INVARIANTS IN THE THEORY OF NUMBERS*

BY

L. E. DICKSON

1. Polynomials in the coefficients of a form $f(x_1, \cdots, x_n)$ which have the invariantive property with respect to all linear homogeneous transformations on $x_1, \cdots, x_n$ with integral coefficients taken modulo p, where p is a prime, are called formal invariants modulo p of f if the coefficients of f are independent variables, but are called modular invariants if the coefficients of f are integers taken modulo p. The concept of formal invariants modulo p was introduced by Hurwitz;† but the only known results concerning them relate to the binary quadratic and cubic forms.‡ On the contrary, a simple and effective theory of modular invariants has been given by the writer. A new method of deriving modular invariants from seminvariants is given in § 8. But the main purpose of this paper is to present a simple general method of constructing formal invariants. The method is applicable also to formal seminvariants and, more generally, to the invariants of any linear congruence group (§ 7). Moreover, the new point of view forms an adequate basis for a general theory of formal invariants.

Construction of Formal Invariants

2. The method of construction will first be illustrated by the simple example of the binary quadratic form

$$Q = ax^2 + bxy + cy^2$$

for the case of modulus 2. The only real points (i. e., with integral coördinates) modulo 2 are

$$P_1 = (1, 0), \qquad P_2 = (0, 1), \qquad P_3 = (1, 1).$$

The corresponding values of Q are

$$a, \qquad c, \qquad s = a + b + c.$$

By the interchange of x and y in Q, a and c are interchanged, also P_1 and P_2.

* Presented to the Society at Providence, September 7, 1914.

† Archiv der Mathematik und Physik, ser. 3, vol. 5 (1903), p. 25.

‡ Dickson, *On Invariants and the Theory of Numbers, Madison Colloquium Lectures*, American Mathematical Society, pp. 40–54.

By the transformation $x' = x + y$, $y' = y$, Q is replaced modulo 2 by a form with the same a and b, but with c replaced by s; then c and s are interchanged, as well as P_2 and P_3. Since any binary linear transformation with integral coefficients modulo 2 is generated by the preceding two, it follows that any such transformation gives rise to a permutation of a, c, s amongst themselves, and the same permutation of P_1, P_2, P_3. Hence *any symmetric function of* a, c, s *is a formal invariant modulo* 2 *of* Q.

The elementary symmetric functions are, modulo 2,

$$b, \qquad q = a^2 + ac + c^2 + (a + c)b, \qquad k = ac(a + b + c).$$

They form* a fundamental system of rational integral formal invariants modulo 2 of Q.

3. Consider the system of forms Q and

$$l = \eta x + \xi y.$$

The values of l at the points P_1, P_2, P_3 are $\eta, \xi, \eta + \xi$, respectively. The latter undergo the same permutation as the P's when l is transformed linearly (§ 2). Hence, if ϕ is any polynomial in two arguments,

$$\phi(a, \eta), \qquad \phi(c, \xi), \qquad \phi(s, \eta + \xi)$$

are permuted amongst themselves when Q and l are transformed linearly modulo 2. Hence any symmetric function of these three ϕ's is a formal invariant modulo 2 of Q and l.

Taking $\phi(a, \eta)$ to be η, $a\eta$, and $a\eta^2$, in turn, and employing the elementary symmetric functions in each case, we get the following formal invariants of Q and l:

$$\lambda = \xi^2 + \xi\eta + \eta^2, \qquad \pi = \xi\eta(\xi + \eta), \qquad j = (a + b)\xi + (b + c)\eta,$$

$$t = ac\xi\eta + s(a\eta + c\xi)(\xi + \eta), \qquad u = (a + b)\xi^2 + (b + c)\eta^2,$$

$$v = ac\xi^2\eta^2 + s(a\eta^2 + c\xi^2)(\xi^2 + \eta^2),$$

and $k\pi$, $k\pi^2$. From $\phi = a\eta^4$, we get

$$U = (a + b)\xi^4 + (b + c)\eta^4 = \lambda u + j\pi.$$

Also t and v can be expressed in terms of simpler invariants:

$$t = q\lambda + j^2 + bu, \qquad v = q\lambda^2 + u^2 + bU.$$

Whether or not the reduced set $b, q, k, \lambda, \pi, j, u$ form a fundamental system of formal invariants modulo 2 of Q and l has not been investigated.

