Leipzig, 1903, p. 31; H. WEBER, Mathematische Annalen, vol. 43 (1893), p. 526.

cally zero in the field as to $a_1, \cdots, a_r$, i. e., if the coefficient of each term of D, when reduced to the form $c_0 + c_1 j + \cdots + c_{n-1} j^{n-1}$ by means of the congruence satisfied by j, has each c_i a multiple of p. If $F_0, F_1, \cdots$ are such formal invariants (with integral coefficients), then $F_0 + F_1 j + \cdots$ is a formal invariant. In this manner, or by direct extension of the previous definition, we have the concept of a formally invariant polynomial with coefficients in the $GF[p^n]$.

We pass to the entirely different concept of *modular* invariants, introduced by DICKSON.* The coefficients $a_1, \cdots, a_r$ of the forms are now undetermined elements of the $GF[p^n]$. A polynomial $F(a_1, \cdots, a_r)$ with coefficients in that field is called a modular invariant of the system of forms under any given group G of linear transformations with coefficients in the field if, for each transformation of G, $D(a_1, \cdots, a_r)$ is zero in the field. To apply this test we may first express† D as a polynomial $\delta(a_1, \cdots, a_r)$ in which the exponents are all less than p^n, and then require that δ shall be identically zero in the field as to $a_1, \cdots, a_r$. We thus see clearly just how the difference in the definitions of formal and modular invariants affects the actual computations. Dickson‡ has given a very simple and elegant theory of modular invariants. No theory has been developed for formal invariants. However, there exists between the two subjects an interesting and important relation, which I shall develop in what follows. I take this opportunity to express my gratitude to Professor Dickson for his interest and many helpful suggestions, in particular for the present formulation of this introductory section.

§ 2. *Statement and application of the fundamental theorem.*

To any modular invariant i of a system of forms under any group G of linear transformations with coefficients in the $GF[p^n]$, there corresponds a formal invariant I under G such that $I = i$ for all sets of values in the field of the coefficients of the system of forms.

This theorem enables us, as in the algebraic theory of invariants, to construct covariants of a system of binary forms in x and y from invariants of this system and an additional linear form whose coefficients are y and $-x$, if the invariants are made formally invariant with respect to x and y. Moreover, every invariant will yield a covariant. Some invariants will yield two or more independent covariants. For example,

$$f = a_0 x^2 + 2a_1 xy + a_2 y^2, \qquad a_0 x^4 + a_1 x^3 y + a_1 xy^3 + a_2 y^4$$

* These Transactions, vol. 8 (1907), p. 205.

† By use of Galois's generalization $a^{p^n} = a$ of Fermat's theorem.

‡ These Transactions, vol. 10 (1909), p. 123; American Journal of Mathematics, vol. 31 (1909), p. 337.

are two independent covariants modulo 3 of f, but as modular invariants of f and an additional linear form they are to be identified. The universal covariant

$$\begin{vmatrix} x & y \\ x^{p^n} & y^{p^n} \end{vmatrix},$$

on the other hand, could not be obtained as an invariant of a linear form, because it vanishes when x and y are in the $GF[p^n]$, as we suppose the coefficients of our forms to be. Whether or not all the covariants of a system of forms can be expressed as functions of this universal covariant and the invariants of this system and a linear form is a question as yet unanswered. In some special cases this has proved to be the case. In later sections will be shown a practical method for constructing covariants together with an illustration of the fact just mentioned. (See §§ 6, 7.)

In order to prove the above theorem, we shall first establish an interesting lemma.

