A THEOREM ON MODULAR COVARIANTS*

BY

OLIVE C. HAZLETT

INTRODUCTION

1. Statement of the problem. This paper answers a question which was raised over five years ago, but which has not been answered so far as I know. Miss Sanderson's theorem† on the relation between formal and modular invariants for the Galois Field $GF[p^n]$ of order p^n enabled her to construct covariants of a system S of binary forms in x and y from invariants of this system S and an additional linear form. This is closely analogous to the situation in the theory of algebraic invariants. In the latter theory the converse also is known to be true—that is, we can form all covariants in this manner. In the case of modular invariants, however, we do not obtain all covariants in this way, for the universal covariant $L = x^{p^n}y - xy^{p^n}$ can not be obtained as a modular invariant of a linear form, since it vanishes whenever x and y are in the field $GF[p^n]$, as we suppose the coefficients of our forms to be. In the paper referred to above, Miss Sanderson raised the question as to whether all covariants of a system S can be expressed as polynomials in L and the modular invariants of the system S enlarged by a linear form. The present paper answers this question in the affirmative.

2. Relation to the literature; definitions. Formal invariants of a form under a group G of linear transformations modulo p, a prime, were first considered by Hurwitz.‡ A few years later, Dickson§ introduced the notion of modular invariants of a form or system of forms.

Consider a system of forms $f_1(x_1, \cdots, x_m), \cdots, f_k(x_1, \cdots, x_m)$, and the group G of linear transformations where the coefficients of the transformations are marks of the $GF[p^n]$. A function of the coefficients of the forms having the invariantive property under this group is called a *formal invariant* if the coefficients of the forms are independent variables. If, on the other hand,

* Presented to the Society, Dec. 28, 1918.

† *Formal modular invariants with an application to binary modular covariants*, these Transactions, vol. 14 (1913), pp. 489–500.

‡ *Ueber höhere Kongruenzen*, Archiv der Mathematik und Physik, ser. 3, vol. 5 (1903), pp. 17–27.

§ *Invariants of binary forms under modular transformations*, these Transactions, vol. 8 (1907), pp. 205–232.

the coefficients of the forms are indeterminates in the $GF[p^n]$, such a function having the invariantive property is called a *modular invariant.* Every formal invariant is a modular invariant, but not every modular invariant is formally invariant. For, if a is any particular coefficient, $a^{p^n} \equiv a$ in the field and thus $a^{p^n} - a$ is a modular invariant, but not a formal invariant. In a formal invariant, we can not replace a^{p^n} by a where a is a coefficient of one of the original forms.

Similarly, we distinguish between formal covariants and modular covariants according as the coefficients of the forms of S are independent variables or indeterminates in the field.

Dickson* has developed a simple and elegant theory of modular invariants. In this paper he proved the finiteness of modular invariants and later† the finiteness of modular covariants. But thus far no theory of formal invariants has been brought forth, though several writers (chiefly Dickson and Glenn) have found fundamental sets of covariants for special cases.

There is, however, an intimate relation between the modular invariants of a system S of forms and the formal (modular) invariants. This is given in Miss Sanderson's theorem mentioned in Article 1, namely, 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 $I \equiv i$ for all sets of values in the field of the coefficients of the system of forms.

This theorem enabled her, as in the classical theory of algebraic invariants, to construct covariants of a system S of binary forms in x and y from invariants of the enlarged system S', where S' consists of the forms of S in the variables ξ and η, and an additional linear form whose coefficients are y and $-x$. As Miss Sanderson‡ points out in her thesis, the universal covariant $L = x^{p^n} y - xy^{p^n}$ can not be obtained as a modular invariant of a linear form, since it vanishes whenever x and y are marks of the $GF[p^n]$, as we suppose the coefficients of our forms to be. She then says, "Whether or not all the (modular) covariants of a system of forms can be expressed as functions of this universal covariant and the (modular) invariants of this system and a linear form is a question as yet unanswered."

While reading Miss Sanderson's paper recently, a method of proof of this

* *General theory of modular invariants,* these Transactions, vol. 10 (1909), pp. 123–158.

† *Proof of the finiteness of modular covariants,* these Transactions, vol. 14 (1913), pp. 299–310.

