Introduction to Algebra

Manjunatha. P

manjup.jnnce@gmail.com

Professor

Dept. of ECE

J.N.N. College of Engineering, Shimoga

September 27, 2013

Syllabus

Syllabus[1]

SEMESTER – III

ERROR CONTROL AND CODING

Subject Code	: **12EC039**	IA Marks	: 50
No. of Lecture Hours /week	: 04	Exam Hours	: 03
Total no. of Lecture Hours	: 52	Exam Marks	: 100

Introduction to Algebra: Groups, Fields, Binary Field Arithmetic, Construction of Galois Field GF (2^m) and its basic properties, Computation using Galois Field GF (2^m) Arithmetic, Vector spaces and Matrices.(Ref.1 Chap.2)

Linear Block Codes: Generator and Parity check Matrices, Encoding circuits, Syndrome and Error Detection, Minimum Distance Considerations, Error detecting and Error correcting capabilities, Standard array and Syndrome decoding, Decoding circuits, Hamming Codes, Reed – Muller codes, The (24, 12) Golay code, Product codes and Interleaved codes.(Ref.1 Chap.3)

Cyclic Codes: Introduction, Generator and Parity check Polynomials, Encoding using Multiplication circuits, Systematic Cyclic codes – Encoding using Feed back shift register circuits, Generator matrix for Cyclic codes, Syndrome computation and Error detection, Meggitt decoder, Error trapping decoding, Cyclic Hamming codes, The (23, 12) Golay code, Shortened cyclic codes.(Ref.1 Chap.5)

BCH Codes: Binary primitive BCH codes, Decoding procedures, Implementation of Galois field Arithmetic, Implementation of Error correction. Non – binary BCH codes: q – ary Linear Block Codes, Primitive BCH codes over GF (q), Reed – Solomon Codes, Decoding of Non – Binary BCH and RS codes: The Berlekamp - Massey Algorithm.(Ref.1 Chap.6)

Majority Logic Decodable Codes: One – Step Majority logic decoding, one – step Majority logic decodable Codes, Two – step Majority logic decoding, Multiple – step Majority logic decoding.(Ref.1 Chap.8)

Convolutional Codes: Encoding of Convolutional codes, Structural properties, Distance properties, Viterbi Decoding Algorithm for decoding, Soft – output Viterbi Algorithm, Stack and Fano sequential decoding Algorithms, Majority logic decoding(Ref.1 Chap.11)

Concatenated Codes & Turbo Codes: Single level Concatenated codes, Multilevel Concatenated codes, Soft decision Multistage decoding, Concatenated coding schemes with Convolutional Inner codes, Introduction to Turbo coding and their distance properties, Design of Turbo codes.(Ref.1 Chap.15)

Burst – Error – Correcting Codes: Burst and Random error correcting codes, Concept of Inter – leaving, cyclic codes for Burst Error correction – Fire codes, Convolutional codes for Burst Error correction.(Ref.1 Chap.21)

REFERENCE BOOKS:

1.Shu Lin & Daniel J. Costello, Jr. "**Error Control Coding**" Pearson / Prentice Hall, Second Edition, 2004. (Major Reference)

2.Blahut, R.E. "**Theory and Practice of Error Control Codes**" Addison Wesley, 1984

1. Groups

1. Groups
2. Fields

1. Groups
2. Fields
3. Binary Field Arithmetic

1. Groups
2. Fields
3. Binary Field Arithmetic
4. Construction of Galois Field GF (2m) and its basic properties

1. Groups
2. Fields
3. Binary Field Arithmetic
4. Construction of Galois Field GF (2m) and its basic properties
5. Computation using Galois Field GF (2m) Arithmetic

1. Groups
2. Fields
3. Binary Field Arithmetic
4. Construction of Galois Field GF (2m) and its basic properties
5. Computation using Galois Field GF (2m) Arithmetic
6. Vector spaces and Matrices

1. Groups
2. Fields
3. Binary Field Arithmetic
4. Construction of Galois Field GF (2m) and its basic properties
5. Computation using Galois Field GF (2m) Arithmetic
6. Vector spaces and Matrices

Groups

Groups

- Let G be a set of elements.

