FUNDAMENTAL SYSTEMS OF FORMAL MODULAR SEMINVARIANTS OF THE BINARY CUBIC*

BY

W. L. G. WILLIAMS

Introduction

The present paper owes its origin to an attempt to solve the problem of Hurwitz in the case of the binary cubic form, viz., to find a set of formal modular invariants of the binary cubic form such that all others could be expressed as polynomials with integral coefficients with these as arguments. In this attempt I have not yet been successful, but methods have been developed which will aid in the solution of the problem and which have resulted in the solution of the similar, though less difficult problem of the determination of a fundamental system of formal modular seminvariants of the binary cubic form, modulis 5 and 7. These methods are so general in their nature that they could easily be used in the determination of a like system with respect to any prime modulus greater than three.

The problem of a fundamental system of the seminvariants of the cubic here solved in the case of the moduli 5 and 7 has already been solved by Dickson in the case of the modulus 5 and the methods which he used in that case could no doubt have been used for its solution in other cases. Whatever interest may attach to the present paper does not then lie in the fact that a solution exists nor yet in the fundamental system exhibited, but in whatever power or generality the methods used in the solution may have, and in the fact, hitherto unknown, that in the case of the cubic the number of members of a fundamental system is a function of the modulus instead of being a constant as in the case of the quadratic.

The method of annihilators, fundamental in the classical theory of invariantive concomitants, seems at first to be almost useless in the formal modular case. This is due to the fact that not only are these annihilators not linear but they are of an order which depends upon the modulus. Their complexity does indeed make the computation of seminvariants and invariants through their use very laborious in any except the simplest cases, but they furnish simple proofs of general theorems of far reaching significance.

* Presented to the Society, October 30, 1920.

A second method of importance is founded on the use of sums and products of linear functions of the coefficients of the form. This method is peculiarly adaptable to the modular in contrast to the algebraic case. Although this method has been previously used by Dickson and Hurwitz for the representation of certain invariants and seminvariants, in the present paper the interesting fact appears that all non-algebraic seminvariants of the cubic for the moduli considered can be easily and elegantly represented in this way, and one is strongly tempted to generalize and to say that this is true of all formal modular seminvariants, and to call this symmetric form their "natural" form.

In the algebraic theory many interesting developments have arisen from the arrangement of seminvariants and invariants in descending powers of the most advanced coefficient. An analogous method in the case of covariants has been used with marked success in the papers of Glenn on the covariants of binary forms. It is by the use of this method of leaders, now used so far as I know for the first time in the case of formal modular seminvariants and invariants, that the completeness of the system exhibited is proved. This part of the paper will no doubt appear to the reader as to the author tedious and awkward. The method of leaders is useful and elegant so long as it is applied in a search for concomitants and in their classification, but there is great need of more direct and powerful methods in the proofs of the completeness of systems.

In Section D, which is in the nature of a postscript to the paper, a fundamental system of protomorphic formal modular seminvariants is derived. In the algebraic case the fundamental system of seminvariants has only four members, in the formal modular case, modulo 5, this number is increased to 12, and when the modulus is 7, to 20; in the case of higher moduli the number is enormous. The protomorphs present a strong contrast; in the algebraic case the number of protomorphs in a fundamental system is 3, and by the addition to these three of the single seminvariant

$$\beta = \prod_{t=0}^{p-1} (at + b) \equiv a^{p-1} b - b^p \; (\text{modulo } p)$$

we obtain a fundamental system of protomorphs for any prime greater than three.

A. General theorems

If a binary form

$$f(x, y) = a_0 x^n + na_1 x^{n-1} y + \cdots + a_n y^n \quad (n \not\equiv 0, \text{modulo } p),$$

in which $a_0, a_1, \cdots, a_n$ are arbitrary variables, be transformed by the substitution

$$(1) \qquad \begin{aligned} x &= lX + mY, \\ y &= l' X + m' Y \end{aligned}$$

(l, m, l', m' being integers, taken modulo p) of determinant

$$D = \begin{vmatrix} l & m \\ l' & m' \end{vmatrix} \not\equiv 0 \ (\text{modulo } p),$$

a binary n-ic form

$$A_0 X^n + nA_1 X^{n-1} Y + \cdots + A_n Y^n$$

results, in which

$$A_0 = f(l, l'),$$

$$A_1 = l^{n-1} ma_0 + \cdots,$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot,$$

$$A_n = f(m, m').$$

A polynomial $P(a_0, \cdots, a_n)$ for which

$$P(A_0, \cdots, A_n) \equiv D^\lambda P(a_0, a_1, \cdots, a_n) \ (\text{modulo } p)$$

identically as to $a_0, \cdots, a_n$ after the A's have been replaced by their values in terms of the a's, under all transformations (1) is called a formal modular invariant, modulo p, of f. In like manner a polynomial

$$Q(a_0, a_1, a_2, \cdots, a_n)$$

which is unchanged, modulo p, by the transformation induced by all substitutions (in which t is integral)

$$x = X + tY,$$

$$y = \quad Y$$

of determinant unity is called a formal modular seminvariant of $f(x, y)$ modulo p. It is clear that all algebraic invariants and seminvariants are also formal modular invariants and seminvariants. In this paper formal modular seminvariants and invariants will be frequently referred to as formal seminvariants and invariants, or simply as seminvariants and invariants.

Invariants of this type were first considered by Hurwitz.* L. E. Dickson† in his *Madison Colloquium Lectures* first exhibited a fundamental system‡ of formal invariants and seminvariants of the binary quadratic form, modulo p, and a fundamental system of seminvariants of the binary cubic, modulo 5.

The object of the present paper is to derive a fundamental system of seminvariants for the same cubic form and the same modulus 5 (practically identical with the system of Dickson) by a different method and to apply the method

*Archiv der Mathematik und Physik (3), vol. 5 (1903).

† *The Madison Colloquium Lectures on Mathematics*, pp. 40–53.

‡ By a fundamental system is meant, as in the algebraic theory, a set of invariants (seminvariants) $S_0, \cdots, S_r$ such that any invariant (seminvariant) can be expressed as a polynomial $P(S_0, \cdots, S_r)$.

to the case of the modulus 7. The present method is general and in the case of several of the seminvariants a general form will be given.

I

In the theory of formal modular concomitants weight is defined exactly as in the algebraic case and plays the same prominent part. In the algebraic theory a concomitant all of whose terms are of the same weight is said to be isobaric and all concomitants which are not homogeneous and isobaric can be expressed as the sums of concomitants which have these properties. In like manner in the present theory a concomitant the weights of whose terms are congruent to each other with respect to the modulus q is said to be modularly isobaric, modulo q; concomitants of a binary form modulo p which are not homogeneous and modularly isobaric with respect to the modulus $p - 1$ can be expressed as sums of concomitants which have these properties. In this paper we confine our attention to such seminvariants and invariants.

II. An annihilator of formal seminvariants

Theorem. *A necessary and sufficient condition that $F(a_0, \cdots, a_n)$, a polynomial with integral coefficients, should be a formal seminvariant of the binary form*

$$a_0 x^n + na_1 x^{n-1} y + \cdots + a_n y^n$$

is that $\Theta F \equiv 0$ modulo p, where Θ is the operator

$$\Theta = \Omega + \frac{\Omega^p}{p!} + \frac{\Omega^{2p-1}}{(2p-1)!} + \cdots,$$

where

$$\Omega = a_0 \frac{\partial}{\partial a_1} + 2a_1 \frac{\partial}{\partial a_2} + \cdots + na_{n-1} \frac{\partial}{\partial a_n}$$

and Ω^q is its qth iteration, while $1, p, 2p - 1, \cdots$ have the common difference $p - 1$.

