THE INVARIANTS OF FORMS UNDER THE BINARY LINEAR HOMOGENEOUS GROUP G_6 MODULO 2*

BY O. E. GLENN

1. *Introduction.* The transformation of an arbitrary binary quantic whose coefficients are written without binomial multipliers,

$$(1)\quad f = (a_0, \ldots, a_m)(x_1, x_2)^m = \prod_{i=0}^{m}(r_2^{(i)}x_1 - r_1^{(i)}x_2),$$

by the formulas

$$T:\ x_1 = \lambda_1 x_1' + \mu_1 x_2',\ x_2 = \lambda_2 x_1' + \mu_2 x_2',$$

in which λ_i, μ_j are such residues of a prime p that T ranges over the total group G of order $(p^2-p)(p^2-1)$, leads to the formal modular concomitant system of f. For various reasons $p = 2$ gives rise to exceptions in this theory; thus quadratic congruence theory becomes very special when $p = 2$, and also certain types of modular concomitants exist† for the even modulus that do not exist for $p > 2$.‡

2. *Analogies.* It is a known result of algebraic (non-modular) invariant theory that every concomitant of (1) is a polynomial in determinants of two types, viz. $(r^{(i)}r^{(k)})$, $(r^{(i)}x)$, i. e., linear forms themselves and resultants of pairs of them. Also the complete system of covariants of any number of quadratic quantics,

$$(2)\quad f_1 = (a_0, \ldots, a_2)(x_1, x_2)^2, \ldots,\ f_r = (l_0, \ldots, l_2)(x_1, x_2)^2,$$

is a set of concomitants that can be formed as transvectants of forms f_i taken in pairs.§ The dyadic combinations therefore furnish the complete seminvariant systems, also, but for the invariants it is found that the eliminants of the triadic combinations of the forms $f_1, \ldots, f_r$ are to be added.

---

* Presented to the Society, December 28, 1923.

† TRANSACTIONS OF THIS SOCIETY, vol. 19 (1918), p. 110.

‡ Dickson, *The Madison Colloquium Lectures,* Lecture III, p. 33-64.

§ Grace and Young, *Algebra of Invariants,* 1903, p. 161.

The facts are more complicated when the transformations form the group G_6 (mod 2). Then a simultaneous system of covariants of only two linear quantics

(3) $$f = a_0 x_1 + a_1 x_2, \qquad g = b_0 x_1 + b_1 x_2,$$

is composed of sixteen concomitants. These are tabulated below. The methods for their derivation are exemplified later in this paper in the corresponding problem for two quadratics although the two problems are not without differences in respect to detail. We shall use the abbreviations

(4) $$E_1 = a_0^2 \frac{\partial}{\partial a_0} + a_1^2 \frac{\partial}{\partial a_1},$$
$$E_2 = b_0^2 \frac{\partial}{\partial b_0} + b_1^2 \frac{\partial}{\partial b_1}, \qquad w = x_1^2 \frac{\partial}{\partial x_1} + x_2^2 \frac{\partial}{\partial x_2}$$

and, if two linear covariants are

$$C = c_0 x_1 + c_1 x_2, \; D = d_0 x_1 + d_1 x_2,$$

$[CD]$ is the covariant

(5) $$[CD] = (c_0 d_0 + c_0 d_1 + c_1 d_0) x_1 + (c_1 d_1 + c_0 d_1 + c_1 d_0) x_2.$$

The covariant R in the list is led by the invariant (ab), viz.:

(6) $$R = (a_0 b_1 + a_1 b_0) x_1^3 + (a_0 b_1 + a_0 b_0 + a_1 b_1) x_1^2 x_2 + (a_1 b_0 + a_0 b_0 + a_1 b_1) x_1 x_2^2 + (a_0 b_1 + a_1 b_0) x_2^3.$$

Covariants of two linear forms under G_6:

Invariants: (ab), $I = a_0^2 + a_0 a_1 + a_1^2$, $J = b_0^2 + b_0 b_1 + b_1^2$,
$L_1 = a_0^2 a_1 + a_0 a_1^2$, $L_2 = b_0^2 b_1 + b_0 b_1^2$.