§ 3. *Linear factors of a certain determinant D.*

Lemma. Let $a_1, \cdots, a_r$ $(r > 1)$ *be arbitrary variables, and* $g_1, \cdots, g_r$ *given elements of the* $GF[p^n]$, $g_r \neq 0$. *Then the determinant*

$$N = \begin{vmatrix} a_1, & \cdots, & a_r \\ a_1^{p^n}, & \cdots, & a_r^{p^n} \\ \cdots & \cdots & \cdots \\ a_1^{p^{(r-1)n}}, & \cdots, & a_r^{p^{(r-1)n}} \end{vmatrix} \tag{1}$$

is divisible in the field by the determinant

$$D = \begin{vmatrix} a_1, & \cdots, & a_r \\ a_1^{p^n}, & \cdots, & a_r^{p^n} \\ \cdots & \cdots & \cdots \\ a_1^{p^{(r-2)n}}, & \cdots, & a_r^{p^{(r-2)n}} \\ g_1, & \cdots, & g_r \end{vmatrix} \tag{2}$$

and the quotient $Q = N/D$ *has the properties*

$$\begin{aligned} &Q \neq 0 \quad \text{if} \quad a_1 = g_1, \cdots, a_r = g_r, \\ &Q = 0 \quad \text{if} \quad a_1 = e_1, \cdots, a_r = e_r, \end{aligned} \tag{3}$$

where $e_1, \cdots, e_r$ *are elements of the field not proportional to* $g_1, \cdots, g_r$.

We know that N is an invariant and is equal to the following product:*

$$N = \prod_{k=1}^{r} \prod_{b} (a_k + b_{k+1} a_{k+1} + \cdots + b_r a_r), \tag{4}$$

where the second product extends over the $p^{(r-k)n}$ sets $b_{k+1}, \cdots, b_r$ obtained when each b ranges independently over the elements of the $GF[p^n]$.

Let us consider the determinant D. We can see at once that it is divisible by

$$a_1 - \frac{g_1}{g_r} a_r, \tag{5}$$

since this divides all the two-rowed minors formed from the first and rth columns. If we transform the variables by setting

$$a_1 = A_1 + \sum_{j=2}^{r} k_j A_j, \qquad a_j = A_j, \qquad (j = 2, \cdots, r), \tag{6}$$

and subtract from the elements of the first column of D the products of the elements of the jth column ($j = 2, \cdots, r$) by k_j, we may write D in the form

$$D = \begin{vmatrix} A_1, & A_2, & \cdots, & A_r \\ \cdots & \cdots & \cdots & \cdots \\ A_1^{p^{(r-2)n}}, & A_2^{p^{(r-2)n}}, & \cdots, & A_r^{p^{(r-2)n}} \\ g_1 - \sum_{j=2}^{r} k_j g_j, & g_2, & \cdots, & g_r \end{vmatrix}. \tag{7}$$

Thus D will be invariant under all transformations (6) for which

$$\sum_{j=2}^{r} k_j g_j = 0. \tag{8}$$

Since $g_r \neq 0$, the first $r-2$ k's may be chosen arbitrarily, hence in $p^{(r-2)n}$ ways, and k_r will be uniquely determined. If we transform (5) by all the transformations (6) which satisfy (8) we get $p^{(r-2)n}$ different linear factors, which upon replacing the A_i by the a_i are

$$a_1 + \sum_{j=2}^{r} k_j a_j - \frac{g_1}{g_r} a_r. \tag{9}$$

These must divide D since D was invariant under all such transformations. From (8) we see easily that all of these linear factors vanish for $a_1 = g_1, \cdots, a_r = g_r$.

Since D is also divisible by

$$a_2 - \frac{g_2}{g_r} a_r, \qquad \cdots, \qquad a_{r-1} - \frac{g_{r-1}}{g_r} a_r, \tag{10}$$

* L. E. Dickson, these Transactions, vol. 12 (1911), p. 76, and references there given.

by using transformations similar to (6), namely,

$$(11)\quad \begin{cases} a_1 = A_1, \quad a_2 = A_2 + \sum_{j=3}^{r} k_j A_j, \quad a_j = A_j \quad (j = 3, \cdots, r), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_j = A_j \ (j = 1, \cdots, r-2), \quad a_{r-1} = A_{r-1} + k_r A_r, \quad a_r = A_r, \end{cases}$$

we find that D is divisible by respectively

$$p^{(r-3)n}, \quad \cdots, \quad p^n, \quad 1$$

new linear factors all of which vanish for $a_1 = g_1, \cdots, a_r = g_r$. These

$$p^{(r-2)n} + p^{(r-3)n} + \cdots + p^n + 1 = w$$

factors are all distinct. Hence D is divisible by their product. But w is exactly the degree of D, so that, apart from the factor $\pm g_r$, D is equal to this product. It may be written

$$(12)\qquad D = \pm g_r \prod_{k=1}^{r} \prod_{[b]} (a_k + b_{k+1} a_{k+1} + \cdots + b_r a_r),$$

where the second product extends over all values of the b_j in the $GF[p^n]$ such that the linear form vanishes for $a_1 = g_1, \cdots, a_r = g_r$.

