MODULAR CONCOMITANT SCALES, WITH A FUNDAMENTAL SYSTEM OF FORMAL COVARIANTS, MODULO 3, OF THE BINARY QUADRATIC*

BY

OLIVER EDMUNDS GLENN

I propose to consider in this paper the invariant theory of the general binary quantic

$$f_m = (a_0, a_1, \cdots, a_m \between x_1, x_2)^m$$

which is subject to the transformations of the total linear group G, modulo p (a prime number), a theory which has been developed only to the extent indicated in the summary below.† Examples of such invariantive functions have been constructed by A. Hurwitz, Miss Sanderson, Dickson, and the present author, and it has been proved that the totality of pure invariants of the type forms a finite system when $m \not\equiv 0 \pmod p$. A variety of construction methods have been invented and certain particular complete systems of seminvariants and invariants derived. The present writer was the first to publish a fundamental system of formal covariants, that of the binary cubic for the modulus 2.

The developments which follow are devoted to processes for the generation of complete systems of covariants and, in particular, give an extension of the principle of the modular covariant scale which was employed in the paper, quoted as IV above, on the system of the cubic modulo 2. In Section 6 the theory of concomitant scales is applied in determining a fundamental system of covariants modulo 3 of the binary quadratic, an interesting system composed of 18 invariants and covariants.

* Presented to the Society, April, 1918.

† A. Hurwitz, Archiv der Mathematik und Physik, vol. 5 (1903), p. 17. Sanderson, these Transactions, vol. 14 (1913), p. 490. Dickson, *Madison Colloquium Lectures* (1913), and these Transactions, vol. 15 (1914), p. 497. See also Reed, Bulletin of the American Mathematical Society, vol. 21 (1915), p. 491. The following papers on this subject, which I have published, will be referred to by number: I. American Journal of Mathematics, vol. 37 (1915), p. 73. II. Bulletin of the American Mathematical Society, vol. 21 (1915), p. 167. III. These Transactions, vol. 17 (1916), p. 545. IV. These Transactions, vol. 19 (1918), p. 109. V. Annals of Mathematics, vol. 19 (1918), p. 201.

1. Residues of the numbers of Pascal's triangle

Important number-theoretic data to be made use of in this paper relate to the plexus of residues obtained by reducing the binomial numbers in Pascal's triangle according to the modulus p. The elements of this reduced triangle are the numbers $0, \cdots, p-1$ so arranged as to form a configuration which can be described with adequate generality to enable one to write down very readily various formulas; for example, that for the most general type of binomial number which contains an arbitrary prime p as a factor. The following formula, determined in this way, yields these numbers and only such numbers:*

$$(1)\qquad \binom{kp^r+j}{i+j} \qquad \begin{array}{l} k = 1, \cdots, \infty; \\ s = 1, \cdots, k; \\ j = 0, \cdots, p^r - 2; \\ i = (s-1)p^r + 1, \cdots, sp^r - 1 - j. \end{array}$$

By an indirect method, based upon the existence of a certain modular invariant (cf. § 2), we shall prove, also, the following

Lemma. *If σ is any integer and $m = \sigma(p-1)$, then the following congruences hold true universally:*

$$(2)\qquad N = \sum_{i=1}^{\sigma-1} \binom{m-s}{i(p-1)-s} \equiv 0 \pmod{p} \; [s \not\equiv 0 \pmod{p-1}].$$

If $s \equiv 0 \pmod{p-1}$, then $N \equiv 1 \pmod{p}$.

This result has a measure of novelty even though it is comprised in a very general formula due to Glaisher.†

2. Concomitant Scales

There is a process in modular covariant theory which is analogous, in a general theoretical way, to symbolical convolution, so-called, in the usual doctrine of algebraical invariants. If, for example,

$$\lambda = (ab)^2(bc)a_x^2 b_x c_x^3$$

is an algebraical covariant of degree three, there exists a finite sequence or scale of concomitants of this degree, obtained by the process of convolution, viz.,

$$\lambda, \quad \lambda' = (ab)^3(bc)a_x c_x^3, \quad \lambda'' = (ab)^2(ac)(bc)a_x b_x c_x^2, \quad \cdots.$$

Upon the existence of such scales the fundamental theorems of the algebraic invariant theory have been found to rest.

* Necessary and sufficient conditions in order that the general multinomial coefficient should be congruent to zero modulo p were first given by Dickson; Annals of Mathematics, ser. 1, vol. 11 (1896), p. 75.

† Quarterly Journal of Mathematics, vol. 30 (1899), p. 361. Glaisher's result has been extended to multinomial numbers by Dickson, Quarterly Journal of Mathematics, vol. 33 (1902), p. 381.

In the modular theory it is true likewise that a covariant of sufficiently high order in comparison with the modulus is a member of a finite scale of derived modular concomitants of the same degree. We proceed to construct covariants modulo p of an appropriate type to afford a definition of the unique modular scale for any chosen covariant.

