Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43)** : 1–13.
ISSN-0037-8712
doi:10.5269/bspm.76034

Construction of Irreducible Polynomials over $\mathbb{F}_5$ and $\mathbb{F}_7$

Neetu Dhiman*, Balkaran Singh, Praveen Agarwal and Shabnam Sharma

ABSTRACT: Construction of irreducible polynomials is crucial because of their implications in formulating error correcting codes, linear feedback shift register designs and to study algebraic complexity of polynomials. Irreducible polynomials also help us to generate non-zero elements of finite fields. In this manuscript, we construct and characterize the structure of $\mathbb{F}^*_{5^n}$ and $\mathbb{F}^*_{7^n}$ in terms of conjugate elements. Further, a technique to generate degree n irreducible polynomials over $\mathbb{F}_5$ and $\mathbb{F}_7$ is also developed.

Key Words: Finite fields, irreducible polynomials, conjugate elements.

Contents

1. Introduction

Finite fields have important role to play in the areas of coding theory and cryptography [8,11]. The initial work in the theory of finite fields was done by Fermat, Euler, Lagrange and Legendre [8]. Further, Gauss $(1777 - 1885)$ and Galois $(1811 - 1832)$ gave the structure of $GF(p^n)$, also called Galois field, where p is a prime.

Finite fields are the fields with finite number of elements. Because of the high relevance of finite fields in many research areas, indepth knowledge of the structure of finite fields is very essential and study of irreducible polynomials is helpful in this task. To write the elements of extension field of a finite field, one needs to construct irreducible polynomials which are quite easy to construct in case of finite fields with lesser number of elements. But, when the characteristic of a finite field increases significantly it becomes very hard to construct the irreducible polynomials. Therefore, constructing irreducible polynomials over finite fields having large number of elements is a challenging problem nowdays, see [2,3,4,5,9,19]. Irreducible polynomials over finite fields have various implimentations in many research areas particularly in cryptography, digital communications and coding theory. Irreducible polynomials also plays fundamental role in generation of galois field used in public key cryptosystem. In the recent years, these polynomials over finite fields are constructed extensively by iteration and composition methods, one may refer to

[*] Corresponding author.
2010 *Mathematics Subject Classification:* 11T06, 12E05, 12E020.
Submitted March 08, 2025. Published September 30, 2025

[7,10,15,16,17,18].
A rational transformation is used by panario et al. [12] for the recursive construction of irreducible polynomials, where authors obtained sequences of irreducible polynomial $\{g_i\}$ over $\mathbb{F}_q$ with degree $(g_i) = mL^i$, where $L/(q+1), m = 2s, s \in \mathbb{Z}^+$ and L is not congruent to 2 module 4. Abrahamyan et al. [1], discussed the irreducibility of composition of polynomials $(x^p - bx + h)f\Big(\dfrac{x^p - bx + c}{x^p - bx + h}\Big)$ over finite fields and gave two simple explicit recursive constructions of sequences of irreducible polynomials of degree $n2^k$ and np^k over $\mathbb{F}_{2^s}$ and $\mathbb{F}_p$ respectively. Graner and Kyureghyan [6] constructed minimal polynomial m_{β^k}, where $k \in \mathbb{Z}^+$ such that $k \nmid (q-1)$ and $\beta \in \mathbb{F}_{q^n}$ for a given minimal polynomial $g = m_\beta$ over $\mathbb{F}_q$. In the present manuscript, we extend the work done by Sharma et. al [13], where structure of elements $\mathbb{F}^*_{3^n}$ were characterized along with generating positive degree n irreducible polynomials over $\mathbb{F}_3$.
The manuscript is organised in five sections. The first section gives a brief introduction about the work done. Second section presents the preliminaries, which are helpful for the better understanding of paper. Third section describes the structure of elements of structure of $\mathbb{F}^*_{5^n}$ and $\mathbb{F}^*_{7^n}$ in such a way that conjugate elements comes in same column. Further, we construct irreducible polynomials of degree 2 over $\mathbb{F}_5$ and $\mathbb{F}_7$ using conjugates of elements. In the fourth section, we describe about the conjugates of elements in the n^{th} row from the ending of the n^{th} row and construct irreducible polynomials of degree 3 over $\mathbb{F}_5$. Finally in fifth section we conclude our results.

2. Preliminaries

The notations used in this paper are :

- n and r are positive integers.
- p is a prime number.
- $F = \mathbb{F}_q$ is a finite field with q elements.
- $q = p^n$, $n \in \mathbb{Z}^+$.

2.1. Structure of non zero elements of $\mathbb{F}_{p^n}$

Consider a vector space $F = \mathbb{F}_{q^n}$ over a finite field $K = \mathbb{F}_q$. Then, there are two types of bases, first one is polynomial basis and other is normal basis. Polynomial basis is defined as :

$$\langle 1, \xi, \xi^q, \xi^{q^2}, \ldots, \xi^{q^{n-1}} \rangle$$

consists of the powers of primitive element $\xi \in F$ such that,

$$\xi^{q^n - 1} \equiv 1 \pmod{p}.$$

The normal basis is denoted as $\langle \xi, \xi^q, \xi^{q^2}, \ldots, \xi^{q^{n-1}} \rangle$, where $\xi \in F$ is a suitable element.
It is evident that the conjugate relation consitutes a relation which is equivalence and the two elements are related to each other if they both belong to same column. The notations $[\xi^k]$ and $[[k]]$ are substitutably applied to signify conjugate class $[\xi^k]$ and [[[i]]] indicate column ξ^i.
Some definitions related to the paper are given below :

Definition 2.1 *[8] A polynomial $l(x) \in \mathbb{F}[x]$ is said to be irreducible in $\mathbb{F}[x]$, if and only if there does not exist a non constant polynomials $p(x), q(x) \in \mathbb{F}[x]$, such that $l(x) = p(x)q(x)$.*

Definition 2.2 *[8] Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^n}$, where K is subfield of F such that $F = K[x]/\big(f(x)\big)$, for degree n irreducible polynomial $f(x)$. Then the conjugates of $\xi \in \mathbb{F}_{q^n}$ are :*

$$\xi, \xi^q, \xi^{q^2}, \ldots, \xi^{q^{n-1}}.$$

Definition 2.3 *[11] For $\xi \in F = \mathbb{F}_{q^n}$, $Tr_{F/K}(\xi)$ of ξ that is trace of ξ over K is defined as:*

$$Tr_{F/K}(\xi) = \xi + \xi^q + \xi^{q^2} + \cdots + \xi^{q^{n-1}},$$

where $K = \mathbb{F}_q$.

