FUNDAMENTAL SYSTEMS OF FORMAL MODULAR PROTOMORPHS OF BINARY FORMS*

BY

W. L. G. WILLIAMS

I

If the binary form

$$(1)\qquad f(x\ ,y)=a_0x^q+\binom{q}{1}a_1x^{q-1}y+\binom{q}{2}a_2x^{q-2}y^2+\cdots+a_qy^q,$$

where $\binom{q}{1}$, $\binom{q}{2}$, $\cdots$ are the binomial coefficients and a_0, a_1, $\cdots$, a_q are independent variables, we make the substitution

$$(2)\qquad \begin{aligned} x&=X+tY\ ,\\ y&=Y\ ,\end{aligned}$$

we obtain a binary form

$$(3)\qquad F(X,\ Y)=A_0X^q+\binom{q}{1}A_1X^{q-1}Y+\cdots+A_qY^q\ ,$$

in which

$$(4)\qquad A_j=a_0t^j+\binom{j}{1}a_1t^{j-1}+\cdots+a_j\qquad (j=1,2,\cdots,q)\ .$$

A polynomial $P(a_0,\ a_1,\cdots,\ a_q\ )$ is said to be an algebraic *seminvariant* of $f(x,\ y)$ if, for all real or complex values of t,

$$P(A_0\ ,A_1\ ,\ \cdots\ ,A_q)=P(a_0\ ,a_1\ ,\ \cdots\ ,a_q)\ ;$$

a *formal modular seminvariant*, mod p, of $f(x,\ y)$ if, for all integral values of t,

$$P(A_0\ ,A_1\ ,A_2\ ,\ \cdots\ ,\ A_q)\equiv P(a_0\ ,a_1\ ,\ \cdots\ ,a_q)\ (\text{mod } p)\ ,$$

and a *formal modular seminvariant in the Galois field* $GF[p^n]$ if, in this field, $P(A_0,A_1,\cdots,A_q)=P(a_0,a_1,\cdots,a_q)$, t being any mark of the $GF[p^n]$.

If S_1, S_2, $\cdots$, S_r are a set of algebraic (formal modular) seminvariants of a binary form such that every algebraic (formal modular) seminvariant, which is by definition a polynomial, is equal (congruent, mod p, or equal in the field) to $S_1^rQ(S_1,\ S_2,\cdots,S_r)$, where Q is a polynomial in its argu-

* The investigation upon which this article is based was in part supported by a grant from the Heckscher Foundation for the Advancement of Research, established by August Heckscher at Cornell University. A preliminary report on this subject was presented to the Society, September 8, 1922, under the title *Fundamental systems of protomorphic formal modular seminvariants of binary forms*. This paper was received by the editors in October, 1925.

ments and r is an integer (positive, negative, or zero), $S_1, S_2, \cdots, S_r$ form a fundamental system of algebraic (formal modular) protomorphs of $f(x,y)$.

One set of algebraic protomorphs* of a form $f(x, y)$ of order q is $S_1, S_2, \cdots, S_q$, where

$$\begin{aligned} &S_1 = a_0, \\ &S_2 = a_0a_2 - a_1^2, \\ &S_3 = a_0^2a_3 - 3a_0a_1a_2 + 2a_1^3, \\ &S_4 = a_0a_4 - 4a_1a_3 + 3a_2^2, \\ (5) \qquad &S_{2m} = a_0a_{2m} - \binom{2m}{1} a_1a_{2m-1} + \binom{2m}{2} a_2a_{2m-2} - \cdots \\ &\qquad + (-1)^{m-1}\binom{2m}{m-1} a_{m-1}a_{m+1} + \frac{1}{2}(-1)^m \binom{2m}{m} a_m^2 , \\ &S_{2m+1} = (a_0\theta - 2a_1)S_{2m} , \text{ where } \theta \text{ is the differential operator} \end{aligned}$$

$$a_1\frac{\partial}{\partial a_0} + a_2\frac{\partial}{\partial a_1} + \cdots + a_q\frac{\partial}{\partial a_{q-1}} .$$

In §II of the present paper we find a fundamental system of formal modular protomorphs, mod p, of $f(x, y)$; in §III we find a fundamental system of formal modular protomorphs, mod p, of s binary forms.

These fundamental systems are remarkable in that they contain no member, not congruent, mod p, to an algebraic seminvariant except

$$\beta = \prod_{t=0}^{p-1} (a_0t + a_1) \equiv a_1^p - a_0^{p-1}a_1 \qquad (\text{mod } p) .$$

The problem of finding a finite set of formal seminvariants, mod p, of $f(x, y)$ such that every formal seminvariant is a polynomial in the members of this finite set is one of considerable difficulty especially as for a given form the minimum number of members of such a set or *fundamental system* may vary with p.† In the solution of this problem a fundamental rôle is played by three kinds of seminvariants; first, those which are congruent, mod p, to algebraic seminvariants; second, those which are expressible as sums of certain powers of linear expressions in the coefficients of $f(x, y)$, and third, those which are expressible as products of linear expressions in the coefficients, such as β.

For example, every seminvariant, mod p ($p>2$) of the binary quadratic, $ax^2+2bxy+cy^2$, is congruent, mod p, to a polynomial in seminvariants

* Elliott, *Algebra of Quantics*, pp. 212-215.

