Construction of Irreducible Polynomials in Galois fields, $GF(2^m)$ Using Normal Bases.

Abraham Aidoo[1], Kwasi Baah Gyamfi[1]

1. *Department of Mathematics, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana.*

Email:*abramkhems09@gmail.com, kwasibaahgyamfi1@gmail.com*

Abstract
This thesis is about Construction of Polynomials in Galois fields Using Normal Bases in finite fields.In this piece of work, we discussed the following in the text; irreducible polynomials, primitive polynomials, field, Galois field or finite fields, and the order of a finite field. We found the actual construction of polynomials in $GF(2^m)$ with degree less than or equal to $m-1$ and also illustrated how this construction can be done using normal bases. Finally, we found the general rule for construction of $GF(p^m)$ using normal bases and even the rule for producing reducible polynomials.

Mathematics Subject Classification: 20D99
Keywords: Irreducible polynomials, Primitive polynomials, Field, Finite fields, Order of a finite field, Normal Bases.

1 Introduction

1.1 Background Of Study

Normal basis in field theory is a special kind of basis for Galois extensions of finite degree, characterised as forming a single orbit for the Galois group. Every finite Galois extension of fields has a normal basis. In algebraic number theory, the study of the more refined question of the existence of a normal integral basis is part of Galois module theory.

In the case of finite fields, this means that each of the bases elements is related to any one of them by applying the Frobenius $p-th$ power mapping repeatedly, where p is the characteristic of the field. Let GF(p^m) be a field with p^m elements, and γ an element of it such that the m elements are linearly independent. Then this set forms a normal basis for GF(p^m) over GF(p). In addition, let F_q be the finite field of order q, where $q = p^m$, p is a prime and m is a natural number. Its extension of degree m, F_{q^m}, is generated algebraically over F_q by a root γ of a (monic) irreducible polynomial $f(x) \in F_q[x]$ of degree m, i.e., $F_{q^m} = F_q(\gamma)$. The Galois group of F_{q^m} over F_q is cyclic and is generated by the Frobenius mapping $\phi(\gamma) = \gamma^q$, $\gamma \in F_{q^m}$ .The set of roots of f then comprises the conjugates $\{\gamma, \gamma^q, \cdots, \gamma^{q^{m-1}}\}$ of γ, [5].

Often it is helpful if γ is a generator of the cyclic multiplicative group $F^*_{q^m}$ (of order q^{m-1}), in which case γ is called a primitive element of F_{q^m}. The conjugates of a primitive element γ of F_{q^m} form the roots of a (monic irreducible) primitive polynomial $f(x) \in F_q[x]$ of degree m.

Alternatively, an element γ that generates F_{p^m} additively could be sought. Though the additive structure of F_{p^m} is apparently more complicated, viewed as a GF-module (G being the Galois group of F_{p^m} over F_q), F_{p^m} is cyclic too. The classical expression of the normal basis theorem is that there exists an element γ whose conjugates form a basis of F_{p^m} over F_p.

Irreducible polynomial $f(x) \in F_q[x]$ of degree m whose roots constitute such a basis is called a normal basis. Then f is referred to as a normal polynomial over F_q and any of its root is called a normal element. Now, because of the subtleties of the $GF-$module structure, it is neither automatic that a normal basis of F_{p^m} over F_p is a normal basis over an intermediate field F_{p^d} (where $d \mid m$) nor vice versa.
There is still less connection between the multiplicative and additive structures of F_{p^m}, a primitive polynomial $f(x) \in F_p[x]$ of degree m need not be normal, or a primitive polynomial normal. Nevertheless, for every extension F_{p^m}/F_p, by Lenstra and Schoof (1987), there exists a polynomial $f(x) \in F_p[x]$ of degree m which is both primitive and normal.

The construction of normal basis of F_p over F_{p^m} is another challenging area. In view of that, much work has not been done in construction of irreducible polynomials in $F_{2^m}[x]$ using normal bases. In this work, a computationally simple construction of polynomials using normal bases over F_{2^n} is presented as well as the formulation of the general rule for constructing polynomials in the field under consideration.

2 Preliminary Definitions And Basic Theorems

In this section we discuss some terms, their supporting theorems and proofs.

2.1 Irreducible Polynomial

2.1.1 Definition

A polynomial $f(x)$ is irreducible in GF(q) if $f(x)$ cannot be factored into product of lower-degree polynomials in GF(q)[x], [2].

1. A polynomial may be irreducible in one ring of polynomials, but reducible in another.
2. In GF(2)[x], if $f(x)$ has degree > 1 and has an even number of terms, then it can't be irreducible. Because 1 is its root, and hence $x + 1$ is one of its factor.

2.1.1 Theorem
Let f be a polynomial over a field (such as the rationals). Then f is irreducible if and only if $g = f(ax+b)$, $a \neq 0$, is irreducible. If f is a polynomial over the integers, then f is irreducible if and only if $g = f(x+b)$ is irreducible, [3].

Proof: We shall show the contrapositive, namely, f is reducible over a area if and most effective if $g = f(ax + b)$, $a \neq 0$, is reducible. Suppose f is reducible. Then $f = p(x)q(x)$ for some polynomials p, q of advantageous diploma. By substituting $ax+b$ for x, we get that $g(x) = f(ax+b) = p(ax+b)q(ax+b)$, whence g is reducible. Note that there is no difference here between fields and integers. Suppose $g = f(ax + b)$ is reducible. Then $g = g(x) = f(ax + b) = p(x)q(x)$ for a few polynomials p, q of effective degree. By substituting $a^{-1}(x - b)$ for x, we get that $f(x) = p(a^{-1}(x - b))q(a^{-1}(x - b))$, whence f is reducible. Note that we used the fact that during a area, a non-zero element has an inverse. Over the integers, if $f(x + b)$ is reducible, we can duplicate the argument with $a = 1$.

2.2 Primitive polynomials

2.2.1 Definition

A primitive polynomial is the minimal polynomial of a primitive element of the extension field GF(p^m) or a polynomial $f(x)$ with coefficients in GF(p) = Z/pZ is a primitive polynomial if its degree is m and it has a root γ in GF(p^m) such that $\{0, 1, \gamma, \gamma^2, \cdots, \gamma^{p^m-1}\}$ is the entire field GF(p^m), [1].