Since all these factors are contained in N, Q is integral. Now D contains all linear forms with unity for the coefficient of the a_j of lowest subscript, which vanish for $a_i = g_i$ $(i = 1, \cdots, r)$. Hence, none of the factors of Q vanish for $a_i = g_i$, so that $Q \neq 0$ for $a_1 = g_1, \cdots, a_r = g_r$.

Some of the factors of the quotient must vanish for $a_1 = e_1, \cdots, a_r = e_r$, where $e_1, \cdots, e_r$ are not proportional to $g_1, \cdots, g_r$. For, there are w factors of N which do vanish, and unless these are the same as the factors of D, Q must vanish. But $r - 1$ of the factors of D, namely,

$$a_1 - \frac{g_1}{g_r} a_r, \qquad a_2 - \frac{g_2}{g_r} a_r, \qquad \cdots, \qquad a_{r-1} - \frac{g_{r-1}}{g_r} a_r,$$

are linearly independent, and hence when equated to zero uniquely determine the ratios of the a's for which D vanishes. Therefore, if Q does not vanish for $a_1 = e_1, \cdots, a_r = e_r$, then $e_1, \cdots, e_r$ must be proportional to $g_1, \cdots, g_r$.

§ 4. *Definition of the classes* C_{ij}.

Consider a system S of forms $f_1, \cdots, f_t$ in m variables with coefficients $a_1, \cdots, a_r$. Following the method of Professor L. E. Dickson,* we shall give the coefficients of S special values in the $GF[p^n]$, and divide the resulting

*These Transactions, vol. 10 (1909), p. 123; American Journal of Mathematics, vol. 31 (1909), p. 337.

set of systems into classes C_i, such that S' and S'' shall belong to the same class if and only if they are equivalent under G. If S' is a particular system of forms $f_1', \cdots, f_t'$, and if k is a constant, we shall say that the system of forms $kf_1', \cdots, kf_t'$ is a multiple of S', and we shall denote it by kS'. Let c_i be a subset of C_i such that if s is in c_i no multiple of s is in c_i, and such that every system S in C_i is a multiple of some system in c_i. Let ρ be a primitive root in the $GF[p^n]$. Suppose e_i to be the smallest exponent for which s' and $\rho^{e_i} s'$ are equivalent under G, where s' is any system in c_i. Then e_i is a factor of $p^n - 1$ and

$$s', \quad \rho^{e_i} s', \quad \cdots, \quad \rho^{(d_i-1)e_i} s' \qquad (d_i e_i = p^n - 1) \tag{13}$$

are all contained in C_i. If S'' is a system in C_i not in set (13), $\rho^{e_i} S''$ will be in C_i. For, S'' may be transformed into s', s' into $\rho^{e_i} s'$, $\rho^{e_i} s'$ into $\rho^{e_i} S''$. Moreover any system S''' in C_i is equal to ρ^{ke_i} times a system s''' in c_i. For we may write

$$S''' = \rho^{ke_i+l} s''' \qquad (0 \leqq l < e_i).$$

Since $\rho^{p^n-1-ke_i} S'''$ is in C_i, $\rho^l s'''$ is in C_i. But e_i is the smallest exponent for which this is possible. Hence $l = 0$. Therefore we may write

$$C_i = \sum_{k=1}^{d_i} c_i \rho^{ke_i},$$

where Σ denotes an aggregate, and $c_i \rho^{ke_i}$ is the set of systems obtained by multiplying each system in c_i by ρ^{ke_i}. If $e_i = 1$, C_i will contain all the multiples of the systems in c_i. In general there are e_i different classes

$$C_{il} = \sum_{k=1}^{d_i} c_i \rho^{ke_i+l} \qquad (l = 0, \cdots, e_i - 1) \tag{14}$$

formed on the subsets c_i, $c_i\rho$, $\cdots$, $c_i \rho^{e_i-1}$ respectively. Thus a complete list of the classes is given by (14), where $i = 1, \cdots, q$, and C_{00} which contains only the identically zero system.

