EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 17, No. 2, 2024, 721-724
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Note on irreducible polynomials over $\mathbb{F}_q[X]$

Alanod M. Sibih

Department of Mathematics, Jamoum University College, Umm Al-Qura University, Holly Makkah 21955, Saudi Arabia

Abstract. In this note, we provide a new criterion of polynomials's irreducibility over $\mathbb{F}_q[X]$, where $\mathbb{F}_q$ is a finite field.

2020 Mathematics Subject Classifications: 11Txx, 11T55

Key Words and Phrases: Polynomials, irreducibility, criterion, finite fields.

1. Introduction

A polynomial is reducible over a given field if it can be expressed as a product of lower degree polynomials with coefficients in the same field. Otherwise, it is called to be irreducible.

We are interested in determining if a particular polynomial is irreducible or not. As a result, a simple test or criterion for obtaining this information is desirable.

Unfortunately, no such criterion that applies to all classes of polynomials has yet been developed; nonetheless, a number of tests, or irreducibility criteria, have been discovered so far that provide useful information for some specific classes of polynomials.

This article focuses on irreducible polynomials with coefficients in $\mathbb{F}_q[X]$, where over $\mathbb{F}_q$ is a finite field.

A. Chandoul et al. [2], proved a widely accepted irreducibility criterion, which states that:

Theorem 1. *If* $\Lambda(Y) = Y^d + \lambda_{d-1}Y^{d-1} + \cdots + \lambda_0$ *be a polynomial with* $\lambda_i \in_q [X],\ \lambda_0 \neq 0$ *and* $\deg \lambda_{d-1} > \deg \lambda_i$, *for each* $i \neq d-1$. *Then* Λ *is irreducible over* $_q[X]$.

This result was the starting point for many researches and the exploration of new criterions, see [1, 3]. For older results, see [4, 5]. In this note, we provide a new criterion of polynomials's irreducibility over $\mathbb{F}_q[X]$.

DOI: https://doi.org/10.29020/nybg.ejpam.v17i2.5095

Email address: amsibih@uqu.edu.sa (A. M. Sibih)

2. Preliminaries

Let $\mathbb{F}_q$ be the finite field and denote by $\mathbb{F}_q[X]$ the ring of polynomials with coefficients in $\mathbb{F}_q$ and by $\mathbb{F}_q(X)$ the quotient field of $\mathbb{F}_q[X]$. Let $\mathbb{F}_q((X^{-1}))$ be the field of Laurent formal power series defined as follows:

$$\mathbb{F}_q((X^{-1})) = \{\sum_{n\geq n_0} a_n X^{-n}, \quad a_n \in \mathbb{F}_q \text{ and } n_0 \in\}.$$

For $w = \sum_{n=n_0}^{+\infty} a_n X^{-n} \in \mathbb{F}_q((X^{-1}))$, we define the integer part $[w]$ of w by $[w] = \sum_{n=n_0}^{0} a_n X^{-n}$ if $n_0 \leq 0$ and $[w] = 0$ if $n_0 > 0$, the fractional part of w by $\{w\} = w - [w] = \sum_{n=1}^{+\infty} a_n X^{-n}$. We have a non-archimedean absolute value $|\cdot|$ on $\mathbb{F}_q((X^{-1}))$, namely, for any element $w \in \mathbb{F}_q((X^{-1}))$ having the form

$$w = \sum_{n=n_0}^{+\infty} a_n X^{-n} \qquad (a_n \in \mathbb{F}_q),$$

we define $|w| = e^{-n_0}$ if $w \neq 0$, where n_0 is the smallest index verifying $a_{n_0} \neq 0$, and $|w| = 0$ if $w = 0$. We know that $\mathbb{F}_q((X^{-1}))$ is complete and locally compact with respect to the metric defined by this absolute value.

We denote by $\overline{\mathbb{F}}_q((X^{-1}))$ an algebraic closure of $\mathbb{F}_q((X^{-1}))$. We note that the absolute value has a unique extension to $\overline{\mathbb{F}}_q((X^{-1}))$. To denote this extended absolute value, we also use the symbol $|\cdot|$.

3. Main results

Theorem 2. *Let $\mathbb{F}_q$ be a finite field of caracteristic p, $n \geq 2$ and let*

$$P(Y) = A_s Y^s + A_{s-1} Y^{s-1} + A_{s-2} Y^{s-2} + \cdots + A_1 Y + A_0$$

be a polynomial over $\mathbb{F}_q[X]$, such that $A_s A_{s-1} A_0 \neq 0$, A_s and A_{s-1} has a same irreducible factor B, with $lcm(A_{s-1}, B) = B^m$ ($A_{s-1} = B^m a_{s-1}$) and $lcm(A_s, B) = B^n$ ($A_s = B^n a_s$). If

$$n > ms + \frac{(s-1)(degA_s - m\deg B) + M}{degB}$$

with $M = \max_{i\neq s}(\deg Ai)$, then P is irreducible over $\mathbb{F}_q[X]$.

