PSEUDO-COVARIANTS OF AN n-IC IN m VARIABLES IN A GALOIS FIELD THAT CONSIST OF TERMS OF THIS n-IC*

BY A. D. CAMPBELL

Let us consider the n-ic in m variables

$$(1) \quad f(x_1, x_2, \cdots, x_m) = \sum a_{i,j,\ldots,k} x_1{}^i x_2{}^j \cdots x_m{}^k = 0,$$

where $i, j, \cdots, k = 0, 1, 2, \cdots, n$, and $i+j+ \cdots +k=n$; also where the coefficients and variables represent numbers in a Galois field of order p^n. If we subject (1) to the transformation

$$(2) \qquad\qquad \rho x_\lambda = \sum \alpha_{\lambda\mu} x_\mu' ,$$

where $\lambda, \mu = 1, 2, \cdots, m$, and the coefficients and variables represent numbers in the same Galois field, we obtain

$$
\begin{aligned}
(3) \quad f'(x_1', x_2', \cdots, x_m') &= \sum a_{i,j,\ldots,k}(\alpha_{11}x_1' + \cdots + \alpha_{1m}x_m')^i \\
&\quad \cdot (\alpha_{21}x_1' + \cdots + \alpha_{2m}x_m')^j \cdots (\alpha_{m1}x_1' + \cdots + \alpha_{mm}x_m')^k \\
&= \sum a'_{i,j,\ldots,k} x_1'{}^i x_2'{}^j \cdots x_m'{}^k = 0.
\end{aligned}
$$

We note from (3) that the only terms in (1) that can furnish terms in the primed variables whose factors all have exponents less than p (the prime modulus of this Galois field) are those terms in (1) whose factors all have exponents less than p. Therefore if such terms are present in (1), the n-ic has what we shall call a pseudo-covariant consisting of the above-mentioned terms of (1), that has the form

$$(4) \qquad\qquad \sum a_{r,s,\ldots,t} x_1{}^r x_2{}^s \cdots x_m{}^t ,$$

where $r+s+ \cdots +t=n$ and $r<p$, $s<p$, $\cdots$, $t<p$. The set of terms (4) contribute also other types of primed terms to (3) after we use (2) on (1), but no other terms in (1) except the set (4) furnish (3) with primed terms of the same type as the unprimed terms of (4).

If (1) has no terms of the form (4), we note that only the terms in (1) having each just one factor of the form $x_i{}^u$, where

---

* Presented to the Society, February 25, 1933.

$p \leqq u < p^2$, can contribute to (3) primed terms of this same form. Therefore, if (1) has no pseudo-covariant (4), it has the pseudo-covariant

$$(5) \qquad \sum a_{u,s,\cdots,t} x_1{}^u x_2{}^s \cdots x_m{}^t,$$

where $u+s+\cdots+t=n$ and just one of the exponents u, s, $\cdots$, t in each term lies between p and p^2, while the other exponents are less than p.

Next if (1) has no terms of the form (5), then the n-ic has the pseudo-covariant

$$(6) \qquad \sum a_{u,v,\cdots,t} x_1{}^u x_2{}^v \cdots x_m{}^t,$$

where $u+v+\cdots+t=n$ and just two of the exponents u, v, $\cdots$, t in each term lie between p and p^2, while the other exponents are less than p.

If (1) has no terms each with just two exponents between p and p^2 and their other exponents less than p, we find a pseudo-covariant whose terms have each just three exponents lying between p and p^2 while their other exponents are less than p.

If (1) has no terms with all their exponents less than p^2, the n-ic has a pseudo-covariant consisting of all the terms in (1) that have each just one factor whose exponent lies between p^2 and p^3 while the other exponents are less than p^2. If no such pseudo-covariant exists then the n-ic has a pseudo-covariant consisting of all the terms in (1) that have each just two factors whose exponents lie between p^2 and p^3 while their other exponents are less than p^2. Similarly we can generalize to the cases of pseudo-covariants consisting of all the terms of (1) having each a certain number of exponents lying between p^3 and p^4 but their other exponents less than p^3, between p^4 and p^5, and so forth.

Let us consider next the relations between the coefficients of (3) and the coefficients of (1), namely,

$$(7) \qquad \sigma a'_{i,j,\cdots,k} = \sum \beta_{\lambda,\mu,\cdots,\nu} a_{\lambda,\mu,\cdots,\nu},$$

where $i, j, \cdots, k$ and $\lambda, \mu, \cdots, \nu$ have the values $0, 1, 2, \cdots, n$. This is the transformation between the coefficients of (1) and (3) that is caused by the transformation (2) upon the variables x_i. Capelli has proved (*Lezioni*, p. 202) that any linear transformation on m variables can be obtained by the successive ap-

plication of a finite number of linear transformations of the following types:

(8)
$$T^{a} : x_1 = x_1', \cdots, x_{l-1} = x_{l-1}', x_l = ax_l',$$
$$x_{l+1} = x_{l+1}', \cdots, x_m = x_m',$$

and

$$T_{lk} : x_1 = x_1', \cdots, x_{l-1} = x_{l-1}', x_l = x_l' + x_k',$$
$$x_{l+1} = x_{l+1}', \cdots, x_m = x_m',$$

or by T_1^{a}, T_{12} supplemented by transformations of the type

$$x_1 = x_j', \; x_j = x_1', \; x_k = x_k', \quad (k \neq 1, \; k \neq j).$$

We note that a must equal the determinant of the transformation (2) that is analyzed into a product of transformations of the form (8). If we subject (1) to T_1^{a}, we see that the determinant of (7) is a power of the determinant of (2).

