Introduction to Algebra

1. Groups
2. Fields
3. Vector Space over GF(2)
4. Linear Combination
5. Dual Space
6. Binary Irreducible Polynomials
7. Construction of Galois Field GF(2^m)

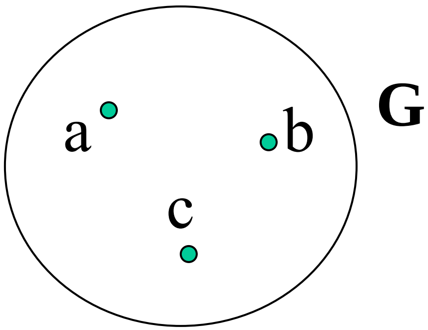
1. Groups

- Group: **G** is a Set

  Rule: an operation $\otimes$ defined on **G**, for which

$$a, b \in \mathrm{G} \qquad\qquad a \otimes b = c \in \mathrm{G}$$

We say that G is closed under the operation $\otimes$



EX2.1.1: $\oplus$ the addition of modulo 3

- **G** = {0, 1, 2}
- identity element 0
- **G** is closed under $\oplus$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Definition:

Let **G** be a set with an operation $\otimes$. The set G is called a group under this operation if the following conditions hold

1. $(a \otimes b) \otimes c = a \otimes (b \otimes c)$ (**associative**)
2. Let e is an identity element of **G,** then

$$a \otimes a' = a' \otimes a = e \ , \quad a \otimes e = e \otimes a = a$$

where a' is called an inverse of a

3. A group **G** is said to be **commutative** if for a and b in **G**, such that

$$a \otimes b = b \otimes a$$

EX:2.1.2 **G** = {1,2,3} over $\otimes$ (the multiplication of modulo 4)

$\otimes$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Since it is not closed, **G** is not a group

EX2.1.3: **G** = {0,1,2,3} with $\otimes$ (the multiplication modulo 4), 1 is an identity element in G

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Since $0 \otimes A \neq 1$, $(A \in G)$, **G** is not a group

EX2.1.4: $\mathbf{G} = \{1,2,3,4\}$ with $\otimes$ (the multiplication of modulo 5)

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

EX2.1.5: **G** = {0,1,2,3,4} with $\oplus$ (the addition of modulo 5)

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Inverse element

$1 \longleftrightarrow 4$

$2 \longleftrightarrow 3$

$0 \longleftrightarrow 0$

EX2.1.6:

real number addition: Associative(A), Commutative (C)

real number subtraction: A(not), C(not)

real number multiplication: A,C

real number division: A(not),C(not)

EX2.1.7: **G** = {1,2,3,4} over $\otimes$ (multiplication of modulo 5)

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

inverse element

$1 \longleftrightarrow 1$

$2 \longleftrightarrow 3$

$4 \longleftrightarrow 4$

$$3 \otimes \frac{1}{4} = 3 \otimes 4 \ (\text{mod}5) = 2$$

$$4 \otimes \frac{1}{2} = 4 \otimes 3 \ (\text{mod}5) = 2$$

EX2.1.8: N={0,1,2,…, ∞} is not a group under the integer number addition (e.g. can not find an inverse number in N).

2. Fields

Definition:

- Let F be a set of elements on which two operations are defined , and F is called a **field** if it has the following properties

(1) F is a **commutative** group under “ $\oplus$ ”

The identity element with respect to this operation is called the zero element 0. The additive inverse of an element *a* is denoted by “-*a*”

(2)F\{0} = F-{0} (without the zero element)

The set of nonzero elements in F forms a **commutative** group under the $\otimes$ operation, and the identity element is called the unit element denoted by 1. The **multiplicative inverse** of an element $a \in$ F-{0} is call a^{-1}.