Linear Covariants: f, g, $E_1 f$, $E_2 g$, $[fg]$, $[gE_1 f]$,
$[fE_2 G]$, $[E_1 f E_2 g]$.

Quadratic covariants: wf, wg, $Q = x_1^2 + x_1 x_2 + x_2^2$.

Cubic covariants: R, $L = x_1^2 x_2 + x_1 x_2^2$.

Thus the independent covariants of a set of linear quantics, under G_6, form an extensive set which increases rapidly as the number of quantics is increased. If we add a third form $h = c_0 x_1 + c_1 x_2$ to the set f, g we shall have to consider concomitants formed from ground-forms in triadic combinations, as is proved by the existence of the following irreducible seminvariant:

(7) $$C = a_0b_0c_1 + a_0b_1c_1 + a_1b_0c_1 + a_1b_1c_0.$$

Similar considerations hold, under more complicated circumstances, for the simultaneous systems, for G_6, of a set of quadratic quantics. The rest of this paper concerns the system of two quadratics.

3. *Seminvariants.* Let Γ be the linear transformations upon a_0, a_1, a_2 which are induced by transforming f by

$$T: \; x = x_1' + x_2', \; x_2 = x_2',$$

and suppose Γ' to be that which corresponds by transformation of g by T, where

$$f = a_0x_1^2 + a_1x_1x_2 + a_2x_2^2, \quad g = b_0x_1^2 + b_1x_1x_2 + b_2x_2^2.$$

Then,

(8) $$\begin{cases} \Gamma: & a_0' = a_0, \; a_1' = a_1, \; a_2' = a_0 + a_1 + a_2, \\ \Gamma': & b_0' = b_0, \; b_1' = b_1, \; b_2' = b_0 + b_1 + b_2. \end{cases}$$

With suitable restrictions we connect the problem of the seminvariants of f and g with a simpler problem, previously solved, by taking $a_0 = 0$, temporarily. We then have two simultaneous groups (mod 2), viz.,

(9) $$\begin{cases} \Gamma_1: & a_1' = a_1, \; a_2' = a_1 + a_2, \\ \Gamma_1': & b_0' = b_0, \; b_1' = b_1, \; b_2' = b_0 + b_1 + b_2, \end{cases}$$

concerning which it is known that a fundamental system of universal concomitants consists of six quantics, as follows:*

(10) $$a_1, \; b_0, \; b_1, \; \psi_1 = a_2^2 + a_1a_2, \; s = (b_0 + b_1 + b_2)b_2,$$
$$\varrho_1 = a_1b_2 + a_2(b_0 + b_1).$$

We desire six seminvariants of the set f, g such that the forms (10) are respectively residual to the six when $a_0 \equiv 0$ (mod 2).

The seminvariant of f of the type of s is $a_0a_2 + \psi_1 = \sigma$. The leading coefficient of $[fg]$† is $a_0b_0 + (fg)$, where (fg) is the invariant

$$(fg) = (a_0 + a_1)(b_1 + b_2) + (b_0 + b_1)(a_1 + a_2) + a_1b_1.$$

The form ϱ_1 is the residue (mod a_0) of $(fg) + (b_0 + b_1)a_1 = x$.

---

* TRANSACTIONS OF THIS SOCIETY, vol. 21 (1920), p. 293.

† The symbolism (fg), $[fg]$, $\{fg\}$, $\{\overline{fg}\}$, explained in (19) in the present article, was first defined in PROCEEDINGS OF THE NATIONAL ACADEMY, vol. 5 (1919), p. 107.

