A SYMBOLIC THEORY OF FORMAL MODULAR COVARIANTS*

BY

OLIVE C. HAZLETT

PART I. INTRODUCTION

1. **Prologue.** Thus far, very little has been published on the general theory of formal modular invariants or covariants. Workers have, on the whole, obtained results for special, more or less isolated, cases; and although some beautiful and important general theorems have been proved, they are more or less unrelated. This is, of course, only natural in any division of knowledge in its formative state.

Nevertheless, no worker in the field could fail to be conscious of a certain uniformity common to the special cases that have been studied in detail; though (alas!) this uniformity usually appeared to be broken ruthlessly in the next case studied. This breaking of an apparent law signified, however, merely that we did not know these special cases with a sufficient thoroughness of illuminating detail, or were trying unwittingly to make the laws conform to certain standards, unconsciously preconceived. This latter handicap was laid on us naturally enough by our thorough knowledge of algebraic invariants and the fact that this newer kind of covariants is, in many ways, strikingly like the older, classic covariants, though so tantalisingly different.

Their similarity and their difference show themselves in the very beginning of the study: in the definitions, in the simplest examples. Perhaps the differences that first come to mind are those which are inherent in the fields of definition, which, in the case of classic covariants, is the field of reals or ordinary complex numbers and, in the case of modular covariants, is a Galois field, $GF[p^n]$, of order p^n. These differences are too obvious to mention in detail, but one who has studied the beautiful proofs given by the old masters of invariant theory has been forced to the conclusion that most of the proofs seemed to use the properties of a field of characteristic zero, not in some accidental manner, but rather in veriest necessity.

Growing from the surface differences between the two fields are two very important distinguishing characteristics of the two kinds of covariants. It

* Part II was presented to the Society, September 7, 1920; Part III, December 28, 1921; Parts IV and V, December 27, 1922.

The reading of the literature in connection with this paper was much facilitated by the purchase of books with a grant made by the American Association for the Advancement of Science and this help is herewith gratefully acknowledged.

is well known that an algebraic covariant is necessarily such that all of its terms have the same weight—i.e., it is isobaric; but a modular covariant is not necessarily isobaric. Nevertheless, although its terms are not in general of exactly the same weight, their weights can differ at most by multiples of $p^n - 1$. Moreover, if two classic invariants are identical in value for all marks of the field, they are necessarily identical in form, and conversely; whereas, if two formal modular invariants are identical for all marks of the field of definition, they are not necessarily identical in form. Nevertheless, although two such invariants can be of different degree and appear quite different in form at a casual glance, yet they necessarily have in common certain fundamental characteristics.* There are other differences that will occur to any worker in the field, but I think that I have mentioned the most refractory.

As indicated above, in spite of the great differences between the algebraic covariants and formal modular covariants, there are certain fundamental likenesses which are more easily sensed than they are analyzed. A feeling that there is some theory which underlies all the special cases, and yet which is comparatively simple, made the writer try to crystallize this theory into words.

In the spring of 1918, came the feeling that the theory of formal modular covariants of a binary form, f, for the field $GF[p^n]$, must be, in essentials, equivalent to the theory of simultaneous algebraic covariants of f and certain other forms obtained from f by replacing the coefficients of f by their respective p^nth powers. This is natural enough, since these powers of the coefficients of f are cogredient with the coefficients of f for the transformations of the group used, and this is the only way in which a formal modular covariant differs from an algebraic covariant of f. Then there appeared other indications that there is an intimate relation between formal modular covariants of f and algebraic covariants of a system of forms consisting of f and related forms. This paper is an attempt to put in systematic form the theorems which emerged when these eventually crystallized.

2. **Summary of literature.** Let

$$f(a; x) = a_0 x^m + a_1 x^{m-1} x_2 + \cdots + a_{m-1} x_1 x^{m-1} + a_m x^m$$

be a binary form and let G be a group of linear transformations

$$x_i = \xi_i x_1' + \eta_i x_2' \qquad (i = 1, 2) \tag{1}$$

whose coefficients, the ξ's and η's, are in the field F. If $I(a)$ be a polynomial in the a's which, under all transformations of the group, is transformed into $I(a')$ such that

$$I(a') = D^w I(a) \quad \text{(in the field)} \tag{2}$$

* Some of these characteristics are indicated in a paper by Hazlett, these Transactions, vol. 22 (1921), pp. 144–157, especially p. 145.

where

$$D = (\xi\eta) = \xi_1 \eta_2 - \xi_2 \eta_1,$$

then I is said to be an invariant of f under the group G. Similarly, if $C(a; x)$ is a polynomial in the a's and the x's which, under all transformations of the group G, is transformed into $C(a'; x')$ such that

$$C(a'; x') = D^w C(a; x) \quad \text{(in the field)}, \tag{3}$$

then C is said to be a covariant of f under the group G. Also, we speak of invariants and covariants of a system S of binary forms f_i.

When the field of definition, F, is the field of all reals or the field of all ordinary complex numbers, the covariants of S are the ordinary covariants of S of the classic invariant theory, with which are associated the names of Cayley, Sylvester, Hermite, Aronhold, Gordan, Clebsch and Hilbert.

When the field of definition, F, is the Galois field, $GF[p^n]$, of order p^n, the covariants of S are called modular covariants. Here the ξ's and η's are marks of the Galois field, $GF[p^n]$, of order p^n* defined by the prime p and an algebraic equation, $P(X) = 0$, of degree n; and thus (2) and (3) are congruences, reduced modulis p and $P(X)$. This means that, in (2) and (3), the left member is identical with the right member if we replace the p^nth power of ξ_i and of η_i by ξ_i and η_i respectively, in view of Galois' generalization of Fermat's theorem.† For a modular field there are two different types of covariants. If the coefficients of the forms (the a's) range over the marks of $GF[p^n]$, and if (2) and (3) are congruences which are true if Fermat's theorem is applied, not only to the ξ's and η's, but also to the a's, then the covariants are called simply *modular covariants*. If, on the other hand, the a's are independent variables, Fermat's theorem does not apply to them; and hence, in (2) and (3), the left member is understood to be identical with the right member without any reduction in the exponents of the a's. Such covariants are called *formal*

* Let p be any prime and let $P(X) = 0$ be any algebraic equation of degree n which has its coefficients integers reduced modulo p and which is irreducible, modulo p. Then, if we reduce any polynomial in X modulis p and $P(X)$, we obtain a polynomial of the form

$$M(X) = c_{n-1} X^{n-1} + c_{n-2} X^{n-2} + \cdots + c_1 X + c_0$$

where each of the c's is an integer of the set $0, 1, \cdots, p-1$. The totality of all polynomials congruent modulis p and $P(X)$ to the same $M(X)$ is said to form a class of residues. Since there is a class of residues for each set of values for the c's, there are p^n such classes. The totality of the classes of residues are closed under addition, subtraction, multiplication and division (provided the divisor is not zero) and so constitute a field containing p^n marks or elements. Any two such fields are the same for a given p and a given n. This is called a Galois field of order p^n and is denoted by $GF[p^n]$. Moreover, any finite field is simply isomorphic with a Galois field.

† If a is any mark of $GF[p^n]$, defined by p and $P(X)$, then $a^{p^n} \equiv a$ (modd p, $P(X)$). See any standard work on Galois fields, such as Dickson, *Linear Groups*, Teubner, 1901, p. 11; Serret, *Cours d'Algèbre Supérieure*, vol. 2, p. 180.

modular covariants. If the covariant is independent of the variables, it is called a *modular invariant* or a *formal modular invariant* according as the a's are marks of the field or independent variables.

Although Hurwitz introduced the notion of formal modular invariants in connection with the determination of the number of solutions of higher congruences,* Dickson discovered them independently four years later from a different point of view.† Practically all important results in the theory are due to Dickson.‡

Clearly, every formal modular covariant of a system S is a modular covariant of S, though not every modular covariant of S is also a formal modular covariant of S. For a modular invariant, I, of S is concerned solely with the values of I for the different sets of values of the a's in the field of definition, whereas a formal modular invariant of S is concerned not only with the values but also with the form of I. This statement has to be modified somewhat for covariants that are not invariants, since, in (2) and (3), the left member is the same as the right member in a purely formal sense as far as the x's are concerned, for both kinds of covariants. For example, if a is any one of the coefficients of f, then $a^{p^n} - a$ always has the value zero when a is a mark of $GF[p^n]$ and hence it is a modular invariant of f; but it is not a formal modular invariant, since it is changed in form if we interchange x_1 and x_2. To take a less trivial example,

$$q = (a + c)(b^2 + ac - 1)$$

is a modular invariant of $f = ax_1^2 + 2bx_1x_2 + cx_2^2$, mod 3, but is not a formal invariant, since $a + c$ goes into $-a - b + c$ under the transformation $x_1 = x_1' + x_2', x_2 = x_2'$.

In 1909,§ Dickson studied modular invariants from a different point of view and introduced the notion of classes of forms. This enables one to see to the very heart of the theory and the finiteness theorem follows almost directly from the definition. Later,|| he proved the finiteness theorem for modular covariants.

* *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.

