# INVARIANTIVE THEORY OF EQUATIONS IN A FINITE FIELD

BY

L. CARLITZ

1. **Introduction.** Let $GF(q)$ denote a fixed finite field and $r$ a fixed integer $\geqq 1$. Consider the set of transformations

$$\phi: \xi_i = \phi_i(\eta_1, \cdots, \eta_r) \qquad (i = 1, \cdots, r) \tag{1.1}$$

possessing an inverse; here $\xi_i, \eta_i \in GF(q)$ and the $\phi_i$ are polynomials with coefficients $\in GF(q)$. The totality of transformations (1.1) form a group isomorphic with the symmetric group on $q^r$ letters. If $f=f(\xi_1, \cdots, \xi_r)$ is an arbitrary polynomial with coefficients $\in GF(q)$ and $\phi f=g$, then $f$ and $g$ are *equivalent*. Two polynomials $f$ and $g$ are defined as equal if $f(\xi_1, \cdots, \xi_r) = g(\xi_1, \cdots, \xi_r)$ for all $\xi_i$. It follows that there are $q^{q^r}$ distinct polynomials. By means of the previously defined equivalence relation they are separated into a certain number of classes; a simple combinatorial argument shows that the number of classes is

$$\binom{q^r + q - 1}{q - 1}, \tag{1.2}$$

where the symbol in (1.2) is a binomial coefficient.

The purpose of this paper is to discuss invariantive properties of the equation $f(\xi_1, \cdots, \xi_r)=0$, where $f$ is an arbitrary polynomial with coefficients in $GF(q)$. In particular if $N_f(\alpha)$ denotes the number of solutions of $f=\alpha$, then the numbers $N_f(\alpha)$ form a complete set of invariants in the following sense: Two polynomials $f$ and $g$ are equivalent if and only if $N_f(\alpha)=N_g(\alpha)$ for all $\alpha \neq 0$. Moreover any invariant of $f$ (with rational values, say) can be exhibited as a polynomial in the $N_f(\alpha)$ with rational coefficients. A number of additional topics and applications are also discussed.

Dickson in [5] and subsequent papers (for references see [11]) initiated the study of modular invariants. The transformations employed are restricted to the group of linear transformations. By contrast we are here considering the larger group of transformations (1.1). Thus many of the invariants introduced by Dickson are no longer invariants from the viewpoint of this paper. While we are here considering only the invariants of a single polynomial, we hope to discuss subsequently the general case of systems of polynomials.

It may be helpful to list the contents of the paper by sections. 1. Introduc-

Presented to the Society, September 5, 1952; received by the editors September 18, 1952.

tion. 2. Notation and terminology. 3. Some preliminary results. 4. Transformations. 5. Classes. 6. Characteristic invariants. 7. Reducibility. 8. Additional properties of $M(f)$. 9. Some applications. 10. Other applications.

**2. Notation and terminology.** The numbers of $GF(q)$ will be denoted by lower case Greek letters $\alpha, \beta, \gamma, \cdots, \xi, \eta$. The letters $q=p^n$ and $r$ will have the meaning assigned above.

By a polynomial $f=f(x_1, \cdots, x_r)$ will be meant a polynomial in the indeterminates $x_1, \cdots, x_r$ with coefficients in $GF(q)$; we write $f \in GF[q, x_1, \cdots, x_r]$. Polynomials will in general be denoted by lower case italics $f, g, \cdots$; however the polynomials constituting the transformation (1.1) will be denoted by lower case $\phi, \psi, \cdots$. Two polynomials $f, g \in GF[q, x_1, \cdots, x_r]$ are *equal* if and only if $f(\xi_1, \cdots, \xi_r)=g(\xi_1, \cdots, \xi_r)$ for all $\xi_i \in GF(q)$. Thus every polynomial $f$ is equal to a unique reduced polynomial in which every exponent $\leqq q-1$ (proof in [4]).

Two polynomials $f, g$ are *equivalent* ($f \sim g$) if there exists a transformation $\phi$ of the form (1.1) such that $\phi f=g$. By a *transformation* will always be understood one of the form (1.1), that is, one possessing an inverse. Equivalent polynomials constitute a *class*. Classes of polynomials will be denoted by capital italics, $A, B, C$; in particular the class containing the polynomial $f$ may be denoted by $A_f$. If the transformation $\psi$ leaves $f$ unaltered (that is, $\psi f=f$) then $\psi$ is an *automorphism* of $f$. Thus the totality of automorphisms of $f$ form a group $G=G_f$ of order $\nu(f)$. If $\phi f=g$, then it is clear that the group of automorphisms $G_g=\phi^{-1}G_f\phi$; in particular $\nu(f)=\nu(g)$. Thus the number of automorphisms is the same for any polynomial of a fixed class $A$; accordingly we write $\nu(A)$ for this number.

If a polynomial $f$ is equivalent to one in $s$ but not fewer variables, then $s$ will be called the *rank* of $f$. We may also call $s$ the rank of $A_f$, the class containing $f$.

If $\alpha \in GF(q)$ we define

$$t(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}, \tag{2.1}$$

so that $t(\alpha)$ is an integer (mod $p$). We next put

$$e(\alpha) = e^{2\pi i t(\alpha)/p}, \tag{2.2}$$

so that

$$e(\alpha+\beta) = e(\alpha)e(\beta), \qquad e(0) = 1,$$

$$\sum_{\alpha \in GF(q)} e(\alpha\beta) = \begin{cases} q & (\beta = 0), \\ 0 & (\beta \neq 0), \end{cases} \tag{2.3}$$

where the summation is over all $\alpha$ in $GF(q)$. If $f$ is an arbitrary polynomial we define

$$M(f) = \sum_{\xi_1, \cdots, \xi_r} e(f(\xi_1, \cdots, \xi_r)) \tag{2.4}$$

and

$$N_f(\alpha) = N\{f(\xi_1, \cdots, \xi_r) = \alpha\}, \tag{2.5}$$

where the $N$ on the right denotes the number of solutions $\xi_1, \cdots, \xi_r$ of the indicated equation. Similarly by the symbol

$$N\{f_1(\xi_1, \cdots, \xi_r) = \alpha_1, \cdots, f_k(\xi_1, \cdots, \xi_r) = \alpha_k\} \tag{2.6}$$

is understood the number of solutions of the indicated system of equations.

It is clear from the definition that

$$\sum_{\alpha \in GF(q)} N_f(\alpha) = q^r; \tag{2.7}$$

a like result holds for (2.6).

For brevity we shall sometimes speak of the point $(\xi_1, \cdots, \xi_r)$; also when convenient we shall write $f(\xi)$ for $f(\xi_1, \cdots, \xi_r)$.

3. **Some preliminary results.** The following theorem is given by Dickson [5, p. 124] and is an immediate consequence of the Lagrange interpolation formula.

THEOREM 3.1. *Let $f(x_1, \cdots, x_r)$ be a polynomial that takes on the values $f(\xi_1, \cdots, \xi_r)$; then we have*

$$f(x_1, \cdots, x_r) = (-1)^r \sum_{\xi_1, \cdots, \xi_r} \frac{x_1^q - x_1}{x_1 - \xi_1} \cdots \frac{x_r^q - x_r}{x_r - \xi_r} f(\xi_1, \cdots, \xi_r). \tag{3.1}$$

The right member of (3.1) is evidently in *reduced* form.

