Lecture 2

Finite Fields and Vector Spaces

2.1 Binary Arithmetic and Field

- Consider the binary set, $\{0, 1\}$. Define two binary operations, called addition "$+$" and multiplication "$\cdot$", on this set as follows:

$$\begin{aligned} 0 + 0 &= 0 & 0 \cdot 0 &= 0 \\ 0 + 1 &= 1 & 0 \cdot 1 &= 0 \\ 1 + 0 &= 1 & 1 \cdot 0 &= 0 \\ 1 + 1 &= 0 & 1 \cdot 1 &= 1 \end{aligned}$$

This two operations are commonly called modulo-2 addition and multiplication, respectively.

- The set $\{0, 1\}$ together with modulo-2 addition and multiplication is said to form a binary field, denoted GF(2). This **binary field** GF(2) plays an important role in error control coding.

2.2 Vector Space over GF(2)

- A binary n-tuple is an ordered sequence,

$$(a_0, a_1, \ldots, a_{n-1})$$

with components from GF(2), i.e., $a_i = 0$ or 1 for $0 \leq i < n$.

- There are 2^n distinct binary n-tuples. We denote this set of 2^n distinct binary n-tuples with $\mathbf{V}_n$.

- Define an **addition operation** on $\mathbf{V}_n$ as follows:

$$(a_0, a_1, \ldots, a_{n-1}) + (b_0, b_1, \ldots, b_{n-1})$$
$$= (a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1}),$$

  where $a_i + b_i$ is carried out in modulo-2 addition.

- The addition of two binary n-tuples in $\mathbf{V}_n$ results in a third binary n-tuple in $\mathbf{V}_n$.

- Define a **scalar multiplication** between an element c in GF(2) and an n-tuple $(a_0, a_1, \ldots, a_{n-1})$ in $\mathbf{V}_n$ as follows:

$$c(a_0, a_1, \ldots, a_{n-1}) = (c \cdot a_0, c \cdot a_1, \ldots, c \cdot a_{n-1}),$$

where $c \cdot a_i$ is carried out in modulo-2 multiplication.

- The scalar multiplication also results in a binary n-tuple in $\mathbf{V}_n$.

- The addition $+$ defined on $\mathbf{V}_n$ is **associative** and **commutative**:

$$((a_0, a_1, \ldots, a_{n-1}) + (b_0, b_1, \ldots, b_{n-1})) + (c_0, c_1, \ldots, c_{n-1})$$
$$= (a_0, a_1, \ldots, a_{n-1}) + ((b_0, b_1, \ldots, b_{n-1}) + (c_0, c_1, \ldots, c_{n-1})),$$

$$(a_0, a_1, \ldots, a_{n-1}) + (b_0, b_1, \ldots, b_{n-1})$$
$$= (b_0, b_1, \ldots, b_{n-1}) + (a_0, a_1, \ldots, a_{n-1}).$$

- The set $\mathbf{V}_n$ together with the addition defined between two n-tuples in $\mathbf{V}_n$ and the scalar multiplication defined between an element in GF(2) and an n-tuple in $\mathbf{V}_n$ is said to form a **vector**

space over GF(2).

- The elements in $\mathbf{V}_n$ are called vectors and the elements of GF(2) are called scalars. Vectors are represented by boldface letters, e.g.,

$$\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}).$$

- Note that $\mathbf{V}_n$ contains the all-zero n-tuple, $\mathbf{0} = (0, 0, \ldots, 0)$.
- Also $0 \cdot (a_0, a_1, \ldots, a_{n-1}) = \mathbf{0}$, and

$$(a_0, a_1, \ldots, a_{n-1}) + (a_0, a_1, \ldots, a_{n-1}) = (0, 0, \ldots, 0).$$

- **Example 2.1:** Let $n = 4$, the vector space $\mathbf{V}_4$ over GF(2)

consists of the following 16 vectors:

$$(0000),\ (0001),\ (0010),\ (0011),$$
$$(0100),\ (0101),\ (0110),\ (0111),$$
$$(1000),\ (1001),\ (1010),\ (1011),$$
$$(1100),\ (1101),\ (1110),\ (1111).$$

- A subset $\mathbf{S}$ of the vector space $\mathbf{V}_n$ over GF(2) is called a **subspace** of $\mathbf{V}_n$ if: (1) The all-zero vector $\mathbf{0}$ is in $\mathbf{S}$; (2) For any c in GF(2) and any vector $\mathbf{a}$ in $\mathbf{S}$, $c \cdot \mathbf{a}$ is a vector in $\mathbf{S}$; and (3) For any two vectors, $\mathbf{a}$ and $\mathbf{b}$, the sum $\mathbf{a} + \mathbf{b}$ is also a vector in $\mathbf{S}$.
- **Example 2.2:** The following set of vectors,

$$(0000),\ (0101),\ (1010),\ (1111),$$

form a subspace of the vector space $\mathbf{V}_4$ over GF(2).

2.3 Linear Combinations of Vectors

- A linear combination of k vectors, $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{k-1}$, in $\mathbf{V}_n$ is a vector of the following form::

$$\mathbf{u} = c_0\mathbf{v}_0 + c_1\mathbf{v}_1 + \ldots + c_{k-1}\mathbf{v}_{k-1},$$

  where $c_i \in GF(2)$ for $0 \leq i < k$. The scalars $c_0, c_1, \ldots, c_{k-1}$ are called the **coefficients** of the linear combination.

- There are 2^k such linear combinations of $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{k-1}$. These 2^k linear combinations give 2^k vectors in $\mathbf{V}_n$ which form a subspace of $\mathbf{V}_n$.

- A set of vectors, $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{k-1}$, in $\mathbf{V}_n$ is said to be **linearly independent** if

$$c_0\mathbf{v}_0 + c_1\mathbf{v}_1 + \ldots + c_{k-1}\mathbf{v}_{k-1} \neq \mathbf{0}$$

  unless all the coefficients $c_0, c_1, \ldots, c_{k-1}$ are the zero element of GF(2).

- A set of vectors, $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{k-1}$, in $\mathbf{V}_n$ is said to be linearly dependent if the there exist k scalars **not all zero** such that

$$c_0\mathbf{v}_0 + c_1\mathbf{v}_1 + \ldots + c_{k-1}\mathbf{v}_{k-1} = \mathbf{0}$$

- The subspace given by the 2^k linear combinations of k **linearly independent** vectors, $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{k-1}$, in $\mathbf{V}_n$ is called a k-dimensional subspace $\mathbf{S}$ of $\mathbf{V}_n$. We say that $\mathbf{S}$ is spanned by these k linearly independent vectors. These k linearly

independent vectors are said to form a **basis** $\mathcal{B}$ of $\mathbf{S}$.

- For a given k-dimensional subspace $\mathbf{S}$ of the vector space $\mathbf{V}_n$ over GF(2), there may be more than one basis with k linearly independent vectors which span the subspace $\mathbf{S}$.
- $\mathbf{V}_n$ is an n-dimensional vector space over GF(2) and is spanned by the n linearly independent vectors, $\mathbf{e}_0, \mathbf{e}_0, \ldots, \mathbf{e}_{n-1}$, where the ith vector,

$$\mathbf{e}_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0),$$

has a 1-component at the ith position and all the other components are zeros. Any vector $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ is given by the following linear combination of $\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{n-1}$:

$$\mathbf{a} = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \ldots + a_{n-1}\mathbf{e}_{n-1}.$$

The set $\{\mathbf{e}_i : 0 \leq i < n\}$ forms a basis of $\mathbf{V}_n$.

