PROOF OF THE FINITENESS OF THE MODULAR COVARIANTS OF A SYSTEM OF BINARY FORMS AND COGREDIENT POINTS[*]

BY

FORBES BAGLEY WILEY

Introduction

1. **Relation to the literature.** The question of the finiteness of the modular covariants of a system of forms and cogredient points is one that arises naturally at this time in view of the fact that the modular covariants of a system of forms and no cogredient points have been shown recently to be finite,[†] where the term finite has the customary meaning attached to it in covariant theory, and still more recently a fundamental system of modular covariants for two cogredient binary points and no forms has been found.[‡]

The present paper is limited to the binary case, although the writer has made considerable advance in the case of ternary forms and one cogredient point.

2. **Definitions.** Let $f_1, \cdots, f_l$ be any system of forms (homogeneous polynomials) in the arbitrary variables x_{01}, x_{02} with undetermined integral coefficients taken modulo p, where p is any prime. Let $c_1, c_2, \cdots$ denote the coefficients arranged in any order. Under the transformation

$$T_0: \qquad x_{0i} = \sum_{j=1}^{2} t_{ij}\, x'_{0j} \pmod{p} \qquad (i = 1, 2)$$

with integral coefficients, let f_i become the form f'_i and let $c'_1, c'_2, \cdots$ denote the coefficients of $f'_1, \cdots, f'_l$ corresponding in position to $c_1, c_2, \cdots$, respectively. Let (x_{k1}, x_{k2}), $k = 1, \cdots, n$, be transformed cogrediently with x_{01}, x_{02}, that is by the transformation

$$T_k: \qquad x_{ki} = \sum_{j=1}^{2} t_{ij}\, x'_{kj} \pmod{p} \quad (i = 1, 2;\ k = 1, \cdots, n).$$

A rational integral function

$$K(c_1, c_2, \cdots;\ x_{01}, x_{11}, \cdots, x_{n1};\ x_{02}, x_{12}, \cdots, x_{n2})$$

[*] Presented to the Society (Providence), September 8, 1914.

[†] Dickson, these Transactions, vol. 14 (1913), pp. 299–305.

[‡] Krathwohl, American Journal of Mathematics, October, 1914.

with integral coefficients taken modulo p is called a modular covariant of the points (x_{k1}, x_{k2}), $k = 1, \cdots, n$, and the forms $f_1, \cdots, f_l$ if, for every transformation T_k $(k = 0, 1, \cdots, n)$,

$$K(c_1', c_2', \cdots; x_{01}', x_{11}', \cdots, x_{n1}'; x_{02}', x_{12}', \cdots, x_{n2}')$$
$$\equiv |t_{ij}|^{\mu} K(c_1, c_2, \cdots; x_{01}, x_{11}, \cdots, x_{n1}; x_{02}, x_{12}, \cdots, x_{n2}) \pmod{p}$$

holds identically in $c_1, c_2, \cdots; x_{01}', \cdots, x_{n1}'; x_{02}', \cdots, x_{n2}'$ after $x_{01}, \cdots, x_{n1}, x_{02}, \cdots, x_{n2}$ are eliminated by means of the congruences T_k $(k = 0, \cdots, n)$ and $c_1', c_2', \cdots$ are replaced by their expressions in terms of $c_1, c_2, \cdots$. The exponent μ is called the index of K.

In this paper we establish the

THEOREM. *The set of all modular covariants of any system of forms in x_{01}, x_{02} and the cogredient points (x_{k1}, x_{k2}), $k = 1, \cdots, n$, is finite in the sense that they are all rational integral functions, with integral coefficients taken modulo p, of a finite number of covariants of the set.*

Professor Dickson has obtained the special case of this theorem where there is a system of forms but no cogredient points.* We extend his method of proof to secure the proof of the theorem as above stated.

3. **Method of proof.** In bare outline the proof of the theorem consists of two parts. First it is shown that for any modular covariant K_1 of the forms and the points there exists a modular covariant K_1' that has the same leader (defined in § 6) and the same index as K_1 has and that is a polynomial in covariants from a definite finite set S of modular covariants of the forms and the points. By taking the difference of K_1 and K_1' we obtain a new covariant K_2 for which we can build up K_2' by the same method as that used on K_1 and by the use of the same set S. The second part of the proof consists in showing that the repetition of this process a finite number of times on any given covariant K_1 leads to a covariant K_m where K_m is such that $K_m - K_m' = 0$. Thus it follows that $K_1 = \Sigma_{i=1}^{i=m} K_i'$ and therefore is expressible as a polynomial in covariants from the set S.

