NOTE ON FACTORABLE POLYNOMIALS

Kenneth S. Williams

(received August 14, 1968)

Let $X_1, X_2, \ldots, X_k$ denote $k \geq 2$ indeterminates and let $f(X_1, \ldots, X_k)$ be a homogeneous polynomial, in $GF(p^n)[X_1, \ldots, X_k]$, which is irreducible but not absolutely irreducible over $GF(p^n)$. Thus f is irreducible in $GF(p^n)[X_1, \ldots, X_k]$ but reducible in some $GF(p^{nm})[X_1, \ldots, X_k]$, $m > 1$. For any polynomial $h(X_1, \ldots, X_k)$ in $GF(p^{n\ell})[X_1, \ldots, X_k]$, $\ell \geq 1$, let $N_{p^n}(h)$ denote the number of $(x_1, \ldots, x_k) \in GF(p^n) \times \ldots \times GF(p^n)$ such that $h(x_1, \ldots, x_k) = 0$. It follows from the work of Birch and Lewis [1] that

$$N_{p^n}(f) = 0_{k,d}(p^{n(k-2)}) \quad , \tag{1}$$

where $d = \deg f$ and the constant implied by the 0-symbol depends only on k and d. If f factors into linear factors in $GF(p^{nm})[X_1, \ldots, X_k]$, following Carlitz [2], we call such polynomials factorable. In this note we obtain a more precise statement than (1) when f is factorable. We prove

THEOREM 1. If $f(X_1, \ldots, X_k) \in GF(p^n)[X_1, \ldots, X_k]$ is an irreducible, factorable, homogeneous polynomial of degree $d \geq 2$ in the $k \geq 2$ indeterminates $X_1, \ldots, X_k$ then there exists an integer $r \equiv r(f)$ depending only on f and satisfying $2 \leq r \leq \min(k,d)$ such that

(2) $$N_{p^n}(f) = p^{n(k-r)} .$$

Proof. Applying the ideas used by Carlitz in §3 of [2] to homogeneous polynomials, we deduce that f is an irreducible, factorable, homogeneous polynomial of degree d over $GF(p^n)$ if and only if there is a factorization

(3) $$f(X_1,\ldots, X_k) = \prod_{i=0}^{d-1} \ell_i(X_1,\ldots, X_k) ,$$

where $\ell_i(X_1,\ldots, X_k) = a_1^{p^{ni}} X_1 +\ldots+ a_k^{p^{ni}} X_k$ and $d =$ l.c.m(deg $a_1,\ldots,$ deg a_k) . (If $a \in GF(p^{nf})$ but $a \notin GF(p^{ne})$ for $1 \le e \le f$, we write deg $a = f$). Clearly each $\ell_i(X_1,\ldots,X_n)$ $\in GF(p^{nd})[X_1,\ldots, X_k]$. Suppose $(x_1,\ldots, x_k) \in GF(p^n)\times\ldots\times GF(p^n)$ is such that $\ell_i(x_1,\ldots, x_k) = 0$. Choose a positive integer u such that $ud + j - i > 0$, where $0 \le j \le d-1$, $j \ne i$. Raising ℓ_i to the $p^{(ud+j-i)n}$th power, we obtain $\ell_j(x_1,\ldots,x_k) = 0$, as each $x_i \in GF(p^n)$ and each $a_i \in GF(p^{nd})$. Thus $(x_1,\ldots, x_k) \in GF(p^n)\times\ldots\times GF(p^n)$ which satisfy $\ell_i(x_1,\ldots, x_k) = 0$ also satisfy $\ell_j(x_1,\ldots, x_k) = 0$ and vice-versa. Hence $N_{p^n}(f) = N_{p^n}(\ell_0)$. Now $GF(p^{nd})$ is a d-dimensional vector space over $GF(p^n)$. Let $\{\alpha_1,\ldots,\alpha_d\}$ be a basis for this vector space. Hence for $i = 1, 2,\ldots, k$ we can write uniquely

(4) $$a_i = \sum_{m=1}^{d} b_{im}\, \alpha_m \qquad (b_{im} \in GF(p^n)) .$$

Raising both sides of (4) to the p^{nj}th power $(j = 0, 1,\ldots,d-1)$ we obtain

https://doi.org/10.4153/CMB-1969-076-4 Published online by Cambridge University Press

(5) $$a_i^{p^{nj}} = \sum_{m=1}^{d} b_{im}\, \alpha_m^{p^{nj}}$$

Hence $A = BC$, where A is the $k \times d$ matrix $(a_i^{p^{nj}})$, B is the $k \times d$ matrix (b_{ij}) and C is the $d \times d$ matrix $(\alpha_i^{p^{nj}})$. Since the α_i form a basis, C is non-singular and so rank A = rank B. We write

(6) $$r(f) = \text{rank } A = \text{rank } B ,$$

so that $r(f)$ depends only on the a_i, that is only on f. Using (4) we obtain

$$\ell_o(X_1,\ldots, X_k) = \sum_{m=1}^{d} \left(\sum_{i=1}^{k} b_{im} X_i \right) \alpha_m ,$$

so that $\ell_o(x_1,\ldots, x_k) = 0$, for $(x_1,\ldots, x_k) \in GF(p^n) \times \ldots \times GF(p^n)$, if and only if

$$\sum_{i=1}^{k} b_{im} x_i = 0 , \quad m = 1, 2,\ldots, d ,$$

that is, if and only if

(7) $$B^T \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

The number of linearly independent solutions $(x_1,\ldots, x_k) \in GF(p^n) \times \ldots \times GF(p^n)$ over $GF(p^n)$ of (7) is k - rank (B^T) = k - rank (B) = $k - r(f)$. Thus the total number of solutions of (7) is $(p^n)^{k-r}$, giving $N_{p^n}(f) = N_{p^n}(\ell_o) = p^{n(k-r)}$, as required.