3. Conjugates of elements of $\mathbb{F}^*_{5^n}$ and $\mathbb{F}^*_{7^n}$ from the beginning of the n^{th} row

In this section, Proposition 3.1 and 3.2 classify conjugate classes of the elements of $\mathbb{F}^*_{5^n}$ and $\mathbb{F}^*_{7^n}$ respectively from the beginning of the n^{th} row. In addition to this, structures of non-zero elements of $\mathbb{F}^*_{5^n}$ and $\mathbb{F}^*_{7^n}$ are constructed with the help of conjugate elements.

Proposition 3.1 *Let $\xi^{5^{n-1}+s}$, $\xi^{5s+1} \in \mathbb{F}^*_{5^n}$, where $s = 0, 1, 2, \dots, (4 \cdot 5^{n-1} - 1)$. Then, $\xi^{5^{n-1}+s}$ and ξ^{5s+1} belongs to the same conjugate class.*

Proof: Here,

$$\begin{aligned}
[\xi^{5^{n-1}+s}] &= [(\xi^{5^{n-1}+s})^5] \\
&= [\xi^{5 \cdot 5^{n-1}+5s}] \\
&= [\xi^{5^n+5s}] \\
&= [\xi^{5s+1}].
\end{aligned}$$

Thus, $\xi^{5^{n-1}+s}$ and ξ^{5s+1} belongs to the same conjugate class. □

3.1. Structure of non-zero elements in $\mathbb{F}_{5^n}$

The structure of non-zero elements of $\mathbb{F}_{2^n}$ and $\mathbb{F}_{3^n}$ along with the construction of irreducible polynomials of degree 2 and 3 is discussed in [14] and [13] respectively.
A characterization of the conjugate classes of elements of $\mathbb{F}^*_{5^n}$ from the beginning of the n^{th} row is presented using Proposition 3.1.

Classes of type $[[\xi^{5^{n-1}+s}]]$ for $s = 0, 1, 2, \dots, (4 \cdot 5^{n-1} - 1)$

Now find conjugates of $\xi \in \mathbb{F}^*_{5^n}$ by the help of proposition 3.1.
When $s = 0$, $[\xi^{5^{n-1}}] = [\xi^1]$ $=[\xi^{5^n}]$.

The column $[\xi^1]$, that is, [[[1]]] is of length n and it has n number of conjugates of $\xi^{5^{n-1}}$ in [[[1]]].

When $s = 1$, $[\xi^{5^{n-1}+1}] = [\xi^6]$ $=[\xi^{5^{n-1}+5^{n-2}}]$.
The column $[\xi^6]$, that is, [[[6]]] is of length n and it has $n-1$ number of conjugates of $\xi^{5^{n-1}+1}$ in [[[6]]].

When $s = 2$, $[\xi^{5^{n-1}+2}] = [\xi^{11}]$ $=[\xi^{5^{n-1}+5^{n-1}+5^{n-2}}]$.

The column $[\xi^{11}]$, that is, [[[11]]] is of length $n-1$ and it has $n-1$ number of conjugates of $\xi^{5^{n-1}+2}$ in [[[11]]].

Continuing in the same manner,
When $s = 5^{n-1}$, $[\xi^{5^{n-1}+5^{n-1}}] = [\xi^{5[5^{n-1}]+1}] = [\xi^{5^n+1}] = [\xi^2] = [\xi^{5^{n-1}+5^{n-1}}]$.

The column $[\xi^{5^{n+1}}]$, that is, $[[[5^{n+1}]]]$ is of length n and it has n number of conjugates of $[\xi^{5^{n-1}+5^{n-1}}]$ in $[[[5^{n+1}]]]$.

When $s = 5^{n-1}+5^{n-1}+5^{n-1}+5^{n-1}-2$, $[\xi^{5^{n-1}+5^{n-1}+5^{n-1}+5^{n-1}+5^{n-1}-2}] = [\xi^{5[5^{n-1}+5^{n-1}+5^{n-1}+5^{n-1}-2]+1}]$ $= [\xi^{5^n+5^n+5^n+5^n-10+1}] = [\xi^{5^n-6}]$.

The column $[\xi^{5^n-6}]$ that is, $[[[5^n - 6]]]$ is of length $n - [log_5(5^n - 6)] = 1$ and it has 1 conjugate of $[\xi^{5^{n-1}+5^{n-1}+5^{n-1}+5^{n-1}-2}]$ in $[[[5^n - 6]]]$.

When $s = 5^{n-1}+5^{n-1}+5^{n-1}+5^{n-1}-1$, $[\xi^{5^{n-1}+5^{n-1}+5^{n-1}+5^{n-1}+5^{n-1}-1}] = [\xi^{5[5^{n-1}+5^{n-1}+5^{n-1}+5^{n-1}-1]+1}]$ $= [\xi^{5^n+5^n+5^n+5^n-5+1}] = [\xi^{5^n-1}]$.

The column $[\xi^{5^n-1}]$ that is, $[[[5^n - 1]]]$ is of length $n - [log_5(5^n - 1)] = 1$ and it has 1 conjugate of $[\xi^{5^{n-1}+5^{n-1}+5^{n-1}+5^{n-1}-1}]$ in $[[[5^n - 1]]]$.

