A THEOREM OF DICKSON ON NONVANISHING CUBIC FORMS IN A FINITE FIELD

L. CARLITZ

Dickson stated that a ternary cubic form with coefficients in GF(q), q = p^n, p > 2, that vanishes only for x = y = z = 0, is the norm of a linear form with coefficients in GF(q^3). The proof [2, p. 161, particularly line 15] does not seem adequate. In this note we sketch another proof.

Let f = f(x, y, z) be a homogeneous cubic polynomial with coefficients in GF(q) that vanishes in GF(q) only for x = y = z = 0. Put

(1) \[ f = f_0x^3 + f_1x^2 + f_2x + f_3, \]

where f_j = f_j(x, y) is homogeneous of degree j. Assume first that f_0 \neq 0, so that we may take f_0 = 1; also we assume to begin with that p \neq 3. Then by means of a linear transformation we may suppose that f_1 = 0. Hence consider

(2) \[ f = z^3 + f_2z + f_3. \]

Now for fixed a, b \in GF(q), a, b not both 0, it is clear that f(a, b, z) is irreducible. Consequently its discriminant is a nonzero square of GF(q); that is

(3) \[ D = D(a, b) = - 4f_2^2(a, b) - 27f_3^2(a, b) \]

is a square for all a, b \in GF(q), D = 0 only for a = b = 0. But Dickson [1, Theorem 3] has proved that for q \geq 13, this implies

\[ D(x, y) = C^2(x, y), \]

where C(x, y) is a homogeneous cubic polynomial. Thus (3) becomes

(4) \[ C^2(x, y) = - 4f_2^3(x, y) - 27f_3^3(x, y). \]

Clearly it is necessary that f_3(x, y) be irreducible, for otherwise there exist two number a, b of the field, not both 0, such that f_3(a, b), and therefore f(a, b, 0) = 0. Thus either f_2 = 0 or (f_2, f_3) = (C, f_3) = 1. Leaving the case f_2 = 0 for the moment, we rewrite (4) as

\[ C^2 + 27f_3^2 = - 4f_2^3 \]

and put \( \alpha^2 = -27 \), where \( \alpha \in GF(q^2) \). Then clearly

Received by the editors June 5, 1956 and, in revised form, February 18, 1957.

975
\[ (5) \quad C + \alpha f_3 = 2\beta u^3, \quad C - \alpha f_3 = -2\beta^{-1}v^3, \]

where \( \beta \in GF(q^2) \) and \( u, v \) are linear forms with coefficients in \( GF(q^2) \). Since (5) implies \( C = \beta u^3 - \beta^{-1}v^3, \alpha f_3 = \beta u^3 + \beta^{-1}v^3, f_2 = uv \), (2) becomes

\[ f = z^3 + uvz + \alpha^{-1}\beta u^3 + \alpha^{-1}\beta^{-1}v^3 \]

or

\[ (6) \quad f = z^3 - 3UVz + U^3 + V^3, \]

where \( U, V \) are linear forms in some \( GF(q^k) \). But (6) evidently implies \( f(-U - V) = 0 \), from which it follows that the linear form \( U + V \) has coefficients in \( GF(q^3) \). Indeed if \( -U - V = \lambda x + \mu y \), then

\[ f(x, y, \lambda x + \mu y) = 0 \]

implies \( f(x, 0, \lambda x) = 0 \), so that \( \lambda \in GF(q^3) \); similarly for \( \mu \). Therefore \( f \) is the norm of a linear form in \( GF(q^3) \).

In the excluded case \( f_2 = 0 \), we have

\[ f = z^3 + f_3(x, y). \]

Since \( f_3 \) is irreducible, it is only necessary to consider the case

\[ (7) \quad f = z^3 + ax^3 + by^3 \quad (ab \neq 0), \]

for the occurrence of a term \( x^2y \) or \( xy^2 \) can be treated as in the previous proof. Next we need only consider the case \( q \equiv 1 \mod 3, ab = 1, a \) not a cube of \( GF(q) \). But by a theorem of Hurwitz [3] which may be extended without difficulty to finite fields, the equation

\[ ax^3 + by^3 + z^3 = 0, \]

where \( a, b \) satisfy the stated conditions, has at least one solution with \( xyz \neq 0 \).

Returning to (1), suppose that \( f_0 = 0 \). If a term in \( x^3 \) or \( y^3 \) occurs, the previous proof applies. We need then consider only the case \( f_2 = ax^2y + bxy^2 \), and this obviously leads to a contradiction.

When \( p = 3 \) the above discussion must be modified somewhat. Returning to (1), we may assume \( f_0 = 1 \) but cannot require that \( f_1 = 0 \). If indeed \( f_1 = 0 \), then (4) reduces to

\[ C^2(x, y) = -4f_2^3(x, y), \]

so that \( C \) is the cube of a linear form; this contradicts the requirement that \( C \) vanishes only for \( x = y = 0 \).

Employing the discriminant of (1) we get

\[ (8) \quad -f_1^3f_3 - f_2^3 + f_1^2f_2^2 = C^2. \]
If $f_2 = 0$, (8) becomes $-f_2^2 f_3 = C^2$, which contradicts the irreducibility of $f_3$. We need then consider only the case $f_1 f_2 \neq 0$. By means of a linear transformation we may suppose that $f_1 = x$, $f_2 = ay^2$; then (8) reduces to

$$- a^3 y^6 + a^2 x^2 y^4 - x^3 f_3 = C^2.$$ 

We may take $a = -1$, $C = y^3 - x^2 y + cx^3$, which yields

$$f_3 = cy^3 - xy^2 + cx^2 y + c^2 x^3.$$ 

In (1) take $f_1 = x$, $f_2 = -y^2$, $z = \alpha x + \beta y$. Substituting in $f(x, y, z) = 0$, we obtain the following conditions on $\alpha, \beta$:

$$\alpha^3 + \alpha^2 = c^2, \quad \beta^3 - \beta = c, \quad \alpha \beta = c, \quad \beta^2 - \alpha = 1.$$ 

It is easily verified that this system is equivalent to

$$\beta^3 - \beta = c, \quad \alpha \beta = c.$$  

Clearly (9) implies $\alpha, \beta \in GF(q^3)$. Hence $f(x, y, z)$ has the linear factor $z - \alpha x - \beta y$, and it follows at once that

$$f(x, y, z) = (z - \alpha x - \beta y)(z - \alpha^2 x - \beta^2 y)(z - \alpha^3 x - \beta^3 y).$$ 

In other words, $f(x, y, z)$ is the norm of a linear form with coefficients in $GF(q^3)$; moreover 1, $\alpha, \beta$ are linearly independent with respect to $GF(q)$.

We may state the following

**Theorem.** Let $f(x, y, z)$ be a homogeneous cubic polynomial with coefficients in $GF(q)$ that vanishes in $GF(q)$ only for $x = y = z = 0$. Then if $p > 2$, $q \geq 13$, $f(x, y, z)$ is the norm of a linear form $\alpha x + \beta y + \gamma z$, where $\alpha, \beta, \gamma$ are in $GF(q^3)$ and are linearly independent with respect to $GF(q)$.

The converse of the theorem is evidently true. Possibly the theorem holds for $p = 2$; the above proof obviously does not apply in that case.

**References**


Duke University