Groups

- Let G be a set of elements.
- A binary operation $*$ on G is a rule that assign to each pair of elements a and b a uniquely defined third element $c = a * b$ in G

Groups

- Let G be a set of elements.
- A binary operation $*$ on G is a rule that assign to each pair of elements a and b a uniquely defined third element $c = a * b$ in G.
- Definition 1.1: A group is a set G with a binary operation $*$ is defined

Groups

- Let G be a set of elements.
- A binary operation $*$ on G is a rule that assign to each pair of elements a and b a uniquely defined third element $c = a * b$ in G.
- Definition 1.1: A group is a set G with a binary operation $*$ is defined.
- The binary operation takes any two elements in G and generates as its result an element that is also in G. Hence G is closed under $*$.

Groups

- Let G be a set of elements.
- A binary operation $*$ on G is a rule that assign to each pair of elements a and b a uniquely defined third element $c = a * b$ in G.
- Definition 1.1: A group is a set G with a binary operation $*$ is defined.
- The binary operation takes any two elements in G and generates as its result an element that is also in G. Hence G is closed under $*$.
- The operation must satisfy the following conditions if G is a group.

Groups

- Let G be a set of elements.
- A binary operation $*$ on G is a rule that assign to each pair of elements a and b a uniquely defined third element $c = a * b$ in G.
- Definition 1.1: A group is a set G with a binary operation $*$ is defined.
- The binary operation takes any two elements in G and generates as its result an element that is also in G. Hence G is closed under $*$.
- The operation must satisfy the following conditions if G is a group.
  i The binary operation is Associative: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$

Groups

- Let G be a set of elements.
- A binary operation $*$ on G is a rule that assign to each pair of elements a and b a uniquely defined third element $c = a * b$ in G.

- Definition 1.1: A group is a set G with a binary operation $*$ is defined.
- The binary operation takes any two elements in G and generates as its result an element that is also in G. Hence G is closed under $*$.
- The operation must satisfy the following conditions if G is a group.

  i The binary operation is Associative: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$

  ii G contains an element such that, for any a in G $a * e = e * a = a$ (Identity)

Groups

- Let G be a set of elements.
- A binary operation $*$ on G is a rule that assign to each pair of elements a and b a uniquely defined third element $c = a * b$ in G.

- Definition 1.1: A group is a set G with a binary operation $*$ is defined.
- The binary operation takes any two elements in G and generates as its result an element that is also in G. Hence G is closed under $*$.
- The operation must satisfy the following conditions if G is a group.
  - i The binary operation is Associative: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
  - ii G contains an element such that, for any a in G $a * e = e * a = a$ (Identity)
  - iii For any element a in G exits a such that $a * a' = a' * a = e$ (Inverse)

Groups

- Let G be a set of elements.
- A binary operation $*$ on G is a rule that assign to each pair of elements a and b a uniquely defined third element $c = a * b$ in G.

- Definition 1.1: A group is a set G with a binary operation $*$ is defined.
- The binary operation takes any two elements in G and generates as its result an element that is also in G. Hence G is closed under $*$.
- The operation must satisfy the following conditions if G is a group.
  - i The binary operation is Associative: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
  - ii G contains an element such that, for any a in G $a * e = e * a = a$ (Identity)
  - iii For any element a in G exits a such that $a * a' = a' * a = e$ (Inverse)

- A group is said to be commutative (or abelian) if it also satisfies Commutativity: for all $a, b \in G$, $a * b = b * a$

Order: The number of elements in a group. It is denoted as $|G|$.

Order: The number of elements in a group. It is denoted as $|G|$.

- The integers with addition as the operation, 0 is the identity element, and $-i$ as the inverse of i, form a group.

Order: The number of elements in a group. It is denoted as $|G|$.