For any primitive element ξ of $\mathbb{F}^*_{5^n}$, the structure of $\mathbb{F}^*_{5^n}$ is as follows :

$$\begin{array}{llllllllllllllllllll}
\xi &&&&& \xi^2 &&&&& \xi^3 &&&&& \xi^4 &&&& \\
\xi^5 & \xi^6 & \xi^7 & \xi^8 & \xi^9 & \xi^{10} & \xi^{11} & \xi^{12} & \xi^{13} & \xi^{14} & \xi^{15} & \xi^{16} & \xi^{17} & \xi^{18} & \xi^{19} & \xi^{20} & \xi^{21} & \xi^{22} & \xi^{23} & \xi^{24} \\
\xi^{25} & \ldots & \ldots &&&&&&&&&&&&&&&&& \\
. &&&&&&&&&&&&&&&&&&& \\
. &&&&&&&&&&&&&&&&&&&
\end{array}$$

Structure of $\mathbb{F}^*_{5^n}$.

3.2. Conjugates of elements of $\mathbb{F}^*_{7^n}$ from starting of n^{th} row

Proposition 3.2 *The elements $\xi^{7^{n-1}+s}$ and ξ^{7s+1} of $\mathbb{F}^*_{7^n}$ belongs to identical conjugate class, where $s = 0, 1, 2, \ldots, (6 \cdot 7^{n-1} - 1)$.*

Proof: It is easy to observe that,

$$\begin{aligned}
[\xi^{7^{n-1}+s}] &= [(\xi^{7^{n-1}+s})^7] \\
&= [\xi^{7 \cdot 7^{n-1}+7s}] \\
&= [\xi^{7^n+7s}] \\
&= [\xi^{7s+1}].
\end{aligned}$$

Hence, the elements $\xi^{7^{n-1}+s}$ and ξ^{7s+1} of $\mathbb{F}^*_{7^n}$ are in identical conjugate class. □

3.3. Structure of non-zero elements of $\mathbb{F}^*_{7^n}$

By the help of Proposition 3.2, we can find the conjugate of each element in the structure of $\mathbb{F}^*_{7^n}$ starting from the beginning of the n^{th} row as explained below :

Classes of type $[[\xi^{7^{n-1}+s}]]$ for $s = 0, 1, 2, \ldots, (6 \cdot 7^{n-1} - 1)$
Classes of conjugates of $\mathbb{F}^*_{7^n}$ are given as follows :
When $s = 0$, $[\xi^{7^{n-1}}] = [\xi^1]$ $=[\xi^{7^n}]$.

The column $[\xi^1]$, that is, $[[[1]]]$ is of length n and it has n number of conjugates of $\xi^{7^{n-1}}$ in $[[[1]]]$.

When $s = 1$, $[\xi^{(7^{n-1}+1)}] = [\xi^8]$ $=[\xi^{(7^{n-1}+7^{n-2})}]$.
The column $[\xi^8]$, that is, $[[[8]]]$ is of length n and it has $n-1$ number of conjugates of $\xi^{7^{n-1}+1}$ in $[[[8]]]$.

When $s = 2$, $[\xi^{(7^{n-1}+2)}] = [\xi^{15}]$ $=[\xi^{(7^{n-1}+7^{n-1}+7^{n-2})}]$.

The column $[\xi^{15}]$, that is, $[[[15]]]$ is of length $n-1$ and it has $n-1$ number of conjugates of $\xi^{7^{n-1}+2}$ in $[[[1]]]$.

Procedding in the same way,

When $s = 7^{n-1}$, $[\xi^{(7^{n-1}+7^{n-1})}] = [\xi^{(7[7^{n-1}]+1)}] = [\xi^{(7^n+1)}] = [\xi^2] = [\xi^{(7^{n-1}+7^{n-1})}]$.

The column $[\xi^{7^{n+1}}]$ that is, $[[[7^{n+1}]]]$ is of length n and it has n number conjugates of $[\xi^{(7^{n-1}+7^{n-1})}]$ in $[[[7^{n+1}]]]$.

When $s = (7^{n-1} + 7^{n-1} + 7^{n-1} + 7^{n-1} + 7^{n-1} + 7^{n-1} - 2)$, $[\xi^{(7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}-2)}]$ $= [\xi^{(7[7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}-2]+1)}] = [\xi^{(7^n+7^n+7^n+7^n+7^n+7^n-14+1)}] = [\xi^{(7^n-8)}]$.

The column $[\xi^{(7^n-8)}]$ that is, $[[[(7^n - 8)]]]$ is of length $(n - [log_7(7^n - 8))] = 1$ and it has 1 conjugate of $[\xi^{(7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}-2)}]$ in $[[[(7^n - 8)]]]$.

When $s = (7^{n-1} + 7^{n-1} + 7^{n-1} + 7^{n-1} + 7^{n-1} + 7^{n-1} - 1)$, $[\xi^{(7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}-1)}]$ $= [\xi^{(7[7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}-1]+1)}] = [\xi^{(7^n+7^n+7^n+7^n+7^n+7^n-7+1)}] = [\xi^{(7^n-1)}]$.

The column $[\xi^{(7^n-1)}]$ that is,$[[[(7^n - 1)]]]$ is of length $(n - [log_7(7^n - 1))] = 1$ and it has one conjugate of $[\xi^{(7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}+7^{n-1}-1)}]$ in $[[[(7^n - 1)]]]$.