1. Given an irreducible polynomial of degree m, to test whether it is primitive, divide it from x^{n-1} where $m < n < p^{m-1}$. If no such n gives 0 remainder, then it is primitive. (The case when $n = p^{m-1}$ is guaranteed to have 0 remainder). If there exists n, $m < n < p^{m-1}$, such that the remainder is not 0, then it is not primitive.
2. A primitive polynomial $p(x) \in$ GF(p)[x] is always irreducible in GF(p)[x] (by definition), but irreducible polynomials are not always primitive.
3. All irreducible polynomials in GF(2)[x] of degree $2, 3, 5$ are primitive.

2.2.1 Theorem
Any minimal polynomial of a primitive element $a \in GF(p^n)$ with $p \geq 2$ prime and $n \geq 1$ is a primitive polynomial, [3].
Proof : Let $f(x)$ be the minimal polynomial of the primitive field element a. Recall a field always contains a primitive element and minimal polynomials exist for each field element. We'll show x is a generator of the field. Suppose to the contrary, that $x^m \equiv 1\ (mod\ f(x), p)$ for some m, $1 \leq m \leq p^m - 2$. Then there is an $g(x)$ such that $x^m - 1 \equiv g(x)f(x)(mod p)$ Since f is a minimal polynomial of a, it has a as

a root: $f(a) \equiv 0\,(mod\, f(x), p)$ so $a^m \equiv 1\,(modf(x), p)$ contradicting the primitivity of 'a' because its order is not maximal. By Fermat's theorem for fields, the non-zero element x satisfies $x^{p^n-1} \equiv 1\ (modf(x), p)$ so x is a generator of the field, and $f(x)$ is a primitive polynomial. ■

2.3 Field

2.3.1 Definition

A field is one of the fundamental algebraic structures used in abstract algebra. It is a commutative ring in which each non-zero element has an inverse, [2].

2.3.1 Theorem

For a prime p and a monic irreducible $\pi(x)$ in $F_p[x]$ of degree m, the ring $Fp[x]/(\pi(x))$ is a field of order p^m, [1].

Proof: The cosets $mod\pi(x)$ are represented by remainders $b_0 + b_1x + \cdots + b_{m-1}x^{m-1}; b_i \in Fp$; and there are p^m of these. Since the $\pi(x)$ is irreducible, the ring $F_p[x]/(\pi(x))$ is a field using the same proof that $Z/(m)$ is a field when m is prime. □

2.4 Finite Field or Galois Field

2.4.1 Definition

A field is said to be a Galois field if it contains finite number of elements. As with any field, a finite field is a set with the operations of multiplication, addition, subtraction and division defined satisfying certain basic rule, [3]. The most common examples of finite fields are given by the integer $modp$ when p is a prime number.

2.4.1 Theorem

For every prime power p^n, a field of order p^n exists, [4].

Proof: Taking our cue from the declaration of Lemma 2.9.1, allow F be a field extension of F_p over which $x^{p^m} - x$ splits absolutely. General theorems from finite theory guarantee there may be such a field. Inside F, the roots of $x^{p^m} - x$ form the set $S = \{t \in F : t^{p^m} = t\}$. This set has length p^m since the polynomial $x^{p^m} - x$ is separable: $(x^{p^m} - x)' = p^m x^{p^m-1} - 1 = -1$ because $p = 0$ in F, so $x^{p^m} - x$ has no roots in common with its derivative. It splits completely over F and has degree p^m, so it has p^m roots in F. We will display S as a sub-field of F. It contains 1 and is simply closed under multiplication and (for nonzero solutions) inversion. It remains to expose S is an additive group. Since $p = 0$ in F, $(a + b)^p = a^p + b^p$ for all a and b in F (the intermediate terms in $(a + b)^p$ coming from the binomial theorem have integral coefficients $\begin{pmatrix} p \\ k \end{pmatrix}$, which are all multiples of p and thus vanish in F). Therefore the pth power map $t \mapsto t^p$ on F is additive. The map $t \mapsto t^{p^n}$ is also additive since it's the n-fold composite of $t \mapsto t^p$ with itself and the composition of homomorphisms is a homomorphism. The fixed factors of an additive map are a group under addition, so S is a group under addition. Therefore S is a field of order p^n.

2.5 Order of Finite Fields

2.5.1 Definition

The number of elements of a finite field is known as its order. A finite field of order q exists if and most effective if the order q is a prime power p^k (p is a prime number and k is a positive integer).

2.5.1 Theorem

Any finite field has prime power order, [1].

Proof: For every commutative ring R there is a unique ring homomorphism $Z \longrightarrow R$, given by

$$m \longmapsto \begin{cases} 1+1+\cdots+1, & \text{if} \quad m \geq 0, \\ m \quad \text{times} & \\ -(1+1+\cdots+1), & \text{if} \quad m < 0. \\ \quad \mid m \mid \quad \text{times} & \end{cases} \tag{1}$$

We apply this to the case when $R = F$ is a finite field. The kernel of $Z \longrightarrow F$ is nonzero since Z is infinite and F is finite. Write the kernel as $(m) = mZ$ for an integer $m > 0$, so $Z/(m)$ embeds as a subring of F. Any subring of a field is a domain, so m has to be a prime number, say $m = p$. Therefore there is an embedding $Z/(p) \hookrightarrow F$. Viewing F as a vector space over $Z/(p)$, it is finite-dimensional since F is finite. Letting $n = dim_{Z/(p)}(F)$ and picking a basis $\{e_1, \cdots, e_n\}$ for F over $Z/(p)$, elements of F can be written uniquely as $c_1e_1 + \cdots + c_ne_n$, $c_i \in Z/(p)$: Each coefficient has p choices, so $\sharp F = p^n$, [4]. $\square$

2.6 Algebraic Extension

2.6.1 Definition

Let E be a finite field extension of F (F is a subfield of E). An element $\gamma \in E$ is said to be algebraic over F if there exist element $a^1, a^2, \cdots, a^n \in F$, $n \geq 1$, not all equal to zero such that $a_o + a_1\gamma + a_2\gamma^2 + \cdots + a_n\gamma^n = 0$. In other words, an element $\gamma \in E$ is algebraic over F if there exist a non-constant polynomial $q(x) \in F[x]$ such that $q(\gamma) = 0$. Otherwise γ is called transcendental over F, [3].

