International Journal of Mathematics and
Computer Science, **19**(2024), no. 4, 921–925

On irreducibility in $\mathbb{F}_q[X][Y]$

Saber Mansour

Department of Mathematical Sciences
Faculty of Applied Sciences
Umm Al-Qura University
Mecca, Saudi Arabia

email: samansour@uqu.edu.sa

(Received June 8, 2023, Accepted February 18, 2024,
Published June 1, 2024)

Abstract

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

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 irreducible.

Characterizing irreducible polynomials over a finite field $\mathbb{F}_q$ or $\mathbb{Q}$ is an intriguing subject that has just lately received attention. It is known that there is no criteria that enables us to determine if such polynomial is reducible or not.

However, a variety of tests, known as irreducibility criteria, have been established that provide useful information for certain types of polynomials.

Lipka [6] identified irreducibility conditions for integer polynomials of the form

$$f(X) = a_n X^n + \cdots + a_1 X + a_0 p^k,$$

Key words and phrases: Polynomials, irreducibility, criterion, finite fields.
AMS (MOS) Subject Classifications: 11Txx, 11T55.
ISSN 1814-0432, 2024, http://ijmcs.future-in-tech.net

where p is a prime number and $p \nmid a_0$. As an example, he proved that such polynomial is irreducible over $\mathbb{Q}$ for all but finitely many positive integers k.

Chandoul et al. [1] proved a widely accepted irreducibility criterion which states that

Theorem 1.1. *If* $\Lambda(Y) = Y^d + \lambda_{d-1}Y^{d-1} + \cdots + \lambda_0$ *be a polynomial with* $\lambda_i \in F_q[X], \lambda_0 \neq 0$ *and* $\deg \lambda_{d-1} > \deg \lambda_i$*, for each* $i \neq d-1$*. Then* Λ *is irreducible over* $F_q[X]$.

In this article, we focus on irreducible polynomials with coefficients in $\mathbb{F}_q[X]$, where $\mathbb{F}_q$ is a finite field.

These results were the starting point for many researches and the exploration of new criterions [2]. For older results, see [3, 4]. In this note, we provide a new criterion for irreducibility of polynomials over $\mathbb{F}_q[X]$.

In this article, we prove an irreducibility criterion over $\mathbb{F}_q[X]$, where $\mathbb{F}_q$ is a finite field.

2 Preliminaries

In this section, we recall some basic concepts and provide the notation.

Throughout this paper, $\mathbb{F}_q$ denotes the finite field with q elements, where q is a power of a prime number.

We 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:

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

Let $w = \sum_{n=n_0}^{\infty} a_n X^{-n}$ be an element of $\mathbb{F}_q((X^{-1}))$.

We denote by $[w] = \sum_{n=n_0}^{0} a_n X^{-n}$ if $n_0 \leq 0$ and $[w] = 0$ if $n_0 > 0$, the integer part $[w]$ of w. Its fractional part $\{w\}$ is defined by $w - [w] = \sum_{n=1}^{\infty} a_n X^{-n}$.

A non-Archimedean absolute value $|\cdot|$ on $\mathbb{F}_q((X^{-1}))$, is defined, for any element $w \in \mathbb{F}_q((X^{-1}))$ having the form

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

by $|w| = e^{-n_0}$ if $w \neq 0$, where n_0 is the smallest index verifying $a_{n_0} \neq 0$, and $|w| = 0$ if $w = 0$ (see [5]).

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

$$P(Y) = A_s Y^s + A_{s-2} Y^{s-2} + A_{s-3} Y^{s-3} + \cdots + A_1 Y + A_0$$

be a polynomial over $\mathbb{F}_q[X]$ such that $A_s A_{s-2} A_0 \neq 0$, A_s and A_{s-2} has a same irreducible factor B, with $lcm(A_{s-2}, B) = B^m$ $(A_{s-2} = B^m a_{s-1})$ and $lcm(A_s, B) = B^n$ $(A_s = B^n a_s)$. If $n \neq m[2]$ and

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

with $M = \max(\deg_{i \neq s, s-1} Ai)$, then P is irreducible over $\mathbb{F}_q[X]$.

Proof. Assume that P decomposes as $P(Y) = Q(Y)H(Y)$ such that Q, H are defined as follows:

$$Q(Y) = Q_j Y^j + Q_{j-1} Y^{j-1} + Q_{j-2} Y^{j-2} + \cdots + Q_1 Y + Q_0$$

and

$$H(Y) = H_k Y^k + H_{k-1} Y^{k-1} + H_{k-2} Y^{k-2} + \cdots + H_1 Y + H_0,$$

where $Q_j, \cdots, Q_0, H_k, \cdots, H_0 \in \mathbb{F}_q[X]$, with $j, k \geq 1$ $j + k = s$, $Q_j H_k = A_s$, $Q_0 H_0 = A_0$ and Let $B^d = lcm(Q_j, B)$, $(Q_j = B^d q_j,\ d \geq 0)$, then $B^{n-d} = lcm(H_k, B)$ $(H_k = B^{m-d} h_k)$ and we must have $d \leq n - d$.

Consider the factorization of P and Q in $\overline{\mathbb{F}_q((X^{-1}))}$. We have

$$P(Y) = A_s(Y-\omega_1)\cdots(Y-\omega_n)$$

and

$$Q(Y) = Q_j(Y-\omega_1)\cdots(Y-\omega_j),$$

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

Consider, now, the non-Archimedean 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

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

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

As a result, we get

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

On the other hand, we have

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

To reach a contradiction, it is still necessary to choose 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 $M = \max(\deg_{i\neq s,s-1} Ai)$. The proof is now complete.

4 Conclusions

Since there is no property that determines whether a polynomial is irreducible or not, it is considered a success to set up a criterion describing some family of irreducible polynomials.

The idea presented in this paper points to a variety of possible directions one could take further research which may enable us to describe new larger families of irreducible polynomials over a finite field.

Acknowledgements

We are very grateful to the anonymous referees for their thoughtful comments.

References

[1] A. Chandoul, M. Jellali, M. Mkaouar, Irreducibility criterion over finite fields, Communications in Algebra, **39,** no. 9, (2011), 3133–3137.

[2] M. Ben Nasr, H. Kthiri, Characterization of 2-Pisot elements in the field of Laurent series over a finite field, Mathematical Notes, **107,** (2020), 552–558.

[3] R. Thangadurai, Irreducibility of polynomials whose coefficients are integers, Mathematics Newsletter (RMS, India), **17,** (2007), 29–37.

[4] H. L. Dorwart, Irreducibility of polynomials, The American Mathematical Monthly, **42,** no. 6, (1935), 369–381.

[5] V. G. Sprindžuk, Mahler's problem in metric number theory Translation of Mathematical monographs, **25,** (1969), Amer. Math. Soc., Providence, RI, USA.

[6] S. Lipka, Über die Irreduzibilit at von Polynomen, Math. Ann., **118,** (1941), 235–245.