A NOTE ON NONSINGULAR FORMS IN A FINITE FIELD

L. CARLITZ

1. Let \( q = p^n, p > 2, r \) a fixed integer \( \geq 1 \). The writer has shown [1, Theorem 8.3] that one can construct quadratic forms \( Q_1, \ldots, Q_r \)

\[ Q_h(x) = \sum_1^r \alpha_{hij}x_ix_j \quad (\alpha_{hij} \in GF(q)), \]

such that

\[ \text{det}(\xi_1Q_1 + \cdots + \xi_rQ_r) \neq 0 \]

for arbitrary \( (\xi_1, \ldots, \xi_r) \neq (0, \ldots, 0) \), \( \xi_i \in GF(q) \). This result suggests the possibility of finding \( r \) homogeneous forms \( f_1, \ldots, f_r \) of degree \( m \), where \( (q, m) = 1 \) such that \( f_1, \ldots, f_r \) vanish simultaneously only at \( (0, \ldots, 0) \), and secondly

\[ f = \xi_1f_1 + \cdots + \xi_rf_r \quad (\xi_i \in GF(q)) \]

has no singular point (except at \( (0, \ldots, 0) \)) for arbitrary \( \xi_i \) not all zero.

To construct such forms let \( \beta \) be a number of \( GF(q^r) \) such that \( \beta, \beta^q, \ldots, \beta^{q^{r-1}} \) are linearly independent relative to \( GF(q) \); Hensel first proved the existence of such \( \beta \). Now put

\[ \phi_i(x) = \sum_{j=1}^r \beta^{s_{ij}}x_j^m \quad (i = 1, \ldots, r). \]

Let \( \gamma_1, \ldots, \gamma_r \) be numbers of \( GF(q^r) \) that are linearly independent relative to \( GF(q) \) and put

\[ x_j = \sum_{k=1}^r \gamma_k^{s_{jk}}y_k \quad (j = 1, \ldots, r). \]

Define \( f_i(y) \) by means of

\[ f_i(y) = \phi_i(x) \quad (i = 1, \ldots, r). \]

Then in the first place

Received by the editors December 24, 1954.

27
\[ f_i(y) = \phi_i(x) = \sum_j \beta^{q^{i+j}} \left( \sum_k \gamma_k^{q^j} y_k \right)^m \\
= \sum_j \beta^{q^{i+j}} \left( \sum_k \gamma_k^{q^j} y_k \right)^m \\
= f_i(y^q), \]
so that the coefficients of \( f_i(y) \) are in \( GF(q) \).

Now assume that
\[ f_1(y) = \cdots = f_r(y) = 0 \]
for some \((y_1, \cdots, y_r)\). Then by (4) and (6), (7) implies
\[ \sum_{i=1}^r \beta^{q^{i+j}} x_i^m = 0 \quad (i = 1, \cdots, r). \]

But since \( \beta, \beta^q, \cdots, \beta^{q^{r-1}} \) are linearly independent we have that the determinant
\[ \det (\beta^{q^{i+j}}) \neq 0. \]

Consequently (8) implies \( x_1 = \cdots = x_r = 0 \) and therefore (7) holds only for \( y_1 = \cdots = y_r = 0 \).

Consider next the form \( f(y) \) defined by (3). We have
\[ \frac{\partial f(y)}{\partial y_i} = \sum_{i,k} \xi_i \frac{\partial \phi_i(x)}{\partial x_k} \frac{\partial x_k}{\partial y_i} = m \sum_{i,k} \xi_i \beta^{q^{i+k}} x_k^{m-1} \gamma_i. \]

We assume that
\[ \frac{\partial f(y)}{\partial y_i} = 0 \quad (i = 1, \cdots, r) \]
for some \((y_1, \cdots, y_r) \neq (0, \cdots, 0)\). If we put
\[ \eta_k = \sum_i \xi_i \beta^{q^{i+k}}, \]
then (10) and (11) imply
\[ \sum_k \eta_k x_k^{m-1} \gamma_i = 0 \quad (i = 1, \cdots, r). \]

But the linear independence of \( \gamma_1, \cdots, \gamma_r \) is equivalent to the non-vanishing of the determinant \( \det (\gamma_i^k) \); thus (12) implies
\[ \eta_k x_k^{m-1} = 0 \quad (k = 1, \cdots, r). \]

Since not all \( x_k \) vanish it follows that
for at least one value of \( k \). But since \( \xi \in GF(q) \), raising (13) to the \( q \)th power it follows that (13) holds for all \( k = 1, \ldots, r \). But in view of (9) this implies \( \xi_1 = \cdots = \xi_r = 0 \).

We have therefore proved the following

**Theorem 1.** Let \( (q, m) = 1, r \geq 1 \). There exist homogeneous polynomials \( f_1, \ldots, f_r \) of degree \( m \) with coefficients in \( GF(q) \), that vanish simultaneously only at \( (0, \ldots, 0) \) and such that

\[
\sum_i \xi_i \beta^{i+k} = 0
\]

has no singular point (except at \( (0, \ldots, 0) \)).

The condition \( \xi \in GF(q) \) is evidently essential.

2. Returning to the case of quadratic forms, the result in (2) cannot be improved. For given \( r+1 \) quadratic forms, then

\[
\det (\xi_0 Q_1 + \cdots + \xi_{r+1} Q_{r+1})
\]

is a polynomial of degree \( r \) in the \( \xi \). Consequently by a well known theorem of Chevalley [2], the determinant (14) vanishes for some \( (\xi_1, \cdots, \xi_{r+1}) \neq (0, \cdots, 0) \).

For the case of arbitrary forms of degree \( m \) let us take

\[
f(y) = \xi_1 f_1(y) + \cdots + \xi_r f_r(y) \quad (\xi_i \in GF(q))
\]

and consider the Hessian

\[
H_f = \det (\partial^2 f / \partial y_i \partial y_j) \quad (i, j = 1, \cdots, r)
\]

as a polynomial in the \( \xi \)'s, \( H_f \) is of degree \( r(m - 2) \). Hence if

\[
s > r(m - 2)
\]

Chevalley's theorem applies. We may state

**Theorem 2.** Let \( f_1(y), \ldots, f_s(y) \) be arbitrary homogeneous polynomials of degree \( m \) with coefficients in \( GF(q) \) and let (17) hold. Then for arbitrary \( y_i \in GF(q) \) there exist \( \xi_i \in GF(q) \) such that the Hessian \( H_f \) vanishes at \( (y_1, \cdots, y_r) \).

**References**