2.4 Dual Space

- **Inner product**: The inner product of two vectors, $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\mathbf{b} = (b_0, b_1, \ldots, b_{n-1})$, in $\mathbf{V}_n$ is defined as follows:

$$\mathbf{a} \cdot \mathbf{b} = a_0 \cdot b_0 + a_1 \cdot b_1 + \ldots + a_{n-1} \cdot b_{n-1},$$

  where $a_i \cdot b_i$ and $a_i \cdot b_i + a_{i+1} \cdot b_{i+1}$ are carried out in modulo-2 multiplication and addition, respectively. Hence, the inner product $a \cdot b$ of a and b is a scalar, either 0 or 1.

- Two vectors $\mathbf{a}$ and $\mathbf{b}$ in $\mathbf{V}_n$ are said to be **orthogonal** if their inner product $\mathbf{a} \cdot \mathbf{b} = 0$.

- **Example 2.3** The inner product of vectors, (11011) and (10101), in the vector space $\mathbf{V}_5$ over GF(2) is

$$\begin{aligned}(11011) \cdot (10101) &= 1 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 \\ &= 1 + 0 + 0 + 0 + 1 \\ &= 0.\end{aligned}$$

  Hence, these two vectors are orthogonal.

- Let $\mathbf{S}$ be a k-dimensional subspace of the vector space $\mathbf{V}_n$ of all the n-tuples over GF(2). Let $\mathbf{S}_d$ be the subset of vectors in $\mathbf{V}_n$ such that for any vector $\mathbf{a} \in \mathbf{S}$ and any vector $\mathbf{b} \in \mathbf{S}_d$,

$$\mathbf{a} \cdot \mathbf{b} = 0$$

- $\mathbf{S}_d$ contains at least the all-zero n-tuple $\mathbf{0}$ and hence it is

non-empty.

- $\mathbf{S}_d$ is an $(n-k)$-dimensional subspace of $\mathbf{V}_n$ and is called the **dual** (or **null**) **space** of S and vice versa. Since $\mathbf{S}_d$ is an $(n-k)$-dimensional subspace of $\mathbf{V}_n$, it must contain $n-k$ linearly independent vectors $\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_{n-k-1}$ that span $\mathbf{S}_d$.
- **Example 2.4:** Consider the vector space $\mathbf{V}_5$ of all the 5-tuples over GF(2). The following 3-dimensional and 2-dimensional subspaces S and $\mathbf{S}_d$ of $\mathbf{V}_5$ are dual spaces to each other.

$\mathbf{S}$	$\mathbf{S}_d$
(00000)	(00000)
(11100)	(10101)
(01010)	(01110)
(10001)	(11011)
(10110)	
(01101)	
(11011)	
(00111)	

2.5 Irreducible Polynomials over GF(2)

- A polynomial

$$f(X) = f_0 + f_1 X + ... + f_n X^n$$

in X with coefficients f_i from the binary field GF(2) is called a polynomial over GF(2) or a binary polynomial. If $f_n \neq 0$, $f(X)$ is said to have degree n, otherwise it has degree less than n.

- For example, $1 + X + X^2, 1 + X + X^4, 1 + X^3 + X^5$ are binary polynomials of degree 2, 4 and 5, respectively.

- A polynomial $p(X)$ over GF(2) of degree m is said to be **irreducible** if it is not divisible by any polynomial over GF(2) of degree less than m but greater than zero.

- For example,
  $1+X+X^2, 1+X+X^4, 1+X^3+X^4, 1+X+X^5, 1+X^2+X^5$
  are irreducible polynomials over GF(2).
- For any positive integer $m \geq 1$, there exists at least one irreducible polynomial of degree m over GF(2).
- An irreducible polynomial $p(X)$ of degree m over GF(2) is said to be **primitive** if the smallest positive integer n for which $p(X)$ divides $X^n + 1$ is $n = 2^m - 1$.
- For example, $1 + X + X^4$ is a primitive polynomial. The smallest positive integer n for which $1 + X + X^4$ divides $X^n + 1$ is $n = 2^4 - 1 = 15$.
- For any positive integer m, there exists a primitive polynomial of degree m over GF(2).

- Table 2.1 gives a list of primitive polynomials.

Table 2.1: A List of Primitive Polynomials

Degree m	Primitive Polynomials
3	$1 + X + X^3$
4	$1 + X + X^4$
5	$1 + X^2 + X^5$
6	$1 + X + X^6$
7	$1 + X^3 + X^7$
8	$1 + X^2 + X^3 + X^4 + X^8$
9	$1 + X^4 + X^9$
10	$1 + X^3 + X^{10}$
11	$1 + X^2 + X^{11}$
12	$1 + X + X^4 + X^6 + X^{12}$
13	$1 + X + X^3 + X^4 + X^{13}$
14	$1 + X + X^6 + X^{10} + X^{14}$
15	$1 + X + X^{15}$
16	$1 + X + X^3 + X^{12} + X^{16}$
17	$1 + X^3 + X^{17}$
18	$1 + X^7 + X^{18}$
19	$1 + X + X^2 + X^5 + X^{19}$
20	$1 + X^3 + X^{20}$
21	$1 + X^2 + X^{21}$
22	$1 + X + X^{22}$
23	$1 + X + X^2 + X^7 + X^{23}$

2.6 Groups

- Let G be a set of elements. A binary operation $*$ on G is a rule that assigns to each pair of elements a and b a uniquely defined third element $c = a * b$ in G. When such a binary operation $*$ is defined on G, we say that G is closed under $*$.
- A binary operation $*$ on G is said to be associative if, for any a and b in G,

$$a * (b * c) = (a * b) * c.$$

- A group is an **algebraic system** with an associate binary operation $*$ defined on it.

- **Definition 2.1:** A set G on which a binary operation $*$ is defined is called a group if the following conditions (or axioms) are satisfied:

(1) The binary operation is associative.

(2) G contains a unique element e such that for any element a in G,

$$a * e = e * a = a.$$

This element e is called the **identity element** of G.

(3) For any element a in G, there exists a unique element $a^{'}$ in G such that

$$a * a^{'} = a^{'} * a = e.$$

The element $a^{'}$ is called the **inverse** of a, and vice versa.

- A group is said to be **commutative** if its binary operation $*$ also satisfies the following condition: For any elements a and b in G,

$$a * b = b * a.$$

- The set of all integers is a commutative group under real addition $+$. The integer 0 is the identity element with respect to real addition $+$, and the integer $-k$ is the inverse of the integer k.
- The set of all rational numbers excluding zero is a commutative group under real multiplication "$\cdot$" . Integer 1 is the identity element with respect to real multiplication "$\cdot$" , and the rational number $\frac{b}{a}$ is the (multiplicative) inverse of $\frac{a}{b}$.
- The number of elements in a group is called the **order** of the

group. A group of finite order is called a **finite group**.

- For any positive integer m, it is possible to construct a group of order m under a binary operation that is very similar to real addition.
- **Example 2.5:** The set $\{0, 1\}$ with modulo-2 addition as defined below:

$\oplus$	0	1
0	0	1
1	1	0

is a commutative group with two elements. We can easily prove that modulo-2 addition satisfies the associative and commutative laws. The 0-element is the identity element with respect the

modulo-2 addition, 0 is its own inverse and 1 is its own inverse.

- Let m be a positive integer. Consider the set of integer $G = \{0, 1, 2, \ldots, m-1\}$. Let $+$ be the real addition. Define a binary operation, denoted $\boxplus$. For any two integers i and j in G,

$$i \boxplus j = r,$$

where r is the **remainder** resulting from dividing the sum $i + j$ by m. By Euclids division algorithm , r is a non-negative integer between 0 and $m - 1$ and is therefore an element in G. Thus G is closed under the binary operation $\boxplus$, which is called modulo-m addition.