Assume, in arbitrary form, a seminvariant S of the set f, g,

(11) $$S = S(a_0, a_1, a_2, b_0, b_1, b_2);$$

then, by (10),

(12) $$S_1 = S(0, a_1, a_2, b_0, b_1, b_2) \equiv F(a_1, b_0, b_1, \psi_1, s, \varrho_1) \pmod{2},$$

where F is a polynomial in its arguments with integral coefficients. Hence we can arrange S as an expression of the form

(13) $$S \equiv F(a_1, b_0, b_1, \sigma, s, x) + a_0 F_1(a_0, a_1, a_2, b_0, b_1, b_2) \pmod{2},$$

and F_1 is evidently a seminvariant of the set f, g. This process of reduction can be applied successively until we reach a coefficient quantic F_r which is free from a_0 (explicitly), it being, therefore, a polynomial in

$$a_1, b_0, b_1, \sigma, s, x,$$

i. e.,

(14) $$S \equiv F + a_0 F_1 + a_0^2 F_2 + \cdots + a_0^r F_r \pmod{2}.$$

THEOREM. *A fundamental system of seminvariants of the set* f, g (mod 2) *consists of the seven forms*

(15) $$a_0, b_0, a_1, b_1, \sigma, s, (fg).$$

4. *Syzygies.* The expressions $k = a_0\sigma$, $\varkappa = b_0 s$, a_1, b_1, $q_1 = \sigma + a_0^2 + a_0 a_1$, $q_2 = s + b_0^2 + b_0 b_1$, (fg) are pure invariants. The following syzygies can be verified:

(16) $$\begin{cases} a_0^3 + a_0^2 a_1 + a_0 q_1 + k = 0, \\ b_0^3 + b_0^2 b_1 + b_0 q_2 + \varkappa = 0, \\ \varrho^2 + (a_0 + a_1)(b_0 + b_1)\varrho + (a_0^2 + a_1^2)s + (b_0^2 + b_1^2)\sigma \\ \qquad + (a_0 b_0 + a_1 b_1)(a_0 b_1 + a_1 b_0) = 0, \end{cases}$$

where $\varrho = (fg) + a_1 b_1$.

These syzygies may be employed as literal moduli of reduction for the purpose of reducing the arbitrary seminvariant $S(a_0, a_1, a_2, b_0, b_1, b_2)$ to a polynomial of finite order in a_0, b_0. We have immediately the following theorem.

THEOREM. *The arbitrary seminvariant S of two quadratic forms f, g can be represented in the finite form*

(17) $$S = \Phi_0 + \Phi_1 b_0 + \Phi_2 b_0^2 + a_0(\psi_0 + \psi_1 b_0 + \psi_2 b_0^2) + a_0^2(\chi_0 + \chi_1 b_0 + \chi_2 b_0^2),$$

in which Φ_i, ψ_i, χ_i are polynomials in the invariants

$$q_1,\ q_2,\ k,\ \varkappa,\ a_1,\ b_1,\ (fg), \tag{18}$$

and the highest power of (fg) which occurs is the first.

5. *A Method in Covariants.* It is known that a complete concomitant scale,* for the modulus 2, of a covariant,

$$C = C_0 x_1^M + C_1 x_1^{M-1} x_2 + \cdots + C_M x_2^M,$$

of a quantic f_m of order m, for the reduction of all concomitants of degree unity in the coefficients of C and of order > 3, is composed of

$$\left\{\begin{aligned} & C,\ (C) = C_1 + C_2 + \cdots + C_{M-1}, \\ & \qquad\qquad [C] = (C_0 + (C))x_1 + ((C) + C_M)x_2, \\ & \{C\} = C_0 x_1^2 + (C)x_1 x_2 + C_M x_2^2, \\ & \{\bar{C}\} = C_0 x_1^3 + J_1 x_1^2 x_2 + J_2 x_1 x_2^2 + C_M x_2^3, \\ & \qquad\qquad (J_1 + J_2 \equiv (C) \pmod 2)). \end{aligned}\right. \tag{19}$$

The latter covariant is existent only when M is an odd number. This scale produces concomitants of f_m from any covariant of the latter by the principle of copied forms.