† Williams, these Transactions, vol. 22 (1921), p. 56.

congruent, mod p, to the algebraic seminvariants a, $\Delta=ac-b^2$, and the formal modular seminvariants

$$\beta=\prod_{t=0}^{p-1}(at+b)$$

and

$$\gamma_0=\prod_{t=0}^{p-1}(at^2+2bt+c)\,.$$ [*]

The case of the binary cubic is more complicated, but for $p=5$ the binary cubic $ax^3+3bx^2y+3cxy^2+dy^3$ has as a fundamental system[†] of formal modular seminvariants

(1) the four algebraic seminvariants

$$a\ ,\ \Delta\ ,\ S_3=a^2d-3abc+2b^3\ ,\ \text{and}\ D=a^2d^2-6abcd+4b^3d+4ac^3-3b^2c^2,$$

(2) two seminvariants of the product type

$$\gamma_0\ \text{and}\ \delta_{00}\ =\prod_{t=0}^{4}(at^3+3bt^2+3ct+d),$$

(3) six seminvariants of the sum type

$$\sum_{t=0}^{4}R^rS^s,\quad \text{where}\ \begin{aligned}&R=at^2+2bt+c,\\&S=at^3+3bt^2+3ct+d\ ,\\&r,s=0,3;\quad 0,4;\quad 2,3;\quad 2,4;\quad 3,3;\quad 3,4.\end{aligned}$$

Although no proof has been given that every formal modular seminvariant is a polynomial in seminvariants of these three types, no exception to such a theorem is known. In §IV we prove that certain seminvariants can be expressed as polynomials in seminvariants of these three types.

Section V is devoted to a brief discussion of the extension of the theorems of the previous articles to the Galois field $GF\,[p^n]$.

II

If $S_1, S_2, \cdots, S_q$ are the set of protomorphs in §I, and $a_0\neq 0$, then

$$\begin{aligned}&a_2=\frac{a_1^2+S_2}{a_0}\ ,\\ (1)\qquad &a_3=\frac{a_1^3+3a_1S_2+S_3}{a_0^2}\ ,\\ &a_i=\frac{P_i(a_1\ ,S_2\ ,S_3\ ,\ \cdots\ ,S_i)}{a_0^{i-1}}\qquad (i=4,5,\ \cdots\ ,q),\end{aligned}$$

[*] Dickson, *Madison Colloquium Lectures*, pp. 42 et seq.

[†] Williams, loc. cit., pp. 69-73.

where P is a polynomial with integral coefficients in its arguments and p is a prime such that the binomial coefficients $\binom{q}{j} \not\equiv 0$, mod p[*] $(j = 1, 2, \cdots, q-1)$; then any formal modular seminvariant (which is by definition a polynomial in $a_0, a_1, a_2, \cdots, a_q$)

$$S(a_0, a_1, \cdots, a_q) = S\left[a_0,\ a_1,\ \frac{a_1^2+S_2}{a_0},\ \cdots,\ \frac{P(a_1, S_2, \cdots, S_q)}{a_0^{q-1}}\right]$$

$$= F\left(a_0, \frac{S_2}{a_0}, \frac{S_3}{a_0^2}, \cdots, \frac{S_q}{a_0^{q-1}}\right)$$

$$+ a_0^k G(a_0, a_1, S_2, \cdots, S_q),$$

where k is an integer, positive, negative, or zero, G is a polynomial in its arguments, and F includes all the terms of S not involving a_1 explicitly. If we write

$$F\left(a_0, \frac{S_2}{a_0}, \cdots, \frac{S_q}{a_0^{q-1}}\right) = \frac{1}{a_0^r}\Phi(a_0, S_2, \cdots, S_q)$$

where Φ is a polynomial in its arguments, we derive the equality $a_0^\lambda G = a_0^\mu S - a_0^\nu \Phi$, where λ, μ, ν are integers $\geqq 0$. Since S and Φ are seminvariants, G is also a seminvariant. Furthermore, G is from the manner of its formation divisible by a_1 and hence by

$$\beta = \prod_{t=0}^{p-1} (a_0 t + a_1) \equiv a_1^p - a_0^{p-1} a_1 \qquad \pmod{p}\ .$$

Treating the seminvariant G/β in like manner, we see that $S = a_0^q P$, where q is an integer, positive, negative, or zero, and P is a polynomial in $a_0, S_2, S_3, \cdots, S_q$. Hence we have proved the

THEOREM. *The seminvariants* $S_i (i = 1, 2, \cdots, q)$ *and* β *form a fundamental system of protomorphs of the binary q-ic form*, mod p, *p being a prime such that* $\binom{q}{j} \not\equiv 0$, mod p $(j = 1, 2, \cdots, q-1)$.

If the coefficients of $f(x, y)$ are integers, reduced mod p (or elements of any Galois field) a polynomial in the coefficients, invariant under the group of transformations considered in this paper, is called a modular seminvariant. Since the seminvariant β vanishes for every set of integral values of a_0, a_1 we have the following corollary.

COROLLARY. *Corresponding to every modular seminvariant S of a binary form none of whose prefixed binomial coefficients is divisible by p there is an*

[*] $\binom{q}{j} = q(q-1) \cdots (q-j+1)/j!$; if any $\binom{q}{j} \equiv 0$, mod p, our form is a special form.

integer $\lambda \geqq 0$ (*and hence an infinite number*) *such that* $a_0^\lambda S$ *is congruent,* mod p, *to a polynomial in the algebraic protomorphs.*

This corollary is closely related to Miss Hazlett's Corollary I, p. 195, American Journal of Mathematics, vol. 43 (1921).