Proof. If we apply to the given form the substitution]

$$x = X + tY, \qquad y = Y \qquad (t \not\equiv 0, \text{modulo } p)$$

we derive the equivalent substitutions

$$\begin{aligned} A_0 &= a_0, \\ A_1 &= a_1 + a_0 t, \\ A_2 &= a_2 + 2a_1 t + a_0 t^2, \\ &\cdots\cdots\cdots\cdots\cdots, \\ A_n &= a_n + na_{n-1} t + \frac{n(n-1)}{2!} a_{n-2} t^2 + \cdots + a_0 t^n, \end{aligned}$$

where $A_0, A_1, A_2, \cdots, A_n$ are the coefficients in the transformed quantic. Expanding $F(A_0, A_1, \cdots, A_n)$ by Taylor's theorem* in powers of t and reducing the powers of t higher than the $(p-1)$th by Fermat's theorem (modulo p) we have

$$F(A_0, A_1, \cdots, A_n) \equiv F(a_0, a_1, \cdots, a_n)$$
$$+t\left(\Omega+\frac{\Omega^p}{p!}+\cdots\right)+\cdots+t^{p-1}\left(\frac{\Omega^{p-1}}{(p-1)!}+\cdots\right) \quad (\text{modulo } p).$$

Now a necessary and sufficient condition that $F(A_0, A_1, \cdots, A_n)$ be independent of t and so $\equiv F(a_0, a_1, \cdots, a_n)$, modulo p, which it is when $t \equiv 0$, modulo p, is that $\partial F/\partial t \equiv 0$, modulo p, and we see that $\partial F/\partial t = \Theta F$, whence the theorem follows.

Remark. It will be evident that $\Omega^p F = p!\,\Phi$ where Φ is a polynomial in $a_0, a_1, \cdots, a_n$ with integral coefficients. By the symbol $(\Omega^p/p!)F$ we mean the polynomial Φ, it being understood that the division by $p!$ has been performed. Similar remarks apply to the other terms of Θ. In the use of this annihilator of formal modular seminvariants no reduction with respect to the modulus is allowable until ΘF has been calculated without such reduction. Practice in the use of this annihilator will aid in the understanding of the proofs which follow and for this reason an example is added.

Example. To show that

$$K \equiv -b^4 - a^2bd + a^2c^2 + ab^2c - c^4 + bc^2d + b^2d^2 - acd^2$$

is a seminvariant, modulo 5, of the binary cubic,

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3.$$

In this case

$$\Omega = a\frac{\partial}{\partial b} + 2b\frac{\partial}{\partial c} + 3c\frac{\partial}{\partial d}$$

and

$$\Theta = \Omega + \frac{\Omega^5}{5!} + \frac{\Omega^9}{9!} + \cdots;$$

however since $\Omega^9K, \Omega^{13}K, \cdots = 0$,

$$\Theta K = \Omega K + \frac{\Omega^5 K}{5!}.$$

* Cf.: E. B. Elliott: *Algebra of Quantics*, p. 114. L. E. Dickson: These Transactions, vol. 8 (1907), p. 209. O. E. Glenn: American Journal of Mathematics, vol. 37 (1915), p. 73.

$$\Omega K = -2ab^3 + 3a^2bc - a^3d - 5ac^2d + 10b^2cd - 5bc^3,$$

$$\frac{\Omega^2 K}{20} = -ac^3 + b^3d,$$

$$\frac{\Omega^3 K}{20} = -6abc^2 + 3ab^2d + 3b^3c,$$

$$\frac{\Omega^4 K}{5!} = -ab^2c + a^2bd + b^4 - a^2c^2,$$

$$\frac{\Omega^5 K}{5!} = -3a^2bc + 2ab^3 + a^3d,$$

whence $\Theta K \equiv 0$, mod 5.

III

Definition. If a seminvariant S of the cubic

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

be arranged in descending powers of d thus,

$$S = S_0d^n + S_1d^{n-1} + \cdots + S_n,$$

S_0d^n is called the leading term of the seminvariant and S_0 is called the leader of the seminvariant.

Theorem. *The leader of any seminvariant of the cubic is a seminvariant of the quadratic when $n \not\equiv 0$, modulo p and either a seminvariant of the quadratic or a constant when $n \equiv 0$, modulo p.*

Proof.

$$\Theta S = (\Theta S_0)d^n + \Bigg\{\Theta S_1 + 3cnS_0 + \frac{3cn}{(p-1)!}(\Omega^{p-1}S_0)$$
$$+ \frac{6nb}{2!(p-2)!}(\Omega^{p-2}S_0) + \frac{6na}{3!(p-3)!}(\Omega^{p-3}S_0) + \cdots\Bigg\}d^{n-1} + \cdots.$$

Since ΘS must vanish identically, modulo p,

$$\Theta S_0 \equiv 0 \quad (\text{modulo } p),$$
$$\Theta S_1 \equiv -3cnS_0 - \cdots \quad (\text{modulo } p),$$

which shows that S_0 is a constant or a seminvariant of the quadratic $ax^2 + 2bxy + cy^2$ [for it contains no terms involving d and is therefore annihilated by Θ when $\Omega = a(\partial/\partial b) + 2b(\partial/\partial c)$]. If $n \not\equiv 0$, modulo p, S_0 cannot be a constant for in that case ΘS would involve a constant multiple of cd^{n-1} and consequently ΘS would not be congruent to zero, modulo p.

If S_0 is an algebraic seminvariant and hence annihilated by Ω the second congruence above reduces to $\Theta S_1 \equiv 0$ (modulo p) when $n \equiv 0$, modulo p, and in this case S_1 is a seminvariant, considerations of homogeneity showing us that it cannot be a constant.

IV

If the cubic

$$F = ax^3 + 3bx^2 y + 3cxy^2 + dy^3$$

be changed into

$$F' = AX^3 + 3BX^2 Y + 3CXY^2 + DY^3$$

by the substitution

$$x = X + Y, \qquad y = Y,$$

then

$$A = a, \qquad B = b + a, \qquad C = c + 2b + a, \qquad D = d + 3c + 3b + a;$$

and the substitution

$$A = -d, \qquad D = a, \qquad B = c, \qquad C = -b,$$

is induced on the coefficients of F by

$$x = Y, \qquad y = -X.$$

Any function of a, b, c, d which is invariant under the first of these substitutions is a seminvariant of F, modulo p,* for if

$$F(a, b, c, d) \equiv F(a,\ b + a,\ c + 2b + a,\ d + 3c + 3b + a) \ \text{(modulo } p\text{)},$$

repeating the substitution $(t - 1)$ times we have

$$F(a, b, c, d) \equiv F(a,\ b + at,\ c + 2bt + at^2,\ d + 3ct + 3bt^2 + at^3) \ \text{(modulo } p\text{)} \quad (t = 1, 2, 3, \cdots, p - 1).$$

But these congruences simply state the truth of the condition that $F(a, b, c, d)$ should be a seminvariant according to the definition given above. All functions of a, b, c, d which are invariant under both sets of transformations are invariants of F, modulo p.†

Dickson has given

$$F_t(a, b, c, d) = a(t^3 - 3kt - j) + 3b(t^2 - k) + 3ct + d \qquad (j, k = 0, 1, 2, \cdots, p - 1)$$

* This fact is, of course, well known; I introduce a proof of it here because it is fundamental for all that follows and because I do not know where in the literature of the subject to refer the reader for a proof.

† *Madison Colloquium Lectures*, p. 49; these Transactions, vol. 8 (1907), pp. 207, 208.

as typical linear polynomials such that

$$F_t(a,\ b+a,\ c+2b+a,\ d+3c+3b+a) = F_{t+1}(a,b,c,d).$$

It is easy to show that every linear polynomial having this property can be obtained from the given one by a proper choice of j and k, or is a constant multiple of one that can be so obtained. Dickson has also given

$$a(t^2-k)+2bt+c \qquad \text{and} \qquad at+b$$

as linear polynomials in a, b, c and a, b, respectively, with similar properties and has pointed out that

$$\delta_{jk} = \prod_{t=0}^{p-1} \{a(t^3-3kt-j)+3b(t^2-k)+3ct+d\} \quad (j, k = 0, \cdots, p-1),$$

$$\gamma_k = \prod_{t=0}^{p-1} \{a(t^2-k)+2bt+c\} \qquad (k = 0, \cdots, p-1)$$

and

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

are seminvariants.* It is obvious that

$$\sum_{t=0}^{p-1} f[a(t^3-3kt-j)+3b(t^2-k)+3ct+d,\ a(t^2-k)+2bt+c,\ at+b]$$

are also seminvariants, f being any polynomial in its arguments with integral coefficients.