For any primitive element $\xi \in \mathbb{F}^*_{7^n}$, structure is formed in different parts as given below:

$$\begin{array}{lllllllllllllllll}
\xi & & & & & & & & & \xi^{2} & & & & & & & \xi^{3}\\
\xi^{7} & \xi^{8} & \xi^{9} & \xi^{10} & \xi^{11} & \xi^{12} & \xi^{13} & \xi^{12} & \xi^{13} & \xi^{14} & \xi^{15} & \xi^{16} & \xi^{17} & \xi^{18} & \xi^{19} & \xi^{20} & \xi^{21}
\end{array}$$

Structure of $\mathbb{F}^*_{7^n}$, part(1),

$$\begin{array}{llllllllllllllll}
 & & & & & & \xi^{4} & & & & & & & \xi^{5} & & \\
\xi^{22} & \xi^{23} & \xi^{24} & \xi^{25} & \xi^{26} & \xi^{27} & \xi^{28} & \xi^{29} & \xi^{30} & \xi^{31} & \xi^{32} & \xi^{33} & \xi^{34} & \xi^{35} & \xi^{36} & \xi^{37}
\end{array}$$

Structure of $\mathbb{F}^*_{7^n}$, part(2),

$$\begin{array}{llllllllllllllll}
 & & & & \xi^{6} & & & & & & & \xi^{7} & & & & \\
\xi^{38} & \xi^{39} & \xi^{40} & \xi^{41} & \xi^{42} & \xi^{43} & \xi^{44} & \xi^{45} & \xi^{46} & \xi^{47} & \xi^{48} & \xi^{49} & \xi^{50} & \xi^{51} & \xi^{52} & \xi^{53}\\
\cdot & & & & & & & & & & & & & & & \\
\cdot & & & & & & & & & & & & & & & \\
\cdot & & & & & & & & & & & & & & & \\
\ldots & & & & & & & & & & & & & & &
\end{array}$$

Structure of $\mathbb{F}^*_{7^n}$, part(3),

Structure of $\mathbb{F}^*_{7^n}$.

4. Construction of irreducible polynomials over $\mathbb{F}_5$ and $\mathbb{F}_7$ from beginning of n^{th} row

Structures of $\mathbb{F}^*_{5^2}$ and $\mathbb{F}^*_{7^2}$ are described here. Characterization of elements of $\mathbb{F}^*_{5^2}$ and $\mathbb{F}^*_{7^2}$ is given in such a way that conjugate elements occur in same column. Here, the notation $(0), (1), (2), (3) \ldots$ denotes the column by which the polynomials $f_0, f_1, f_2, f_3, \ldots$ are constructed respectively.

4.1. Construction of irreducible polynomials over $\mathbb{F}_5$

Structure of $\mathbb{F}_{5^2}$ can be given as :

ξ					ξ^2					ξ^3					ξ^4				
ξ^5	ξ^6	ξ^7	ξ^8	ξ^9	ξ^{10}	ξ^{11}	ξ^{12}	ξ^{13}	ξ^{14}	ξ^{15}	ξ^{16}	ξ^{17}	ξ^{18}	ξ^{19}	ξ^{20}	ξ^{21}	ξ^{22}	ξ^{23}	ξ^{24}
(0)	(*)	(1)	(2)	(3)	(4)	(1)	(*)	(5)	(6)	(7)	(2)	(5)	(*)	(8)	(9)	(3)	(6)	(8)	(*)

Structure of $\mathbb{F}^*_{5^2}$.

By Proposition 3.1, we know that $[\xi^{5^{n-1}+r}]$ and $[\xi^{5r+1}]$ are conjugates and these conjugates are the roots of irreducible polynomials in $\mathbb{F}^*_{5^2}$ over $\mathbb{F}_5$. By changing the value of r, we get all the conjugate elements and hence irreducible polynomials. The symbol "(*)" means there is no irreducible polynomials of degree 2.

Therefore, the second degree irreducible polynomials over $\mathbb{F}_5$ using conjugate element are constructed as described below :

$$f_0(x) = \prod_{i=0}^{1}(x - \xi^{5^i}),$$

$$f_1(x) = (x - \xi^7)(x - \xi^{11}),$$

$$f_2(x) = (x - \xi^8)(x - \xi^{16}),$$

$$f_3(x) = (x - \xi^9)(x - \xi^{21}),$$

$$f_4(x) = \textstyle\prod_{i=0}^{1}(x - \xi^{2\times 5^i}),$$

$$f_5(x) = (x - \xi^{13})(x - \xi^{17}),$$

$$f_6(x) = (x - \xi^{14})(x - \xi^{22}),$$

$$f_7(x) = \textstyle\prod_{i=0}^{1}(x - \xi^{3\times 5^i}),$$

$$f_8(x) = (x - \xi^{19})(x - \xi^{23})$$

and

$$f_9(x) = \textstyle\prod_{i=0}^{1}(x - \xi^{4\times 5^i}).$$

4.2. Construction of irreducible polynomials of degree 2 over $\mathbb{F}_7$

As described in the subsection 3.3 of section 3, the structure of $\mathbb{F}^*_{7^2}$ is given as follows :

ξ							ξ^2							ξ^3
ξ^7	ξ^8	ξ^9	ξ^{10}	ξ^{11}	ξ^{12}	ξ^{13}	ξ^{14}	ξ^{15}	ξ^{16}	ξ^{17}	ξ^{18}	ξ^{19}	ξ^{20}	ξ^{21}
(0)	(*)	(1)	(2)	(3)	(4)	(5)	(6)	(*)	(*)	(7)	(8)	(9)	(10)	(11)

Structure of $\mathbb{F}^*_{7^2}$, part(1),

						ξ^4							ξ^5		
ξ^{22}	ξ^{23}	ξ^{24}	ξ^{25}	ξ^{26}	ξ^{27}	ξ^{28}	ξ^{29}	ξ^{30}	ξ^{31}	ξ^{32}	ξ^{33}	ξ^{34}	ξ^{35}	ξ^{36}	ξ^{37}
(2)	(7)	(*)	(12)	(13)	(14)	(15)	(3)	(8)	(12)	(*)	(16)	(17)	(18)	(4)	(9)

Structure of $\mathbb{F}^*_{7^2}$, part(2),

				ξ^6						
ξ^{38}	ξ^{39}	ξ^{40}	ξ^{41}	ξ^{42}	ξ^{43}	ξ^{44}	ξ^{45}	ξ^{46}	ξ^{47}	ξ^{48}
(19)	(16)	(*)	(20)	(21)	(5)	(10)	(14)	(17)	(20)	(*)

Structure of $\mathbb{F}^*_{7^2}$, part(3).

