NEW PROOFS OF CERTAIN FINITENESS THEOREMS IN THE THEORY OF MODULAR COVARIANTS*

BY

OLIVE C. HAZLETT

1. Introduction. In a recent paper of mine† it was proved that every modular covariant of a system of forms S (with variables x and y) is a polynomial in the universal covariant L and modular invariants of the system of forms S (with variables ξ and η) enlarged by the linear form $\eta x - \xi y$ which have been made formally invariant as to x and y. As pointed out in that paper, we have as a corollary the following:

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 the set K' of all modular concomitants 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.

Here x and y may be the variables of the system S or a pair of variables which is cogredient with the variables of the system or even a pair of variables which is cogredient with the variables aside from a power of the determinant of the transformation. In fact, every modular covariant of the set K' is a polynomial in L and the concomitants of the set K which have been made formally invariant as to x and y. In the present paper we give a few extensions and applications of this theorem.

§§ 2–3. New proofs of some finiteness theorems

2. Finiteness theorem for modular covariants. Dickson has already shown that modular invariants from their very nature have the finiteness property.‡ He has also proved§ that modular covariants have the finiteness property. We now proceed to give a proof of the finiteness theorem for modular covariants directly from the finiteness theorem for modular invariants.

* Presented to the Society, October 25, 1919.

† *A Theorem on Modular Covariants*, these Transactions, vol. 21 (1920), p. 247.

‡ *General Theory of Modular Invariants*, these Transactions, vol. 10 (1909), p. 126.

§ *Proof of the Finiteness of Modular Covariants*, these Transactions, vol. 14 (1913), p. 300.

For, in the first place, every modular covariant of a system S of forms is a polynomial in L and the modular invariants of the enlarged system S' which have been made formally invariant as to x and y. Now the modular invariants of S' have the "finiteness" property—i.e., they are all expressible as polynomials in a finite subset. This is not, however, the same as saying that the modular invariants of S' which have been made formally invariant as to x and y have the finiteness property, since any one modular invariant of S' produces a number of modular invariants which are formally invariant as to x and y. Let $I_1, I_2, \cdots, I_\nu$ be modular invariants of S' which are congruent to I when x and y are in the field and are formally invariant as to x and y. Moreover, let I_1 be such an invariant of the lowest possible degree, say d, in x and y; let I_2 be of degree $d + p^n - 1$, if there be any such;* let I_3 be of degree $d + 2(p^n - 1)$, if there be any such; and finally let I_ν be of degree $d + (p^n - 1)^2$. From the proof of the fundamental theorem of the paper mentioned in the introduction, every invariant of S' of degree d which is formally invariant as to x and y and which is congruent to I when x and y are in the field is of the form $I_1 + LI_1$, where I_1 is a modular invariant of S' which is formally invariant as to x and y and is of a degree in x and y which is less than d. A similar remark applies to invariants of S' which are congruent to I when x and y are in the field and which are of degree $d + (p^n - 1), \cdots; d + (p^n - 1)^2$ in x and y.

We can readily construct an invariant of S' which is of degree $d + p^n(p^n - 1)$ and is congruent to I when x and y are in the field, for QI_1 is such an invariant. Similarly, we can express every modular invariant of S' which is formally invariant as to x and y and which is congruent to I whenever x and y are in the field as a polynomial in $I_1, I_2, \cdots, I_\nu, L, Q$ and modular invariants of lower order which are formally invariant as to x and y. Hence, by induction, we prove the finiteness theorem for the modular invariants of S' which are formally invariant as to x and y.

In fact, we can so choose a fundamental set of invariants of S' which are formally invariant as to x and y that to each invariant of a fundamental set of modular invariants of S there correspond at most p^n invariants in a fundamental set of invariants of S' which are formally invariant as to x and y. In addition, we have to put L and Q in our fundamental set. We can, if we wish, think of Q as a modular invariant of S' which is formally invariant as to x and y, arising from the modular invariant 1. Notice that the degree of 1 is congruent to $p^n(p^n - 1)$ modulo $p^n - 1$. Also, L can be regarded as a

* It is to be noted that there is not necessarily any such invariant of degree $d + p^n - 1$, nor of degree $d + 2(p^n - 1)$, etc. For example, if I be unity, the only homogeneous formal invariants congruent to I for values of x and y in the field are 1 and powers of $Q = I_1$. In this case there are no invariants $I_2, I_3, \cdots, I_\nu$.

modular invariant of S' which has been made formally invariant as to x and y—it is a formal invariant arising from the modular invariant 0. At first there appears to be a discrepancy here, since the degree of L is $p^n + 1 \not\equiv 0 \pmod{p^n - 1}$. This discrepancy, however, is only apparent; for, if x and y are in the field, L becomes $xy - xy = 0$. In other words, L reduces to a quadratic which "telescopes," so to speak.