III

Definition of a fundamental system of protomorphs of s binary forms: *Given s binary forms of order* $q_i (i=1, 2, \cdots, s)$

$$a_0^{(i)}\ x^{q_i}+\binom{q_i}{1}a_1^{(i)}\ x^{q_i-1}y+\ \cdots\ +a_{q_i}^{(i)}y^{q_i}$$

and p *a modulus not a factor of any* $\binom{q_i}{j}$ $(j=1, 2, \cdots, q_i-1)$, *we define* $K_1, K_2, \cdots, K_\lambda$, *a finite number of seminvariants of the s forms, to be a fundamental system of protomorphs of the s forms if they have the property that any seminvariant of the s forms is a rational function of* $K_1, K_2, \cdots, K_\lambda$.

It is a known fact that the $\sum_{i-1}^{s} q_i$ seminvariants*

$$S_1^{(i)},\ S_2^{(i)},\ \cdots,\ S_{q_i}^{(i)} \qquad (i=1, 2, \cdots, s)$$

and the $(s-1)$ joint seminvariants

$$J_i=a_0a_1^{(i)}-a_1a_0^{(i)} \qquad (i=2, 3, \cdots, s)$$

have the property that any algebraic seminvariant of our s forms is a rational function of these. In the following theorem we prove the fact, which seems very remarkable, that these algebraic seminvariants together with the single formal modular seminvariant

$$\beta_1=\prod_{t=0}^{p-1}(a_0^{(1)}t+a_1^{(1)})\equiv[a_1^{(1)}]^p-[a_0^{(1)}]^{p-1}a_1^{(1)} \qquad (\text{mod } p),$$

form a fundamental system of formal modular seminvariants of the s forms, viz.

THEOREM. *The* $\sum_{i=1}^{s} q_i$ *seminvariants* $S_1^{(i)}, S_2^{(i)}, \cdots, S_{q_i}^{(i)}$ $(i=1, 2, \cdots, s)$ *where* $S_1^{(i)}=a_0^{(i)}$, $S_2^{(i)}=a_0^{(i)}a_2^{(i)}-a_1^{(i)2}$, *etc. as in* §I, *the* $(s-1)$ *seminvariants* $J_i=a_0^{(1)}a_1^{(i)}-a_1^{(1)}a_0^{(i)}$ $(i=2, 3, \cdots, s)$, *and the single seminvariant*

$$\beta_1=\prod_{t=0}^{p-1}(a_0^{(1)}t+a_1^{(1)})\equiv[a_1^{(1)}]^p-[a_0^{(1)}]^{p-1}a_1^{(1)} \qquad (\text{mod } p),$$

* By $S_1^{(i)}, S_2^{(i)}, \cdots, S_{q_i}^{(i)}$ we mean the set of protomorphs in §I for the ith of our s forms.

are a fundamental system of formal modular protomorphs, mod p, *of the* s *binary forms*

$$a_0^{(i)}x^{q_i}+\binom{q}{1}a_1^{(i)}x^{q_i-1}y+\cdots+a_{q_i}^{(i)}y^{q_i}\quad(i=1,\,2,\,\cdots,s)$$

p being a prime such that no $\binom{q_i}{j}\equiv 0$, mod p.

Proof. As in §II,

$$a_2^{(i)}=\frac{\left[a_1^{(i)}\right]^2+S_2^{(i)}}{a_0^{(i)}},$$

$$a_3^{(i)}=\frac{\left[a_1^{(i)}\right]^3+3a_1^{(i)}S_2^{(i)}+S_3^{(i)}}{a_0^{(i)2}},$$

$$a_j^{(i)}=P(a_1^{(i)}\ ,S_1^{(i)}\ ,S_2^{(i)}\ ,\ \cdots\ ,S_j^{(i)})\ (i=1\ ,2\ ,\cdots,s\ ;j=4,5,6,\cdots,q_i)$$

where P is a polynomial with integral coefficients in its arguments; furthermore,

$$a_1^{(i)}=J_i+\frac{a_1^{(1)}a_0^{(i)}}{a_0^{(1)}}.$$

Making the above substitutions in any seminvariant

$$S(a_0^{(1)}\ ,a_1^{(1)}\ ,\ \cdots\ ,a_{q_1}^{(1)}\ ;\ \cdots\ ;a_0^{(s)}\ ,a_1^{(s)}\ ,\ \cdots\ ,a_{q_s}^{(s)}),$$

and separating into parts as in §II, we have

$$S=F(S_1^{(1)}\ ,\ \cdots\ ,S_{q_s}^{(s)};J_1,J_2,\ \cdots\ ,J_s)+a_0^{(1)^{\mu_1}}a_0^{(2)^{\mu_2}}\cdots a_0^{(s)^{\mu_s}}$$
$$\times G(a_1^{(1)},S_1^{(1)},\ \cdots,J_1,\ \cdots),$$

$\mu_1,\mu_2,\cdots,\mu_s$ being integers and G a polynomial in $a_1^{(1)}$ and the seminvariants $S_j^{(i)}$, J_k. As in §II, G is a seminvariant of the system, divisible by $a_1^{(1)}$ and hence by β_1; the theorem follows by induction.

