JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

OLIVE C. HAZLETT

On formal modular invariants

Journal de mathématiques pures et appliquées 9^e série, tome 9 (1930), p. 327-332.
<http://www.numdam.org/item?id=JMPA_1930_9_9__327_0>

On formal modular invariants;

By Olive C. HAZLETT.

1. *Summary and relation to the literature.* — This note gives an extension of the principal results containd in a paper (1) by W. L.-G. Williams in this journal. In Part I, he proves that

$$a_0 \prod_{t=0}^{p-1} \left[a_0 t^q + \binom{q}{1} a_1 t^{q-1} + \ldots + a_q \right]$$

and

$$\mathrm{K} = a_0^{p-1} + \sum_{t=0}^{p-1} \left[a_0 t^q + \binom{q}{1} a_1 t^{q-1} + \ldots + a_q \right]^{\lambda(p-1)} \qquad (\lambda = 1, 2, \ldots),$$

are formal modular invariants, modulo p, of the binary $q - ic$ form

$$a_0 x^q + \binom{q}{1} a_1 x^{q-1} y + \ldots + a_q y^q,$$

where p and q are such that none of the binomial coefficients $\binom{q}{k}$ is divisible by p. He also proved that(if p is odd and λ is an integer such that $\lambda(p-1)/q$ is integer, then

$$\mathrm{L} = a_0^{\lambda(p-1)/q} + \sum_{t=0}^{p-1} \left[a_0 t^q + \binom{q}{1} a_1 + \ldots + a_q \right]^{\lambda(p-1)/q},$$

is a formal modular invariant of the above $q - ic$. These he calls, in

(1) *On the formal modular invariants of binary forms* (*Journal de Mathématiques*, 9e série, t. 4, 1925, p. 169-192).

order, Theorems I, II and III. The first two are due to Hurwitz (1) and the third is a generalization of the second. In part III, he proves four theorems (2) each of wich asserts that, if

$$f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3,$$

then certain special polynomials in the values of $f(x, y)$ when x, y are marks of the Galois field, GF[p], of order p — where p is a prime — are formal modular invariants of $f(x, y)$.

These theorems are not only very special in that they are stated for special invariants, but they are special in another sense, since they are stated and proved only for the cases where no one of the binomial coefficients is congruent to zero modulo p. This last is more than a slight restriction. For, if the study of formal modular invariants ever approach completion, we shall want to study the invariants of the quadratic, cubic, quartic, etc. modulo 2 and similarly modulo p where p is any fixed prime. But, when $p = 2$, we can not use binomial coefficients for the binary $q - ic$ when $q = 2, 4, 5, 6, 8, 9, 10$, etc., when $p = 3$, we can not use binomial coefficients when $q = 3, 4, 6, 7, 9, 10$, etc.; nor if $p = 5$, when $q = 5, 6, 7, 8, 10$, etc.; and similarly larger primes.

In none of the cases just indicated, do the proofs in Mr. Williams' paper hold. Hence it would seem desirable to have proofs that hold without exception. The present note not only gives such proofs, but also generalizes the invariants to which the theorems apply. As will be seen, the proofs are exceedingly simple and use no technical knowledge of the subject.

2. *Definitions.* — Consider the polynomial

$$f(x_1, x_2) = a_0x_1^q + a_1x_2^{q-1}x_2 + \ldots + a_qx_2^q, \tag{1}$$

in wich the coefficients a_0, a_1, ... are indéterminates and subject the

(1) *Höhere Congruenzen* (*Archiv der Math. u. Physik*, 3e série, vol. 5, 1903, p. 17-27).

(2) Each of the first two theorems also asserts that no invariant whose leading term is a power of d is essentially different from those given by the formula in the theorem.

variables to any transformation

$$(2)\qquad \begin{cases} x_1 = \xi_1 x'_1 + \eta_1 x'_2, \\ x_2 = \xi_2 x'_1 + \eta_2 x'_2, \end{cases}$$

in which the coefficients ξ_1, ξ_2, η_1, η_2 are integers reduced modulo p, a prime, subject to the restriction that the determinant of the transformation is not congruent to zero, modulo p. Any polynomial in the x's which is unaltered in form, modulo p, under the total group of all such transformations is called a *formal modular invariant* of (1), modulo p. For simplicity, we shall use the fact that this group is generated by the transformations

$$(3)\qquad \begin{cases} x_1 = x'_1 + x'_2, \\ x_2 = \quad x'_2, \end{cases}$$

and

$$(4)\qquad \begin{cases} x_1 = \quad x'_2, \\ x'_2 = -x'_1, \end{cases}$$

of determinant unity and the transformation

$$(5)\qquad \begin{cases} x_1 = \quad x'_1 \\ x_2 = \rho x'_2 \end{cases} \qquad (\rho \text{ a primitive root of the field}).$$

Similary we hawe the notion of a formal modular invariant of (1) with respect to the Galois field, GF$[p^n]$, of order p^n.