To find what power of a the determinant a' of (7) is we arrange (1) in ascending powers of x_1. We note that the number of terms in a homogeneous form of degree k in l variables is

(9)
$$_kS_l = \frac{(k + 1)(k + 2)(k + 3) \cdots (k + l - 1)}{(l - 1)!}.$$

We subject (1) to T_1^{a}. We note that the coefficient $a'_{i,j,\ldots,k}$ in (7) resulting from T_1^{a} has the value $a^i a_{i,j,\ldots,k}$. There are $_{n-1}S_{m-1}$ similar coefficients in (3) for any given i. From this we see that the determinant of (7) is

(10)
$$a' = a^{n^p m},$$

where

$$_np_m = 0 \; _nS_{m-1} + 1 \; _{n-1}S_{m-1} + 2 \; _{n-2}S_{m-1} + \cdots + n \; _0S_{m-1}.$$

Next we see that the coefficients of each of the several pseudo-covariants are transformed by a transformation whose determinant a'' is also a power of the determinant a of (2). To find what power a'' is of a, we suppose the highest exponent of any factor in any term to be s. We arrange the pseudo-covariant in descending powers of x_1. We subject (1) to T_1^{a}. The coefficient $a'_{s,j,\ldots,k}$ has the value $a^s a_{s,j,\ldots,k}$. We count the number of partitions of $n - s$ into sums of numbers less than or equal to s. If the terms of the pseudo-covariant have each just one factor with exponent equal to s (where $p \leq s < p^2$, say) we take only

the partitions of $n-s$ into the sums of numbers less than s. A similar remark applies to each of the other types of pseudo-covariants.

We treat the case with $p \leq s < p^2$ and with only one such exponent s per term. The generalization to the other cases is evident. To each of these partitions we affix the number of permutations of $m-1$ things taken l at a time, where l is the number of terms in the partition, allowing for repetitions. The sum of all these affixed numbers we label Π_1. By this means we count all the terms in the pseudo-covariant each of which has $x_1{}^s$ as a factor.

Next we consider the coefficients $a'_{s-1,j,\ldots,k}$. We take the number of partitions of $n-s-(s-1)$ into sums of numbers less than s. We add up all the permutations of $m-2$ things taken l at a time associated with these partitions as above and we call this sum Π_2. We multiply Π_2 by $m-1$ because the exponent s may be placed on any one of the variables $x_2, x_3, \cdots, x_m$. Next we consider the coefficients $a'_{s-2,j,\ldots,k}$ and the partitions of $n-s-(s-2)$ with the associated number Π_3. We must multiply Π_3 by $m-1$.

From the above discussion we see that the transformation of the coefficients of the pseudo-covariant has the determinant

$$(11) \qquad\qquad a'' = a^{\Pi},$$

where

$$\Pi = \Pi_1 s + (m-1)[\Pi_2(s-1) + \Pi_3(s-2) + \cdots + \Pi_s].$$

An interesting special case of the above is found when $p = 2$ and the n-ic (1) has terms consisting entirely of linear factors. This can happen only when $m \geq n$. In this case the above mentioned determinant is a so-called compound determinant of the determinant of (2). Compare Metzler-Muir, *Determinants*, page 178. In this case we have $a'' = a^{m-1}C_{n-1}$, where $_{m-1}C_{n-1}$ is the number of combinations of $m-1$ things taken $n-1$ at a time. If $m = n$ we have $a'' = a$.

The next question that arises is as to the form of the transformation (7). We note that the general case is given in a previous paper.* We give now a method of obtaining (7) and also of

* *Note on linear transformations of n-ics in m variables*, this Bulletin, vol. 35 (1929), pp. 691–694.

obtaining the transformations of the coefficients of the several pseudo-covariants. We note the multinomial expansion

$$(12) \quad (a + b + \cdots + k)^n = \sum \frac{n!}{\alpha! \beta! \cdots \kappa!} a^\alpha b^\beta \cdots k^\kappa,$$

where $\alpha + \beta + \cdots + \kappa = n$.

We shall illustrate the method by a particular case. The generalization will then be evident. Suppose we have a term $a_{23} x_1^2 x_2^3$ of a quintic in three variables and we wish to find the coefficient a'_{221} of the term in $x_1'^2 x_2'^2 x_3'$ that (2) yields us from this term. We put

$$y_1 = \alpha_{11} x_1', \quad y_2 = \alpha_{12} x_2', \quad \cdots, \quad z_1 = \alpha_{21} x_1', \quad \cdots, \quad z_3 = \alpha_{23} x_3',$$

and we have

$$a_{23}(y_1 + y_2 + y_3)^2 (z_1 + z_2 + z_3)^3$$

$$= a_{23} \left(\sum \frac{2!}{\alpha_1! \beta_1! \gamma_1!} y_1^{\alpha_1} y_2^{\beta_1} y_3^{\gamma_1} \right) \left(\sum \frac{3!}{\alpha_2! \beta_2! \gamma_2!} z_1^{\alpha_2} z_2^{\beta_2} z_3^{\gamma_2} \right).$$

To obtain a'_{221} we multiply a_{23} by the sum s of all the products of powers of $\alpha_{11}, \alpha_{12}, \cdots$ obtained from the above parentheses when we set

$$\alpha_1 + \alpha_2 = 2, \qquad \beta_1 + \beta_2 = 2, \qquad \gamma_1 + \gamma_2 = 1,$$

$$\alpha_1 + \beta_1 + \gamma_1 = 2, \qquad \alpha_2 + \beta_2 + \gamma_2 = 3.$$

SYRACUSE UNIVERSITY