THEOREM. *If $f = (a_0, a_1, \cdots, a_m \between x_1, x_2)^m$ is any quantic of order $m = \sigma(p-1)\,(\sigma > 1)$ there exists a unique invariant modulo p of degree unity,*

$$P \equiv a_{p-1} + a_{2(p-1)} + \cdots + a_{(\sigma-1)(p-1)}.$$

The coördinates of the real points mod p are $(0, 1)$, $(1, 0)$, $(1, 1)$, $(1, 2)$, $\cdots$, $(1, p-1)$. The result of substituting these for (x_1, x_2) in f is a set of $p+1$ linear expressions in $a_0, \cdots, a_m$, and any symmetric function of these expressions which does not vanish is a formal invariant* of f. Their sum, for instance, is

$$P_1 = a_0 + a_m + \sum_{\mu=0}^{m} \sum_{i=1}^{p-1} i^\mu a_\mu .$$

Consider the symmetric function of the $p-1$ residues

$$\Sigma = \sum_{i=1}^{p-1} i^\mu ,$$

which is the coefficient of a_μ in P_1. To multiply the numbers $1, 2, \cdots, p-1$ each by an integer s is merely to permute them (mod p). Hence†

$$\Sigma \equiv \sum_{i=1}^{p-1} (si)^\mu \equiv s^\mu \Sigma \pmod{p},$$

$$(s^\mu - 1)\Sigma \equiv 0 \qquad \text{and} \qquad \Sigma \equiv 0 \pmod{p}\ (\mu \not\equiv 0 \pmod{p-1}).$$

If $\mu \equiv 0 \pmod{p-1}$, then, evidently $\Sigma \equiv p-1$. Hence

$$P_1 \equiv (p-1)P \pmod{p},$$

which proves the theorem.

The lemma at the end of the preceding section may now be proved. The transformation $t: x_1 = x_1' + x_2',\ x_2 = x_2'$, under which P remains unaltered, induces the substitutions‡

$$(3)\quad a_j' \equiv \binom{m}{j} a_0 + \binom{m-1}{j-1} a_1 + \cdots + \binom{m-j+1}{1} a_{j-1} + a_j \pmod{p}$$

* Dickson, these Transactions, vol. 15, 1914, p. 497.

† Vandiver, Annals of Mathematics, Ser. 2, vol. 18, p. 105.

‡ Note that $a_m' = a_0 + \cdots + a_m$ may be written $a_0 + a_m + P + H$.

$(j = 0, \cdots, m)$, and P', the function P in the primed a-s, is

$$P' \equiv \sum_{s=0}^{k} \sum_{i=1}^{\sigma-1} \binom{m-s}{i(p-1)-s} a_s, \qquad k = i(p-1).$$

But we can have $P' \equiv P \pmod p$ only provided the congruences (2) hold.

THEOREM. *There is a unique covariant C of order $p-1$ of $f_{\sigma(p-1)}$ led by the seminvariant*

$$S = a_0 + P.$$

According to a method developed in III we can derive this covariant by substituting from the following transformations induced by

$$t_1 : x_1 = x_1' + t x_2', \qquad x_2 = x_2',$$

in $a_m + P$:

$$(3_1) \qquad a_j' \equiv \binom{m}{j} t^j a_0 + \binom{m-1}{j-1} t^{j-1} a_1 + \cdots + a_j.$$

Since P is an invariant we obtain a function of the type

$$F' = P + \sum_{i=0}^{m} t^{m-i} a_i,$$

and when the various powers of t are reduced by Fermat's theorem we have

$$(4) \quad \begin{aligned} F \equiv (a_m + P) + \sum_{r=1}^{p-1} (a_{m-r} &+ a_{m-p-r+1} + a_{m-2p-r+2} \\ &+ \cdots + a_{m-(\sigma-1)p-r+\sigma-1}) t^r \pmod p, \end{aligned}$$

in which the coefficient of t^{p-1} is evidently $S = a_0 + P$. The covariant sought is the homogeneous form of F, i. e.,

$$(5) \quad \begin{aligned} C = S x_1^{p-1} + \sum_{r=1}^{p-2} (a_{m-r} &+ a_{m-p-r+1} + a_{m-2p-r+2} \\ &+ \cdots + a_{m-(\sigma-1)(p-1)-r}) x_1^r x_2^{p-1-r} + (a_m + P) x_2^{p-1}. \end{aligned}$$

Direct verification of the covariancy of C would involve the relations (2).

We can now build up our concomitant scale for f_m by polarization of C, using the processes established in II. Thus, successive applications of the operator

$$w = x_1^p \frac{\partial}{\partial x_1} + x_2^p \frac{\partial}{\partial x_2},$$

yield the p covariants $w^i C$ $(i = 0, \cdots, p-1)$ of respective orders (P being adjoined)

$$0, \quad p-1, \quad 2(p-1), \quad \cdots, \quad p(p-1),$$

and having a common seminvariant leading coefficient $S = a_0 + P$.

If $K_n = C_0 x_1^n + C_1 x_1^{n-1} x_2 + \cdots + C_n x_2^n$ is any covariant of f_m of order $n = \tau(p-1)$, a scale for K_n constructed on the model of the concomitants P, $w^i C$, will be a set of concomitants mod p of f_m. This process of forming successive concomitant scales is a prolific method of building complete systems and if the scales used are all complete for their respective orders the process is definitive.

We add the remark that all forms of orders p^2 or greater possess covariants of lower order led by a_0,* and also that the case of the even modulus 2 presents a number of exceptional circumstances and thus requires a special treatment (cf. IV).