Hence, applying the fundamental theorem quoted in the introduction, we have proved

THEOREM I. *The set of all modular covariants of a system S of binary forms has the finiteness property—i.e., there is a finite number of covariants of the set such that every covariant of S is expressible as a polynomial in the covariants of the subset.*

3. Finiteness theorem for modular invariants of a system of forms and cogredient points. The above theorem may, for convenience, be restated thus: Let K be the class of all modular concomitants of the system Σ which are formally invariant as to certain sets of coefficients and variables, but not formally invariant as to x and y; and let K' be the class of all modular concomitants of the same system Σ 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. Here, as in § 1, x and y may be the variables of the system Σ or a pair of variables which is cogredient with the variables of the system or even a pair of variables which is cogredient with the variables aside from a power of the determinant of the transformation. Then, if the set K has the finiteness property, the set K' has the finiteness property.

Now consider the set of all modular invariants of a system of forms S and the cogredient points $(x_1, y_1), (x_2, y_2), \cdots, (x_k, y_k)$. In the body of the proof of the fundamental theorem of the Chicago paper,* it was proved that the set of all invariants of the system S and the cogredient points is identical with the set of all invariants of the system S enlarged by the linear forms $\eta_1 x_1 - \xi_1 y_1$, $\eta_2 x_2 - \xi_2 y_2$, $\cdots$, $\eta_k x_k - \xi_k y_k$ where it is understood that now the ξ's and η's are the variables and the x's and y's are coefficients which are independent variables. That is, the invariants of S and the cogredient points are the invariants of the enlarged system S' which are formally invariant as to the x's and y's.

Let S' be the system Σ of the beginning of this section, and apply Theorem I as reworded above, making the set of modular invariants of S' formally invariant as to the pairs (x_i, y_i) one at a time. By induction, we thus prove

THEOREM II. *The set of all modular invariants of a system S of binary forms*

* These Transactions, vol. 21 (1920), pp. 251–252 and p. 254.

and the cogredient points (x_1, y_1), (x_2, y_2), $\cdots$, (x_k, y_k) *has the finiteness property.*

This is the theorem of Professor F. B. Wiley's Chicago dissertation;* but the present proof has the advantage of showing the relation between the modular invariants of S' on the one hand and the invariants of the original system S on the other hand. It also shows the relation between the invariants of S and $k-1$ cogredient points, and the invariants of S and k cogredient points.

This theorem includes as a special case the finiteness theorem for the modular invariants of any number m of cogredient (binary) points. For $m = 1$, Dickson† has already shown that a fundamental set of invariants consists of L and Q. This affords a simple illustration of the fundamental theorem quoted in § 1. For the invariants of the point (x, y) are the same as the formal invariants of the linear form $l = \eta x - \xi y$, where ξ and η are the variables, and hence (by the theorem) are simply the modular invariants of l which have been made formally invariant as to x and y. Now there are two classes of linear forms l—(i) when $x = y = 0$, (ii) when x and y are in the field but $(x, y) \neq (0, 0)$. Accordingly we may take as a set of modular invariants which characterize the classes for l: (i) a function which is $= 0$ whenever x and y are in the field, (ii) a function which is $= 1$ when x and y are in the field, but $(x, y) \neq (0, 0)$, and $= 0$ when $(x, y) = (0, 0)$. By Dickson's fundamental memoir‡ all modular invariants are linear combinations of these two functions. Now L is a formal invariant which satisfies condition (i), and Q is a formal invariant which satisfies condition (ii).

If $m = 2$, a fundamental set of invariants§ for the Galois field $GF[p]$ is

$$L_i = \begin{vmatrix} x_i^p & y_i^p \\ x_i & y_i \end{vmatrix}, \qquad Q_i = \frac{1}{L_i}\begin{vmatrix} x_i^{p^2} & y_i^{p^2} \\ x_i & y_i \end{vmatrix} \qquad (i = 1, 2),$$

$$M = x_2 y_1 - y_2 x_1, \qquad M_1 = x_2 y_1^p - y_2 x_1^p, \qquad M_2 = x_2^p y_1 - y_2^p x_1,$$

$$N_s = \frac{M_2^{s+1} L_1^{p-s-1} + (-1)^s M_1^{p-s} L_2^s}{M^p} \qquad (1 \leq s \leq p-2).$$

The invariants Q_i and N_s are all integral functions of x_1, x_2, y_1, y_2. This gives another simple illustration of the theorem of my Chicago paper. For the invariants of the two points (x_1, y_1) and (x_2, y_2) are identical with the formal invariants of two linear forms $l_1 = \eta_1 x_1 - \xi_1 y$ and $l_2 = \eta_2 x_2 - \xi_2 y_2$ (where the variables are the ξ's and η's), which in turn are the modular

* These Transactions, vol. 15 (1914), pp. 431–438.

† *Madison Colloquium Lectures*, p. 38; these Transactions, vol. 12 (1911), p. 1; Quarterly Journal of Mathematics, 1911, p. 158.

‡ These Transactions, vol. 10 (1909), p. 126.

§ W. C. Krathwohl, *Modular invariants of two pairs of cogredient variables* (Chicago dissertation), American Journal of Mathematics, vol. 36 (1914), pp. 449–460.

invariants of l_1 and l_2 which have been made formally invariant as to the x's and y's. Now the classes of the pairs of linear forms are

(1) $(x_1, y_1) = (x_2, y_2) = (0, 0)$.

(2) $(x_1, y_1) = (0, 0)$, (x_2, y_2) in the field but $\neq (0, 0)$,

(3) $(x_2, y_2) = (0, 0)$, (x_1, y_1) in the field but $\neq (0, 0)$.