But if we pass to modular invariants by regarding a, b, c, ξ, η to be integers

* *Madison Colloquium Lectures*, p. 42.

taken modulo 2, we have $k \equiv bq$, $\pi \equiv 0$, $u \equiv j$, and the reduced set b, q, λ, j form* a fundamental system of modular invariants of Q and l.

4. Passing to the general case, let

$$f_1(x_1, \cdots, x_n), \quad \cdots, \quad f_t(x_1, \cdots, x_n)$$

be forms of total degrees $d_1, \cdots, d_t$ in the independent variables $x_1, \cdots, x_n$. Let the modulus be p and let g_i be the greatest common divisor of $p-1$ and d_i. Set $q_i = (p-1)/g_i$. Then for any integer ρ not divisible by p,

$$\rho^{d_i q_i} = (\rho^{p-1})^{d_i/g_i} \equiv 1 \pmod{p},$$

by Fermat's theorem. Hence, since f_i is of degree d_i,

$$[f_i(\rho x_1, \cdots, \rho x_n)]^{q_i} \equiv [f_i(x_1, \cdots, x_n)]^{q_i} \pmod{p}.$$

Using homogeneous coördinates, let $(x_1, \cdots, x_n)$ be the same point as $(\rho x_1, \cdots, \rho x_n)$, when ρ is any integer not divisible by p. The preceding formula shows that $f_i^{q_i}$ has a definite value at each real point (i. e., one with integral coördinates taken modulo p). The values at the various real points are merely permuted amongst themselves by any linear homogeneous transformation on $x_1, \cdots, x_n$ with integral coefficients taken modulo p. In fact, the real points are permuted by such a transformation. We thus have the

THEOREM. *We obtain a formal invariant modulo p of the system of forms $f_i(x_1, \cdots, x_n)$, $i = 1, \cdots, t$, if we take any symmetric function with integral coefficients of the quantities*

$$\phi(f_1^{q_1}, \cdots, f_t^{q_t})$$

given by substituting in turn for the x's the coördinates of the

$$P = 1 + p + p^2 + \cdots + p^{n-1}$$

real points. Here ϕ is any polynomial in its t arguments with integral coefficients, and q_i is the quotient of $p-1$ by the greatest common divisor of $p-1$ and the degree of f_i.

Each q_i is unity if $p = 2$ (cf. §§ 2, 3); also if $p = 3$ and each f_i is of even degree. For example, if $t = 1$ and

$$f = f_1 = ax^2 + 2bxy + cy^2,$$

and $p = 3$, the values of f at the $P = 4$ real points $(1, 0)$, $(0, 1)$, $(1, 1)$, $(-1, 1)$ are respectively

$$a, \quad c, \quad a - b + c, \quad a + b + c.$$

* *Madison Colloquium Lectures*, p. 57.

The elementary symmetric functions reduce modulo 2 to zero and

$$ac - b^2, \qquad (a + c)(a + b - c)(a - b - c),$$

$$ac(a + b + c)(a - b + c),$$

respectively. The first is the discriminant D of f. The last two are $\gamma_2 = \Gamma$ and $a\gamma_0 = J$ in the notations of the *Madison Colloquium Lectures*, pages 43–45.

A further evident invariant is the product of all non-proportional linear functions of a, b, c with integral coefficients taken modulo 3. Hence its quotient

$$B = b(b + a)(b - a)(c - a)(c - b)(c + b)$$

by ΓJ is a formal invariant. In the place just cited it was proved that D, Γ, J, B form a fundamental system of formal invariants modulo 3 of f.

If $p = 5$, the sum of the products by twos of the squares of the values of f at the six real points is

$$3(ac - b^2)^2 \pmod 5.$$

Hence as before we are led to the algebraic discriminant, as well as to invariants peculiar to the number theory case.

5. The present method is particularly useful for forms in three or more variables, since the construction of formal or modular invariants by earlier methods is excessively laborious and dependent largely upon special devices.