It follows at once from Theorem 3.1 that the number of distinct polynomials in $r$ variables is $q^{q^r}$. Another consequence of Theorem 3.1 can be stated as follows: *The residue class ring $GF[q, x_1, \cdots, x_r]$ modulo $(x_1^q - x_1, \cdots, x_r^q - x_r)$ is a direct sum of $q^r$ fields $GF(q)$.*

THEOREM 3.2. *If $M(f)$ and $N_f(\alpha)$ are defined by* (2.3) *and* (2.4), *respectively, then*

$$N_f(\alpha) = q^{-1} \sum_{\beta} e(-\alpha\beta) M(\beta f). \tag{3.2}$$

To prove (3.2) we consider the sum

$$\sum_{\xi_1, \cdots, \xi_r} \sum_{\beta} e\{\beta f(\xi_1, \cdots, \xi_r) - \alpha\beta\}. \tag{3.3}$$

On the one hand it is evident from (2.3) that (3.3) is $qN_f(\alpha)$; on the other hand, interchanging the order of summation, we get

$$\sum_{\beta} e(-\alpha\beta) \sum_{\xi_1, \cdots, \xi_r} e(\beta f(\xi_1, \cdots, \xi_r)).$$

Applying (2.3) we get (3.2).

THEOREM 3.3. *In the notation of Theorem* 3.2, *we have*

$$M(\gamma f) = \sum_{\alpha} e(\alpha\gamma)N_f(\alpha) \qquad (\gamma \in GF(q)), \tag{3.4}$$

*and in particular*

$$M(f) = \sum_{\alpha} e(\alpha)N_f(\alpha). \tag{3.5}$$

To prove (3.4), we multiply both members of (3.2) by $e(\alpha\gamma)$ and sum:

$$\sum_{\alpha} e(\alpha\gamma)N_f(\alpha) = q^{-1}\sum_{\beta}\sum_{\alpha} e((\gamma - \beta)\alpha)M(\beta f).$$

Now apply (2.3) to the inner sum on the right, and (3.4) follows.

THEOREM 3.4. *If* $f \sim g$ *then* $M(f) = M(g)$ *and* $N_f(\alpha) = N_g(\alpha)$ *for all* $\alpha \in GF(q)$.

Let $g(\xi) = f(\eta)$, where

$$\eta_i = \phi_i(\xi_1, \cdots, \xi_r) \qquad (i = 1, \cdots, r). \tag{3.6}$$

Then clearly to each solution of $g(\xi) = \alpha$ corresponds a unique solution of $f(\eta) = \alpha$. Conversely since (3.6) has an inverse, to each solution of $f(\eta) = \alpha$ corresponds a unique solution of $g(\xi) = \alpha$. This proves the second half of the theorem. The first half now follows on applying (3.5).

By Theorem 3.4, $M(f)$ and $N_f(\alpha)$ are *class invariants*; hence if $f \in A$ we may define

$$M(A) = M(f), \qquad N_A(\alpha) = N_f(\alpha). \tag{3.7}$$

Note that by (2.7) we have

$$\sum_{\alpha} N_A(\alpha) = q^r \tag{3.8}$$

so that the numbers $N_A(\alpha)$ are not independent. However aside from the relation (3.8) the integers $N_A(\alpha)$ can be chosen arbitrarily. More precisely we prove

THEOREM 3.5. *Given integers* $h(\alpha) \geqq 0$ *such that*

$$\sum_{\alpha} h(\alpha) = q^r, \tag{3.9}$$

*then there exists a polynomial* $f$ *such that*

$$N_f(\alpha) = h(\alpha) \qquad \text{for all } \alpha \in GF(q). \tag{3.10}$$

This theorem can be thought of as a corollary of Theorem 3.1. For the numbers $f(\xi_1, \cdots, \xi_r)$ in (3.1) are arbitrary quantities in $GF(q)$ and $N_f(\alpha)$ denotes the number of terms in the right member of (3.1) such that $f(\xi_1, \cdots, \xi_r) = \alpha$, that is, $h(\alpha)$. The necessity of (3.9) is merely a restatement of (3.8).

A word may be added about such equations as (3.2) and (3.4). If $R(\alpha)$, $S(\alpha)$ are two complex-valued functions of $\alpha$ such that

$$R(\alpha) = \sum_{\beta} e(\alpha\beta)S(\beta), \tag{3.11}$$

then it is easily proved using (2.3) that

$$S(\alpha) = q^{-1} \sum_{\beta} (-\alpha\beta)R(\beta); \tag{3.12}$$

conversely if we assume (3.12) then (3.11) follows. Moreover we have

$$\sum_{\gamma} S(\gamma)\overline{S}(\alpha + \gamma) = q^{-1} \sum_{\beta} e(\alpha\beta) \mid R(\beta) \mid^2, \tag{3.13}$$

where $\overline{S}$ denotes the complex conjugate of $S$. For a fuller discussion and generalization of these formulas see [12; 13]. Incidentally, for the special functions $N_f$ and $M$, (3.13) becomes

$$\begin{aligned} \sum_{\gamma} N_f(\gamma)N_f(\alpha + \gamma) &= q^{-1} \sum_{\beta} e(\alpha\beta) \mid M(\beta f) \mid^2, \\ \sum_{\gamma} M(\gamma f)\overline{M}((\alpha + \gamma)f) &= q \sum_{\beta} e(-\alpha\beta)N_f^2(\beta), \end{aligned} \tag{3.14}$$

and in particular for $\alpha = 0$,

$$\sum_{\gamma} \mid M(\gamma f) \mid^2 = q \sum_{\beta} N_f^2(\beta). \tag{3.15}$$

4. **Transformations.** We first prove

THEOREM 4.1. *The totality of transformations* (1.1) *constitute a group isomorphic to* $\mathfrak{S}_{q^r}$, *the symmetric group on* $q^r$ *letters.*

It suffices to show that every permutation of the points $(\xi_1, \cdots, \xi_r)$ can be effected by means of a transformation (1.1). This again is a consequence of Theorem 3.1. For consider the polynomials

$$\phi_i(x_1, \cdots, x_r) = (-1)^r \sum_{\xi_1, \cdots, \xi_r} \frac{x_1^q - x_1}{x_1 - \xi_1} \cdots \frac{x_r^q - x_r}{x_r - \xi_r} \eta_i \quad (i = 1, \cdots, r). \tag{4.1}$$

Clearly (4.1) implies $\phi_i(\xi_1, \cdots, \xi_r) = \eta_i$ $(i = 1, \cdots, r)$. This evidently proves the theorem.

THEOREM 4.2. *Two polynomials* $f$, $g$ *are equivalent if and only if*

$$N_f(\alpha) = N_g(\alpha) \qquad \textit{for all } \alpha \in GF(q). \tag{4.2}$$

REMARK. In view of (3.8) it suffices to assert (4.2) for all but one value of $\alpha$.

The necessity of Theorem 4.2 has already been proved in Theorem 3.4.

To prove the sufficiency let $\alpha$ be a fixed number of $GF(q)$ and let

$$f(\beta_1^{(j)}, \cdots, \beta_r^{(j)}) = g(\gamma_1^{(j)}, \cdots, \gamma_r^{(j)}) = \alpha \quad (j = 1, \cdots, s),$$

where $s = N_f(\alpha) = N_g(\alpha)$. Now consider the permutation

$$(\beta_1^{(j)}, \cdots, \beta_r^{(j)}) \to (\gamma_1^{(j)}, \cdots, \gamma_r^{(j)}) \tag{4.3}$$

as both $j$ and $\alpha$ assume all permissible values. By Theorem 4.1 the permutation (4.3) can be effected by means of a certain transformation and this transformation clearly carries $f$ into $g$. The transformation is in general not unique.

THEOREM 4.3. *Two polynomials $f$, $g$ are equivalent if and only if*

$$M(\beta f) = M(\beta g) \qquad \text{for all } \beta \neq 0. \tag{4.4}$$

It will suffice to show that condition (4.4) is satisfied if and only if (4.2) is satisfied. Suppose (4.2) holds; then by (3.4) it follows that (4.4) holds. Conversely if (4.4) holds, then by (3.2) it follows that (4.2) holds. Hence the theorem is proved.