$(4)_\lambda$ $(x_1, y_1) = (a, b)$, $(x_2, y_2) = (\lambda a, \lambda b)$, $\lambda \neq 0$ and $(a, b) \neq (0, 0)$,

$(5)_\Delta$ $(x_1, y_1) = (a, b)$, $(x_2, y_2) = (c, d)$, where a, b, c, d are in the field, but $\Delta = ad - bc \neq 0$.

Now for the different classes, the invariants above take the following values

	L_1, L_2	Q_1	Q_2	M, M_1, M_2	N_s
Class 1	0	0	0	0	0
Class 2	0	0	1	0	0
Class 3	0	1	0	0	0
Class 4_λ	0	1	1	0	λ^{p^s}
Class 5_Δ	0	1	1	Δ	0

Thus the theorem is verified for this special case.

§§ 4–9. Application to formal covariants

4. A lemma. In this section we will prove an important lemma which shows the intimate relation between modular covariants and formal covariants. This lemma is not new, but is a special case of Miss Sanderson's theorem.* The present proof is given because it is elementary in nature and because it furnishes a simple formula for a formal covariant which is congruent to a given modular covariant C whenever the coefficients are in the field.

Let $\phi(a, b, c, \cdots; x, y) = C$ be a modular covariant of the system S under the group G of linear transformations with coefficients in the field $GF[p^n]$. Moreover, let ϕ be of index w. There is no loss of generality in assuming that ϕ is pseudo-homogeneous† in the k coefficients $a, b, c, \cdots$ of degree d. For, if ϕ is not pseudo-homogeneous in the coefficients, it is the sum of a finite number of modular covariants which are pseudo-homogeneous in the $a, b, c, \cdots$.

First, we construct a function K which is homogeneous in the k independent

* These Transactions, vol. 14 (1913), pp. 489–500.

† A function f is said to be pseudo-homogeneous of degree d if, when the arguments $a, b, c, \cdots$ are multiplied by ρ, any non-zero mark of the field $GF[p^n]$, the function f is multiplied by ρ^d. If f is a polynomial, this means that the degrees of the different terms of f differ at most by integral multiples of $p^n - 1$.

variables $a, b, c, \cdots$ and such that $K \equiv C$ whenever $a, b, c, \cdots$ are in the field. We can take

$$K = \sum \left[\phi(a_0, b_0, c_0, \cdots; x, y) \left\{ \frac{Q\begin{pmatrix} a, & b, & c, & \cdots \\ a_0, & b_0, & c_0, & \cdots \end{pmatrix}}{Q\begin{pmatrix} a_0, & b_0, & c_0, & \cdots \\ a_0, & b_0, & c_0, & \cdots \end{pmatrix}} \right\}^d \right].$$

Here Σ denotes the sum of all terms of the type indicated as the k-tuple $(a_0, b_0, c_0, \cdots)$ ranges over the k-tuples of a certain set σ defined below. Inside the bracket,

$$Q\begin{pmatrix} a, & b, & c, & \cdots \\ a_0, & b_0, & c_0, & \cdots \end{pmatrix}$$

stands for

$$\frac{\begin{vmatrix} a & b & c & \cdots \\ a^{p^n} & b^{p^n} & c^{p^n} & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a^{p^{(k-2)n}} & b^{p^{(k-2)n}} & c^{p^{(k-2)n}} & \cdots \\ a^{p^{(k-1)n}} & b^{p^{(k-1)n}} & c^{p^{(k-1)n}} & \cdots \end{vmatrix}}{\begin{vmatrix} a & b & c & \cdots \\ a^{p^n} & b^{p^n} & c^{p^n} & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a^{p^{(k-2)n}} & b^{p^{(k-2)n}} & c^{p^{(k-2)n}} & \cdots \\ a_0 & b_0 & c_0 & \cdots \end{vmatrix}}$$

and

$$Q\begin{pmatrix} a_0, & b_0, & c_0, & \cdots \\ a_0, & b_0, & c_0, & \cdots \end{pmatrix}$$

stands for the value of Q when $a = a_0, b = b_0, c = c_0, \cdots$. Miss Sanderson has already shown that $Q \equiv 0$ if and only if $a, b, c, \cdots$ are not proportional to $a_0, b_0, c_0, \cdots$.* The numerator of Q is the product of all essentially distinct linear functions of $a, b, c, \cdots$ in which the coefficients are marks of the field, and the denominator of Q is the product of all those essentially distinct linear functions of $a, b, c, \cdots$ (in which the coefficients are marks of the field) which vanish whenever the $a, b, c, \cdots$ are proportional to $a_0, b_0, c_0, \cdots$. Notice that $Q\begin{pmatrix} a, & b, & c, & \cdots \\ a_0, & b_0, & c_0, & \cdots \end{pmatrix}$ is a polynomial of degree $p^{(k-1)n}$ in the coefficients $a, b, c, \cdots$, and thus K is homogeneous in the $a, b, c, \cdots$ of degree $d(p^{(k-1)n})$ which is congruent to d modulo $p^n - 1$.†

Into the set σ we put k-tuples $(a_i, b_i, c_i, \cdots)$—where the $a_i, b_i, c_i, \cdots$ are in the field—such that, if any particular k-tuple $(a_i, b_i, c_i, \cdots)$ is in the set σ,

* These Transactions, vol. 14 (1913), p. 491.