‡ Dickson, *On invariants and the theory of numbers, Madison Colloquium,* pp. 41–53; *Invariants in the theory of numbers,* these Transactions, vol. 1 (1914), pp. 497–503. Glenn, *Formal modular invariant theory of binary quantics,* ibid., vol. 17 (1916), pp. 545–556; *A fundamental system of formal covariants modulo 2 of the binary cubic,* ibid., vol. 19 (1918), pp. 109–118.

theorem occurred to the writer, and then a proof of a generalization to the case of a system of forms in several cogredient binary variables.

The chief interest of this theorem seems to be in the light it throws on the very difficult and, thus far, unsolved problem of formal covariants, since the theory of modular covariants is a stepping stone from the theory of modular invariants to the theory of formal covariants. For a modular invariant is an invariantive function of certain quantities which are all marks of the field; while a modular covariant is an invariantive function of certain sets of quantities all of which are in the field except one pair (i.e., the variables x and y); finally a formal covariant is an invariantive function of certain quantities of which all are independent variables. The present paper shows the relation between the theory of modular invariants and the theory of modular covariants; it shows a way of basing the theory of modular covariants on the theory of modular invariants, and thus may serve to suggest a way of basing the theory of formal covariants on the theory of modular covariants and hence in turn on the theory of modular invariants.*

FUNDAMENTAL THEOREM

3. Preliminary lemma. Consider a system S of binary forms in the variables x and y with the coefficients $a_0, a_1, \cdots, b_0, b_1, \cdots, c_0, c_1, \cdots$. There is one and only one modular invariant which is of degree $\leqq p^n - 1$ in each of the coefficients and which assumes the set of values v_i as the a's, b's, $\cdots$ range over all sets of values $a_0^{(i)}, a_1^{(i)}, \cdots, b_0^{(i)}, b_1^{(i)}, \cdots, c_0^{(i)}, c_1^{(i)}, \cdots$ in the field.† Dickson proves this theorem by applying his general theorem on interpolation in a finite field,‡ viz., within the $GF[p^n]$, there exists one and but one polynomial $\phi(x_1, \cdots, x_k)$ which has each exponent $\leqq p^n - 1$ and which takes prescribed values $v_{x_1, \cdots, x_k}$ for every set of elements $x_1, \cdots, x_k$ in the field.

We may also prove the

LEMMA. *If I is a modular invariant of the system S of forms and the linear form $\eta x - \xi y$, then we can make I formally invariant as to ξ and η.*

This lemma is a special case of Miss Sanderson's fundamental theorem already referred to, but her theorem does not furnish a simple formula for constructing an invariant C which is congruent to I and which is formally invariant as to ξ and η.

Let $\phi(a, b, c, \cdots; \xi, \eta) = I$ be a modular invariant of weight w. There is no loss of generality in assuming that ϕ is pseudo-homogeneous in ξ and η of degree d. (We shall say that a function f is pseudo-homogeneous of

* In this connection see Dickson, *Madison Colloquium*, pp. 57–58.

† Dickson, these Transactions, vol. 10, p. 125.

‡ Loc. cit., p. 124.

degree d if, when ξ and η are multiplied by ρ, any non-zero mark of the field, the function f is multiplied by ρ^d; that is, the degrees of the different terms of f differ by integral multiples of $p^n - 1$.) For, if ϕ is not pseudo-homogeneous in ξ and η, it is the sum of a finite number of modular invariants which are pseudo-homogeneous in ξ and η.

First, we construct a function C which is homogeneous in the independent variables ξ and η, and such that $C \equiv I$ whenever ξ and η are in the field. Take

$$C = \sum\left[\phi(a, b, c, \cdots; \kappa, \lambda)\frac{\prod'(\nu\xi - \mu\eta)^d}{\prod'(\nu\kappa - \mu\lambda)^d}\right].$$

Here $\sum$ indicates the sum of all terms of the type indicated, as κ, λ range over the pairs $(-1, 0)$, $(0, 1)$, $(\beta, 1)$, $\cdots$, $(\beta^k, 1)$, $\cdots$ where β is a primitive root of the $GF[p^n]$. Call these the pairs of the set σ. Inside the bracket, Π' indicates the product of all terms of the type indicated, as μ, ν range over all pairs of the set σ except the pair κ, λ occurring in the coefficient $\phi(a, b, c, \cdots; \kappa, \lambda)$ in that bracket. Notice that there are p^n distinct factors in each Π'.