THEOREM 4.4. *The number of automorphisms $\nu(A)$ of the class $A$ is determined by*

$$\nu(A) = \prod_{\alpha} (N_A(\alpha))!, \tag{4.5}$$

*the product extending over all $\alpha \in GF(q)$.*

Let $f \in A$ and as in the proof of the previous theorem let

$$f(\beta_1^{(j)}, \cdots, \beta_r^{(j)}) = \alpha \qquad (j = 1, \cdots, N_f(\alpha)).$$

Clearly every automorphism of $f$ is obtained by permutating the points

$$(\beta_1^{(j)}, \cdots, \beta_r^{(j)}) \qquad (j = 1, \cdots, N_f(\alpha))$$

for each $\alpha$. Thus

$$\nu(f) = \prod_{\alpha} (N_f(\alpha))!$$

which is the same as (4.5).

THEOREM 4.5. *The number of polynomials $\mu(A)$ in the class $A$ satisfies*

$$\mu(A)\nu(A) = q^r!. \tag{4.6}$$

Let $f$ be any polynomial $\in A$ and let us apply to $f$ each of the $q^r!$ transformations of $\mathfrak{S}_{q^r}$. Since the number of automorphisms depends only on the

class, it is clear that $f$ is carried into each polynomial of $A$ and that each occurs the same number of times, namely $\nu(A)$. Therefore (4.6) is proved.

We next prove some theorems of a somewhat different nature. Let $\phi_1=\phi_1(x_1, \cdots, x_r)$ be one of the polynomials in the transformation (1.1). Clearly $\phi_1$ can be transformed into $x_1$ and conversely if a polynomial $\phi_1$ is equivalent to $x_1$, then we can find $r-1$ additional polynomials $\phi_2, \cdots, \phi_r$ so that the set of $r$ polynomials define a transformation. Generally given $k$ polynomials $\phi_1, \cdots, \phi_k$, then one can find $r-k$ additional polynomials $\phi_{k+1}, \cdots, \phi_r$ such that $\phi_1, \cdots, \phi_r$ define a transformation if and only if one can simultaneously transform $\phi_1, \cdots, \phi_k$ into $x_1, \cdots, x_k$, respectively.

Now if a polynomial $\phi$ is equivalent to $x_1$ then it is clear that

$$N_\phi(\alpha) = q^{r-1} \qquad \text{for all } \alpha. \tag{4.7}$$

Using (3.4) and (3.2) it is easily seen that (4.7) is equivalent to

$$M(\gamma\phi) = 0 \qquad \text{for all } \gamma \neq 0. \tag{4.8}$$

Thus when (4.8) holds we have, using (3.2),

$$N_\phi(\alpha) = q^{-1}M(0) + q^{-1}\sum_{\beta\neq 0} e(-\alpha\beta)M(\gamma\phi) = q^{r-1}.$$

In the next place if we have two polynomials $\phi_1, \phi_2$ which can be simultaneously transformed into $\xi_1, \xi_2$, then it is evident that the number of solutions $N_{\alpha_1\alpha_2}$ of the system

$$\phi_1(\xi_1, \cdots, \xi_r) = \alpha_1, \qquad \phi_2(\xi_1, \cdots, \xi_r) = \alpha_2$$

is $q^{r-2}$ for all $\alpha_1, \alpha_2$, and conversely. Now by (2.3) it is clear that

$$\begin{aligned} q^2 N_{\alpha_1\alpha_2} &= \sum_{\beta_1,\beta_2} e(-\alpha_1\beta_1 - \alpha_2\beta_2) \sum_{\xi_1,\cdots,\xi_r} e\{\beta_1\phi_1(\xi) + \beta_2\phi_2(\xi)\} \\ &= q^r + \sum_{\beta_1,\beta_2}{}' e(-\alpha_1\beta_1 - \alpha_2\beta_2)M(\beta_1\phi_1 + \beta_2\phi_2), \end{aligned} \tag{4.9}$$

where in the sum on the right the combination $\beta_1=\beta_2=0$ is excluded. If we multiply (4.9) by $e(\alpha_1\gamma_1+\alpha_2\gamma_2)$ and sum we get, again using (2.3),

$$M(\gamma_1\phi_1 + \gamma_2\phi_2) = \sum_{\alpha_1,\alpha_2} e(\alpha_1\gamma_1 + \alpha_2\gamma_2)N_{\alpha_1\alpha_2}. \tag{4.10}$$

By means of (4.9) and (4.10) we see that the condition $N_{\alpha_1\alpha_2}=q^{r-2}$ for all $\alpha_1, \alpha_2$ is equivalent to $M(\gamma_1\phi_1+\gamma_2\phi_2)=0$ ($\gamma_1, \gamma_2$ not both 0). It is now evident how to prove generally the following

THEOREM 4.6. *Let $1\leqq k\leqq r$. Let $N$ denote the number of solutions of the system*

$$\phi_i(\xi_1, \cdots, \xi_r) = \alpha_i \qquad (i = 1, \cdots, k). \tag{4.11}$$

*Then the condition*

(4.12) $N = q^{r-k}$ (*for all* $\alpha_1, \cdots, \alpha_k$)

*is equivalent to*

(4.13) $M(\gamma_1\phi_1 + \cdots + \gamma_k\phi_k) = 0$ ($\gamma_i$ *not all* 0).

In particular for $k=r$, we have the following corollary.

THEOREM 4.7. *The set of polynomials* $\phi_1, \cdots, \phi_r$ *define a transformation* (1.1) *if and only if*

(4.14) $M(\gamma_1\phi_1 + \cdots + \gamma_r\phi_r) = 0$ ($\gamma_i$ *not all* 0).

We need only observe that when $k=r$, (4.12) becomes $N=1$ for all $\alpha_1, \cdots, \alpha_r$.

*Rank.* The rank of a polynomial has been defined in §2. We now prove

THEOREM 4.8. *If* $q \mid N_f(\alpha)$ *for all* $\alpha$, *then* $f$ *is of rank* $\leqq r-1$.

**Proof.** The non-negative integers $h(\alpha) = q^{-1}N_f(\alpha)$ satisfy $\sum_\alpha h(\alpha) = q^{r-1}$. Hence by Theorem 3.5 there exists a polynomial $g(\eta_1, \cdots, \eta_{r-1})$ such that $N_g'(\alpha) = h(\alpha)$, where the prime indicates that $\eta_r$ is ignored in counting the number of solutions. Consequently $N_g(\alpha) = qh(\alpha) = N_f(\alpha)$ and therefore by Theorem 4.1 we have $f \sim g$.

THEOREM 4.9. *If* $q^s$ *is the highest power of* $q$ *such that* $q^s \mid N_f(\alpha)$ *for all* $\alpha$, *then* $f$ *is of rank* $r-s$.

This theorem is evidently a consequence of Theorem 4.8 since it is clear that if $f$ is of rank $r-s$ then $q^s \mid N_f(\alpha)$.

If $f$ is a quadratic form with nonvanishing discriminant ($p \neq 2$), then by the familiar formulas the highest power of $q$ dividing $N_f(\alpha)$ is $q^{s-1}$ for $r=2s$ and $q^s$ for $r=2s+1$. Consequently by the last theorem the rank is $s+1$ in either case; thus the rank $<r$ for $r \geqq 3$. In particular, then, the rank as defined here is not to be confused with the ordinary rank of a quadratic form.

5. **Classes.** Theorems 4.2 and 4.3 furnish criteria for the equivalence of two polynomials, Theorem 4.4 determines the number of automorphisms of a class, and Theorem 4.5 determines the number of polynomials in a class. We shall now determine the number of classes of polynomials in $r$ variables.

