EISENSTEIN'S CRITERIA FOR ABSOLUTE IRREDUCIBILITY OVER A FINITE FIELD

Kenneth S. Williams

(received May 9, 1966)

Let p denote a prime and n a positive integer. Write $q = p^n$ and let k_q denote the Galois field with q elements. The unique factorization domain of polynomials in $m(\geq 2)$ indeterminates $x_1, \ldots, x_m$ with coefficients in k_q is denoted by $k_q[x_1, \ldots, x_m]$. It is the purpose of this note to prove the following generalization of Eisenstein's irreducibility criteria and to point out some of its consequences.

THEOREM 1. Suppose $f(x_1, \ldots, x_m)$ is a (not necessarily homogeneous) polynomial $\in k_q[x_1, \ldots, x_m]$, such that, if f is regarded as a polynomial in some indeterminate $x_i (1 \leq i \leq m)$ of degree $d(1 \leq d < q)$ then there exists an absolutely irreducible polynomial $\mathfrak{p}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m)$ with coefficients in k_q, with the properties

$$\mathfrak{p} \nmid f_d, \quad \mathfrak{p} \mid f_r \ (r = 0, 1, \ldots, d-1) \text{ and } \mathfrak{p}^2 \nmid f_o,$$

where f_r denotes the coefficient of x_i^r $(r = 0, 1, \ldots, d)$. Then f is absolutely irreducible in $k_q[x_1, \ldots, x_m]$.

Proof. Without loss of generality we can take $i = m$. As $k_q[x_1, \ldots, x_{m-1}]$ is a unique factorization domain and $\mathfrak{p}$ is an irreducible element in it, by Eisenstein's irreducibility criteria (see for example [2]), f is irreducible in $k_q[x_1, \ldots, x_m]$. Suppose however that f is not absolutely irreducible in

https://doi.org/10.4153/CMB-1966-071-1 Published online by Cambridge University Press

$k_q[x_1, \ldots, x_m]$. Then there is a normal extension k_q' of k_q over which f splits into $a \geq 2$ conjugate factors, say,

$$f(x_1, \ldots, x_m) = \prod_{s=1}^{a} (g_s(x_1, \ldots, x_m).$$

Taking $x_m = 0$ we obtain

$$f_o(x_1, \ldots, x_{m-1}) = \prod_{s=1}^{a} h_s(x_1, \ldots, x_{m-1}),$$

where

$$h_s(x_1, \ldots, x_{m-1}) = g_s(x_1, \ldots, x_{m-1}, 0).$$

As $\mathfrak{p} \mid f_o$ over k_q and so over k_q' we have

$$\mathfrak{p} \mid \prod_{s=1}^{a} h_s$$

over k_q'. But $\mathfrak{p}$ is absolutely irreducible over k_q and so is irreducible over k_q'. Hence

$$\mathfrak{p} \mid h_s$$

over k_q', for some $s(1 \leq s \leq a)$. By conjugacy this is true for all $s(1 \leq s \leq a)$.

Let

$$h_s = \mathfrak{p}\ell_s \quad (s = 1, 2, \ldots, a)$$

where $\ell_s = \ell_s(x_1, \ldots, x_{m-1}) \in k_q'[x_1, \ldots, x_{m-1}]$. Then

$$f_o = \prod_{s=1}^{a} h_s = \mathfrak{p}^a \ell,$$

where $\ell = \prod_{s=1}^{a} \ell_s$ is defined over k_q. This contradicts

https://doi.org/10.4153/CMB-1966-071-1 Published online by Cambridge University Press

$a \geq 2$ as $\mathfrak{p}^2 \nmid f_o$.

COROLLARY 1. Suppose f is such that there exists a linear polynomial $\ell(x_1, \ldots, x_{m-1}) \in k_q[x_1, \ldots, x_{m-1}]$ with the properties

$$\ell \nmid f_d, \quad \ell \mid f_r \; (r = 0, 1, \ldots, d-1) \text{ and } \ell^2 \nmid f_o .$$

Then f is absolutely irreducible in $k_q[x_1, \ldots, x_m]$.

Proof. This follows immediately from theorem 1 as a linear polynomial is always absolutely irreducible.

