JOURNAL OF NUMBER THEORY 28, 62–65 (1988)

Discriminants and the Irreducibility of a Class of Polynomials in a Finite Field of Arbitrary Characteristic

OSCAR MORENO

Department of Mathematics, University of Puerto Rico, Río Piedras, Puerto Rico

Received May 6, 1983

There has been some interest in finding irreducible polynomials of the type $f(A(x))$ for certain classes of linearized polynomial $A(x)$ over a finite field $GF(p^m)$. The main result of this paper proves the stronger result that there are no further irrducible cases of $f(A(x))$ for an extended class that contains that of linearized polynomials, but for $p \neq 2$. (The case $p=2$ we have considered in [O. Moreno, Discriminants and the irreducibility of a class of polynomials, "Lecture Notes in Computer Science," Vol. 228, Proc. 2nd Int. Conf. AAECL-2, pp. 178–181]). In order to reach this result, and also of independent interest, the discriminant and the parity of the factors of polynomials $f(A(x))$ are computed. Also a new proof of a result first established in [S. Agou, Irréductibilité des polynômes $f(\sum_{i=0}^{m} a_i X^{p^i})$ sur un corp fini F_{p^s}, *Canad. Math. Bull.* **23** (1980), 207–212] is given. © 1988 Academic Press, Inc.

INTRODUCTION

Ore in [6] was the first to consider the irreducibility of polynomials of the type $f(A(x))$ for a certain class of linearized polynomials $A(x)$. Agou in [1–3] in a very general form also considered them.

In the present paper we consider discriminants of this type of polynomial for $A(x)$ that contains the class of linearized polynomials, but for $p \neq 2$. We deal in this way with the problem of irreducibility using Stickelberger's theorem.

The discriminant D of a polynomial $A(x) = \prod_{i=1}^{n} (x - \alpha_i)$ is defined $D(A) = \prod\prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2$. Then it is note hard to prove (see [4]) that

$$D(A) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} A'(\alpha_i).$$

Let us consider now a polynomial with coefficients in $GF(p^k)$ $(p \neq 2)$,

$$A(x) = X^{pi} + A_1 X^{p(i-1)} + \cdots + A_{i-1} X^{p2} + A_i X + A_{i+1};$$

0022-314X/88 $3.00

i.e., $A(x)$ is such that the degree of every term of degree >1 is divisible by p. (This includes the affine polynomials, where every term has degree p^j instead of pj as we have here.) We will compute the discriminant in this case, but considering it as an element of $GF(p^k)$.

LEMMA 1. *For $A(x)$ as defined above we have* $D(A)=(-1)^{pi(pi-1)/2}(A_i)^{pi}$, *when we consider $D(A)$ as an element of $GF(p^k)$.*

Proof. Obvious using the formula for $D(A)$ in terms of $A'(x)$, since $p=0$ in $GF(p^k)$.

We will deal now with the discriminant of a composition of polynomials $f(g(x))$ where $g(X)=X^n+g_1X^{n-1}+\cdots+g_{n-1}+g_n$ and let $f(x)=x^m+f_1x^{m-1}+\cdots+f_{m-1}x+f_m$ be an irreducible polynomial where f and g have coefficients in the finite field $GF(p^k)$.

LEMMA 2. *If $D(g)=D(g+\gamma)$ whenever $\gamma\in GF(p^k)$ then*

$$D(f(g(X))=(D(f))^n\,(D(g))^m.$$

Proof. $f(g(X))=\prod_{i=1}^{nm}(X-\beta_i)$ and furthermore for every root γ_j of f, $g(\beta_i)=\gamma_j$ for exactly n values of i. Then using again the formula for D in terms of derivatives and denoting $s=(-1)^{nm(nm-1)/2}$,

$$\begin{aligned} D(f(g(X))&=s\prod_{i=1}^{nm}(f(g(X))'(\beta_i)\\ &=s\prod_{i=1}^{nm}f'(g(\beta_i))\prod_{i=1}^{nm}g'(\beta_i)\\ &=s\prod_{j=1}^{m}(f'(\gamma_j))^m\prod_{i=1}^{nm}(g'(\beta_i))\\ &=s'(D(f))^n\prod_{i=1}^{nm}g'(\beta_i), \qquad \text{where}\quad s'=s(-1)^{nm(m-1)/2} \end{aligned}$$

(note that $s'(-1)^{nm(n-1)/2}=1$). But $\prod_{i=1}^{nm}g'(\beta_i)=\prod_{j=1}^{m}\prod_{g(\beta_i)=\gamma_j}g'(\beta_i)$ and the inner product is equal to $(-1)^{n(n-1)/2}D(g(X)-\gamma_j)=(-1)^{n(n-1)/2}D(g)$ and the rest follows easily. Now we will prove

THEOREM 1. *Let n, r_g, r_f be the number of irreducible factors in $GF(p^k)$ of $f(A)$, g, f, respectively, and let $D(g)$ be as in Lemma 2. Then*

$$r\equiv nr_f+mr_g+nm(\text{mod }2).$$

Proof. We will consider the case $p\neq 2$. We will use the Stickelberger theorem (for $p \neq 2$) whose proof can be found in [4]. This theorem states that if v is a polynomial of degree l with coefficients in $GP(p^k)$ and n_v is the number of its irreducible factors in $GF(p^k)$ then $n_v \equiv l$[1] iff $D(v)$ is a square in $GF(p^k)$. Therefore $r \equiv nm$ iff $D(f(g))$ is a square in $GF(p^k)$, and from Lemma 3 this is so iff $(D(f))^n$, $(D(g))^m$ are both squares or both nonsquares in $GF(p^k)$. Clearly it is enough to prove that the last condition is true iff $nr_f + mr_g \equiv 0$. But it is clear that this is true if n and m are even. If only one, say n, is even, then $nr_f + mr_g \equiv r_f$ and $r_g \equiv n \equiv 0$ iff $r_f \equiv r_g$ iff $(D(f))^n$, $(D(g))^m$ are both squares or both nonsquares in $GR(P^k)$.