V

Theorem. *The sum of the coefficients of the powers of t whose exponents are congruent to zero, modulo $p-1$, the exponent zero itself excepted, in the expansion in powers of t of any polynomial in one or more of the functions $(at^3+3bt^2+3ct+d)$, $(at^2+2bt+c)$, $(at+b)$ is a seminvariant of the cubic, modulo p.*

Proof. By Article IV

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

is a seminvariant of the cubic, modulo p. Now suppose P to be expanded so that

$$P = S_0 + S_1 t + \cdots + S_n t^n.$$

Then

$$\sum_{t=0}^{p-1} P = \sum_{t=0}^{p-1} S_0 + S_1 \sum_{t=0}^{p-1} t + \cdots + S_n \sum_{t=0}^{p-1} t^n.$$

Since

$$\sum_{t=0}^{p-1} t^r \equiv 0, \text{ modulo } p,$$

* *Madison Colloquium Lectures,* pp. 43 and 49.

when $r = 0$ and when $r \not\equiv 0$, modulo $p - 1$, and

$$\sum_{t=0}^{p-1} t^r \equiv -1, \text{ modulo } p,$$

when $r \neq 0$, but is congruent to zero, modulo $p - 1$,* therefore

$$\sum_{t=0}^{p-1} P = -(S_{p-1} + S_{2(p-1)} + \cdots)$$

which proves the theorem.

If we ascribe to t the weight 1 and to a, b, c, d the weights $0, 1, 2, 3$ respectively, P is absolutely isobaric, and consequently $S_{p-1}, S_{2(p-1)}, \cdots$ differ in weight by multiples of $p - 1$. Therefore

$$\sum_0^{p-1} P \quad \text{and} \quad (S_{p-1} + S_{2(p-1)} + \cdots)$$

are modularly isobaric, modulo $p - 1$.

VI

THEOREM. *If any formal modular seminvariant S be operated upon with the differential operators Ω, $F = a(\partial/\partial c) + 3b(\partial/\partial d)$ and $\partial/\partial d$, formal modular seminvariants result.*

Proof.† $S = \sum (a^r b^s c^t d^u)$. Since S is a seminvariant

$$\sum (a^r b^s c^t d^u) \equiv \sum \{a^r (b + a)^s (c + 2b + a)^t (d + 3c + 3b + a)^u\} \quad (\text{modulo } p).$$

Operating on this congruence successively with Ω, F, and $\partial/\partial d$ we have respectively

$$\begin{aligned}(1)\quad & \sum (sa^{r+1} b^{s-1} c^t d^u + 2ta^r b^{s+1} c^{t-1} d^u + 3ua^r b^s c^{t+1} d^{u-1}) \\ & \equiv \sum \{sa^{r+1} (b + a)^{s-1} (c + 2b + a)^t (d + 3c + 3b + a)^u \\ & + 2ta^r (b + a)^{s+1} (c + 2b + a)^{t-1} (d + 3c + 3b + a)^u \\ & + 3ua^r (b + a)^s (c + 2b + a)^{t+1} (d + 3c + 3b + a)^{u-1}\} \quad (\text{modulo } p),\end{aligned}$$

$$\begin{aligned}(2)\quad & \sum \{ta^{r+1} b^s c^{t-1} d^u + 3ua^r b^{s+1} c^t d^{u-1}\} \\ & \equiv \sum \{ta^{r+1} (b + a)^s (c + 2b + a)^{t-1} (d + 3c + 3b + a)^u \\ & + 3ua^r (b + a)^{s+1} (c + 2b + a)^t (d + 3c + 3b + a)^{u-1}\} \quad (\text{modulo } p),\end{aligned}$$

* Glenn, these Transactions, vol. 20 (1919), p. 156. Vandiver, Annals of Mathematics, ser. 2, vol. 18 (1916), p. 105.

† The proof as here given does not hold for terms in which one or more of $r, s, t, u \equiv 0$, modulo p; the reader will have no difficulty in extending the proof to such cases.

and

$$\sum ua^r b^s c^t d^{u-1} \equiv \sum \{ua^r (b+a)^s (c+2b+a)^t (d+3c + 3b+a)^{u-1}\} \pmod{p}. \tag{3}$$

The congruences (1), (2), and (3) demonstrate the truth of the theorem.

VII

THEOREM. *In any seminvariant of the cubic* (*modulo* p)

$$S = S_0 d^{pq+r} + S_1 d^{pq+r-1} + \cdots + S_r d^{pq} + \cdots + S_{pq+r} \quad (p > r > 0,\ q \geqq 0),$$

$$S_1 d^{pq+r-1}, \cdots, S_r d^{pq}$$

all occur and the terms of highest weight in them are of the same absolute weight as the term or terms of highest weight in $S_0 d^{pq+r}$.

Proof. Let $H_0, H_1, \cdots, H_r$ be the terms of highest weight in $S_0, S_1, \cdots, S_r$ respectively.

$$\begin{aligned}\Theta S = (\Theta S_0) d^{pq+r} &+ \{3(pq+r) cH_0 + \Omega H_1 + \text{terms of lower weight}\} d^{pq+r} \\ &+ \{3(pq+r-1) cH_1 + \Omega H_2 + \text{terms of lower weight}\} d^{pq+r-1} \\ &+ \cdots\cdots\cdots\cdots\cdots\cdots \\ &+ \{3(pq+1) cH_{r-1} + \Omega H_r + \text{terms of lower weight}\} d^{pq} \\ &+ \cdots\cdots\cdots\cdots\cdots\cdots.\end{aligned}$$

Since

$$\Theta S \equiv 0 \pmod{p},$$

equating the coefficients of $d^{pq+r-1}, \cdots, d^{pq}$ to zero, modulo p, and paying attention to weights, we have:

weight of cH_0 = weight of ΩH_1, i.e., weight of $H_0 d^{pq+r}$ = weight of $H_1 d^{pq+r-1}$,

weight of cH_1 = weight of ΩH_2, i.e., weight of $H_1 d^{pq+r-1}$ = weight of $H_2 d^{pq+r-2}$,

. . . . ,

weight of cH_{r-1} = weight of ΩH_r, i.e., weight of $H_{r-1} d^{pq+1}$ = weight of $H_r d^{pq}$,

whence we see that weight of $H_0 d^{pq+r}$ = weight of $H_r d^{pq}$.

The existence of H_0 necessitates the existence of $H_1, H_2, \cdots, H_r$.

VIII

THEOREM. *The seminvariants whose leading terms are βd^{q-1} $(q \geqq 1)$, where β is the seminvariant*

$$\prod_{t=0}^{p-1} (at+b) \equiv b^p - a^{p-1} b \text{ (modulo } p),$$

are sums of seminvariants whose leading terms are numerical multiples of

$$a^2 \Delta^{(p-3)/2} d^q, \qquad \textit{where} \qquad \Delta = b^2 - ac.$$

Proof. In the identity

$$a(at^2+2bt+c)^{p-2}(at^3+3bt^2+3ct+d)^q$$
$$+ 2\left\{ (b^2-ac)t + \frac{bc-ad}{2} \right\}(at^2+2bt+c)^{p-2}(at^3+3bt^2+3ct+d)^{q-1}$$
$$= (at+b)(at^2+2bt+c)^{p-1}(at^3+3bt^2+3ct+d)^{q-1} \qquad (q \geqq 1)$$

the coefficients of like powers of d on the two sides of the equality sign are identical. Furthermore, the sum of the coefficients of t^{p-1}, $t^{2(p-1)}$, $\cdots$ in the expansion of the first quantity on the left-hand side of the equality sign is a seminvariant, by Article V above; also the sum of the coefficients of the same powers of t in the expansion of the quantity on the right side is a seminvariant, and the same must be true in the case of the second quantity on the left-hand side in virtue of the identity. Let us call the seminvariants arising from the first, second, and third of these quantities S_1, S_2, S_3, respectively; then $S_1 + S_2 \equiv S_3$, modulo p. The coefficient of d^q in S_3 is evidently zero; consequently the leading terms of S_1 and S_2 differ only in sign. We propose to prove in Lemma I that the leading term of S_1 is

$$-\tfrac{1}{2}a^2 \Delta^{(p-3)/2} d^q \qquad (q \geqq 1),$$

and it will then be clear that the leading term of S_2 is

$$\tfrac{1}{2}a^2 \Delta^{(p-3)/2} d^q \qquad (q \geqq 1);$$

in Lemma II it will be shown that the leading term of S_3 is

$$\beta d^{q-1} \qquad (q \geqq 1).$$

The proof of these two lemmas will complete the proof of the theorem.