As we saw in the proof of Theorems 4.3 and 4.4, for every polynomial $f$ there is a partition $q^r = \sum_\alpha N_f(\alpha)$ and for each $\alpha$ a set of $s = N_f(\alpha)$ points $(\beta_1^{(j)}, \cdots, \beta_r^{(j)})$ such that

$$f(\beta_1^{(j)}, \cdots, \beta_r^{(j)}) = \alpha \qquad (j = 1, \cdots, s).$$

It is convenient at this point to define a *category* of polynomials. Two polynomials $f$, $g$ belong to the same category if the set of integers $\{N_f(\alpha)\}$ is some permutation of the set of integers $\{N_g(\alpha)\}$. Thus by Theorem 4.2 equivalent polynomials fall in the same category; in other words each cate-

gory consists of a certain number of classes. It is clear from the definition that the number of categories is the number of partitions

$$q^r = \sum_i k_i \qquad (k_1 \geqq k_2 \geqq \cdots \geqq 1), \tag{5.1}$$

where the number of summands is at most $q$; in other words the number of categories is the number of partitions of $q^r$ into at most $q$ parts. In particular for $r=1$ the number of categories is the number of unrestricted partitions of $q$.

Now corresponding to each partition (5.1) we get a certain number of classes, which can be determined as follows. Clearly it is necessary only to count the number of permutations of the $k_i$ making due allowance for repetitions. Now, changing the notation, suppose we rewrite (5.1) as

$$q^r = e_1 + 2e_2 + 3e_3 + \cdots \qquad (e_i \geqq 0). \tag{5.2}$$

Then the number of permutations in question is

$$\frac{q!}{e_0!e_1!e_2!\cdots} \qquad (e_0 + e_1 + e_2 + \cdots = q); \tag{5.3}$$

since the number of values that $f$ takes on is $q$, the sum of the $e_i$ must also be $q$. Thus the number of classes is

$$\sum \frac{q!}{e_0!e_1!e_2!\cdots} \tag{5.4}$$

where the summation is over all $e_i$ satisfying (5.2) and $e_0$ is defined by the second of (5.3). To evaluate (5.4) we construct the generating function

$$G(x) = 1 + \sum_{m=1}^{\infty} x^m \sum \frac{q!}{e_0!e_1!e_2!\cdots} \tag{5.5}$$

where the inner sum is over all $e_i$ such that

$$m = e_1 + 2e_2 + 3e_3 + \cdots, \qquad q = e_0 + e_1 + e_2 + \cdots. \tag{5.6}$$

Now, on the other hand, consider the expansion [10, p. 60] of

$$(a_0 + a_1x + a_2x^2 + \cdots)^k = \sum_{m=0}^{\infty} A_m x^m;$$

it is easily verified that

$$A_m = \sum \frac{k!}{e_0!e_1!e_2!\cdots} a_0^{e_0} a_1^{e_1} a_2^{e_2} \cdots,$$

where

$$e_0 + e_1 + e_2 + \cdots = k, \qquad e_1 + 2e_2 + 3e_3 + \cdots = m.$$

Comparing with (5.5) and (5.6) we see that the coefficient of $x^m$ in $G(x)$ is equal to the coefficient of $x^m$ in

$$(1 + x + x^2 + \cdots)^q = (1 - x)^{-q} = \sum_{m=0}^{\infty} \binom{q + m - 1}{q - 1} x^m.$$

Thus for $m = q^r$ we see that (5.4) reduces to

$$\binom{q^r + q - 1}{q - 1}. \tag{5.7}$$

We have therefore proved

THEOREM 5.1. *The number of classes of polynomials in r variables is determined by* (5.7).

It may be helpful to illustrate the theorem in one or two simple cases. For $q = 5$, $r = 1$, we have the following table.

| | | |
|---|---|---|
| I | [5] | 5 |
| II | [41] | 20 |
| III | [32] | 20 |
| IV | [311] | 30 |
| V | [221] | 30 |
| VI | [2111] | 20 |
| VII | [11111] | 1 |
| | | 126 |

There are seven categories as indicated by the Roman numerals. The second column indicates the partition defining each category, the third column the number of classes in each category. Note that the total number of classes is

$$126 = \binom{9}{4}$$

in accord with (5.7). We remark that category I contains the constants 0, 1, 2, 3, 4, while category VII consists of the class with representative $\xi_1$. Again $\xi_1^2$ is a representative of one of the 30 classes in category V.

For a second illustration we take $q = 2$, $r = 3$. There are now 5 categories and 9 classes.

| | | | |
|---|---|---|---|
| I | [8] | 2 | 0, 1 |
| II | [71] | 2 | $\xi_1\xi_2\xi_3$, $\xi_1\xi_2\xi_3 + 1$ |
| III | [62] | 2 | $\xi_1\xi_2$, $\xi_1\xi_2 + 1$ |
| IV | [53] | 2 | $\xi_1\xi_2\xi_3 + \xi_1$, $\xi_1\xi_2\xi_3 + \xi_1 + 1$ |
| V | [44] | 1 | $\xi_1$ |

The fourth column contains representatives of the several classes.

A somewhat more instructive example is furnished by $q=3$, $r=2$. There are now 12 categories and 55 classes. However we shall not take the space to exhibit the table.

We can refine Theorem 5.1 somewhat by determining the number of classes of rank $s$, $0 \leqq s \leqq r$. The result is contained in

THEOREM 5.2. *Let $1 \leqq s \leqq r$. The number of classes of rank $s$ is determined by*

$$\binom{q^s + q - 1}{q - 1} - \binom{q^{s-1} + q - 1}{q - 1}. \tag{5.8}$$

To prove this result we need only observe that the classes of rank $\leqq s$ may also be obtained by means of the polynomials in $s$ variables; moreover each class will be counted only once. Hence (5.8) follows at once.

We remark that the second example above also illustrates Theorem 5.2. Indeed it also illustrates the following

THEOREM 5.3. *All the classes in a fixed category have the same rank.*

This theorem follows immediately from Theorem 4.9 and the definition of category. We have also

THEOREM 5.4. *The number of categories of rank $s$ is equal to the number of partitions of $q^s$ into at most $q$ parts with greatest common divisor not divisible by $q$.*

**6. Characteristic invariants.** Following Dickson [5; 6], we define the following functions

$$I_A(B) = \begin{cases} 1 & (B = A), \\ 0 & (B \neq A), \end{cases} \tag{6.1}$$

where $A$ and $B$ denote classes. The $I_A$ are called characteristic invariants. It is to be understood that the values 0, 1 taken on by these functions lie in the complex field. The following properties are immediate consequences of (6.1):

$$I_A I_B = \delta_{AB} = \begin{cases} I_A & (A = B), \\ 0 & (A \neq B), \end{cases} \tag{6.2}$$

$$\sum_A I_A = 1. \tag{6.3}$$

If $h(A)$ is any function of $A$ (with values in the complex field), then we have the representation

$$h(A) = \sum_B h(B) I_B(A). \tag{6.4}$$

Moreover the representation (6.4) is unique as follows from (6.2).

The $I_A$ can be expressed in terms of a single invariant $J$ now to be defined. Let the classes be ordered $A_1, A_2, \cdots, A_w$ in any convenient manner, where $w$ is given by (5.7). Now define the function $J(A)$ by means of

$$J(A_i) = i \qquad (i = 1, \cdots, w). \tag{6.5}$$

Then we have the easily verified formula

$$I_{A_i}(X) = \prod_{j \neq i} \frac{J(X) - J(A_j)}{J(A_i) - J(A_j)}, \tag{6.6}$$

where $X$ denotes an arbitrary class. Thus $I_A$ is a polynomial in $J$.

The exact values taken on by $J$ in (6.5) are not essential; it is necessary only that they be distinct. With the particular choice in (6.5) we can rewrite (6.6) as follows

$$I_{A_i}(X) = (-1)^{w-i} \frac{1}{(w-1)!} \binom{w-1}{i-1} \prod_{j \neq i} (J(X) - J(A_j)).$$

We have proved

THEOREM 6.1. *The characteristic invariant $I_A$ can be expressed as a polynomial in $J$ by means of* (6.6).