‡ Anyone wishing to gain familiarity with this beautiful theory should read the article by Hurwitz mentioned above and Dickson's papers, of which the most fundamental are I. *General theory of modular invariants*, these Transactions, vol. 10 (1909), pp. 123–158; II. *Proof of the finiteness of modular covariants*, ibid., vol. 14 (1913), pp. 299–310. Also one should read the brief but important paper by Miss Sanderson, *Formal modular invariants with application to binary modular covariants*, these Transactions, vol. 14 (1913), pp. 489–500. All results obtained up to 1914 are summarized in Dickson's *Madison Colloquium Lectures*, and all essential results published up to August, 1922, are summarized briefly in Chapter 19 of his *History of the Theory of Numbers*, vol. 3.

§ Dickson, I.

|| Dickson, II.

There is, however, an intimate relation between modular invariants and formal modular invariants. For Miss Sanderson's theorem* tells us that, corresponding to any modular invariant, i, of a system S under any group G of linear transformations with coefficients in $GF[p^n]$, there is 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 S. This enabled her to construct modular covariants of a system S of binary forms, f_i, from the modular invariants of another system S', consisting of the forms f_i and an additional linear form with coefficients x_2 and $-x_1$. Moreover, every modular covariant of S is a polynomial in the universal covariant, $L = x_1^{p^n} x_2 - x_1 x_2^{p^n}$, and the modular covariants obtained in the manner indicated by Miss Sanderson's theorem.† Since every algebraic covariant of S is obtained from the algebraic invariants of S' without the need of any additional covariant, analogous to L, this result shows one of the fundamental differences between algebraic and modular covariants.

In connection with this last remark, several minor results are of interest, as they point the way toward more general results. In 1920, it was shown that, for the field $GF[p^n]$ with $p \neq 2$, every modular covariant of a binary form, f, whose degree is not divisible by p, is expressible as a rational function of the universal modular covariants, L and Q, and of algebraic covariants of f. For formal modular covariants of f, there is a theorem which is more complicated in statement but similar in essence.‡ Then, in 1922, W. L. G. Williams announced that every formal modular seminvariant of f (aside from a power of a_0) is a polynomial in the algebraic protomorphs and in

$$\beta = a_1^p - a_1 a_0^{p-1}$$

for $GF[p]$ when the form f is such that binomial coefficients can be used.§ He also proved the analogous theorem for formal seminvariants of two or more binary forms. In this latter, it is interesting to note that, to a fundamental set of algebraic protomorphs, it is necessary to adjoin only one new seminvariant, namely, one of the same type as β but formed for any one of the forms f_i. It will be seen that these results indicate relations between modular covariants and algebraic covariants, in spite of their superficial differences.

3. **Summary of this paper.** We first explain a symbolic notation for formal modular covariants which is like that generally used for algebraic covariants in most respects, but is (necessarily) different from the latter in one essential.

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

† Hazlett, *A theorem on modular covariants*, these Transactions, vol. 21 (1920), pp. 247–254.

‡ Hazlett, *Associated forms in the general theory of modular covariants*, American Journal of Mathematics, vol. 43 (1921), pp. 194–196.

§ *Fundamental systems of protomorphic formal modular seminvariants of binary forms*, read before the Society (Rochester, N. Y.), Sept. 8, 1922. I saw this article in MS. after announcing to the Society (Toronto), on December 28, 1921, the results of Part III of this paper.

This notation, however, has the advantage that it can be used for both algebraic covariants and formal modular covariants; and thus, by its use, the proof of every theorem in this paper is such that it applies both to the modular and the non-modular cases. To help the reader appreciate the diversity of these two interpretations of this theory, the more important theorems are applied to a number of special cases.

As in the symbolic theory of algebraic covariants, it is readily seen that all formal modular covariants are polynomials in a finite number of symbolic expressions having the invariant property. Then are proved several other elementary theorems which assume a simple and familiar form for algebraic covariants, but which, for formal modular covariants, assume a form rather strikingly different.

It is then shown that every isobaric formal modular covariant, C, of the system S is congruent, in the field, to a function of the coefficients of S which is (in a certain general sense) an algebraic covariant of S. When, however, C is not isobaric, it is not congruent to an algebraic covariant of S; but it is, nevertheless, congruent to an algebraic covariant of an enlarged system, S', consisting of the forms of S and other forms obtained from the forms of S by replacing the coefficients of S by their p^nth powers. By various devices, there are expressed in symbolic form the formal modular invariants of a fundamental set for the cubic, modulo 2, and for the quadratic, modulo 3; and the above theorems are verified.

Finally, by using the same theorems, we prove that the set of all formal modular covariants of any binary system, S, with respect to the Galois field, $GF[p^n]$, is such that (1) all syzygies among them are consequences of a finite number of such syzygies; and (2) all formal modular covariants are expressible as polynomials in a finite number of such covariants.

Part II. Symbolic notation

4. **Explanation of the notation.** As in the theory of algebraic covariants, formal modular covariants of a binary form, f, assume a form which is both simple and elegant when the form f is expressed as a product of symbolic linear factors. In the theory of algebraic covariants, it is customary to express a binary form f of degree m as a symbolic mth power; but, for reasons which were explained elsewhere in detail,* it is not possible to express the general form f of degree m as a symbolic mth power and then express all formal modular covariants by means of these symbols for the general Galois field.

For this reason, represent

$$f = a_0 x_1^m + a_1 x_1^{m-1} x_2 + \cdots$$

* *New proofs of certain finiteness theorems in the theory of modular covariants*, these Transactions, vol. 22 (1921), pp. 152–153.

as

$$f = \pi\alpha_x = \pi(\alpha_1 x_1 + \alpha_2 x_2) = (\alpha_1 x_1 + \alpha_2 x_2)(\beta_1 x_1 + \beta_2 x_2) \cdots$$

where it is understood that there are m symbolic factors which are symbolically distinct, and consider its formal modular covariants under the group of transformations (1) where the ξ's and η's are any marks of the Galois field, $GF[p^n]$, of order p^n such that the determinant is not zero in the field. Then, as has been proved elsewhere,* every rational integral covariant (both classic and modular) of f is a polynomial in the symbols $\alpha, \beta, \cdots$ and in the x's. The converse is also true; though, in order that a polynomial in the x's and in the symbols be rational in the a's, (i) it must be symmetric in the m pairs (α_1, α_2), $(\beta_1, \beta_2), \cdots$ and such that each term contains as many α's as β's, as many β's as γ's, etc.; or (ii) it must be a sum of a number of expressions described under (i). Similar remarks apply to covariants of several binary forms. For convenience, any polynomial in the x's and the symbols which has the invariantive property under a transformation of the group will be called a symbolic covariant, even if it do not satisfy the conditions that it be rational in the a's.

5. **Fundamental set of symbolic covariants.** Early in the symbolic theory of algebraic covariants, it is proved that all algebraic invariants are expressible as polynomials in a finite number of symbolic invariants of the type

$$(\alpha\beta) = \alpha_1\beta_2 - \alpha_2\beta_1.$$

Similarly, all algebraic covariants are expressible as polynomials in a finite number of symbolic covariants of the type $(\alpha\beta)$ and $\alpha_x = \alpha_1 x_1 + \alpha_2 x_2$. For formal modular covariants we have a similar theorem, though we have to use new types of symbolic covariants.

For simplicity, we shall first consider covariants of a single form, $f = \pi\alpha_x$. Now it is known that the pair (α_1, α_2) is pseudo-cogredient with $(x_2, -x_1)$.† Accordingly, any formal modular covariant may be regarded, for any purpose not involving the notions of weight or index, as if it were actually an invariant of $m+1$ cogredient pairs, consisting of the pairs of symbols and the pair $(x_2, -x_1)$. But it is known that the formal modular invariants of a number of cogredient points have the finiteness property.‡ Notice that this argument applies equally well to a system of binary forms, and thus we have

THEOREM I. *All rational integral formal modular covariants of a system of binary forms,* $f_i = \pi(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_x\beta_x \cdots$, *with respect to the Galois*

* Preceding reference, top of p. 153.

† That is, the two pairs are cogredient aside from a multiplicative factor which is a power of the determinant of the transformation.

‡ F. B. Wiley, *Proof of the finiteness of the modular covariants of a system of binary forms and cogredient points*, these Transactions, vol. 15 (1914), pp. 431–438.

field $GF[p^n]$, of order p^n, are polynomials in a finite number of symbolic covariants which are polynomials in the x's and in the α's, β's, $\cdots$.