An example of the protomorphic representation of joint seminvariants is here given. In the seminvariant, mod 5, of

$$a_1x^2+2b_1xy+c_1y^2\ \text{ and }\ a_2x^2+2b_2xy+c_2y^2,$$

$$S=-\sum_{t=0}^{4}(a_1t^2+2b_1t+c_1)^4(a_2t^2+2b_2t+c_2)^2$$

$$\equiv a_1^2a_2^2c_1^2+3a_1a_2^2b_1^2c_1+a_2^2b_1^4+a_2^2c_1^4+a_1^2a_2b_1b_2c_1+3a_1a_2b_1^3b_2$$

$$+2a_2b_1b_2c_1^3+3a_1^2b_1^2a_2c_2+3a_1^3a_2c_1c_2+a_1^3b_2^2c_1+a_1^2b_1^2b_2^2+3a_1a_2c_1^3c_2$$

$$+3a_2b_1^2c_1^2c_2+a_1b_1^2c_1^3+b_1^2b_2^2c_1^2+2a_1^3b_1b_2c_2+a_1b_1b_2c_1^2c_2+a_1^4c_2^2$$

$$+3b_1^3b_2c_1c_2+a_1^2c_1^2c_2^2+3a_1b_1^2c_1c_2^2+b_1^4c_2^2 \qquad \text{(mod 5)},$$

substitute

$$b_2=\frac{J+a_2b_1}{a_1}, \qquad c_1=\frac{b_1^2-\Delta_1}{a_1},$$

$$c_2=\frac{J^2+2a_2b_1J+a_2^2b_1^2-a_1^2\Delta_2}{a_1^2a_2},$$

where $\Delta_1=b_1^2-a_1c_1$, $\Delta_2=b_2^2-a_2c_2$ and $J=a_1b_2-a_2b_1$. After making the above substitutions and collecting terms, we find that

$$S=\frac{1}{a_1^4a_2^2}(a_1^4a_2^4\Delta_1^2+a_1^4\Delta_1^4+a_1^4a_2^2\Delta_1J^2+3a_1^6a_2^2\Delta_1\Delta_2+a_2^2\Delta_1^3J^2$$

$$+3a_1^2a_2^2\Delta_1^3\Delta_2+a_1^4J^4+a_1^8\Delta_2^2+3a_1^6\Delta_2J^2+\Delta_1^2J^4$$

$$+a_1^4\Delta_1^2\Delta_2^2+3a_1^2\Delta_1^2\Delta_2J^2+4\beta_1a_2^3\Delta_1J+4\beta_1a_2J^3+\beta_1a_1^2a_2\Delta_2J),$$

where

$$\beta_1=b_1^5-a_1^4b_1\ .$$

A much simpler case is that of

$$\beta_2=b_2^p-a_2^{p-1}b_2,$$

which is easily reduced to

$$\frac{J^p-a_1^{p-1}a_2^{p-1}J+a_2^p\beta_1}{a_1^p},$$

whence we derive the syzygy

$$a_1^p\beta_2-a_2^p\beta_1+a_1^{p-1}a_2^{p-1}J+J^p\equiv 0 \qquad (\text{mod } p).$$

IV

A necessary and sufficient condition that a polynomial in the coefficients of a binary q-ic form be a formal seminvariant, mod p, of that form is, obviously, that it be unaltered, mod p, by the substitution T on $a_0, a_1, \cdots, a_q$:

$$(1)\qquad \begin{pmatrix} a_0 & a_1 & \cdots & a_q \\ a_0 & a_0+a_1 & \cdots & a_0+\binom{q}{1}a_1+\binom{q}{2}a_2+\cdots+a_q \end{pmatrix},$$

p not being a factor of any $\binom{q}{k}$ in f.

Let

$$(2)\qquad R_j(t)=a_0t^j+\binom{j}{1}a_1t^{j-1}+\cdots+a_j \qquad (j=0, 1, 2, \cdots, q).$$

Then

$$R_j(0)=a_j, \quad\text{and}\quad TR_j(0)=R_j(1),$$

and in general

$$T^mR_j(0)=R_j(m) \qquad (m=1, 2, \cdots, p).$$

In particular

$$T^pR_j(0)=R_j(p)=R_j(0) .$$

Hence if for $R_i(t)$ we write R_i,

$$\sum_{t=0}^{p-1} R_0^{v_0}R_1^{v_1}\cdots R_q^{v_q} ,$$

where $v_0, v_1, \cdots, v_q$ are positive integers or zero, is a seminvariant.

Such a seminvariant we shall call a σ-seminvariant; a σ-seminvariant may, of course, be congruent to zero, mod p.

$$\Pi_1=\beta=\prod_{t=0}^{p-1} R_1(t)\equiv a_1^p-a_0^{p-1}a_1 \qquad (\text{mod } p),$$

the very important seminvariant which we have already met, is a particular case of

$$\Pi_j=\prod_{t=0}^{p-1} R_j(t)\equiv a_i^p+\cdots (\text{mod } p) \qquad (j=1, 2, \cdots, q).$$

These j seminvariants of a binary form we call π-seminvariants.