https://doi.org/10.4153/CMB-1969-076-4 Published online by Cambridge University Press

As A is $k \times d$, clearly $r \leq \min(k,d)$. We note next that $r \geq 2$. As f is not identically zero, $r \neq 0$. Suppose $r = 1$; then there exists a row of A, without loss of generality the first one, such that every other row is a multiple of it. Hence $a_i = \lambda_i a_1$ ($\lambda_i \in GF(p^n)$, $i = 2,\ldots,k$) giving

$$f(X_1,\ldots, X_n) = a_1^{1+p^n+p^{2n}+\ldots+p^{(d-1)n}}(X_1+\lambda_2 X_2 +\ldots+ \lambda_k X_k)^d ,$$

which is a contradiction as $d \geq 2$, since f is irreducible over $GF(p^n)$.

The author is grateful to the referee for pointing out that a special case of theorem 1 has been given by Carlitz (see formula (5.3) in [3]). Carlitz considers the case $k = d$, $\det(a_i^{p^{nj}}) \neq 0$, so that $r(f) = k$ and $N_{p^n}(f) = 1$.

Theorem 1 can be extended to irreducible factorable polynomials which are not homogeneous. If $f(X_1,\ldots, X_n) \in GF(p^n)[X_1,\ldots, X_k]$ is an irreducible factorable polynomial which is not homogeneous, we set

$$(8) \qquad f^*(X_1,\ldots, X_{k+1}) = X_{k+1}^d f(X_1/X_{k+1},\ldots, X_k/X_{k+1})$$

and

$$(9) \qquad f^{**}(X_1,\ldots, X_k) = f^*(X_1,\ldots, X_k,0) ,$$

where d is the total degree of f, so that f^* and f^{**} are both homogeneous of degree d. f^* is irreducible and factorable but f^{**} need not be. We examine the possibilities for f^{**}. We write

$$f(X_1,\ldots, X_k) = \prod_{j=0}^{d-1} (a_1^{p^{nj}} X_1 +\ldots+ a_k^{p^{nj}} X_k + a_{k+1}^{p^{nj}}) ,$$

where $d = \text{l.c.m}(\deg a_1,\ldots, \deg a_k, \deg a_{k+1})$.

Then

$$f^{**}(X_1,\ldots,X_k) = \prod_{j=0}^{d-1} (a_1^{p^{nj}} X_1 +\ldots+ a_k^{p^{nj}} X_k) . \tag{10}$$

Let $e = \text{l.c.m}(\deg a_1,\ldots, \deg a_k)$ so that $e|d$. We consider two possibilities: (i) $e \neq 1$; (ii) $e = 1$. If (i) holds (10) becomes

$$f^{**}(X_1,\ldots, X_k) = \{g(X_1,\ldots, X_k)\}^{d/e} ,$$

where

$$g(X_1,\ldots, X_k) = \prod_{j=0}^{e-1} (a_1^{p^{nj}} X_1 +\ldots+ a_k^{p^{nj}} X_k)$$

is an irreducible factorable homogeneous polynomial of degree e.

Hence by Theorem 1

$$N_{p^n}(f^{**}) = N_{p^n}(g) = p^{n(k-s)} , \tag{11}$$

where $s = r(g) = r(f^{**})$ satisfies $2 \leq s \leq \min(k,e)$. If (ii) holds (10) becomes

$$f^{**}(X_1,\ldots, X_k) = \{\ell(X_1,\ldots, X_k)\}^{d} ,$$

where

$$\ell(X_1,\ldots, X_k) = a_1X_1 +\ldots+ a_kX_k \in GF(p^n)[X_1,\ldots, X_k] .$$

Hence

$$N_{p^n}(f^{**}) = N_{p^n}(\ell) = p^{n(k-1)} . \tag{12}$$

Also by Theorem 1 we have

$$N_{p^n}(f^*) = p^{n(k+1-t)} , \tag{13}$$

where $t = r(f^*)$ satisfies $2 \leq t \leq \min(k+1,d)$. By the definition of s and t as ranks clearly $t = s$ or $s + 1$. Moreover, when $e = 1$ we have $s = 1$, $t = 2$. Now

$$N_{p^n}(f) = \frac{N_{p^n}(f^*) - N_{p^n}(f^{**})}{p^n - 1} , \tag{14}$$

so from (11), (12), (13) and (14) we have

THEOREM 2. If $f(X_1, \ldots, X_k) \in GF(p^n)[X_1, \ldots, X_k]$ is an irreducible, factorable, non-homogeneous polynomial of degree $d \geq 2$ in the $k \geq 2$ indeterminates $X_1, X_2, \ldots, X_k$ then

$$N_{p^n}(f) = \begin{cases} p^{n(k-r(f^*))} , & \text{if } e \neq 1, \ r(f^*) = r(f^{**}) , \\ 0 , & \text{otherwise,} \end{cases}$$

where f^*, f^{**} are defined by (8), (9) respectively.

REFERENCES

1. B. J. Birch and D. J. Lewis, p-adic forms. J. Indian Math. Soc. 23 (1959) 11-32.

2. L. Carlitz, On factorable polynomials in several indeterminates. Duke Math. J. 2 (1936) 660-670.

3. L. Carlitz, The number of solutions of some special equations in a finite field. Pacific J. Math. 4 (1954) 207-217.

Summer Research Institute
Queen's University
Kingston

Carleton University
Ottawa

https://doi.org/10.4153/CMB-1969-076-4 Published online by Cambridge University Press