As an illustration, consider

$$F(x) = a_1 x_2 x_3 + a_2 x_1 x_3 + a_3 x_1 x_2 + b_1 x_1^2 + b_2 x_2^2 + b_3 x_3^2$$

for the modulus 2. Its values v_j for the seven real points are

$$b_1, \quad b_2, \quad b_3, \quad a_1 + b_2 + b_3, \quad a_2 + b_1 + b_3, \quad a_3 + b_1 + b_2,$$

$$\sum_{i=1}^{3} (a_i + b_i).$$

Since their sum is zero modulo 2, we readily get

$$\sum v_1 v_2 = \sum a_1 b_1 + \sum a_1^2 + a_1 a_2 + a_1 a_3 + a_2 a_3 = \alpha,$$

$$\sum v_1^2 v_2 = \sum v_1 v_2 v_3 = \sum a_1 b_1^2 + \sum a_1^2 b_1 + \sum a_1 a_2^2,$$

$$\sum v_1 v_2 v_3 v_4 = \alpha \sum b_1^2 + \sum a_1 b_1 (a_1 + b_1)(b_2 + b_3) + \sum a_1 a_2 b_1 b_2$$

$$+ (a_1 a_2 a_3 + a_1 a_2 b_3 + a_1 a_3 b_2 + a_2 a_3 b_1) \sum a_1$$

$$+ \sum b_1^4 + \sum b_1^2 b_2^2 + b_1 b_2 b_3 \sum b_1.$$

The second is congruent to the sum of the formal invariants

$$\Delta = a_1 a_2 a_3 + \sum a_1^2 b_1, \qquad \Delta_1 = a_1 a_2 a_3 + \sum a_1 b_1^2 + \sum a_1 a_2^2,$$

which, with a modular invariant J, are given on pages 69 and 74 of the *Madison Colloquium Lectures*. Note that Δ is the discriminant of F.

If we take each a_i and b_i to be an integer modulo 2, we find that our third invariant reduces to the modular invariant $J + \alpha + 1$. Set $A = \alpha + \Delta + 1$. It is proved on page 76 of the same book that Δ, A, and J form a fundamental system of modular invariants of F.

As shown indirectly in § 6, we cannot construct a fundamental system of modular invariants of F by use of the real points only, but succeed if we use also points whose coördinates are Galois imaginaries.

Criteria for the Equivalence of Modular Forms

6. An important application of modular invariants is that to the question of the equivalence of two modular forms under linear transformation with integral coefficients taken modulo p. We can treat this question by means of the idea underlying the foregoing construction of invariants, without actually constructing them. For example, consider the ternary quadratic form modulo 2. As well known, such a form is equivalent to one and but one of the forms

$$x_1 x_2 + x_3^2\,[4], \qquad x_1 x_2 + x_1^2 + x_2^2\,[6], \qquad x_1 x_2\,[2], \qquad x_1^2\,[4], \qquad 0\,[0].$$

After each form we have given the number of real points for which it is congruent to unity modulo 2. Hence no two of these forms are equivalent, with a possible exception in the case of the first and fourth. To show by the same method that the latter are not equivalent, we employ the points each of whose coördinates are $0, 1, j$ or $j+1$, where j is the Galois imaginary for which

$$j^2 + j + 1 \equiv 0 \pmod 2. \tag{1}$$

Now x_1^2 vanishes for just five such points, viz., $(0,0,1)$ and $(0,1,a)$, where $a = 0, 1, j$ or $j+1$. But $x_1 x_2 + x_3^2$ vanishes for just nine such points, viz., $(0,b,0)$, $(b,0,0)$, $(1,b,b^2)$, where $b = 1, j$, or $j+1$. Hence the two forms are not equivalent.

The second of our five forms vanishes for just nine such points, viz., $(0,0,1)$, $(1,j,a)$, $(1,j+1,a)$. Finally, $x_1 x_2$ vanishes only for nine such points. Hence the five forms vanish for respectively 6, 8, 4, 2, 14 imaginary points whose coördinates depend upon j. Thus *the classes of conics modulo 2 are completely characterized by the number of their imaginary points whose coördinates are functions of a root of* (1).

We readily find the characteristic invariant I_k for the kth class, i. e., an invariant with the value unity for any form in the kth class and the value zero for the remaining forms. For the class represented by our second form,

I_2 is the sum of the products six at a time of the values of F for the seven real points. For the class represented by $x_1 x_2$, I_3 is the sum of the products by twos of those values. We get $I_1 + I_4$ by using the products by fours; to get I_1 itself, we employ imaginary points as above. Finally,

$$1 + I_1 + I_2 + I_3 + I_4 = I_5.$$

Construction of Formal Seminvariants

7. The preceding method is readily extended to the general case of the formal invariants of any system of forms under any group of linear transformations modulo p.