§ 5. *Characteristic invariants.*

All invariants of the system S of forms can be expressed in terms of characteristic invariants* i_{kl} which have the value one for systems of the class C_{kl} and the value zero for systems in the remaining classes. To prove the theorem of § 2, it suffices to construct formal invariants I_{kl} which reduce for values of the coefficients in the $GF[p^n]$ to the characteristic invariants i_{kl}. For the construction of the I_{kl} it is convenient to employ the invariants

$$J_i = \sum_{g_1, \cdots, g_r}^{c_i} [Q(g_1, \cdots, g_r)]^{d_i} \qquad (i = 1, \cdots, q), \tag{15}$$

* L. E. Dickson, l. c. (preceding foot-note).

where the sum extends over the different sets of coefficients in c_i. When the variables are transformed under G, the coefficients $a_1, \cdots, a_r$ undergo an induced transformation which is also linear with coefficients in the $GF[p^n]$. J_i is a formal invariant since the numerators are invariant apart from a factor which is the d_ith power of the determinant of the induced transformation, and the denominators are permuted among themselves apart from the same factor.

Consider any particular denominator

$$(16) \qquad \begin{vmatrix} a_1, & \cdots, & a_r \\ \cdot & \cdots & \cdot \\ a_1^{p^{(r-2)n}}, & \cdots, & a_r^{p^{(r-2)n}} \\ g_1', & \cdots, & g_r' \end{vmatrix}^{d_i}.$$

Since $g_1', \cdots, g_r'$ are the coefficients of a system of c_i, this system is also in C_{i0}. After transformation this will become

$$(17) \qquad \begin{vmatrix} \sum_{j=1}^{r} c_{1j} A_j & \cdots, & \sum_{j=1}^{r} c_{rj} A_j \\ \cdot & \cdots & \cdot \\ \Sigma c_{1j} A_j^{p^{(r-2)n}}, & \cdots, & \Sigma c_{rj} A_j^{p^{(r-2)n}} \\ \Sigma c_{1j} G_j, & \cdots, & \Sigma c_{rj} G_j \end{vmatrix}^{d_i},$$

where $G_1, \cdots, G_r$ are also the coefficients of a system in C_{i0} and hence may be written $\rho^{le_i} g_1'', \cdots, \rho^{le_i} g_r''$, where $g_1'', \cdots, g_r''$ are the coefficients of a system in c_i. Hence (17) becomes

$$(18) \qquad \rho^{le_i d_i} \mid c_{tj} \mid^{d_i} \begin{vmatrix} A_1, & \cdots, & A_r \\ \cdot & \cdots & \cdot \\ A_1^{p^{(r-2)n}}, & \cdots, & A_r^{p^{(r-2)n}} \\ g_1'', & \cdots, & g_r'' \end{vmatrix}^{d_i}.$$

Since $\rho^{le_i d_i} = 1$, this denominator apart from the factor $\mid c_{tj} \mid^{d_i}$ occurs among the denominators in the sum (15), and the factor $\mid c_{tj} \mid^{d_i}$ is canceled by the same factor which is brought into the numerator by the transformation. Hence J_i is a formal invariant.