(3)For a, b and c in F, the **distribution** law holds, i.e.,

$$(a \oplus b) \otimes c = a \otimes c \oplus b \otimes c$$

EX 2.2.1: $F = \{0,1,\ldots,P-1\}$, P is prime

(1)F is a field of P elements under modulo P addition and modulo P multiplication. For example, P = 3, and $F = \{0,1,2\}$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	1	2
1	1	2
2	2	1

- **Characteristic**: the smallest positive integer λ for which $\sum_{1}^{\lambda} \oplus 1 = \underbrace{1+1+1\cdots+1}_{\lambda} = 0$
- **Order**:(1)the number of elements in a finite field

  (2)the minimum positive number n such that

$$a^n = a \otimes a \cdots \otimes a = 1$$

n is the order of the element a

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

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

- In a finite field F = {0,1,…, q-1}, a nonzero element $a \in$ F is said to be primitive if the order of a is q-1, i.e.

$$a^{q-1} = 1$$

- Ex2.2.2: F = {0,1,2,3,4},

  $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, $2^4 = 1$, since the order of 2 is 4, therefore 2 is a primitive element in F. Similarly, 3 is the other primitive element.

- Ex2.2.3: F = {0,1,…,6},

  $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 1$, so that the order of 2 is 3 and 2 is not a primitive element in F.

- These two operations are commonly called modulo-2 addition and multiplication respectively. The modulo-2 addition can be implemented with an X-OR gate and the modulo-2 multiplication can be implemented with an AND gate
- The set {0,1} together with **modulo-2 addition** and **multiplication** is called a **binary field** , denoted **GF(2)**.
- The binary field **GF(2)** plays an important role binary coding.

3. Vector Space over GF(2)

- A binary n-tuple is an ordered sequence, $(a_1, a_2, \cdots, a_n)$ $a_i = 0 \text{ or } 1$ with components from GF(2).
- There are 2^n distinct binary *n*-tuples.
- Define an addition operation for any two binary *n*-tuples as follows :

  $$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) = (a_1 + b_1, \cdots, a_n + b_n)$$

  where $a_i + b_i, \quad 1 \le i \le n$, is carried out in modulo-2 addition.
- The addition of two binary *n*-tuple results in a third binary *n*-tuple

- Define a **scalar** multiplication between an element c in GF(2) and a binary n-tuple $(a_1,a_2,\ldots,a_n)$ as follows:

$$c\cdot(a_1,a_2,...,a_n)=(c\cdot a_1,c\cdot a_2,...,c\cdot a_n)$$

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

- The scalar multiplication also results in a binary n-tuple.
- The set V_n together with the addition defined for any two binary n-tuple in V_n and the scalar multiplication defined between an element in GF(2) and a binary n-tuple in V_n is called a **vector space** over GF(2).

- The elements in V_n are called vectors.
- Note that V_n contains the all-zero binary n-tuple (0, 0, …, 0) and

$$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) = (0, 0, \cdots, 0)$$

- Ex 2.3.1: Let $n = 4$. The vector space V_4 consists of the following 16 vectors:

$$
\begin{array}{ll}
(0\,0\,0\,0), & (0\,0\,0\,1) \\
(0\,0\,1\,0), & (0\,0\,1\,1) \\
(0\,1\,0\,0), & (0\,1\,0\,1) \\
(0\,1\,1\,0), & (0\,1\,1\,1) \\
(1\,0\,0\,0), & (1\,0\,0\,1) \\
(1\,0\,1\,0), & (1\,0\,1\,1) \\
(1\,1\,0\,0), & (1\,1\,0\,1) \\
(1\,1\,1\,0), & (1\,1\,1\,1)
\end{array}
$$

According to the rule for vector addition,

$$(0\ 1\ 0\ 1) + (1\ 1\ 1\ 0) = (0 + 1 , 1 + 1, 0 + 1 , 1 + 0)$$
$$= (1\ 0\ 1\ 1)$$

According to the rule for scalar multiplication,

$$1 \cdot (1\ 0\ 1\ 1) = (1 \cdot 1 , 1 \cdot 0 , 1 \cdot 1 , 1 \cdot 1)$$
$$= (1\ 0\ 1\ 1)$$
$$0 \cdot (1\ 0\ 1\ 1) = (0 \cdot 1 , 0 \cdot 0 , 0 \cdot 1 , 0 \cdot 1)$$
$$= (0\ 0\ 0\ 0)$$