LEMMA I. *The leading term of S_1 is*

$$-\tfrac{1}{2}a^2 \Delta^{(p-3)/2} d^q \qquad (q \geqq 1).$$

Proof. The coefficient of d^q, the highest power of d occurring in S_1, is simply the coefficient of t^{p-1} in $a(at^2+2bt+c)^{p-2}$, and this coefficient is

a times the coefficient of t^{p-1} in $(at^2 + 2bt + c)^{p-2}$. We must now calculate this latter coefficient. Ascribing to t, a, b, c the same weights as previously, $(at^2 + 2bt + c)^{p-2}$ is (absolutely) isobaric, weight $2p - 4$. The term in t^{p-1} is then $kA_{p-3}\,t^{p-1}$, k being a constant and A_{p-3} a homogeneous, (absolutely) isobaric function of a, b, c of weight $p - 3$. kA_{p-3} is then a homogeneous, (absolutely) isobaric seminvariant of the quadratic and must be a function of a and Δ only.* The only such function of a and Δ of degree $p - 2$ and weight $p - 3$ is $ka\Delta^{(p-3)/2}$. As the coefficient of ab^{p-3} in the coefficient of t^{p-1} is $(p - 2)2^{p-3}$,

$$k = (p - 2)2^{p-3} \equiv -2\frac{2^{p-1}}{2^2} \equiv -\tfrac{1}{2}\,(\mathrm{mod}\, p).$$

The lemma is now proved.

Lemma II. *The leading term of S_3 is βd^{q-1}.*

Proof. The coefficient of d^{q-1}, the highest power of d occurring in S_3, is the sum of the coefficients of t^{p-1} and t^{2p-2} in

$$(at + b)(at^2 + 2bt + c)^{p-1}.$$

We propose to show that the sum of these coefficients is β.

Consider the expansion

$$(at^2 + 2bt + c)^p = a^p t^{2p} + A_1 t^{2p-1} + \cdots + A_p t^p + \cdots + A_{2p-2}.$$

Differentiating and dividing by $2p$, we have

$$(at^2 + 2bt + c)^{p-1}(at + b) = a^p t^{2p-1} + \frac{2p-1}{2p} A_1 t^{2p-2}$$
$$+ \cdots + \tfrac{1}{2}A_p t^{p-1} + \cdots + \frac{A_{2p-1}}{2p}.$$

Let us first determine A_p; this can be done by differentiating the next to last identity p times, setting $t = 0$ and dividing by $p!$ To do this we proceed as follows:

$$(at^2 + 2bt + c)^p = a^p(t + \alpha)^p(t + \gamma)^p,$$

where

$$\alpha = \frac{b + \sqrt{b^2 - ac}}{a}, \quad \gamma = \frac{b - \sqrt{b^2 - ac}}{a},$$

$$\frac{\partial^p}{\partial t^p}(at^2 + 2bt + c)^p = a^p\left\{\frac{\partial^p}{\partial t^p}[(t + \alpha)^p(t + \gamma)^p]\right\}.$$

Applying Leibniz's theorem

$$\frac{\partial^p}{\partial t^p}[(t + \alpha)^p(t + \gamma)^p] = p!(t + \alpha)^p + p^2(\qquad) + p!(t + \gamma)^p.$$

Setting $t = 0$ and multiplying by a^p we have

* Dickson, *Madison Colloquium Lectures*, p. 42 et seq.

$$\left\{\frac{\partial^p}{\partial t^p}(at^2+2bt+c)^p\right\}_{t=0} = p!(\alpha^p+\gamma^p)a^p + p^2a^p(\qquad).$$

But

$$\alpha^p+\gamma^p = 2\frac{b^p}{a^p}+p(\qquad).$$

Therefore

$$(at^2+2bt+c)^p = p!\,2b^p + p^2(\qquad).$$

Dividing by $p!$, $A_p \equiv 2b^p$, modulo p, and the coefficient of t^{p-1} in the second expansion above, namely $\frac{1}{2}A_p \equiv b^p$, modulo p. It is immediately evident that $A_1 = 2pa^{p-1}b$. Therefore the coefficient of t^{2p-2}, viz.,

$$\frac{2p-1}{2p}A_1 \equiv -a^{p-1}b, \text{ modulo } p.$$

Hence the lemma is proved.

IX. Seminvariants led by a

Theorem. *Any seminvariant led by a is either a itself or has the same leading term as a* $(\delta_{00})^r$, *where* $r \geqq 1$, *and* δ_{00} *is the seminvariant obtained by setting* $j=0$, $k=0$ *in the* δ_{jk} *mentioned in Article IV.*

Proof. Let a seminvariant led by a be

$$S = ad^q + A_1d^{q-1} + \cdots + A_q.$$

Operating on this with Θ we get a term $3qacd^{q-1}$, unless $q \equiv 0$, modulo p. Supposing for the moment that $q \not\equiv 0$, modulo p, we see that another term mus+ occur in the result of the operation which is congruent to $-3qacd^{q-1}$, modulo p, in order that the seminvariant may be annihilated. Such a term could only come from $-3qbcd^{q-1}$. As this term must occur in the original seminvariant it too is operated on by Θ; operating on it we get a term $-6qb^2d^{q-1}$, which could not be made to disappear in the attempted annihilation as a corresponding term could not arise in the operation. Thus it follows that S is not a seminvariant when $q \not\equiv 0$, modulo p. A seminvariant $ad^q + \cdots$ exists for every value of q such that $q \equiv 0$, modulo p; when $q = 0$, the seminvariant is a itself and when $q = pr$ $(r \geqq 1)$, it is $a(\delta_{00})^r$.

X. Seminvariants led by γ^r

Let such a seminvariant be $\gamma_0^r d^q + \cdots$. In this seminvariant there is a term $c^{pr}d^q$; operating on this with Θ we get $(q \not\equiv 0$, mod $p)$ $3qc^{pr+1}d^{q-1}$ and such a term could arise in the operation in no other way. Consequently the supposed seminvariant cannot exist as it cannot be annihilated by Θ. When $q \equiv 0$, mod p, a seminvariant $\gamma_0^r d^q$ exists for every such value of q, but every such seminvariant must have the same leading term as $\gamma_0^r(\delta_{00})^{q/p}$ $(q \geqq 0)$.

XI. Seminvariants led by $a\gamma_0^r$

Let such a seminvariant be $a\gamma_0^r d^q + \cdots$. A term $ac^{pr} d^q$ appears in the seminvariant. Operating with Θ we get ($q \not\equiv 0$, modulo p) $3qac^{pr+1} d^{q-1}$ and another term must appear in the operation which will cancel with this if S is a seminvariant. This term must come from a multiple of $bc^{pr+1} d^{q-1}$. There must be another term of this sort in order that the seminvariant be annihilated; this last could only come from a multiple of $b^2 c^{pr-1} d^q$, but the existence of such a term would contradict the original hypothesis that the coefficient of d^q in the seminvariant was divisible by a. Consequently, for values of q not congruent to zero, modulo p, there exist no seminvariants whose leading terms are $a\gamma_0^r d^q$; for every value of q such that $q \equiv 0$, modulo p, there exists such a seminvariant, viz., $a\gamma_0^r$ or $a\gamma_0^r(\delta_{00})^{pr}$, according as $q = 0$ or $q = pr'$ ($r' \geqq 1$). Accordingly any seminvariant $a\gamma_0^r d^q + \cdots$ involving d has as a leading term the same leading term as $a\gamma_0^r(\delta_{00})^{pr}$.

XII. Seminvariants whose leading terms are d^q

A seminvariant $d^q + \cdots$ must be annihilated if operated upon with Θ. If $q \not\equiv 0$, modulo p, a term $3qcd^{q-1}$, which is not congruent to zero, modulo p, appears in the result of the operation. As this term cannot be obained in any other way $d^q + \cdots$ cannot be annihilated and consequently is not a seminvariant.

If $q \equiv 0$, modulo p, there exists a seminvariant $d^q + \cdots$ for every value of q, viz., $(\delta_{00})^{q/p}$. Thus we have shown that from δ_{00} we can construct a seminvariant with the same leading term as any existing seminvariant whose leading term is d^q.