† These Transactions, vol. 14 (1913), pp. 492, 493.

then $(\rho a_i, \rho b_i, \rho c_i, \cdots)$ is not in the set σ when ρ is any non-zero mark of the field; and such, moreover, that if $(\alpha, \beta, \gamma, \cdots)$ is any k-tuple of marks of the field, then there is in the set σ some k-tuple $(a_i, b_i, c_i, \cdots)$ such that $\alpha = \rho a_i, \beta = \rho b_i, \gamma = \rho c_i, \cdots$ for ρ some non-zero mark of the field.

If we now give to $a, b, c, \cdots$ any set of values in the field, this set of values is of the form $\rho a_1, \rho b_1, \rho c_1, \cdots$, where $(a_1, b_1, c_1, \cdots)$ is a k-tuple of the set σ. Then K has the value

$$\sum \left[\phi(a_0, b_0, c_0, \cdots; x, y) \left\{ \frac{Q\begin{pmatrix} a_1, b_1, c_1, \cdots \\ a_0, b_0, c_0, \cdots \end{pmatrix}}{Q\begin{pmatrix} a_0, b_0, c_0, \cdots \\ a_0, b_0, c_0, \cdots \end{pmatrix}} \right\}^d \rho^{dp^{(k-1)n}} \right]$$

$$\equiv \phi(a_1, b_1, c_1, \cdots; x, y)\rho^d$$

$$\equiv \phi(\rho a_1, \rho b_1, \rho c_1, \cdots; x, y) \equiv C$$

since C is pseudo-homogeneous in $a, b, c, \cdots$ of degree d.

If we now subject the variables x and y to any transformation of determinant Δ of the group G, the indeterminates $a, b, c, \cdots$ are subjected to an induced transformation which carries any particular k-tuple of the set σ into a k-tuple of the form $(\rho a_1, \rho b_1, \rho c_1, \cdots)$ where $(a_1, b_1, c_1, \cdots)$ is a k-tuple of the set σ and ρ is some mark of the field. Let the indeterminates $a, b, c, \cdots$ go into $a', b', c', \cdots$ and let $a_0, b_0, c_0, \cdots$ go into $\rho a_0', \rho b_0', \rho c_0', \cdots$ where $(a_0', b_0', c_0', \cdots)$ is a k-tuple of the set σ. Since C is a modular covariant of index w which is pseudo-homogeneous in $a, b, c, \cdots$ of degree d,

$$\Delta^w \phi(a_0, b_0, c_0, \cdots; x, y) = \rho^d \phi(a_0', b_0', c_0', \cdots; x', y').$$

At the same time, since $(a, b, c, \cdots), (a^{p^n}, b^{p^n}, c^{p^n}, \cdots)$, etc. are cogredient,

$$Q\begin{pmatrix} a, b, c, \cdots \\ a_0, b_0, c_0, \cdots \end{pmatrix} \equiv \frac{1}{\rho} Q\begin{pmatrix} a', b', c', \cdots \\ a_0', b_0', c_0', \cdots \end{pmatrix}$$

and

$$Q\begin{pmatrix} a_0, b_0, c_0, \cdots \\ a_0, b_0, c_0, \cdots \end{pmatrix} \equiv \rho^{p^{(k-1)n-1}} Q\begin{pmatrix} a_0', b_0', c_0', \cdots \\ a_0', b_0', c_0', \cdots \end{pmatrix}.$$

Thus

$$\Delta^w K = \sum \left[\rho^d \phi(a_0', b_0', c_0', \cdots; x', y') \left\{ \frac{Q\begin{pmatrix} a', b', c', \cdots \\ a_0', b_0', c_0', \cdots \end{pmatrix}}{Q\begin{pmatrix} a_0', b_0', c_0', \cdots \\ a_0', b_0', c_0', \cdots \end{pmatrix}} \right\}^d \frac{1}{\rho^{dp^{(k-1)n}}} \right]$$

$$\equiv \sum \left[\phi(a_0', b_0', c_0', \cdots; x', y') \left\{ \frac{Q\begin{pmatrix} a', b', c', \cdots \\ a_0', b_0', c_0', \cdots \end{pmatrix}}{Q\begin{pmatrix} a_0', b_0', c_0', \cdots \\ a_0', b_0', c_0', \cdots \end{pmatrix}} \right\}^d \right] = K'.$$

Notice that in this congruence the $a, b, c, \cdots$ and the $a', b', c', \cdots$ are two sets of indeterminates. Thus the lemma is proved.