Let $J_i(C_{jk})$ denote the value which J_i has for systems of the class C_{jk}. Obviously $J_i(C_{00}) = 0$. In view of (15) and (3),

$$(19) \qquad J_i(C_{kl}) = 0 \quad (k \neq i), \; J_i(C_{il}) \neq 0.$$

Since $J_i(C_{i0}) \neq 0$, we may set

$$J_i(C_{i0}) = \rho^l. \tag{20}$$

We can easily see that

$$J_i(C_{ik}) = \rho^{l+kd_i} \qquad (k = 0, 1, \cdots, e_i - 1). \tag{21}$$

By making use of the fact that any invariant I may be written in the form*

$$I = \sum_{jk} v_{jk} I_{jk},$$

where v_{jk} is the value which I has for systems in the class C_{jk}, we obtain the following equations for the determination of the I_{ik}:

$$J_i^g = \sum_{k=0}^{e_i-1} \rho^{g(l+kd_i)} I_{ik} \qquad (g = 1, \cdots, e_i). \tag{22}$$

The determinant of the coefficients is

$$\left| \rho^{g(l+kd_i)} \right| = \rho^{l(1+2+\cdots+e_i)} \left| (\rho^{d_i})^{gk} \right| \quad (k = 0, \cdots, e_i - 1;\ g = 1, \cdots, e_i). \tag{23}$$

This is not zero since it is equal to the product of differences of distinct powers of ρ. Hence we can solve (22) uniquely for the I_{ik}.

The characteristic invariant for the class C_{00} is

$$I_{00} = 1 - \sum_{g_1, \cdots g_r}^{c} [Q(g_1, \cdots, g_r)]^{p^n - 1} \tag{24}$$

where c is the set of all subsets c_i.

§ 6. *Construction of binary covariants.*

Let us consider the covariants of a form f of the mth degree with coefficients in the $GF[p^n]$ under the group of all binary linear transformations with coefficients in the $GF[p^n]$. We may assume that it has been broken up into m linear factors whose coefficients are in a Galois Field of order $p^{m!n}$ or lower. We shall write it

$$f = \prod_{j=1}^{m} (\alpha_1^{(j)} x_1 + \alpha_2^{(j)} x_2) = \prod_{j=1}^{m} \alpha_x^{(j)} = \prod_{j=1}^{m} x_{a(j)}. \tag{25}$$

When the variables are transformed, the coefficients of each linear form are transformed contragrediently to the variables. Any function F of the α's and the x's which is invariant and which is unchanged when the superscripts on any two sets of α's are interchanged will be a covariant of the form f. If we call any two of the linear factors of f α_x and β_x, F may obviously contain

* L. E. Dickson, l. c.

functions of the type

$$\alpha_x, \quad \alpha_x{}^{p^n} = \alpha_1 x_1^{p^n} + \alpha_2 x_2^{p^n}, \quad x_a{}^{p^n},$$

$$(26) \qquad \begin{vmatrix} \alpha_1^{p^n} & \alpha_2^{p^n} \\ \alpha_1^{p^{kn}} & \alpha_2^{p^{kn}} \end{vmatrix} = (\alpha^{p^n} \quad \alpha^{p^{kn}}),$$

$$\begin{vmatrix} \alpha_1^{p^n} & \alpha_2^{p^n} \\ \beta_1^{p^{kn}} & \beta_2^{p^{kn}} \end{vmatrix} = (\alpha^{p^n} \quad \beta^{p^{kn}}),$$

$$\begin{vmatrix} x_1^{p^n} & x_2^{p^n} \\ x_1^{p^{kn}} & x_2^{p^{kn}} \end{vmatrix} = (x^{p^n} \quad x^{p^{kn}}).$$

It is not necessary that F should be integral in these functions, but if the covariant is to be integral, F must be integral in the α's and x's.

§ 7. *The covariants of a binary quadratic form in the* $GF[p^n]$ $(p > 2)$.

Consider the form

$$(27) \qquad f = ax_1^2 + 2bx_1 x_2 + cx_2^2 = \alpha_x \beta_x$$

with coefficients in the $GF[p^n]$. We wish to find the covariants of this form under the group of all binary linear transformations with coefficients in the $GF[p^n]$. The coefficient of the highest power of x_1 is a seminvariant, that is, it is invariant under all the transformations of the type

$$(28) \qquad x_1 = x_1' + \lambda x_2', \qquad x_2 = x_2'.$$

We shall first find the seminvariants of the form, and then construct covariants from these.