3. The general seminvariant, modulo 3, of f_2

Dickson has derived complete systems both of pure invariants and of seminvariants of the binary quadratic $f_2 = a_0 x_1^2 + 2a_1 x_1 x_2 + a_2 x_2^2$, modulo p.† For $p = 3$ the seminvariants are
a_0, $\Delta = a_1^2 - a_0 a_2$, $\gamma_0 = (a_0 + a_1 + a_2)(a_0 + 2a_1 + a_2) a_2$, $\beta = a_1^3 - a_0^2 a_1$,
and the system of invariants is

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

Expanding Γ we find, by simple combinations, the congruences

$$\left.\begin{aligned} a_0^3 + 2\Delta a_0 + \gamma_0 + 2\Gamma &\equiv 0, \\ a_0^4 + 2\Delta a_0^2 + 2\Gamma a_0 + J &\equiv 0, \\ \beta^2 + 2\gamma_0 a_0^3 + 2\Delta(\Delta - a_0^2)^2 &\equiv 0, \end{aligned}\right\} \pmod{3}, \tag{6}$$

the last one of which was given previously by Dickson; who also showed that any formal seminvariant is of the form

$$S = \beta^\epsilon \phi(a_0, \Delta, \gamma_0) \qquad (\epsilon = 0 \text{ or } 1),$$

in which ϕ is a polynomial in its arguments, having numerical coefficients. The seminvariants a_0, Δ, γ_0, and therefore ϕ, are of even weight, but β is skew.

It now follows that if we employ the congruences (6) as moduli the general seminvariant mod 3 of f_2 can be reduced to the form

$$S \equiv \beta^\epsilon (S_0 + S_1 a_0 + S_2 a_0^2 + S_3 a_0^3), \tag{7}$$

($\epsilon = 0$ or 1), where S_i ($i = 0, \cdots, 3$) is a polynomial in the invariants Δ, J, Γ alone, with numerical coefficients. This is, therefore, the general form of the leading coefficient of a covariant modulo 3 of f_2.

* Cf. these Transactions, vol. 18, 1917, p. 443; and V, p. 201.

† *Madison Colloquium Lectures*, 1913, p. 42.

Similarly the general seminvariant of f_2 modulo p can be reduced to a finite form.

4. Covariants led by pure invariants

The complete concomitant scale for a covariant mod p of f_m will, in general, contain certain covariants whose leading coefficients are invariants, and we now establish certain necessary conditions for the existence of these forms.

Lemma. *If the leading coefficient C_0 of any formal covariant,*

$$K_n = C_0 x_1^n + C_1 x_1^{n-1} x_2 + \cdots + C_n x_2^n, \tag{8}$$

is an invariant, then

$$C_0 \equiv (p-1)(C_1 + C_2 + \cdots + C_{n-1}) \pmod{p}. \tag{9}$$

To prove this let the increment of C_i $(i = 0, \cdots, n)$ when f is transformed into f' by $t : x_1 = x_1' + x_2'$, $x_2 = x_2'$, be δC_i. Then if K_n' is the K_n function constructed for f', we get

$$K_n' = \sum_{i=0}^{n} (C_i + \delta C_i)(x_1 - x_2)^{n-i} x_2^i \equiv K_n \pmod{p},$$

whence follows, by a simple inductive proof, the set of congruences

$$\delta C_r \equiv \binom{n}{r} C_0 + \binom{n-1}{r-1} C_1 + \cdots + \binom{n-r+1}{1} C_{r-1} \pmod{p}, \qquad (r = 0, \cdots, n). \tag{10}$$

In (10) make $r = n$; then, if C_0 is an invariant, C_n is also a pure invariant and $\delta C_n \equiv 0 \pmod{p}$. The congruence (10) then reduces to (9).

An example of a concomitant which satisfies this lemma is IQ, where Q is the well-known universal covariant of order $p(p-1)$ of the total group G, viz.,

$$Q = x_1^{p(p-1)} + x_1^{(p-1)(p-1)} x_2^{p-1} + \cdots + x_2^{p(p-1)},$$

and I is any formal invariant modulo p.

Definition. Suppose $n = \tau(p-1)$, $\tau = rp - \nu$, and that $p > 2$. Assume that K_n is a formal covariant modulo p of any quantic f_m of arbitrary order m. Construct the $\mu = p + \nu + 2$ invariantive functions P_n, $w^i K_n$ $(i = 0, \cdots, \nu)$, $w^j C_n$ $(j = 0, \cdots, p-1)$, where P_n, C_n are concomitants of K_n, constructed on the models of P and C respectively (§ 2). Then these μ concomitants of f_m will be designated the *μ-adic scale* for K_n.

A scale for any covariant K will be said to be *complete* when it includes all concomitants of the first degree in the coefficients of K, which are derivable by empirical or modular invariantive processes. More explicitly a scale is complete when it constitutes a fundamental system of first degree modular concomitants of K.