Now let

$$(3)\qquad S=\sum K_{k_0,k_1,\cdots,k_q}\, a_0^{k_0}a_1^{k_1}\cdots a_q^{k_q}$$

be any formal seminvariant, mod p, of a binary form f of order q with prefixed binomial coefficients no one of which is divisible by p, and let σ be a seminvariant of the kind which we call σ-seminvariants, viz.

$$(4)\qquad \sigma=\sum_{t=0}^{p-1} [R_0(t)]^{v_0}\cdots[R_q(t)]^{v_q} ,$$

where

$$R_0(t)=a_0,\ R_1(t)=a_0t+a_1,\ \cdots,\ R_q(t)=a_0t^q+\cdots+a_q.$$

Multiplying S by

$$a_0^{v} a_1^{v_1} \cdots a_q^{v_q}$$

and expanding, we have

$$a_0^{v_0} a_1^{v_1} \cdots a_q^{v_q} S = \sum L_{l_0, l_1, \cdots, l_q} a_0^{l_0} a_1^{l_1} \cdots a_q^{l_q}. \tag{5}$$

By use of the syzygies

$$a_1^p \equiv \beta + a_0^{p-1} a_1 \qquad (\text{mod } p),$$

$$a_j^p \equiv \Pi_j + \cdots \qquad (\text{mod } p) \ (j = 2, 3, \cdots, q),$$

we may express

$$\sum L_{l_0, l_1, \cdots, l_q} a_0^{l_0} a_1^{l_1} \cdots a_q^{l_q}$$

in the form

$$\sum M_{m_0, m_1, \cdots, m_q} a_0^{m_0} a_1^{m_1} \cdots a_q^{m_q} Q_{m_0, m_1, \cdots, m_q}(\beta_1, \Pi_1, \cdots, \Pi_q).$$

We shall then have the equality

$$a_0^{v_0} a_1^{v_1} \cdots a_q^{v_q} S \equiv \sum M_{m_0, m_1, \cdots, m_q} a_0^{m_0} a_1^{m_1} \cdots a_q^{m_q} Q_{m_0, m_1, \cdots, m_q} \ (\text{mod } p) \tag{6}$$

where each of $m_1, m_2, \cdots, m_q$ is less than p and the Q's are polynomials (with integral coefficients) in $\beta_1, \Pi_2, \cdots, \Pi_q$. The relation (6) and the $p-2$ congruences obtained by applying to (6) the substitution (1) $p-2$ times may be combined in the one relation

$$\begin{aligned}[R_0(t)]^{v_0}[R_1(t)]^{v_1} \cdots [R_q(t)]^{v_q} S \equiv \sum M_{m_0, m_1, \cdots, m_q} [R_0(t)]^{m_0} \cdots \\ \times [R_q(t)]^{m_q} Q_{m_0, \cdots, m_q} \ (\text{mod } p)\ (t = 0, 1, 2, \cdots, p-1).\end{aligned} \tag{7}$$

Adding the p congruences represented by (7) we have, since S and the Q's are seminvariants, and since σ has the value given in (4),

$$\sigma S \equiv \sum M_{m_0, m_1, \cdots, m_q} P_{m_0, m_1, \cdots, m_q} Q_{m_0, m_1, \cdots, m_q} \qquad (\text{mod } p), \tag{8}$$

where

$$P_{m_0, m_1, \cdots, m_q} \equiv a_0^{m_0} \sum_{t=0}^{p-1} [R_0(t)]^{m_1} \cdots [R_q(t)]^{m_q} \qquad (\text{mod } p); \tag{9}$$

since each of $m_1, m_2, \cdots, m_q$ is less than p,

$$[R_0(t)]^{m_1} \cdots [R_q(t)]^{m_q}$$

represents a finite number μ of seminvariants, S_i $(i = 1, 2, \cdots, \mu)$. We have thus proved the

THEOREM. *The product of any formal seminvariant S of a binary form f of order q, with prefixed binomial coefficients with respect to any prime p which is not a factor of any of the binomial coefficients* $\binom{q}{1}, \binom{q}{2}, \cdots, \binom{q}{q-1}$, *by any σ-seminvariant is a polynomial in a_0 and a finite number of σ-seminvariants and π-seminvariants.*

This theorem may also be stated thus:

THEOREM. *The seminvariants a_0, Π_i $(i=1, 2, \cdots, q)$ and S_j $(j=1, 2, \cdots, \mu)$ form a finite set of protomorphs of the binary form f.*

We have thus shown how to express any formal seminvariant S fractionally in terms of a finite number of seminvariants in a variety of ways. Some examples of the application of the above method follow.