- The modulo-m addition is associative and commutative. G is a group under the modulo-m addition where: (1) the integer 0 is

the identity element; and (2) for any integer $i \in G$, $m - i$ is also in G and is the inverse of i with respect to $\boxplus$, called the additive inverse of i. Clearly, i is the additive inverse of $m - i$.

- The above group under modulo-m addition is called an **additive group**. The order of the group is m.
- **Example 2.6:** Let $m = 7$. Table 2.2 displays the additive group $G = \{0, 1, 2, 3, 4, 5, 6\}$ under modulo-7 addition.

Table 2.2: The additive group with modulo-7 addition

$\boxplus$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

- Next we present a class of finite groups under a binary operation

similar to real multiplication.

- Let p be a prime, say $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$
- Consider the set of nonzero integers less than p, $G = \{1, 2, \ldots, p-1\}$. Let $\cdot$ denote real multiplication. Note that every integer in G is relatively prime to p. Define a binary operation, denoted $\boxdot$, on G as follows: For any two integers, i and j, in G,

$$i \boxdot j = r,$$

where r is the remainder resulting from dividing the real product $i \cdot j$ by p. Since both i and j are relative to p, the real product $i \cdot j$ is not divisible by p and hence r is in G and G is closed under $\boxdot$. The binary operation $\boxdot$ is referred to as the modulo-p multiplication. Since real multiplication is associative and

commutative, the modulo-p multiplication $\boxdot$ is also associative and commutative. The integer 1 is the identity element of G with respect to $\boxdot$. It can be proved that every element i in G has a unique inverse with respect to $\boxdot$, which is called the **multiplicative inverse** of i. G is called a **multiplicative group**.

- **Example 2.7** Let $p = 7$. Table 2.3 displays the multiplicative group $G = \{1, 2, 3, 4, 5, 6\}$ under modulo-7 multiplication.

Table 2.3: The multiplicative group with modulo-7 multiplication

$\boxdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

From the table, we can easily check that every integer in G has a multiplicative inverse, e.g., the multiplicative inverse of 3 is 5.

- Consider the multiplicative group $G = \{1, 2, \ldots, p-1\}$ under modulo-p multiplication. Let α be an element in G. We define the powers of a as follows:

  $$\alpha^1 = \alpha,\ \alpha^2 = \alpha \boxdot \alpha,\ \alpha^3 = \alpha \boxdot \alpha \boxdot \alpha, \ldots, \alpha^i = \alpha \boxdot \alpha \boxdot \ldots \boxdot \alpha, \ldots$$

  Clearly, these powers of α are element of G.

- **Definition 2.2**: A multiplicative group G is said to be **cyclic** if there exists an element α in G such that for any element β in G, there is an non-negative integer i for which $\beta = \alpha^i$. Such element α is called the **generator** of the cyclic group and we write $G = < \alpha >$.

- Consider the multiplicative group $G = \{1, 2, 3, 4, 5, 6\}$ under the modulo-7 multiplication given by Table 2.3. The powers of

3 are:

$$3^1 = 3,$$
$$3^2 = 3 \boxdot 3 = 2,$$
$$3^3 = 3^2 \boxdot 3 = 2 \boxdot 3 = 6,$$
$$3^4 = 3^3 \boxdot 3 = 6 \boxdot 3 = 4,$$
$$3^5 = 3^4 \boxdot 3 = 4 \boxdot 3 = 5,$$
$$3^6 = 3^5 \boxdot 3 = 5 \boxdot 3 = 1.$$

- Hence G is a cyclic group with 3 as a generator.
- **Definition 2.3**: An non-empty subset H of a group G with a binary operation $*$ defined on it is called a **subgroup** of G if H is itself a group with respect to the binary operation $*$ of G, i.e., H satisfies all the axioms of a group under the same operation $*$

of G.

- To determine whether a subset H of a group G with a binary operation $*$ is a subgroup, we need not to verify all the axioms. The following axioms are sufficient:

  (S1) For any two elements a and b in H, $a * b$ is also an element in H.

  (S2) For any element a in H, its inverse is also an element in H.

- The axiom S1 implies that H is closed under operation $*$. Axioms S1 and S2 together imply that H contains the identity element e of G. H satisfies the associative law by virtue that every element in H is also in G and $*$ is an operation on H.

- **Example 2.8:** Consider the additive group

$G = \{0, 1, 2, 3, 4, 5, 6, 7\}$ under modulation-8 addition given by Table 2.4. The subset $H = \{0, 2, 4, 6\}$ forms a subgroup of G under modulo-8 addition as shown in Table 2.5.

Table 2.4: The additive group under modulo-8 addition

$\boxplus$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Table 2.5: A subgroup of the additive group under modulo-8 addition

$\boxplus$	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

2.7 Finite Fields

- A **field** is a set of elements in which we can perform addition, subtraction, multiplication and division **without leaving the set**. Addition and multiplication satisfy associative, commutative and **distributive laws**.
- The system of real numbers is a field, called the real-number field. The system of complex numbers is also a field, known as the complex-number field.
- The complex-number field is actually constructed from the real-number field by requiring the symbol $i = \sqrt{-1}$ as a root of the irreducible polynomial $X^2 + 1$ over the real-number field.

- Every complex number is of the form, $a + bi$, where a and b are real numbers.
- The complex-number field contains the real-number field as a **subfield**. We say that the complex-number field is an **extension field** of the real-number field. Both the real and complex number fields have infinite number of elements.
- **Definition 2.4:** Let F be a set of elements on which two binary operations, called **addition** "$+$" and **multiplication** "$\cdot$", are defined. F is a field under these two operations, if the following conditions (or axioms) are satisfied:

  (1) F is a **commutative group** under addition "$+$". The identity element with respect to addition $+$ is called the **zero**

element (or the additive identity) of F and is denoted by 0.

(2) The set $F\backslash\{0\}$ of nonzero elements of F forms a **commutative group** under multiplication "$\cdot$". The identify element with respect to multiplication $\cdot$ is called the **unit element** (or multiplicative identity) of F and is denoted by 1.

(3) For any three elements a, b and c in F,

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

The above equality is called the **distributive law**, i.e., multiplication is **distributive across addition**.

- From the definition, we see that a field consists of two groups with respect to two binary operations, addition and multiplication. The group under addition is called the **additive**

group of the field, and the group under multiplication is called the **multiplicative group** of the field.

- Since each group must contain an identity element, a field must contain at least two elements.
- In a field, the additive inverse of an element a is denoted by "$-a$", and the multiplicative inverse of a **nonzero element** b is denoted by "b^{-1}".
- Based on addition and multiplication operations, additive and multiplicative inverses of elements of a field, two other operations, namely **subtraction** "$-$" and **division** "$\div$", can be defined.
- Subtracting a field element b from a field element a is defined as

adding the additive inverse $-b$ of b to a, i.e.,

$$a - b \triangleq a + (-b).$$

It is clear $a - a = 0$.

- Dividing a field element a by a nonzero element b is defined as multiplying a by the multiplicative inverse b^{-1} of b to a, i.e.,

$$a \div b = a \cdot (b^{-1}).$$

It is clear $a \div a = 1$ provided $a \neq 0$.

- **Definition 2.5:** The number of elements in a field is called the **order** of the field. A field with finite order is called a **finite field**, otherwise called an **infinite field**.
- The real-number and complex-number fields are examples of

infinite fields.

- The real-number and complex-number fields are examples of infinite fields.
- It is possible to construct finite fields. Finite fields are also called **Galois fields** after their discoverer, a French mathematician Galois.
- For any **prime** p and any positive integer m, there exists a Galois field, denoted GF(p^m), with p^m elements. The most important subclass of Galois fields is the subclass with $p = 2$.
- **Prime Field**: Let p be a prime. We have shown in Section 2.6 that the set $\{0, 1, \ldots, p-1\}$ forms a commutative group under modulo-p addition and the subset $\{1, 2, \ldots, p-1\}$ forms a

commutative group under modulo-p multiplication. Based on the definitions of modulo-p addition and multiplication, and the fact that real addition and multiplication satisfy the distributive law, we can prove that modulo-p addition and multiplication also satisfy the distributive law. Therefore, the set

$$GF(p) = \{0, 1, ..., p-1\}$$

forms a finite field with p elements. This finite field is called a **prime field**.