Next, referring to (6.4), we get

THEOREM 6.2. *Any function $H(A)$ with values in the complex field can be exhibited as a polynomial in $J$ of degree $<w$.*

We shall now show that $J(A)$ can be expressed as a linear combination of $N_A(\alpha)$, $\alpha \neq 0$. Consider the sum

$$F(A) = \sum_{\alpha \neq 0} c_\alpha N_A(\alpha); \tag{6.7}$$

we seek a set of rational numbers $c_\alpha$ such that the numbers $F(A)$ are distinct. We shall again suppose that the classes have been numbered $A_1, \cdots, A_w$. Then by Theorem 4.2 we can find a set of rational numbers $\{c_\alpha^1\}$ such that

$$F_1(A_1) \neq F_1(A_2), \qquad \text{where } F_1(A) = \sum_{\alpha \neq 0} {}^1c_\alpha N_A(\alpha).$$

If $F_1(A_1) = F_1(A_3)$, we pick a set $\{c_\alpha^2\}$ such that

$$F_2(A_1) \neq F_2(A_3), \qquad \text{where } F_2(A) = \sum_{\alpha \neq 0} {}^2c_\alpha N_A(\alpha);$$

then we can choose $k$ so that if $F_{12} = F_1 + kF_2$, then $F_{12}(A_1) \neq F_{12}(A_2)$, $F_{12}(A_1) \neq F_{12}(A_3)$ are all distinct. If now $F_{12}(A_1) = F_{12}(A_4)$, we pick a set $\{c_\alpha^3\}$ such that $F_3(A_1) \neq F_3(A_4)$, and proceed as before. Eventually we shall arrive at a set $\{c_\alpha\}$ such that the function (6.7) has the asserted property, that is, the

numbers $F(A)$ are distinct. Comparing with the proof of Theorem 6.2 we infer the following fundamental property of the function $N_A(\alpha)$.

THEOREM 6.3. *Any function $H(A)$ with values in the rational field can be exhibited as a polynomial in $N_A(\alpha)$, $\alpha \neq 0$, with rational coefficients and of degree $< w$.*

Alternatively $H(A)$ can be expressed as a polynomial in $M(\beta A)$, but the coefficients need not be rational.

In view of Theorem 6.3, the set of invariants $N_A(\alpha)$, $\alpha \neq 0$, may be called a *fundamental* set. The same remark applies to the set $M(\beta A)$, $\beta \neq 0$.

7. **Reducibility.** A polynomial $f(\xi_1, \cdots, \xi_r)$ is *reducible* if it is equivalent to a sum

$$g(\eta_1, \cdots, \eta_s) + h(\eta_{s+1}, \cdots, \eta_r), \tag{7.1}$$

where $g$ and $h$ are each of rank $\geqq 1$; otherwise it is *irreducible*. A class is reducible if it consists of reducible polynomials.

To derive a criterion for irreducibility note that the definition implies

$$N_f(\alpha) = \sum_{\beta+\gamma=\alpha} N_g(\beta) N_h(\gamma) \tag{7.2}$$

which is equivalent to

$$M(\gamma f) = M_s(\gamma g) M_{r-s}(\gamma h) \qquad (\gamma \neq 0), \tag{7.3}$$

where $M_s(g) = \sum_{\xi_1, \cdots, \xi_s} e(g(\xi))$.

We recall that by (3.4)

$$m(\gamma) = M(\gamma f) = \sum_{\alpha} e(\alpha\gamma) N_f(\alpha), \tag{7.4}$$

where the notation $m(\gamma)$ indicates that $f$ is fixed. When $\gamma = 0$ we have

$$m(0) = M(0) = \sum_{\alpha} N_f(\alpha) = q^r.$$

Put $\rho = e^{2\pi i/p}$ and let $Z$ denote the field $R(\rho)$, where $R$ is the rational field. Thus $m(\gamma)$ is an algebraic integer in $Z$. Since, by (2.2), $e(\alpha\gamma)$ is some power of $\rho$ for all $\alpha$ it follows that

$$m(\gamma) \equiv m(0) \equiv 0 \pmod{1 - \rho}.$$

In other words $m(\gamma)$ is divisible by the prime ideal $\mathfrak{p} = (1-\rho)$. Thus (7.3) implies the following sufficient condition for irreducibility.

THEOREM 7.1. *If $m(\gamma) \not\equiv 0 (\mathfrak{p}^2)$ for at least one value of $\gamma$, then $f$ is irreducible.*

It is now easy to exhibit irreducible polynomials. Consider the polynomial

$$f = (1 - \xi_1^{q-1}) \cdots (1 - \xi_r^{q-1}). \tag{7.5}$$

We shall compute

$$m(1) = M(f) = \sum_{\xi_1, \cdots, \xi_r} e\{(1 - \xi_1^{q-1}) \cdots (1 - \xi_r^{q-1})\}. \tag{7.6}$$

It is clear from (7.5) that

$$f = \begin{cases} 1 & ((\xi_1, \cdots, \xi_r) = (0, \cdots, 0)), \\ 0 & ((\xi_1, \cdots, \xi_r) \neq (0, \cdots, 0)). \end{cases}$$

Thus (7.6) becomes

$$m(1) = (q^r - 1) + p^n; \tag{7.7}$$

since $(q) = (p^n) = \mathfrak{p}^{n(p-1)}$, it is evident that (7.7) implies $m(1) \not\equiv 0(\mathfrak{p}^2)$ provided $p \nmid n$. This proves

THEOREM 7.2. *The polynomial* (7.5) *is irreducible provided* $p \nmid n$.

The same argument proves the following more general result.

THEOREM 7.3. *Let* $f$ *be a polynomial such that* $f=0$ *has* $N_0$ *solutions and* $f=1$ *has* $N_1$ *solutions where* $N_0+N_1=q^r$. *Then if* $(q, N_1)=1$ *and* $p \nmid n$ *it follows that* $f$ *is irreducible.*

Returning to (7.3) and making use of Theorem 3.5 we can state a necessary and sufficient condition for reducibility.

THEOREM 7.4. *The polynomial* $f$ *is reducible if and only if there exist sets of non-negative integers* $m_1(\alpha)$, $m_2(\alpha)$ *satisfying*

$$\begin{aligned} m(\gamma) &= \sum_{\alpha} e(\alpha\gamma) m_1(\alpha) \sum_{\beta} e(\beta\gamma) m_2(\gamma) && (\gamma \not\equiv 0), \\ \sum_{\alpha} m_1(\alpha) &= q^s, \qquad \sum_{\beta} m_2(\beta) = q^{r-s} && (1 \leqq s < r). \end{aligned} \tag{7.8}$$

Alternatively, we may get a similar criterion by means of (7.2) and Theorem 3.5. We state

THEOREM 7.5. *Using the notation of the last theorem,* $f$ *is reducible if and only if*

$$N_f(\alpha) = \sum_{\beta+\gamma=\alpha} m_1(\beta) m_2(\gamma). \tag{7.9}$$

In proving these theorems it is only necessary to observe that, by Theorem 3.5, the condition $\sum_\alpha m_1(\alpha) = q^s$ implies the existence of a polynomial $g(\xi_1, \cdots, \xi_s)$ such that $N_g(\alpha) = m_1(\alpha)$, where in counting the number of solutions only the first $s$ unknowns are considered.

Theorem 7.5 may be compared with Theorem 4.9.

Repeated application of (7.1) evidently leads to a decomposition

$$f \sim g_1 + \cdots + g_s \qquad (g_i = g_i(\xi_{i1}, \cdots, \xi_{ir_i})), \tag{7.10}$$

where $r_i \geqq 1$, $\sum r_i = r$; no two of the $g$'s have any common unknowns. Moreover each $g$ is irreducible and of rank $\geqq 1$. A natural question is whether the decomposition (7.10) is unique, that is, whether a second decomposition into irreducible components $f \sim h_1 + \cdots + h_t$ implies $s = t$ and (possibly after renumbering) $h_i \sim g_i$ for $i = 1, \cdots, s$. Some restriction on the $g_i$ is necessary since we may obviously add and subtract constants; we may for example assume that $f$ and all the $g_i$ vanish at $(0, \cdots, 0)$. It is also necessary to take into account such equivalences as $\xi_1 + g(\xi_2, \cdots, \xi_r) \sim \xi_1$. We hope to discuss the question of unique decomposition on a later occasion.