2.6.1 Theorem
Let F_q be a finite field and F_{q^n} a finite extension field. Then F_{q^n} is a simple algebraic extension of F_q and every primitive element of F_{q^n} can serve as a defining element of F_{q^n} over F_q , [3].
Proof: Let ξ be a primitive element (the generator of the cyclic group F_q^* of F_{q^n}. We clearly have $F_q(\xi)$ $\subseteq F_{q^n}$. On the other hand, $F_q(\xi)$ contains 0 and all powers of ξ, and so all elements of F_{q^n}. Therefore $F_{q^n} = F_q(\xi)$. $\square$

2.7 Normal basis

2.7.1 Definition

Let $K = F_q$ and $F = F_{q^m}$. Then a basis of F over K of the form $\{\gamma, \gamma^q, \cdots, \gamma^{q^{m-1}}\}$, consisting of a suitable element $\gamma \in F$ and its conjugates with respect to K, is referred to as a normal bases of F over K.

2.7.1 Theorem
Let $N = \{\beta_0, \beta_1, \cdots, \beta_{n-1}\}$ be a normal bases of F_{q^n} over F_q. Then an element $\gamma = \sum_{i=0}^{n-1} a_i\beta_i$, where $a_i \in F_q$, is a normal element if and only if the polynomial $\gamma(x) = \sum_{i=0}^{n-1} a_ix_i \in F_q[x]$ is relatively prime to $x^n - 1$, [6].

Proof : Note that

$$\begin{pmatrix} \gamma \\ \gamma^q \\ \vdots \\ \gamma^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{n-1} \end{pmatrix}. \tag{2}$$

The n elements $\gamma, \gamma^q, \cdots, \gamma^{q^{n-1}}$ are linearly independent if and only if the circulant matrix $c[a_0, a_1, \cdots, a_{n-1}]$ is nonsingular, that is, if and only if the polynomial $\gamma(x) = \sum_{i=0}^{n-1} a_ix_i \in F_q[x]$ is relatively prime to $x^n - 1$.
$\square$

3 Main Result

3.1 Overview

In this section we present to you how polynomials are constructed in Galois field, and how irreducible polynomials are constructed in $GF(2^m)$ over normal bases.

3.1.1 Construction Of Polynomial Over $GF(p^m)$

The construction of $GF(p^m)$ is basically given as;

$$F_{p^m} = \{a_0 + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1} : a_i \in F_p\} = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{p^m-2}\}, \alpha^{p^m-1} = 1,$$

$\pi(\alpha) = 0$, is a set of polynomials with coefficient in F_p of degree less than or equal to $m-1$.

3.1.2 Multiplication(•) In F_p

In Constructing polynomials in $F_p[x]$, we need an irreducible polynomial $\pi(x)$ of degree m in $F_p[x]$ such that $F_p[x] mod \pi(x)$ produces a polynomial as a remainder which will be of degree less than or equal to $m-1$ and with the choice of $\pi(x)$, we take $\pi(x) = 0$.

For illustration, we first let $q = 4 = 2^2 = p^m$.
$F_{p^m} = \{$polynomials of degree less than or equal to $1 : a_i \in F_p\}$ where $p = 2$ and $m = 2$.
The possible elements of $F_4 = \{0, 1, \alpha, \alpha^2\}$. Taking an irreducible polynomial of degree two, that is, $\pi(x) = x^2 + x + 1$ and for $\pi(x) = 0$ we have $x^2 + x + 1 = 0$, implying that $\alpha^2 = x^2 = x + 1$. So we have the construction as;

$$F_4 = \{0, 1, x, x+1\} = \{0, 1, \alpha, \alpha^2\}, \quad \text{where} \quad \alpha^3 = 1 \quad \text{and} \quad \alpha^4 = 0.$$

Let also consider the case when $q = 8 = 2^3 = p^m$.
$F_{p^m} = \{$polynomials of degree less than or equal to $2 : a_i \in F_p\}$ where $p = 2, m = 3$.
The possible elements of $F_8 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ where $\alpha^7 = 1$ and $\alpha^8 = 0$. Choosing an irreducible polynomial of degree three, ie. $\pi(x) = x^3 + x + 1$, for $\pi(x) = 0$, implying that $x^3 = x + 1$, we have;

$\alpha = x$	$\alpha^5 = x^2 + x + 1$
$\alpha^2 = x^2$	$\alpha^6 = x^2 + 1$
$\alpha^3 = x + 1$	$\alpha^7 = 1$
$\alpha^4 = x^2 + x$	$\alpha^8 = 0$

$\therefore F_8 = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ where $\alpha^7 = 1$ in F_8.

Let $q = 16 = 2^4 = p^m$.
$F_{p^m} = \{$polynomials of degree less than or equal to $3 : a_i \in F_p\}$ where $p = 2, m = 4$.
The possible elements of $F^*_{16} = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}, \alpha^{15}\}$. Choosing an irreducible polynomial of degree four, ie. $\pi(x) = x^4 + x + 1$, for $\pi(x) = 0$, implying that $x^4 = x + 1$, we have;

$\alpha = x$	$\alpha^6 = x^3 + x^2$	$\alpha^{11} = x^3 + x^2 + x$
$\alpha^2 = x^2$	$\alpha^7 = x^3 + x + 1$	$\alpha^{12} = x^3 + x^2 + x + 1$
$\alpha^3 = x^3$	$\alpha^8 = x^2 + 1$	$\alpha^{13} = x^3 + x^2 + 1$
$\alpha^4 = x + 1$	$\alpha^9 = x^3 + x$	$\alpha^{14} = x^3 + 1$
$\alpha^5 = x^2 + x$	$\alpha^{10} = x^2 + x + 1$	$\alpha^{15} = 1$

$\therefore F^*_{16} = \{1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+1, x^3+x, x^3+x^2, x^3+x+1, x^3+x^2+x, x^3+x^2+x+1, x^3+x^2+1\} = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}, \alpha^{15}\}$ where $\alpha^{15} = 1$ in F^*_{16} and each element has a multiplicative inverse.