To carry out this method in detail we establish in § 4 a lemma which is an extension of the lemma† used by Professor Dickson in the case he considered. In § 5 we prove the theorem for n not greater than 1 and in § 6 we give the proof where n is any finite positive integer, including the value $n = 0$.

* Dickson, loc. cit. Professor Dickson secures his theorem for forms in any finite number of variables.

† Dickson, American Journal of Mathematics, vol. 35 (1913), pp. 414–415.

Finiteness of the Modular Covariants

4. **Lemma.** *Any set S of functions of the type*

$$F = x_0^{e_0} x_1^{e_1} \cdots x_n^{e_n} \qquad (e\text{'s integers} \geqq 0;\ e_0 \geqq e_1, \cdots, e_0 \geqq e_n) \tag{1}$$

contains a finite number of functions $F_1, \cdots, F_k$ such that each function F of the set S can be expressed as a product $F_i f$ where f is of the form (1), *with the same property of the exponents, but is not necessarily in the set S.*

For the moment designate the possible relations

$$e_i - e_{i+1} \geqq 0, \qquad e_i - e_{i+1} < 0 \qquad (i = 1, \cdots, n)$$

between the exponents of F as decreases and increases, respectively. Since the e's of F occur in a definite order, indicated in (1), the order in which the increases and decreases of a given F occur is unique. The functions F of S can be classified into sets S_j $(j = 1, \cdots, t;\ t \leqq n!)$ such that functions from no two sets will have their increases and decreases occurring in the same order, while the increases and decreases of functions in the same set occur in the same order.

Let S_k be one of the sets S_j, say the one in which there are no increases. It is evident that the functions of any set S_j can be written in the form of the functions of S_k by a substitution which amounts to a rearrangement of the x's. Write the functions $F^{(k)}$ of S_k in the form

$$\prod_{j=0}^{n} \left[\prod_{i=0}^{j} x_i \right]^{e_j - e_{j+1}} \qquad (e_{n+1} = 0).$$

Make the substitutions

$$\prod_{i=0}^{j} x_i = y_j, \qquad e_j - e_{j+1} = \epsilon_j \qquad (j = 1, \cdots, n) \tag{2}$$

on the variables and the exponents of $F^{(k)}$, respectively. We thus have a set S_k of functions

$$\phi^{(k)} = \prod_{j=0}^{n} y_j^{\epsilon_j} \qquad (\epsilon\text{'s integers} \geqq 0).$$

There exists* a finite number of functions $\phi_i^{(k)}$ $(i = 1, \cdots, h)$ belonging to the set S_k such that any function $\phi^{(k)}$ of the set S_k may be written

$$\phi^{(k)} = \phi_i^{(k)} f,$$

where

$$f = \prod_{j=0}^{n} y_j^{a_j} \qquad (a\text{'s integers} \geqq 0) \tag{3}$$

and i has some one of the values $1, \cdots, h$. Transforming (3) by the inverse

* See reference last cited; also Gordan, Journal de Mathématiques, ser. 5, vol. 6 (1900), pp. 141–149.

of (2_1), we have

$$f = \prod_{j=0}^{n} x_j^{\sum_{i=j}^{n} a_i} .$$

The lemma thus holds for the set S_k and similarly for each one of the t sets S_j; hence it holds for the set S.

5. **One cogredient point.** We make use of the known* rational integral modular covariants

$$L_i = x_{i1}^p x_{i2} - x_{i1} x_{i2}^p \qquad (i = 0, 1),$$

$$Q_i = \frac{x_{i1}^{p^2} x_{i2} - x_{i1} x_{i1}^{p^2}}{L_i} = x_{i1}^{p^2-p} + x_{i2}(\ ) \qquad (i = 0, 1),$$

$$M = x_{01} x_{12} - x_{02} x_{11} .$$

The covariants L_i and M have the index -1, while the Q_i are absolute.†

As any covariant is the sum of covariants that are homogeneous in each pair of variables separately, it is sufficient for us to consider covariants of the type $K(x_{01}, x_{02}, x_{11}, x_{12})$ of total degree ω_0 in x_{01}, x_{02} and of total degree ω_1 in x_{11}, x_{12}. If one of the ω's is zero, we have the case which Professor Dickson considered.