- A subset S of V_n is called a **subspace** of V_n if (1) the all-zero vector is in S and (2) the sum of two vectors in S is also a vector in S.
- Ex 2.3.2: The following set of vector,

$$(0\ 0\ 0\ 0) \quad (0\ 1\ 0\ 1)$$

$$(1\ 0\ 1\ 0) \quad (1\ 1\ 1\ 1)$$

forms a subspace of the vector space V_4

4. Linear Combination

- A linear combination of k vectors, $\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_k$, in V_n is a **vector** of the form

$$\bar{u} = c_1\bar{v}_1 + c_2\bar{v}_2 + \ldots + c_k\bar{v}_k$$

where $c_i \in$ GF(2) and is called the coefficients of $\bar{v}_i$

- There are 2^k such linear combinations of $\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_k$

  These 2^k linear combinations give 2^k vectors in V_n which form a subspace of V_n .

- A set of vectors, $\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_k$, in V_n is said to be linearly **independent** if unless all $c_1, c_2, . . , c_k$ are the zero elements in GF(2).

$$c_1\overline{v}_1 + c_2\overline{v}_2 + \ldots + c_k\overline{v}_k \neq 0$$

- The subspace formed by the 2^k linear combinations of k linearly independent vectors in V_n is called a ***k*-dimensional** subspace of V_n. There k vectors are said to **span** a k-dimensional subspace of V_n.

Ex2.4.1:

$$V_2 = \begin{Bmatrix} \bar{v}_0 = (0,0) \\ \bar{v}_1 = (1,0) \\ \bar{v}_2 = (0,1) \\ \bar{v}_3 = (1,1) \end{Bmatrix}$$

$$(1)\begin{Bmatrix} \bar{v}_1 = (1,0) \\ \bar{v}_2 = (0,1) \end{Bmatrix} \qquad (2)\begin{Bmatrix} \bar{v}_1 = (1,0) \\ \bar{v}_3 = (1,1) \end{Bmatrix}$$

$$(3)\begin{Bmatrix} \bar{v}_2 = (0,1) \\ \bar{v}_3 = (1,1) \end{Bmatrix} \qquad \bar{v}_i = a_1\bar{e}_1 + a_2\bar{e}_2 \qquad a_1, a_2 \in \{0,1\}$$

There are two independent vectors.

Ex2.4.2:

$$S = \begin{Bmatrix} \bar{v}_0 = (0,0,0,0) \\ \bar{v}_1 = (1,0,1,0) \\ \bar{v}_2 = (0,1,0,1) \\ \bar{v}_3 = (1,1,1,1) \end{Bmatrix}$$

Since there are two independent vectors, the dimension of S is 2, i.e. $k = 2$.

5. Dual Space

- Inner Product : The inner product of two vectors, $\bar{a} = (a_1 , a_2 , \ldots , a_n)$ and $\bar{b} = (b_1 , b_2 , \ldots , b_n)$, is defined as follows:

  $$\bar{a} \cdot \bar{b} = a_1 \cdot b_1 + a_2 \cdot b_2 + \cdots a_n \cdot b_n$$

  where $a_i \cdot b_i$ and $a_i \cdot b_i + a_{i+1} \cdot b_{i+1}$ are caried out in modulo-2 multiplication and addition .

- Ex 2.5.1:

$$(1\ 1\ 0\ 1\ 1) \cdot (1\ 0\ 1\ 1\ 1)$$
$$=1 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 1$$
$$=1 + 0 + 0 + 1 + 1$$
$$=1$$

- Two vectors , $\overline{a}$ and $\overline{b}$, are said to be orthogonal if

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

- Ex 2.5.2 :

$$(1\ 0\ 1\ 1\ 0) \cdot (1\ 1\ 0\ 1\ 1)$$
$$= 1 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1$$
$$= 1 + 0 + 0 + 1 + 0$$
$$= 0$$