B. A fundamental system of formal seminvariants of the cubic modulo 5

XIII. Seminvariants led by a^2; seminvariants led by a^r ($r \geqq 3$)

Seminvariants led by a^2 are the algebraic seminvariants,

$$S_3 = a^2 d - 3abc + 2b^3,$$

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

and the formal modular seminvariants* (modulo 5):

* I have followed the notation of Dickson (*Madison Colloquium Lectures*, p. 52) because his σ_6 and mine have the same leading term, and the leading term of my σ_5 differs only in sign from that of his.

$$\sigma_5 \equiv -\sum_{t=0}^{4}(at^2+2bt+c)^2(at^3+3bt^2+3ct+d)^3$$

$$\equiv a^2d^3+(abc+b^3)d^2+(b^2c^2+2ac^3+a^2b^2+4ac^3)d+3a^4b$$

$$+2a^2bc^2+2ab^3c+3b^5+4bc^4, \quad \text{mod } 5,$$

$$\sigma_6 \equiv -\sum_{t=0}^{4}(at^2+2bt+c)^2(at^3+3bt^2+3ct+d)^4$$

$$\equiv a^2d^4+(3abc+3b^3)d^3+(2b^2c^2+3a^3c+4ac^3+2a^2b^2)d^2$$

$$+(2a^4b+3a^2bc^2+3ab^3c+2b^5+bc^4)d+c^6+4a^2b^4+4a^4c^2$$

$$+a^2c^4+b^4c^2+a^6, \quad \text{mod } 5.$$

Now multiplying these seminvariants whose leading terms are a^2d^2, a^2d^3, and a^2d^4 by $(\delta_{00})^r$, we obtain seminvariants whose leading terms are a^2d^{1+5r}, a^2d^{2+5r}, a^2d^{3+5r}, a^2d^{4+5r} $(r \geqq 1)$. We have thus constructed seminvariants whose leading terms are a^2d^q $(q \geqq 1)$.

By multiplying these seminvariants by the proper power of a we can construct a seminvariant whose leading term is a^td^q, where t is any integer greater than or equal to 2. We have thus shown that any seminvariant led by a^2 or any higher power of a has the same leading term as a seminvariant which can be constructed from a, S_3, D, σ_5, σ_6, and δ_{00}.

XIV. Seminvariants led by Δ^r $(r \geqq 1)$

Seminvariants whose leading terms are Δd and Δd^2 are

$$\sigma_3 \equiv \frac{1}{2}\sum_{t=0}^{4}(at^3+3bt^2+3ct+d)^3 \equiv (b^2-ac)d+2a^2b+3bc^2, \quad \text{mod } 5,$$

and the invariant[*]

$$K \equiv \sum_{t=0}^{4}(at^3+3bt^2+3ct+d)^4+a^4$$

$$\equiv (b^2-ac)d^2+(bc^2-a^2b)d-b^4-c^4+a^2c^2+ab^2c, \quad \text{mod } 5.$$

By multiplying Δ, σ_3, and K by $(\delta_{00})^r$ we obtain seminvariants whose leading terms are Δd^{5r}, Δd^{5r+1}, and Δd^{5r+2} $(r \geqq 1)$. That no seminvariants exist whose leading terms are Δd^{5r+3} and Δd^{5r+4} is evident from Article VII above.

$\Delta\sigma_3$, ΔK, $\sigma_3 K$, and K^2 are seminvariants whose leading terms are $\Delta^2 d$,

[*] K as here given differs only in sign from the K given by Dickson: *Madison Colloquium Lectures*, p. 51. Cf. also: Hurwitz, Archiv der Mathematik und Physik (3), vol. 5 (1903), p. 25; Dickson, these Transactions, vol. 8 (1907), p. 221; ibid., vol. 10 (1909), p. 154, footnote; Dickson, Bulletin of the American Mathematical Society, vol. 14 (1908), p. 316.

$\Delta^2 d^2$, $\Delta^2 d^3$, $\Delta^2 d^4$. Multiplying these and Δ^2 by $(\delta_{00})^r$ we have seminvariants whose leading terms are $\Delta^2 d^q$ $(q \geqq 1)$.

By multiplying these seminvariants by the proper power of Δ we have (together with those just given) seminvariants whose leading terms are $\Delta^r d^q$ where r is any integer greater than or equal to 2. We have thus shown that any existing seminvariant led by any power of Δ, has the same leading term as a seminvariant which can be constructed from Δ, σ_3, K, and δ_{00}.

XV. Seminvariants led by $a^r\Delta^s$ $(r, s \geqq 1)$

Seminvariants with leading terms $a\Delta d$, $a\Delta d^2$, $a\Delta d^3$, and $a\Delta d^4$ are* $a\sigma_3$, aK,

$$\begin{aligned} G_1 &\equiv \frac{1}{2}\sum_{t=0}^{4}(at^2+2bt+c)^3(at^3+3bt^2+3ct+d)^3 \\ &\equiv a\Delta d^3+(a^3b-abc^2)d^2+(2ac^4-a^5-ab^4-a^2b^2c)d-bc^5+b^5c \\ &\qquad\qquad +a^4bc-2ab^3c^2+2a^2bc^3, \quad \text{mod } 5, \\ \sigma_7 &\equiv \frac{1}{2}\sum_{t=0}^{4}(at^2+2bt+c)^3(at^3+3bt^2+3ct+d)^4 \\ &\equiv a\Delta d^4+(2abc^2+3a^3b)d^3+(3a^5+4ac^4+3a^2b^2c+3ab^4)d^2 \\ &\qquad +(bc^5-b^5c-a^4bc+2ab^3c^2+3a^2bc^3)d+(3c^7+3a^2c^5+ab^2c^4 \\ &\qquad +2b^4c^3+4a^5b^2+3ab^6+2a^3b^2c^2+a^4c^3-a^2b^4c), \quad \text{mod } 5. \end{aligned}$$

From these by multiplying by powers of δ_{00} and then by $a^{r-1}\Delta^{s-1}$ $(r, s \geqq 2)$ we obtain seminvariants having the same leading terms as any seminvariant led by any power of a multiplied by any power of Δ.

XVI. Seminvariants led by $a^r\Delta^s\gamma_0^t\beta^u$ $(r, s, t \geqq 0;\ u \geqq 1)$

We have shown in Article VIII above how to express a seminvariant $\beta d^{q-1}+\cdots$ $(q>0)$ as the sum of seminvariants whose leading terms are numerical multiples of $a^2\Delta^{(p-3)/2}d^q$. For the modulus 5 we may verify by actual multiplication that

$$\begin{aligned} \beta &\equiv 2(u^2\sigma_3-\Delta S_3), && \text{mod } 5, \\ \beta d+\cdots &\equiv a^2K-\Delta D, && \text{mod } 5, \\ \beta d^2+\cdots &\equiv \Delta\sigma_5-aG_1, && \text{mod } 5, \\ \beta d^3+\cdots &\equiv DK-\Delta\sigma_6, && \text{mod } 5, \\ \beta d^4+\cdots &\equiv \sigma_5K-a^2\Delta\delta_{00}, && \text{mod } 5. \end{aligned}$$

Multiplying these by $(\delta_{00})^r$ $(r \geqq 1)$, we obtain (together with those just

* $2g_1 = G + a\delta_{00} + a\Delta\sigma_3 + 3a^3S_3$, modulo 5, G being the invariant G of *Madison Colloquium Lectures*, p. 50.

given) seminvariants whose leading terms are βd^q $(q \geqq 0)$. Multiplying these by $a^r \Delta^s \gamma_0^t \beta^{u-1}$ $(r, s, t \geqq 0;\ u \geqq 1)$, we obtain seminvariants whose leading terms are $a^r \Delta^s \gamma_0^t \beta^u d^q$ $(q \geqq 0)$. Thus we see that from a, Δ, S_3, σ_3, D, K, σ_5, σ_6, γ_0, and δ_{00} we can make up seminvariants having the same leading terms as any seminvariant led by $a^r \Delta^s \gamma_0^t \beta^u$.