3. *The two theorems.* — First we prove a generalization of Prof. Williams theorems of his Part I. Since the transformation (3) permutes the pairs $(t, 1)(t = 0, 1, \ldots, p-1)$ modulo p, any symmetric function of all the values of $f(x_1, x_2)$ as (x_1, x_2) ranges over the above pairs and the pair $(0, 1)$ is invariant modulo p under (3). Under (4), $f(1, 0)$ goes into $f(0, 1)$, $f(0, 1)$ goes into $f(-1, 0) = (-1)^n f(1, 0)$ and when $t \neq 0$, $f(t, 1)$ goes into $f(-1, t) = t^n f(t', 1)$ where $t' = -1/t$. Finally, under (5), $f(1, 0)$ is invariant and $f(t, 1)$ goes into $f(t, \rho) = \rho^n f(t'', 1)$ where $t'' = -t/\rho$. Hence if λ be an integer such that $k = \lambda(p-1)/q$ is an integer, then the k^{th} powers of the values of $f(x_1, x_2)$ where (x_1, x_2) range over the above set-are merely permuted among themselves by any transformation (3), (4), (5) and hence by any transformation (2), Thus we have.

THEOREM 1. — *Let* $f(x_1, x_2) = a_0 x_1^q + a_1 x_1^{q-1} x_2 + \ldots + a_q x_2^q$ *be any binary* q*—ic and let* k *be any integer of the form* $\lambda(p-1)/q$ *where* λ *is an integer. Then any symmetric function of the* k^{th} *powers of* $f(1, 0)$ *and* $f(t, 1)(t = 0, \ldots, p-1)$ *is a formal modular invariant of* f *with respect to the Galois field,* GF[p], *of order* p *if there is made no lowering of the exponents is made by application of Fermat's theorem.*

Special cases of this are the three theorems of Williams' Part I of wich the first two are due to Hurwitz. In essentially the same is proved the

COROLLARY. — *This is Theorem* 1 *stated for the general Galois field,* GF[p^n], *of order* p^n.

In his paper, he used essentially the symbolic notation of classic invariant theory which can not, however, be used for formal modular invariants of a binary $q - ic$ in case any of the binomial coefficients is congruent to zero, modulo p. But the above theorem and corollary can be proved equally well for the general binary $q - ic$ by using the symbolic notation, for formal modular invariants (1). In this latter notation

$$f(x_1, x_2) \equiv \prod_{\alpha} (\alpha_1 x_1 + \alpha_2 x_2) = (\alpha_1 x_1 + \alpha_2 x_2)(\beta_1 x_1 + \beta_2 x_2) \ldots$$

where the q symbolic linear factors are symbolically distinct. Since (α_1, α_2) are subjected to a linear transformation when the x's are subjected to a linear transformation (2), then $L(\alpha) = \prod_{t} (\alpha_1 t_1 + \alpha_2 t_2)$ is a formal modular invariant of $f(x_1, x_2)$ when (t_1, t_2) range over the set τ : (1, 0), $(t, 1)$ $(t = 0, 1, \ldots, p-1)$. Similarly with $L(\beta)$, $L(\gamma)$, etc. Hence $\prod_{\alpha} L(\alpha) = f(t_1, t_2)$ is a formal modular invariant of $f(x_1, x_2)$ and thus we have Theorem 1 in part I. Similarly, we prove Theorem 2 and 3 of Part II.

---

(1) HAZLETT, *A symbolic theory of formal modular invariants* (*Transactions of the Amer. Math. Soc.*, vol. 24, 1922, p. 286-311).

In the same manner as above, we may also prove the four theorems in Part III. We do not make any actual change in his proof, but merely note that he does not actually use the binomial coefficients in his proof in any way. His proofs hold with complete generality although that was not true of his proofs of the theorems in his Part I. Moreover, they are special cases of a more general theorem which we shall now proceed to prove.