- **Remark:** If m is not a prime, the set $\{0, 1, 2, \ldots, m-1\}$ does not form a field under modulo-m addition and multiplication.
- **Example 2.9** The smallest prime is $p = 2$. Therefore, the set $\{0, 1\}$ forms a field GF(2) with two elements under modulo-2

addition and multiplication as defined below:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

This field is also called the binary field as was introduced in Section 2.1.

- **Example 2.10:** Let $p = 7$. The set GF(7)$= \{0, 1, 2, \ldots, 6\}$ forms a field with 7 elements under modulo-7 addition and multiplication as defined in Table 2.2 and 2.3, respectively.

$\boxplus$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\boxdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

- **Definition 2.6:** Let F be a field. A subset K of F that is itself a field under the operations of F is called a **subfield** of F. In this context, F is called an **extension field** of K. If $K \neq F$, we say that K is a **proper subfield** of F. A field containing no proper subfields is called a **prime field**.

- Fundamental Properties of a field F:

  (1) For every element a in F, $a \cdot 0 = 0 \cdot a = 0$.

  (2) For any two nonzero elements a and b in F, $a \cdot b \neq 0$.

  (3) For two elements a and b in F, $a \cdot b = 0$ implies that either $a = 0$ or $b = 0$.

(4) For any two elements a and b in F,

$$-(a \cdot b) = (-a) \cdot b = a \cdot (-b).$$

(5) For $a \neq 0$, $a \cdot b = a \cdot c$ implies that $b = c$ (called **cancelation law**).

- **Definition 2.7:** Let F be a field and 1 be its unit element (or multiplicative identity). The **characteristic** of F is defined as the smallest positive integer λ such that

$$\sum_{i=1}^{\lambda} 1 = \underbrace{1 + 1 + \ldots + 1}_{\lambda} = 0,$$

where the summation represents repeated applications of addition $+$ of the field $\lambda - 1$ times (or sum of the unit element

of F λ times). If no such λ exits, F is said to have **zero characteristic**, i.e., $\lambda = 0$.

- The characteristic λ of a finite field is a prime. The characteristic of the prime field GF(p) is p.
- **Definition 2.8:** Let b be a nonzero element of a finite field GF(q), where q is a power of a prime. The smallest positive integer n such that $b^n = 1$ is called the **order** of the nonzero field element b.
- Consider the element 2 of the prime field GF(7) given by Tables 2.2 and 2.3. The powers of 2 are:

$$2,\ 2^2 = 4,\ 2^3 = 1$$

Therefore, the smallest positive integer n for with $2^n = 1$ is

$n = 3$. Hence the order of 2 is 3.

- The powers, $b^0, b, \ldots, b^{n-1}$ form a cyclic subgroup of the multiplicative group of GF(q).
- Again, consider the element 2 of the prime field GF(7) given by Tables 2.2 and 2.3. The set $\{1, 2, 4\}$ form a cyclic subgroup of the multiplicative group of GF(7) given by Table 2.3.
- **Theorem 2.1:** The order n any nonzero element b of GF(q) divides $q - 1$.
- **Definition 2.9:** A nonzero element a of a finite field GF(q) is called a **primitive element** if its order is $q - 1$. That is the powers of α,

$$\alpha^0 = 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}$$

form all the nonzero elements of GF(q).

- Every finite field has at least one primitive element.
- Consider the element 3 of the prime field GF(7). Using the Table 2.3, we find that the powers of element 3 are:

$$3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1.$$

The order of element 3 is 6 and hence 3 is a primitive element of GF(7). The element 5 is also a primitive element of GF(7).

2.8 Construction of Galois Field GF(2^m)

- Construction begins with a primitive polynomial (irreducible) $p(X) = 1 + p_1 X + ... + p_{m-1} X^{m-1} + X^m$ of degree m over GF(2).
- Since $p(X)$ is irreducible over GF(2), it has no root in GF(2), i.e., neither 0 or 1 is a root of $p(X)$.
- Since $p(X)$ has degree m, it has m roots. These m roots must be in a larger field that contains GF(2) as a subfield.
- Let α be a root of $p(X)$, i.e.,

$$p(\alpha) = 0.$$

- Starting from the binary field GF(2)=$\{0, 1\}$ and α, we define a multiplication "$\cdot$" to introduce a **sequence of powers** of α as

follows:

$$
\begin{aligned}
&0 \cdot 0 = 0, \\
&0 \cdot 1 = 1 \cdot 0 = 0. \\
&1 \cdot 1 = 1 \\
&0 \cdot \alpha = \alpha \cdot 0 = 0 \\
&1 \cdot \alpha = \alpha \cdot 1 = \alpha \\
&\alpha^2 = \alpha \cdot \alpha \\
&\alpha^3 = \alpha \cdot \alpha \cdot \alpha \\
&\vdots \\
&\alpha^j = \alpha \cdot \alpha \cdot \alpha \cdots \alpha \ (j \text{ times}) \\
&\vdots
\end{aligned}
\tag{2.1}
$$

- From the definition of multiplication "$\cdot$", we see that

$$\begin{aligned} 0 \cdot a^j &= a^j \cdot 0 = 0 \\ 1 \cdot \alpha^j &= \alpha^j \cdot 1 = \alpha^j \\ \alpha^i \cdot \alpha^j &= \alpha^{i+j} \end{aligned} \tag{2.2}$$

- Now we have the following set of elements:

$$F = 0, 1, \alpha, \alpha^2, \ldots, \alpha^j, \ldots, \tag{2.3}$$

  which is closed under multiplication "$\cdot$".

- Since α is a root of $p(X)$ and $p(X)$ divides $X^{2^m-1} + 1$, α must be a root of $X^{2^m-1} + 1$. Hence, $\alpha^{2^m-1} + 1 = 0$, which implies that

$$\alpha^{2^m-1} = 1. \tag{2.4}$$

- As a result, F consists of finite number of elements,

$$F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}. \tag{2.5}$$

- Let $\alpha^0 = 1$.
- The multiplication defined by (2.1) is carried out as follows using equality of (2.4): For $0 \leq i, j < 2^m$,

$$\alpha^i \cdot \alpha^j = \alpha^{i+j} = \alpha^r, \tag{2.6}$$

where r is the remainder resulting from dividing $i + j$ by $2^m - 1$. Since $0 \leq r < 2^m - 1$, α^r is an element in F given by (2.5). hence F is closed under the multiplication "$\cdot$" defined by (2.6).

- For $0 \leq i < 2^m - 1$,

$$\alpha^i \cdot \alpha^{2^m-1-i} = \alpha^{2^m-1} = 1.$$

Hence α^{2^m-1-i} is the inverse of α^i (vice versa) with respect to the multiplication "$\cdot$", defined by (2.6).

- Using the fact $\alpha^{2^m-1} = 1$, we can write

$$\alpha^{2^m-1-i} = \alpha^{2^m-1} \cdot \alpha^{-i} = 1 \cdot \alpha^{-i} = \alpha^{-i}. \tag{2.7}$$

- We use α^{-i} to denote the multiplicative inverse of α^i.
- The element "1" in F is the multiplicative identity (or the unit element) of F.
- Based on the definition of the multiplication "$\cdot$" given by (2.6), we can readily prove that multiplication "$\cdot$" is both associative and commutative. Hence, $F\backslash\{0\}$ is a group under the multiplication "$\cdot$", defined by (2.6).