5. A theorem on formal covariants. Let C be a modular covariant of the system S of forms with coefficients $a, b, c, \cdots$. As above, there is no loss of generality in assuming that C is pseudo-homogeneous of degree d in the coefficients as well as homogeneous in the variables x and y. By the preceding section, we know that there is at least one homogeneous formal covariant K of the system S which is congruent to C whenever the coefficients $a, b, c, \cdots$ are marks of the field. Let K_0 be one such covariant of lowest degree ω in $a, b, c, \cdots$. If there is a second covariant K which is of degree ω in $a, b, c, \cdots$ and which is congruent to C whenever $a, b, c, \cdots$ are in the field, then $K - K_0 = K_1$ is a homogeneous formal covariant of S which is congruent to zero whenever the coefficients are in the field—that is, K_1 vanishes for all classes of forms of the system S. There are two possibilities: (1) K_1 is the product of two or more rational formal covariants of which none vanishes for all sets of coefficients in the field; (2) K_1 contains as a factor a formal covariant which can not be expressed as the product of several covariants and which does vanish for all classes of S.

Thus any formal covariant K of the system S is expressible in one of the two following forms:

(1) $$K = K_0 + M_1 M_2 \cdots M_r,$$

where $M_1, M_2, \cdots, M_r$ are formal covariants of S which do not vanish for all sets of values of the coefficients in the field;

(2) $$K = K_0 + VK_1$$

in which V and K_1 are formal covariants of S where V vanishes whenever the $a, b, c, \cdots$ are in the field and is not the product of two or more formal covariants of S. Notice, moreover, that we can use the same formal covariant K_0 for all formal covariants which are of the same degree in $a, b, c, \cdots$ and of the same order in x and y and which, moreover, are congruent to the same modular covariant C when $a, b, c, \cdots$ are in the field.

Now let Σ denote a set of formal covariants of S determined in the following manner. Consider any particular modular covariant C of S (in which all the exponents of $a, b, c, \cdots$ are $\leq p^n - 1$) and the totality of all formal covariants K which are congruent to C whenever the coefficients are marks of the field. The degrees of these covariants K will be of the form $\omega + q(p^n - 1)$ where q is a positive integer and ω is the least such degree. For each such degree, choose one formal covariant K to put in the set Σ.* Do this for every

* It must be borne in mind that there are not necessarily any formal covariants for *each* such degree. Compare the third footnote in § 2.

modular covariant C of a fundamental set of modular covariants of S, and let Σ denote the set of all such formal covariants.

Then, proceeding by induction, we see that every formal covariant of S is a polynomial in the covariants of the set Σ and in those irreducible formal covariants of S which vanish whenever the coefficients $a, b, c, \cdots$ are marks of the field. Thus we have proved

THEOREM III. *Every formal modular covariant of a system S of binary forms with respect to the Galois Field GF[p^n] is a polynomial in the modular covariants which have been made formally invariant as to the coefficients of the forms, and in the irreducible covariants which are congruent to zero whenever the coefficients are marks of the field.*

It will now be interesting to give a more elegant proof of this theorem by the aid of a symbolic notation.

6. Symbolic Notation. In the symbolic theory of algebraic invariants, Aronhold, Clebsch and Gordan* express any binary form f of order m as the mth power of a symbolic linear function of the variables thus,—

$$f = a_0 x^m + a_1 x_1^{m-1} x_2 + \cdots = (\alpha_1 x_1 + \alpha_2 x_2)^m = \alpha_x^m.$$

Then $a_0 = \alpha_1^m$, $a_1 = m\alpha_1^{m-1}\alpha_2$, and in general $a_r = {}_mC_r\, \alpha_1^{m-r}\alpha_2^r$. In order that the a's may be independent variables, the agreement is made that we never use any term of more than the mth degree in the α's. Accordingly, if we wish to express a product of two or more a's in symbolic form, we have to introduce two or more equivalent sets of symbols, say (α_1, α_2), (β_1, β_2), etc. Then $f = \alpha_x^m = \beta_x^m = \gamma_x^m = \cdots$; and thus we can write $a_0 a_2$ as $\alpha_1^m(m\beta_1^{m-1}\beta_2)$ or as $\beta_1^m(m\alpha_1^{m-1}\alpha_2)$, etc. Then every polynomial in these symbols which has the invariantive property will be an invariant of f; though, in order that such an invariant may be rational and integral in the a's it must be homogeneous of the mth degree in the α's, homogeneous of the mth degree in the β's, etc.

In the theory of modular invariants (formal and otherwise), we can not, however, use this classical symbolic notation for the binary form f over the general Galois field $GF[p^n]$. In the first place, the binomial coefficients which naturally arise in this way may be zero in the field. In the second place, we know that $L_\alpha = (\alpha^{p^n}\alpha) = \alpha_1^{p^n}\alpha_2 - \alpha_1\alpha_2^{p^n}$ is an invariant symbol, since $\alpha_1^{p^n}$, $\alpha_2^{p^n}$ are cogredient with α_1, α_2. But in case $p^n + 1 > m$, we have no right to use this symbol, as explained above. Accordingly we must adopt some other symbolism.

---

*Aronhold, Journal für Mathematik, vol. 62 (1863), p. 281; Clebsch, Journal für Mathematik, vol. 59 (1860), p. 1; Gordan, Mathematische Annalen, vol. 2 (1870), p. 227, vol. 5 (1872), p. 595; Clebsch, *Theorie der binären algebraischen Formen* (1872); Gordan, *Vorlesungen über Invariantentheorie* (1887).