XVII. Seminvariants led by $a^r \gamma_0^t$; seminvariants led by $\Delta^s \gamma_0^t$; seminvariants led by $a^r \Delta^s \gamma_0^t$

1. We have already treated the case of $a^r \gamma_0^t$ when $r = 1$ in XI above and we have shown in XIII how to form seminvariants whose leading terms are $a^r d^q$ $(r \geqq 2;\ q \geqq 1)$. Multiplying these by γ_0^t $(t \geqq 1)$ we have seminvariants with the same leading terms as all seminvariants led by $a^r \gamma_0^t$.

2. We have shown in Article XIV how to construct seminvariants whose leading terms are $\Delta d^{5r'}$, $\Delta d^{5r'+1}$, $\Delta d^{5r'+2}$, $\Delta^s d^q$ $(r', q \geqq 0;\ s \geqq 2)$. Multiplying these by γ_0^t we construct seminvariants whose leading terms are $\Delta^s \gamma_0^t d^{5r'}$, $\Delta^s \gamma_0^t d^{5r'+1}$, $\Delta^s \gamma_0^t d^{5r'+2}$, and $\Delta^s \gamma_0^t d^q$. It is easy to show by the use of Article VII that no seminvariants exist with leading terms $\Delta^s \gamma_0^t d^{5r'+3}$ and $\Delta^s \gamma_0^t d^{5r'+4}$. Thus from Δ, σ_3, K, γ_0, and δ_{00} we can make up seminvariants with the same leading terms as any existing seminvariants led by $\Delta^s \gamma_0^t$.

3. We have shown in Article XIV how to construct seminvariants with the same leading terms as any existing seminvariants led by $a^r \Delta^s$ $(r, s \geqq 1)$. Multiplying these by γ_0^t we obtain seminvariants with the same leading terms as any existing seminvariants led by $a^r \Delta^s \gamma_0^t$.

XVIII. Proof that the twelve seminvariants a, Δ, γ_0, S_3, D, σ_3, K, σ_5, σ_6, σ_7, G_1, and δ_{00} form a fundamental system of the cubic, modulo 5

We propose to prove this theorem by showing how actually to construct from these twelve seminvariants any rational integral homogeneous modularly isobaric (modulo 4) seminvariant of the cubic, modulo 5. It has been shown in Article III that any seminvariant S of the cubic is of the form

$$S = (S_0 + S_1 + \cdots + S_n) d^q + \cdots,$$

where S_0, S_1, $\cdots$, S_n are seminvariants of the quadratic (mod 5) or constants. It is this seminvariant S so arranged that we propose to construct. If one of S_0, S_1, $\cdots$, S_n is a constant, consideration of homogeneity shows that all the others are constants and that S has the same leader as a power of δ_{00}. Subtracting the proper numerical multiple of the proper power of δ_{00} from S we have a seminvariant which involves no higher power of d than d^{q-1}. If on the other hand S_0, S_1, $\cdots$, S_n be seminvariants of the quadratic, each of them is a polynomial in a, Δ, β, and γ_0. We now consider this case, first when $q \equiv 0$, modulo 5, and second, when $q \not\equiv 0$, modulo 5.

(1) *When $q \equiv 0$, modulo* 5. The leader $S_0 + S_1 + \cdots + S_n$ of the seminvariant is a rational integral function of a, Δ, β, γ_0; constructing it from these and multiplying by $(\delta_{00})^q$ $(q = 5, 10, 15, \cdots)$, we construct from a, Δ, β, γ_0, and δ_{00} a seminvariant whose leading term is the same as that of S. Subtracting this from S we have a seminvariant which involves no power of d higher than d^{q-1}.

(2) *When $q \not\equiv 0$, modulo* 5. If q is equal to or greater than 1 none of the summands of the leader of S can be γ_0^t or $a\gamma_0^t$ for reasons similar to those given in Articles X and XI for the non-existence of seminvariants with these leaders $(t \geqq 1)$.

We have shown in Articles XVI and XVII how to construct from a, S_3, σ_3, D, K, σ_5, σ_6, G_1, and δ_{00} seminvariants whose leading terms are $a^r \Delta^s \gamma_0^t \beta^u d^q$ $(q \geqq 1; t \geqq 1; r, s, u$ ranging over all integral values except ones which will give the terms $a\gamma_0^t d^q$ and $\gamma_0^t d^q)$. Then subtracting from S seminvariants with the proper leaders made up from a, Δ, γ_0, S_3, σ_3, D, K, σ_5, σ_6, G_1, and δ_{00} we obtain a seminvariant whose leading term is free from γ_0.

We have shown in Articles VIII and XVI how to construct from a, Δ, S_3, σ_3, D, K, σ_5, σ_6, and δ_{00} seminvariants whose leading terms are $a^r \Delta^s \beta^u d^q$ $(r, s \geqq 0; u \geqq 1; q \geqq 1)$. Then subtracting from the remaining seminvariant the proper seminvariants constructed from a, Δ, S_3, σ_3, D, K, σ_5, σ_6, and δ_{00} we obtain a seminvariant whose leader is a polynomial in a and Δ. In Article XVI we have shown how to construct from a, Δ, G_1, σ_3, K, σ_7, and δ_{00} seminvariants with the same leading terms as all seminvariants whose leaders are $a^r \Delta^s$ $(r, s \geqq 1)$. Subtracting as before, we obtain a seminvariant whose leader is of the form $Aa^m + B\Delta^s$; the hypothesis of homogeneity shows that if $m = 1$, $B = 0$; but no such seminvariant can exist (vide IX supra). Therefore m is greater than 1 (if A is not zero). In Article XII we showed how to construct from a, S_3, D, and δ_{00} seminvariants led by $a^r d^q$ $(r \geqq 2)$. Subtracting as before we obtain a seminvariant whose leader is a numerical multiple of Δ^s. Directions for constructing from Δ, σ_3, K, and δ_{00} a seminvariant with the same leader as any existing seminvariant with such a leader have been given in Article XIII. Subtracting the proper seminvariant we have at last a seminvariant whose leading term involves no power of d higher than d^{q-1}.

Thus we have shown that by subtracting from any rational integral homogeneous modularly isobaric seminvariant S a seminvariant which is a polynomial in the thirteen seminvariants a, Δ, β, γ_0, σ_3, S_3, D, K, σ_5, σ_6, σ_7, G_1, and δ_{00} we may reduce S by at least one degree in d. By induction it follows that S is a polynomial in these thirteen seminvariants. Reducing β by the identity of XVI we have the following

THEOREM. *The twelve seminvariants* a, Δ, γ_0, S_3, D, σ_3, K, σ_5, σ_6, σ_7, G_1, *and* δ_{00} *are a fundamental system of seminvariants of the binary cubic form, modulo* 5.

C. A FUNDAMENTAL SYSTEM OF SEMINVARIANTS OF THE CUBIC, MODULO 7

XIX. SEMINVARIANTS LED BY a^r $(r \geqq 2)$

The case of seminvariants led by a, modulo p, has been treated in Article IX above. Seminvariants led by a^2 are the algebraic seminvariants S_3 and D, and the formal modular seminvariants

$$B_1 \equiv -\frac{1}{3}\sum_{t=0}^{6}(at^3+3bt^2+3ct+d)^5 \equiv a^2 d^3 + \cdots \quad (\text{mod } 7),$$

$$K \equiv -\sum_{t=0}^{6}(at^3+3bt^2+3ct+d)^6 \equiv a^2 d^4 + \cdots \quad (\text{mod } 7).$$

It follows from the theorem of Article VII that no seminvariants exist whose leading terms are $a^2 d^5$ and $a^2 d^6$; seminvariants whose leading terms are $a^2 d^{7r}$, $a^2 d^{7r+1}$, $a^2 d^{7r+2}$, $a^2 d^{7r+3}$, and $a^2 d^{7r+4}$ can be formed by the multiplication of the seminvariants S_3, D, B_1, and K by the proper power of δ_{00}; but the theorem of Article VII shows that no seminvariants exist whose leading terms are $a^2 d^{7r+5}$ and $a^2 d^{7r+6}$ $(r \geqq 1)$. Seminvariants whose leading terms are $a^3 d^q$ $(q = 1, 2, 3, 4, 5. 6)$ are aS_3, aD_6, aB_1, aK, and

$$B_2 \equiv -\sum_{t=0}^{6}(at^2+2bt+c)^3(at^3+3bt^2+3ct+d)^5 \equiv a^3 d^5 + \cdots \quad (\text{mod } 7),$$

$$B_3 \equiv -\sum_{t=0}^{6}(at^2+2bt+c)^3(at^3+3bt^2+3ct+d)^6 \equiv a^3 d^6 + \cdots \quad (\text{mod } 7).$$

Multiplying these and a^3 by the proper power of δ_{00} we have seminvariants led by $a^3 d^q$ $(q \geqq 7)$ and multiplying these by a^{r-3} $(r \geqq 4)$ we have seminvariants whose leading terms are $a^r d^q$ $(r \geqq 4;\ q \geqq 7)$.