COROLLARY 1. *A necessary condition for $f(g)$ to be irreducible is that m be even, and n odd, or that m be odd and r_g be odd.*

Now we prove that there are no unknown cases of irreducible polynomials of the form $f(A(X))$ for a linearized polynomial $A(X)$, (i.e., $A(X)$ is of the form $A(X) = x^{p^n} + A_1 X^{p^{i-1}} + \cdots + A_n X$). This is another proof of a result first done in [2]. Since $p = 2$ has been treated in [8] and $n \leqslant 2$ in [1, 3], we will assume in Theorem 2 that $p \neq 2$ and $n > 2$. We can further assume f to be irreducible, since otherwise we know that $f(A(X))$ is not irreducible.

LEMMA 3. *Assume $f(X)$, $g(X) \in GF(p^k)[X]$ and $f(X)$ is an irreducible polynomial of degree m. The polynomial $f(g(X))$ is irreducible over $GF(p^k)$ iff $g(X) + \beta$ is irreducible over $GF(p^{km})$ for β any root of $f(X)$.*

Proof. We first notice that if $g(X) + \beta$ is irreducible over $GF(p^{km})$ for β a root of $f(X)$, then it is so for any root of $f(X)$, and the reason is that β, $\beta^{p^k}, \ldots, \beta^{p^{(m-1)k}}$ are exactly the roots of $f(X)$. But if u is a root of $f(g(X))$ it is a root of $g(X) + \beta$ for some root β of $f(X)$. Now $f(g(X))$ is irreducible over $GF(p^k)$ iff $GF(p^k)(u)$ has degree nm over $GF(p^k)$, where nm is the degree of $f(g(X))$. We usually denote this $[GF(p^k)(u):GF(p^k)] = nm$. Then since $g(u) + \beta = 0$ it is clear that $GF(p^k)(u) \supset GF(p^k)(\beta) \supset GF(p^k)$ and it is well known that $[GF(p^k)(u):GF(p^k)] = [GF(p^k)(u):GF(p^k)(\beta)][GF(p^k)(\beta): GF(p^k)]$. Since the rightmost one is m it is clear that $f(g(X))$ is irreducible iff $[GF(p^k)(u):GF(p^k)(\beta)] = n$ and since $g(X) + \beta$ is a polynomial for u over $GF(p^k)(\beta)$ of degree n this is true iff $g(X) + \beta$ is irreducible. We are now ready for our next theorem.

THEOREM 2. *The polynomial $f(A(X)) \in GF(p^k)[X]$ for a linearized polynomial $A(X)$, with $n > 2$, is not irreducible over $GF(p^k)$.*

Proof. As mentioned before we can assume $p \neq 2$. From Lemma 4 it is sufficient to prove that an affine polynomial $A(X) + \beta$, with $n > 2$, is

[1] All the congruences in this theorem are mod 2.

irreducible (over $GF(p^{km})$). This we will prove by induction on the degree of $A(X)+\beta$. To start the induction we know this is true for $n=2$, from the main result in [3]. Assume $n>2$; if $A(X)$ has some root α in $GF(p^{km})$ then we know $A(X)+\beta=L(X^p+\alpha^{p-1})+\beta$ for some linearized polynomial $L(X)\in GF(p^{km})[X]$ of degree $<n$ (see [5]). From this the result will follow from the induction hypothesis. To finish consider now the case in which $A(X)$ has no roots in $GF(p^{km})$. But we know $A(X)$ provides a linear map (of vector spaces over $GF(p)$) of the field $GF(p^{km})$ into itself. If $A(X)$ has no roots in $GF(p^{km})$ then this map is 1–1 and therefore onto. As a consequence $A(X)+\beta$ always has a root in $GF(p^{km})$ for any β and is not irreducible.

REFERENCES

1. S. AGOU, Factorization sur un corp finit F_pn des polynômes composes $f(x^{p^n}-ax)$, lorsque $f(x)$ est un polynôme irreductible de $F_pn[X]$. *J. Number Theory* **9** (1977), 229–239.
2. S. AGOU, Irreductibilité des polynômes $f(\sum_{i=0}^{m} a_i X^{p^i})$ sur un corp fini F_{p^s}, *Canad. Math. Bull.* **23** (1980), 207-212.
3. S. AGOU, Irreductibilité des polynômes $f(x^{p^{2r}}-ax^{p^r}-bx)$ sur un corps fini F_{p^s}, *J. Number Theory* **10** (1978), 64–69.
4. E. R. BELEKAMP, "Algebraic Coding Theory," McGraw–Hill, New York, 1968.
5. O. ORE, On a special class of polynomials, *Trans. Amer. Math. Soc.* **35** (1933), 559–584.
6. O. ORE, Contributions to the theory of finite fields, *Trans. Amer. Math. Soc.* **36** (1934), 243–274.
7. R. G. SWAN, Factorization of polynomials over finite fields, *Pacific J. Math.* **12** (1962), 1099–1106.
8. O. MORENO, Discriminants and the irreducibility of a class of polynomials, "Lecture Notes in Computer Science," Vol. 228, Proc. 2nd Int. Conf. AAECL-2, pp. 178–181.