EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 2, Article Number 5996
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Some Irreducible Polynomials Over a Finite Field

Amara Chandoul[1,*], Abdallah Assiry[2]

[1]{*Department of Mathematics, Higher Institute of Informatics and Multimedia of Sfax (ISIMS), Sfax University, Sfax, Tunisia*
[2] *Departement of Mathematics, College of Science, Umm Al-Qura University. Mecca 21955, Saudi Arabia*

Abstract. The irreducibility of a polynomial over a finite field refers to whether the polynomial, with coefficients in that field, cannot be factored into nontrivial polynomials. It is surprising to discover that there exist very efficient but still little-known divisibility criteria. In this paper, we give some irreducibility criterions of a given polynomial with coefficients in $\mathbb{F}_q[X]$, were $\mathbb{F}_q$ is a finite field. The arguments can be extended to discuss our results, including potential applications or future research directions.

2020 Mathematics Subject Classifications: 11A05, 11C08, 11T06, 11T55, 12E05

Key Words and Phrases: Polynomial, irreducible polynomial, finite field, divisibility, divisibility criteria

1. Introduction

Finite fields, also known as Galois fields, are fundamental structures in mathematics with far-reaching applications in coding theory, cryptography, combinatorics, and computational algebra. At the heart of many of these applications lies the study of irreducible polynomials over finite fields. These polynomials serve as the building blocks for constructing finite field extensions, enabling the representation and manipulation of elements in higher-dimensional spaces.

The theory of irreducible polynomials over finite fields is both rich and elegant, blending algebraic rigor with practical utility. From the enumeration of irreducible polynomials to the development of efficient algorithms for their construction and testing, this area of research has witnessed significant advancements over the past century. Moreover, the study of specific families of irreducible polynomials—such as binomials, trinomials, and cyclotomic polynomials—has led to deep insights into their structural properties and their role in theoretical and applied contexts.

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i2.5996

Email addresses: amarachandoul@yahoo.fr (Amara Chandoul), aaassiry@uqu.edu.sa (A. Assiry)

Some of application of irreducibility is to explore its relationship with special elements, as Salem formal power series, which are algebraic elements (roots of monic integer polynomials) with a special property: they have exactly one conjugate outside the unit circle and all other conjugates on the unit circle. the connection to irreducible polynomials arises because Salem numbers are defined by their minimal polynomials, which are irreducible [1].

2. Preliminaries

Let $\mathbb{F}_q$ represent the finite field containing q elements, with q being a power of a prime. The ring of polynomials whose coefficients lie in $\mathbb{F}_q$ is denoted by $\mathbb{F}_q[X]$, while $\mathbb{F}_q(X)$ signifies the field of rational functions over $\mathbb{F}_q$.

The field of formal Laurent series in X^{-1} over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q((X^{-1}))$ and is defined as:

$$\mathbb{F}_q((X^{-1})) = \left\{ \sum_{n=n_0}^{\infty} a_n X^{-n} \;\middle|\; a_n \in \mathbb{F}_q \text{ for some integer } n_0 \right\}.$$

For an element $w = \sum_{n=n_0}^{+\infty} a_n X^{-n} \in \mathbb{F}_q((X^{-1}))$, we define its integer part $[w]$ as:

$$[w] = \begin{cases} \sum_{n=n_0}^{0} a_n X^{-n} & \text{if } n_0 \leq 0, \\ 0 & \text{if } n_0 > 0. \end{cases}$$

The fractional part of w is denoted by $\{w\}$ and is given by:

$$\{w\} = w - [w] = \sum_{n=1}^{+\infty} a_n X^{-n}.$$

A non-Archimedean absolute value $|\cdot|$ defined on a field $\mathbb{F}_q((X^{-1}))^*$ by

$$|w| = e^{-n_0},$$

where n_0 is the smallest index such that $a_{n_0} \neq 0$. If $w = 0$, we set $|w| = 0$. This absolute value makes $\mathbb{F}_q((X^{-1}))$ a complete and locally compact metric space.

Let $\overline{\mathbb{F}}_q((X^{-1}))$ denote the algebraic closure of $\mathbb{F}_q((X^{-1}))$. The absolute value $|\cdot|$ extends uniquely to $\overline{\mathbb{F}}_q((X^{-1}))$, and we use the same notation for this extended absolute value.