Structure of $\mathbb{F}^*_{7^2}$.

According to Proposition 3.2, $\xi^{7^{n-1}+s}$ and ξ^{7s+1} of $\mathbb{F}^*_{7^n}$ are in identical conjugate class. Conjugate elements are roots of irreducible polynomials over $\mathbb{F}_7$. So, by computing conjugate elements we can construct the following irreducible polynomials of second degree over $\mathbb{F}_7$:

$$f_0(x) = \prod_{i=0}^{1}(x - \xi^{7^i}),$$

$$f_1(x) = (x - \xi^9)(x - \xi^{15}),$$

$$f_2(x) = (x - \xi^{10})(x - \xi^{22}),$$

$$f_3(x) = (x - \xi^{11})(x - \xi^{29}),$$

$$f_4(x) = (x - \xi^{12})(x - \xi^{36}),$$

$$f_5(x) = (x - \xi^{13})(x - \xi^{43}),$$

$$f_6(x) = \prod_{i=0}^{1}(x - \xi^{2\times 7^i}),$$

$$f_7(x) = (x - \xi^{23})(x - \xi^{17}),$$

$$f_8(x) = (x - \xi^{18})(x - \xi^{30}),$$

$$f_9(x) = (x - \xi^{19})(x - \xi^{37}),$$

$$f_{10}(x) = (x - \xi^{20})(x - \xi^{44}),$$

$$f_{11}(x) = \prod_{i=0}^{1}(x - \xi^{3\times 7^i}),$$

$$f_{12}(x) = (x - \xi^{25})(x - \xi^{31}),$$

$$f_{13}(x) = (x - \xi^{26})(x - \xi^{38}),$$

$$f_{14}(x) = (x - \xi^{27})(x - \xi^{45}),$$

$$f_{15}(x) = \prod_{i=0}^{1}(x - \xi^{4\times 7^i}),$$

$$f_{16}(x) = (x - \xi^{33})(x - \xi^{39}),$$

$$f_{17}(x) = (x - \xi^{34})(x - \xi^{46}),$$

$$f_{18}(x) = \prod_{i=0}^{1}(x - \xi^{5\times 7^i}),$$

$$f_{19}(x) = (x - \xi^{38})(x - \xi^{26}),$$

$$f_{20}(x) = (x - \xi^{41})(x - \xi^{47})$$

and

$$f_{21}(x) = \prod_{i=0}^{1}(x - \xi^{6\times 7^i}).$$

5. Conjugate of elements in n^{th} row from the ending of the n^{th} row

In this section, we classify the conjugate elements of $\mathbb{F}_{5^n}^*$ from the ending of the n^{th} row and find some special classes of irreducible polynomials. Further, structure of $\mathbb{F}_{5^3}^*$ is given and with the use of Proposition 5.1 irreducible polynomials of degree 3 are generated over $\mathbb{F}_5$.

Proposition 5.1 *Let ξ^{5^n-k}, $\xi^{5^n-(5k-4)} \in \mathbb{F}_{5^n}^*$, where $k = 0, 1, 2, \ldots, (5^{n-1} - 1)$. Then ξ^{5^n-k} and $\xi^{5^n-(5k-4)}$ belongs to the same conjugate class.*

Proof: Let $\xi = \xi^{5^n-k}$

$$\begin{aligned} \xi^5 &= [(\xi^{5^n-k})^5] \\ &= [\xi^{5\cdot 5^n-5k}] \\ &= [\xi^{5^n+4\cdot 5^n-5k}] \\ &= [\xi^{5^n+4-5k}] \\ &= [\xi^{5^n-(5k-4)}]. \end{aligned}$$

Thus, ξ^{5^n-k} and $\xi^{5^n-(5k-4)}$ belongs to the same conjugate class. □

Theorem 5.1 *For $t_1, t_2, \ldots, t_l \in \mathbb{Z}^+$ such that $t_1 > t_2 > t_3 > \cdots > t_l \geq 0$, $s+t_1 \leq n-1$ and $s \in \mathbb{Z}^+ \cup \{0\}$. Then, the conjugate of $\xi^{5^n-(5^{s+t_1}+5^{s+t_2}+5^{s+t_3}+\cdots+5^{s+t_l}+1)}$ is $\xi^{5^n-(5^{s+t_1+1}+5^{s+t_2+1}+5^{s+t_3+1}+\cdots+5^{s+t_l+1}+1)}$ and*

$$\begin{aligned} [[5^n - (5^{t_1} + 5^{t_2} + 5^{t_3} + \cdots + 5^{t_l} + 1)]] &= [[5^n - (5^{t_1+1} + 5^{t_2+1} + 5^{t_3+1} + \cdots + 5^{t_l+1} + 1)]] \\ &= [[5^n - (5^{t_1+2} + 5^{t_2+2} + 5^{t_3+2} + \cdots + 5^{t_l+2} + 1)]] \\ &= \ldots \\ &.. \end{aligned}$$

Proof:

We know that,

$$\begin{aligned} \left(\xi^{5^n-(5^{s+t_1}+5^{s+t_2}+5^{s+t_3}+\cdots+5^{s+t_l}+1)}\right)^5 &= \xi^{5^{n+1}-(5^{s+t_1+1}+5^{s+t_2+1}+5^{s+t_3+1}+\cdots+5^{s+t_l+1}+5)} \\ &= \xi^{5^n+5^n+5^n+5^n+5^n-(5^{s+t_1+1}+5^{s+t_2+1}+5^{s+t_3+1}+\cdots+5^{s+t_l+1}+5)} \\ &= \xi^{5^n+4-(5^{s+t_1+1}+5^{s+t_2+1}+5^{s+t_3+1}+\cdots+5^{s+t_l+1}+5)} \\ &= \xi^{5^n-(5^{s+t_1+1}+5^{s+t_2+1}+5^{s+t_3+1}+\cdots+5^{s+t_l+1}+1)} \end{aligned}$$

and

$$\begin{aligned}[[5^n-(5^{t_1}+5^{t_2}+5^{t_3}+\cdots+5^{t_l}+1)]] &= [[5^n+4-5(5^{t_1}+5^{t_2}+5^{t_3}+\cdots+5^{t_l}+1)]]\\ &= [[5^n-\big((5^{t_1+1}+5^{t_2+1}+5^{t_3+1}+\cdots+5^{t_l+1}+5)-4\big)]]\\ &= [[5^n-(5^{t_1+1}+5^{t_2+1}+5^{t_3+1}+\cdots+5^{t_l+1}+1)]].\end{aligned}$$

□

Proposition 5.1 and Theorem 5.1 are used to find the irreducible polynomials of some special classes.

Class of type $\xi^{5^n-(5^s+1)}$:

Using Theorem 5.1, $\xi^{5^n-(5^{s+t_1})}$ for $s=0,1,\ldots,n-1$ are n^{th} row conjugates of $\xi^{5^{n-2}}$ as given below :

$$\begin{aligned}[[5^n-2]] &= [[5^n-6]]\\ &= [[5^n-26]\\ &= \ldots \qquad\qquad\qquad\qquad\qquad\qquad = ..\\ &= .\\ &= [[5^n-5^{n-1}-1]].\end{aligned}$$

Hence, the polynomials which are irreducible are :

$$\prod_{s=0}^{n-1}\big(x-\xi^{5^n-(5^s+1)}\big).$$

In this way, we can obtain irreducible polynomials for different classes of conjugate elements as follows:

- Irreducible polynomials in the class of type $\xi^{5^n-(5^{s+1}+5^s+1)}$ are :

$$\prod_{s=0}^{n-1}\big(x-\xi^{5^n-(5^{s+1}+5^s+1)}\big).$$

- Irreducible polynomials in the class of type $\xi^{5^n-(5^{s+2}+5^s+1)}$:

$$\prod_{s=0}^{n-1}\big(x-\xi^{5^n-(5^{s+2}+5^s+1)}\big).$$

- Irreducible polynomials in the class of type $\xi^{5^n-(5^{s+3}+5^s+1)}$:

$$\prod_{s=0}^{n-1}\big(x-\xi^{5^n-(5^{s+3}+5^s+1)}\big).$$

- Irreducible polynomials in the class of type $\xi^{5^n-(5^{s+4}+5^s+1)}$:

$$\prod_{s=0}^{n-1}\big(x-\xi^{5^n-(5^{s+4}+5^s+1)}\big).$$

5.1. Construction of degree 3 irreducible polynomials over $\mathbb{F}_5$ from the ending of n^{th} row

In the following structure, Proposition 5.1 is used for the generation of degree 3 irreducible polynomials over $\mathbb{F}_5$, we proceed with the elements that has been placed in the end of the n^{th} row in structure of $\mathbb{F}^*_{5^3}$:

ξ															
ξ^{5}					ξ^{6}					ξ^{7}					ξ^{8}
ξ^{25}	ξ^{26}	ξ^{27}	ξ^{28}	ξ^{29}	ξ^{30}	ξ^{31}	ξ^{32}	ξ^{33}	ξ^{34}	ξ^{35}	ξ^{36}	ξ^{37}	ξ^{38}	ξ^{39}	ξ^{40}
(0)	(39)	(36)	(29)	(16)	(39)	(*)	(35)	(28)	(15)	(37)	(35)	(33)	(27)	(14)	(31)

Structure of $\mathbb{F}^*_{5^3}$, part(1),

					ξ^{2}															
ξ^{9}					ξ^{10}					ξ^{11}					ξ^{12}					ξ^{13}
ξ^{45}	ξ^{46}	ξ^{47}	ξ^{48}	ξ^{49}	ξ^{50}	ξ^{51}	ξ^{52}	ξ^{53}	ξ^{54}	ξ^{55}	ξ^{56}	ξ^{57}	ξ^{58}	ξ^{59}	ξ^{60}	ξ^{61}	ξ^{62}	ξ^{63}	ξ^{64}	ξ^{65}
(19)	(15)	(11)	(7)	(3)	(38)	(37)	(34)	(26)	(12)	(36)	(35)	(33)	(25)	(11)	(34)	(33)	(*)	(24)	(10)	(30)

Structure of $\mathbb{F}^*_{5^3}$, part(2),

									ξ^{3}										
				ξ^{14}					ξ^{15}					ξ^{16}					ξ^{17}
ξ^{66}	ξ^{67}	ξ^{68}	ξ^{69}	ξ^{70}	ξ^{71}	ξ^{72}	ξ^{73}	ξ^{74}	ξ^{75}	ξ^{76}	ξ^{77}	ξ^{78}	ξ^{79}	ξ^{80}	ξ^{81}	ξ^{82}	ξ^{83}	ξ^{84}	ξ^{85}
(27)	(24)	(21)	(9)	(18)	(14)	(10)	(6)	(2)	(32)	(31)	(30)	(23)	(8)	(29)	(28)	(27)	(22)	(7)	(26)

Structure of $\mathbb{F}^*_{5^3}$, part(3),

														ξ^{4}					
				ξ^{18}					ξ^{19}					ξ^{20}					ξ^{21}
ξ^{86}	ξ^{87}	ξ^{88}	ξ^{89}	ξ^{90}	ξ^{91}	ξ^{92}	ξ^{93}	ξ^{94}	ξ^{95}	ξ^{96}	ξ^{97}	ξ^{98}	ξ^{99}	ξ^{100}	ξ^{101}	ξ^{102}	ξ^{103}	ξ^{104}	ξ^{105}
(25)	(24)	(21)	(6)	(23)	(22)	(21)	(*)	(5)	(17)	(13)	(9)	(5)	(1)	(20)	(19)	(18)	(17)	(4)	(16)