With this in mind, represent the binary form as

$$f = \prod(\alpha_1 x_1 + \alpha_2 x_2) = (\alpha_1 x_1 + \alpha_2 x_2)(\beta_1 x_1 + \beta_2 x_2) \cdots = \prod \alpha_x \beta_x \cdots,$$

where it is understood that there are m distinct symbolic factors. Now every invariantive function of the variables and the coefficients of f is an invariantive function of the symbols $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \cdots$ and x_1, x_2. Conversely, an invariantive function C of the symbols is a symbolic covariant of f; and if it is rational in the a's it is actually a covariant. If, however, C is to be rational in the a's it must be such that, if we interchange any two pairs of symbols—say (α_1, α_2) and (β_1, β_2)—it is unchanged in form, and every term of C must be of the same degree in the α's that it is in the β's, etc. If these two conditions are satisfied, then conversely C is rational in the a's. For C is then a symmetric function of the pairs $(\alpha_1, \alpha_2), (\beta_1, \beta_2), \cdots$ and hence, by the theory of symmetric functions, is well-known to be rational in a certain finite set of such functions, which are simply the a's.

7. Symbolic proof of the theorem of section 5. As in the theory of algebraic invariants, we notice that $(\alpha_1, \alpha_2), (\beta_1, \beta_2), \cdots$ are what we might call pseudo-cogredient with $(x_2, -x_1)$ that is, $(\alpha_1, \alpha_2), (\beta_1, \beta_2), \cdots$ are cogredient with $(x_2, -x_1)$ aside from a power of the modulus. For, if x_1 and x_2 are subjected to the non-singular transformation

$$\begin{cases} x_1 = ax_1' + bx_2', \\ x_2 = cx_1' + dx_2', \end{cases} \qquad \Delta = ad - bc \neq 0,$$

then, since $\alpha_1 x_1 + \alpha_2 x_2 = \alpha_1' x_1' + \alpha_2' x_2'$,

$$\begin{cases} \alpha_2 = \dfrac{1}{\Delta}[a\alpha_2' + b(-\alpha_1')], \\ -\alpha_1 = \dfrac{1}{\Delta}[c\alpha_2' + d(-\alpha_1')]. \end{cases}$$

Hence every modular covariant of a system S of forms is a modular invariant of certain pairs $(\alpha_1, \alpha_2), (\beta_1, \beta_2), \cdots, (x_2, -x_1)$ which are pseudo-cogredient; or every modular covariant of the system S may be regarded as a modular invariant of certain cogredient pairs $(\alpha_1, \alpha_2), (\beta_1, \beta_2), \cdots, (x_2, -x_1)$. The converse is also true, though not every invariant of the symbolic pairs is a rational covariant of the system S. As proved at the end of § 6, a necessary and sufficient condition that an invariant of the symbolic pairs be rational is that it be symmetric in these pairs. A similar remark applies to the covariants.

In fact, by the proof of the fundamental theorem, any formal modular covariant C of a single binary form f is of the form $M + V$, where M is a modular invariant of the $n + 1$ pairs which has been made formally invariant

and V is a formal invariant of the $n+1$ pairs which vanishes whenever the α's, β's, $\cdots$ are all in the field. This M can be taken as the same for all covariants C which are congruent to the same modular covariant when the α's, β's, $\cdots$ are all in the field.

It can readily be proved that we can so choose M and V that they are symmetric in the pairs (α_1, α_2), (β_1, β_2), $\cdots$. For, by the proof of the fundamental theorem, $C = M_\alpha + L_\alpha M_{1\alpha}$, where M_α and $M_{1\alpha}$ are two formal modular invariants of the $n+1$ pairs. Similarly $C = M_\beta + L_\beta M_{1\beta}$, etc. Now M_β and $M_{1\beta}$ can be so chosen that they are obtained from M_α and $M_{1\alpha}$ respectively by interchanging the pairs (α_1, α_2) and (β_1, β_2). Hence

$$C = M_{\alpha\beta} + (L_\alpha N_\alpha + L_\beta N_\beta + L_\alpha L_\beta N_{\alpha\beta}),$$

where N_β is obtained from N_α by interchanging the pairs (α_1, α_2) and (β_1, β_2) and where $M_{\alpha\beta}$ and $N_{\alpha\beta}$ are symmetric in these two pairs. By induction, we see that the statement at the beginning of this paragraph is true.

With slight changes, this proof holds for a system of binary forms.

It is to be noted that the symbol L_α vanishes whenever α_1 and α_2 are marks of the field; similarly with L_β, etc. But any formal modular invariant which evanesces whenever the α's, β's, etc. are all in the field (such as those of the type $L_\alpha N_\alpha + L_\beta N_\beta + L_\alpha L_\beta N_{\alpha\beta} + \cdots$) does not necessarily vanish whenever the coefficients of the system S are in the field. Hence we have proved Theorem III.

This second proof, besides beauty of form, has the advantage of indicating the relation between formal modular covariants of two forms of different degrees. Although it has the obvious disadvantage that it does not furnish a definite formula by which we can determine the formal modular covariants of a system of forms, nevertheless it suggests that some day there may be evolved a symbolic theory of formal covariants.