LEMMA. *If there exists a covariant D of order $\tau(p-1)$ of f_m, led by an invariant, the μ-adic scale of D involves p covariants led by*

$$-D_n = -C_1 - \cdots - C_{n-1} + P_n.$$

Under the hypothesis we write

$$D = (p-1)(D_n + P_n)x_1^n + C_1 x_1^{n-1} x_2 + \cdots \\ + C_{n-1} x_1 x_2^{n-1} + (p-1)(P_n + D_n)x_2^n; \tag{11}$$

according to the preceding lemma, where P_n, D_n are the invariants

$$P_n = C_{p-1} + C_{2(p-1)} + \cdots + C_{(\tau-1)(p-1)}, \\ D_n = C_1 + C_2 + \cdots + C_{n-1} - P_n. \tag{12}$$

Then the leading coefficient of the covariant C_n constructed on the model of C of § 2 is

$$S = (p-1)(D_n + P_n) + P_n \equiv -D_n \pmod{p}.$$

Therefore the one condition necessary for the existence of $w^i C_n$ $(i = 0, \cdots, p-1)$ is $D_n \not\equiv 0 \pmod{p}$, and this proves the theorem.

COROLLARIES. The condition $D_n \not\equiv 0 \pmod{p}$ implied in the preceding lemma is not sufficient. In fact if $p = 3$ we get

$$C_n \equiv -D_n(x_1^2 + 2x_1 x_2 + x_2^2) \pmod{3}, \tag{13}$$

which is not a covariant unless $D_n \equiv 0 \pmod{3}$, when it may be regarded as a vanishing covariant. If D_n is zero $(p = 3)$ D can exist, in the simplified form

$$D = 2P_n x_1^n + C_1 x_1^{n-1} x_2 + \cdots + 2P_n x_2^n, \tag{14}$$

but D will not exist if $p = 3$ and $D_n \not\equiv 0 \pmod{3}$.

If $p = 3$, $D_n \equiv 0$, $n = 4$ and D exists it reduces to the form

$$D = 2P_4 x_1^4 + C_1 x_1^3 x_2 + P_4 x_1^2 x_2^2 - C_1 x_1 x_2^3 + 2P_4 x_2^4. \tag{15}$$

An actual example of D, $n = 6$, $D_6 \equiv 0 \pmod{3}$, is

$$IQ = Ix_1^6 + Ix_1^4 x_2^2 + Ix_1^2 x_2^4 + Ix_2^6,$$

where I is any invariant modulo 3 of f_m.

5. CONCOMITANT SCALES MODULO p OF f_2

An idea which was illustrated in connection with formula (5) of Section 2 will now be amplified.

If a chosen seminvariant S of a binary form f_m satisfies certain conditions as established in my paper which was quoted as III above, it will be the leading coefficient of a definite covariant of order $p - 1$. This covariant can be obtained in explicit form by making the substitutions of the induced transformations (3_1), under

$$t_1 : x_1 = x_1' + tx_2', \qquad x_2 = x_2' \qquad (t \text{ any residue mod } p),$$

in the function obtained from S by operating upon the latter by the permutational substitution

$$s = (a_0 \, a_m)(a_1 \, a_{m-1}) \cdots .$$

When $m = 2$ the induced transformations are

$$a_0' = a_0, \qquad a_1' = a_0 t + a_1, \qquad a_2' = a_0 t^2 + 2a_1 t + a_2.$$

If, in this case, one selects the seminvariant to be the known type

$$S = a_0^{p-1} a_1 - a_1^p,$$

the aforesaid process yields

$$F_1 = (a_0 t + a_1)^p - (a_0 t + a_1)(a_0 t^2 + 2a_1 t + a_2)^{p-1},$$

and expansion of F_1, reduction of powers of t by Fermat's theorem, and replacement of t by x_1/x_2, gives a formal covariant F of order $p - 1$.

Without formulating the laws which the terms of F, so expanded and reduced, satisfy, we may write the resulting covariants for the cases $p = 3$, $p = 5$. These are the following respectively:

$$\begin{aligned} C_1 &= (a_0^2 a_1 - a_1^3) x_1^2 + (a_0 - a_2)(a_1^2 + a_0 a_2) x_1 x_2 + (a_1^3 - a_1 a_2^2) x_2^2, \\ C_1' &= (a_0^4 a_1 - a_1^5) x_1^4 + (3a_0^3 a_1^2 + 2a_0 a_1^2 a_2^2 + 3a_1^4 a_2 \\ &\quad + a_0^4 a_2 + a_0^2 a_2^3) x_1^3 x_2 + (2a_0^3 a_1 a_2 + 4a_0^2 a_1^3 + a_1^3 a_2^2 \\ &\quad + 3a_0 a_1 a_2^3) x_1^2 x_2^2 + (3a_0^2 a_1^2 a_2 + 2a_0 a_1^4 + 2a_1^2 a_2^3 \\ &\quad + 4a_0^3 a_2^2 + 4a_0 a_2^4) x_1 x_2^3 + (a_1^5 - a_1 a_2^4) x_2^4. \end{aligned} \tag{16}$$

The product of F by f_2^{p-1} gives a covariant of order $3(p - 1)$ for which a μ-adic scale may be constructed.

Likewise the polar of f_2 by means of the operator

$$w = x_1^p \frac{\partial}{\partial x_1} + x_2^p \frac{\partial}{\partial x_2} \tag{17}$$

is

$$wf_2 = 2a_0 x_1^{p+1} + 2a_1 (x_1^p x_2 + x_1 x_2^p) + 2a_2 x_2^{p+1}. \tag{18}$$

The product of this covariant by f_2^{p-2} is a covariant K of order $3(p - 1)$ and of the $(p - 1)$-th degree. In the μ-adic scale for K the invariant $P_{3(p-1)}$, $p = 3$, cannot be other than the discriminant Δ of f_2 (cf. § 3), and the covariant of order $p - 1$ in the scale is led by $a_0^2 + \Delta$. Illustrations of such scales will be given in the next section.