- The integers with addition as the operation, 0 is the identity element, and $-i$ as the inverse of i, form a group.
- The non-zero rational numbers with multiplication is the operation, 1 is the identity element, and b/a is the inverse of a/b, form a group.

Order: The number of elements in a group. It is denoted as $|G|$.

- The integers with addition as the operation, 0 is the identity element, and $-i$ as the inverse of i, form a group.
- The non-zero rational numbers with multiplication is the operation, 1 is the identity element, and b/a is the inverse of a/b, form a group.

Example 1.1

- Consider the set of two integers, $G = \{0, 1\}$. Let us define a binary operation, denoted by $\oplus$, on G as follows:

Order: The number of elements in a group. It is denoted as $|G|$.

- The integers with addition as the operation, 0 is the identity element, and $-i$ as the inverse of i, form a group.
- The non-zero rational numbers with multiplication is the operation, 1 is the identity element, and b/a is the inverse of a/b, form a group.

Example 1.1

- Consider the set of two integers, $G = \{0, 1\}$. Let us define a binary operation, denoted by $\oplus$, on G as follows:
- $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$

Order: The number of elements in a group. It is denoted as $|G|$.

- The integers with addition as the operation, 0 is the identity element, and $-i$ as the inverse of i, form a group.
- The non-zero rational numbers with multiplication is the operation, 1 is the identity element, and b/a is the inverse of a/b, form a group.

Example 1.1

- Consider the set of two integers, $G = \{0, 1\}$. Let us define a binary operation, denoted by $\oplus$, on G as follows:
- $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$
- This binary operation is called modulo-2 addition.

Order: The number of elements in a group. It is denoted as $|G|$.

- The integers with addition as the operation, 0 is the identity element, and $-i$ as the inverse of i, form a group.
- The non-zero rational numbers with multiplication is the operation, 1 is the identity element, and b/a is the inverse of a/b, form a group.

Example 1.1

- Consider the set of two integers, $G = \{0, 1\}$. Let us define a binary operation, denoted by $\oplus$, on G as follows:
- $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$
- This binary operation is called modulo-2 addition.
- The set $G = \{0, 1\}$ is a group under modulo-2 addition.

Order: The number of elements in a group. It is denoted as $|G|$.

- The integers with addition as the operation, 0 is the identity element, and $-i$ as the inverse of i, form a group.
- The non-zero rational numbers with multiplication is the operation, 1 is the identity element, and b/a is the inverse of a/b, form a group.

Example 1.1

- Consider the set of two integers, $G = \{0, 1\}$. Let us define a binary operation, denoted by $\oplus$, on G as follows:
- $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$
- This binary operation is called modulo-2 addition.
- The set $G = \{0, 1\}$ is a group under modulo-2 addition.
- It follows from the definition of modulo-2 addition $\oplus$ that G is closed under $\oplus$.

Order: The number of elements in a group. It is denoted as $|G|$.

- The integers with addition as the operation, 0 is the identity element, and $-i$ as the inverse of i, form a group.
- The non-zero rational numbers with multiplication is the operation, 1 is the identity element, and b/a is the inverse of a/b, form a group.

Example 1.1

- Consider the set of two integers, $G = \{0, 1\}$. Let us define a binary operation, denoted by $\oplus$, on G as follows:
- $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$
- This binary operation is called modulo-2 addition.
- The set $G = \{0, 1\}$ is a group under modulo-2 addition.
- It follows from the definition of modulo-2 addition $\oplus$ that G is closed under $\oplus$.
- 0 is the identity element and the inverse of 0 is itself and the inverse of 1 is also itself.

Order: The number of elements in a group. It is denoted as $|G|$.

- The integers with addition as the operation, 0 is the identity element, and $-i$ as the inverse of i, form a group.
- The non-zero rational numbers with multiplication is the operation, 1 is the identity element, and b/a is the inverse of a/b, form a group.

