A NOTE ON NONSINGULAR FORMS IN A FINITE FIELD

L. CARLITZ

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

$$Q_h(x) = \sum_1^r \alpha_{hij} x_i x_j \qquad (\alpha_{hij} \in GF(q)), \tag{1}$$

such that

$$\det (\xi_1 Q_1 + \cdots + \xi_r Q_r) \neq 0 \tag{2}$$

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

$$f = \xi_1 f_1 + \cdots + \xi_r f_r \qquad (\xi_i \in GF(q)) \tag{3}$$

has no singular point (except at $(0, \cdots, 0)$) for arbitrary ξ_i not all zero.

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

$$\phi_i(x) = \sum_{j=1}^r \beta^{q^{i+j}} x_j^m \qquad (i = 1, \cdots, r). \tag{4}$$

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

$$x_j = \sum_{k=1}^r \gamma_k^{q^j} y_k \qquad (j = 1, \cdots, r). \tag{5}$$

Define $f_i(y)$ by means of

$$f_i(y) = \phi_i(x) \qquad (i = 1, \cdots, r). \tag{6}$$

Then in the first place

Received by the editors December 24, 1954.

$$f_i^q(y) = \phi_i^q(x) = \sum_j \beta^{q^{i+j+1}} \left(\sum_k \gamma_k^{q^{j+1}} y_k^q \right)^m$$
$$= \sum_j \beta^{q^{i+j}} \left(\sum_k \gamma_k^{q^j} y_k^q \right)^m$$
$$= f_i(y^q),$$

so that the coefficients of $f_i(y)$ are in $GF(q)$.

Now assume that

$$f_1(y) = \cdots = f_r(y) = 0 \tag{7}$$

for some $(y_1, \cdots, y_r)$. Then by (4) and (6), (7) implies

$$\sum_{j=1}^{r} \beta^{q^{i+j}} x_j^m = 0 \qquad (i = 1, \cdots, r). \tag{8}$$

But since $\beta, \beta^q, \cdots, \beta^{q^{r-1}}$ are linearly independent we have that the determinant

$$\det (\beta^{q^{i+j}}) \neq 0. \tag{9}$$

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

$$\frac{\partial f(y)}{\partial y_i} = \sum_{j,k} \xi_j \frac{\partial \phi_j(x)}{\partial x_k} \frac{\partial x_k}{\partial y_i} = m \sum_{j,k} \xi_j \beta^{q^{j+k}} x_k^{m-1} \gamma_i^{q^k}. \tag{10}$$

We assume that

$$\frac{\partial f(y)}{\partial y_i} = 0 \qquad (i = 1, \cdots, r) \tag{11}$$

for some $(y_1, \cdots, y_r) \neq (0, \cdots, 0)$. If we put

$$\eta_k = \sum_j \xi_j \beta^{q^{j+k}},$$

then (10) and (11) imply

$$\sum_k \eta_k x_k^{m-1} \gamma_i^{q^k} = 0 \qquad (i = 1, \cdots, r). \tag{12}$$

But the linear independence of $\gamma_1, \cdots, \gamma_r$ is equivalent to the non-vanishing of the determinant $\det (\gamma_i^{q^k})$; thus (12) implies

$$\eta_k x_k^{m-1} = 0 \qquad (k = 1, \cdots, r).$$

Since not all x_k vanish it follows that

$$\sum_j \xi_j \beta^{q^j+k} = 0 \tag{13}$$

for at least one value of k. But since $\xi_j \in GF(q)$, raising (13) to the qth power it follows that (13) holds for all $k = 1, \cdots, r$. But in view of (9) this implies $\xi_1 = \cdots = \xi_r = 0$.

We have therefore proved the following

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

$$f = \xi_1 f_1 + \cdots + \xi_r f_r \qquad (\xi_i \in GF(q))$$

has no singular point (*except at* $(0, \cdots, 0)$).

The condition $\xi_i \in GF(q)$ 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

$$\det\,(\xi_1 Q_1 + \cdots + \xi_{r+1} Q_{r+1}) \tag{14}$$

is a polynomial of degree r in the ξ. 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

$$f(y) = \xi_1 f_1(y) + \cdots + \xi_s f_s(y) \qquad (\xi_i \in GF(q)) \tag{15}$$

and consider the Hessian

$$H_f = \det\,(\partial^2 f/\partial y_i \partial y_j) \qquad (i, j = 1, \cdots, r) \tag{16}$$

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

$$s > r(m-2) \tag{17}$$

Chevalley's theorem applies. We may state

THEOREM 2. *Let* $f_1(y), \cdots, f_s(y)$ *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

1. L. Carlitz, *Invariant theory of systems of equations in a finite field*, Journal d'Analyse Mathématique vol. 3 (1954) pp. 382–413.

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

DUKE UNIVERSITY