It is essential to add that the covariants of a scale exist when τ, in the order $n = \tau(p-1)$ of K_n, exceeds $p + 1$. But we cannot then say that our scale is complete. As was mentioned in Section 2, if $n > p^2 - 1$ there exist first degree covariants of f_m of lower order which, in the paper cited above as V, I have designated as principal covariants, and whose leading coefficient is a_0.

6. A complete system of the quadratic, modulo 3

The theory of the preceding sections, concerning concomitant scales for covariants modulo p of order $n = \tau(p-1)$, applies without change, to *all* covariants modulo 3 of f_m, since the latter are necessarily all of even order.* We can therefore proceed to derive a fundamental system of covariants of f_2 modulo 3 along the following lines.

Any covariant K of order n is of the type (cf. (7))

$$K = S\, x_1^n + C_1\, x_1^{n-1} x_2 + \cdots \; (n \text{ even}), \tag{19}$$

where

$$S = \beta^\epsilon (S_0 + S_1 a_0 + S_2 a_0^2 + S_3 a_0^3) \; (\epsilon = 0 \text{ or } 1),$$

and S_i $(i = 0, \cdots, 3)$ is a polynomial in the invariants Δ, J, Γ. If $\epsilon = 1$, K is skew, otherwise it is of even index. We construct covariants led by the different terms of S, and if four such are A, B, C, D, then, with proper heed of considerations as to orders and as to isobarism we can be assured that $h = K - A - B - C - D$ is also a covariant in which, however, the coefficient of x_1^n is zero. Hence $h \equiv L h_1$ where

$$L = x_1^3 x_2 - x_1 x_2^3,$$

and h_1 is a covariant of order $n - 4$. Employment of the same reduction method† in the case of h_1 and the forms analogous to h_1 in succession gives finally a reduction of h in terms of the universal covariants Q, L, and the irreducible concomitants used to construct A, B, C, D, together with such irreducible concomitants as occur in the last relation $h_i \equiv h_{i+1} L \pmod 3$. In this manner we can isolate a complete covariant system, as will now be shown.

The required covariants A, B, C, D may be built from the concomitants occurring in definite μ-adic scales. To this end we start with f_2 itself and C_1 of (16):

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

and first construct skew covariants led by S $(\epsilon = 1)$, that is, by the different terms of S; and it is necessary to treat the cases $n = 6\nu$, $n = 6\nu + 2$, $n = 6\nu + 4$ separately.

* Cf. I, p. 75.

† Dickson, these Transactions, vol. 14 (1913), p. 299.

Skew covariants. The covariant $-S_0 C_1$ is a skew quadratic led by $+S_0 \beta$. Polarization of $S_0 C_1$ by w gives a quartic and a sextic led by $S_0 \beta$, viz. $-S_0 w C_1$ and $-S_0 w^2 C_1$:

$$
\begin{aligned}
-\zeta_4 = wC_1 &= 2(a_0^2 a_1 - a_1^3)x_1^4 + (a_0 - a_2)(a_1^2 + a_0 a_2)(x_1^3 x_2 + x_1 x_2^3) \\
&\quad + 2(a_1^3 - a_1 a_2^2)x_2^4, \\
-\zeta_6 = \tfrac{1}{2}w^2 C_1 &= -\beta x_1^6 + (a_0 - a_2)(a_1^2 + a_0 a_2)x_1^3 x_2^3 + (a_1^3 - a_1 a_2^2)x_2^6.
\end{aligned} \tag{20}
$$

A quadratic, a quartic, and a sextic covariant, each having $a_0 \beta$ for a leading coefficient will be found by forming the covariants of the hexadic scale for the quartic $-\vartheta_4 = f_2 C_1$. Thus we find, by calculating formulas (5) and (11) for ϑ_4,

$$
\begin{aligned}
\vartheta_2 &= a_0 \beta x_1^2 + (a_0 a_2^3 - a_0^3 a_2)x_1 x_2 + (a_1 a_2^3 - a_1^3 a_2)x_2^2, \\
2w\vartheta_2 &\equiv a_0 \beta x_1^4 + 2(a_0 a_2^3 - a_0^3 a_2)(x_1^3 x_2 + x_1 x_2^3) + (a_1 a_2^3 - a_1^3 a_2)x_2^4, \\
2w^2 \vartheta_2 &\equiv a_0 \beta x_1^6 + (a_0 a_2^3 - a_0^3 a_2)x_1^3 x_2^3 + (a_1 a_2^3 - a_1^3 a_2)x_2^6.
\end{aligned} \tag{21}
$$

In the formulas in which these covariants are to be used $2w\vartheta_2$ may be replaced by ϑ_4 and $2w^2 \vartheta_2$ by $\vartheta_6 = 2f_4 C_1 = a_0 \beta x_1^6 + \cdots$. In fact

$$
w\vartheta_2 \equiv f_2 C_1 + (2\Delta^2 + J)L \pmod 3,
$$

and $2w^2 \vartheta_2$ is reducible in a similar manner.