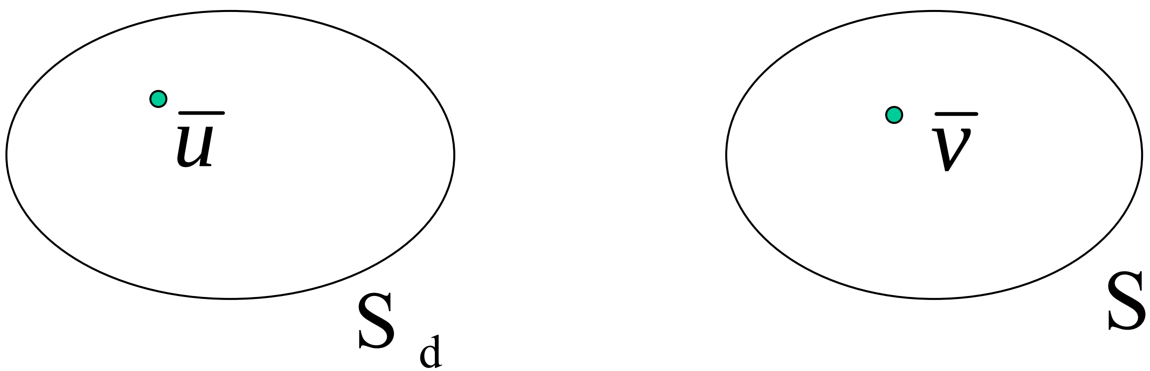
- Let S be a k-dimensional subspace of V_n. Let S_d be the subset of vectors in V_n , for any $\bar{a}$ in S and any $\bar{b}$ in S_d, such that

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

S_d is called the **dual space** (or **null space**) of S.

- The **dimension** of S_d is $n - k$, where k is the dimension of S.

- S_d is called the dual space (null space) of S



$$\overline{u} \cdot \overline{v} = 0$$

- Ex 2.5.3 : Consider V_5, the vector space of all 5-tuples over GF(2),

S	S_d
(00000)	(00000)
(11100)	(10101)
(01010)	(01110)
(10001)	(11011)
(10110)	
(01101)	
(11011)	
(00111)	

where the dimension of S is 3, and the dimension of S_d is 2.

HW #1

1. Construct the prime field GF(5) with modulo-5 addition and multiplication. Find all the primitive elements and determine the order of the other elements.
2. Construct the vector space of all 3-tuples over GF(5). Form a two-dimensional subspace and its dual space.

6. Binary Irreducible Polynomials

- A polynomial with coefficients from the binary field GF(2) is called a binary polynomial.
- For example, $1+X^2$, $1+X+X^3$, $1+X^3+X^5$ are binary polynomials.
- A binary polynomials $P(X)$ of degree *m* is said to be irreducible if it is **not divisible** by any binary polynomial of degree less then ***m*** and greater then zero.
- For example , $1+X+X^3$, $1+X+X^5$ and $1+X^3+X^5$ are irreducible polynomials .

- For any positive integer $m \geq \mathbf{1}$, there exists at least **one irreducible polynomial** of degree *m*.
- An irreducible polynomial $P(X)$ of degree *m* is said to be primitive if the smallest positive integer *n* for which

  $P(X)$ divides $X^n + 1$, and $n = 2^m - 1$.
- For any positive integer *m* , there exists a primitive polynomial of degree *m* .
- Table 2-1 gives a list of primitive polynomial .

Ex2.6.1: $g(X) = X^2 + 1$ (irreducible or reducible polynomial ?)