Since

$$-\sum_{t=0}^{4}(b+at)^4\equiv a^4 \pmod{5},$$

and

$$D=a^2d^2-6abcd+4b^3d+4ac^3-3b^2c^2$$

is an (algebraic) invariant of the binary cubic, let $\sigma=a^4$ and $S=D$. Applying the method which has just been described, we write down

$$(10)\qquad -b^4D=-a^2b^4d^2+6ab^5cd-4b^7d-4ab^4c^3+3b^6c^2;$$

since $b^5\equiv\beta+a^4b$, mod 5,

$$(11)\qquad -b^4D=-a^2b^4d^2-4acd\beta-4a^5bcd-4b^2d\beta-4a^4b^3d-4ab^4c^3 \qquad (\mathrm{mod}\,5)\ .$$

Making the four seminvariant substitutions and adding, we have

$$(12)\qquad \begin{aligned} -a^4D\equiv a^2&\sum_{t=0}^{4}(at+b)^4(at^3+3bt^2+3ct+d)\\ +4a\beta&\sum_{t=0}^{4}(at^2+2bt+c)\ (at^3+3bt^2+3ct+d)\\ +4a^5&\sum_{t=0}^{4}(at+b)\ (at^2+2bt+c)\ (at^3+3bt^2+3ct+d)\\ +4\beta&\sum_{t=0}^{4}(at+b)^2(at^3+3bt^2+3ct+d)\\ +4a^4&\sum_{t=0}^{4}(at+b)^3(at^3+3bt^2+3ct+d)\\ +4a&\sum_{t=0}^{4}(at+b)^4(at^2+2bt+c)^3\\ +2\beta&\sum_{t=0}^{4}(at+b)\ (at^2+2bt+c)^2\\ +2a^4&\sum_{t=0}^{4}(at+b)^2(at^2+2bt+c)^2 \qquad (\mathrm{mod}\ p). \end{aligned}$$

Thus not only are all seminvariants, whether congruent to algebraic seminvariants or not, expressible fractionally in terms of algebraic seminvariants and β, but in turn all seminvariants, whether congruent to algebraic seminvariants or not, are expressible in terms of a and a finite number of seminvariants of the σ and π forms. By choosing $\sigma = a^{p-1} \equiv -\sum_{t=0}^{p-1} (at+b)^{p-1}$ we may express $a^{p-1}S$, where S is any seminvariant, in like manner. Since

$$(13) \qquad -\sum_{t=0}^{p-1} (at^2+2bt+c)^{p-1} \equiv a^{p-1}+\Delta^{(p-1)/2} \qquad (\mathrm{mod}\ p),$$

where $\Delta = b^2-ac (p>2)$, multiplication of any seminvariant S by c^{p-1} and application of this method gives an expression of $(a^{p-1}+\Delta^{(p-1)/2})S$ in terms of a and σ- and π-seminvariants; subtracting the expression for $a^{p-1}S$ we have an expression for $\Delta^{(p-1)/2}S$ in terms of a and σ- and π-seminvariants. Setting $S=\Delta^\gamma$ $(\gamma=1, 2, \cdots)$ and applying the present method we have the

THEOREM. *Δ^δ, where $\delta \geqq (p-1)/2$, is congruent to a polynomial in a the seminvariants β and* Π_2 *and the seminvariants*

$$\sum_{t=0}^{p-1} [R_1(t)]^{v_1} [R_2(t)]^{v_2} \textit{ where } v_1, v_2 < p.$$

By using the congruence proved in the following lemma we may readily prove the

THEOREM. *If D is the discriminant of the form $ax^3+3bx^2y+3cxy^2+dy^3$ and p is a prime of the form $3m+1$, D^δ, where $\delta \geqq (p-1)/6$, is congruent,* mod p, *to a polynomial in a, the seminvariants* Π_1, Π_2, Π_3 *and* $\sum_{t=0}^{p-1} [R_1(t)]^{v_1} \times [R_2(t)]^{v_2}$ $[R_3(t)]^{v_3}$ *(v_1, v_2, v_3 ranging over values $<p$).*

LEMMA. *If p is a prime of the form $3k+1$,*

$$a^{2(p-1)/3} - \sum_{t=0}^{p-1} (at^3+bt^2+3ct+d)^{2(p-1)/3}$$
$$\equiv \binom{2(p-1)/3}{(p-1)/3} D^{(p-1)/6} \qquad (\mathrm{mod}\ p),$$

where $D=a^2d^2-6abcd+4b^3d+4ac^3-3b^2c^2$, the discriminant of $ax^3+3bx^2y+3cxy^2+dy^3$.

Proof.

$$at^3+3bt^2+3ct+d = \frac{1}{a^2}[(at+b)^3+3\Delta(at+b)+S_3],$$

where $\Delta=ac-b^2$, $S_3=a^2d-3abc+2b^3$ and $a\neq 0$. Since $\sum_{t=0}^{p-1}t^k\equiv 0$, mod p, when k is 0 and when k is not a multiple of $p-1$ and $\sum_{t=0}^{p-1}t^k\equiv -1$, when k is a non-zero multiple of $p-1$,

$a^{2(p-1)/3}-\sum_{t=0}^{p-1}(at^3+3bt^2+3ct+d)^{2(p-1)/3}\equiv +$ [coefficient of t^{p-1} in the expansion of $(at^3+3bt^2+3ct+d)^{2(p-1)/3}]\equiv +$[coefficient of t^{p-1} in the expansion of $\dfrac{1}{a^{4(p-1)/3}}$ $\times\{(at+b)^3+3\Delta(at+b)+S_3\}^{2(p-1)/3}]$ $\equiv +\{$coefficient of t^{p-1} in the expansion of $\dfrac{1}{a^{4(p-1)/3}}(S_3+3\Delta at+a^3t^3)^{2(p-1)/3}+\dfrac{b}{a^{4(p-1)/3}}P(a,b,c,d)\}$, mod p, where $P.(a,b,c,d)$ is a polynomial.