Similarly a set of covariants led by $a_0^2 \beta$ is found by forming the pentadic scale for the sextic covariant $\xi_6 = -f_2^2 C_1$. The quadratic in this scale is

$$
\begin{aligned}
\xi_2 = a_0^2 \beta x_1^2 &+ (a_0^3 a_1^2 + 2a_0^4 a_2 + 2a_0 a_1^4 + a_1^4 a_2 + 2a_0^3 a_2^2 \\
&+ a_0^2 a_2^3 + 2a_1^2 a_2^3 + a_0 a_2^4)x_1 x_2 + (a_1 a_2^4 - a_1^3 a_2^2)x_2^2.
\end{aligned} \tag{22}
$$

The quartic and sextic covariants in the scale, both of which are reducible, will be replaced, in what follows, by $\xi_4 = f_2 \vartheta_2 = a_0^2 \beta x_1^4 + \cdots$, and $\xi_6 \equiv a_0^2 \beta x_1^6 + \cdots$, respectively.

Finally a similar trio of covariants whose common leading coefficient is

$$
a_0^3 \beta + B \equiv (2\Delta a_0 + \Gamma)\beta \pmod 3,
$$

where B is the skew invariant of degree six in Dickson's system of pure invariants, is obtained by constructing the hexadic scale for the quartic $X_4 = -Ef_2 C_1$, in which

$$
E = a_0^3 \frac{\partial}{\partial a_0} + a_1^3 \frac{\partial}{\partial a_1} + a_2^3 \frac{\partial}{\partial a_2}.
$$

The quadratic member is

$$
\begin{aligned}
\mathrm{X}_2 = (a_0^3 \beta + B) x_1^2 + (2a_0^5 a_2 + 2a_0^4 a_1^2 + a_0^3 a_1^2 a_2 + a_0^4 a_2^2 + a_0^2 a_1^4 \\
+ 2a_0 a_1^2 a_2^3 + 2a_0^2 a_2^4 + a_1^2 a_2^4 + a_0 a_2^5 + 2a_1^4 a_2^2) x_1 x_2 \\
+ (B + a_1 a_2^5 - a_1^3 a_2^3) x_2^2.
\end{aligned}
\tag{23}
$$

In addition we have the reducible covariants X_4 and $\mathrm{X}_6 = f_2 \xi_4 = a_0^3 \beta x_1^6 + \cdots$.

Covariants of even weight. Consider next the covariants which are of even weight and therefore of the form

$$
\begin{aligned}
K &= S' x_1^n + C_1 x_1^{n-1} x_2 + \cdots \ (n \text{ even}); \\
S' &= S_0 + S_1 a_0 + S_2 a_0^2 + S_3 a_0^3.
\end{aligned}
$$

For the purposes above outlined we construct a triad of covariants led by each seminvariant a_0, a_0^2, a_0^3.

The polars of f_2 by w are (cf. (18))

$$
\begin{aligned}
f_2 &= a_0 x^2 + 2a_1 x_1 x_2 + a_2 x_2^2, \\
f_4 &= 2wf_2 \equiv a_0 x_1^4 + a_1 (x_1^3 x_2 + x_1 x_2^3) + a_2 x_2^4, \\
f_6 &= 2w^2 f_2 = a_0 x_1^6 + 2a_1 x_1^3 x_2^3 + a_2 x_2^6.
\end{aligned}
\tag{24}
$$

The hexadic scale for the form f_2^2 contains the covariants (cf. § 5)

$$
\begin{aligned}
C_2 &= (a_0^2 + \Delta) x_1^2 + a_1 (a_0 + a_2) x_1 x_2 + (a_2^2 + \Delta) x_2^2, \\
C_4 = 2wC_2 &= (a_0^2 + \Delta) x_1^4 + 2a_1 (a_0 + a_2)(x_1^3 x_2 + x_1 x_2^3) \\
&\quad + (a_2^2 + \Delta) x_2^4, \\
C_6 = 2w^2 C_2 &= (a_0^2 + \Delta) x_1^6 + a_1 (a_0 + a_2) x_1^3 x_2^3 + (a_2^2 + \Delta) x_2^6 \\
&\equiv f_2 f_4 + \Delta Q \pmod 3,
\end{aligned}
\tag{25}
$$

and the scale for Ef_2 the covariants

$$
\begin{aligned}
\phi_2 &= Ef_2 = a_0^3 x_1^2 + 2a_1^3 x_1 x_2 + a_2^3 x_2^2, \\
\phi_4 &= 2w\phi_2 = a_0^3 x_1^4 + a_1^3 (x_1^3 x_2 + x_1 x_2^3) + a_2^3 x_2^4, \\
\phi_6 &= 2w^2 \phi_2 = a_0^3 x_1^6 + 2a_1^3 x_1^3 x_2^3 + a_2^3 x_2^6 \equiv f_2^3 \pmod 3.
\end{aligned}
\tag{26}
$$

To these lists we add the quantics f_2^2, $wf_2^2 = A_6$,

$$
\begin{aligned}
f_2^2 &= a_0^2 x_1^4 + a_0 a_1 x_1^3 x_2 + \Delta x_1^2 x_2^2 + a_1 a_2 x_1 x_2^3 + a_2^2 x_2^4, \\
A_6 &= a_0^2 x_1^6 + 2\Delta (x_1^4 x_2^2 + x_1^2 x_2^4) + (a_0 a_1 + a_1 a_2) x_1^3 x_2^3 + a_2^2 x_2^6.
\end{aligned}
\tag{27}
$$

Note that A_6 is reducible; $A_6 \equiv f_2 f_4 \pmod 3$.