Example 1.1

- Consider the set of two integers, $G = \{0, 1\}$. Let us define a binary operation, denoted by $\oplus$, on G as follows:
- $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$
- This binary operation is called modulo-2 addition.
- The set $G = \{0, 1\}$ is a group under modulo-2 addition.
- It follows from the definition of modulo-2 addition $\oplus$ that G is closed under $\oplus$.
- 0 is the identity element and the inverse of 0 is itself and the inverse of 1 is also itself.
- It is easy to show that $\oplus$ is associative and commutative.

Order: The number of elements in a group. It is denoted as $|G|$.

- The integers with addition as the operation, 0 is the identity element, and $-i$ as the inverse of i, form a group.
- The non-zero rational numbers with multiplication is the operation, 1 is the identity element, and b/a is the inverse of a/b, form a group.

Example 1.1

- Consider the set of two integers, $G = \{0, 1\}$. Let us define a binary operation, denoted by $\oplus$, on G as follows:
- $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$
- This binary operation is called modulo-2 addition.
- The set $G = \{0, 1\}$ is a group under modulo-2 addition.
- It follows from the definition of modulo-2 addition $\oplus$ that G is closed under $\oplus$.
- 0 is the identity element and the inverse of 0 is itself and the inverse of 1 is also itself.
- It is easy to show that $\oplus$ is associative and commutative.
- Thus, G together with $\oplus$ is a commutative group.

Example 1.2

- Let m be a positive integer. Consider the set of integer $G = \{0, 1, 2, ..., m-1\}$. Let $+$ denote real addition.
- Define a binary operation $\boxplus$ (Boxplus) on G as follows:
- For any integers i and j in G, $i \boxplus j = r$, where r is the remainder resulting from dividing $i + j$ by m.
- The remainder r is an integer between 0 and $m - 1$ (Euclids division algorithm) and is therefore in G.
- Hence G is closed under the binary operation $\boxplus$, called modulo-m addition.
- First we see that 0 is the identity element.
- For $0 < i < m$, i and $m - i$ are both in G. Since $i + (m - i) = (m - i) + i = m$
- It follows from the definition of modulo-m addition that $i \boxplus (m - i) = (m - i) \boxplus i = 0$ Therefore, i and $m - i$ are inverses to each other with respect to $\boxplus$.

- It is also clear that the inverse of 0 is itself.
- Since real addition is commutative, it follows from the definition of modulo-m addition that, for any integers i and j in G, $i \boxplus j = j \boxplus i$.
- Therefore modulo-m addition is commutative.
- Next we show that modulo-m addition is also associative.
- Let i, j, and k be three integers in G. Since real addition is associative, we have
- $i + j + k = (i + j) + k = i + (j + k)$
- Dividing $i + j + k$ by m, we obtain $i + j + k = qm + r$, where q and r are the quotient and the remainder, respectively.
- Now, dividing i + j by m, we have

$$i + j = q1m + r1 \tag{1}$$

, with $0 \leq r_1 < m$

- Therefore, $i \boxplus j = r1$. Dividing r1 + k by m, we obtain

$$r1 + k = q2m + r2 \tag{2}$$

with $0 \leq r_1 < m$

- Hence $r1 \boxplus k = r2$ and $(i \boxplus j) \boxplus k = r2$. Combining (1) and (2), we have $i + j + k = (q1 + q2)m + r2$,
- This implies that r2 is also the remainder when $i + j + k$ is divided by m. Since the remainder resulting from dividing an integer by another integer is unique, we must have $r2 = r$. As a result, we have
- $(i \boxplus j) \boxplus k = r$.
- Similarly, we can show that $i \boxplus (j \boxplus k) = r$. Therefore $(i \boxplus j) \boxplus k = i \boxplus (j \boxplus k)$ and modulo-m addition is associative.
- This concludes our proof that the set $G = \{0, 1, 2, ..., m - 1\}$ is a group under modulo-m addition. We shall call this group an additive group.