We shall call such a covariant K a regular covariant of the forms and the cogredient point if it has neither of the x_{i2} $(i = 1, 2)$ as a factor, while we shall call it irregular if it has either one of these variables as a factor or both as factors. Any irregular covariant is the product of $L_0^s L_1^t$ $(s, t = 0, 1, \cdots;$ s and t not both zero) by a regular covariant, since‡ any covariant that has the factor x_{i2} has the factor L_i. We need, therefore, to consider only regular covariants.

Let K be such a covariant and let it be of total degree ω_i in the two variables x_{i1}, x_{i2} $(i = 0, 1)$. We write K in the form

$$K = x_{i1}^{\omega_i} \sum_{j=0}^{\omega_k} S_j x_{k1}^{\omega_k - j} x_{k2}^{j} + x_{i2}(\ ) \qquad (\omega_i \geqq \omega_k;\ i,\ k = 0,\ 1;\ i \neq k), \tag{4}$$

where at least one S_j is not zero. We rewrite (4) in the notation

$$K = S x_{i1}^{A} x_{k1}^{B} x_{k2}^{C} + \cdots \qquad (S = S_0,\ A = \omega_i,\ B + C = \omega_k), \tag{5}$$

where B is the highest exponent which x_{k1} carries in a term containing x_{i1}^A. Denote the set of all regular covariants (5) with a fixed leader S and

$$A \equiv a, \qquad B \equiv b, \qquad C \equiv c \qquad (\text{mod } P) \qquad (P = p^2 - p),$$

* Dickson, *The Madison Colloquium Lectures on Mathematics*, pp. 35, 37. M is an algebraic covariant.

† Of index $\mu = 0$.

‡ Dickson, *The Madison Colloquium Lectures*, p. 35.

where each of the numbers a, b, c is at least zero and is less than P, by $[S, a, b, c]_i$. The number of such sets is finite since a, b, c are limited in value and the number of seminvariant leaders S is finite. These leaders are finite because each S is a polynomial in the coefficients c_i of the forms and thus all exponents can be reduced to $p - 1$ or less by use of Fermat's theorem. All covariants belonging to the same set S have the same index μ. By means of the Lemma (§ 4), we may select from the set $[S, a, b, c]$ a finite number t of covariants

$$K_h = Sx_{i1}^{A_h} x_{k1}^{B_h} x_{k2}^{C_h} + \cdots + x_{i2}(\;) \qquad (h = 1, \cdots, t), \tag{6}$$

such that for any covariant (5) of the set $[S, a, b, c]$ it is true that

$$A \geqq A_h, \qquad B \geqq B_h, \qquad C \geqq C_h, \qquad A - A_h \geqq C - C_h$$

$$(\text{for some value} \leqq t \text{ of } h).$$

But A and A_h (and likewise for B and B_h, C and C_h) are congruent to a modulo P; thus any covariant of the set $[S, a, b, c]$ has the form

$$K = Sx_{i1}{}^{A_h + uP} x_{k1}{}^{B_h + vP} x_{k2}{}^{C_h + wP} + \cdots \qquad (u \geqq w),$$

where u, v, w are positive integers or zero and h is some one of the integers $1, \cdots, t$.

From the absolute covariants Q_i, Q_k, M^P, and the covariant K_h, we construct a covariant of the same index as K and having the same initial term as K, and see that the difference

$$K' = K - K_h Q_i^{u-w} Q_k^v M^{wP} + \cdots$$

will be a covariant either irregular or with the leader

$$S' x_{i1}^{A} x_{k1}^{B'} x_{k2}^{C'} \qquad (A \geqq B' + C',\ B' < B,\ C' > C).$$

If K' is an irregular covariant, take out the factors L_i that ocour and call the quotient K''. If K' is regular, call it K''. Hence

$$K = \psi_1(L_1, L_2, Q_1, Q_2, M, K_h, K''),$$

where ψ_1 is a polynomial in its arguments.

Arrange K'' in the form (6) and repeat for it the reduction process used on the regular covariant K. Whenever the exponent B in one of the regular covariants, say $K^{(e)}$, is zero, the next step in the process gives an irregular covariant with the factor x_{i2}, thus allowing a reduction of the degree in x_{i1} and x_{i2} by the removal of the factor L_i. If we let K_h $(h = 1, \cdots, \tau)$ serve for all sets $[S, a, b, c]$ as K_h $(h = 1, \cdots, t)$ served for the particular one, we see that every covariant K may be expressed as

$$K = \psi_m(K_1, \cdots, K_\tau, L_1, L_2, Q_1, Q_2, M),$$

where ψ_m is a polynomial in its arguments and is linear in the $K_1, \cdots, K_\tau$.