6. **Illustration of Theorem I.** Dickson* has shown that all formal modular invariants of the binary quadratic $f = a_0 x_1^2 + 2a_1 x_1 x_2 + a_2 x_2^2$, modulo 3, are polynomials in

$$\Delta = a_1^2 - a_0 a_2, \qquad J = a_0 \gamma_0 = a_0 (a_0 + a_1 + a_2)(a_0 + 2a_1 + a_2) a_2,$$
$$B = \beta\gamma_1 \equiv a_1 (a_1^2 - a_0^2)(a_2 - a_0)(a_2^2 - a_1^2),$$
$$\Gamma = (a_0 + a_2)(2a_0 + 2a_1 + a_2)(2a_0 + a_1 + a_2).$$

If we express f in symbolic form (§ 4) as $f = (\alpha_1 x_1 + \alpha_2 x_2)(\beta_1 x_1 + \beta_2 x_2)$, then $a_0 = \alpha_1\beta_1$, $a_1 \equiv -(\alpha_1\beta_2 + \alpha_2\beta_1) \mod 3$, $a_2 = \alpha_2\beta_2$. Hence it is readily seen that

$$\Delta \equiv (\alpha\beta)^2, \qquad J = (\alpha^3\alpha)(\beta^3\beta),$$
$$B \equiv \sum (\alpha^3\beta)^2 (\beta^3\beta),$$
$$\Gamma \equiv -N_1 \pmod 3,$$

where

$$N_1 = [(\alpha^3\beta)^2 (\beta^3\beta) - (\beta^3\alpha)^2 (\alpha^2\alpha)]/(\alpha\beta)^3$$

is one of a fundamental set of formal invariants of the pairs (α_1, α_2) and (β_1, β_2) and is an integral function of the α's and β's. Thus Theorem I is verified for this case. Note, also, that the rational invariants of f are expressible as rational functions in the determinantal symbolic invariants, $(\alpha\beta)$, $(\alpha^3\beta)$, $(\alpha\beta^3)$, $(\alpha^3\alpha)$, $(\beta^3\beta)$.

Part III. Relation between classic and modular covariants

7. **Two kinds of congruences.** In the following sections, we shall frequently have to distinguish between two kinds of congruences, identical congruences and residual congruences. Two polynomials $\phi_1(x)$ and $\phi_2(x)$, with integral coefficients, are said to be *residually congruent* with respect to the field $GF[p^n]$ if $\phi_1(x) \equiv \phi_2(x)$ whenever x is any mark of the field; if, however, $\phi_1(x) \equiv \phi_2(x)$ when x is any number whatsoever, then $\phi_1(x)$ is said to be *identically congruent* to $\phi_2(x)$. For example, $x^{p^n} \equiv x$ is a residual congruence, and $(p+1)x \equiv x$ is an identical congruence.

Moreover, if ϕ_1 and ϕ_2 are polynomials in two sets of variables, the x_i and y_i, then we might have a congruence which is residual as far as the x's are concerned, but which is identical as far as the y's are concerned. For example, when C is a modular covariant, (3) in § 2 is a residual congruence as far as the a's are concerned but is an identical congruence as far as the x's are concerned. If, on the other hand, C is a formal covariant, then (3) is an identical congruence with respect to both the a's and the x's. In each case, however, (3)

* *Madison Colloquium Lectures*, p. 42.

is a residual congruence with respect to the ξ's and η's. Since there is no simple notation which will indicate those variables with respect to which a congruence is residual, we shall indicate them in words directly after each congruence.

8. **Manner in which covariants are transformed.** An algebraic covariant, C, is usually defined as a function such that its transform, C', is given by the formula $C' = D^w C$ where D is the determinant of the general transformation of the group; but it is often defined as a function such that $C' = MC$ where M depends merely on the coefficients of the transformation, and the multiplier is then proved to be a power of D. Now it has been customary thus far to define a formal modular covariant in a manner analogous to the first of these methods, but, in this paper, we shall use the second definition and then prove it is equivalent to the first.

Although the definition of a formal modular covariant says nothing explicitly about the nature of its transform except for values of the ξ's and η's in the field, let us see if this indirectly imposes any restriction on the actual form of the transform before we reduce the exponents of the ξ's and η's by Fermat's theorem. For example, under the transformation (1), $L_1 = \alpha_1^{p^n} \alpha_2 - \alpha_1 \alpha_2^{p^n}$ is replaced by the same function of the primed letters, which is identically equal to

$$D_1 \alpha_1^{p^n+1} + D_2 \alpha_1^{p^n} \alpha_2 - D_3 \alpha_1 \alpha_2^{p^n} + D_4 \alpha_2^{p^n+1},$$

where

$$D_1 = \xi_1^{p^n} \eta_1 - \xi_1 \eta_1^{p^n}, \qquad D_2 = \xi_1^{p^n} \eta_2 - \eta_1^{p^n} \xi_2,$$
$$D_3 = \xi_1 \eta_2^{p^n} - \xi_2^{p^n} \eta_1, \qquad D_4 = \xi_2^{p^n} \eta_2 - \xi_2 \eta_2^{p^n}.$$

It will be observed that each D_i is a formal modular invariant of the two pairs (ξ_1, η_1) and (ξ_2, η_2) when they are transformed cogrediently, and that $D_1 \equiv D_4 \equiv 0$, $D_2 \equiv D_3 \equiv D$, when the ξ's and η's are all in the field.

Let C be any formal covariant of the system S. Then, under (1), C formally —i.e., before any reduction is made modulo p—goes into

$$C(a'; x') = \Sigma D_i(\xi, \eta) P_i(a; x) \tag{4}$$

where each D_i* and each P_i is a polynomial in its arguments. If (1) is followed by the transformation

$$x_i' = e_i x_1'' + f_i x_2'' \qquad (i = 1, 2),$$

where

$$\Delta = e_1 f_2 - e_2 f_1 \not\equiv 0 \quad \text{(in the field)},$$

this is equivalent to applying to the original forms of S the single transformation

$$x_i = \xi_i' x_1'' + \eta_i' x_2'' \qquad (i = 1, 2), \tag{1'}$$

* These multipliers, D_i, will depend on the covariant, C. When C is L, then the D's are as given in the preceding paragraph.

where the two pairs (ξ_1', η_1') and (ξ_2', η_2') are obtained respectively from the pairs (ξ_1, η_1) and (ξ_2, η_2) by applying the transformation of matrix

$$\begin{pmatrix} e_1 & e_2 \\ f_1 & f_2 \end{pmatrix}. \tag{5}$$

Accordingly, if in (4) we replace the a' and the x' by the corresponding a'' and x'', and apply the transformation (5) to the pairs (ξ, η), then we get an equation of the type (4) but formed for the new transformation (1'). Thus, before any reduction is made modulo p,

$$C(a''; x'') = \Sigma D_i(\xi', \eta') P_i(a; x); \tag{4'}$$

and also

$$C(a''; x'') \equiv MC(a'; x') \quad \text{(in the field)}, \tag{6}$$

whenever the e's and f's are in the field. Both (4) and (4') are ordinary equations, but (6) is a congruence in the field, being an identical congruence with respect to the a's and x's. Combining these, we have

$$D_i(\xi', \eta') \equiv MD_i(\xi, \eta)$$

as an identical congruence in the ξ's and η's. Hence we have proved

THEOREM II. *If C is any formal modular covariant of a system, S, of binary forms with respect to the Galois field $GF[p^n]$, of order p^n, then under any linear transformation* (1) *of the group, C is formally replaced by an expression of the form $\Sigma D_i(\xi, \eta) P_i(a; x)$ where each P_i is a polynomial in the a's and x's and each D_i is a formal modular invariant of the two cogredient pairs (ξ_1, η_1) and (ξ_2, η_2).*

In a later section, we shall prove that each D_i which is not congruent to zero when the ξ's and η's are in the field is congruent to a power of D (the determinant of the transformation) whenever the ξ's and η's are marks of the field. For isobaric covariants, see Lemma 4 (§ 10); for pseudo-isobaric covariants, see § 16.

Note that this proof holds equally well for classic covariants, and thus, both for classic covariants and modular covariants, the theory of covariants of a system of binary forms has its foundations in the theory of invariants of two cogredient points. The essential differences between the modular and classic theories are, accordingly, associated with two facts: (1) in the classic case, all invariants of two cogredient points are polynomials in one invariant, the determinant $\xi_1 \eta_2 - \eta_1 \xi_2$; whereas, in the modular case, several other types arise; (2) in the classic case there is no invariant, other than zero itself, which vanishes whenever the ξ's and η's are in the field; whereas, in the modular case, there are invariants of the two pairs which are not identically congruent to zero and yet vanish whenever the ξ's and η's are in the field. From (1)

we see why the transform of a modular covariant is not in general identically a multiple of the original covariant, and from (2) we see why the transform of a modular covariant in general contains terms having no counterpart in the original covariant, before Fermat's theorem is applied. Both remarks are illustrated by L at the beginning of this section.

9. **Remarks on isobarism.** Another fundamental difference between algebraic and modular covariants was mentioned in the introduction and will now be discussed briefly. An algebraic covariant is always isobaric—i.e., all its terms have the same weight.* In fact, an elementary way of determining classic invariants of $f(a; x)$ is to write down a general linear combination of all possible terms having the same degree in the a's and the same weight and then determine what the coefficients of these terms must be in order that the expression be an invariant of f.† But a modular covariant is not in general isobaric, though the weights of any two of its terms can differ at most by a multiple of $p^n - 1$.

These differences are well shown by the algebraic invariants of

$$f = a_0 x_1^2 + 2a_1 x_1 x_2 + a_2 x_2^2$$

and the formal invariants of the same form, modulo 3. All algebraic invariants of f are polynomials in‡

$$\Delta = a_1^2 - a_0 a_2,$$

and the modular invariants are polynomials in Δ, J, B and Γ (see § 6). It will be noticed that of the modular invariants, only one is isobaric and that is the one which is also an algebraic invariant of f; the weights of any terms of the others differ at most by multiples of $p^n - 1 = 2$.