Now the coefficient of t^{p-1} in the expansion of $(S_3+3\Delta at+a^3t^3)^{2(p-1)/3}$

$$\equiv a^{p-1}\sum_{m=0}^{(p-1)/6}\frac{\left[\frac{2}{3}(p-1)\right]!}{\left[\frac{p-1}{3}-m\right]!\left[\frac{p-1}{3}-2m\right]![3m]!}S_3{}^{(p-1)/3-2m}\Delta^{3m}3^{3m}\quad(\text{mod } p),$$

where $0!=1$.

For any m from 0 to $(p-1)/6$*

$$\frac{\left[\frac{2}{3}(p-1)\right]!\,3^{3m}}{\left[\frac{p-1}{3}-m\right]!\left[\frac{p-1}{3}-2m\right]![3m]!}$$
$$\equiv\frac{\left[\frac{2}{3}(p-1)\right]!\left[\frac{p-1}{6}\right]!2^{2m}}{\left[\frac{1}{3}(p-1)\right]!\left[\frac{1}{3}(p-1)\right]!\left[\frac{p-1}{6}-m\right]![m]!}\quad(\text{mod } p),$$

a relation which may be proved by noticing that it is equivalent to the relation

$$\frac{3^{3m}\left[\frac{p-1}{6}-m\right]!\,m!\left[\frac{p-1}{3}\right]!\left[\frac{p-1}{3}\right]!}{\left[\frac{p-1}{3}-m\right]!\left[\frac{p-1}{3}-2m\right]![3m]!2^{2m}}\equiv 1\quad(\text{mod } p)\,.$$

* For the following elegant proof of this relation I am indebted to Professor W. A. Hurwitz

This last relation is evidently true when $m=0$; and for $0\leqq m\leqq (p-1)/6$ when m is replaced by $m+1$, its left hand side is multiplied by

$$\frac{3^3(m+1)((p-1)/3-m)((p-1)/3-2m)((p-1)/3-2m-1)}{2^2((p-1)/6-m)(3m+1)(3m+2)(3m+3)},$$

which is readily proved congruent to unity, mod p. Hence

$$\begin{aligned} a^{p-1}\sum_{m=0}^{(p-1)/6}&\frac{[\frac{2}{3}(p-1)]!}{[(p-1)/3-m]!\,[(p-1)/3-2m]!\,[3m]!}S_3{}^{(p-1)/3-m}\Delta^{3m}3^{3m}\\ &\equiv\binom{2(p-1)/3}{(p-1)/3}a^{p-1}\sum_{m=0}^{(p-1)/6}\binom{(p-1)/6}{m}(S_3^2)^{(p-1)/6-m}(4\Delta^3)^m\\ &\equiv\binom{2(p-1)/3}{(p-1)/3}a^{p-1}(S_3^2+4\Delta^3)^{(p-1)/6}\\ &\equiv a^{4(p-1)/3}\binom{2(p-1)/3}{(p-1)/3}D^{(p-1)/6} \qquad \pmod{p}, \end{aligned}$$

the last congruence following from the algebraic identity

$$a^2D=S_3^2+4\Delta^3\ .$$

We have then proved that

$$a^{2(p-1)/3}-\sum_{t=0}^{p-1}(at^3+3bt^2+3ct+d)^{2(p-1)/3}\equiv\binom{2(p-1)/3}{(p-1)/3}D^{(p-1)/6}+bP(a,b,c,d) \pmod{p}.$$

It is well known that the left hand side of this last congruence is a formal modular invariant; we now proceed to prove that it is absolutely isobaric. Obviously

$$(at^3+3bt^2+3ct+d)^{2(p-1)/3}=\sum_{i=0}^{2(p-1)}P_i(a,b,c,d)t^i.$$

If we assign to a, b, c, d the weights 0, 1, 2, 3 respectively and to t the weight 1 and expand the left hand side, each term of this expansion will have the weight $2(p-1)$ and hence each P_i (a, b, c, d) t^i is absolutely isobaric and of weight $2(p-1)$, i. e. each $P_i(a, b, c, d)$ is absolutely isobaric and has the weight $2\ (p-1)-i$; this last is, of course, quite independent of t and from this point on we do not use the fact that we have assigned a weight to t. Now consider the following relation:

$$\begin{aligned} a^{2(p-1)/3}-\sum_{t=0}^{p-1}(at^3+3bt^2+3ct+d)^{2(p-1)/3}&=a^{2(p-1)/3}+a^{2(p-1)/3}\sum_{t=0}^{p-1}t^{2(p-1)}\\ +P_{2p-3}(a,b,c,d)\sum_{t=0}^{p-1}t^{2p-3}&+\cdots+P_{p-1}(a,b,c,d)\sum_{t=0}^{p-1}t^{p-1}\\ +\cdots+pP_0(a,b,c,d)&\equiv -P_{p-1}(a,b,c,d) \qquad \pmod{p}\ , \end{aligned}$$

since

$$\sum_{t=0}^{p-1} t^k \equiv 0, \text{ mod } p, \quad k=0 \text{ and } \not\equiv 0, \text{ mod } p-1,$$

$$\equiv -1, \text{ mod } p, \ k \text{ a non-zero multiple of } p-1.$$

We see therefore that each member of our congruence except $bP(a, b, c, d)$ is an absolutely isobaric formal modular invariant of weight $p-1$; accordingly, the same must be true of this remaining term unless it is congruent to zero, mod p. But if $bP(a, b, c, d)$ is an invariant divisible by b, it is also divisible, mod p, by $a+b$, whence