6. **Case of n cogredient points.** We use the L_i and the Q_i of § 5 with $i = 1, \cdots, n$. In addition to these we use the known modular covariants

$$M_{ik,n} = x_{i1}x_{k2}^{p^n} - x_{i2}x_{k1}^{p^n} \quad (i, k = 0, \cdots, n;\ i \neq k).$$

As in § 5 so here also we need consider only those covariants of the forms $f_1, \cdots, f_l$ and the cogredient points (x_{k1}, x_{k2}), $k = 1, \cdots, n$, which are homogeneous in each pair of variables separately.

We shall call such a covariant a regular covariant if it has none of the x_{i2} $(i = 0, \cdots, n)$ as factors, while we shall call it irregular if it has one or more such factors. Since any irregular covariant is the product of

$$\prod_{i=0}^{n} L_i^{s_i} \qquad (s_i = 0, 1, \cdots;\ \text{at least one } s_i \neq 0)$$

and a regular covariant, we need to consider only regular covariants.

Let K be such a covariant and let ω_i be the order of K in x_{i1}, x_{i2}. Each x_{i1} will occur in at least one term of K with an exponent equal to the order ω_i. There exists some ω_i, say ω_0 for convenience in notation,* such that $\omega_0 \geqq \omega_j$ $(j = 1, \cdots, n)$. Write K with those terms leading that contain the factor $x_0^{\omega_0}$, the order of these terms being such that the sums of the exponents of the factors x_{i1} in them occur in the order of the decreasing natural numbers. The order among themselves of those terms for which such sums are equal is arbitrary. Denote the first term of K so written as the leader. By the help of zero exponents where necessary, write the leader of K so that every variable except x_{02} appears in it notationally as a factor. Arrange these factors in the ascending order of their subscripts so that we have

$$K = S\prod_{i=0}^{n} x_{i1}^{A_i}\prod_{j=1}^{n} x_{j2}^{B_j} + \cdots \quad (A_0 = \omega_0,\ A_i + B_i = \omega_i,\ \omega_0 \geqq \omega_i). \tag{7}$$

Denote by

$$[S, a_0, a_1, \cdots, a_n; b_1, b_2, \cdots, b_n] \tag{8}$$

the set of all covariants (7) with a given seminvariant leader S and with

$$A_i \equiv a_i, \qquad B_i \equiv b_i \pmod X; \qquad X = p^{n+1}(p-1),$$

where each a_i and each b_i is at least zero and less than X. The number of sets (8) is finite. All covariants (7) belonging to the same set (8) have the same index μ. By the Lemma (§ 4), there exists a finite number of covariants

$$K_h = S\prod_{i=0}^{n} x_{i1}^{A_{ih}}\prod_{j=1}^{n} x_{j2}^{B_{jh}} + \cdots \qquad (h = 1, \cdots, t) \tag{9}$$

belonging to the set (8) such that the leader of any covariant (7) that belongs

* It is only slightly more cumbersome to carry the argument through for ω_g.

to set (8) can be expressed as the product of the leader of some covariant of (9) by f, where f is of the form (7), with the same property of the exponents, but has no factor S. Thus we may write

$$K = S \prod_{i=0}^{n} x_{i1}{}^{A_{ih}+q_i X} \prod_{j=1}^{n} x_{j2}{}^{B_{jh}+q'_j X} + \cdots . \tag{10}$$

Therefore

$$f = \left(\prod_{i=0}^{n} x_{i1}^{q_i} \prod_{j=1}^{n} x_{j2}^{q'_j} \right)^X$$
$$(q_0 \geqq q_1, \cdots, q_0 \geqq q_n; \; q_0 \geqq q_1', \cdots, q_0 \geqq q_n').$$

By the aid of zero exponents where necessary, let each variable except x_{02} appear notationally as a factor in f. Arrange the factors x_{i2} of f in the order of decreasing exponents. The order among themselves of those factors x_{i2} whose exponents are equal is arbitrary. Arrange the x_{i1} factors in the same order as their corresponding x_{i2} 's. Write f thus arranged in the notation

$$f = \left(x_{01}^{q_0} \prod_{i=1}^{n} x_{h_i 1}^{q_{h_i}} \prod_{j=1}^{n} x_{h_j 2}^{q'_{h_j}} \right)^X .$$