Under the group of transformations (28), the forms f are seen to belong to one of the following classes:

$$(29) \qquad C_{\rho^i, d}, \qquad C_{\rho^i}, \qquad {}_{\rho^i}C, \qquad C_0 \qquad (d = 0, \rho, \rho^2, \cdots, \rho^{p^n-1};\ i = 1, \cdots, p^n - 1),$$

where ρ is a primitive root in the $GF[p^n]$. The canonical forms are respectively:

$$(30) \qquad \rho^i (x_1^2 + dx_2^2), \qquad \rho^i x_1 x_2, \qquad \rho^i x_2^2, \qquad 0.$$

The classes are completely characterized by the seminvariants

$$(31) \qquad \begin{aligned} D &= \tfrac{1}{4}(\alpha\beta)^2 = b^2 - ac, \\ a &= \alpha_1 \beta_1, \\ R &= (\alpha_1^{p^n-1} \alpha_2 - \alpha_2^{p^n})(\beta_1^{p^n-1} \beta_2 - \beta_2^{p^n}), \\ B &= \tfrac{1}{2} \sum_2 (\alpha^{p^n} \beta) \beta_1^{p^n-1} = a^{p^n-1} b - b^{p^n}, \end{aligned}$$

as is seen by the accompanying table which gives the value that each seminvariant has for the respective classes. They also form a fundamental set.

(32)

	$C_{\rho^i, d}$	C_{ρ^i}	${}_{\rho^i}C$	C_0
D	$-\rho^{2i} d$	$\rho^{2i}/4$	0	0
a	ρ^i	0	0	0
R	$(-d$ square$)$ 0 $(-d$ not square$)$ $4\rho^i d$ $(-d$ zero$)$ 0	0	ρ^i	0
B	0	$-\rho^i/2$	0	0

All seminvariants must then be functions of these. However, there are some others which have very simple expressions, but which as functions of these four might be very complicated. They are

$$B_j = \tfrac{1}{2} \sum_2 (\alpha^{p^n} \beta)^j \beta_1^{j(p^n-1)},$$

(33)
$$S = \sum_2 \alpha_1^{2\tau p^n} \frac{(\beta\beta^{p^{2n}})}{(\beta\beta^{p^n})} \qquad \left(\tau = \frac{p^n - 1}{2}\right),$$

$$q = (a^\tau + c^\tau) \sum_{i=0}^{\tau} a^i c^i b^{2\tau-2i} - a^{3\tau} - c^{3\tau}.$$

The only invariants among these are D and q, and these form a fundamental system of invariants.*

By comparing the values which the different seminvariants have for the different classes according to tables (32) and

(34)

	$C_{\rho^i, d}$	C_{ρ^i}	${}_{\rho^i}C$	C_0
q	$(-1)^i [d^{2\tau} - 1]$	0	$(-1)^{i+1}$	0
B_j	$\binom{j \text{ even}}{-d \text{ square}} 2^j \rho^{ji} (-d)^{\frac{j}{2}}$ (otherwise) 0	$\frac{1}{2}(-1)^j \rho^{ji}$	0	0
S	$(-d$ square$)$ 2 $(-d$ not square$)$ 0 $(-d$ zero$)$ 2	1	0	0

we find various syzygies, among which are

(35)
$$D^\tau + a^{2\tau} = S + a^\tau q,$$

(36)
$$q = R^\tau a^{2\tau} + D^{2\tau} S^{2\tau} a^\tau - S^{2\tau} a^\tau - R^\tau.$$

*L. E. Dickson, American Journal of Mathematics, vol. 31 (1909) p. 109; these Transactions, vol. 10 (1909), p. 132.

Covariants are formed very easily from the seminvariants a, $B = B_1$, B_j, S and powers of these by replacing α_1 and β_1 by α_x and β_x or $\alpha_{x^{p^n}}$ and $\beta_{x^{p^n}}$, and by replacing $\alpha_1^{p^n}$ and $\beta_1^{p^n}$ by $x_{a^{p^n}}$ and $x_{\beta^{p^n}}$, wherever the α_1 and β_1 do not occur in one of the invariant determinants.