Let F_1 be any polynomial in $f(1,0)$ and the $f(t,1)(t=0,1,\ldots,p-1)$. Then F_1 is a polynomial in the a's in which we understand that no reduction in the exponents of the a's has been made by applying Fermat's theorem. If we apply any particular transformation (2), F_1 is replaced by another polynomial in the a's in which, also, we understand that there has been made no reduction in the exponents of the a's. If these two polynomials are always identical (modulo p) — that is, if F_1 be formally unaltered under all transformation — it is a formal modular invariant of $f(x_1, x_2)$. If, however, F_1 be altered by some transformation σ_1, let F_2 be the transform of F_1 under σ_1, let F_3 be the transform of F_2 under σ_1, etc. If Φ_1, denote any symmetric function of those conjugates of F_1 under the group S_1 generated by σ_1 which are incongruent modulo p, then Φ_1 is formally unaltered under the group S_1. Now let Φ_2 be the conjugate of Φ_1 under some transformation σ_2 of the group (2) not in S_1, and similarly Φ_1 has conjugates under the various transformations of the group generated by σ_2. If Φ_1 be unaltered under σ_2, then Φ_1 is an invariant under the group S_2 of transformations generated by σ_1 and σ_2. If Φ_1 be note unaltered under σ_2, let us form the same symmetric function Ψ_1 of $\Phi_1, \Phi_2, \ldots$, that Φ_1 is of $F_1, F_2, \ldots$. Then Ψ_1 is invariant under the group S_2. Continue in this way. Since there is only a finite number of conjugate of F_1, incongruent modulo p, under the group (2) this simple process is feasible in the modular case at it would not be in the classic case.

Another natural process for forming the formal modular invariants obtained in the above manner is the following (1). Let F_1 be as above. Under any particular transformation (2), F_1 is replaced by the pro-

(1) Strictly speaking, the invariant obtained by the first method is a constant multiple of the one obtained by the second method.

duct of a non-zéro ρ^{qk} — where k is the degree of F_1 in the a's, — and F_i, where F_i is here obtained from F_1 by changing the order of the pairs τ. Consider the γ' th powers, $P^{\gamma'}$, of F_i where γ is an integer of the form $\lambda(p-1)/qk$ in which λ is a fixed positive integer. Then any symmetric function of the P_i is a formal modular invariant. In a similar manner we prove

THEOREM 2. — *Let $f(x_1, x_2)$ be any homogeneous polynomial in two variables of order q and let F_1 be any homogeneous polynomial in $f(1, 0)$ and the $f(t, 1)$ t ranges over the marks of the Galois field $GF[p^n]$ of order p^n. Let F_i range over all the conjugates of F_1 under the permutations of the pairs τ which are incongruent in the Galois field, $GF[p^n]$, of order p^n. If $\gamma = \lambda(p-1)/q$ be an integer (where is some fixed integer), then any symmetric function of the γ' th powers of the F_i is a formal modular invariant under the group* (2).

4. *More than two variables.* — Now let $f(x_1, x_2, \ldots, x_n)$ be the general homogeneous polynomial in n variables with coefficients denoted by a with suitable subscripts. We subject the variables to the transformations of the group

$$x_i = \Sigma \alpha_{ij} x'_j \qquad (i, j = 1, \ldots, n), \tag{6}$$

where the α's are marks of the Galois field, $GF[p^m]$, of order p^m such that their determinant is not zero in the field. Instead of the former set τ of pairs (x_1, x_2) we have the set σ: $(1, 0, \ldots, 0)$, $(\rho_1, 0, \ldots, 0)$, $(\rho_1, \rho_2, 1, 0, \ldots, 0)$, $\ldots$, $(\rho_1, \rho_2, \ldots, \rho_{n-1}, 1)$. A proof closely parallel to the one above for the binary case holds here although the symbolic proofs do not seem to hold. Thus we have

THEOREM 3. — *Let $f(x_1, \ldots, x_n)$ be any homogeneous polynomial in n variables of order q and let F_1 be any homogeneous polynomial in the values of f as the $(x_1, \ldots, x_n)$ range over the set σ. Let F_i range over all these conjugates of F_1 under the transformations of the group* (6), *which are incongruent in the field. If $\gamma = \lambda(p^m-1)/q$ be an integer (where λ is some fixed positive integer), then any symetric function of the γ' th powers of the F_i is a formal modular invariant of f under the group* (6) *with respect to the field $GF[p^m]$.*