Let m be a positive integer. Consider the set of integer $G = \{0, 1, 2, ..., m-1\}$. 0 is the identity element it turns out that for any a in the set there is some b such that $a \boxplus b = 0$, so inverse exist. Modulo-m addition for the case m = 5 is as shown in in table 2:

- the inverse of 0 is 0: $0 \boxplus 0 = 0$
- the inverse of 1 is 4: $1 \boxplus 4 = 5 = 5 \bmod 5$
- the inverse of 2 is 3: $2 \boxplus 3 = 5 = 5 \bmod 5$
- the inverse of 3 is 2: $3 \boxplus 2 = 5 = 5 \bmod 5$
- the inverse of 4 is 1: $4 \boxplus 1 = 5 = 5 \bmod 5$

Table: Modulo-5 addition

$\boxplus$	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

Example 1.3:

- Let p be a prime (e.g. $p = 2, 3, 5, 7, 11, ...$).

Example 1.3:

- Let p be a prime (e.g. $p = 2, 3, 5, 7, 11, \ldots$).Consider the set of integers, $G = \{1, 2, \ldots, p - 1\}$. Let $\cdot$ denote real multiplication.

Example 1.3:

- Let p be a prime (e.g. $p = 2, 3, 5, 7, 11, \dots$).Consider the set of integers, $G = \{1, 2, \dots, p-1\}$. Let $\cdot$ denote real multiplication.
- Define a binary operation $\boxdot$ on G as follows: For i and j in G,
- $$i \boxdot j = r$$

Example 1.3:

- Let p be a prime (e.g. $p = 2, 3, 5, 7, 11, ...$).Consider the set of integers, $G = \{1, 2, ..., p - 1\}$. Let $\cdot$ denote real multiplication.
- Define a binary operation $\boxdot$ on G as follows: For i and j in G,
- $$i \boxdot j = r$$
- where r is the remainder resulting from dividing $i \cdot j$ by p.

Example 1.3:

- Let p be a prime (e.g. $p = 2, 3, 5, 7, 11, ...$).Consider the set of integers, $G = \{1, 2, ..., p - 1\}$. Let $\cdot$ denote real multiplication.
- Define a binary operation $\boxdot$ on G as follows: For i and j in G,
- $$i \boxdot j = r$$
- where r is the remainder resulting from dividing $i \cdot j$ by p.
- The set $G = \{1, 2, ..., p - 1\}$ is a group under modulo-p multiplication.

Example 1.3:

- Let p be a prime (e.g. $p = 2, 3, 5, 7, 11, ...$).Consider the set of integers, $G = \{1, 2, ..., p - 1\}$. Let $\cdot$ denote real multiplication.
- Define a binary operation $\boxdot$ on G as follows: For i and j in G,
- $$i \boxdot j = r$$
- where r is the remainder resulting from dividing $i \cdot j$ by p.
- The set $G = \{1, 2, ..., p - 1\}$ is a group under modulo-p multiplication.
- First we note that $i \cdot j$ is not divisible by p.

Example 1.3:

- Let p be a prime (e.g. $p = 2, 3, 5, 7, 11, ...$).Consider the set of integers, $G = \{1, 2, ..., p - 1\}$. Let $\cdot$ denote real multiplication.
- Define a binary operation $\boxdot$ on G as follows: For i and j in G,
- $$i \boxdot j = r$$
- where r is the remainder resulting from dividing $i \cdot j$ by p.
- The set $G = \{1, 2, ..., p - 1\}$ is a group under modulo-p multiplication.
- First we note that $i \cdot j$ is not divisible by p.
- Hence $0 < r < p$ and r is an element in G.

Example 1.3:

- Let p be a prime (e.g. $p = 2, 3, 5, 7, 11, ...$).Consider the set of integers, $G = \{1, 2, ..., p - 1\}$. Let $\cdot$ denote real multiplication.
- Define a binary operation $\boxdot$ on G as follows: For i and j in G,
- $$i \boxdot j = r$$
- where r is the remainder resulting from dividing $i \cdot j$ by p.
- The set $G = \{1, 2, ..., p - 1\}$ is a group under modulo-p multiplication.
- First we note that $i \cdot j$ is not divisible by p.
- Hence $0 < r < p$ and r is an element in G.
- Therefore, the set G is closed under the binary operation $\boxdot$, referred to as modulo-p multiplication.