- Next we define an addition "+" on F to make F as a group under this addition operation.
- For $0 \leq i < 2^m - 1$, dividing X^i by $p(X)$, we obtain

$$X^i = q_i(X)p(X) + b_i(X), \tag{2.8}$$

where $q_i(X)$ and $b_i(X)$ are quotient and remainder, respectively. The remainder is a polynomial over GF(2) with degree $m-1$ or less and is of the following form:

$$b_i(X) = b_{i,0} + b_{i,1}X + \ldots + b_{i,m-1}X^{m-1}. \tag{2.9}$$

with $b_{i,j} \in GF(2)$.

- Since $p(X)$ is an irreducible polynomial over GF(2) and X and $p(X)$ are relatively prime, X^i is not divisible by $p(X)$. Hence

for $0 \leq i < 2^m - 1$,

$$b_i(X) \neq 0.$$

- For $0 \leq i, j < 2^m - 1$ and $i \neq j$, we can readily prove that

$$b_i(X) \neq b_j(X). \tag{2.10}$$

- Replacing X of (2.8) by α, we have

$$\begin{aligned} \alpha^i &= q_i(\alpha)p(\alpha) + b(\alpha) \\ &= q_i(\alpha) \cdot 0 + b(\alpha) \\ &= b_{i,0} + b_{i,1}\alpha + ...b_{i,m-1}\alpha^{m-1}. \end{aligned} \tag{2.11}$$

- Since $b(X) \neq 0$, $\alpha^i \neq 0$.
- Eq. (2.11) shows that each nonzero element in F can be expressed as a polynomial of α with degree $m - 1$ or less. It

follows from (2.10) that for $i \neq j$,

$$\alpha^i \neq \alpha^j.$$

This says that all the nonzero elements in F are distinct.

- The 0-element in F may be represented by the zero polynomial.
- Note that there are exactly 2^m polynomials of α over GF(2) with degree $m-1$ or less. Each of the 2^m elements in F is represented by **one and only one** of these polynomials, and each of these polynomials represents **one and only one** element in F.
- Now we define an addition "$+$" on F using the polynomial representations of the elements in F. Consider two elements α^i

and α^j of F in polynomial form,

$$\alpha^i = b_{i,0} + b_{i,1}\alpha + \ldots + b_{i,m-1}\alpha^{m-1}$$
$$\alpha^j = b_{j,0} + b_{j,1}\alpha + \ldots + b_{j,m-1}\alpha^{m-1}$$

- The addition of two elements α^i and α^j in F is defined as follows:

$$\begin{aligned}\alpha^i + \alpha^j &= (b_{i,0} + b_{i,1}\alpha + \ldots + b_{i,m-1}\alpha^{m-1}) \\ &\quad + (b_{j,0} + b_{j,1}\alpha + \ldots + b_{j,m-1}\alpha^{m-1}) \\ &= (b_{i,0} + b_{j,0}) + (b_{i,1} + b_{j,1})\alpha + \ldots + (b_{i,m-1} + b_{j,m-1})\alpha^{m-1}.\end{aligned} \tag{2.12}$$

  where $b_{i,k} + b_{j,k}$ is carried out over GF(2) (modulo-2 addition).

- The polynomial given by (2.12) is a polynomial of α with

degree $m-1$ or less over GF(2) and hence represents an element α^l in F. From (2.12), we can easily verify that

$$0 + \alpha^i = \alpha^i + 0. \tag{2.13}$$

Therefore, F is close under the addition "+" defined by (2.12).

- Since modulo-2 addition is associative and commutative, we can readily verify that the addition defined by (2.12) is also associative and commutative.

- Note that

$$\begin{aligned}\alpha^i + \alpha^i &= (b_{i,0} + b_{i,0}) + (b_{i,1} + b_{i,1})\alpha + \ldots + (b_{i,m-1} + b_{i,m-1})\alpha^{m-1} \\ &= 0 + 0 \cdot \alpha + \ldots + 0 \cdot \alpha^{m-1} = 0.\end{aligned} \tag{2.14}$$

Hence α^i is its own inverse with respect to the addition "$+$" defined by (2.12).

- Based on the above developments, we conclude that F is a commutative group under the addition defined by (2.12) with 0 as the additive identity.
- We can prove that the multiplication defined by (2.6) satisfies the distributive law across addition defined by (2.12).
- Up to this point, we have proved that: (1) F is a commutative group under the addition "$+$" defined by (2.12): (2) $F\backslash\{0\}$ is a commutative group under the multiplication defined by (2.6); and (3) multiplication and addition defined on F satisfy the

distributive law. Hence,

$$F = \{\alpha^{\infty} = 0, \alpha^0 = 1, \alpha, ..., \alpha^{2^m-2}\}$$

is a field with 2^m elements, denote GF(2^m).

- Let $-\alpha^i$ denote the additive inverse of the element α^i. From (2.14), we see that

$$-\alpha^i = \alpha^i.$$

- Note that the correspondence

$$b_{i,0} + b_{i,1}\alpha + \ldots + b_{i,m-1}\alpha^{m-1}$$
$$\Longleftrightarrow \ (b_{i,0}, b_{i,1}, \ldots, b_{i,m-1})$$

is one-to-one.

- Therefore, every element in GF(2^m) can be represented in three

forms: (1) power form; (2) polynomial form; and (3) vector form.

- It is easier to carry out addition in either polynomial form or vector form. It is much easier to perform multiplication in power form.
- **Example 2.10:** Let $m = 4$. In this example, we give the construction of the Galois field GF(2^4) with 16 elements. First, we choose a primitive polynomial of degree 4 over GF(2),

$$p(X) = X^4 + X + 1.$$

- Let α be a root of $p(X)$. Then

$$p(\alpha) = \alpha^4 + \alpha + 1 = 0.$$

Using the facts $\alpha^4 + \alpha^4 = 0$ and $\alpha^4 + 0 = 0$, we have

$$\alpha^4 = \alpha + 1.$$

- Consider the set,

$$\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}.$$

  Note $\alpha^{15} = 1$.

- Using the identity $\alpha^4 = \alpha + 1$, every power α^i can be expressed

as a polynomial of a with degree 3 or less as follows:

$$0$$

$$1 = 1$$

$$\alpha = \alpha$$

$$\alpha^2 = \alpha^2$$

$$\alpha^3 = \alpha^3$$

$$\alpha^4 = 1 + \alpha$$

$$\alpha^5 = \alpha \cdot \alpha^4 = \alpha \cdot (1 + \alpha) = \alpha + \alpha^2$$

$$\alpha^6 = \alpha \cdot \alpha^5 = \alpha \cdot (\alpha + \alpha^2) = \alpha^2 + \alpha^3$$

$$\alpha^7 = \alpha \cdot \alpha^6 = \alpha \cdot (\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = 1 + \alpha + \alpha^3$$

$$\alpha^8 = \alpha \cdot \alpha^7 = \alpha \cdot (\alpha + \alpha + \alpha^4) = \alpha + \alpha^2 + \alpha^4 = 1 + \alpha^2$$

$$\alpha^9 = \alpha \cdot \alpha^7 = \alpha \cdot (1 + \alpha^2) = \alpha + \alpha^3$$

$$\alpha^{10} = \alpha \cdot \alpha^9 = \alpha \cdot (\alpha + \alpha^3) = \alpha^2 + \alpha^4 = 1 + \alpha + \alpha^2$$

$$\alpha^{11} = \alpha \cdot \alpha^{10} = \alpha \cdot (1 + \alpha + \alpha^2) = \alpha + \alpha^2 + \alpha^3$$

$$\alpha^{12} = \alpha \cdot \alpha^{11} = \alpha \cdot (\alpha + \alpha^2 + \alpha^3) = \alpha^2 + \alpha^3 + \alpha^4 = 1 + \alpha + \alpha^2 + \alpha^3$$

$$\alpha^{13} = \alpha \cdot \alpha^{12} = \alpha \cdot (1 + \alpha + \alpha^2 + \alpha^3) = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 1 + \alpha^2 + \alpha^3$$

$$\alpha^{14} = \alpha \cdot \alpha^{13} = \alpha \cdot (1 + \alpha^2 + \alpha^3) = \alpha + \alpha^3 + \alpha^4 = 1 + \alpha^3$$

$$\alpha^{15} = \alpha \cdot \alpha^{14} = \alpha \cdot (1 + \alpha^3) = \alpha + \alpha^4 = 1$$

- Table 2.6 gives the field of GF(2^4) with 16 elements in three different forms.