Isobaric covariants

10. **Preliminary lemmas.**

Lemma I. *Let C be a formal modular covariant of a system, S, of binary forms and a number of cogredient points under a group G with coefficients in the Galois field $GF[p^n]$, of order p^n. Then, if C is isobaric, it is invariant modulo p under any transformation* (1) *where the ξ's and η's are independent variables.*

For, since C is invariant modulo p under the transformation

$$x_1 = x_1' + x_2',$$
$$x_2 = \quad x_2',$$

* In the binary form $f = a_0 x_1^m + a_1 x_1^{m-1} x_2 + \cdots + a_m x_2^m$, the weight of the coefficient a_i is defined to be i, and the variables x_1 and x_2 are assigned the weights 1 and 0 respectively. See any standard book on algebraic invariants, such as Elliott, *Algebra of Quantics*, first edition, pp. 36, 48; Dickson, *Algebraic Invariants*, pp. 31, 38.

† For examples, see Elliott, pp. 125–126; Dickson, pp. 36–37.

‡ Dickson, *Algebraic Invariants*, pp. 48, 84; Elliott, loc. cit., pp. 98–99.

and is isobaric, it is formally invariant, modulo p, under any transformation

$$\begin{aligned} x_1 &= x_1' + kx_2', \\ x_2 &= \quad kx_2', \end{aligned}$$

where k is a general non-zero scalar. Again using the isobarism, it follows from this last that C is invariant modulo p under the transformation

$$\begin{aligned} x_1 &= x_1' + kx_2', \\ x_2 &= \quad x_2'. \end{aligned} \tag{7}$$

Also, C satisfies the condition for covariancy under the transformation

$$\begin{aligned} x_1 &= x_2', \\ x_2 &= x_1', \end{aligned} \tag{8}$$

without using Fermat's theorem. Now, using (7) and (8) in conjunction with the isobarism, we prove the lemma.

LEMMA II. *If a formal modular covariant is isobaric, then every one of its factors is necessarily isobaric.*

For, let C_1 and C_2 be any two formal modular covariants which are not isobaric. Then the totality of terms in $C_1 C_2$ which have the greatest (least) weight is simply the product of the terms of C_1 which have the greatest (least) weight by the terms of C_2 which have the greatest (least) weight. The lemma follows at once.

LEMMA III. *When a formal modular covariant C is isobaric, each of the multipliers $D_i(\xi, \eta)$ of Theorem* II *is also isobaric.*

For, by Theorem II, under any transformation (1), we have (3) holding formally as to the a's, x's, ξ's and η's. Since C is isobaric, it is invariant whenever x_1 or x_2 is multiplied by ρ, where ρ is any non-zero scalar. This means that the right member of (3) is homogeneous in ξ_1 and η_1, and also in ξ_2 and η_2. Being also invariant whenever we interchange the x's, the right member of (3) must be of the same degree in ξ_1 and η_1 that it is in ξ_2 and η_2. Hence, if w_1, w_2, w_3 and w_4 are the degrees of any term of some D_i in ξ_1, η_1, ξ_2 and η_2, respectively, then $w_1 + w_2 = w_3 + w_4$. Similarly, since C is invariant formally whenever x_1' or x_2' is multiplied by ρ, we have $w_1 + w_3 = w_2 + w_4$. Therefore $w_1 = w_4$ and $w_2 = w_3$.

LEMMA IV. *When a formal modular covariant, C, is isobaric, each of the multipliers D_i of Theorem* II *is either identically congruent to zero or to a power of the determinant, D, of the transformation.*

By Lemma III, D_i is a linear combination of terms of the form $\xi_1^k \eta_1^{w-k} \xi_2^{w-k} \eta_2^k$, where w is constant for a given covariant, C; and thus each D_i which is not congruent to zero for every transformation of the group is of the form*

* For if D_i is not congruent to zero when the ξ's and η's are in the field, then it must be equal to unity for the identical transformation and hence must contain a term in $\xi_1^w \eta_2^w$ with coefficient unity.

$$D_i = (\xi_1 \eta_2 - \eta_1 \xi_2)^w + \Delta_i, \tag{9}$$

where Δ_i is divisible by $\eta_1 \xi_2$ and vanishes whenever the ξ's and η's are in the field. But D_i and $\xi_1 \eta_2 - \eta_1 \xi_2$ are both formal modular invariants of the two pairs, (ξ_i, η_i), and are also isobaric; hence Δ_i is likewise. Being divisible by η_1 and ξ_2, Δ_i is divisible by $L_i = \xi_i^{p^n} \eta_i - \xi_i \eta_i^{p^n}$ $(i = 1, 2)$. By Lemma II, this is impossible unless Δ_i is identically zero in the field. Finally, each D_i which is congruent to zero whenever the ξ's and η's are in the field is of the same type as the Δ_i above. Thus the lemma is proved.

11. **Isobaric seminvariants in terms of the roots.** If a formal modular seminvariant I of a system, S, of binary forms with respect to the field $GF[p^n]$ is isobaric, then, by Lemma I, it is invariant, modulo p, under any transformation

$$\begin{aligned} x_1 &= x_1' + M x_2', \\ x_2 &= x_2', \end{aligned} \tag{10}$$

where M is a general scalar. Hence, as in the theory of algebraic seminvariants, we can prove

LEMMA V. *Let I be any isobaric formal modular seminvariant of a system, S, of binary forms with respect to the Galois field, $GF[p^n]$, of order p^n which is of degree d and weight w. Then I is congruent, modulo p, to the product of a_0^d by a symmetric polynomial, S, in the symbolic ratios α_2/α_1, β_2/β_1, $\cdots$ which is homogeneous in these ratios of degree w. Moreover, S is expressible as a polynomial in the differences of these ratios.*

The proof proceeds as in the theory of classic seminvariants, but (for the sake of completeness) we shall reproduce it for the case when S contains only one form. Since I is isobaric, it can not contain a_0 as a factor, by Lemma II. Hence I is a_0^d multiplied by a polynomial, S, of degree d in a_1/a_0, a_2/a_0, $\cdots$, a_m/a_0. Thus S is a polynomial in the elementary symmetric functions of the symbolic ratios

$$A = \frac{\alpha_2}{\alpha_1}, \frac{\beta_2}{\beta_1}, \frac{\gamma_2}{\gamma_1}, \cdots,$$

and is of degree d in each such ratio; and since I is isobaric, S is homogeneous in these symbolic ratios of total degree w.

But, since I is formally unaltered, modulo p, under transformation (10), it is formally unaltered, modulo p, when the symbolic ratios are diminished by any scalar, M. Accordingly, set

$$\frac{\beta_2}{\beta_1} = \left(\frac{\beta_2}{\beta_1} - \frac{\alpha_2}{\alpha_1}\right) + A,$$

and similarly with the other ratios; and thus

$$S = \left(\frac{\alpha_2}{\alpha_1}\right)^k A_k + \left(\frac{\alpha_2}{\alpha_1}\right)^{k-1} A_{k-1} + \cdots + A_0, \tag{11}$$

where each A_i is a polynomial in the differences such as $(\beta_2/\beta_1) - (\alpha_2/\alpha_1)$, $(\gamma_2/\gamma_1) - (\alpha_2/\alpha_1)$, $\cdots$. As in classic invariant theory, this is impossible unless the A_i $(i \geqq 1)$ are all zero in the field. Hence the lemma is proved. The converse is also readily proved, but will not be needed here.

12. **Isobaric invariants in terms of the ratios.** When I is an isobaric formal modular invariant of a binary form, f, then (by Lemma I) its transform under any transformation (1) when the ξ's and η's are general scalars is connected with I by the relation (2), where (2) is an identical congruence as to the a's and thus is essentially of the same type as the corresponding relation for an algebraic invariant of f. Hence, as in the theory of algebraic invariants, we can prove for invariants the result which is a generalization of Lemma V. A similar argument obtains for an invariant of a system of binary forms and hence for covariants of a system of forms.* Thus we have

LEMMA VI. *Let C (a formal modular covariant of a system S of binary forms, f_i) be of degree d_i in the coefficients of f_i and of degree d in the variables, x_1 and x_2, and let it be isobaric of weight w.*

I. *Then C is identically congruent, modulo p, to $\Pi a_0^{d_1} x_2^d$ multiplied by a linear combination, K, of products of the expressions $(x_1/x_2) + (\alpha_2/\alpha_1)$, and of differences of the type $(\beta_2/\beta_1) - (\alpha_2/\alpha_1)$, where the α's and β's may be symbols arising from the same form, f_i, or may be symbols arising from two different forms.*

II. *Moreover, K is homogeneous in the symbols for each form, f_i, and such that each ratio α_2/α_1 for this form, f_i, occurs in exactly d_i factors in each product.*

III. *Finally, K is symmetric, modulo p, in these symbols for each form f_i.*

In applying the results of §§ 11 and 12, the reader must remember that, although the seminvariant (or invariant) is always symmetric in the pairs (α_1, α_2), (β_1, β_2), $\cdots$ in the form in which it first appears, yet the polynomial, K, in the differences $(\beta_2/\beta_1) - (\alpha_2/\alpha_1)$ is not in general symmetric in the ratios α_2/α_1, β_2/β_1, $\cdots$, but is merely symmetric modulo p. For the binary quadratic $f = a_0 x_1^2 + a_1 x_1 x_2 + a_2 x_2^2 = \alpha_x \beta_x$ has the formal modular invariant $a_1 = \alpha_1 \beta_2 + \alpha_2 \beta_1 \equiv \alpha_1 \beta_1 [(\beta_2/\beta_1) - (\alpha_2/\alpha_1)]$, modulo 2. The first is actually symmetric; but the second is not symmetric, though it is symmetric modulo $p = 2$.