We define a non-constant polynomial P over $\mathbb{F}$ as irreducible if $P = QH$ with Q and H in $\mathbb{F}$, which implies that either Q or H is a constant. Otherwise, it is called to be reducible.

Irreducible polynomials are commonly studied in fields such as number theory, combinatorics, and algebraic geometry. They also play a significant role in practical domains, including coding theory, cryptography, complexity theory, and computer science[2].

Constructing and Characterizing irreducible polynomials over finite fields $\mathbb{F}_q$ is one of the main challenges in the theory of finite fields that has just lately received attention.

During the last fifty years, constructions of irreducible polynomials over finite fields have been extensively studied.

However, it is recognized that there is no general criteria for determining whether such a polynomial is reducible or irreducible.

Despite this, numerous tests referred to as irreducibility criteria have been established to offer valuable insights into specific classes of polynomials.

In [3], Lipka derived conditions for the irreducibility of integer polynomials of the form

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

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

For older results, one can see [4, 5]. In the first part of this paper we prove an irreducibility criterion for lacunary polynomials with coefficients in $\mathbb{F}_q[X]$, which is similar to the first result of Lipka.

In [6], Ben Nasr and kthiri proved, using the upper Newton polygon, that

Theorem 1. *Let* $\Lambda(Y) = Y^d + \lambda_{d-1}Y^{d-1} + \cdots + \lambda_0$ *be a polynomial with* $\lambda_i \in \mathbb{F}_q[X]$, $\lambda_0 \neq 0$, *and* $\deg \lambda_{d-2} > \deg \lambda_i$ *for all* $i \neq d-2$. *Suppose further that* $\deg \lambda_{d-2}$ *is odd and satisfies* $\deg \lambda_{d-2} \geq 2 \deg \lambda_{d-1}$. *Then,* $\Lambda(Y)$ *is irreducible over* $\mathbb{F}_q[X]$.

Recall that Newton polygons can be used to determine the behavior of roots in polynomials over a field.

Let

$$P(Y) = A_s Y^s + A_{s-1}Y^{s-1} + A_{s-3}Y^{s-3} + \cdots + A_1 Y + A_0$$

be a polynomial over $\mathbb{F}_q[X]$, and assume, for simplicity, that $A_s A_0 \neq 0$.

To each term A_i of $P(Y)$, we assign the point in the following manner:

- If $A_i \neq 0$ take the point : $(i, \deg A_i)$
- If $A_i = 0$ disregard the nonexistent point : (i, ∞)

Then, the points we plot for the polynomial $P(Y)$ are

$$(0, \deg A_0), \cdots (s, \deg A_s)$$

We begin by connecting the points with line segments. The process starts at the point $(0, \deg A_0)$, which is connected to a point, denoted as B, that yields the least feasible slope for the first line segment. Subsequently, B is connected to the next point to its right, ensuring the smallest possible slope for the second line segment, and so forth.

To geometrically visualize this construction, imagine a string fixed at one end to the point $(0, \deg A_0)$ and being pulled counterclockwise around the points by the other end. As the string wraps around each point, it forms a "bend" at that location. The process concludes once all finite points have been wrapped in this manner.

There should be a note here for points of the form $(i, \deg 0)$. Because $\deg 0 = \infty$, these points have no interfer on our construction because it does not yield small slopes while constructing line segments. It is better to completely ignore such points together.

The final structure is referred to as the **upper Newton polygon** of $P(Y)$.

Observe that the upper Newton polygon consists of a sequence of line segments with strictly decreasing and distinct slopes. The condition $A_s A_0 \neq 0$ ensures that the polygon begins at a finite point and terminates at another finite point.

For example, the slope of a line segment in the Newton polygon of $P(Y)$ connecting the point $(r, \deg A_r)$ to the point $(r+m, \deg A_{r+m})$ is computed as:

$$\text{Slope} = k = \frac{\deg A_{r+m} - \deg A_r}{m}.$$

Denote by $\mathbf{K}_P$ the set of slopes.