3.1.3 General Rule for Producing Reducible Polynomials

The general rule below can be used to produce reducible polynomials which is a product of irreducible polynomials where at least one is a primitive polynomial which we used in constructing of Galois field

above using normal bases.

Let consider $GF(8)$, we have $(x^3+x^2+1)(x+1) = x^4+x^2+x+1$

$$= x^{8/2} + x^{8/4} + x + 1$$

$$\left(\sum_{i=2^j}^{8/2} x^{8/i}\right) + x + 1 = 1 + x + \left(\sum_{i=2^j}^{4} x^{8/i}\right) \quad : \text{f or} \quad j = 1, \quad \text{and} \quad 2$$

Therefore we finally have the general rule for constructing reducible polynomial as;

$$f(x) = 1 + x + \left(\sum_{i=2^j}^{q/2} x^{q/i}\right) \tag{3}$$

where $j = 1, 2, 3, \cdots, q$ is the order of $GF(p^m)$, that is $GF(2^m) = GF(q)$ and $\left(\sum_{i=2^j}^{q/2} x^{q/i}\right)$ is zero when $q \leq 2$.

3.1.4 Multiplication In F_{2^m} Using Normal Bases

Here, we first consider multiplication in F_4 to see how the construction is done using normal bases. Let $q = 4 = 2^2 = p^m$. Then $GF(4) = GF(2^2) = F_2(j)/(j^2+j+1)$ which is a polynomial of degree two.
From j^2+j+1 we have $j^2+j = 1$ and $j^2 = j+1$, implying that j^2, j are the bases of $GF(4)$. We know that the generator polynomial for $GF(4)$ is x^2+x+1. Therefore we have the normal bases as $j = (0 \quad 1)$ and $j^2 = j.j = (1 \quad 0)$.
For $j^3 = j.j^2 = j(j+1) = j^2+j$, adding these bases, we have
$j^3 = (1 \quad 0) + (0 \quad 1) = (1 \quad 1)$.

We further consider $q = 8 = 2^3 = p^m$.
The $GF(8) = GF(2^3) = F_2(j)/(j^3+j^2+1)$ which is a polynomial of degree three. From $\alpha(j) = j^3+j^2+1$, for $\alpha(j) = 0$, we have $j^3 = j^2+1$. But the reducible polynomial for $GF(8)$ is $x^4+x^2+x+1 = 0$.
We have, $x^4+x^2+x+1 = 0 = (x^3+x^2+1)(x+1)$ showing that x^3+x^2+1 is the irreducible polynomial because its degree is equal to m of $GF(8)$. So, we multiply through the equation by j to have $j^3.j = j(j^2+1)$.
Then, $j^4 = j^3+j$ but $j^3 = j^2+1$, connoting that, $j^4 = j^2+j+1$, hence the bases of $GF(8)$ are j, j^2, j^4.
The normal bases for $GF(8)$ are as follow;
$j = (0 \quad 0 \quad 1)$, $j = (0 \quad 1 \quad 0)$, $j = (1 \quad 0 \quad 0)$ since $j^4+j^2+j = 1$ in $GF(8)$.
But we know that, $j^4 = j^3+j$.
$j^3 = j^4+j$, so adding these bases, we have
$j^3 = (1 \quad 0 \quad 0) + (0 \quad 0 \quad 1) = (1 \quad 0 \quad 1)$.

Also, $j^5 = j.j^4$ but $j^4 = j^2+j+1$
$j^5 = j.(j^2+j+1) = j^3+j^2+j$. We have the addition as;
$j^5 = (1 \quad 0 \quad 1) + (0 \quad 1 \quad 0) + (0 \quad 0 \quad 1)$
$J^5 = (1 \quad 1 \quad 0)$

For $j^6 = j^2.j^4 = j^2(j^2+j+1) = j^4+j^3+j^2$, adding the bases, we have
$j^6 = (1 \quad 0 \quad 0) + (1 \quad 0 \quad 1) + (0 \quad 1 \quad 0)$
$j^6 = (0 \quad 1 \quad 1)$

For $j^8 = j^4.j^4 = j^4(j^2+j+1) = j^6+j^5+j^4$
$j^8 = (0 \quad 1 \quad 1) + (1 \quad 1 \quad 0) + (1 \quad 0 \quad 0)$
$j^8 = (0 \quad 0 \quad 1)$.

Next, let consider the case when $q = 16 = 2^4 = p^m$. The GF(16) =GF(2^4) is a polynomial of degree 4.
$\pi(j) = 1+j^2+j^4+j^8$ and squaring $\pi(j)$, $\pi(j)^2 = (1+j+j^2+j^4+j^8)^2 = (1+j^2+j^4+j^8+^{16})$.
Therefore we have the bases j, j^2, j^4, j^8, hence $j, j^2, j^4, j^8 = 1 \quad 1 \quad 1 \quad 1$, implying that j is the root of the polynomial $x^8+x^4+x^2+x+1 = 0$ which is the reducing polynomial for GF(16). We factorize the

polynomial $x^8 + x^4 + x^2 + x + 1 = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$ into two irreducible polynomials. This, thus, gives two choices for the construction.
The normal bases for GF(16) are as follow;
$j = (0\ 0\ 0\ 1)$, $j^2 = (0\ 0\ 1\ 0)$, $j^4 = (0\ 1\ 0\ 0)$ and $j^8 = (1\ 0\ 0\ 0)$ since $j + j^2 + j^4 + j^8 = (1\ 1\ 1\ 1)$. So considering the irreducible polynomial $x^4 + x^3 + 1$. $j^3 = j.j^2$ but from the irreducible polynomial, we have $j^3 = j^4 + 1$ and $j^4 = j^3 + 1$. But we know that $j^4 = j^8 + j^2 + j + 1$.
$j^3 + 1 = j^8 + j^2 + j + 1 + 1 \Rightarrow j^3 = j^8 + j^2 + j$
$= (1\ 0\ 0\ 0) + (0\ 0\ 1\ 0) + (0\ 0\ 0\ 1)$
$j^3 = (1\ 0\ 1\ 1)$

for $j^5 = j.j^4 = j(j^3 + 1) = j^4 + j$
$= (0\ 1\ 0\ 0) + (0\ 0\ 0\ 1)$
$j^5 = (0\ 1\ 0\ 1)$