Covariants led by invariants. In pursuance of our plan to secure a reduction of the general covariant K_n we now proceed to construct a formula for the most general concomitant whose leading coefficient is an invariant of even weight, i. e., a polynomial in the fundamental invariants Δ, Γ, J.*

Modular quantics of low orders, led by invariants, may be constructed as follows:

$$
(28) \qquad \begin{aligned} D_4 &= C_4 - f_2^2 = \Delta x_1^4 + (a_0 a_1 - a_1 a_2)(x_1^3 x_2 - x_1 x_2^3) + 2\Delta x_1^2 x_2^2 + \Delta x_2^4, \\ D_6 &= wD_4 = \Delta(x_1^6 + x_1^4 x_2^2 + x_1^2 x_2^4 + x_2^6) = \Delta Q. \end{aligned}
$$

The following covariants have, for leading coefficients, the invariant J:

$$
(29) \qquad \left.\begin{aligned} \lambda_4 &= 2f_2 \phi_2 + \Delta f_2^2 + \Gamma f_4 \equiv J x_1^4 + \cdots, \\ \lambda_6 &= JQ \equiv J x_1^6 + \cdots, \\ \lambda_8 &= 2f_2^4 + \Delta f_4^2 + \Gamma Q f_2 \equiv J x_1^8 + \cdots \end{aligned}\right\} \pmod 3.
$$

LEMMA. *There exists no covariant (modd 3; L), whose leading coefficient is the invariant Γ^e, other than $\Gamma^e Q^k$ ($k = 1, 2, \cdots$).*

Supposing that a covariant K_n exists in the form

$$
K_n = \Gamma^e x_1^n + C_1 x_1^{n-1} x_2 + \cdots, \qquad (n \not\equiv 0 \pmod 6),
$$

we have from (10),

$$
(30) \qquad \delta C_1 \equiv n\Gamma^e \pmod 3.
$$

But Γ^e contains the term a_2^{3e}, while C_1 is of the $3e$-th degree and

$$
(31) \qquad \delta a_0 = 0, \qquad \delta a_1 = a_0, \qquad \delta a_2 = a_0 + 2a_1.
$$

Hence (30) is impossible as, under (31), the increment of a $3e$-th degree function in a_0, a_1, a_2 cannot contain the term a_2^{3e}.

The arbitrary invariant leading coefficient of a covariant can now be written in the form

$$
S_0 = \Omega_1 \Delta + \Omega_2 J,
$$

in which Ω_1, Ω_2 are polynomials in Γ, Δ, and J only or are numerical.

By (13) there exists no quadratic covariant led by an invariant.

The general covariant of even weight and of order $6k + 4$, with an invariant as leader, may be written congruent to

$$
(32) \qquad (\Omega_1 D_4 + \Omega_2 \lambda_4) Q^k \ (\text{modd } 3;\ L),
$$

that of order $6k$ is evidently of the form AQ^k, where A is any invariant whatever, of even weight.

There is no concomitant of order $6k + 2$ led by the first power of Δ, and D_4^2 is an octic whose leader is Δ^2. Hence the general form of a covariant of

* In view of the syzygy $B^2 \equiv \Delta^3 \Gamma^2 + J(J - \Delta^2)^2 \pmod p$. Cf. Dickson, *Madison Colloquium Lectures*, p. 48.

the present type, of order $6k + 2 > 2$, is congruent (modd 3; L) to

$$(33) \qquad (w_1 D_4^2 + w_2 \lambda_8) Q^{k-1} \quad (k \neq 0),$$

where w_1, w_2, like Ω_1, Ω_2, are polynomials in Δ, J, Γ, or else are numerical.

The fundamental system of f_2. It is now evident that the general skew covariant of order $n = 6k + 4$, $k = 0, 1, \cdots$, as K_{6k+4}, is reduced, in the form which is suggested by the form of the seminvariant leader

$$S = \beta (S_0 + S_1 a_0 + S_2 a_0^2 + S_3 a_0^3).$$

That is,

$$(34) \qquad K_{6k+4} \equiv Q^k (- S_0 \zeta_4 + S_1 \vartheta_4 + S_2 \xi_4 + S_3 X_4) + LC' \pmod 3,$$

where C' is a non-skew covariant of order $6k$.

In the same manner K_{6k}, the arbitrary skew concomitant of order $6k$, is reducible as follows:

$$(35) \qquad K_{6k} \equiv Q^{k-1} (S_0 \zeta_6 + S_1 \vartheta_6 + S_2 \xi_6 + S_3 f_2 \xi_4) + LC' \pmod 3,$$

where C' is of order $6(k-1) + 2$, and is necessarily a covariant if it does not vanish, as $k > 0$.

As the next possibility to be treated take the general covariant K_{6k+2} of order $6k + 2 > 2 (k > 0)$. Again we can perform the required reduction in a simple manner, and the result is

$$(36) \quad K_{6k+2} \equiv Q^k (- S_0 C_1 + S_1 \vartheta_2 + S_2 \xi_2) + Q^{k-1} S_3 f_4 \xi_4 + LC' \pmod 3,$$

in which C' is of order $6(k-1) + 4$ and of even weight.