This may be written

$$f = \Big[x_{01}^{q_0 - q'_{h_1}} \prod_{i=1}^{n} x_{h_i 1}^{q_{h_i}} (x_{01} \, x_{h_1 2})^{q'_{h_1} - q'_{h_2}} (x_{01} \, x_{h_1 2} \, x_{h_2 2})^{q'_{h_2} - q'_{h_3}} \cdots (x_{01} \cdots x_{h_{n-1} 2})^{q_{h_{n-1}} - q'_{h_n}} (x_{01} \cdots x_{h_n 2})^{q'_{h_n}} \Big]^X . \tag{11}$$

We now build up the absolute covariants

$$P_r = Q_0^{p^{n-r}} \prod_{k=h_1}^{h_r} M_{0k,\,n}^{p^2-p} + \cdots \qquad (1 \gtreqless r \gtreqless n),$$

which we may write in the form

$$P_r = \left[x_{01} \prod_{k=h_1}^{h_r} x_{h_k 2} \right]^X + \cdots .$$

From the absolute covariants Q_0, Q_{h_i}, P_r, and the covariant K_h, which is one of the covariants (9), we construct a covariant of the same index as K and having the same initial term as K so that it follows that the difference

$$K' = K - K_h \, Q_0^{(q_0 - q'_1)p^n} \prod_{i=1}^{n} Q_{h_i}^{q_{h_i} - p^n} \prod_{r=1}^{n} P_r^{q'_{h_j} - q'_{h_{j+1}}} \qquad (q'_{h_{n+1}} = 0)$$

will be a covariant either irregular or with a leader that can be written in the form (10). If K' is irregular, take out the factors L_i that occur and call the quotient K''. If K' is regular, call it K''. Thus we have

$$K = \psi (L_1, \cdots, L_n, Q_1, \cdots, Q_n, K_h, P_1, \cdots, P_l)$$

where h is one of the values $1, \cdots, t$ and ψ is a polynomial in its arguments. Arrange K'' in the form (10) and subject it to the reduction process used on the regular covariant K, thus obtaining a regular covariant $K^{(\mathrm{IV})}$. After a finite number of repetitions of this process, we obtain either an irregular covariant or a regular one, say $K^{(q)}$, for which the sum of the exponents of the factors x_{i1} $(i = 1, \cdots, n)$ in its leader is less than the like sum for the leader of K. After repeating the process a finite number of times from this point, we obtain either an irregular covariant or one, say $K^{(l)}$, for which the sum of the exponents of the x_{i1} $(i = 1, \cdots, n)$ factors is zero. The next repetition of the reduction process reduces the exponent of x_{01} and gives an irregular covariant with the factor L_0 which, when removed, still further reduces the degree of x_{01}.

If we let K_h $(h = 1, \cdots, \tau)$ serve for all sets (8) as K_h $(h = 1, \cdots, t)$ served for one of them, we see that any covariant of the binary forms $f_1, \cdots, f_l$ and the n cogredient points is a polynomial in $K_1, \cdots, K_\tau; L_1, \cdots, L_n; Q_1, \cdots, Q_n; P_1, \cdots, P_n$, linear in $K_1, \cdots, K_\tau$.

The covariants P_r are polynomials in Q_0 and $M_{0k,\, n}$. It is of interest to note that by means of the recursion formula

$$M_{0k,\, n} = Q_k^{p^{n-2}} M_{0k,\, n-1} - L_k^{(p-1)p^{n-2}} M_{0k,\, n-2} \qquad (n > 1),$$

we are able to express any $M_{0k,\, n}$ as a rational integral function of $M_{0k,\, 1}$, $M_{0k,\, 0}$, Q_k, and L_k, linear in the $M_{0k,\, 1}$, $M_{0k,\, 0}$. It follows that any covariant K of the binary forms and the n points may be written as a polynomial in $K_1, \cdots, K_\tau; L_1, \cdots, L_n; Q_1, \cdots, Q_n; M_{01,\, 1}, \cdots, M_{0n,\, 1}; M_{01,\, 0}, \cdots, M_{0n,\, 0}$, linear in the $K_1, \cdots, K_\tau$.