Now, when ξ and η are in the field, they are of the form κ, λ or $\rho\kappa, \rho\lambda$ where κ, λ is a pair of the set σ. In the first case, we evidently have $C \equiv I$; and similarly in the second case, since ϕ is pseudo-homogeneous in ξ and η of degree d.

Next, we wish to show that C is formally invariant as to ξ and η under transformations of the group G. It will be sufficient to prove this for the generators of the group.

The transformation

$$T_\alpha \qquad \begin{aligned} \xi' &= \xi + \alpha\eta, \\ \eta' &= \eta, \end{aligned}$$

of determinant unity, carries $(\xi, \eta) = (-1, 0)$ into itself and interchanges the other pairs of the set σ, and hence interchanges the factors $\nu\xi - \mu\eta$. Also $\phi(a', b', c', \cdots; \kappa', \lambda') = \phi(a, b, c, \cdots; \kappa, \lambda)$, where (κ', λ') is in the set σ if (κ, λ) is, and conversely. Hence C is formally invariant as to ξ and η under T_α.

Under the transformation

$$T \qquad \begin{aligned} \xi' &= -\eta, \\ \eta' &= \xi, \end{aligned}$$

of determinant unity, the pairs of the set σ and the factors $\nu\xi - \mu\eta$ are transformed as follows:—the new $(-1, 0)$ is the old $(0, 1)$, the new $(0, 1)$ is the old $(1, 0)$ and the new $(\beta^k, 1)$ is the old $(1, -\beta^k)$; while $\eta' = \xi$, $\xi' = -\eta$ and $\xi' - \beta^k\eta' = -\beta^k[\xi - (-\beta^{k(p^n-2)})\eta]$. Hence any one of

the pairs of the set σ, say (κ', λ'), is equal to $(A\kappa, A\lambda)$, where (κ, λ) is a pair of the set σ. Also, the corresponding product $\Pi'(\nu'\xi' - \mu'\eta')$ is equal to $\Pi'(\nu\xi - \mu\eta)$ multiplied by ± 1 times a power of β. Call this multiplier B. Hence $\Pi'(\nu'\kappa' - \mu'\lambda') = AB\Pi'(\nu\kappa - \mu\lambda)$. But

$$\phi(a', b', c', \cdots; \kappa', \lambda') = \phi(a, b, c, \cdots; A\kappa, A\lambda) \equiv A^d \phi(a, b, c, \cdots; \kappa, \lambda).$$

Therefore, under the transformation T,

$$\phi(a', b', c', \cdots; \kappa', \lambda') \frac{\Pi'(\nu'\xi' - \mu'\eta')^d}{\Pi'(\nu'\kappa' - \mu'\lambda')^d} \equiv \phi(a, b, c, \cdots; \kappa, \lambda) \frac{\Pi'(\nu\xi - \mu\eta)^d}{\Pi'(\nu\kappa - \mu\lambda)^d}$$

where ξ and η are independent variables.

Similarly, it may be proved that, under the transformation

$$T'_\gamma \qquad \begin{aligned} \xi' &= \gamma\xi, \\ \eta' &= \eta \end{aligned} \qquad (\gamma \neq 0 \text{ in the field}),$$

C is formally invariant as to ξ and η.

Since the transformations T_α, T, and T'_γ generate the group G, we see that C is a modular invariant of the system which is formally invariant as to ξ and η.

4. Fundamental theorem for a pair of binary variables. Let $K(a, b, c, \cdots; x, y)$ be a modular covariant of the system S of binary forms which is homogeneous of degree d in x and y. Let the original coefficients be $a_0, a_1, \cdots, b_0, b_1, \cdots, c_0, c_1, \cdots$. When we subject the variables x, y to the non-singular linear transformation with coefficients in the $GF[p^n]$,

$$(4) \qquad \begin{aligned} x &= \alpha X + \beta Y, \\ y &= \gamma X + \delta Y, \end{aligned} \qquad \Delta = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \neq 0,$$

let the coefficients of the transformed forms be respectively $A_0, A_1, \cdots, B_0, B_1, \cdots, C_0, C_1, \cdots$. Then if K is of weight w,

$$(5) \qquad K(A, B, C, \cdots; X, Y) = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}^w K(a, b, c, \cdots; x, y).$$

If, now, x', y' and X', Y' are two pairs of variables so related that

$$(4') \qquad \begin{aligned} x' &= \alpha X' + \beta Y', \\ y' &= \gamma X' + \delta Y', \end{aligned}$$

then

$$(5') \qquad K(A, B, C, \cdots; X', Y') = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}^w K(a, b, c, \cdots; x', y').$$