Structure of $\mathbb{F}^*_{5^3}$, part(4),

				ξ^{22}					ξ^{23}					ξ^{24}
ξ^{106}	ξ^{107}	ξ^{108}	ξ^{109}	ξ^{110}	ξ^{111}	ξ^{112}	ξ^{113}	ξ^{114}	ξ^{115}	ξ^{116}	ξ^{117}	ξ^{118}	ξ^{119}	ξ^{120}
(15)	(14)	(13)	(3)	(12)	(11)	(10)	(9)	(2)	(8)	(7)	(6)	(5)	(1)	(4)

Structure of $\mathbb{F}^*_{5^3}$, part(5),

ξ^{41}	ξ^{42}	ξ^{43}	ξ^{44}				
				ξ^{121}	ξ^{122}	ξ^{123}	ξ^{124}
(28)	(25)	(22)	(13)	(3)	(2)	(1)	(*)

Structure of $\mathbb{F}^*_{5^3}$, part(5),

Structure of $\mathbb{F}^*_{5^3}$,

The construction irreducible polynomials of degree 3 over $\mathbb{F}_5$ using conjugate elements obtained here are :

$$f_0(x) = \prod_{i=0}^{2}(x - \xi^{5^i}),$$

$$f_1(x) = (x-\xi^{123})(x-\xi^{119})(x-\xi^{99}),$$

$$f_2(x) = (x-\xi^{122})(x-\xi^{114})(x-\xi^{74}),$$

$$f_3(x) = (x-\xi^{121})(x-\xi^{109})(x-\xi^{49}),$$

$$f_4(x) = (x-\xi^{104})\prod_{i=0}^{1}(x-\xi^{5^i\times 24}),$$

$$f_5(x) = (x-\xi^{118})(x-\xi^{94})(x-\xi^{98}),$$

$$f_6(x) = (x-\xi^{117})(x-\xi^{89})(x-\xi^{73}),$$

$$f_7(x) = (x-\xi^{116})(x-\xi^{84})(x-\xi^{48}),$$

$$f_8(x) = (x-\xi^{79})\prod_{i=0}^{1}(x-\xi^{23\times 5^i}),$$

$$f_9(x) = (x-\xi^{113})(x-\xi^{69})(x-\xi^{97}),$$

$$f_{10}(x) = (x-\xi^{112})(x-\xi^{64})(x-\xi^{72}),$$

$$f_{11}(x) = (x-\xi^{111})(x-\xi^{59})(x-\xi^{47}),$$

$$f_{12}(x) = (x-\xi^{54})\prod_{i=0}^{1}(x-\xi^{22\times 5^i}),$$

$$f_{13}(x) = (x-\xi^{108})(x-\xi^{44})(x-\xi^{96}),$$

$$f_{14}(x) = (x-\xi^{107})(x-\xi^{39})(x-\xi^{71}),$$

$$f_{15}(x) = (x-\xi^{106})(x-\xi^{34})(x-\xi^{46}),$$

$$f_{16}(x) = (x-\xi^{29})\prod_{i=0}^{1}(x-\xi^{21\times 5^i}),$$

$$f_{17}(x) = (x-\xi^{103})\prod_{i=0}^{1}(x-\xi^{19\times 5^i}),$$

$$f_{18}(x) = (x-\xi^{102})\prod_{i=0}^{1}(x-\xi^{14\times 5^i}),$$

$$f_{19}(x) = (x-\xi^{101})\prod_{i=0}^{1}(x-\xi^{9\times 5^i}),$$

$$f_{20}(x) = \prod_{i=0}^{2}(x-\xi^{4\times 5^i}),$$

$$f_{21}(x) = (x-\xi^{92})(x-\xi^{88})(x-\xi^{68}),$$

$$f_{22}(x) = (x-\xi^{91})(x-\xi^{83})(x-\xi^{43}),$$

$$f_{23}(x) = (x-\xi^{78})\prod_{i=0}^{1}(x-\xi^{18\times 5^i}),$$

$$f_{24}(x) = (x-\xi^{87})(x-\xi^{63})(x-\xi^{67}),$$

$$f_{25}(x) = (x-\xi^{58})(x-\xi^{86})(x-\xi^{42}),$$

$$f_{26}(x) = (x-\xi^{53})\prod_{i=0}^{1}(x-\xi^{17\times 5^i}),$$

$$f_{27}(x) = (x-\xi^{82})(x-\xi^{38})(x-\xi^{66}),$$

$$f_{28}(x) = (x-\xi^{81})(x-\xi^{33})(x-\xi^{41}),$$

$$f_{29}(x) = (x-\xi^{28})\prod_{i=0}^{1}(x-\xi^{16\times 5^i}),$$

$$f_{30}(x) = (x-\xi^{77})\prod_{i=0}^{1}(x-\xi^{13\times 5^i}),$$

$$f_{31}(x) = (x-\xi^{76})\prod_{i=0}^{1}(x-\xi^{8\times 5^i}),$$

$$f_{32}(x) = \prod_{i=0}^{2}(x-\xi^{3\times 5^i}),$$

$$f_{33}(x) = (x-\xi^{61})(x-\xi^{57})(x-\xi^{37}),$$

$$f_{34}(x) = (x-\xi^{52})\prod_{i=0}^{1}(x-\xi^{12\times 5^i}),$$

$$f_{35}(x) = (x-\xi^{56})(x-\xi^{36})(x-\xi^{32}),$$

$$f_{36}(x) = (x-\xi^{27})\prod_{i=0}^{1}(x-\xi^{11\times 5^i}),$$

$$f_{37}(x) = (x-\xi^{51})\prod_{i=0}^{1}(x-\xi^{7\times 5^i}),$$

$$f_{38}(x) = \prod_{i=0}^{2}(x-\xi^{2\times 5^i})$$

and

$$f_{39}(x) = (x-\xi^{26})\prod_{i=0}^{1}(x-\xi^{6\times 5^i}).$$

6. Conclusion

The structures of non zero elements of $\mathbb{F}_{5^n}$ and $\mathbb{F}_{7^n}$ using conjugate of any primitive element of the extension fields $\mathbb{F}_{5^n}$ and $\mathbb{F}_{7^n}$ are presented in the present communication. Then, a characterization of conjugate classes of the elements of $\mathbb{F}^*_{5^2}$, $\mathbb{F}^*_{7^2}$ and $\mathbb{F}^*_{5^3}$ is disscussed. Further, irreducible polynomials of positive degree n are constructed over $\mathbb{F}_5$ and $\mathbb{F}_7$ showing implication of the above mentioned structures from the beginning and ending of the n^{th} row. The results derived in the manuscript have application in coding theory and cryptography.

Statements and Declarations

The authors have no conflict of interest.

Acknowledgments

The second author acknowledge the financial assistance of CSIR.

References