8. Application to the binary quadratic, modulo 3. Dickson* has shown that a fundamental set of modular invariants of the binary quadratic,

$$f_2 = a_0 x_1^2 + 2a_1 x_1 x_2 + a_2 x_2^2,$$

modulo 3 is

$$\Delta = a_1^2 - a_0 a_2, \qquad q = (a_0 + a_2)(a_1^2 + a_0 a_2 - 1);$$

while he has shown† that a fundamental set of formal invariants consists of

$$\Delta = a_1^2 - a_0 a_2, \qquad J = a_0(a_0 + a_1 + a_2)(a_0 + 2a_1 + a_2)a_2,$$

$$B = a_1(a_1 + a_0)(a_1 - a_0)(2a_0 + a_2)(2a_1 + a_2)(a_1 + a_2),$$

$$\Gamma = (a_0 + a_2)(2a_0 + 2a_1 + a_2)(2a_0 + a_1 + a_2).$$

* These Transactions, vol. 8 (1907), p. 209.

† These Transactions, vol. 14 (1913), p. 310.

To verify Theorem III for the invariants of f_2, we compute the values of q, Δ, J, B and Γ for the different classes and find that

Class	f_2	q	Δ	J	B	Γ
1	0	0	0	0	0	0
2	x^2	2	0	0	0	1
3	$-x^2$	1	0	0	0	2
4	x^2+y^2	0	2	1	0	0
5	$2xy$	0	1	0	0	0

Hence, whenever the a's are in the field, $\Gamma \equiv -q$, $J \equiv 2\Delta^2 + \Delta$, $B \equiv 0$.

Dickson† has also shown that a fundamental set of modular covariants consists of

$$q,\ \Delta,\ L,\ Q,\ f_2,\ f_4 = a_0 x_1^4 + a_1(x_1^3 x_2 + x_1 x_2^3) + a_2 x_2^4,$$

$$C_1 = (a_0^2 a_1 - a_1^3)x_1^2 + (a_0 - a_2)(a_1^2 + a_0 a_2)x_1 x_2 + (a_1^3 - a_1 a_2^2)x_2^2,$$

$$C_2 = (a_0^2 + \Delta)x_1^2 + a_1(a_0 + a_2)x_1 x_2 + (a_2^2 + \Delta)x_2^2.$$

Glenn* later showed that a fundamental set of formal covariants consists of eighteen forms:

$$\Delta,\ J,\ B,\ \Gamma,\ L,\ Q,\ f_2,\ f_4,\ f_6 = a_0 x_1^6 + 2a_1 x_1^3 x_2^3 + a_2 x_2^6,$$

$$C_1,\ C_2,\ C_4 = (a_0^2 + \Delta)x_1^4 + 2a_1(a_0 + a_2)(x_1^3 x_2 + x_1 x_2^3) + (a_2^2 + \Delta)x_2^4,$$

$$\zeta_4 = (a_0^2 a_1 - a_1^3)x_1^4 - (a_0 - a_2)(a_1^2 + a_0 a_2)(x_1^3 x_2 + x_1 x_2^3) + (a_1^3 - a_1 a_2^2)x_2^4,$$

$$-\zeta_6 = (a_0^2 a_1 - a_1^3)x_1^6 + (a_0 - a_2)(a_1^2 + a_0 a_2)x_1^3 x_2^3 + (a_1^3 - a_1 a_2^2)x_2^6,$$

$$\phi_2 = a_0^3 x_1^2 + 2a_1^3 x_1 x_2 + a_2^3 x_2^2,$$

$$\phi_4 = a_0^3 x_1^4 + a_1^3(x_1^3 x_2 + x_1 x_2^3) + a_2^3 x_2^4,$$

$$\vartheta_2 = (a_0 a_1^3 - a_0^3 a_1)x_1^2 + (a_0 a_2^3 - a_0^3 a_2)x_1 x_2 + (a_1 a_2^3 - a_1^3 a_2)x_2^2,$$

$$\xi_2 = (a_0^2 a_1^3 - a_0^4 a_1)x_1^2 + (a_0^3 a_1^2 + 2a_0^4 a_2 + 2a_0 a_1^4 + a_1^4 a_2 + 2a_0^3 a_2^2 + a_0^2 a_2^3 + 2a_1^2 a_2^3 + a_0 a_2^4)x_1 x_2 + (a_1 a_2^4 - a_1^3 a_2^2)x_2^2.$$

Of the formal covariants not in the fundamental set of modular covariants, $f_6 \equiv f_2^3$, $C_4 \equiv (\Delta + 1)f_2^2 + C_1^2$, $-\zeta_6 \equiv C_1^3$, $\zeta_4 \equiv C_1 C_2$, $\phi_2 \equiv f_2$ and $\phi_4 \equiv f_4$ whenever the a's are in the field. Finally, $\vartheta_2 \equiv \xi_2 \equiv 0$ whenever the a's are in the field. Thus the theorem is verified.

* These Transactions, vol. 20 (1919), pp. 154–168. For convenience, we have used C_4 instead of D_4, which is legitimate, since $D_4 = C_4 - f_2^2$.

The writer has also applied the theorem to the set of fundamental formal covariants of the binary cubic, modulo 2, which has been found by Glenn.* We leave the details to the reader.

9. A general application. Theorem III enables us at once to narrow down the question of the finiteness of formal covariants of a system S of forms with respect to the Galois field $GF[p^n]$. There is no loss of generality to consider only homogeneous formal covariants and invariants.