$X+1 \mid g(X) \longrightarrow \therefore g(X)$ is reducible

Ex2.6.2: $g(\mathrm{X}) = X^2 + X + 1$

$P(X) = X,$ or $X + 1$

$P(X) \nmid g(X)$

$\therefore g(X)$ is irreducible

Table 2-1: A list of primitive polynomial

m		m	
3	$1+X+X^3$	14	$1+X+X^6+X^{10}+X^{14}$
4	$1+X+X^4$	15	$1+X+X^{15}$
5	$1+X^2+X^5$	16	$1+X+X^3+X^{12}+X^{16}$
6	$1+X+X^6$	17	$1+X^3+X^{17}$
7	$1+X^3+X^7$	18	$1+X^7+X^{18}$
8	$1+X^2+X^3+X^4+X^8$	19	$1+X+X^2+X^5+X^{19}$
9	$1+X^4+X^9$	20	$1+X^3+X^{20}$
10	$1+X^3+X^{10}$	21	$1+X^2+X^{21}$
11	$1+X^2+X^{11}$	22	$1+X+X^{22}$
12	$1+X+X^4+X^6+X^{12}$	23	$1+X^5+X^{23}$
13	$1+X+X^3+X^4+X^{13}$	24	$1+X+X^2+X^7+X^{24}$

7. Construction of Galois Field GF(2^m)

- A **field** is a set of elements (or symbols) in which we can do **addition**, **subtraction**, **multiplication**, and **division** without leaving the set. Addition and multiplication satisfy the **commutative**, **associative** 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.

$$i = \sqrt{-\mathbf{1}},$$

as a root of the **irreducible** (over the real number field) **polynomial** $X^2 + 1$, i.e.,

$$(\sqrt{-\mathbf{1}})^2 + 1 = 0$$

- 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 sub-field.
- The complex-number field is an **extension** field of the real-number field.
- The complex-umber and real-number fields have infinite elements.

Finite Field

- It is possible to construct fields with finite number of elements. Such fields are called **finite fields**.
- Finite fields are also known as **Galois fields** after their discoverer.
- For any positive integer $m \geq 1$, there exists a Galois field of 2^m elements, denoted $GF(2^m)$.
- The construction of $GF(2^m)$ is very much the same as the construction of the complex-number field from the real-number field.

- We begin with a primitive (irreducible) polynomial $P(X)$ of degree m with coefficients from the binary field GF(2).
- Since $P(X)$ has degree m, it must have roots somewhere.
- Let α be the root of $P(X)$,i.e., $P(\alpha) = 0$

(Just as we let the symbol $i = \sqrt{-1}$ as the root of the irreducible polynomial X^2+1 over the real-number field.)

- Starting from GF(2) = {0,1} and α , we define a multiplication "•" to introduce a sequence of powers of α as follows:

$$0 \bullet 0 = 0$$

$$0 \bullet 1 = 1 \bullet 0 = 0$$

$$1 \bullet 1 = 1$$

$$0 \bullet \alpha = \alpha \bullet 0 = 0$$

$$1 \bullet \alpha = \alpha \bullet 1 = \alpha$$

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

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

$$\bullet\bullet\bullet$$

$$\alpha^i = \underbrace{\alpha \bullet \alpha \bullet \bullet \bullet \bullet}_{i \text{ times}} \alpha$$

- From the definition of multiplication "•",we see that

$$0 \cdot \alpha^i = \alpha^i \cdot 0 = 0$$

$$1 \cdot \alpha^i = \alpha^i \cdot 1 = \alpha^i$$

$$\alpha^i \cdot \alpha^j = \alpha^{i+j}.$$

- Now we have the following set of elements,

$$F = \{0, 1, \alpha, \alpha^2, \alpha^3, \ldots\ldots,\}$$

which is closed under multiplication "•".

- Since α is a root of $P(X)$ which divides $X^{2^m-1}+1$, α must also be a root of $X^{2^m-1}+1$.
- Hence

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

- This implies that

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

- As a result , F is finite and consists of following elements ,

$$F = \{ 0 , 1 , \alpha , \alpha^2 , \cdots , \alpha^{2^m - 2} \} \cdot$$

- Let $\alpha^0 = 1$, and multiplication is carried out as follows :

For $0 \leq i \ , j \ \leq \ 2^m\text{-}1$, $\alpha^i \bullet \alpha^j = \alpha^{i+j} = \alpha^r$

where r is the remainder resulting from dividing $i + j$ by 2^m-1 . I.e.,

$$r = i + j \bmod (2^m - 1)$$

- Note that

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

- Hence $\alpha^{2^{m}-1-i}$ is called the **multiplicative inverse** of α^{i} and vise versa.
- We can write

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

- We use α^{-i} to denote the multiplicative inverse of α^{i}.
- The element "1" is called the multiplicative identity (or the unit element).
- Next we define division as follows:

$$\alpha^{i} \div \alpha^{j} = \alpha^{i} \bullet \alpha^{-j} = \alpha^{i-j}.$$

- Now we define an addition " +" on F.