8. **Additional properties of $M(f)$.** It is an immediate consequence of (2.4) that

$$\sum_f M(f) = \sum_A \mu(A) M(A) = 0, \tag{8.1}$$

where $\mu(A)$ is the number of polynomials in the class $A$. We have also

$$\sum_f{}' M(f) = q^{q^r - 1}, \tag{8.2}$$

where the summation in (8.2) is restricted to all $f$ without constant term. To prove (8.2) it is necessary to examine only the terms of first degree in $f$:

$$f = \alpha_1 \xi_1 + \cdots + \alpha_r \xi_r + \cdots .$$

Summing over $\alpha_i$ it follows from (2.3) that $\xi_i = 0$ so that the left member of (8.2) reduces to the number of $f$ without constant term.

In the next place consider

$$\sum_f | M(f) |^2 = \sum_A \mu(A) | M(A) |^2. \tag{8.3}$$

We have

$$\sum_f | M(f) |^2 = \sum_{\xi_i} \sum_{\eta_i} \sum_f e(f(\xi) - f(\eta)).$$

Examining the terms of first degree as in the proof of (8.2), we see that the innermost sum vanishes unless $\xi_i = \eta_i$. Thus the multiple sum reduces to

$$\sum_{\xi_i} \sum_f 1 = q^r q^{q^r}.$$

This proves

$$\sum_f | M(f) |^2 = q^r q^{q^r}, \tag{8.4}$$

so that *on the average* $| M(f) |$ is $q^{r/2}$. Indeed (8.4) implies a bit more. Let $N$ be

the number of polynomials $f$ such that

$$M(f) \geqq \eta q^{(r+\epsilon)/2} \qquad (\eta > 0,\ \epsilon > 0). \tag{8.5}$$

Then by (8.4) and (8.5), $q^{rq^r} \geqq N\eta^2 q^{r+\epsilon}$, so that

$$N \leqq \frac{q^{q^r}}{\eta^2 q^{\epsilon}}. \tag{8.6}$$

This proves the following theorem:

THEOREM 8.1. *Let* $\epsilon > 0$, $\eta > 0$. *If* $N$ *is the number of polynomials for which* (8.5) *holds, then* $N$ *satisfies* (8.6).

In other words, if $q$ is large and $r$ fixed, then for "almost all" polynomials we have

$$M(f) = O(q^{(r+\epsilon)/2}), \tag{8.7}$$

where $O$ has its usual meaning. However (8.7) need not hold for some $f$. To take a trivial example, if $f$=constant then $|M(f)| = q^r$. Again for the special polynomial (7.5) we have seen that

$$M(f) = q^r - 1 + p^n,$$

which contradicts (8.7). Other examples of this sort are easily constructed. On the other hand for certain polynomials not only (8.7) but the stronger result

$$M(f) = O(q^{r/2}) \tag{8.8}$$

can be asserted. For example (8.8) holds (in more precise form) when $f$ is an ordinary quadratic form.

One or two additional examples may be mentioned. For example, for the polynomial $f = \xi_1 \cdots \xi_r$ we have

$$M(f) = \sum_{\xi_2, \cdots, \xi_r} \sum_{\xi_1} e(\xi_1 \xi_2 \cdots \xi_r).$$

The inner sum vanishes unless $\xi_2 \cdots \xi_r = 0$. This will happen $q^{r-1} - (q-1)^{r-1}$ times. It follows that

$$M(f) = q(q^{r-1} - (q-1)^{r-1}) = (r-1)q^{r-1} + \cdots,$$

so that $M(f)$ is of order $q^{r-1}$. Then for $r > 3$, (8.7) is not satisfied. A similar example is furnished by $f = \xi_1^2 \cdots \xi_r^2$. In this instance we have

$$\begin{aligned} M(f) &= \sum_{\xi_2 \cdots \xi_r = 0} \sum_{\xi_1} 1 + \sum_{\xi_2 \cdots \xi_r \neq 0} \sum_{\xi_1} e(\xi_1^2 \cdots \xi_r^2) \\ &= q(q^{r-1} - (q-1)^{r-1}) + (q-1)^{r-1} S, \end{aligned} \tag{8.9}$$

where $S$ is the Gauss sum [2, §3]

$$S = \sum_{\xi} e(\xi^2), \qquad |S| = q^{1/2}. \tag{8.10}$$

It follows from (8.9) and (8.10) that $M(f)$ is of order $q^{r-1/2}$. Somewhat similar results can be obtained for

$$f = \xi_1^{e_1} \cdots \xi_r^{e_r} \qquad (e_i \geqq 0).$$

It should be remarked that while $M(f)$ is a class invariant it is not an invariant of a category. For example, if $q=p>2$ and $r=1$, consider the category containing the polynomial $\xi^2$. The partition defining the category (compare the example following Theorem 5.1) is evidently $[2 \cdots 21]$. Now define $f(\xi)$ as follows:

$$f(0) = 0, \qquad f(2s) = f(2s-1) = 2s-1 \qquad (1 \leqq s \leqq (p-1)/2).$$

Then we have

$$M(f) = 1 + 2\sum_{s=1}^{(p-1)/2} \rho^{2s-1} = 1 + 2\rho\,\frac{1-\rho^{p-1}}{1-\rho^2} = \frac{\rho-1}{\rho+1},$$

from which it is evident that

$$M(f) = o(1) \qquad (p \to \infty). \tag{8.11}$$

On the other hand, by (8.10), $|M(\xi^2)| = q^{1/2}$.

Incidentally (8.11) furnishes an example of a polynomial with $M(f)\to 0$ but $M(f)\neq 0$. The restriction $q=p$ is not essential and other examples of the same kind can easily be constructed.

While $M(f)$ is not an invariant of a category the functions $\mu(f)$ and $\nu(f)$ are invariants. If we use the fuller notation

$$[k_1^{e_1} k_2^{e_2} \cdots k_s^{e_s}] \qquad (k_1 > k_2 > \cdots > k_s \geqq 1;\ e_i \geqq 1) \tag{8.12}$$

for the partition defining a category $K$, then (5.3) furnishes the number of classes in $K$. Consequently the total number of polynomials in the category is

$$\frac{q!}{e_0!e_1!\cdots e_s!}\,\frac{q^r!}{(k_1!)^{e_1}\cdots(k_s!)^{e_s}}. \tag{8.13}$$

THEOREM 8.2. *The number of polynomials in the category defined by the partition* (8.12) *is given by* (8.13).

9. **Some applications.** Consider a polynomial $f$ that has the property:

$$N_f(\alpha) = l \qquad \text{for all } \alpha \neq 0. \tag{9.1}$$

If we put $N_f(0)=l_0$, then (9.1) implies

$$l_0 + (q-1)l = q^r. \tag{9.2}$$

Hence by (3.4)

$$M(\gamma f) = l_0 + l\sum_{\alpha\neq 0} e(\alpha\gamma). \tag{9.3}$$

It is convenient at this point to define a function

$$k(\alpha) = \begin{cases} q-1 & (\alpha = 0), \\ -1 & (\alpha \neq 0). \end{cases} \tag{9.4}$$

Then (9.3) becomes

$$M(\gamma f) = l_0 + lk(\gamma) \tag{9.5}$$

and using (9.2) this yields

$$M(\gamma f) = \begin{cases} q^r & (\gamma = 0), \\ q^r - ql & (\gamma \neq 0). \end{cases} \tag{9.6}$$

Conversely, given (9.6), then (3.2) implies

$$\begin{aligned} N_f(\alpha) &= q^{-1}M(0) + q^{-1}M(1)\sum_{\gamma\neq 0} e(-\alpha\gamma) \\ &= q^{r-1} + (q^{r-1} - l)k(\alpha) \\ &= \begin{cases} l_0 & (\alpha = 0), \\ l & (\alpha \neq 0); \end{cases} \end{aligned}$$

in other words $f$ satisfies (9.1). This proves

THEOREM 9.1. *A polynomial $f$ satisfies* (9.1) *if and only if it satisfies* (9.6).