13. **Isobaric formal covariants as algebraic covariants.** From Lemma VI it is evident that, if we express a_0 for each form, f_i, in terms of the symbols, we have

THEOREM III. *Every isobaric formal modular covariant, C, of a system of binary forms is expressible as a polynomial in symbolic covariants of the type $\alpha_x = \alpha_1 x_1 + \alpha_2 x_2$ and in determinantal symbolic invariants of the type*

* For every formal covariant of the system S is a formal modular invariant of the system S' consisting of the forms of S and the additional linear form $l = X_2 x_1 - X_1 x_2$ in which X_1, X_2 have been replaced by x_1, x_2, respectively. The proof of this is the same as for algebraic covariants.

$$(\alpha\beta) = \alpha_1\beta_2 - \alpha_2\beta_1.$$

But it is well known that the product, P, of $x_2^d \Pi a_0^{d_1}$ by any expression, K, in the symbols satisfying the conditions I and II of Lemma VI is an algebraic covariant of the system S of forms, though not necessarily a rational one.* A necessary and sufficient condition that P be rational in the coefficients of f_i is that K be actually symmetric in the ratios β_2/β_1, α_2/α_1, $\cdots$ formed for f_i. This is stronger than condition III of Lemma VI, as is illustrated by the symbolic invariant $(\alpha\beta)$ for the binary quadratic, mod 2 (see § 12). The kth power of $(\alpha\beta)$ is symmetric, mod 2, for any k; but is actually symmetric only when k is even. Thus we have

COROLLARY 1. *Every isobaric formal modular covariant of a system, S, of binary forms with respect to the Galois field, $GF[p^n]$ of order p^n, is congruent, modulo p, to an algebraic covariant of S, either rational or irrational.*

But every irrational algebraic covariant of S is known to be a root of an algebraic equation whose coefficients are rational, algebraic covariants of S, and thus we have

COROLLARY 2. *Every isobaric formal modular covariant of S is congruent, modulo p, to a root of an algebraic equation whose coefficients are rational algebraic covariants of S.*

PSEUDO-ISOBARIC COVARIANTS

14. **Informal discussion.** In the preceding sections, we have considered formal modular covariants that are actually isobaric and have seen that, in many ways, such a covariant is much the same as an ordinary classic covariant. But if a formal modular covariant is not isobaric, what then? For example, consider the formal modular invariants of a point with respect to the field $GF[p^n]$. Any such invariant, I, whose degree, d, is less than $p^n + 1$ must be an ordinary invariant of the point. For, since the weights of any two terms would have to be congruent, mod $p^n - 1$, I would have to be of the form $Ax_1^{p^n-1} + Bx_2^{p^n-1}$ where A and B are constants. But, if the degree is $< p^n$, there is no opportunity to apply Fermat's theorem to the coefficients of the transformation, and thus I must be invariant in the classic sense and therefore identically zero in the field. If $p^n < d \leqq p^{2n}$, it can be shown by a

* Dickson, *Algebraic Invariants*, p. 55, ex. 7; Elliott, loc. cit., p. 93. (Some people do not agree with my statement, and (in justification) say that P in general has no actual meaning in the a's. But any polynomial, P, in the symbols which is not actually symmetric in the symbols, α_1, α_2, β_1, β_2, $\cdots$ for a particular form, f_i, is a root of an algebraic equation whose coefficients are the elementary symmetric functions of P and the other symbolic invariants obtained from P by interchanging any two pairs of symbols for this form f_i; and hence P is a root of an algebraic equation whose coefficients are polynomials in the coefficients of f_i. Similarly, P is a root of an algebraic equation whose coefficients are polynomials in the coefficients of S, and thus P is an algebraic function of the coefficients of S, though it is not necessarily an explicit algebraic function of these coefficients. Hence why is it not an algebraic covariant of S?)

similar argument that either I is an ordinary invariant of the two cogredient pairs, (x_1, x_2), $(x_1^{p^n}, x_2^{p^n})$, and therefore $I = kL$ where k is a constant and $L = x_1^{p^n} x_2 - x_1 x_2^{p^n}$; or LI is an ordinary invariant of the two cogredient pairs (x_1, x_2) and $(x_1^{p^{2n}}, x_2^{p^{2n}})$, and therefore $LI = k(x_1^{p^{2n}} x_2 - x_1 x_2^{p^{2n}})$. In fact, it is well known that all formal modular invariants of the point (x_1, x_2) are polynomials in L and $Q = (x_1^{p^{2n}} x_2 - x_1 x_2^{p^{2n}})/L$. This might be stated more strikingly by saying that every such invariant is a rational, integral algebraic invariant of three points, or is a quotient of two such invariants. Moreover, a similar statement is true of the formal modular invariants of a pair of cogredient points, (x_1, x_2) and (y_1, y_2).* Is this true more generally?

15. **Preliminary lemmas.** Consider a formal modular invariant, $I = \sum I_j$ of the binary form $f(a; x)$ which is of degree d and which is not isobaric. In particular, let I_0 be a term of I whose weight, w_0, is less than or equal to that of any other term of I, and let I_1 be any other term of I. Then, since I is pseudo-isobaric, the weight of I_1 will be $w_1 = w_0 + l(p^n - 1)$ where l is an integer, positive or zero. When the coefficients of $f(a; x)$ are replaced by the corresponding functions of the symbols $\alpha_1, \alpha_2, \beta_1, \beta_2, \cdots$, I is homogeneous of degree md in these symbols. Also, if I_j is of weight w_j, it is of degree $md - w_j$ in symbols with subscript 1 and of degree w_j in symbols with subscript 2. Their difference, $md - 2w_j$, we shall call the excess, as in classic invariant theory.

LEMMA VII. *The excess of any term of a formal modular covariant is congruent to zero, modulo* $p^n - 1$.†

For, by interchanging the subscripts 1 and 2 throughout I, it follows that I contains a term whose degree in the symbols with subscript 1 is w_j and whose degree in the symbols with subscript 2 is $md - w_j$, and therefore of weight $md - w_j$. Hence $md - w_j \equiv w_j \pmod{p^n - 1}$, and the excess of any term of I is a multiple of $p^n - 1$, say $E_j(p^n - 1)$.

Now I^{p^n} is identically congruent in the field to $\sum I_j^{p^n}$,‡ and thus the latter is a formal modular invariant of $f(a; x)$. It may also be regarded as an invariant of $f(a^{p^n}; x)$, but we shall show that it is better for our purpose to regard it as a simultaneous invariant of $f(a; x)$ and $f(a^{p^n}; x)$.

For in I^{p^n} the term $I_0^{p^n}$ is of excess $E_0 p^n (p^n - 1)$, and hence, if we replace $E_0(p^n - 1)$ factors of the form $\alpha_1^{p^n}$ by as many factors of the form $\overline{\alpha}_1$, the excess of the resulting symbolic expression is $E_0(p^n - 1)$. If $w_0 \geqq E_0$, then by replacing E_0 additional factors of the form $\alpha_1^{p^n}$ by as many factors α_1,

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

† After finishing this MS., I discovered that Professor Glenn stated and proved this in *Concerning an analogy between formal modular invariants and the class of algebraic invariants called Booleans*, American Journal of Mathematics, vol. 37 (1915), p. 75.

‡ Dickson, *Linear Groups*, p. 15.

the excess of the resulting symbolic expression is zero. $I_0^{p^n}$ is now of degree $E_0 p^n$ in $\bar{\alpha}$'s having subscript 1 and of degree zero in $\bar{\alpha}$'s having subscript 2; also, it is of degree $(w_0 - E_0) p^n$ in α's having subscript 1 and of degree $w_0 p^n$ in the α's having subscript 2. Here and elsewhere in this work, we use the expression "symbols α's" to denote any and all symbols such as $\alpha_1, \alpha_2, \beta_1, \gamma_1, \cdots$; similarly with the expression "symbols $\bar{\alpha}$."