Another method, not previously described, for the construction of covariants of f_m, to any prime modulus p, is to make an appropriate selection of a primary quantic,

$$P_0 = q_0 x_1^\alpha + q_1 x_1^{\alpha-1} x_2 + \cdots + q_\alpha x_2^\alpha, \tag{20}$$

of given degree-order (i, α) and apply to it, simultaneously, the substitutions of the group upon the variables generated by $x_1 = x_1' + x_2'$, $x_2 = x_2'$, and the corresponding substitutions of the induced group upon the coefficients. We thus obtain p quantics

$$P_0,\ P_1 = (q_0', \ldots, q_\alpha')(x_1, x_2)^\alpha,\ \ldots,\qquad P_{p-1} = (q_0^{(p-1)}, \ldots, q_\alpha^{(p-1)})(x_1, x_2)^\alpha, \tag{21}$$

and, if we assume that the primary quantic has been properly selected, any symmetric function of $P_0, P_1, \ldots, P_{p-1}$ is a covariant, modulo p, of f_m. Not many rules, other than em-

---

* TRANSACTIONS OF THIS SOCIETY, vol. 19 (1918), p. 110; vol. 20 (1919), p. 155.

pirical ones, for the determination of primary quantics, are known to the writer, but examples of the method are shown in the next paragraph. Obviously P_0 should be such that the assumed symmetric function is invariantive under the other two generators of the total group (mod p), i. e., $x_1 = x_1'$, $x_2 = \lambda x_2'$; $x_1 = x_2'$, $x_2 = -x_1'$.

6. *Fundamental Covariants.* We are evidently able to reduce all covariants in terms of those of orders 0, 1, 2, 3 led by seminvariants $a_0^i b_0^j$, $(i, j = 0, 1, 2)$ and by the invariants of which Φ_0 in (17) is a function. A formula showing this reduction in general form will be derived.

We find the following covariants with the leading coefficients which are adjoined. Abbreviations employed are

$$E_1 = a_0^2\frac{\partial}{\partial a_0} + a_1^2\frac{\partial}{\partial a_1} + a_2^2\frac{\partial}{\partial a_2},$$

$$E_2 = b_0^2\frac{\partial}{\partial b_0} + b_1^2\frac{\partial}{\partial b_1} + b_2^2\frac{\partial}{\partial b_2}.$$

Linear forms:

$a_0 + a_1, [f]$; $b_0 + b_1, [g]$; $a_0 b_0 + (fg), [fg]$;
$a_0^2 + a_1^2, [E_1 f]$; $b_0^2 + b_1^2, [E_2 g]$; $a_0 b_0^2 + (fE_2 g), [fE_2 g]$;
$a_0^2 b_0 + (gE_1 f), [gE_1 f]$; $a_0^2 b_0^2 + (E_1 f E_2 g), [E_1 f E_2 g]$.

Quadratic forms:

a_0, f; b_0, g; $a_0^2, E_1 f$; $b_0^2, E_2 g$; $a_0 b_0, \{fg\}$;
$a_0^2 b_0, \{gE_1 f\}$; $a_0 b_0^2, \{fE_2 g\}$; $a_0^2 b_0^2, \{E_1 f E_2 g\}$.

There are no linear covariants, in the domain, led by invariants, and the only quadratic covariants whose leading coefficients are invariants are comprised in the formula IQ, where I is an arbitrary invariant. The only invariantive leader of covariants of the third order which we shall be required to consider is Φ_0 (cf. (17)). Let ζ be the operation of applying to a primary quantic P_0 the substitutions

(22) $$x_1 = x_1' + x_2', \quad x_2 = x_2'.$$
$$a_0' = a_0, \quad a_1' = a_1, \quad a_2' = a_0 + a_1 + a_2.$$

If the primary is

(23) $$P_0 = (a_0 + a_2)x_1 + (a_0 + a_1)x_2,$$

then

$$P_1 = \zeta P_0 = (a_1 + a_2)x_1 + (a_0 + a_2)x_2,$$

so that

$$(24)\quad \begin{cases} \sum P_0 = (a_0+a_1)x_1+(a_1+a_2)x_2 = [f], \\ \Delta_1 = \sum P_0P_1 = [(a_0+a_2)x_1+(a_0+a_1)x_2] \\ \qquad\qquad \times[(a_1+a_2)x_1+(a_0+a_2)x_2]. \end{cases}$$