But if $\eta x - \xi y$ is a linear form with coefficients which are independent variables, and $\mathrm{H}X - \Xi Y$ is its transform, then

$$\xi = \alpha\frac{\Xi}{\Delta} + \beta\frac{\mathrm{H}}{\Delta}, \qquad \eta = \gamma\frac{\Xi}{\Delta} + \delta\frac{\mathrm{H}}{\Delta}; \tag{6}$$

or ξ, η and Ξ/Δ, H/Δ are two such pairs of variables. Thus

$$K\left(A, B, C, \cdots; \frac{\Xi}{\Delta}, \frac{\mathrm{H}}{\Delta}\right) = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}^{w} K(a, b, c, \cdots; \xi, \eta).$$

Since $K(a, b, c, \cdots; x, y)$ is homogeneous in x and y of degree d, this equation is equivalent to

$$K(A, B, C, \cdots; \Xi, \mathrm{H}) = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}^{w+d} K(a, b, c, \cdots; \xi, \eta). \tag{7}$$

That is, to every equation (5) where x and y are the variables of the system S of binary forms there corresponds an equation (7) where ξ and η are independent variables and η, $-\xi$ are the coefficients of the linear form $\eta x - \xi y$. In particular, (7) holds whenever ξ, η and Ξ, H are marks of the field so related that (6) holds. Let $K(a, b, c, \cdots; \xi, \eta)$ become $I(a, b, c, \cdots; \xi, \eta)$ when ξ and η are in the field. Then, by the foregoing, $I(a, b, c, \cdots; \xi, \eta)$ is a modular invariant of the system S' consisting of the forms of S together with the linear form $\eta x - \xi y$, which is of weight $w + d$.

If $I(\xi, \eta)$ is the same as $K(\xi, \eta)$, our theorem is proved for the covariant K. We shall, accordingly, consider the case where $I(\xi, \eta)$ is not identically equal to $K(\xi, \eta)$.

Let I be congruent to $A_0(a, b, c, \cdots)$ for $\xi = 1$, $\eta = 0$. Then A_0 is the leader of $K(x, y)$. Accordingly consider the function

$$K'(\xi, \eta) = A_0(a, b, c, \cdots)\xi^d + A_1(a, b, c, \cdots)\xi^{d-1}\eta + \cdots + A_d(a, b, c, \cdots)\eta^d,$$

where $A_1, A_2, \cdots, A_d$ are polynomials in a's, b's, c's, $\cdots$ to be determined. In order that this shall be an invariant of S' which is formally invariant as to ξ and η, $A_0, A_1, \cdots, A_d$ must satisfy certain relations.* What these relations are does not concern us here. We do know, however, that these relations are consistent for at least one set of coefficients $A_0, \cdots, A_d$. Accordingly, let $A_1, A_2, \cdots, A_d$ be one set of polynomials satisfying these relations. Then K' and K are both invariants of S' of the same degree in ξ and η which are congruent when $\eta = 0$. Hence $K - K'$ is such an invariant of S' which vanishes for $\eta = 0$. Thus either $K - K'$ is identically zero in

*O. E. Glenn, *The formal modular invariant theory of binary quantics*, these Transactions, vol. 17 (1916), p. 547 et seq.

ξ and η, or η is a factor of $K - K'$. In the latter case, since $K - K'$ is an invariant which is homogeneous in ξ and η, $L(\xi, \eta) = \xi^{p^n}\eta - \xi\eta^{p^n}$ must be a factor of it.

That is, any invariant K of S' which is formally invariant as to ξ and η is of the form

$$K(\xi, \eta) = K'(\xi, \eta) + L(\xi, \eta)K_0(\xi, \eta)$$

where K_0 is a homogeneous polynomial in ξ and η with coefficients in the field. Notice, moreover, that for all invariants of the same degree in ξ and η which are congruent to the same modular invariant I we can use the same invariant K'. Since K, K', and L are invariants of S' which are formally invariant as to ξ and η, K_0 will be an invariant of S' which is formally invariant as to ξ and η and which is of degree $< d$ in ξ and η.

Hence every covariant $K(x, y)$ of the system S is of the form $K'(x, y) + L(x, y)K_0(x, y)$ where $K'(x, y)$ is the same function for every covariant of a given order and with a given leader, and where K_0 is a covariant of S of order $< d$.