This result of Ben Nasr and kthiri was a continuation of an idea we started in [7]. We established a well-known criterion for irreducibility, which can be formulated as follows:

Theorem 2. *Let $\Lambda(Y) = Y^d + \lambda_{d-1}Y^{d-1} + \cdots + \lambda_0$ be a polynomial with coefficients $\lambda_i \in \mathbb{F}_q[X]$, where $\lambda_0 \neq 0$. If $\deg \lambda_{d-1} > \deg \lambda_i$ for all $i \neq d-1$, then Λ is irreducible over $\mathbb{F}_q[X]$.*

However, the authors did not refer to our findings, maybe because they were unaware of it or because they were focused on studying Pisot numbers. Then their results on irreducibility was an unintended incidental result.

In a second part of this paper, we generalize these two results and provide a new criterion of polynomials's irreducibility over $\mathbb{F}_q[X]$.

3. Results

Now, we are prepared to give the main results.

Theorem 3. *Let $\mathbb{F}_q$ ($q = p^n, n \geq 2$ and p be a prime) be a finite field of characteristic p. Consider the polynomial*

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

defined over $\mathbb{F}_q[X]$, such that $A_s A_{s-1} A_0 \neq 0$. Here, B is an irreducible factor of both A_s and A_{s-1}, but B does not divide $A_s A_{s-1}$.

If the inequality

$$n > ms + \frac{(s-1)(\deg A_s - m \deg B) + \max\left(\max_{0 \leq i \leq s-2} \deg A_i, \deg(B^m A_{s-1})\right)}{\deg B}$$

holds, then the polynomial P is irreducible over $\mathbb{F}_q[X]$.

Proof. Assume that P can be expressed as the product $P(Y) = Q(Y)H(Y)$, where Q and H are in $\mathbb{F}_q[X][Y]$. let

$$\mathrm{Q(Y)}= \mathrm{B}^d Q_j Y^j + Q_{j-1}Y^{j-1} + Q_{j-2}Y^{j-2} + \cdots + Q_1 Y + Q_0$$
$$\textit{and} \quad \mathrm{H(Y)}= \mathrm{B}^{n-d} H_k Y^k + H_{k-1}Y^{k-1} + H_{k-2}Y^{k-2} + \cdots + H_1 Y + H_0$$

where $j+k=s$, $Q_jH_k = A_s$, $Q_0H_0 = A_0$, $A_{s-1} = B^dQ_jH_{k-1}+B^{m-d}H_kQ_{j-1}$. Assume that $d \leq n-d$.

Consider the factorization of the polynomials P and Q in the algebraic closure of the field of formal Laurent series $\overline{\mathbb{F}_q((X^{-1}))}$. We can express P and Q as:

$$P(Y) = A_s \prod_{i=1}^{n}(Y-\omega_i) \quad \text{and} \quad Q(Y) = Q_j \prod_{i=1}^{j}(Y-\omega_i),$$

where ω_i are in $\overline{\mathbb{F}_q((X^{-1}))}$ for all $i = 1, \ldots, n$.

Consider now the non-Archimedean absolute value defined over a field where each element ω_i belongs to the algebraic closure of $\mathbb{F}_q((X^{-1}))$ for all $i = 1, \ldots, n$, and set a real number $\alpha \geq 0$ such that

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

Then, applying Viète's theorem, we obtain

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

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

Consequently, we find

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

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 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 α is greater than or equal to the quantity

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

A possible expression for α could be $sm\deg B + s(\deg A_s - n\deg B)$. However, this results in a contradiction when

$$n > ms + \frac{(s-1)(degA_s - m\deg B) + \max(\underset{0\leq i\leq s-2}{\deg Ai}\,, B^m A_{s-1})}{degB}.$$

What was to be proved.