Table 2.6: GF(2^4) generated by the primitive polynomial $p(X) = 1 + X + X^4$

Power representation	Polynomial representation	Vector representation
0	0	(0 0 0 0)
1	1	(1 0 0 0)
α	α	(0 1 0 0)
α^2	α^2	(0 0 1 0)
α^3	α^3	(0 0 0 1)
α^4	$1 + \alpha$	(1 1 0 0)
α^5	$\alpha + \alpha^2$	(0 1 1 0)
α^6	$\alpha^2 + \alpha^3$	(0 0 1 1)
α^7	$1 + \alpha + \alpha^3$	(1 1 0 1)
α^8	$1 + \alpha^2$	(1 0 1 0)
α^9	$\alpha + \alpha^3$	(0 1 0 1)
α^{10}	$1 + \alpha + \alpha^2$	(1 1 1 0)
α^{11}	$\alpha + \alpha^2 + \alpha^3$	(0 1 1 1)
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	(1 1 1 1)
α^{13}	$1 + \alpha^2 + \alpha^3$	(1 0 1 1)
α^{14}	$1 + \alpha^3$	(1 0 0 1)

- The primitive polynomial $p(X) = X^4 + X + 1$ that generates GF(2^4) given in Table 2.6 has four roots, α, α^2, α^4 and α^8. To verify this, we replace X of $p(X)$ by α, α^2, α^4 and α^8 in turn as follows (using Table 2.6):

$$p(\alpha) = \alpha^4 + \alpha + 1 = 1 + \alpha + \alpha + 1 = 0$$
$$p(\alpha^2) = \alpha^8 + \alpha^2 + 1 = 1 + \alpha^2 + \alpha^2 + 1 = 0$$
$$p(\alpha^4) = \alpha^{16} + \alpha^4 + 1 = \alpha + 1 + \alpha + 1 = 0$$
$$p(\alpha^8) = \alpha^{32} + \alpha^8 + 1 = \alpha^2 + 1 + \alpha^2 + 1 = 0.$$

- The roots α, α^2, α^4 and α^8 are called **conjugate roots** of $p(X)$.
- Hence, $p(X) = (X + \alpha)(X + \alpha^2)(X + \alpha^4)(X + \alpha^8)$. Using

Table 2.6, we find that

$$\begin{aligned}
p(X) =& (X+\alpha)(X+\alpha^2)(X+\alpha^4)(X+\alpha^8) \\
=& (X^2+(\alpha+\alpha^2)X+\alpha^3)(X^2+(\alpha^4+\alpha^8)X+\alpha^{12}) \\
=& (X^2+\alpha^5X+\alpha^3)(X^2+\alpha^5X+\alpha^{12}) \\
=& X^4+(\alpha^5+\alpha^5)X^3+(\alpha^{12}+\alpha^{10}+\alpha^3)X^2+(\alpha^8+\alpha^{17})X \\
& +\alpha^{15} \\
=& X^4+X+1.
\end{aligned}$$

- GF(2^m) is called an **extension field** of GF(2) and GF(2) is called a **ground field** of GF(2^m).
- Every Galois field GF(2^m) of 2^m elements is generated by a primitive polynomial of degree over GF(2).

- **Isomorphism:** To construct an extension field GF(2^m) of degree m of GF(2), we need a primitive polynomial $p(X)$ of degree m over GF(2). If a different primitive polynomial $p^*(X)$ of degree m over GF(2) is used, the construction results in an extension field GF*(2^m) of degree m of GF(2) that has the same set of elements as that of GF(2^m). There is a one-to-one correspondence between GF(2^m) and GF*(2^m) such that if $a \longleftrightarrow a^*$, $b \longleftrightarrow b^*$, $c \longleftrightarrow c^*$, then

$$a + b \longleftrightarrow a^* + b^*$$

$$a \cdot b \longleftrightarrow a^* \cdot b^*$$

$$(a + b) + c \longleftrightarrow (a^* + b^*) + c^*$$

$$(a \cdot b) \cdot c \longleftrightarrow (a^* \cdot b^*) \cdot c^*$$

$$a \cdot (b + c) \longleftrightarrow a^* \cdot (b^* + c^*).$$

- GF(2^m) and GF*(2^m) are said to be *isomorphic*. That is, GF(2^m) and GF*(2^m) are structurally identical. In this sense, we may say that any primitive polynomial $p(X)$ of degree m over GF(2) give the same extension field GF(2^m) of degree m. This implies the **uniqueness** of the extension field GF(2^m).

Some Fundamental Properties of Galois Field GF(2^m)

- Let $f(X) = f_0 + f_1 X + \ldots + f_n X^n$ be a polynomial over GF(2). Then for any nonnegative integer t, the following equality holds,

$$[f(X)]^{2^t} = f(X^{2^t}).$$

- **Theorem 2.2:** Let $f(X)$ be a polynomial over GF(2). Let β be a nonzero element of GF(2^m). If β is a root of $f(X)$ (i.e., $f(\beta) = 0$), then for any nonnegative integer t, β^{2^t} is also a root of $f(X)$ (i.e., $f(\beta^{2^t}) = 0$).

- The element β^{2^t} is called a **conjugate** of β. It follows from Theorem 2.1 that

$$\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^t}, \ldots$$

are also roots of $f(X)$.

- For a finite field, the number of conjugates of a nonzero element β in GF(2^m) must be finite. Let e be the **smallest nonnegative integer** for which

$$\beta^{2^e} = \beta.$$

This integer e is called the **exponent** of β. The powers,

$$\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{e-1}}$$

are distinct and form all the conjugates of β.

- Let β be a nonzero element of GF(2^m) with order n (i.e., n is the smallest nonnegative integer such that $\beta^n = 1$). It follows from Theorem 2.1 that n divides $2^m - 1$. Let $2^m - 1 = kn$.
- Consider β^{2^m-1}. Then $\beta^{2^m-1} = \beta^{kn} = (\beta^n)^k$. Since $\beta^n = 1$,

$$\beta^{2^m-1} = 1.$$

  This implies that β is a root of $X^{2^m-1} + 1$.

- **Theorem 2.3:** The $2^m - 1$ nonzero elements of GF(2^m) form all the roots of $X^{2^m-1} + 1$. Conversely, all the $2^m - 1$ roots of $X^{2^m-1} + 1$ form all the nonzero elements of GF(2^m).
- It follows from Theorem 2.3 that

$$X^{2^m-1} + 1 = (X + 1)(X + \alpha)(X + \alpha^2)...(X + \alpha^{2^m-2}).$$

- **Definition 2.10:** Let β be an element of GF(2^m). Let $\phi(X)$ be the polynomial of the **smallest degree** over GF(2) that has β as a root, i.e., $\phi(\beta) = 0$. This polynomial $\phi(X)$ is called the **minimal polynomial** of β.
- **Theorem 2.4:** The minimal polynomial $\phi(X)$ of a field element β is irreducible.
- **Theorem 2.5:** The minimal polynomial $\phi(X)$ of a field element β is unique.
- **Theorem 2.6:** Let $f(X)$ be a polynomial over GF(2). Let $\phi(X)$ be the minimal polynomial of an element β in GF(2^m). If β is a root of $f(X)$, then $f(X)$ is divisible by $\phi(X)$.
- **Theorem 2.7:** Let $p(X)$ be an irreducible over GF(2). Let β be

an element of GF(2^m) and $\phi(X)$ be its minimal polynomial. If β is a root of $p(X)$, then $\phi(X) = p(X)$.