Now let $\Sigma(\xi, \eta)$ denote a set of invariants $K(\xi, \eta)$ of S' determined in the following manner. Consider any particular modular invariant I of S' (all of whose exponents are $\leqq p^n - 1$) and the totality of all invariants K which are $\equiv I$ and which in addition are formally invariant as to ξ and η. These invariants $K(\xi, \eta)$ will be of degrees, d, $d + p^n - 1$, $d + 2(p^n - 1)$, $\cdots$, $d + q(p^n - 1)$, $\cdots$ in ξ and η where d is a suitable positive integer. For each degree, choose one invariant K to put in the set $\Sigma(\xi, \eta)$. Do this for every $I \not\equiv 0$, and let $\Sigma(\xi, \eta)$ denote the set of such invariants $K(\xi, \eta)$ and the invariant I which is identically zero. We shall use $\Sigma(x, y)$ to denote this set of functions with ξ, η replaced by x, y. The members of $\Sigma(x, y)$ are covariants of S.

Then, proceeding by induction, we see that every modular covariant of S is a polynomial in $L = x^{p^n}y - xy^{p^n}$ whose coefficients are modular covariants of the set $\Sigma(x, y)$. Moreover, in view of the above argument, this expansion of any covariant K as a polynomial in L is unique for any given set Σ, though the covariants of the set Σ are not uniquely determinable. Thus we have proved

THEOREM I. *Let S be a system of binary forms in the variables x and y and let S' be the system consisting of the forms of S (where the variables are now ξ and η) together with the linear from $\eta x - \xi y$. Then every modular covariant of the system S is a polynomial in L with coefficients which are modular invariants of the system S' chosen form the set Σ.*

This theorem has already been verified by Miss Sanderson* for some special cases including the binary quadratic, modulo 3.

* Loc. cit., p. 491, 499.

Notice that in the proof of this theorem no use was made of the assumption as to the character of K except that it was formally invariant as to x and y—that is, no assumption was made as to whether or not K was formally invariant as to any or all sets of coefficients or a pair of variables cogredient with x and y. In short, we have the following

COROLLARY. *If K is the class of all modular concomitants of the system S which are formally invariant as to certain sets of coefficients and variables but not formally invariant as to x and y, then the theorem tells us how to construct all modular concomitants of S which are formally invariant as to x and y in addition to being formally invariant as to those sets of coefficients and variables with respect to which K is formally invariant.*

5. Generalization to m pairs of binary variables. Consider a system S of forms in the two pairs of binary variables x_1, y_1 and x_2, y_2, and let K be a modular (mixed) concomitant of S under a group G of linear transformations with coefficients in the $GF[p^n]$. Let S' be the system consisting of the forms of S (where x_1, y_1 have been replaced by ξ_1, η_1) together with the additional linear form $l_1 = \eta_1 x_1 - \xi_1 y_1$; and let S'' be the system consisting of the forms of S together with the two additional forms l_1 and $l_2 = \eta_2 x_2 - \xi_2 y_2$. By the theorem of § 4 in its extended form as given in the corollary, K is a polynomial in $L_1 = x^{p^n} y_1 - x_1 y^{p^n}$ and those invariantive functions of x_2, y_2 and of the coefficients of S' which have been made formally invariant as to x_1 and y_1. Applying the corollary to the modular covariants K' of S', we see that K is a polynomial in L_1, $L_2 = x^{p^n} y_2 - x_2 y^{p^n}$ and the modular invariants of S'' which have been made formally invariant as to x_1, y_1 and x_2, y_2.

Proceeding by induction, we prove

THEOREM II. *Let S be a system of binary forms in the m pairs of variables $(x_1, y_1), (x_2, y_2), \cdots, (x_m, y_m)$. Let $S^{(m)}$ be the system consisting of the forms of S (where now the variables are the ξ_i, η_i) together with the linear forms $l_i = \eta_i x_i - \xi_i y_i$ $(i = 1, \cdots, m)$. Then every modular mixed concomitant of S is a polynomial in the $L_i = x^{p^n} y_i - x_i y^{p^n}$ $(i = 1, \cdots, m)$ and in the modular invariants of $S^{(m)}$ which have been made formally invariant as to the x_i, y_i $(i = 1, \cdots, m)$.*

MOUNT HOLYOKE COLLEGE,
SOUTH HADLEY, MASS.