Theorem 4. *Let $\mathbb{F}_q$ ($q = p^n, n \geq 2$ and p be a prime) be a finite field of characteristic p and let*

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

be a polynomial over $\mathbb{F}_q[X]$, such that $A_s A_{s-2} A_0 \neq 0$, B is an irreducible polynomial over $\mathbb{F}_q$ and $B \nmid A_s A_{s-2}$. If $n - m$ is odd, and

$$n > ms + \frac{(s-1)(degA_s - m\deg B) + \max(\underset{0\leq i\leq s-3}{\deg Ai}\,, B^m A_{s-2})}{degB},$$

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

$$\begin{aligned} \mathrm{Q(Y)} &= \mathrm{Q}_j Y^j + Q_{j-1}Y^{j-1} + Q_{j-2}Y^{j-2} + \cdots + Q_1 Y + Q_0 \\ \textit{and}\quad \mathrm{H(Y)} &= \mathrm{H}_k Y^k + H_{k-1}Y^{k-1} + H_{k-2}Y^{k-2} + \cdots + H_1 Y + H_0 \end{aligned}$$

where $j + k = s$, $Q_j H_k = A_s$, $Q_0 H_0 = A_0$ and $B^m A_{s-1} = Q_j H_{k-1} + H_k Q_{j-1}$. Assume that $n - d \geq d$. Then, using precisely the same justifications as in the proof of Theorem 3. The remainder of the proof is similar to that of Theorem 4, using $\max(\underset{0\leq i\leq s-3}{\deg Ai}\,, B^m A_{s-2})$ instead of $\max(\underset{0\leq i\leq s-2}{\deg Ai}\,, B^m A_{s-1})$

Theorem 5. *Let $P(Y) = Y^n + A_{n-1}Y^{n-1} + \cdots + A_{n-k+1}Y^{n-k+1} + A_{n-k}Y^{n-k} + \cdots + A_1 Y + A_0$ with $A_0 \neq 0$ and $|A_{n-k}| > \underset{i\neq n-k}{|A_i|}$ be a polynomial over $\mathbb{F}_q[X]$ of degree $\geq k+1$. If $\deg A_{n-k} > k \max\limits_{1\leq i\leq k-1} \deg A_{n-i}$ and $k \nmid \deg A_{n-k}$, then, P has no root in $\mathbb{F}_q((X^{-1}))$ with modulus strictly greater than 1. Moreover P is irreducible over $\mathbb{F}_q[X^{-1}]$.*

To prove this theorem, We use the idea of a Newton polygon and the following proposition :

Proposition 1. *(Weiss, pp 73-75) Let*

$$P(Y) = A_n Y^n + A_{n-1}Y^{n-1} + \cdots + A_1 Y + A_0$$

with $A_n A_0 \neq 0$ be a polynomial over $\mathbb{F}_q[X]$. Let $\mathbf{K}_P$ the set of slopes of its Newton polygon. Then for all $k = \dfrac{\deg A_{r+m} - \deg A_r}{m} \in \mathbf{K}_P$

- *(i) P has m roots $\alpha_1, \cdots, \alpha_m$ such that* $\mid \alpha_1 \mid = \cdots = \mid \alpha_m \mid = e^{-k}$
- *(ii) the polynomial* $P_k(Y) = \prod_{i=1}^{m}(Y - \alpha_i)$ *and* $P(Y) = \prod_{k \in \mathbf{K}_P} P_k(Y)$

Proposition 2. *Let $P(Y) = Y^n + A_{n-1}Y^{n-1} + \cdots + A_1 Y + A_0$ with $A_0 \neq 0$ be a polynomial over $\mathbb{F}_q[X]$ of degree $\geq k+1$. Then, P has exactly k roots with modulus strictly greater than 1 and all the remaining roots lie inside of the unit disc if and only if $|A_{n-k}| > |A_i|$ for all $i \neq n-k$.*

Proof. "$\Longrightarrow$" Let $\omega_1, \cdots, \omega_n$ be the roots of P. Assuming that

$$|\omega_1| \geq \cdots \geq |\omega_k| > |\omega_{n-k+1}| \geq \cdots \geq |\omega_n|$$

Using the Viète theorem, we get

$$|A_{n-l}| = \mid \sum_{i_1 < \cdots < i_l \leq n} \omega_{i_1} \cdots \omega_{i_l} \mid \leq \mid \omega_1 \cdots \omega_l \mid < \mid \omega_1 \cdots \omega_k \mid = |A_{n-k}|$$

"$\Longleftarrow$" Suppose that $|A_{n-k}| > |A_i|$ for all $i \neq n-k$. It is easy to remark, using the Viète theorem, that P has at least one root with modulus strictly greater than 1. Assume now, that P has $l \neq k$ roots $\omega_1, \cdots, \omega_l$ such that

$$|\omega_1| \geq \cdots \geq |\omega_l| > |\omega_{n-l+1}| \geq \cdots \geq |\omega_n|.$$