for $j^9 = j.j^8 = j(j^4 + j^2 + j + 1) = j^5 + j^3 + j^2 + j$
$j^9 = (0\ 1\ 0\ 1) + (1\ 0\ 1\ 1) + (0\ 0\ 1\ 0) + (0\ 0\ 0\ 1) = (1\ 1\ 0\ 1)$

for $j^6 = j^2.j^4 = j^2(j^3 + 1) = j^5 + j^2$
$= (0\ 1\ 0\ 1) + (0\ 0\ 1\ 0)$
$j^6 = (0\ 1\ 1\ 1)$

for $j^{10} = j^2.j^8 = j^2(j^4 + j^2 + j + 1) = j^6 + j^4 + j^3 + j^2$
$= (0\ 1\ 1\ 1) + (0\ 0\ 1\ 0) + (1\ 0\ 1\ 1) + (0\ 1\ 0\ 0)$
$j^{10} = (1\ 0\ 1\ 0)$

for $j^{12} = j^4.j^8 = j^4(j^4 + j^2 + j + 1) = j^8 + j^6 + j^5 + j^4$
$= (1\ 0\ 0\ 0) + (0\ 1\ 1\ 1) + (0\ 1\ 0\ 1) + (0\ 1\ 0\ 0)$
$j^{12} = (1\ 1\ 1\ 0)$

for $j^{16} = j^8.j^8 = j^8(j^4 + j^2 + j + 1) = j^{12} + j^{10} + j^9 + j^8$
$= (1\ 1\ 1\ 0) + (1\ 0\ 1\ 0) + (1\ 1\ 0\ 1) + (1\ 0\ 0\ 0)$
$j^{16} = (0\ 0\ 0\ 1)$

We again illustrate the multiplication of the normal bases using $x^4 + x^3 + x^2 + x + 1$. $j = (0\ 0\ 0\ 1)$, $j^2 = (0\ 0\ 1\ 0)$, $j^4 = (0\ 1\ 0\ 0)$ and $j^8 = (1\ 0\ 0\ 0)$.
For $j^3 = j.j^2$ but from the irreducible polynomial, $j^3 = j^4 + j^2 + j + 1$ and $1 = j^4 + j^3 + j^2 + j$. Also, $1 = j^8 + j^4 + j^2 + j$
Then $j^4 + j^3 + j^2 + j = j^8 + j^4 + j^2 + j$
$j^3 = j^8$
$j^3 = (1\ 0\ 0\ 0)$

for $j^5 = j.j^4$
$= j(j^3 + j^2 + j + 1)$
$= j^4 + j^3 + j^2 + j = (0\ 1\ 0\ 0) + (1\ 0\ 0\ 0) + (0\ 0\ 1\ 0) + (0\ 0\ 0\ 1)$
$j^5 = (1\ 1\ 1\ 1)$

for $j^6 = j^2.j^4 = j^2(j^3 + j^2 + j + 1) = j^5 + j^4 + j^3 + j^2$
$= (1\ 1\ 1\ 1) + (0\ 1\ 0\ 0) + (1\ 0\ 0\ 0) + (0\ 0\ 1\ 0)$
$j^6 = (0\ 0\ 0\ 1)$

for $j^9 = j.j^8$; But $j^8 = j^4 + j^2 + j + 1$
$j^9 = j(j^4 + j^2 + j + 1) = j^5 + j^3 + j^2 + j$
$= (1\ 1\ 1\ 1) + (1\ 0\ 0\ 0) + (0\ 0\ 1\ 0) + (0\ 0\ 0\ 1)$
$j^9 = (0\ 1\ 0\ 0)$

for $j^{10} = j^2.j^8 = j^2(j^4 + j^2 + j + 1) = j^6 + j^4 + j^3 + j^2$
$= (1\ 0\ 0\ 1) + (0\ 1\ 0\ 0) + (1\ 0\ 0\ 0) + (0\ 0\ 1\ 0)$
$j10 = (1\ 1\ 1\ 1)$

for $j^{12} = j^4.j^8 = j^4(j^4 + j^2 + j + 1) = j^8 + j^6 + j^5 + j^4$
$= (1\ 0\ 0\ 0) + (0\ 0\ 0\ 1) + (1\ 1\ 1\ 1) + (0\ 1\ 0\ 0)$
$j^{12} = (0\ 1\ 0\ 0)$
for $j^{16} = j^8.j^8 = j^8(j^4 + j^2 + j + 1) = (j^{12} + j^{10} + j^9 + j^8)$
$= (0\ 0\ 1\ 0) + (1\ 1\ 1\ 1) + (0\ 1\ 0\ 0) + (1\ 0\ 0\ 0)$
$j^{16} = (0\ 0\ 0\ 1)$

We consider also the case of $q = 32 = 2^5 = p^m$ which is a polynomial of degree five. The bases associated with GF(32) are j, j^2, j^4, j^8, j^{16}. Therefore the polynomial is $x^{16} + x^8 + x^4 + x^2 + x + 1$. We factorize and get the associated irreducible polynomials
$x^{16}+x^8+x^4+x^2+x+1 = (x+1)(x^5+x^4+x^2+x+1)(x^5+x^4+x^3+x+1)(x^5+x^4+x^3+x^2+1)$ where $(x^5+x^4+x^2+x+1), (x^5+x^4+x^3+x+1), (x^5+x^4+x^3+x^2+1)$ are the irreducible polynomials and these gives us three options. The normal bases for using $x^5 + x^4 + x^2 + x + 1$ is as follows; $j = (0\ 0\ 0\ 0\ 1)$,$j^2 = (0\ 0\ 0\ 1\ 0)$, $j^4 = (0\ 0\ 1\ 0\ 0)$,$j^8 = (0\ 1\ 0\ 0\ 0)$,$j^{16} = (1\ 0\ 0\ 0\ 0)$. Since $\alpha = j + j^2 + j^4 + j^8 + j^{16} = (1\ 1\ 1\ 1)$.
$j^3 = j.j^2$, but from the irreducible polynomial, we have $j^5 = j^4 + j^2 + j + 1$ also $j + j^2 + j^4 + j^8 + j^{16} = 1$
$j^6 = j.j^5 = j(j^4 + j^2 + j + 1) = j^5 + j^3 + j^2 + j$
$= j^4 + j^2 + j + 1 + j^3 + j^2 + j$
$j^6 = j^4 + j^3 + 1$