Moreover, if $w_0 \geqq E_0$, the same device will serve to make all terms of I^{p^n} of excess zero and also to make all terms of the same weight, w_0. For the weight of any term, I_ν, of I is $w_0 + k(p^n - 1)$ and hence is of excess $(E_0 - 2k)(p^n - 1)$ which we shall assume positive for convenience. Accordingly, if in $I_\nu^{p^n}$ we replace $(E_0 - 2k)(p^n)$ factors of the form $\alpha_1^{p^n}$ by as many factors $\bar{\alpha}_1$, the result is of excess zero, but of weight $[w_0 + k(p^n - 1)]\, p^n$. Next replace kp^n factors $\alpha_1^{p^n}$ by as many factors $\bar{\alpha}_1$ and replace kp^n factors $\alpha_2^{p^n}$ by as many factors $\bar{\alpha}_2$, and we get an expression whose excess is zero and weight is $w_0 p^n$. This is legal, since $w_0 \geqq E_0 - k + 1$ and $w_0 \geqq k$. In case the excess of I_ν is negative, interchange the subscripts 1 and 2 in the foregoing by an argument similar to that used in Lemma VII. Thus the remark at the beginning of this paragraph is proved.

For convenience, we shall speak of the α's, β's, $\cdots$ (the symbolic coefficients of the linear factors $\alpha_x, \beta_x, \cdots$ of $f(a; x)$) as the *primary symbols*; and we shall speak of the totality of the original symbols $\alpha_1, \alpha_2, \beta_1, \beta_2, \cdots$ together with the new symbols $\bar{\alpha}_1, \bar{\alpha}_2, \bar{\beta}_1, \bar{\beta}_2, \cdots$, and any other symbolic coefficients introduced in the above manner as the *secondary symbols.*

We see, accordingly, that every pseudo-isobaric formal modular invariant, I, of $f(a; x)$ is such that a suitable power of I is isobaric in the coefficients of the symbolic linear factors of $f(a; x)$ and of $f(a^{p^n}; x)$, provided $0 \neq w_0 \geqq E_0$. Even if $0 \neq w_0 < E_0$, this argument shows that the excess of I^{p^n} in the secondary symbols is $(E_0 - w_0)(p^n - 1)$ less than that of the original I. But, since the excess is finite, it follows that, by repeating this process at most $[E_0/w_0]^*$ times, we prove Lemma VIII for the case $w_0 \neq 0$. It will be observed, however, that for this purpose we have to introduce another set of new symbols, say $\bar{\bar{\alpha}}_1, \bar{\bar{\alpha}}_2, \bar{\bar{\beta}}_1, \bar{\bar{\beta}}_2, \cdots$, and possibly still other sets having three or more dashes. These, together with those introduced above, we group under the heading "secondary symbols."

When $w_0 = 0$, we first multiply I by any invariant which is not an absolute invariant and then proceed as above. Thus we have

LEMMA VIII. *Let I be a pseudo-isobaric invariant of a binary form*

$$f(a; x) = \Pi \alpha_x$$

with respect to the Galois field, $GF[p^n]$, of order p^n; and let the lowest weight of all

* Here $[E_0/w_0]$ means the smallest integer which is not less than E_0/w_0.

the terms of I be denoted by w_0. Then, if $w_0 \neq 0$, some finite power of I is congruent to a polynomial in the secondary symbols for f which is isobaric. If $w_0 = 0$, then some power of I is congruent to the quotient of two polynomials in the secondary symbols each of which is isobaric For examples, see Part IV.

16. **Pseudo-isobaric modular covariants as algebraic covariants.** Let J denote that formal modular invariant of f which is obtained as a result of applying the method of Lemma VIII to the pseudo-isobaric invariant I and which is, accordingly, isobaric of weight w in the secondary symbols. If we apply to J the transformation (1), then the transform $J' = J(\alpha')$ is identically equal to

$$J(\alpha'; \bar{\alpha}'; \bar{\bar{\alpha}}'; \cdots) = \sum D_k(\xi, \eta) P_k(\alpha; \bar{\alpha}; \bar{\bar{\alpha}}; \cdots) + \tau \tag{12}$$

where each D_k (i) is a formal modular invariant of the two pairs (ξ_1, η_1) and (ξ_2, η_2), (ii) is congruent to zero or to D^w whenever the ξ's and η's are all in the field, (iii) is isobaric of weight w in the ξ's and η's; and where τ is a polynomial in the ξ's and η's and in the secondary symbols which vanishes whenever the dashed symbols are replaced by the proper powers of the corresponding primary symbols. That is, J is not in general an invariant function of the secondary symbols when these symbols are taken as independent, but it is an invariant function when the dashed symbols are replaced by the proper expressions in the primary symbols.

Since J is isobaric in the secondary symbols, Lemmas I–IV apply to J. If we proceed to Lemma V, we see that the proof applies to J with the exception that, since J is not in general rational in the coefficients of $f(a; x), f(a^{p^n}; x), f(a^{p^{2n}}; x), \cdots$, then J is not in general congruent (modulo p) to the product of a_0^d by a symmetric polynomial, S, in the secondary symbolic ratios; but, nevertheless, J is congruent (modulo p) to a product of secondary symbols with subscript 1 by a polynomial, S, in the secondary symbolic ratios. Hence, as before, S is expressible as a polynomial in the differences of the secondary symbolic ratios. Thus the proof of Lemma VI applies to J with the restrictions noted.

Hence we prove Theorem III and its corollaries for J, and we have

THEOREM IV. *If I is a formal modular covariant of a system of binary forms with respect to the Galois field $GF[p^n]$ of order p^n, then I^q (where q is a sufficiently large integer) is congruent to one of the two following forms:*

(1) *a polynomial in symbolic covariants of the types α_x, α_X, A_x, $(\alpha\beta)$, $(A\beta)$, etc., where $X = x^{p^n}$ and $A = \alpha^{p^n}$;*

(2) *a quotient of two polynomials described in* (1).

Since these symbolic expressions are (symbolic) algebraic covariants of $f(a; x), f(a^{p^n}; x)$, etc., we have

COROLLARY 1. *Every pseudo-isobaric formal modular covariant, C, of a system S of binary forms with respect to the Galois field $GF[p^n]$ is congruent,*

modulo p, to a symbolic algebraic covariant, C, of the forms of S and certain related forms obtained from the forms of S by replacing each coefficient of these forms by its p^nth power.

In particular, this means that the function J may be chosen in such a way that, under the transformation (1), J goes into J', where J' is equal to (not merely congruent to) $D^w J$, when J is expressed as an isobaric function of the secondary symbols. Note, however, that J is not necessarily rational in the coefficients of the forms of S and the related forms. These remarks are illustrated by examples given in Part IV.

17. **Finiteness of determinantal symbols.** In the preceding section, we proved that all formal modular invariants I of a binary system, S, are congruent, modulo p, to rational functions in symbolic invariants of S of a certain special type called determinantal symbols. That is, I is congruent, modulo p, to a rational function of symbolic invariants of the types $(\alpha\beta)$, $(\alpha^{p^n}\alpha)$ and symbols obtained from these by replacing a pair of symbols by their p^nth powers one or more times. Conceivably, as the degree of I increases, the degree of the requisite determinantal symbols might increase without bound, so that we would need an infinite number of determinantal symbols to obtain all formal modular invariants of S.

But, in Part II, we proved that all formal modular invariants of S are congruent to polynomials in a finite number of symbolic invariants which are formal modular invariants of the (symbolic) coefficients of the symbolic linear factors of the forms of S. Now apply Theorem IV to these symbolic invariants, and we see that all symbolic invariants of S are congruent to rational functions of determinantal symbols. Hence we have

THEOREM V. *All formal modular covariants of a system of binary forms are congruent, in the field, to rational functions of a finite number of symbolic covariants of the types described in Theorem* IV.

In fact, this theorem could have have been proved directly in much the same manner as Theorem IV was proved and then Theorem IV would have followed as a corollary of Theorems I and V.

PART IV. EXPRESSION OF COVARIANTS IN SYMBOLIC FORM

18. **Method for algebraic covariants.** In the symbolic theory of algebraic covariants, after proving that every such covariant is expressible as a polynomial in symbols of the two types, $(\alpha\beta)$ and α_x, there is then given a clear-cut method for expressing any covariant in terms of these symbolic covariants. For completeness, this method will be reproduced here, as we shall need to refer to several of the results.

Let I be any algebraic invariant, of weight w, of a system of forms whose coefficients are the a's; and let $I(a')$ be its transform under (1). Under this

transformation, α_1 and α_2 go into α_ξ and α_η, respectively; and similarly for the β's, γ's, etc. Just as the a's are polynomials in $\alpha_1, \alpha_2, \beta_1, \beta_2, \cdots$, so their transforms are polynomials in $\alpha_\xi, \alpha_\eta, \beta_\xi, \beta_\eta, \cdots$. Hence, in the equation (2),

(i) replace every a' by the corresponding polynomial in α_ξ, α_η, etc.;

(ii) operate on both sides of the resulting equation w times with

$$V = \frac{\partial^2}{\partial\xi_1\,\partial\eta_2} - \frac{\partial^2}{\partial\xi_2\,\partial\eta_1};$$

(iii) divide both sides of the result of (ii) by $(w+1)!\,w!$.

From the left we get a polynomial in the symbolic invariants of the type $(\alpha\beta)$, and from the right we get $I(a)$.