By way of illustration, consider the form Q of § 2 and the group composed of the identity and

$$T: \qquad x' \equiv x + y, \qquad y' \equiv y \pmod 2.$$

It is therefore the question of the formal seminvariants of Q. Since T leaves unaltered the point P_1 of § 2 and interchanges the points P_2 and P_3, a and any symmetric function of c and s are formal seminvariants. The elementary symmetric functions are $a + b$ and cs. These with a form in fact a fundamental system of formal seminvariants modulo 2 of Q (*Madison Colloquium*, page 42).

Similarly, the system of forms Q and l (§ 3) have the formal seminvariants modulo 2

$$a, \qquad \eta, \qquad \phi(c, \xi) + \phi(s, \eta + \xi), \qquad \phi(c, \xi) \cdot \phi(s, \eta + \xi),$$

where ϕ is any polynomial in its two arguments.

Derivation of Modular Invariants from Seminvariants

8. The method will be illustrated for the binary quadratic form Q (§ 2) and the modulus 2. The coefficients are integers taken modulo 2. To make the treatment self-contained, we shall first derive a fundamental system of modular seminvariants. The transformation

$$(x + ty, y): \qquad x' = x + ty, \qquad y' = y$$

replaces Q by $ax^2 + bxy + c'y^2$, where $c' = c + (a + b)t$. Hence a and b are seminvariants of Q. If $a + b \equiv 1$, we take $t = c$ and have $c' \equiv 0$. If $a + b \equiv 0$, then $c' \equiv c$ and the value of c is given by

$$J = (1 + a + b)c.$$

Since J has the same value for equivalent forms Q, it is a seminvariant. The first column of the following table gives a representative of each class $c_1, \cdots, c_6$ of forms Q.

Representative of the Class	Determined by Seminvariants	Characteristic Seminvariant
$Q_1 = x^2 + xy + y^2$	$a = b = 1,\ J = 1$	$\pi = abJ \equiv abc$
$Q_2 = x^2 + xy$	$a = b = 1,\ J = 0$	$ab(J+1) = \pi + ab$
$Q_3 = y^2$	$a = b = 0,\ J = 1$	$(a+1)(b+1)J = \pi + J$
$Q_4 \equiv 0$	$a = b = 0,\ J = 0$	$(a+1)(b+1)(J+1) = I$
$Q_5 = x^2$	$a = 1,\ b = 0$	$a(b+1)$
$Q_6 = xy$	$a = 0,\ b = 1$	$(a+1)b$

By definition, the characteristic seminvariant of a class c_i is one having the value unity for each form of the class c_i and the value zero for each form in the remaining classes. In the present case, the characteristic seminvariant of class c_i was found by inspection from the values of the seminvariants in the second column which specify that class,—it is a product in which any factor is one of those seminvariants or the sum of it and unity, according as the seminvariant is 1 or 0 for the class.

To derive the invariants of Q from its characteristic seminvariants, we separate the forms Q into classes C_i of equivalent forms under the group G of all binary linear transformations modulo 2. Now G is generated by $(x + y, y)$ and (y, x). Since classes $c_1, \cdots, c_4$ are each composed of a single form, and since the forms Q_1 and Q_4 are unaltered by (y, x), while Q_2 is changed into a form of c_6, and Q_3 into Q_5, we see that the classes under G are

$$C_1 = c_1, \qquad C_2 = c_2 + c_6, \qquad C_3 = c_3 + c_5, \qquad C_4 = c_4.$$

Hence, for $i = 1$ or 4, the characteristic invariant I_i for class C_i is the characteristic seminvariant for c_i. But I_2 is the sum of the characteristic seminvariants for c_2 and c_6, and I_3 the sum of those for c_3 and c_5. Thus the characteristic invariants are

$$I_1 = \pi, \qquad I_2 = \pi + b, \qquad I_3 = \pi + J + ab + a = I + b + 1, \qquad I_4 = I.$$

In § 2 it was shown that b, q, k form a fundamental system of formal invariants modulo 2 of Q. Taking the coefficients to be integers modulo 2, we obtain the modular invariants b, $q \equiv \delta$, $k \equiv b\delta$, where

$$b = I_1 + I_2, \qquad \delta = ac + (b+1)(a+c) = I_1 + I_3.$$

Conversely, from b and δ we get

$$\pi = b\delta, \qquad I = (b+1)(\delta+1).$$

This new method of deriving all modular invariants from the seminvariants is more direct and simpler than the method employed in the *Madison Colloquium*, pages 28–32.