Example 1.3:

- Let p be a prime (e.g. $p = 2, 3, 5, 7, 11, ...$).Consider the set of integers, $G = \{1, 2, ..., p-1\}$. Let $\cdot$ denote real multiplication.
- Define a binary operation $\boxdot$ on G as follows: For i and j in G,
- $$i \boxdot j = r$$
- where r is the remainder resulting from dividing $i \cdot j$ by p.
- The set $G = \{1, 2, ..., p-1\}$ is a group under modulo-p multiplication.
- First we note that $i \cdot j$ is not divisible by p.
- Hence $0 < r < p$ and r is an element in G.
- Therefore, the set G is closed under the binary operation $\boxdot$, referred to as modulo-p multiplication.
- We can easily check that modulo-p multiplication is commutative and associative. The identity element is 1.

Example 1.3:

- Let p be a prime (e.g. $p = 2, 3, 5, 7, 11, ...$).Consider the set of integers, $G = \{1, 2, ..., p-1\}$. Let $\cdot$ denote real multiplication.
- Define a binary operation $\boxdot$ on G as follows: For i and j in G,
- $$i \boxdot j = r$$
- where r is the remainder resulting from dividing $i \cdot j$ by p.
- The set $G = \{1, 2, ..., p-1\}$ is a group under modulo-p multiplication.
- First we note that $i \cdot j$ is not divisible by p.
- Hence $0 < r < p$ and r is an element in G.
- Therefore, the set G is closed under the binary operation $\boxdot$, referred to as modulo-p multiplication.
- We can easily check that modulo-p multiplication is commutative and associative. The identity element is 1.
- The only thing left to be proved is that every element in G has an inverse.

- Commutative $i \boxdot j = j \boxdot i$
- Associative $i \boxdot (j \boxdot k) = (i \boxdot j) \boxdot k$

- Let i be an element in G. Since p is a prime and $i < p$, i and p must be relatively prime (i.e. i and p don't have any common factor great than 1).
- It is well known that there exist two integers a and b such that
- $$a \cdot i + b \cdot p = 1 \tag{3}$$
- and a and p are relatively prime (Euclids theorem). Rearranging
- $$a \cdot i = -b \cdot p + 1 \tag{4}$$
- This says that when $a \cdot i$ is divided by p, the remainder is 1.
- If $0 < a < p$, a is in G and it follows from (4) and the definition of modulo-p multiplication that .
- $$a \boxdot i = i \boxdot a = 1$$

- Therefore a is the inverse of i. However, if a is not in G, we divide a by p ,
- $$a = q \cdot p + r \quad (5)$$

  .
- Since a and p are relatively prime, the remainder r cannot be 0 and it must be between 1 and $p - 1$.
- Therefore r is in G. Now combining (4) and (5), we obtain
- $$r \cdot i = -(b + qi)p + 1.$$
- Therefore $r \boxdot i = i \boxdot r = 1$ and r is the inverse of i. Hence any element i in G has an inverse with respect to modulo-p multiplication.
- The group $G = \{1, 2, ..., p - 1\}$ under modulo-p multiplication is called a multiplicative group.
- If p is not a prime, the set $G = \{1, 2, ..., p - 1\}$ is not a group under modulo-p multiplication

Let p be any prime. G={1,2,3,.....p-1} is a group under the operation of modulo-p multiplication: 1 is the identity element it turns out that for any a in the set there is some b such that $a \cdot b = 1$, so inverse exist. Modulo-p multiplication for the case p = 5 is as shown in in table 2:

- the inverse of 1 is 1: $1 \times 1 = 1$
- the inverse of 2 is 3: $2 \times 3 = 6 = 1$ mod 5
- the inverse of 3 is 2: $3 \times 2 = 6 = 1$ mod 5
- the inverse of 4 is 4: $4 \times 4 = 16 = 1$ mod 5

Table: Modulo-5 multiplicaiton

$\boxdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Cyclic groups

- In the previous group, the element 3 is called a generator: if we look at the sequence

Cyclic groups

- In the previous group, the element 3 is called a generator: if we look at the sequence
- 3, 3·3; 3·3·3, ...