Thus with a as a leader we get the two distinct covariants:

$$f = \alpha_x \beta_x, \qquad f_1 = \tfrac{1}{2} \sum_2 \alpha_{x^{p^n}} \beta_x. \tag{37}$$

Covariants led by B_j, where $j < p^n$, are

$$\tfrac{1}{2} \sum_2 (\alpha^{p^n} \beta)^j \beta_x^{j(p^n-1)}, \qquad \tfrac{1}{2} \sum_2 (\alpha^{p^n} \beta)^j x_{\beta^{p^n}} \beta_x^{(j-1)p^n - j}, \tag{38}$$

$$\cdots\cdots, \qquad \tfrac{1}{2} \sum_2 (\alpha^{p^n} \beta)^j x_{\beta^{p^n}}^{j-1} \beta_x^{p^n - j}.$$

The seminvariant S will lead the covariants:

$$\sum_2 x_{a^{p^n}}^k \alpha_x^{(2\tau - k)p^n} \frac{(\beta\beta^{p^{2n}})}{(\beta\beta^{p^n})} \qquad (k = 0, 1, \cdots, p^n - 1). \tag{39}$$

A simple method has not yet been found for constructing covariants with a leading coefficient R.

In addition to those already mentioned, should be noted the universal covariants*

$$L = (xx^{p^n}), \qquad Q = \frac{(xx^{p^{2n}})}{(xx^{p^n})}. \tag{40}$$

For the general Galois Field of order p^n, a complete system of covariants of the binary quadratic form has not yet been found. For the case $p^n = 3$ Professor L. E. DICKSON† has found the complete system, but not their expressions in terms of the present symbols. The fundamental covariants are included among those mentioned above. They are

$$\begin{aligned} D &= (\alpha\beta)^2 = b^2 - ac, \\ q &= \frac{(\alpha^3\beta)^2 (\alpha\beta)(\alpha\alpha^3) - (\alpha\beta^3)(\alpha\alpha^9)}{(\alpha\alpha^3)^2} \\ &= ac^2 + a^2 c + b^2 c + b^2 a - a^3 - c^3, \qquad (41) \\ f &= \alpha_x \beta_x, \\ f_1 &= \tfrac{1}{2} \sum_2 \alpha_{x^3} \beta_x = a x_1^4 + b x_1^3 x_2 + b x_1 x_2^3 + c x_2^4, \\ L &= (xx^3), \end{aligned}$$

* L. E. DICKSON, these Transactions, vol. 12 (1911), p. 1, p. 75.

† These Transactions, vol. 14 (1913), pp. 306–310.

$$Q = \frac{(xx^9)}{(xx^3)} = x_1^6 + x_1^4 x_2^2 + x_1^2 x_2^4 + x_2^6,$$

$$C_1 = \tfrac{1}{2} \sum_2 (\alpha^3 \beta)\, \beta_x^2$$

$$= (a^2 b - b^3)\, x_1^2 + 2\,(ac^2 - a^2 c + b^2 c - b^2 a)\, x_1 x_2 + (b^3 - bc^2)\, x_2^2, \tag{41}$$

$$C_2 = \sum_2 \frac{(\alpha\alpha^9)}{(\alpha\alpha^3)} x_{\beta^3}^2 + \alpha_x \beta_x q$$

$$= (D + a^2)\, x_1^2 - 2\,(ab + bc)\, x_1 x_2 + (D + c^2)\, x_2^2.$$

It should be noticed that no covariant led by R occurs in this set. In this case it is expressible in terms of the others. In this case D, a, B, and q completely characterize the classes (24), but, for $p^n > 3$, q cannot be substituted for R in characterizing the classes.

The covariant C_2 is an interesting one because of the fact that the covariants of lowest order led by D and a^2 alone are respectively

$$DQ, \qquad f^2, \tag{42}$$

which are of order six and four respectively. One might expect that $D + a^2$ would lead no covariant of order less than twelve. One of this order is

$$DQ^2 + f^6. \tag{43}$$