We have thus shown that any existing seminvariant led by a or any higher power of a has the same leading term as a seminvariant which can be constructed from a, S_3, D, B_1, K, B_2, B_3, and δ_{00}.

XX. SEMINVARIANTS LED BY Δ^s $(s \geqq 1)$

There is a seminvariant led by Δ for every power q of d such that $q \equiv 0$, modulo 7, viz., $\Delta(\delta_{00})^r$ $(r \geqq 1)$. For other powers of d there exist no seminvariants led by Δ. For a seminvariant led by Δ would be

$$\Delta d^q + Abc^2 d^{q-1} + \cdots$$

and terms involving d^{q-1} after this is operated upon by Θ are

$$3q\Delta c d^{q-1} + Aac^2\, d^{q-1} + 4Ab^2\, cd^{q-1}.$$

In order that the supposed seminvariant be annihilated the sum of the coefficients of d^{q-1} must vanish, modulo 7. This requires that

$$3q + 4A \equiv 0,\ \text{modulo } 7,$$

$$-\ 3q + A \equiv 0,\ \text{modulo } 7,$$

whence $A \equiv 0$, modulo 7. Applying the theorem of Article VII, we see that no such seminvariants exist.

Seminvariants whose leading terms are $\Delta^2\, d^q\ (q \geqq 1)$ are

$$C_1 \equiv -\tfrac{1}{3}\sum_{t=0}^{6}(at^2 + 2bt + c)^2(at^3 + 3bt^2 + 3ct + d)^3 \equiv \Delta^2 d\ + \cdots,$$

$$C_2 \equiv \sum_{t=0}^{6}(at^2 + 2bt + c)^2(at^3 + 3bt^2 + 3ct + d)^4 \equiv \Delta^2 d^2 + \cdots,$$

$$C_3 \equiv \tfrac{1}{4}\sum_{t=0}^{6}(at^2 + 2bt + c)^2(at^3 + 3bt^2 + 3ct + d)^5 \equiv \Delta^2 d^3 + \cdots,$$

$$C_4 \equiv -\sum_{t=0}^{6}(at^2 + 2bt + c)^2(at^3 + 3bt^2 + 3ct + d)^6 \equiv \Delta^2 d^4 + \cdots.$$

By multiplying these and Δ^2 by the proper powers of δ_{00}, we have seminvariants whose leading terms are $\Delta^2\, d^q\ (q \equiv 1, 2, 3, 4,\ \text{modulo } 7)$. That no seminvariants with the leading terms $\Delta^2\, d^q\ (q \equiv 5, 6,\ \text{modulo } 7)$ exist follows from the theorem of Article VII.

Seminvariants led by Δ^3 are ΔC_1, ΔC_2, ΔC_3, ΔC_4, and

$$C_5 \equiv a^3 B_2 - \sum_{t=0}^{6}(at^2 + 2bt + c)^6(at^3 + 3bt^2 + 3ct + d)^5 \equiv \Delta^3 d^5 + \cdots,$$

$$C_6 \equiv a^3 B_3 - \sum_{t=0}^{6}(at^2 + 2bt + c)^6(at^3 + 3bt^2 + 3ct + d)^6 \equiv \Delta^3 d^6 + \cdots.$$

By multiplying these and Δ^3 by $\Delta^{s-3}(\delta_{00})^t$ we obtain seminvariants whose leading terms are $\Delta^s\, d^{q+7t}\ (s \geqq 4;\ t \geqq 1;\ q \geqq 1)$.

We have thus shown that any seminvariant led by Δ, Δ^2, or any higher power of Δ has the same leading term as a seminvariant which can be constructed from Δ, C_1, C_2, C_3, C_4, C_5, C_6, and δ_{00}.

XXI. Seminvariants led by $a^r\,\Delta^s\ (r, s \geqq 1)$

Seminvariants with the leader $a\Delta$ exist for every power q of d such that $q \equiv 0$, modulo 7, viz., $a\Delta(\delta_{00})^t$, $(t \geqq 1)$. For other powers of d no seminvariants led by $a\Delta$ exist. For such a seminvariant would be

$$a\Delta d^q + (Aabc^2 + Bb^3 c) d^{q-1} + \cdots$$

and the terms involving d^{q-1} after this is operated upon by Θ are

$$(3qab^2 c - 3qa^2 c^2 + Aa^2 c^2 + 4Aab^2 c + 3Bab^2 c + 2Bb^4) d^{q-1},$$

whence

$$\begin{aligned} 3q + 4A + 3B &\equiv 0, \text{ modulo } 7, \\ -3q + A &\equiv 0, \text{ modulo } 7, \\ 2B &\equiv 0, \text{ modulo } 7, \end{aligned}$$

whence $A \equiv B \equiv 0$, modulo 7. This proves that no such seminvariants exist.

Seminvariants whose leading terms are $a^2 \Delta d^5$ and $a^2 \Delta d^6$, $a\Delta^2 d^5$ and $a\Delta^2 d^6$ are

$$E_1 \equiv \frac{1}{4}\sum_{t=0}^{6} (at^2 + 2bt + c)^4 (at^3 + 3bt^2 + 3ct + d)^5,$$

$$E_2 \equiv \frac{1}{4}\sum_{t=0}^{6} (at^2 + 2bt + c)^4 (at^3 + 3bt^2 + 3ct + d)^6,$$

$$E_3 \equiv \frac{1}{4}\sum_{t=0}^{6} (at^2 + 2bt + c)^5 (at^3 + 3bt^2 + 3ct + d)^5,$$

$$E_4 \equiv \frac{1}{4}\sum_{t=0}^{6} (at^2 + 2bt + c)^5 (at^3 + 3bt^2 + 3ct + d)^6.$$

By multiplying these together with S_3, D, K, B_1, C_1, C_2, C_3, and C_4, by proper powers of a, Δ, and δ_{00} we may show that any seminvariant led by $a^r \Delta^s$ has the same leading term as a seminvariant which can be constructed from a, Δ, S_3, D, B_1, K, C_1, C_2, C_3, C_4, δ_{00}, E_1, E_2, E_3, and E_4.

XXII. Seminvariants led by $a^r \Delta^s \gamma_0^t \beta^u$ $(r, s, t \geqq 0;\ u \geqq 1)$

We have shown in Article VIII above how to express βd^{q-1} $(q \geqq 1)$ as the sum of seminvariants whose leading terms are numerical multiples of $a^2 \Delta^{(p-3)/2} d^q$. For the modulus 7

$$\begin{aligned} \beta &\equiv 4\Delta^2 S_3 + 3a^2 C_1, \\ \beta d + \cdots &\equiv 2\Delta^2 D + 5a^2 C_2, \\ \beta d^2 + \cdots &\equiv 6\Delta^2 B_1 + a^2 C_3, \\ \beta d^3 + \cdots &\equiv \Delta^2 K + 6a^2 C_4, \\ \beta d^4 + \cdots &\equiv 3\Delta E_1 + 4aE_3, \\ \beta d^5 + \cdots &\equiv 5\Delta E_2 + 2aE_4, \\ \beta d^6 + \cdots &\equiv 6a^2 \Delta^2 \delta_{00} + KC_3. \end{aligned}$$

Proceeding as in the case of the modulus 5 we see that from a, Δ, γ_0, S_3, D, B_1, C_1, C_2, C_3, C_4, E_1, E_2, E_3, E_4, K, and δ_{00} we can construct seminvariants with the same leading terms as any seminvariant led by $a^r\,\Delta^s\,\gamma_0^t\,\beta^u$.