Cyclic groups

- In the previous group, the element 3 is called a generator: if we look at the sequence
- 3, 3·3; 3·3·3, ...
- we reach every element of the group: the sequence is the same as
- 3, 4, 2, 1, 3, 4, 2, 1, ...

Cyclic groups

- In the previous group, the element 3 is called a generator: if we look at the sequence
- 3, 3·3; 3·3·3, ...
- we reach every element of the group: the sequence is the same as
- 3, 4, 2, 1, 3, 4, 2, 1, ...
- Because multiplying by 3 takes us round and round this loop, hitting all the elements as we go, the group is called cyclic.

Abelian groups

- A group is called Abelian if its binary operation is commutative: that is, if
- $a * b = b * a$

Abelian groups

- A group is called Abelian if its binary operation is commutative: that is, if
- $a * b = b * a$
- for all a and b in the group.

Abelian groups

- A group is called Abelian if its binary operation is commutative: that is, if
- $a * b = b * a$
- for all a and b in the group.
- All the groups we've seen that are based on addition or multiplication of numbers are Abelian, because addition and multiplication are themselves commutative.

Abelian groups

- A group is called Abelian if its binary operation is commutative: that is, if
- $a * b = b * a$
- for all a and b in the group.
- All the groups we've seen that are based on addition or multiplication of numbers are Abelian, because addition and multiplication are themselves commutative.

Examples of groups

- The integers with addition as the operation, 0 as the (identity) unit, and ..n as the inverse of n, form a group.
- The non-zero rational numbers with multiplication as the operation, 1 as the unit, and 1/x as the inverse of x, form a group.

Non-examples of groups! Some non-examples:

- The natural numbers with addition as the operation do not form a group because there's no inverse for any $n > 0$.
- The integers with multiplication do not form a group because no number other than 1 has an inverse.
- The rationals with multiplication do not form a group because 0 has no inverse.

Subgroup

- Def: Let H be a nonempty subset of G. The subset H is said to be a subgroup of G if H is a closed under the group operation of G and satisfies all the conditions of a group.

Subgroup

- Def: Let H be a nonempty subset of G. The subset H is said to be a subgroup of G if H is a closed under the group operation of G and satisfies all the conditions of a group.
- For example the set of all rational numbers is a group under real addition.

Subgroup

- Def: Let H be a nonempty subset of G. The subset H is said to be a subgroup of G if H is a closed under the group operation of G and satisfies all the conditions of a group.
- For example the set of all rational numbers is a group under real addition.
- The set of all integers is a subgroup of the group of rational numbers under real addition.

Subgroup

- Def: Let H be a nonempty subset of G. The subset H is said to be a subgroup of G if H is a closed under the group operation of G and satisfies all the conditions of a group.
- For example the set of all rational numbers is a group under real addition.
- The set of all integers is a subgroup of the group of rational numbers under real addition.
- A subgroup of G that is not identical to G is called a proper subgroup of G

Subgroup

- Def: Let H be a nonempty subset of G. The subset H is said to be a subgroup of G if H is a closed under the group operation of G and satisfies all the conditions of a group.
- For example the set of all rational numbers is a group under real addition.
- The set of all integers is a subgroup of the group of rational numbers under real addition.
- A subgroup of G that is not identical to G is called a proper subgroup of G
- Theorem 2.3: Let G be a group under the binary operation $*$. Let H be a nonempty subset of G. Then H is a subgroup of G if the following conditions hold:

Subgroup

- Def: Let H be a nonempty subset of G. The subset H is said to be a subgroup of G if H is a closed under the group operation of G and satisfies all the conditions of a group.
- For example the set of all rational numbers is a group under real addition.
- The set of all integers is a subgroup of the group of rational numbers under real addition.
- A subgroup of G that is not identical to G is called a proper subgroup of G
- Theorem 2.3: Let G be a group under the binary operation $*$. Let H be a nonempty subset of G. Then H is a subgroup of G if the following conditions hold:
- i H is closed under the binary operation $*$.