- The minimal polynomial of the 0-element of GF(2^m) is X.
- It follows from Theorems 2.3 and 2.6 that we have Theorem 2.8.
- **Theorem 2.8:** Let $\phi(X)$ be the minimal polynomial of a nonzero element of GF(2^m). Then $\phi(X)$ divides $X^{2^m-1} + 1$.
- **Theorem 2.9:** Let $\phi(X)$ be the minimal polynomial of an element β of GF(2^m) whose exponent is e. Then

$$\phi(X) = \prod_{i=0}^{e-1} (X + \beta^{2^t}).$$

- **Example 2.11:** Consider the field GF(2^4) given by Table 2.6.

The conjugates of α^3 are:

$$\alpha^3, (\alpha^3)^2 = \alpha^6, (\alpha^3)^{2^2} = \alpha^{12}, (\alpha^3)^{2^3} = \alpha^{24} = \alpha^9.$$

Note that $(\alpha^3)^{2^4} = \alpha^{48} = \alpha^3$. Hence, the minimal polynomial of α^3 is

$$\phi(X) = (X + \alpha^3)(X + \alpha^6)(X + \alpha^9)(X + \alpha^{12}).$$

Expanding the right-hand side of the above equation, we have

$$\phi(X) = X^4 + X^3 + X^2 + X + 1,$$

which is irreducible.

Consider the element α^5 of GF(2^4). The conjugates of α^5 are α^5 and α^{10}. Since $(\alpha^5)^{2^2} = \alpha^{20} = \alpha^5$, the exponent of α^5 is $e = 2$.

The minimal polynomial of α^5 is then

$$\begin{aligned}\phi(X) &= (X+\alpha^5)(X+\alpha^{10}) = X^2 + (\alpha^5+\alpha^{10})X + \alpha^{15} \\ &= X^2 + X + 1.\end{aligned}$$

2.9 Construction of Galois Field GF(q)

- Construction of a Galois field GF(q) with $q = p^m$ elements, where p is a prime, is similar to the construction of Galois field GF(2^m) with 2^m elements.
- Construction begins with a prime field GF(p) as the ground field and a (**monic**) primitive polynomial

$$p(X) = p_0 + p_1 X + \ldots + p_{m-1} X^{m-1} + X^m$$

degree m over GF(p), where $p_0 \neq 0$.

- Let α be a root of $p(X)$. Then the construction process of GF(p^m) is exactly the same as that of GF(2^m) from the binary ground field and a binary primitive polynomial $p(X)$.
- The fundamental properties of GF(p^m) are exactly the same as those of GF(2^m).
- In fact, we can construct a Galois field GF(q^m) with q^m elements from a ground field GF(q), where q is a power of prime, and a (monic) primitive polynomial $p(X)$ of degree m over GF(q). Again, the construction of GF(q^m) is exactly the same as that of GF(2^m) from GF(2).

2.10 Vector spaces

- **Definition 2.11:** Let F be a field. Let $\mathbf{V}$ be a set of elements on which a binary operation called addition $+$ is defined. A multiplication operation, denoted by "$\cdot$", is defined between the elements of F and the elements of $\mathbf{V}$. The set $\mathbf{V}$ is called a vector space over the field F if it satisfies the following axioms:

  (1) $\mathbf{V}$ is a commutative group under addition $+$ defined on $\mathbf{V}$.

  (2) For any element a in F and any element $\mathbf{v}$ in $\mathbf{V}$, $a \cdot \mathbf{v}$ is an element in $\mathbf{V}$.

(3) For any elements a and b in F and any element $\mathbf{v}$ in $\mathbf{V}$, the following associative law holds:

$$(a \cdot b) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v}).$$

(4) For any element a in F and any elements $\mathbf{u}$ and $\mathbf{v}$ in $\mathbf{V}$, the following distributive law holds:

$$a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}.$$

(5) For any two elements a and b in F and any element $\mathbf{v}$ in $\mathbf{V}$, the following distributive law holds:

$$(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}.$$

(6) Let 1 be the unit element of F. Then, for any element $\mathbf{v}$ in

$\mathbf{V}$,

$$1 \cdot \mathbf{v} = \mathbf{v}.$$

- The elements of $\mathbf{V}$ are called **vectors** and denoted by boldface lower-case letters, $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$, etc. The elements of F are called **scalars** and denoted by lower-case letters, a,b, c, etc. The addition $+$ on $\mathbf{V}$ is called **vector addition**, the multiplication "$\cdot$" that combines a scalar a in F and a vector $\mathbf{v}$ in $\mathbf{V}$ into a vector $a \cdot \mathbf{v}$ in $\mathbf{V}$ is referred to as **scalar multiplication**, and the vector $a \cdot \mathbf{v}$ is called the **product** of a and $\mathbf{v}$.
- The additive identity of $\mathbf{V}$ is denoted by the boldface $\mathbf{0}$, called the **zero vector** of $\mathbf{V}$.
- Note that we use $+$ for both additions on $\mathbf{V}$ and F. It should be clear that when we combine two vectors in $\mathbf{V}$, $+$ means the

vector addition; and when we combine two scalars in F, $+$ means the addition defined on the field F. We also use "$\cdot$" for both scalar multiplication and multiplication defined on the field F. When a scalar in F and a vector in $\mathbf{V}$ are combined, "$\cdot$" means scalar multiplication: and when two scalars in F are combined, "$\cdot$" means multiplication on F.

- Some basic properties of a vector space $\mathbf{V}$ over a field F are given below:

  (1) Let 0 be the zero element of the field F. For any vector $\mathbf{v}$ in $\mathbf{V}$,

  $$0 \cdot \mathbf{v} = \mathbf{0}.$$

  (2) For any element a in F, $a \cdot \mathbf{0} = \mathbf{0}$.

(3) For any element a in F and vectors $\mathbf{v}$ in $\mathbf{V}$,

$$-a \cdot \mathbf{v} = a \cdot (-\mathbf{v}) = -(a \cdot \mathbf{v}),$$

i.e., either $-a \cdot \mathbf{v}$ or $a \cdot (-\mathbf{v})$ is the additive inverse of the vector $a \cdot \mathbf{v}$.

- **Definition 2.12:** Let $\mathbf{S}$ be a nonempty subset of a vector space $\mathbf{V}$ over a field $\mathbf{F}$. $\mathbf{S}$ is called a **subspace** of $\mathbf{V}$ if it satisfies the axioms for a vector space given by Definition 2.11.

- To determine whether a subset $\mathbf{S}$ of a vector space $\mathbf{V}$ over a field F is subspace, it is sufficient to prove that:

(S1) For any two vectors $\mathbf{u}$ and $\mathbf{v}$ in $\mathbf{S}$, $\mathbf{u} + \mathbf{v}$ is also a vector in $\mathbf{S}$.

(S2) For any element a in F and any vector $\mathbf{u}$ in S, $a \cdot \mathbf{u}$ is also in $\mathbf{S}$.

- The most commonly used vector space in error control coding is the vector space $\mathbf{V}_n$ of all the n-tuples over a finite filed GF(q). This vector space consists of q^m vectors (or n-tuples). The case for $q = 2$ was presented in Section 2.2.