Condition (9.1) is satisfied when $f$ is a quadratic form in $r=2s$ variables with discriminant $\delta\neq 0$ and $q$ odd. Let $\psi(\alpha)=0, +1, -1$ according as $\alpha=0$, square, or nonsquare of $GF(q)$. Then as is familiar

$$N_f(\alpha) = q^{2s-1} + q^{s-1}k(\alpha)\psi((-1)^s\delta) \tag{9.7}$$

so that

$$l = q^{2s-1} - q^{s-1}\psi((-1)^s\delta). \tag{9.8}$$

Thus in this case (9.6) becomes

$$M(\gamma f) = q^s\psi((-1)^s\delta) \qquad (\gamma \neq 0).$$

When $r=2s+1$, then in place of (9.7) we have

$$N_f(\alpha) = q^{2s} + q^s\psi((-1)^s\alpha\delta). \tag{9.9}$$

This suggests consideration of polynomials $f$ having the property

$$N_f(\alpha) = l_0 + l\psi(\alpha). \tag{9.10}$$

Summing over $\alpha$ we get $l_0 = q^{r-1}$. Application of (3.4) yields

$$M(\gamma f) = l\psi(\gamma)S \qquad (\gamma \neq 0), \tag{9.11}$$

where $S$ is the Gauss sum defined by (8.10). Conversely if (9.11) holds, then (3.2) implies

$$\begin{aligned} N_f(\alpha) &= q^{r-1} + q^{-1}lS \sum_{\beta \neq 0} e(-\alpha\beta)\psi(\beta) \\ &= q^{r-1} + q^{-1}lS^2\psi(-\alpha) = q^{r-1} + l\psi(\alpha). \end{aligned}$$

This proves

THEOREM 9.2. *A polynomial satisfies $N_f(\alpha) = q^{r-1} + l\psi(\alpha)$, where $l$ is independent of $\alpha$ if and only if it satisfies* (9.11).

If $f$ satisfies (9.1), $r = 2s$, and $l$ is defined by (9.8), then, by Theorem 7, $f$ is equivalent to a quadratic form in $2s$ variables with discriminant $\delta$. In the same way if $f$ satisfies (9.10) with $r = 2s+1$ and

$$l = q^s\psi((-1)^s\delta), \tag{9.12}$$

then $f$ is equivalent to a quadratic form in $2s+1$ variables with the discriminant $\delta$. We may state

THEOREM 9.3. *A necessary and sufficient condition that a polynomial be equivalent to a quadratic form of discriminant $\delta$ is furnished by* (9.1) *and* (9.8) *when $r = 2s$, and by* (9.10) *and* (9.12) *when $r = 2s+1$.*

We may mention an example of a different kind that also falls under (9.1). The writer has proved the following result [1, Theorem 4]. Given the equation

$$\sum_{i=1}^{s} \alpha_i \prod_{j=1}^{r_i} \xi_{ij}^{a_{ij}} = \alpha \qquad (\alpha_i \neq 0), \tag{9.13}$$

where

$$(a_{i1}, \cdots, a_{ir_i}) = 1 \qquad (i = 1, \cdots, s) \tag{9.14}$$

and the $r_i$ are arbitrary integers $\geqq 1$. Then the number of solutions $\xi_{ij}$ of (9.13) is

$$q^{r-1} + q^{-1}k(\alpha) \prod_{i=1}^{s} (q^{r_i} - q(q-1)^{r_i-1}), \tag{9.15}$$

where $r = r_1 + \cdots + r_s$ and $k(\alpha)$ is defined in (9.4). To compare (9.15) with (9.1) we note first that $r$ has the same meaning in both cases. Thus we have

$$l_0 = q^{r-1} + q^{-1}(q-1)W, \qquad l = q^{r-1} - q^{-1}W,$$

where $W$ stands for the product in (9.15).

The result (9.15) is particularly simple when all $r_i=2$. We then find that the number of solutions of

$$\alpha_1\xi_1^{a_1}\eta_1^{b_1}+\cdots+\alpha_s\xi_s^{a_s}\eta_s^{b_s}=\alpha \qquad ((a_i, b_i)=1) \tag{9.16}$$

is

$$q^{2s-1}+q^{s-1}k(\alpha). \tag{9.17}$$

Comparing (9.17) with (9.7) it follows at once by Theorem 7 that the polynomial in the left member of (9.16) is equivalent to an ordinary quadratic form with $\psi((-1)^s\delta)=+1$.

Returning to the general case (9.13), we observe that (9.15) is independent of the coefficients $\alpha_i$ and the exponents $a_{ij}$. Consequently Theorem 4.1 implies the following

THEOREM 9.4. *The polynomials*

$$\sum_{i=1}^{s}\alpha_i\prod_{j=1}^{r_i}\xi_{ij}^{a_{ij}} \qquad (\alpha_i\neq 0), \tag{9.18}$$

*where the $a_{ij}$ satisfy* (9.14) *and the $r_i$ are fixed, are all equivalent. In particular when all $r_i=2$, the polynomials* (9.18) *are equivalent to a quadratic form with* $\psi((-1)^s\delta)=+1$.

By Theorem 4.9, the rank of (9.18) is $r-s+1$ provided all $r_i>1$.

Another example that falls under (9.1) depends upon the following result of Fine and Niven [8]: Let $\Delta$ denote the determinant $|\xi_{ij}|$ of order $s$ in the $s^2$ letters $\xi_{ij}$. Then the number of solutions of the equation $\Delta=\alpha$ is given by

$$N_\Delta(\alpha)=q^{s^2-1}+q^{s^2-1}k(\alpha)\left\{1-\frac{q}{q-1}\prod_{i=1}^{s}(1-q^{-i})\right\}. \tag{9.19}$$

By Theorem 4.8 the rank of $\Delta$ is $s(s+1)/2$.

It may be of interest to remark that if a polynomial satisfies

$$f(\eta\xi_1, \cdots, \eta\xi_r)=\eta^s f(\xi_1, \cdots, \xi_r) \qquad ((s, q-1)=1), \tag{9.20}$$

then it also satisfies (9.1). The condition (9.20) is a kind of homogeneity condition and in view of $(s, q-1)=1$ might seem to imply linearity; however even when $s=1$ this is not necessarily the case.

Now assuming (9.20), we have for $\gamma\neq 0$,

$$\begin{aligned} M(\gamma^s f) &= \sum_{\xi_1,\cdots,\xi_r} e(\gamma^s f(\xi_1, \cdots, \xi_r)) \\ &= \sum_{\xi_1,\cdots,\xi_r} e(f(\gamma\xi_1, \cdots, \gamma\xi_r)) \\ &= \sum_{\xi_1,\cdots,\xi_r} e(f(\xi_1, \cdots, \xi_r)) = M(f), \end{aligned}$$

so that $M(\gamma f) = M(f)$ for all $\gamma \neq 0$. Consequently by Theorem 9.1, $f$ satisfies (9.1).

Similarly if a polynomial satisfies

$$f(\eta\xi_1, \cdots, \eta\xi_r) = \eta^s f(\xi_1, \cdots, \xi_r) \qquad ((s, q-1) = 2), \tag{9.21}$$

then if $\psi(\beta) = +1$, we have

$$M(\beta f) = M(\gamma^s f) = M(f)$$

as above, while if $\psi(\beta) = -1$, $M(\beta\gamma^s f) = M(\beta f)$. Thus it follows from (3.2) that

$$q^r((q-1)/2)(M(f) + M(\beta f)) = qN_f(0) \qquad (\psi(\beta) = -1).$$

If in addition we assume $N_f(0) = q^{r-1}$, then (9.11) holds. This proves

THEOREM 9.5. *If a polynomial satisfies* (9.20), *then it also satisfies* (9.1). *If a polynomial satisfies* (9.21) *and in addition* $N_f(0) = q^{r-1}$, *then it satisfies* (9.11).