If the primary quantic is

$$P_0 = (b_0+b_2)x_1+(b_0+b_1)x_2,$$

we obtain, similarly,

$$(25)\quad \begin{cases} \sum P_0 = (b_0+b_1)x_1+(b_1+b_2)x_2 = [g], \\ \Delta_2 = \sum P_0P_1 = [(b_0+b_2)x_1+(b_0+b_1)x_2] \\ \qquad\qquad \times[(b_1+b_2)x_1+(b_0+b_2)x_2]. \end{cases}$$

The respective seminvariant leading coefficients of the covariants $[f]\Delta_1$, $[g]\Delta_2$ are the invariants

$$(26)\qquad a_1q_1+k, \quad b_1q_2+\varkappa,$$

and these may replace k, $\varkappa$, respectively, in the system (18). Instead of (fg) in the fundamental system (15), we may employ $(fg)_1 = (fg)+a_1b_1$, which is the resultant of $[f]$ and $[g]$. A cubic covariant led by $(fg)_1$ is

$$(27)\qquad B = [fg]Q+[f]g+a_1[g]Q.$$

There exist no cubic covariants led by any of the invariants k, $\varkappa$, q_1, q_2, due to the fact that all of these invariants contain a term which is left unaltered by the permutational substitution* $(a_0a_2)(a_1)(b_0b_2)(b_1) = S_1$.

The cubic covariants which we require, with their leading coefficients, are listed below.

Cubic forms:

a_0+a_1, $[f]Q$; $a_0^2+a_1^2$, $[E_1f]Q$; b_0+b_1, $[g]Q$;
$b_0^2+b_1^2$, $[E_2g]Q$; $a_0b_0+(fg)$, $[fg]Q$; $a_0^2b_0+E_1(fg)$, $[E_1fg]Q$;
$a_0b_0^2+E_2(fg)$, $[fE_2g]Q$; $a_0^2b_0^2+E_1E_2(fg)$, $[E_1fE_2g]Q$; $(fg)_1$, B.

THEOREM. *An invariant leading coefficient Φ_0 of a cubic covariant of f, g is necessarily congruent modulo 2 to the expression*

$$(28)\qquad C = (a_1q_1+k)\psi_1'+(b_1q_2+\varkappa)\psi_2'+(fg)_1\psi_3',$$

where the quantics ψ_i' are invariants.

* TRANSACTIONS OF THIS SOCIETY, vol. 19 (1918), p. 111.

To prove this we note that the invariant Φ_0 (cf. (17)) is always of the form

$$F(q_1, q_2, a_1, b_1) + C = \Phi_0, \tag{29}$$

where F is an integral form in its arguments. We have constructed covariants whose leaders are the invariants of the set

$$a_1 q_1 + k,\ b_1 q_2 + \varkappa,\ (fg)_1.$$

If G is a covariant whose leader is Φ_0, we have that

$$G + \psi_1'[f]\Delta_1 + \psi_2'[g]\Delta_2 + \psi_3 B \tag{30}$$

is a cubic covariant led by F, and this is an absurdity because every possible form F evidently contains* a term which is left unaltered by S_1. Hence $F \equiv 0 \pmod 2$, $\Phi_0 \equiv C$ (mod 2), which was to be proved.

7. *Reductions of the Arbitrary Linear, Quadratic, and Cubic Covariants.* Let $\sum_1$ represent a covariant of order unity whose seminvariant leading coefficient is S (cf. 17)). We have, identically, $S = I + J$, where

$$(31)\quad \begin{cases} I = (b_0 + b_1)\Phi_1 + (b_0^2 + b_1^2)\Phi_2 + (a_0 + a_1)\psi_0 \\ \quad + [a_0 b_0 + (fg)]\psi_1 + [a_0 b_0^2 + (fE_2 g)]\psi_2 + (a_0^2 + a_1^2)\chi_0 \\ \quad + [a_0^2 b_0 + (gE_1 f)]\chi_1 + [a_0^2 b_0^2 + (E_1 f E_2 g)]\chi_2; \\ J = \Phi_0 + b_1\Phi_1 + b_1^2\Phi_2 + a_1\psi_0 + (fg)\psi_1 + (fE_2 g)\psi_2 \\ \quad + a_1^2\chi_0 + (gE_1 f)\chi_1 + (E_1 f E_2 g)\chi_2. \end{cases}$$