$j^7 = j.j^6 = j^5 + j^4 + j$
$= j^4 + j^2 + j + 1 + j^4 + j$
$j^7 = j^2 + 1 = j^2 + j + j^2 + j^4 + j^8 + j^{16} = j + j^4 + j^8 + j^{16}$
$j^8 = j.j^7 = j^3 + j$
$j^3 = j^8 + j = (0\ 1\ 0\ 0\ 0) + (0\ 0\ 0\ 0\ 1)$
$j^3 = (0\ 1\ 0\ 0\ 1)$

We know that from above, $j^5 = j^4 + j^2 + j + 1$ *and* $1 = j + j^2 + j^4 + j^8 + j^{16}$
Then, $j^5 = j^4 + j^2 + j + j + j^2 + j^4 + j^8 + j^{16}$
$= j^8 + j^{16}$
$= (0\ 1\ 0\ 0\ 0) + (1\ 0\ 0\ 0\ 1)$
$j^5 = (1\ 1\ 0\ 0\ 0)$

We also know that $j^6 = j^4 + j^3 + 1$, therefore, $j^6 = j^4 + j^3 + j^{16} + j^8 + j^4 + j^2 + j$
$= j^{16} + j^8 + j^3 + j^2 + j$
$= (1\ 0\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 1) + (0\ 0\ 0\ 1\ 0) + (0\ 0\ 0\ 0\ 1)$
$j^6 = (1\ 0\ 0\ 1\ 0)$

For $j.j^8 = j^9 = j(j^3 + j) = j^4 + j^2$
$j^9 = (0\ 0\ 1\ 0\ 0) + (0\ 0\ 0\ 1\ 0)$
$j^9 = (0\ 0\ 1\ 1\ 0)$

For $j.j^8 = j^9 = j(j^3 + j) = j^4 + j^2$
$j^9 = (0\ 0\ 1\ 0\ 0) + (0\ 0\ 0\ 1\ 0)$
$j^9 = (0\ 0\ 1\ 1\ 0)$

For $j^{10} = j^2.j^8 = j^2(j^3 + j) = j^5 + j^3$
$= (1\ 1\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 1)$
$j^{10} = (1\ 0\ 0\ 0\ 1)$

For $j^{12} = j^4.j^8 = j^4(j^3 + j) = j^7 + j^5$
But $j^7 = j^{16} + j^8 + j^4 + j$
$j^{12} = j^{16} + j^8 + j^5 + j^4 + j$
$= (1\ 0\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 0) + (1\ 1\ 0\ 0\ 0) + (0\ 0\ 1\ 0\ 0) + (0\ 0\ 0\ 0\ 1)$
$j^{12} = (0\ 0\ 1\ 0\ 1)$

For $j^{17} = j.j^{16}$ but $= (j^8)^2 = (j^3 + j)^2 = j^7 + j^5$
Then, $j^{17} = j(j^3 + j)^2 = j(j^6 + j^2) = (j^7 + j^3)$

$j^{17} = j + j^4 + j^8 + j^{16} + j^3$ but $j^3 = j^8 + j$
$= j + j^4 + j^8 + j^{16} + j^8 + j$
$= j^{16} + j^4$
$= (1\ 0\ 0\ 0\ 0) + (0\ 0\ 1\ 0\ 0)$
$j^{17} = (1\ 0\ 1\ 0\ 0)$

For $j^{18} = j^2.j^{16} = j^2(j^6 + j^2) = j^8 + j^4$
$= (0\ 1\ 0\ 0\ 0) + (0\ 0\ 1\ 0\ 0)$
$j^{18} = (0\ 1\ 1\ 0\ 0)$

For $j^{20} = j^{16}.j^4 = j^4(j^6 + j^2) = j^{10} + j^6$
$= (1\ 0\ 0\ 0\ 1) + (1\ 0\ 0\ 1\ 0)$
$j^{20} = (0\ 0\ 0\ 1\ 1)$

For $j^{24} = j^{16}.j^8 = j^8(j^6 + j^2) = j^{14} + j^{10}$
but $j^{14} = j^7.j^7 = (j^2 + 1)^2 = j^4 + 1 = j^{16} + j^8 + j^4 + j + j^4 + j^2$
$= j^{16} + j^8 + j$
Hence, $j^{24} = j^{16} + j^{10} + j^8 + j^2 + j$
$= (1\ 0\ 0\ 0\ 1) + (1\ 0\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 0) + (0\ 0\ 0\ 1\ 0) + (0\ 0\ 0\ 0\ 1)$
$j^{24} = (0\ 1\ 0\ 1\ 0)$

For $j^{32} = (j^{16})^2 = (j^6 + j^2)^2 = j^{12} + j^4$
$= (0\ 0\ 1\ 0\ 1) + (0\ 0\ 1\ 0\ 0)$
$j^{32} = (0\ 0\ 0\ 0\ 1)$

For the irreducible polynomial $x^5 + x^4 + x^3 + x + 1$, we have $j = (0\ 0\ 0\ 0\ 1)$,$j^2 = (0\ 0\ 0\ 1\ 0)$, $j^4 = (0\ 0\ 1\ 0\ 1)$,$j^8 = (0\ 1\ 0\ 0\ 0)$,$j^{16} = (1\ 0\ 0\ 0\ 0)$ and $1 = j + j^2 + j^4 + j^8 + j^{16}$. For $j^3 = j^2.j$, but from the polynomial, $j^5 = j^4 + j^3 + j + 1$
$j^6 = j.j^5 = j(j^4 + j^3 + j + 1) = j^5 + j^4 + j^2 + j$
$= j^4 + j^3 + j + 1 + j^4 + j^2 + j$
$j^6 = j^3 + j^2 + 1$

$j^7 = j.j^6 = j^4 + j^3 + j$

$j^8 = j.j^7 = j^5 + j^4 + j^2 = j^4 + j^3 + j + 1 + j^4 + j^2$
$j^8 = j^3 + j^2 + j + 1 = j^3 + j^2 + j + j + j^2 + j^4 + j^8 + j^{16}$
$j^8 = j^{16} + j^8 + j^4 + j^3$
Then, $j^3 = j^8 + j^8 + j^{16} + j^4$
$j^3 = j^{16} + j^8 + j^4 = (1\ 0\ 0\ 0\ 0) + (0\ 0\ 1\ 0\ 0)$
$j^3 = (1\ 0\ 1\ 0\ 0)$