Proof. Suppose that $P(Y) = Q(Y)H(Y)$, where $Q, H \in \mathbb{F}_q[X][Y]$. let

$$\begin{aligned} &\mathrm{Q(Y)}= \mathrm{Q}_jY^j + Q_{j-1}Y^{j-1} + Q_{j-2}Y^{j-2} + \cdots + Q_1Y + Q_0 \\ \textit{and}\quad &\mathrm{H(Y)}= \mathrm{H}_kY^k + H_{k-1}Y^{k-1} + H_{k-2}Y^{k-2} + \cdots + H_1Y + H_0 \end{aligned}$$

where $j + k = s$, $Q_jH_k = A_s$, $Q_0H_0 = A_0$ and $A_{s-1} = Q_jH_{k-1} + H_kQ_{j-1}$. Let $B^d = lcm(Q_j, B)$, $(Q_j = B^dq_j)$, then $B^{n-d} = lcm(H_k, B)$ $(H_k = B^{m-d}h_k)$ and we must have $m \geq d$.

Consider the factorisation of P and Q in $\overline{\mathbb{F}_q((X^{-1}))}$, we have

$$\begin{aligned} &\mathrm{P(Y)}=\mathrm{A}_s(Y-\omega_1)\cdots(Y-\omega_n) \\ \textit{and}\quad &\mathrm{Q(Y)}=\mathrm{Q}_j(Y-\omega_1)\cdots(Y-\omega_j) \end{aligned}$$

where $\omega_i \in \overline{\mathbb{F}_q((X^{-1}))}$, forall $i := 1, \cdots, n$.

Consider, now, the nonarchimedean absolute value, and set a real number $\alpha \geq 0$ such that

$$|A_s| > e^{\alpha} \max_{i\neq s} |Ai|$$

then, using the viète theorem, we have

$$|\omega_1 \cdots \omega_s| = |\omega_1| \cdots |\omega_s| = \frac{|A_0|}{|A_s|} < \frac{|A_0|}{e^{\alpha} \max_{i\neq s} |Ai|} < \frac{1}{e^{\alpha}},$$

thus, for any $j := 1, \cdots, n$, we must have $|\omega_j| < \dfrac{1}{e^{\alpha/s}}$.

So that, we get

$$|\omega_1 \cdots \omega_j| < \frac{1}{e^{j\alpha/s}}.$$

On the other hand, we have

$$|\omega_1 \cdots \omega_j| = \left|\frac{Q_0}{Q_j}\right| = \left|\frac{Q_0}{B^dq_j}\right| \geq \frac{1}{|B^m|\,|a_s|}.$$

To reach a contraduction, it is still necessary to chose α such that

$$\frac{1}{|B^m|\,|a_s|} \geq \frac{1}{e^{j\alpha/s}}.$$

It can be sufficient to choose α such that

$$|B^m|\,|a_s| \leq e^{\alpha/s}.$$

Or, equivalently

$$\alpha \geq sm \deg B + s(\deg A_s - n \deg B).$$

A conceivable value for α is $sm \deg B + s(\deg A_s - n \deg B)$, which leads to a contradiction if $n > ms + \dfrac{(s-1)(degA_s - m \deg B) + M}{degB}$ where $M = \max\limits_{i\neq s}(\deg Ai)$, what was to be proved.

References

[1] M Ben Nasr and Hassen Kthiri. Characterization of 2-pisot elements in the field of laurent series over a finite field. *Mathematical Notes*, 107:552–558, 2020.

[2] A Chandoul, M Jellali, and M Mkaouar. Irreducibility criterion over finite fields. *Communications in Algebra*, 39(9):3133–3137, 2011.

[3] Amara Chandoul and Alanod M Sibih. Note on irreducible polynomials over finite field. *European Journal of Pure and Applied Mathematics*, 14(1):265–267, 2021.

[4] HL Dorwart. Irreducibility of polynomials. *The American Mathematical Monthly*, 42(6):369–381, 1935.

[5] Ravindranathan Thangadurai. Irreducibility of polynomials whose coefficients are integers. *Mathematics Newsletter*, 17:29–61, 2007.