$$bP(a, b, c, d) \equiv (a+b)Q(a, b, c, d) \qquad (\text{mod } p),$$

where Q is a polynomial. But $bP(a, b, c, d)$, if it is $\not\equiv 0$, mod p, is absolutely isobaric and of weight $p-1$. Hence $(a+b)Q(a, b, c, d)$ is absolutely isobaric, and hence $Q(a, b, c, d)$ is not absolutely isobaric. Then let

$$Q(a, b, c, d) = Q_0(a, b, c, d) + Q_1(a, b, c, d) + \cdots + Q_k(a, b, c, d),$$

where each $Q_i\ (a, b, c, d) \not\equiv 0$, mod p, and is absolutely isobaric, Q_0 containing the terms of least weight, Q_1 those of next highest weight, etc. Then

$$bP(a, b, c, d) \equiv (a+b)Q(a, b, c, d) \equiv aQ_0 + \cdots + bQ_k \qquad (\text{mod } p).$$

Since the weight of Q_0 is $<$ the weight of Q_k, the weight of aQ_0 is $<$ the weight of bQ_k which contradicts the hypothesis that $bP(a, b, c, d)$ is absolutely isobaric of weight $p-1$. Hence $P\equiv 0$, mod p.

Thus the lemma has been proved for all a, b, c, d for which $a\neq 0$. For $a=0$, its truth may be verified directly.

Not every algebraic seminvariant of a binary form is congruent, with respect to some prime, to a polynomial in a and the σ- and π-seminvariants of that form. For example, if $p\geqq 7$, Π_1 and Π_2 are each of degree 7 and any σ-seminvariant

$$\sigma = \sum_{t=0}^{p-1} a^{v_0}(at+b)^{v_1}(at^2+2bt+c)^{v_2}$$

is of degree 3, since

$$\sum_{t=0}^{p-1} t^\lambda \equiv 0 \qquad (\text{mod } p),$$

for all $\lambda < p-1$. Hence any seminvariant of degree 2 with respect to any prime $\geqq 7$, which is a polynomial in a and the σ- and π-seminvariants of the binary quadratic is congruent to a numerical multiple of a^2; the algebraic seminvariant $ac-b^2$ is therefore not congruent, mod p $(p\geqq 7)$ to a polynomial in a, and the σ- and the π-seminvariants of the binary quadratic. However, the interesting and difficult problem presents itself, as remarked in I: Is every formal modular seminvariant, mod p, of a binary form congruent, mod p, to a polynomial in the algebraic seminvariants and the σ- and π-seminvariants of that form?

For the sake of simplicity of statement, attention has in this article been directed to seminvariants of one form only; the method of the present article is, however, applicable to the seminvariants of any number of forms, though we shall, of course, be confronted with what may be termed "mixed seminvariants" such as

$$\sum_{t=0}^{p-1} (a_0t^2+2a_1t+a_2)^{p-1}(b_0t^2+2b_1t+b_2)^{p-1},$$

where a_0, a_1, a_2 are coefficients of the form $(a_0, a_1, \cdots, a_{q_1})(x,y)^{q_1}$ and b_0, b_1, b_2 of the form $(b_0, b_1, \cdots, b_{q_2})(x, y)^{q_2}$.

The theorem for s forms is obviously as follows:

THEOREM. *The seminvariants of s binary forms* $(a_0, a_1, \cdots, a_q)(x,y)^{q_i}$ $(i=1, 2, \cdots, s)$*(every binomial coefficient* $\not\equiv 0$, mod p) *can be expressed fractionally in terms of* $a_0^{(i)}$ $(i=1, 2, \cdots, s)$, *σ-seminvariants, pure and mixed, and π-seminvariants of the s forms, the exponents of the σ-seminvariants all being* $< p$ *and the set consequently being finite.*

In the preceding sections we have, for simplicity, considered only formal invariants under linear non-singular transformations whose coefficients are integers reduced mod p. Our results are easily generalized; to obtain a generalization we consider as before a binary form of order q with prefixed binomial coefficients, but take the coefficients of our non-singular linear transformations to be elements of a $GF[p^n]$, where p is any prime not a factor of any of the prefixed binomial coefficients of the form.

Following the same method of proof as in §II we prove the

THEOREM. *The seminvariants* S_i $(i=1, 2, \cdots, q)$ *and* $\beta=b^{p^n}-a^{p^{n-1}}b$ *form a set of formal protomorphs of the binary q-ic form over the* $GF[p^n]$.

As in §III, we prove the theorem of that article; the fundamental system is changed in only one particular; we now have

$$\beta_1= \prod_t [a_0^{(1)}t+a_1^{(1)}] = [a_1^{(1)}]^{p^n}-[a_0^{(1)}]^{p^{n-1}} a_1,$$

the product being taken for all values of t in the $GF[p^n]$, and the equality being true in that field. As an example, the syzygy given in the last line of §III holds in the $GF[p^n]$, if

$$\beta_i= \prod_t [a_0^{(i)}t+a_1^{(i)}] \qquad (i=1, 2),$$

t ranging over all the elements of the $GF[p^n]$.

McGILL UNIVERSITY,
MONTREAL, CANADA