We know that $j^5 = j^4 + j^3 + j + 1 = j^4 + j^3 + j + j + j^2 + j^4 + j^8 + j^{16}$
$= j^{16} + j^8 + j^3 + j^2 = (1\ 0\ 1\ 0\ 0) + (1\ 0\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 0) + (0\ 0\ 0\ 1\ 0)$
$j^3 = (0\ 0\ 1\ 1\ 0)$

We also know that $j^6 = j^3 + j^2 + 1 = j^3 + j^2 + j + j + j^2 + j^4 + j^8 + j^{16} = j^{16} + j^8 + j^4 + j^3 + j$
$= (1\ 0\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 0) + (0\ 0\ 1\ 0\ 0) + (1\ 0\ 1\ 0\ 0) + (0\ 0\ 0\ 0\ 1)$
$j^6 = (0\ 1\ 0\ 0\ 1)$

For $j^9 = j^8.j = j(j^3 + j^2 + j + 1) = j^4 + j^3 + j^2 + j$
$= (0\ 0\ 1\ 0\ 0) + (1\ 0\ 1\ 0\ 0) + (0\ 0\ 0\ 1\ 0) + (0\ 0\ 0\ 0\ 1)$
$j^9 = (1\ 0\ 0\ 1\ 1)$

For $j^{10} = j^2.j^8 = j^2(j^3 + j^2 + j + 1) = j^5 + j^4 + j^3 + j(2)$
$= (0\ 1\ 1\ 1\ 0) + (0\ 0\ 1\ 0\ 0) + (1\ 0\ 1\ 0\ 0) + (0\ 0\ 0\ 1\ 0)$
$j^{10} = (1\ 1\ 1\ 0\ 0)$

For $j^{12} = j^4.j^8 = j^4(j^3 + j^2 + j + 1) = j^7 + j^6 + j^5 + j^4$

but $j^7 = j^4 + j^3 + j$
Then, $j^{12} = j^4 + j^3 + j + j^6 + j^5 + j^(4) = j^6 + j^5 + j^3 + j$
$= (1\ 0\ 1\ 0\ 0) + (0\ 0\ 0\ 0\ 1) + (0\ 1\ 0\ 0\ 1) + (0\ 1\ 1\ 1\ 0)$
$j^{12} = (1\ 0\ 0\ 1\ 0)$

For $j^{17} = j.j^{16} = j.(j^8)^2 = j(j^3 + j^2 + j + 1)^2 = j.(j^6 + j^4 + j^2 + 1) = j^7 + j^5 + j^3 + j$
but $j^7 = j^4 + j^3 + j$
Then, $j^{17} = j^4 + j^3 + j + j^5 + j^3 + j = j^5 + j^4$
$= (0\ 1\ 1\ 1\ 0) + (0\ 0\ 1\ 0\ 0)$
$j^{17} = (0\ 1\ 0\ 1\ 0)$

For $j^{18} = j^2.j^{16} = j^2(j^3 + j^2 + j + 1)^2 = j^2(j^6 + j^4 + j^2 + 1) = j^8 + j^6 + j^4 + j^2$
$= (0\ 1\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 1) + (0\ 0\ 1\ 0\ 0) + (0\ 0\ 0\ 1\ 0)$
$j^{18} = (0\ 0\ 1\ 1\ 1)$

For $j^{20} = j^4.j^{16} = j^4(j^3 + j^2 + j + 1)^2 = j^4(j^6 + j^4 + j^2 + 1) = j^{10} + j^8 + j^6 + j^4$
$= (1\ 1\ 1\ 0\ 0) + (0\ 1\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 1) + (0\ 0\ 1\ 0\ 0)$
$j^{20} = (1\ 1\ 0\ 0\ 1)$

For $j^{24} = j^8.j^{16} = j^8(j^6 + j^4 + j^2 + 1) = j^{14} + j^{12} + j^{10} + j^8$
but $j^{14} = (j^7)^2 = (j^4 + j^3 + j)^2 = j^8 + j^6 + j^2$
Hence, $j^{24} = j^8 + j^6 + j^2 + j^{12} + j^{10} + j^8$
$= j^{12} + j^{10} + j^6 + j^2$
$= (1\ 0\ 0\ 1\ 0) + (1\ 1\ 1\ 0\ 0) + (0\ 1\ 0\ 0\ 1) + (0\ 0\ 0\ 1\ 0)$
$j^{24} = (0\ 0\ 1\ 0\ 1)$

For $j^{32} = (j^{16})^2 = (j^6 + j^4 + j^2 + 1)^2 = j^{12} + j^8 + j^4 + 1 = j^{12} + j^8 + j^4 + j + j^2 + j^4 + j^8 + j^{16}$
$= j^{16} + j^{12} + j^2 + j$
$= (1\ 0\ 0\ 0\ 0) + (1\ 0\ 0\ 1\ 0) + (0\ 0\ 0\ 1\ 0) + (0\ 0\ 0\ 0\ 1)$
$j^{32} = (0\ 0\ 0\ 0\ 1)$

For the irreducible polynomial $x^5 + x^4 + x^3 + x^2 + 1$, we have the normal bases as:
$j^2.j = j^3$, but from the polynomial, $j^5 = j^4 + j^3 + j^2 + j + 1$
$j^6 = j.j^5 = j^5 + j^4 + j^3 + j = j^4 + j^3 + j^2 + 1 + j^4 + j^3 + j$
$j^6 = j^2 + j + 1$

$j^7 = j.j^6 = j(j^2 + j + 1) = j^2 + j^2 + j$
$j^8 = j.j^7 = j^4 + j^3 + j^2$
$= j^3 = j^8 + j^4 + j^2$
$= (1\ 0\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 0) + (0\ 0\ 1\ 0\ 0)$
$j^3 = (0\ 1\ 1\ 1\ 0)$