- For $0 \le i \le 2^m - 2$, we divide X^i by $P(X)$. This results in

$$X^i = a(X)P(X) + b(X)$$

where $b(X)$ is the remainder and

$$b(X) = b_0 + b_1 X + \cdots + b_{m-1} X^{m-1}$$

- Replacing X by α, we have

$$\begin{aligned} \alpha^i &= a(\alpha)P(\alpha) + b(\alpha) \\ &= a(\alpha) \cdot 0 + b(\alpha) \\ &= b_0 + b_1 \alpha + \cdots + b_{m-1} \alpha^{m-1} \end{aligned}$$

- This says that each nonzero element in F can be expressed as a polynomial of α with degree $m - 1$ or less.
- Of course, 0 can be expressed as a zero polynomial.
- Suppose

$$\alpha^i = b_0 + b_1\alpha + \ldots + b_{m-1}\alpha^{m-1}$$
$$\alpha^j = c_0 + c_1\alpha + \ldots + c_{m-1}\alpha^{m-1}$$

- We define addition " + " as follows :

$$\alpha^i+\alpha^j = (b_0+c_0) + (b_1+c_1)\,\alpha + \ldots + (b_{m-1}+c_{m-1})\,\alpha^{m-1}$$
$$= \alpha^k$$

where b_i+c_i is carried out with modulo 2 addition.

- Clearly $\alpha^i + \alpha^i = 0$.
- α^i is its own additive inverse .
- let $-\alpha^i$ denote the additive inverse of α^i . Then

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

- Subtraction is defined as follows :

$$\alpha^i - \alpha^j = \alpha^i + (-\alpha^j) = \alpha^i + \alpha^j .$$

- Hence **subtraction** is the same as **addition** .
- $F = \{ 0 , 1 , \alpha , \alpha^2 , \ldots , \alpha^{2^m - 2} \}$ together with the multiplication and addition defined above form a field of 2^m elements

- Note that the correspondence

  $b_0+b_1\alpha+\ldots+b_{m\text{-}1}\alpha^{m\text{-}1}$ and its vector form

  $(b_0\,, b_1\,,\ldots,b_{m\text{-}1}\,)$ is one to one.
- Every element in $GF(2^m)$ can be represented in three forms: (1) power, (2) polynomial, and (3) vector forms.
- It is easier to perform multiplication in power form.
- It is easier to carry out addition in polynomial or vector forms

Ex 2.7.1: Let $m = 4$. The polynomial

$$P(X) = X^4 + X + 1$$

is a binary primitive polynomial of degree 4.

- Let α be a root of $P(X)$.
- Then, $P(\alpha) = \alpha^4 + \alpha + 1 = 0$
- Using the fact that $\alpha^4 + \alpha^4 = 0$ and $\alpha^4 + 0 = \alpha^4$, we have

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

- Now we 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 that $\alpha^{15} = 1$.
- 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 shown in Table 2-2.
- For example,

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

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

$$\alpha^7 = \alpha \bullet \alpha^6 = \alpha \bullet (\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3,$$

$$= \alpha + 1 + \alpha^3 = \alpha^3 + \alpha + 1,$$

.

.

.

Table 2-2 The elements of GF(2^4) generated by $P(X) = 1 + X + X^4$

Power representation	Polynomial representation	4-Tuple 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)

- Addition is done in polynomial form.
- Let

$$\alpha^i = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$$
$$\alpha^j = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3$$

- Then,

$$\alpha^i + \alpha^j = (a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3) + (b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3)$$
$$= (a_0 + b_0) + (a_1 + b_1)\ \alpha + (a_2 + b_2)\ \alpha^2 + (a_3 + b_3)\alpha^3$$
$$= \alpha^k$$ (from Table 2-2).

where it is carried out with modulo-2 addition.