In proving this, use is made of the following:

LEMMA A.

$$V^w(\xi\eta)^w = (w+1)!\,w!.$$

LEMMA B. *The result of operating by V^w on a product of k terms of type α_ξ and l terms of the type β_η is a sum of terms each containing $k-w$ factors α_ξ, $l-w$ factors β_η and w factors $(\alpha\beta)$.*

19. **Difficulties in modular case.** It is at once evident that this method is not applicable directly to formal modular invariants, since the divisor in (iii) is congruent to zero in the field whenever $w \geqq p-1$. This difficulty, of course, might be superficial in the sense that it might be due to some accidental peculiarity in the proof and not to any essential characteristic of the problem; but, as will be apparent presently, there is a deep-seated difficulty.

Lemma B is proved by direct verification combined with induction, and thus is lost the full significance of the reason why it is true. Now each symbolic expression α_ξ and each β_η is an invariant of the two points (ξ_1, ξ_2) and (η_1, η_2), which are transformed cogrediently when the original variables are subjected to any linear transformation

$$\begin{aligned} x_1 &= \kappa\bar{x}_1 + \lambda\bar{x}_2, \\ x_2 &= \mu\bar{x}_1 + \nu\bar{x}_2, \end{aligned} \qquad \Delta = \kappa\nu - \lambda\mu \neq 0, \tag{13}$$

thus replacing (1) by

$$\begin{aligned} \bar{x}_1 &= \bar{\xi}_1 x_1' + \bar{\eta}_1 x_2', \\ \bar{x}_2 &= \bar{\xi}_2 x_1' + \bar{\eta}_2 x_2', \end{aligned} \tag{14}$$

where the $\bar{\xi}$'s and $\bar{\eta}$'s are cogredient with the x's. Moreover, V is an invariantive operator whenever the ξ's and η's are transformed cogrediently. Lemma B is an inevitable consequence of these facts.

If we look at Theorem II (§ 8), we see that in the modular case we have the identity (4) where each D_i is a formal modular invariant of (ξ_1, η_1) and

(ξ_2, η_2) when they are transformed cogrediently; but D_i is not in general a formal modular invariant of the two pairs (ξ_1, ξ_2) and (η_1, η_2), though it is clearly a modular invariant of these pairs. Moreover, the only way to operate on a product of a number of symbols of the type α_ξ and β_η in such a way as (i) to eliminate the ξ's and η's and (ii) to obtain as result a formal modular invariant of the α's, β's, etc., is to use an operator which has the invariantive property when (ξ_1, ξ_2) and (η_1, η_2) are transformed cogrediently. Now the natural analogues of V for the formal modular case are, by Theorem II, those formed on

$$\xi_1^{p^n}\eta_2 - \eta_1^{p^n}\xi_2, \quad \text{etc.},$$

as models—i.e., by replacing each ξ by the operator indicating partial differentiation with respect to that ξ, and similarly with the η's—but they can not give the desired results since these operators are not invariantive when the ξ's are transformed cogrediently with the η's.

20. **Significance of results of Part III.** Such is the essential difficulty of the problem and such is one of the reasons for proving the theorems of Part III. There it is shown that (i) if C is isobaric, then each D_i is an algebraic invariant of the two pairs (ξ_1, η_1) and (ξ_2, η_2) and hence is an invariant of the two pairs (ξ_1, ξ_2) and (η_1, η_2); (ii) if C is not isobaric, then a suitably high power of C, say C^q, is such that, when (2) is formed for C^q, then each D_i is an algebraic invariant of the two pairs (ξ_1, η_1) and (ξ_2, η_2) and hence is an invariant of the pairs (ξ_1, ξ_2) and (η_1, η_2). In view of the remarks of § 19, these results smooth out some of the difficulties.

21. **First method.** Let I be any formal modular invariant of a system S of binary forms with respect to the Galois field, $GF[p^n]$, of order p^n, and let J be a formal modular invariant of S which is obtained from I by applying the method of Lemma VIII and which is isobaric in the secondary symbols. The first method of expressing J in symbolic form is suggested by the proof of Lemma V (§ 11). Although it lacks originality, it has the advantage that it leads at once to a result without exception or qualification. If J is of degree d_i in the coefficients of f_i, divide J by $\pi\alpha_1^{d_i}$ where the α_1 range over all symbols for f_i having subscript 1. Do this for every form f_i. The quotient, S, is a polynomial in the ratios $\alpha_2/\alpha_1, \beta_2/\beta_1, \cdots, \overline{\alpha}_2/\overline{\alpha}_1, \cdots$ with coefficients which are marks of the field. Single out any particular ratio of the primary symbols, say α_2/α_1, and select all terms of S which do not contain α_2/α_1 as a factor. In the resulting expression, replace β_2/β_1 by $(\beta_2/\beta_1) - (\alpha_2/\alpha_1)$, $\alpha_2^{p^n}/\alpha_1^{p^n}$ by $(\alpha_2^{p^n}/\alpha_1^{p^n}) - (\alpha_2/\alpha_1)$, and similarly for all symbolic ratios. The resulting expression, E, is clearly an invariant, since it is a polynomial in the determinantal symbols. Moreover, it is identically congruent, modulo p, to J, for it is simply A_0 in equation (11).

22. **Second method.** It is usually easy to determine by inspection a product, π, of determinantal symbols in such a way that the terms of π which have the greatest excess are among the terms of J which have the greatest excess; and hence, by a finite number of steps, we can express J in symbolic form. No attempt has been made to crystallize this into a definitive, systematic process, though possibly this might be done.

For example, consider $a_0 x_1^2 + 2a_1 x_1 x_2 + a_2 x_2^2$. Modulo 3, this has the formal modular invariant

$$\begin{aligned} B &= a_1(a_1 - a_0)(a_1 + a_0)(2a_0 + a_2)(2a_1 + a_2)(a_1 + a_2) \\ &\equiv (\alpha_1\beta_2 + \alpha_2\beta_1)(\alpha_1\beta_2 + \alpha_2\beta_1 + \alpha_1\beta_1)(\alpha_1\beta_2 + \alpha_2\beta_1 - \alpha_1\beta_1) \\ &\qquad \times (-\alpha_1\beta_1 + \alpha_2\beta_2)(\alpha_1\beta_2 + \alpha_2\beta_1 + \alpha_2\beta_2)(\alpha_1\beta_2 + \alpha_2\beta_1 - \alpha_2\beta_2) \\ &\equiv \sum\alpha_1^6\beta_1^3\beta_2^3 - \sum\alpha_1^6\beta_1\beta_2^5 + \sum\alpha_1^4\beta_1^3\alpha_2^2\beta_2^3 \\ &\qquad - \sum\alpha_1^3\beta_1^2\alpha_2^3\beta_2^4 + \sum\alpha_1^5\alpha_2\beta_2^6 - \sum\alpha_1^3\alpha_2^3\beta_2^6 \\ &\equiv \sum(\alpha^3\beta)^2(\beta^3\beta) \pmod 3. \end{aligned}$$

The terms of greatest excess in B are $\sum\alpha_1^6\beta_1^3\beta_2^3$ which suggests that we use to "kill off" these terms $\sum(\alpha^3\beta)^2(\beta^3\beta)$, since the only way to express $\alpha_1^6\beta_1^3\beta_2^3$ in the secondary symbols $\alpha_1, \alpha_2, \beta_1, \beta_2, \alpha_1^3, \alpha_2^3, \beta_1^3, \beta_2^3$ in such a way that it shall be isobaric in these secondary symbols is $\alpha_1^3\beta_2\,\alpha_1^3\beta_2\,\beta_1^3\beta_2$. Thus we take as π, $(\alpha^3\beta)^2(\beta^3\beta)$. It is then readily discovered that $\sum(\alpha^3\beta)^2(\beta^3\beta)$ accounts for all terms, modulo 3.

23. **Third method.** The preceding method is closely related to the one about to be explained. Although the second method has none of that generality which attracts the artist in pure mathematics, yet it has the advantage in any concrete case, while the present method is to be preferred in any general argument.

Under transformation (1), J is carried into

$$J(a') \equiv D^w J(a) \pmod p \tag{15}$$

where this is an identical congruence in the a's and the coefficients of the transformation. Moreover, it is understood that $J(a')$ is so written that it is isobaric of weight w in the secondary symbols as in Lemma VIII. Thus, if each a' is replaced by its expression in terms of the α_ξ and α_η, $\overline{\alpha}_\xi$ and $\overline{\alpha}_\eta$, etc., the left member of (15) is the sum of a number of terms each of which is a product of w linear functions of the ξ's and w linear functions of the η's.

Now operate on both sides of (15) with V^w as given in (ii), § 18. Since the left member is isobaric in the secondary symbols, we can apply Lemma B. Hence, from the left member we get a sum of a number of terms, each of which is a product of w determinantal symbols such as $(\alpha\beta)$, $(\alpha^{p^n}\beta)$, $(\alpha^{p^n}\alpha)$, etc. From the right we get $(w+1)!\,w!\,J(a)$. Call the result equation E.