2.11. Remarks

- Galois fields are important in studying of the theory of error-correcting codes.
- In particular, they are used for constructing BCH, Reed-Solomon and low-density parity-check codes.

The Field of Real Numbers

- The set of real numbers with real addition and multiplication forms a field.

- Real addition is associative and commutative, i.e.,

$$(a+b)+c=a+(b+c)=a+b+c.$$

$$a+b=b+a.$$

- For any real number a, there exists a unique number –a such that

$$a+(-a)=0.$$

The number –a is called the additive inverse of a and vise versa.

- For any real number a,

$$0+a=a+0=a.$$

- The element 0 is called the additive identity or just "zero".

- The set of real numbers, R, is said to form a group under the real addition "+", called an additive group.

- Real multiplication "." is associative and commutative, i.e.,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),$$

$$a \cdot b = b \cdot a.$$

- For any nonzero number a, there exists a unique number a^{-1} for which

$$a \cdot a^{-1} = 1$$

The number a^{-1} is called the multiplicative inverse of a, and vise versa.

- For any real number a,

$$1 \cdot a = a \cdot 1 = a.$$

- The number 1 is called the multiplicative identity element, or the unit element or just "one".

- The nonzero elements of R is said to form a multiplicative group to form a multiplicative group under real multiplication.

- Distributive law holds,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

- Also

$$a \cdot 0 = 0 \cdot a = 0$$

- Subtraction of a real number "b" from a real number "a" is defined as adding the additive inverse –b of b to a, i.e.,

$$a - b \underline{\underline{\Delta}} a + (-b).$$

- Dividing a real number "a" by a nonzero real number "b" is defined as multiplying a by the multiplicative inverse b^{-1} of b,

$$a \div b \underline{\underline{\Delta}} a \cdot (b^{-1}).$$

- R consists of two groups, an additive group and a multiplicative group.

- Basically, we can add, subtract, multiply and divide without leaving the system of real numbers.

- From the real-number field R, we can construct the field of complex numbers, which is called an extension field of R.

Important Properties of GF(2^m)

- Consider the Galois field GF(2^m). Let α be a primitive element of GF(2^m). Then

$$\alpha^0 = 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}$$

form the $2^m - 1$ nonzero elements of GF(2^m) and

$$\alpha^{2^m-1} = 1.$$

- **Theorem 1** *For any nonzero element β in GF(2^m), $\beta^{2^m-1} = 1$.*

  Proof: Since β is a nonzero element of GF(2^m), it must be a power of α, say $\beta = \alpha^j$. Consider

  $$\beta^{2^m-1} = (\alpha^j)^{2^m-1} = (\alpha^{2^m-1})^j = (\alpha^0)^j = 1.$$

  This proves the theorem.

- **Theorem 2** *The $2^m - 1$ nonzero elements of GF(2^m) form all the roots of $X^{2^m-1} + 1$.*

  Proof: Let β be a nonzero element of GF(2^m). It follows from Theorem 1 that $\beta^{2^m-1} = 1$. Hence $\beta^{2^m-1} + 1 = 0$. This implies that β is a root of $X^{2^m-1} + 1$.

- **Theorem 3** *The roots of* $X^{2^m-1}+1$ *give all the nonzero elements of* $GF(2^m)$.

Proof: This theorem is a direct consequence of Theorem 2.

- **Theorem 4** *The order n of a nonzero element β of GF(2^m) divides $2^m - 1$.*

  Proof: Suppose n does not divide $2^m - 1$. Dividing $2^m - 1$ by n, we have

  $$2^m - 1 = qn + r$$

  where $0 < r < n$ (i.e., r is a positive integer less than n). Consider

  $$\beta^{2^m-1} = \beta^{qn+r} = (\beta^{qn})(\beta^r).$$

  Since $\beta^{2^m-1} = 1$ and $\beta^n = 1$. It follows from the above expression that we have $\beta^r = 1$. Since $0 < r < n$ and n is the smallest positive integer for which $\beta^n = 1$, then $\beta^r = 1$ is not possible. Therefore, our hypothesis that n does not divide $2^m - 1$ is invalid. Consequently, n must divide $2^m - 1$.

- **Theorem 5** *Let β be an element of GF(2^m). The minimal polynomial $\phi(X)$ of β is unique.*

  Proof: Let $\phi'(X)$ be another minimal polynomial of β. Then, $\phi(X)$ and $\phi'(X)$ must have the same degree, say k. The sum $\phi(X) + \phi'(X)$ is a polynomial of degree less than k. Since β is a root of both $\phi(X)$ and $\phi'(X)$, then

  $$\phi(\beta) + \phi'(\beta) = 0.$$

  If $\phi(X) \neq \phi'(X)$, we would have a nonzero polynomial $\phi(X) + \phi'(X)$ over GF(2) with degree less than k that has β as a root. This contradicts to the fact that $\phi(X)$ is the smallest degree polynomial over GF(2) which has β as a root. Hence, we must have $\phi(X) = \phi'(X)$. This implies that $\phi(X)$ is unique.

- **Theorem 6** *The minimal polynomial $\phi(X)$ of an element β of GF(2^m) is irreducible.*

  Proof: Suppose $\phi(X)$ is not irreducible (i.e. reducible). Then $\phi(X) = \phi_1(X)\phi_2(X)$ with

  $$0 < \deg\phi_1(X), \deg\phi_2(X) < \deg\phi(X).$$

  Since

  $$\phi(\beta) = \phi_1(\beta)\phi_2(\beta) = 0,$$

  then either $\phi_1(\beta) = 0$ or $\phi_2(\beta) = 0$. This contradicts to the fact that $\phi(X)$ is the smallest degree polynomial over GF(2) for which $\phi(\beta) = 0$. Hence $\phi(X)$ can not be factored over GF(2) and must be irreducible.

- **Theorem 7** *Let $\phi(X)$ be the minimal polynomial of the element β of GF(2^m). Let $f(X)$ be a polynomial over GF(2). If $f(\beta) = 0$, then $f(X)$ is divisible by $\phi(X)$.*

  Proof: Dividing $f(X)$ by $\phi(X)$, we have

$$f(X) = q(X)\phi(X) + r(X)$$

  with deg$r(X) <$ deg$\phi(X)$. Suppose $r(X) \neq 0$ (the zero polynomial). Consider

$$f(\beta) = q(\beta)\phi(\beta) + r(\beta).$$

  Since $f(\beta)$ and $\phi(\beta) = 0$, we must have

$$r(\beta) = 0.$$

  This says that β is a root of $r(X)$. This contradicts to the fact

that $\phi(X)$ is the smallest degree polynomial over GF(2) that has β as a root. Hence, $r(X)$ must be the zero polynomial and $\phi(X)$ must divide $f(X)$.

- **Theorem 8** *The minimal polynomial $\phi(X)$ of any nonzero element β of GF(2^m) divides $X^{2^m-1}+1$.*

  Proof: Since β is a root of $X^{2^m-1}+1$ (Theorem 2), it follows from Theorem 7 that $\phi(X)$ divides $X^{2^m-1}+1$.

- **Theorem 9** *Let $\phi(X)$ be the minimal polynomial of the element β of GF(2^m). Let $p(X)$ be an irreducible polynomial over GF(2) such that $p(\beta)=0$. Then, $\phi(X)=p(X)$.*

  Proof: This theorem is a direct consequence of Theorem 7.

- Let β be an element of GF(2^m). Let e be exponent of β, i.e., e is the smallest positive integer for which $\beta^{2^e} = \beta$. Then

$$\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{e-1}}$$

  are all the distinct conjugates of β.

- **Theorem 10** *Let β be an element of GF(2^m) with exponent e. Then, the minimal polynomial of β is given by* $\phi(X) = \prod_0^{e-1}(X + \beta^{2^i})$.