- For example,

$$\alpha^5 + \alpha^{13} = (\alpha+\alpha^2)+(1+\alpha^2+\alpha^3) = 1+\alpha+\alpha^3 = \alpha^7$$

$$\alpha^{11} + \alpha^3 = (\alpha+\alpha^2+\alpha^3)+\alpha^3 = \alpha+\alpha^2 = \alpha^5$$

$$\alpha^7 + \alpha^7 = (1+\alpha+\alpha^3)+(1+\alpha+\alpha^3) = 0$$

- Since $\alpha^i + \alpha^i = 0$, α^i is its own additive inverse, i.e.,

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

- Hence

$$\alpha^i - \alpha^i = \alpha^i + (-\alpha^j) = \alpha^i + \alpha^j$$

- Subtraction is identical to addition.
- This complete our construction of Galois field $GF(2^4)$.

- We say that GF(2^4) is generated by the primitive polynomial $P(X) = X^4 + X + 1$.
- Note that there is a one-to-one correspondence between the polynomial ,

$$a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 ,$$

and the 4-tuple,

$$(a_0 , a_1 , a_2 , a_3 ,a_4)$$

- Hence every element in GF(2^4) power form, the polynomial form and the vector form, as shown in Table 2-2.

- The primitive polynomial $P(X) = X^4 + X + 1$ has 4 roots which are all in GF(2^4). They are

$$\alpha\,, \quad \alpha^2\,, \quad \alpha^{2^2} = \alpha^4\,, \qquad \alpha^{2^3} = \alpha^8\,.$$

- For example,

$$\begin{aligned} P(\alpha^4) &= (\alpha^4)^4 + (\alpha^4) + 1 \\ &= \alpha^{16} + \alpha^4 + 1 \\ &= \alpha \bullet \alpha^{15} + \alpha^4 + 1 \\ &= \alpha + \alpha^4 + 1 \\ &= \alpha^4 + \alpha + 1 = 0\,. \end{aligned}$$

- α^2 , α^4 and α^8 are called conjugate roots of α.

- We can easily show that

$$P(X) = (X + \alpha)(X + \alpha^2)(X + \alpha^4)(X + \alpha^8)$$
$$= X^4 + X + 1$$

Remark

- Galois fields are important in the study of a special class of block codes, called cyclic codes. In particular, they are used for constructing the well known random error correcting BCH and Reed-Solomon code.
- GF(2^m) is also called the extension field of GF(2).
- Every Galois field of 2^m elements is generated by a binary primitive polynomial of degree m.

7. Primitive Elements

- Consider the Galois field GF(2^m) generated by the primitive polynomial

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

- The element α (a root of $P(X)$) whose powers generate all the nonzero elements GF(2^m) is called a **primitive element** of GF(2^m).
- In fact, any element β in GF(2^m) whose powers generate all the nonzero elements of GF(2^m) is a primitive element.

Ex 2.7.2 : Consider the Galois field GF(2^4) given in Table 2-2 . The powers of α^4 are

$$(\alpha^4)^0 = 1 \quad , \quad (\alpha^4)^1 = \alpha^4 \quad , \quad (\alpha^4)^2 = \alpha^8 \quad ,$$
$$(\alpha^4)^3 = \alpha^{12} \quad , \quad (\alpha^4)^4 = \alpha^{16} = \alpha \quad , \quad (\alpha^4)^5 = \alpha^{20} = \alpha^5 \quad ,$$
$$(\alpha^4)^6 = \alpha^{24} = \alpha^9 \quad , \quad (\alpha^4)^7 = \alpha^{28} = \alpha^{13} \quad , \quad (\alpha^4)^8 = \alpha^{32} = \alpha^2 \quad ,$$
$$(\alpha^4)^9 = \alpha^{36} = \alpha^6 \quad , \quad (\alpha^4)^{10} = \alpha^{40} = \alpha^{10} \quad , \quad (\alpha^4)^{11} = \alpha^{44} = \alpha^{14} \quad ,$$
$$(\alpha^4)^{12} = \alpha^{48} = \alpha^3 \quad , \quad (\alpha^4)^{13} = \alpha^{52} = \alpha^7 \quad , \quad (\alpha^4)^{14} = \alpha^{56} = \alpha^{11} \quad .$$

which α^4 generates all the 15 nonzero elements of GF(2^4) . Thus α^4 is a primitive element, and α^7 is also a primitive element.