Therefore, we get two cases:
Case 1 : $l < k$, then from the above we can conclude that $|A_{n-l}| > |A_i|$ for all $i \neq n-l$, which contraduct our assume.
Case 2 : $l > k$, we have

$$\begin{aligned} |A_{n-l}| &= \mid \textstyle\sum_{i_1 < \cdots < i_l \leq n} \omega_{i_1} \cdots \omega_{i_l} \mid \\ &= \mid \omega_1 \cdots \omega_l \mid \\ &> \mid \textstyle\sum_{i_1 < \cdots < i_l \leq n} \omega_{i_1} \cdots \omega_{i_k} \mid \\ &\geq |A_{n-k}| \end{aligned}$$

Contraduction.

Proof. of theorem 5; Using the proposition 2, P has exactly k-Pisot elements.

Since $\deg A_{n-k} > k \max_{1 \leq i \leq k-1} \deg A_{n-i}$, therefore, the upper Newton polygon of P contains the line segment joining $(n, 0)$ to $(n-1, \deg A - n - 1)$. The slope of this line segment is $-\dfrac{\deg A_{n-k}}{k}$. Applaying the proposition 1, item (i), P has $n-(n-k) = k$ Pisot elements with same absolute value

$$\mid \omega_1 \mid = \cdots = \mid \omega_k \mid = q^{\dfrac{\deg A_{n-k}}{k}}$$

So that, $\omega_1, \cdots, \omega_k \notin \mathbb{F}_q((X^{-1}))$.

Now, assume that P decomposes as $P(Y) = Q(Y)H(Y)$, such that Q, H are defined as follow:

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

where $Q(Y), H(Y) \in \mathbb{F}_q[X][Y] \setminus \mathbb{F}_q$.

Case 1 : If one of the polynomials Q or H, say Q, vanishes all the k roots with absolute values greater than 1. which implies that everyone of the roots of H have an absolute values less than 1. which, given $\mid H_0 \mid \geq 1$, is not possible.

Case 2 : If Q have l roots with absolute values greater than 1 and H have l roots with absolute values greater than 1, such that $l + m = k$. Then,

$$\deg Q_{s-l} > \deg_{i \neq s-l} Q_i, \text{ and } \deg H_{t-m} > \deg_{i \neq t-m} Q_i.$$

Or $\deg A_{n-k} > k \max_{1 \leq i \leq k-1} \deg A_{n-i}$, then $\deg Q_{s-l} = \deg H_{t-m}$. In addition

$$\deg A_{n-k} = \deg \sum_{i+j=k} Q_{s-i}H_{t-j} = \deg Q_{s-l} + \deg H_{t-m} = 2 \deg Q_{s-l}.$$

Absurd. Then, we deduce that P is irreducible over $\mathbb{F}_q[X]$.

Acknowledgements

The authors extend their appreciation to Umm Al-Qura University, Saudi Arabia for funding this research work through grant number: 25UQU4270201GSSR01.

Funding

This research work was funded by Umm Al-Qura University, Saudi Arabia under grant number : 25UQU4270201GSSR01.

References

[1] Oussama Dammak and Saber Mansour. On salem formal power series. *European Journal of Pure and Applied Mathematics*, 15(3):1321–1330, 2022.

[2] Ahmed Cherchem, Soufyane Bouguebrine, and Hamza Boughambouz. On the construction of irreducible and primitive polynomials from fqm [x] to fq [x]. *Finite Fields and Their Applications*, 78:101971, 2022.

[3] Stephan Lipka. Über die irreduzibilität von polynomen. *Mathematische Annalen*, 118(1):235–245, 1941.

[4] Ravindranathan Thangadurai. Irreducibility of polynomials whose coefficients are integers. *Mathematics Newsletter*, 17:29–61, 2007.
[5] HL Dorwart. Irreducibility of polynomials. *The American Mathematical Monthly*, 42(6):369–381, 1935.
[6] 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.
[7] A Chandoul, M Jellali, and M Mkaouar. Irreducibility criterion over finite fields. *Communications in Algebra*, 39(9):3133–3137, 2011.