XXIII. Seminvariants led by $a^r\,\gamma_0^t$; seminvariants led by $\Delta^s\,\gamma_0^t$; seminvariants led by $a^r\,\Delta^s\,\gamma_0^t$

(1) This case may be treated exactly as was the case with seminvariants modulo 5, led by $a^r\,\gamma_0^t$ (vide XVII: 1 supra); the reader will notice that by Article VII no seminvariants exist whose leading terms are $a^2\,\gamma_0^t\,d^{5+7w}$ and $a^2\,\gamma_0^t\,d^{6+7w}$ $(w \geqq 0)$.

(2) No seminvariants exist whose leaders are $\Delta\gamma_0^t$ with the exception of $\Delta\gamma_0^t\,d^{7s} + \cdots$ $(s \geqq 0)$ (and these have the same leading terms as $\Delta\gamma_0^t\,(\delta_{00})^s$), for if such seminvariants existed they would be of the form

$$(\Delta c^{7t} + \text{terms of lower weight})\,d^q$$
$$+\ (Abc^{7t+2} + \text{terms of lower weight})\,d^{q-1} + \cdots.$$

Operating on this supposed seminvariant with Θ we obtain

$$\{3q\Delta c^{7t+1} + Aac^{7t+2} + (14r+4)\,Ab^2\,c^{7t+1}\}\,d^{q-1}$$
$$+\ (\text{terms of lower weight})\,d^q + \cdots$$

and as the sum of the terms of highest weight in the coefficient of d^{q-1} must be congruent to zero, modulo 7, we have

$$3q + (14r+4)\,A \equiv 0,\ \text{modulo } 7,$$
$$-\,3q + A \equiv 0,\ \text{modulo } 7,$$

whence $A \equiv 0$, modulo 7, and the non-existence of the supposed seminvariant is proven, for by Article VII $Abc^{7t+2}\,d^{q-1}$ must not be zero if the supposed seminvariant exists.

C_v $(v = 1, 2, 3, 4)$ are seminvariants whose leading terms are numerical multiples of $\Delta^2\,d^q$ $(q = 1, 2, 3, 4)$. Multiplication of these and $\Delta^2\,\gamma_0^t$ by $(\delta_{00})^w$ gives us seminvariants whose leading terms are $\Delta^2\,\gamma_0^t\,d^{7w+m}$ $(w \geqq 1;$ $m = 0, 1, 2, 3, 4)$. The theorem of Article VII again proves the non-existence of such seminvariants when $m = 5$ and 6. From the seminvariants whose leading terms are $\Delta^s\,d^q$ $(s \geqq 3;\ q \geqq 1)$ already derived in Article XX we can by multiplication by $(\delta_{00})^n$ form seminvariants whose leading terms are $\Delta^s\,\gamma_0^t\,d^q$ $(s \geqq 3;\ t \geqq 1;\ q \geqq 1)$. We have thus shown how from Δ, γ_0, C_1, C_2, C_3, C_4, C_5, C_6, and δ_{00} to construct a seminvariant with the same leading term as any seminvariant led by $\Delta^s\,\gamma_0^t$.

(3) There exists for every value of q such that $q \equiv 0$, modulo 7, a semin-

variant led by a $\Delta\gamma_0^t$, viz., $a\Delta\gamma_0^t(\delta_{00})^r$ $(r \geqq 1)$. When $q \not\equiv 0$, modulo 7, no such seminvariant exists; for if there did it would be of the form

$$(a\Delta c^{7t} + \text{terms of lower weight})\,d^q$$
$$+ (Aabc^{7t+2} + Bb^3c^{7t+1} + \text{terms of lower weight})\,d^{q-1} + \cdots.$$

The terms of highest weight in the coefficient of d^{q-1} in the result of operating with Θ are

$$3qa\Delta c^{7t+1} + Aa^2c^{7t+2} + (14t+4)Aab^2c^{7t+1} + 3Bab^2c^{7t+1} + (14t+2)Bb^4c^{7t}.$$

Setting this congruent to zero, modulo 7, and proceeding as before we obtain inconsistent congruences in A and B.

We have shown in Article XXI how to construct from a, Δ, S_3, D, B_1, K, C_1, C_2, C_3, C_4, E_1, E_2, E_3, E_4, and δ_{00} seminvariants whose leading terms are $a^r\Delta^s d^q$ $(r, s \geqq 2;\ q \geqq 1)$. Multiplying these by γ_0^t we have (together with those given above) seminvariants with the same leading terms as any seminvariants led by $a^r\Delta^s\gamma_0^t$.

XXIV

The reader will now have no difficulty in seeing that by the method of Article XVIII it can be proved that *the twenty seminvariants* a, Δ, S_3, γ_0, D, K, B_1, B_2, B_3, C_1, C_2, C_3, C_4, C_5, C_6, E_1, E_2, E_3, E_4, *and* δ_{00} *are a fundamental system of seminvariants of the cubic form, modulo* 7.

That no one of these except γ_0 can be a polynomial in the others is evident from the fact that if we so multiply sets of them as to obtain a certain leading term in two ways the leader of the new seminvariant obtained by taking the difference of the two has in the most favorable case a leader of higher degree than the leader of any of the fundamental system except γ_0. Nor can the difference of any two such seminvariants be γ_0, for every term in the leader of the difference of two such seminvariants involves either a or b, whereas γ_0 has a term involving neither a nor b.

D. A FUNDAMENTAL SYSTEM OF FORMAL MODULAR PROTOMORPHS OF THE BINARY CUBIC, MODULO p

XXV

While one of the chief aims in the theory of algebraic seminvariants was the isolation of sets of seminvariants called fundamental, in terms of which every seminvariant could be expressed rationally and integrally, yet there have been discovered interesting sets of protomorphic seminvariants or protomorphs P_1, P_2, P_3, $\cdots$, P_n such that any seminvariant S of the form under consideration can be expressed in the form $A_1^q P(A_1, A_2, A_3, \cdots, A_n)$ where q

is a positive, negative or zero integer and P is a polynomial with integral coefficients in $A_1, A_2, A_3, \cdots, A_n$.

There is a corresponding theory of protomorphs in the formal modular seminvariant theory which has additional interest in the case of the binary cubic on account of the fact that while the number of members of a fundamental system of seminvariants of this form, modulo p, is a function of p, the number of protomorphs in a fundamental system is constant for any prime greater than 3. The set of protomorphs is also much simpler than the set of seminvariants, for it has only four members, and all of these save one are algebraic.

THEOREM. *The seminvariants a, Δ, S_3, and β form a set of protomorphs of the binary cubic, modulo p.*

Proof. Since

$$c = \frac{b^2 - \Delta}{a},$$

$$d = \frac{S_3 + 3abc - 2b^3}{a^2} = \frac{S_3 + b^3 - 3b\Delta}{a^2},$$

any seminvariant S of the cubic, modulo p, can be expressed as

$$\begin{aligned} S(a, b, c, d) &= S\left(a, b, \frac{b^2 - \Delta}{a}, \frac{S_3 + b^3 - 3b\Delta}{a^2}\right) \\ &= F\left(a, \frac{\Delta}{a}, \frac{S_3}{a^2}\right) + a^{-k}\, G(a, b, S_3, \Delta), \end{aligned}$$

where G is a polynomial in its arguments and F includes all the terms of S not involving b explicitly. Then G is divisible by b and hence by β. Treating the new seminvariant $H = G/\beta$ in like manner we see that $S = a^q P$, where q is a positive, negative, or zero integer, and P is a polynomial in a, Δ, S_3, and β.

Of the syzygies obtained, the following are examples, modulo 5:

$$\sigma_3 \equiv \frac{3\beta + \Delta S_3}{a^2}, \text{ modulo } 5;$$

$$\begin{aligned} \delta_{00} \equiv \frac{1}{a^{10}} (S_3^5 &+ 2a^4 \Delta S_3^3 + 3a^8 \Delta^2 S_3 + 4a^4 \Delta^4 S_3 + 4a^{12} S_3 \\ &+ 3a^4 S_3^2 \beta + 3\beta\Delta^5 + \beta^3 + 4a^4 \beta\Delta^3 + 2a^8 \beta\Delta), \text{ modulo } 5. \end{aligned}$$

WILLIAMSBURG, VIRGINIA,
February 5, 1920.