10. **Other applications.** If $N_f(\alpha)$ is known and $f \sim g$, then $N_g(\alpha)$ is also known. Theoretically this should enable us to determine $N_f(\alpha)$ for a variety of polynomials derived from a few standard ones. In practice however it does not seem easy to construct interesting examples.

Let $g(\xi_1, \cdots, \xi_s)$ denote a polynomial that never takes on the value 0, and consider the set of equations

$$\eta_s = g_{s-1}(\xi_1, \cdots, \xi_{s-1})\xi_s \qquad (s = 1, \cdots, r), \tag{10.1}$$

where $g_0 = 1$. Clearly (10.1) defines a transformation (1.1). Hence applying (10.1) to the quadratic form, $Q(\eta_1, \cdots, \eta_r)$, we infer that the number of solutions of

$$Q(\xi_1, g_1(\xi_1)\xi_2, \cdots, g_{r-1}(\xi_1, \cdots, \xi_{r-1})\xi_r) = \alpha \tag{10.2}$$

is given by (9.7) or (9.9) according as $s = 2r$ or $2r+1$. When the hypothesis $g_s \neq 0$ is weakened it may still be possible to find the number of solutions of (10.2); however we shall not discuss that problem at present. The transformation (10.1) may also be applied to the other results of §9.

In view of (10.2) one is led to consider such equations as

$$\alpha_1\xi_1^2 + \alpha_2 g_1(\xi_1)\xi_2^2 + \cdots + \alpha_r g_{r-1}(\xi_1, \cdots, \xi_{r-1})\xi_r^2 = \alpha, \tag{10.3}$$

where as above the $g_s$ never vanish. If we specialize further, we can determine the number of solutions in simple form. For example consider the special case

$$Q_1(\xi_1, \cdots, \xi_{2s}) + g(\xi_1, \cdots, \xi_{2s})Q_2(\eta_1, \cdots, \eta_{2t}) = \alpha, \tag{10.4}$$

where $Q_1$, $Q_2$ denote quadratic forms and $g$ does not vanish. Clearly the number of solutions of (10.4) is

$$\sum_{\beta+\gamma=\alpha} \sum_{A_1(\xi)=\beta} \sum_{g(\xi)Q_2(\eta)=\gamma} 1. \tag{10.5}$$

Since $g(\xi_1, \cdots, \xi_{2s}) \not\equiv 0$ for any choice of $\xi_i$, a glance at (9.7) shows that the innermost sum is precisely the number of solutions of $Q_2(\eta)=\gamma$. Thus (10.5) becomes

$$\begin{aligned}\sum_{\beta+\gamma=\alpha} \sum_{Q_1(\xi)=\beta} \sum_{Q_2(\eta)=\gamma} 1 &= N_{Q_1+Q_2}(\alpha) \\ &= q^{2s+2t-1} + q^{s+t-1}k(\alpha)\psi((-1)^{s+t}\delta_1\delta_2),\end{aligned} \tag{10.6}$$

where $\delta_1$, $\delta_2$ are the discriminants of $Q_1$, $Q_2$, respectively. We now state

THEOREM 10.1. *The number of solutions of* (10.4) *is determined by* (10.6). *Moreover the left member of* (10.4) *is equivalent to a quadratic form in* $2s+2t$ *variables of discriminant* $\delta_1\delta_2$.

The second part of the theorem is of course a consequence of Theorem 4.1. Once again, as in §9, we have determined the number of solutions of a certain problem and then inferred equivalence. It is not difficult to generalize (10.4) considerably; also one may consider the case in which the quadratic form contains an odd number of variables.

Even when $N_f(\alpha)$ is not known for all $\alpha$, application of a transformation to $f$ may lead to interesting results. For example, it follows from a result of Hua and Vandiver [9, Theorem 2] that the number of solutions of

$$\alpha_1\xi_1^{e_1} + \cdots + \alpha_r\xi_r^{e_r} = 0, \tag{10.7}$$

where $(e_i, e_j)=1$, is $q^{r-1}$. Consequently applying (10.1) it follows that the number of solutions of

$$\alpha_1\xi_1^{e_1} + \alpha_2 g_1^{e_2}(\xi_1)\xi_2^{e_2} + \cdots + \alpha_r g_{r-1}^{e_r}(\xi_1, \cdots, \xi_{r-1})\xi_r^{e_r} = 0$$

is also $q^{t-1}$.

A similar remark applies to a number of other special results. For example the equation [3, Theorem 7]

$$Q(\xi_1, \cdots, \xi_r) = \eta^k \qquad (k \geqq 1,\ p \neq 2) \tag{10.8}$$

may be cited. The number of solutions of (10.8) is $q^r$ for $r$ even or $r$ odd and $k$ odd, while for $r=2s+1$, $k$ even the number of solutions is

$$q^{2s+1} + q^s(q-1)\psi((-1)^s\delta).$$

The same therefore is true of

$$Q(\xi_1, \cdots, \xi_r) = \eta^k g(\xi_1, \cdots, \xi_r)$$

and more generally of

$$Q(\xi_1, g_1\xi_2, \cdots, g_{r-1}\xi_r) = \eta^k g(\xi_1, \cdots, \xi_r),$$

where the $g$'s have the same meaning as above. More elaborate examples of this kind can easily be constructed. In particular this applies to the determinantal equation $\Delta = \alpha$ cited at the end of §9 as well as a recent paper by O. B. Faircloth [7] concerning the number of solutions of the equation

$$\alpha_1\xi_1^{e_1} + \cdots + \alpha_r\xi_r^{e_s} = \alpha.$$

Returning to (10.1) we may remark that the equation

$$\eta_s = \xi_s + h_{s-1}(\xi_1, \cdots, \xi_{s-1}) \qquad (s = 1, \cdots, r), \tag{10.9}$$

where $h_0 = 0$ and $h_1, \cdots, h_{r-1}$ are arbitrary polynomials, also defines a transformation. Thus (10.9) can be used in place of (10.1) in some of the above results.

## References

1. L. Carlitz, *The number of solutions of certain equations in a finite field*, Proc. Nat. Acad Sci. U.S.A. vol. 38 (1952) pp. 515–519.

2. ———, *The singular series for sums of squares of polynomials*, Duke Math. J. vol. 14 (1947) pp. 1105–1120.

3. ———, *Some special equations in a finite field*, Pacific Journal of Mathematics vol. 3 (1953) pp. 13–24.

4. C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Hansischen Univ. vol. 11 (1936) pp. 73–75.

5. L. E. Dickson, *General theory of modular invariants*, Trans. Amer. Math. Soc. vol. 10 (1909) pp. 123–158.

6. ———, *A theory of invariants*, Amer. J. Math. vol. 31 (1909) pp. 337–354.

7. O. B. Faircloth, *On the number of solutions of some general types of equations in a finite field*, Canadian Journal of Mathematics vol. 4 (1952) pp. 343–351.

8. N. J. Fine and I. Niven, *The probability that a determinant be congruent to a* (mod $m$), Bull. Amer. Math. Soc. vol. 50 (1944) pp. 89–93.

9. L. K. Hua and H. S. Vandiver, *On the nature of the solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. vol. 35 (1941) pp. 481–487.

10. E. Netto, *Lehrbuch der Combinatorik*, Leipzig and Berlin, 1927.

11. D. E. Rutherford, *Modular invariants*, Cambridge, 1932.

12. A. L. Whiteman, *Finite Fourier series and cyclotomy*, Proc. Nat. Acad. Sci. U.S.A. vol. 37 (1951) pp. 373–378.

13. ———, *Finite Fourier series and equations in a finite field*, Trans. Amer. Math. Soc. vol. 74 (1953) pp. 78–98.

Duke University,
Durham, N. C.