The following covariant is led by I:

$$(32)\quad \begin{cases} K_1 = \Phi_1[g] + \Phi_2[E_2 g] + \psi_0[f] + \psi_1[fg] + \psi_2[fE_2 g] \\ \qquad + \chi_0[E_1 f] + \chi_1[gE_1 f] + \chi_2[E_1 f E_2 G]. \end{cases}$$

Therefore, there would exist a linear covariant led by the invariant J, viz., $\sum_1 + K_1$, unless $J \equiv 0 \pmod 2$. Thus every linear covariant $\sum_1$ is reduced by the formula (32), ($\sum_1 = K_1$).

Let $\sum_2$ represent an arbitrary quadratic covariant which is led by S. The following covariant has S for seminvariant leader:

$$(33)\quad \begin{cases} K_2 = \Phi_0 Q + \Phi_1 g + \Phi_2 E_2 g + \psi_0 f + \psi_1\{fg\} \\ \qquad + \psi_2\{fE_2 g\} + \chi_0 E_1 f + \chi_1\{gE_1 f\} + \chi_2\{E_1 f E_2 g\}. \end{cases}$$

Then K_2 differs from $\sum_2$ by some covariant which contains x_2

* The number $\binom{2m}{m}$ is even for all integers m.

as a factor; but, as no quadratic covariant can be factored thus, we have $\sum_2 \equiv K_2$ (mod 2), i. e., the arbitrary quadratic covariant is reduced.

Let $\sum_3$ represent an arbitrary covariant of order 3 with seminvariant leader S. The following is a cubic covariant whose leading coefficient is I (cf. (31)): $K_3 = K_1 Q$. Note therefore that $\sum_3 + K_3 = \Gamma_3$ is a covariant whose leader is J. Hence, by (28) (Theorem),

$$J \equiv C + (fE_2g)_1\psi_2 + (gE_1f)_1\chi_1 + (E_1fE_2g)_1\chi_2,$$

that is,

$$(34) \qquad \Gamma_3 = \psi_1'[f]\Delta_1 + \psi_2'[g]\Delta_2 + \psi_3'B + (\psi_2E_2 + \chi_1E_1 + \chi_2E_1E_2)B,$$

where $(fE_2g)_1 = E_2(fg)_1 = (fE_2g) + a_1b_1^2$, (cf. (27)). Note that operations by E_1, E_2 upon B produce only polynomials in covariants already listed. We have now reduced $\sum_3$ to the form

$$(35) \qquad \sum_3 = K_3 + \Gamma_3 + \Theta L \quad (\text{mod } 2),$$

since L is the only cubic covariant which contains x_2 as a factor. The quantic Θ is a pure invariant, but it is not known whether it is reducible, in all cases, entirely in terms of the invariants of the set (18). The following theorem has now been established.

THEOREM. *A fundamental system of formal covariants of the set consisting of the two binary quadratics*

$$(36) \quad f = (a_0, a_1, a_2)(x_1, x_2)^2, \quad g = (b_0, b_1, b_2)(x_1, x_2)^2,$$

under the total group G_6, *modulo* 2, *is composed of* 21 *quantics, namely, seven invariants,* $q_1, q_2, k, \varkappa, a_1, b_1, (fg)$, *eight linear covariants,* $[f]$, $[g]$, $[fg]$, $[E_1f]$, $[E_2g]$, $[fE_2g]$, $[gE_1f]$, $[E_1fE_2g]$, *five quadratic covariants,* Q, f, g, Δ_1, Δ_2, *and one cubic covariant,* L.

The remaining forms are reducible, as follows:

$$E_1f = [f]^2 + a_1^2Q, \quad E_2g = [g]^2 + b_1^2Q,$$
$$\{fg\} = [f][g] + a_1g + b_1f + a_1b_1Q, \quad \{gE_1f\} = E_1\{fg\},$$
$$\{fE_2g\} = E_2\{fg\}, \quad \{E_1fE_2g\} = E_1E_2\{fg\}.$$

THE UNIVERSITY OF PENNSYLVANIA