1. S. Abrahamyan, M. Alizadeh, and M. K. Kyureghyan, *Recursive constructions of irreducible polynomials over finite fields,* Finite Fields and Their Applications, vol. 18, no. 4, pp. 738-745, (2012).

2. M. Alan and B. Duman, *A note on construction of irreducible polynomials over finite fields with characteristic 2*, International Journal of Pure and Applied Mathematics, vol. 115, no. 3, pp. 529-532, (2017).

3. M. Alizadeh, *Constructing methods for irreducible polynomials,* Mathematical Problems of Computer Science, vol. 35, pp. 26-32, (2011).

4. K. Cheng, *A new direction on constructing irreducible polynomials over finite fields,* Finite Fields and Their Applications, vol. 95, pp. 102368, (2024).

5. S. D. Cohen, *On irreducible polynomials of certain types in finite fields,* Mathematical Proceedings of the Cambridge Philosophical Society, vol. 66, no. 2, pp. 335-344 (1969).
6. A. M. Graner and G. M. Kyureghyan, *Constructing irreducible polynomials recursively with a reverse composition method,* Designs, Codes and Cryptography, vol. 92, no. 3, pp. 695-708, (2024).
7. G. M. Kyureghyan and M. K. Kyureghyan, *A recurrent construction of irreducible polynomials of fixed degree over finite fields,*Applicable Algebra in Engineering, Communication and Computing, vol. 33, no. 2, pp. 163-71, (2022).
8. R. Lidl and H. Niederreiter *Finite Fields*, Cambridge University Press, Second Edition, (1983).
9. C. Luo, Y. Wang, Y. Fu, P. Zhou and M. Wang, *Constructing dynamic S-boxes based on chaos and irreducible polynomials for image encryption,* Nonlinear Dynamics, vol. 112, pp. 6695-6713, (2024).
10. H. Meyn, *On the construction of irreducible self-reciprocal polynomials over finite fields*, Applicable Algebra in Engineering, Communication and Computing, vol. 1, pp. 43-53, (1990).
11. G. L. Mullen, and D. Panario, *Handbook of Finite Fields*, CRC Press, (2013).
12. D. Panario, L. Reis and Q. Wang, *Construction of irreducible polynomials through rational transformations,* Journal of Pure and Applied Algebra, vol. 224, no. 5, pp. 106241, (2020).
13. P. L. Sharma, S. Sharma and M. Rehan, *On construction of irreducible polynomials over* $\mathbb{F}_3$*,* Journal of Discrete Mathematical Sciences and Cryptography, vol. 18, no. 4, pp. 335-347, (2015).
14. R. K. Sharma, W. Shukla and S. Ramasamy, *A note on identification of irreducible polynomials over* $\mathbb{F}_2$, International Electronic Journal of Pure and Applied Mathematics, vol. 4, no. 2, pp. 59-70 (2012).
15. V. Shoup, *Fast construction of irreducible polynomials over finite fields,*Journal of Symbolic Computation, vol. 17, no. 5, pp. 371-91, (1994).
16. V. Shoup, *New algorithms for finding irreducible polynomials over finite fields,*Mathematics of Computation, vol. 54, no. 189, pp. 435-47, (1990).
17. A., Bassa, G. Bisson and R. Oyono, *Iterative constructions of irreducible polynomials from isogenies*, Finite Fields and Their Applications, vol. 97, pp. 102429, (2024).
18. A. Cherchem, Bouguebrine, S. and H. Boughambouz, *On the construction of irreducible and primitive polynomials from* $\mathbb{F}_{q^m}[x]$ *to* $\mathbb{F}_q[x]$*,* Finite Fields and Their Applications, vol. 78, pp. 101971, (2022).
19. R. Kim, *Some relations between the irreducible polynomials over a finite field and its quadratic extension,* Discrete Applied Mathematics, vol. 344, pp. 106-111, (2024).

Neetu Dhiman,
University Institute of Technology,
Himachal Pradesh University, Shimla, 171005,
Himachal Pradesh, India.
E-mail address: dhimanneetu278@gmail.com

and

Balkaran Singh,
Department of Mathematics and Statistics,
Himachal Pradesh University, Shimla, 171005,
Himachal Pradesh, India.
E-mail address: balkaransingh895@gmail.com

and

Praveen Agarwal,
Department of Mathematics,
Anand International College of Engineering, Jaipur, 303012,
Rajasthan, India.
E-mail address: praveen.agarwal@anandice.ac.in

and

Shabnam Sharma,
PVCNSSK Govt. Polytechnic College, Bilaspur, 174035,
Himachal Pradesh, India.
E-mail address: shabz0887@gmail.com