$j^5 = j^4 + j^3 + j^2 + 1 = j^4 + j^3 + j^2 + j^{16} + j^8 + j^4 + j^2 + j$
$= j^{16} + j^8 + j^3$
$= (1\ 0\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 0) + (0\ 1\ 1\ 1\ 0)$
$j^5 = (1\ 0\ 1\ 1\ 1)$

$j^6 = j^2 + j + 1 = j^2 + j + j + j^2 + j^4 + j^8 + j^{16} = j^{16} + j^8 + j^4$
$= (1\ 0\ 0\ 0\ 0) + (0\ 1\ 0\ 0\ 0) + (0\ 0\ 1\ 0\ 0)$
$j^6 = (1\ 1\ 1\ 0\ 0)$

$j^9 = j.j^8 = j(j^4 + j^3 + j^2) = j^5 + j^4 + j^3$
$= (1\ 0\ 1\ 1\ 1) + (0\ 0\ 1\ 0\ 0) + (0\ 1\ 1\ 1\ 0)$
$j^9 = (1\ 1\ 1\ 0\ 1)$

$j^{10} = j^2.j^8 = j^2(j^4 + j^3 + j^2) = j^6 + j^5 + j^4$
$= (1\ 1\ 1\ 0\ 0) + (1\ 0\ 1\ 1\ 1) + (0\ 0\ 1\ 0\ 0)$
$j^{10} = (0\ 1\ 1\ 1\ 1)$

$j^{12} = j^4.j^8 = j^4(j^4 + j^3 + j^2) = j^8 + j^7 + j^6 = j^8 + j^6 + j^3 + j^2 + j$
$= (0\ 1\ 0\ 0\ 0) + (1\ 1\ 1\ 0\ 0) + (0\ 1\ 1\ 1\ 0) + (0\ 0\ 0\ 1\ 0) + (0\ 0\ 0\ 0\ 1)$
$j^{12} = (1\ 1\ 0\ 0\ 1)$

$j^{17} = j.j^{16} = j(j^8)^2 = j(j^8 + j^6 + j^4) = j^9 + j^7 + j^5 = j^9 + j^5 + j^3 + j^2 + j$
$= (1\ 1\ 1\ 0\ 1) + (1\ 0\ 1\ 1\ 1) + (0\ 1\ 1\ 1\ 0) + (0\ 0\ 0\ 1\ 0) + (0\ 0\ 0\ 0\ 1)$
$j^{17} = (0\ 0\ 1\ 1\ 1)$

$j^{18} = j^2.j^{16} = j^2(j^8 + j^6 + j^4) = j^{10} + j^8 + j^6$
$= (0\ 1\ 1\ 1\ 1) + (0\ 1\ 0\ 0\ 0) + (1\ 1\ 1\ 0\ 0)$
$j^{18} = (1\ 1\ 0\ 1\ 1)$

$j^{20} = j^4.j^{16} = j^4(j^8 + j^6 + j^4) = j^{12} + j^{10} + j^8$
$= (1\ 1\ 0\ 0\ 1) + (0\ 1\ 1\ 1\ 1) + (0\ 1\ 0\ 0\ 0)$
$j^{20} = (1\ 1\ 1\ 1\ 0)$

$j^{24} = j^8.j^6 = j^8(j^8 + j^6 + j^4) = j^{16} + j^{14} + j^{12}$
but $\quad j^{14} = (j^7)^2 = (j^3.j^2 + j)^2 = (j^6 + j^4 + j^2)$
Hence, $j^{24} = j^{16} + j^{12} + j^6 + j^4 + j^2$
$= (1\ 0\ 0\ 0\ 0) + (1\ 1\ 0\ 0\ 1) + (1\ 1\ 1\ 0\ 0) + (0\ 0\ 1\ 0\ 0) + (0\ 0\ 0\ 1\ 0)$
$j^{24} = (1\ 0\ 0\ 1\ 1)$

$j^{32} = (j^{16})^2 = (j^8 + j^6 + j^4)^2 = j^{16} + j^{12} + j^8$
$= (1\ 0\ 0\ 0\ 0) + (1\ 1\ 0\ 0\ 1) + (0\ 1\ 0\ 0\ 0)$
$j^{32} = (0\ 0\ 0\ 0\ 1)$

3.1.5 General Construction Of $GF(p^m)$ Using Normal Bases

We postulate the general rule for constructing Galois field using the normal bases expressed above.

For all Γ, $\beta \in GF(p^m)$, we uniquely express them as;

$$\beta = \sum_{k=0}^{m-1} b_k j^{p^k}, \quad \text{and} \quad \Gamma = \sum_{i=0}^{m-1} a_i j^{p^i}, \qquad \forall a_i, b_k \in F_2$$

Let

$$Z = \Gamma \bullet \beta$$

$$Z = \left(\sum_{i=0}^{m-1} a_i j^{p^i}\right) \bullet \left(\sum_{k=0}^{m-1} b_k j^{p^k}\right)$$

$$Z = \sum_{i=0}^{m-1} \sum_{k=0}^{m-1} \left(a_i b_k j^{p^i} \bullet j^{p^k}\right) \tag{4}$$

4 Conclusion

In conclusion, polynomials from Galois fields using normal bases have been constructed as well as the general rule for constructing polynomials in finite fields with normal bases in the field under consideration.

References

[1] Anthony Y. Aidoo, Kwasi Baah-Gyamfi, Joseph Ackora-Prah, *Explicit construction of finite fields using normal bases*, International Journal of Pure and Applied Mathematics, Volume 70 No. 4 2011 (2011), 559-569.

[2] Rotman, J. J., *A first course in abstract algebra with application,* (3/E), Pearson Education, Inc., 2006.

[3] Lidl, R., and Niederreiter, H., *Introduction to Finite Fields and their applications,* Cambridge University Press, 1997.

[4] Conrad, K. finite fields:, *http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/ finitefields.pdf*

[5] Girstmair, K., *An algorithm for the construction of a normal basis*, International Journal of Pure and Applied Mathematics, Volume 70 No. 4 2011 (2011), 559-569.

[6] Mahmood Alizadeh, Saeid Mehrabi, *Construction of self-reciprocal normal polynomials over finite fields of even characteristic*, Turkish Journal of Mathematics ht tp://journals.tubitak.gov.t r/ma th/ (2015).