COROLLARY 2. If $f(x_1, \ldots, x_{m-1}) \in k_q[x_1, \ldots, x_{m-1}]$ has at least one absolutely irreducible factor $\mathfrak{p}(x_1, \ldots, x_{m-1}) \in k_q[x_1, \ldots, x_{m-1}]$ such that $\mathfrak{p}^2 \nmid f$ then

$$f(x_1, \ldots, x_{m-1}) - x_m^d$$

is absolutely irreducible in $k_q[x_1, \ldots, x_m]$.

Proof. This is obviously a special case of theorem 1 and provides a generalization of lemma 3 of [1].

Note. Theorem 1 need not be confined to finite fields, it could have been stated for any field which is not algebraically closed, as the proof is quite general.

We now prove theorem 2 which provides a generalization of corollary 3 of [1].

THEOREM 2. Let $f(x_1, \ldots, x_m)$ be a (not necessarily homogeneous) polynomial $\in k_q[x_1, \ldots, x_m]$ of degree $d (1 \leq d < q)$ and let $a \in k_q$. Set

$$f_a(x_1, \ldots, x_m) = f(x_1, \ldots, x_m) - a$$

and

https://doi.org/10.4153/CMB-1966-071-1 Published online by Cambridge University Press

$$f_a^*(x_o, \ldots, x_m) = x_o^d f_a(x_1/x_o, \ldots, x_m/x_o).$$

Also for $r = 0, 1, \ldots, d$ let

$$f_a^r(x_1, \ldots, x_m) = \frac{1}{r!} \left. \frac{\partial^r f_a^*}{\partial x_o^r} \right|_{x_o = 0}.$$

(Note that f_a^r only depends on a when $r = d$). Suppose there exists an absolutely irreducible polynomial $\wp(x_1, \ldots, x_m) \in k_q[x_1, \ldots, x_m]$ with the properties

$$\wp \mid f_a^r \ (r = 0, 1, \ldots, d-1) \text{ and } \wp^2 \nmid f_a^o .$$

Then f is universal - that is, for any $a \in k_q$ there are $y_1, \ldots, y_m \in k_q$ such that

$$f(y_1, \ldots, y_m) = a,$$

provided $q > D(m, d)$, where D depends only on m and d.

<u>Proof.</u> We have

$$f_a^*(x_o, \ldots, x_m) = \sum_{r=0}^{d} f_a^r(x_1, \ldots, x_m) x_o^r .$$

As f_a^d is a constant $\wp \nmid f_a^d$ except when the constant is zero. In that case $(y_1, \ldots, y_m) = (0, \ldots, 0)$. Otherwise, by theorem 1, f_a^* is absolutely irreducible in k_q. Hence by a theorem of Lang and Weil (see for example [1], p. 12) the number N of zeros of f_a^* in k_q satisfies

$$|N - q^m| < A(m, d) q^{m-1/2},$$

where $A(m, d)$ depends only on m and d. Let N_1 denote the number of zeros of f_a^* in k_q with $x_o = 0$. Then (see for

https://doi.org/10.4153/CMB-1966-071-1 Published online by Cambridge University Press

example [1], p. 12)

$$N_1 < B(m, d)q^{m-1},$$

where $B(m, d)$ depends only on m and d. Now N_2 - the number of zeros of f_a^* in k_q with $x_o = 1$ - satisfies

$$N_1 + (q-1)N_2 = N$$

so

$$N_2 - q^{m-1} = \frac{1}{q-1} \{(N-q^m) - N_1 + q^{m-1}\} .$$

Hence

$$|N_2 - q^{m-1}| \leq \frac{1}{q-1} \{ |N - q^m| + N_1 + q^{m-1}\}$$

$$< \frac{1}{q-1} \{ Aq^{m-1/2} + Bq^{m-1} + q^{m-1} \}$$

$$\leq \frac{2}{q} \{ Aq^{m-1/2} + Bq^{m-1/2} + q^{m-1/2} \}$$

$$= Cq^{m-3/2} ,$$

where $C = 2(A + B + 1)$ depends only on m and d.

Hence

$$N_2 > q^{m-1} - Cq^{m-3/2}$$

and so

$$N_2 > 0$$

provided

$$q > D(m, d),$$

where $D = C^2$ depends only on m and d as required.

https://doi.org/10.4153/CMB-1966-071-1 Published online by Cambridge University Press

REFERENCES

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

2. B.L. Van der Waerden, Modern Algebra. Fred. Ungar Publish. Co. N.Y., (1953), page 74.

Carleton University, Ottawa