Consider next the case omitted from (36), i. e., the general form of a skew covariant of order 2. We may write this in the form

$$(37) \qquad K_2 \equiv \beta (S_0 + S_1 a_0 + S_2 a_0^2 + S_3 a_0^3) x_1^2 + \cdots.$$

But there exists no quadratic covariant K led by $a_0^3 \beta$, for, if one existed, then $K - X_2$ would be a quadratic covariant led by the invariant $2B$, which is an impossibility. This amounts to a proof that $S_3 \equiv 0 \pmod 3$, in (37), the reduced form of K_2 being

$$(38) \qquad K_2 \equiv - S_0 C_1 + S_1 \vartheta_2 + S_2 \xi_2 \pmod 3.$$

In accordance with this principle, for example,

$$X_2 \equiv \beta (2\Delta a_0 + \Gamma) x_1^2 + \cdots,$$

is reducible in the form

$$X_2 \equiv 2\Delta \vartheta_2 - \Gamma C_1 \pmod 3.$$

Collecting the irreducible covariants which occur in the reduced forms of those quantics which enter the formulas (34), (35), (36), (38) we reach the conclusion that all skew concomitants are reducible in terms of invariants and the set given below; together with concomitants of even weight:

$$Q,\ L,\ f_2,\ C_1,\ \phi_2,\ \vartheta_2,\ \xi_2,\ f_4,\ \zeta_4,\ \zeta_6.$$

Fundamental covariants of even weight. Concomitants of even weight are necessarily of the form $K_n = S' x_1^n + \cdots$, where

$$S' \equiv S_0 + S_1 a_0 + S_2 a_0^2 + S_3 a_0^3,$$

and hence, if $n = 6k + 4$,

$$K_n \equiv Q^k (\Omega_1 D_4 + \Omega_2 \lambda_4) + Q^k (S_1 f_4 + S_2 f_2^2 + S_3 \phi_4) + LC' \pmod 3, \tag{39}$$

and C' is a covariant of odd weight and order $6k$.

If $n = 6k > 0$, then

$$K_n \equiv Q^{k-1} (QS_0 + S_1 f_6 + S_2 f_2 f_4 + S_3 f_2^3) + LC' \pmod 3, \tag{40}$$

wherein C' is skew and of order $6(k - 1) + 2$.

In the same way the reduced form of the covariant of order $n = 6k + 2 > 2$ is

$$\begin{aligned} K_n = Q^{k-1} (w_1 D_4^2 + w_2 \lambda_8) + Q^k S_1 f_2 + Q^{k-1} (S_2 f_2 f_6 + S_3 f_2^2 f_4) \\ + LC' \pmod 3, \end{aligned} \tag{41}$$

C' being a skew covariant of order $6(k - 1) + 4$.

Passing to quadratic covariants led by S', note that

$$S' \equiv (S_0 + 2\Delta S_2) + S_2 (a_0^2 + \Delta) + S_1 a_0 + S_3 a_0^3 \pmod 3,$$

and hence, as quadratics led by $a_0^2 + \Delta$, a_0, and a_0^3 have been found, in order to avoid quadratic covariants led by invariants, we must have

$$S_0 + 2\Delta S_2 \equiv 0 \pmod 3.$$

The arbitrary non-skew quadratic covariant K_2 of the most general type possible is reduced, therefore, according to the formula

$$K_2 \equiv S_1 f_2 + S_2 C_2 + S_3 \phi_2 \pmod 3. \tag{42}$$

Summary. It is now evident that the successive application of the reduction processes represented in the congruential formulas (34) to (42), to the covariants C' appearing in these formulas, will completely reduce, in terms of the irreducible concomitants involved in the scales (20) to (27), all covariants which are reducible. Collecting the irreducible covariants so employed and not shown in the set given at the end of the preceding paragraph we have

$$C_2,\ D_4,\ \phi_4,\ f_6,$$

and hence we have demonstrated the following

THEOREM. *A fundamental system of formal invariants and covariants, modulo* 3, *of the binary quadratic form* f_2, *consists of eighteen quantics, as follows: four invariants* Δ, J, Γ, B; *six quadratic covariants* f_2, C_1, C_2, ϕ_2, ϑ_2, ξ_2; *four quartic covariants* f_4, D_4, ϕ_4, ζ_4; *two sextic covariants* f_6, ζ_6; *together with the two universal covariants* Q, L *of the total group* G_{48}.

It should be noted that this system contains as a subset the equivalents of the eight forms discovered by Dickson* and proved by him to compose a complete system of *modular* concomitants, i. e., those existing when the coefficients a_0, a_1, a_2 are themselves assumed to be, instead of independent variables, parameters representing least positive residues mod 3.

We append a table of the system found, constructed with reference to the degree-orders.

Order	Degree						
	0	1	2	3	4	5	6
0			Δ	Γ	J		B
2		f_2	C_2	C_1, φ_2	ϑ_2	ξ_2	
4	L	f_4	D_4	ζ_4, φ_4			
6	Q	f_6		ζ_6			

UNIVERSITY OF PENNSYLVANIA.

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