Minimum Polynomials

Consider the Galois field GF(2^m) generated by a primitive polynomial $P(X)$ of degree *m*.

Let β be a nonzero element of GF(2^m).

- Consider the powers,

$$\beta^{2^0}, \beta^{2^1}, \beta^{2^2}, \ldots, \beta^{2^i}, \ldots$$

- Let *e* be the smallest nonnegative integer for which $\beta^{2^e} = \beta$
- The integer "*e*" is called the **exponent** of β.
- The powers, $\beta \;, \beta^{2} \;, \beta^{2^2}, \ldots., \beta^{2^{e-1}}$

are distinct and called **conjugates** of β.

- Consider the product,

$$\phi(X) = (X+\beta)(X+\beta^2)\ldots.(X+\beta^{2^{e-1}})$$
$$= a_0 + a_1 X + \ldots + a_{e-1} X^{e-1} + X^e$$

is a polynomial of degree e.

- $\phi(X)$ is binary and irreducible over GF(2).
- $\phi(X)$ is called the minimal polynomial of the element β.
- $\phi(X)$ is the binary irreducible polynomial of minimum degree which has β as root.
- $\phi(X)$ has $\beta, \beta^2, \ldots, \beta^{2^{e-1}}$ as all its roots.

Ex 2.7.3: Consider the field $GF(2^4)$ given in Table 2-2

- Let $\beta = \alpha^3$
- We form the following power sequence:

$$\beta = \alpha^3, \;\; \beta^2 = \alpha^6, \;\; \beta^4 = \alpha^{12}, \;\; \beta^8 = \alpha^{24} = \alpha^9$$

$$\beta^{16} = \alpha^{48} = \alpha^3 = \beta$$

- Since $\beta^{2^4} = \beta$, the exponent of β is 4.
- We see that $\beta = \alpha^3$, $\beta^2 = \alpha^6$, $\beta^4 = \alpha^{12}$ and $\beta^8 = \alpha^9$ are all distinct.
- The minimum polynomial of $\beta = \alpha^3$ is

$$\phi(X) = (X+\beta)(X+\beta^2)(X+\beta^{2^2})(X+\beta^{2^3})$$
$$= (X+\alpha^3)(X+\alpha^6)(X+\alpha^{12})(X+\alpha^9)$$
$$= X^4 + (\alpha^3+\alpha^6+\alpha^9+\alpha^{12})X^3$$
$$+ (\alpha^9+\alpha^{12}+\alpha^{15}+\alpha^{15}+\alpha^{18}+\alpha^{21})X^2$$
$$+ (\alpha^{15}+\alpha^{21}+\alpha^{24}+\alpha^{27})X + \alpha^{30}$$
$$= X^4 + X^3 + X^2 + X + 1$$

which is irreducible.

Table 2-3: Minimal polynomials of the elements in GF(2^4) generated by $P(X) = X^4 + X + 1$

Conjugate Roots	Minimal Polynomials
0	X
1	$X + 1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$X^4 + X + 1$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$X^4 + X^3 + X^2 + X + 1$
α^5, α^{10}	$X^2 + X + 1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$X^4 + X^3 + 1$

HW#2

1. Show that $X^5 + X^3 + 1$ is irreducible over GF(2). You may use the statement "gfdeconv" in MATLAB to help.

2. Construct a table for GF(2^3) based on the primitive polynomial $P(X) = X^3 + X + 1$. Display the power, polynomial, and vector representations of each element. Determine the order of each element.