If $(w+1)!\,w! \equiv 0$ (modulo p), then the totality of those terms on the right of equation E whose coefficients are not congruent to zero, modulo p, constitute a syzygy, modulo p. Moreover, since the right member of (15) is symmetric, modulo p, in the primary symbols, this syzygy must be symmetric, modulo p, in these symbols and hence congruent to a function which is rational in the coefficients of the ground forms, f. Hence, if we know the necessary syzygies or use discretion, we can replace equation E by one (i) which is equivalent to E and (ii) which has each coefficient congruent to zero, modulo p. If we now cancel p from both sides of this equation, we have an equation, E_1, of the same type as E, but such that the multiplier on the right is not divisible by so high a power of p. Now treat equation E_1 as we treated E above. These steps are all justified, since J is an algebraic invariant of certain forms.

24. **Illustrations.** A fundamental system of formal modular invariants, modulo 3, of the binary quadratic was expressed in symbolic form in § 6.

It is known that a fundamental set of formal modular invariants, modulo 2, of the cubic

$$a_0 x_1^3 + a_1 x_1^2 x_2 + a_2 x_1 x_2^2 + a_3 x_2^3 = \pi\alpha_x = (\alpha_1 x_1 + \alpha_2 x_2)(\beta_1 x_1 + \beta_2 x_2)(\gamma_1 x_1 + \gamma_2 x_2)$$

is

$$K = a_1 + a_2, \qquad \Delta = a_0 a_3 + a_1 a_2, \qquad I = a_0^2 + a_0 K + \delta_{00},$$

$$k = a_0 \delta_{00}, \qquad g = \beta_2^2 + \beta(\Delta + K^2) + (\Delta + \delta_{00})(\beta + a_0 K + K^2)$$

where

$$\beta = a_0 a_1 + a_1^2,$$
$$\delta_{00} = (a_0 + a_1 + a_2 + a_3) a_3.$$

After a little computation, it is readily seen that

$$\Delta \equiv (\alpha\beta)(\beta\gamma)(\gamma\alpha),$$
$$I \equiv \frac{(\alpha^4\alpha)(\beta^4\beta)(\gamma^4\gamma)}{(\alpha^2\alpha)(\beta^2\beta)(\gamma^2\gamma)} + K^2 + \Delta,$$
$$k = (\alpha^2\alpha)(\beta^2\beta)(\gamma^2\gamma).$$

But every attempt to express K as a polynomial in the determinantal symbols is bound to fail, since it is not possible to express K as an isobaric function of the secondary symbols. In fact, K is the invariant which forced the author to realize Theorem IV and the lemmas that lead thereto. It is easy to show that

$$K^2 \equiv \sum(\alpha^2\gamma)(\beta^2\gamma) + (\alpha\beta)(\beta\gamma)(\gamma\alpha).$$

Similarly, it is not possible to express g as a polynomial in determinantal symbols, though (by Theorem IV) a power of g is so expressible.

The author has also expressed some covariants of these two forms in symbolic form, but the amount of numerical work necessary to do this seemed to increase rapidly with the degree of the covariant called J in Part III. In short, the author would not recommend that the theory of Part III be applied in detail to any but the simplest concrete case, unless there should prove to be some powerful systematic procedure not yet discovered.

Part V. Finiteness theorems

25. **Preliminary.** In Part III, we saw that every formal modular covariant of a system, S, of binary forms with respect to the Galois field $GF[p^n]$, of order p^n, is expressible as a polynomial in a finite number of symbolic covariants. Moreover, if the covariant is rational and integral, it must be such that when expressed in terms of these symbolic covariants it is unaltered, modulo p, when any two pairs of primary symbols, (α_1, α_2) and (β_1, β_2), are interchanged. It must be carefully noted, however, that this is not equivalent to saying that it is symmetric in the symbolic covariants.

Using this result, we can prove that the set of all formal modular covariants of S which are rational and integral possesses the finiteness property—i.e., they are all expressible as polynomials in a finite number of these covariants. The proof given below is Hilbert's proof of the finiteness theorem for algebraic covariants, with only one slight modification. The theorem is proved for invariants of a general binary system, S, since the covariants of a system S are coextensive with the invariants of another system S'.

It is readily seen that Hilbert's beautiful proof,* when shorn of non-essentials, depends entirely on the following properties of algebraic invariants:

I. All invariants are polynomials in a finite number of polynomials, P, in a certain finite set of pairs of auxiliary variables. Since these polynomials, P, are invariants under the group, we shall call them elemental invariants. In the case of algebraic invariants, these auxiliary variables are the coefficients of the symbolic linear factors of the forms of S and the elemental invariants are the determinantal symbolic invariants of type $(\alpha\beta)$.

II. If the invariant is rational and integral, it must be such that, when expressed in terms of the elemental invariants, it is unaltered (with respect to the field of definition) when any two pairs of the auxiliary variables are interchanged.

His proof uses the following theorem about diophantine equations: A system of any number of linear diophantine equations has only a finite number of simple sets of solutions, all other solutions being sums of positive multiples of this finite number of sets of solutions.

* *Ueber die Endlichkeit des Invariantensystems für binäre Grundformen*, Mathematische Annalen, vol. 33 (1889), pp. 223–226.

Now Part II proves that these two properties hold for formal modular invariants where the auxiliary variables are the primary symbols $\alpha_1, \alpha_2, \beta_1, \beta_2, \cdots$ and where the elemental invariants are the finite number of symbolic invariants of Theorem I. Moreover, Hilbert's proof makes no use of properties peculiar to a field of characteristic zero except in one place which is readily avoided. Thus his proof applies here.

26. **Finiteness of covariants.** For convenience, let $I_1, I_2, \cdots, I_\mu$ be a fundamental set of symbolic formal modular invariants of S. Then every formal modular invariant of S is expressible in the form

$$I = \sum M_i I_1^{s_1} I_2^{s_2} \cdots I_\mu^{s_\mu} \tag{16}$$

where the exponents, s_j, are positive integers or zero and the coefficients, M_i, are marks of the Galois field, $GF[p^n]$. Necessary and sufficient conditions that I be a rational and integral function of the coefficients of the forms of S are that (i) when the right member of (16) is expanded, it is a function of the pairs $(\alpha_1, \alpha_2), (\beta_1, \beta_2), \cdots$ which is symmetric, modulo p, (ii) each term of this expansion contains the same number of α's as β's, the same number of β's as γ's, etc.

If $d_j(\alpha)$ denotes the degree of I_j in the pair (α_1, α_2), then the last condition gives a set of linear diophantine equations of which two are

$$\begin{aligned} d &= s_1 d_1(\alpha) + s_2 d_2(\alpha) + \cdots + s_\mu d_\mu(\alpha) \\ &= s_1 d_1(\beta) + s_2 d_2(\beta) + \cdots + s_\mu d_\mu(\beta), \end{aligned} \tag{17}$$

there being one such equation for every pair of symbols. By the theory of linear diophantine equations, it follows that every rational integral invariant, I, is expressible in the form

$$I = \sum N_i C_1^{t_1} C_2^{t_2} \cdots C_r^{t_r}, \tag{18}$$

where each C_i is a symbolic invariant of S which has the property (ii) above and where (iii) there is one C_i corresponding to each simple set of solutions of the set of diophantine equations (17), and (iv) the C_i are the same for all invariants, I, of the system S.

Moreover, if σ_i is the number of the symbolic invariants which are not identically congruent, modulo p, and which are obtained from a particular C_i by interchanging any two pairs of symbols, then C_i satisfies an algebraic equation of degree σ_i where the coefficients of the various terms are (aside from sign) the elementary symmetric functions of C_i and its conjugates. Since C_i and therefore each of its conjugates has the property (ii), these coefficients, K_j, are formal modular invariants of S which are rational and integral in the a's. Hence I may be written

$$I = \sum L_j \left(\sum Q_i C_1^{t_1} C_2^{t_2} \cdots C_r^{t_r}\right) \qquad (0 \leqq t_i < \sigma_i) \tag{19}$$

where the Q's are in the field and where the summation in the parentheses is symmetric, modulo p, in the pairs of symbols (α_1, α_2), (β_1, β_2), etc. Moreover, the L_j are polynomials in a finite set of rational, integral formal modular invariants, viz., the K's.

Hence by referring to the sufficient conditions given above that a symbolic invariant be rational and integral, we have

THEOREM VI. *Let S be a system of binary forms with coefficients which are independent variables and let G be the total group of linear transformations on the variables whose coefficients are marks of the Galois field, $GF[p^n]$, of order p^n. Then all formal modular covariants of S under the group G are expressible as polynomials in a finite number of such covariants.*

27. **Finiteness of syzygies.** By using, as in classic invariant theory, Hilbert's useful theorem about an infinite sequence of polynomials, we can show that every syzygy, $S \equiv 0$, among the covariants of the system S is of the form

$$S \equiv \sum H_j S_j,$$

where (i) the H_j are formal modular covariants of S;

(ii) the S_j are polynomials in the formal modular covariants such that $S_j \equiv 0$ is a syzygy among the formal modular covariants of S;

(iii) the S_j are finite in number and are the same for all syzygies.

Thus we have

THEOREM VII. *The syzygies among the formal modular covariants of the system S possess the finiteness property in the sense that all of them are consequences of a finite number of them, $S_1 \equiv 0$, $S_2 \equiv 0$, $\cdots$, $S_k \equiv 0$.*

MOUNT HOLYOKE COLLEGE,
SOUTH HADLEY, MASS.