Let Q_1 be a homogeneous formal invariant of lowest degree q which is $\equiv 1$ whenever the coefficients are in the field, but not all zero. Now there are polynomials in the coefficients which are $\equiv 1$ for all sets of values of coefficients in the field not all zero and which are formally invariant. For let $I_1, I_2, \cdots, I_\nu$ be the characteristic modular invariants for all classes except the one in which all forms are identically zero, and let $I_1', I_2', \cdots, I_\nu'$ be formal invariants of lowest degree which are congruent to $I_1, I_2, \cdots, I_\nu$ respectively whenever the coefficients are in the field. Let the degrees of $I_1', I_2', \cdots, I_\nu'$ be $d_1, d_2, \cdots, d_\nu$ respectively. Then, if D be the least common multiple of the d's,

$$Q' = I_1'^{\delta_1} + I_2'^{\delta_2} + \cdots + I_\nu'^{\delta_\nu} \qquad (\delta_i = D/d_i)$$

is a homogeneous formal invariant which is congruent to 1 whenever the coefficients are marks of the field not all zero.

Now let C be any modular covariant of the system S of order ω, and let C_1 be a formal covariant which is congruent to C whenever the coefficients are in the field; moreover, let C_1 be such a covariant of order ω and of lowest degree in the coefficients. Also, let $C_1, C_2, \cdots, C_k$ be formal covariants of order ω which are congruent to C for all sets of the coefficients in the field and which are of all possible degrees ranging from c_1 up to but not including $c_1 + q$. Let their degrees be respectively $c_1, c_2, \cdots, c_k$.

If K_i be any formal covariant of order ω which is congruent to C whenever the coefficients are in the field, but not all zero and which is of degree c_i, then K_i is identically equal to $C_i +$ (a formal covariant which is congruent to zero whenever the coefficients are in the field).

Now $C_1 Q_1, \cdots, C_k Q_1$ are all formal covariants which are congruent to C for all sets of coefficients in the field. The degrees of $C_1 Q_1, \cdots, C_k Q_1$ are $c_1 + q, c_2 + q, \cdots, c_k + q$ and range from $c_1 + q$ up to but not including $c_1 + 2q$. If there be any formal covariants of order ω which are congruent to C and which are of a degree different from $c_1 + q, c_2 + q, \cdots, c_k + q$ and yet whose degree lies between $c_1 + q$ and $c_1 + 2q$, select one representative covariant of each such possible degree. Let these additional covariants be denoted by $A_1, \cdots, A_l$. Since there is only a finite number of integers

*These Transactions, vol. 19 (1918), pp. 109–118. The invariants had already been found by Dickson (*Madison Colloquium Lectures*, p. 56).

between $c_1 + q$ and $c_1 + 2q$, there is only a finite number of such additional representative covariants.

Thus if K' be any formal covariant of order ω which is congruent to C whenever the coefficients are in the field and which is of a degree between $c_1 + q$ and $c_1 + 2q$, then K' is identically equal to (some C_i) $\times$ Q_1 + (a formal covariant which is congruent to zero whenever the coefficients are in the field); or K' is identically equal to (some A_i) + (a formal covariant which is congruent to zero whenever the coefficients are in the field).

Proceed similarly with the formal covariants of order ω which are congruent to C whenever the coefficients are in the field and which are of a degree between $c_1 + 2q$ and $c_1 + 3q$; between $c_1 + 3q$ and $c_1 + 4q$; etc.

Thus we have a set of those formal covariants of order ω which are congruent to C whenever the coefficients are in the field which is such that there is one and only one such covariant for each such possible degree. Moreover, in view of the preceding argument and in view of the fact that there is only a finite number of additional representative covariants (such as $A_1, \cdots, A_l$, etc.), all the representative covariants of order ω which are congruent to C are expressible as the product of a power of Q_1 by one of a finite number of these representative covariants.

Combining these results, we see that all formal covariants of order ω which are congruent to C for all sets of the coefficients in the field are expressible in terms of Q_1, a finite number of such covariants, and the formal covariants of order ω which are congruent to zero for all sets of the coefficients in the field.

By a similar line of reasoning, we can deduce that all formal covariants of degree d which are congruent to C whenever the coefficients are in the field are expressible in the form (one of a finite subset of such covariants) $\times$ (a power of Q) + (a formal covariant which is congruent to zero whenever the coefficients are in the field).

If we now combine these two results, and make use of the fact* that the set of all modular covariants possesses the finiteness property, we then prove by induction

THEOREM IV. *The set of all formal covariants of a system S of binary forms with respect to the Galois field $GF[p^n]$ is of such a nature that every such covariant is expressible as a polynomial in Q, Q_1, members of a finite subset of formal covariants of S and the irreducible covariants which are congruent to zero whenever the coefficients are in the field.*

Thus we reach the conclusion that the set of all formal covariants of a system S possesses the finiteness property if and only if the set of all irreducible covariants which are congruent to zero for all sets of coefficients in the field possesses the finiteness property.

MOUNT HOLYOKE COLLEGE,
SOUTH HADLEY, MASS.

* See section 2 of this paper.