Subgroup

- Def: Let H be a nonempty subset of G. The subset H is said to be a subgroup of G if H is a closed under the group operation of G and satisfies all the conditions of a group.
- For example the set of all rational numbers is a group under real addition.
- The set of all integers is a subgroup of the group of rational numbers under real addition.
- A subgroup of G that is not identical to G is called a proper subgroup of G
- Theorem 2.3: Let G be a group under the binary operation $*$. Let H be a nonempty subset of G. Then H is a subgroup of G if the following conditions hold:
-
  i H is closed under the binary operation $*$.
  ii For any element a in H, the inverse of a is also in H.

Subgroup

- Def: Let H be a nonempty subset of G. The subset H is said to be a subgroup of G if H is a closed under the group operation of G and satisfies all the conditions of a group.
- For example the set of all rational numbers is a group under real addition.
- The set of all integers is a subgroup of the group of rational numbers under real addition.
- A subgroup of G that is not identical to G is called a proper subgroup of G
- Theorem 2.3: Let G be a group under the binary operation $*$. Let H be a nonempty subset of G. Then H is a subgroup of G if the following conditions hold:
-
  - i H is closed under the binary operation $*$.
  - ii For any element a in H, the inverse of a is also in H.

Coset

Proof:

- Condition (ii) says that every element of H has an inverse in H. Condition (i) & (ii) ensure that the identity element of G is also in H ($a * a' = e$ is an element of H).

Coset

Proof:

- Condition (ii) says that every element of H has an inverse in H. Condition (i) & (ii) ensure that the identity element of G is also in H ($a * a' = e$ is an element of H).
- Because the elements in H are elements in G, the associative condition on $*$ holds automatically.

Coset

Proof:

- Condition (ii) says that every element of H has an inverse in H. Condition (i) & (ii) ensure that the identity element of G is also in H ($a * a' = e$ is an element of H).
- Because the elements in H are elements in G, the associative condition on $*$ holds automatically.
- H satisfies all the conditions of a group and is a subgroup of G.

Coset

Proof:

- Condition (ii) says that every element of H has an inverse in H. Condition (i) & (ii) ensure that the identity element of G is also in H ($a * a' = e$ is an element of H).
- Because the elements in H are elements in G, the associative condition on $*$ holds automatically.
- H satisfies all the conditions of a group and is a subgroup of G.
- Definition 2.2: Let H be a subgroup of a group G with binary operation $*$. Let a be an element of G.

Coset

Proof:

- Condition (ii) says that every element of H has an inverse in H. Condition (i) & (ii) ensure that the identity element of G is also in H ($a * a' = e$ is an element of H).
- Because the elements in H are elements in G, the associative condition on $*$ holds automatically.
- H satisfies all the conditions of a group and is a subgroup of G.
- Definition 2.2: Let H be a subgroup of a group G with binary operation $*$. Let a be an element of G.
- Then the set of elements is called a $a * aH \triangleq (a * ah : h \in H)$ is called a left coset of H; the set of elements is called a right coset of H.

Coset

Proof:

- Condition (ii) says that every element of H has an inverse in H. Condition (i) & (ii) ensure that the identity element of G is also in H ($a * a' = e$ is an element of H).
- Because the elements in H are elements in G, the associative condition on $*$ holds automatically.
- H satisfies all the conditions of a group and is a subgroup of G.
- Definition 2.2: Let H be a subgroup of a group G with binary operation $*$. Let a be an element of G.
- Then the set of elements is called a $a * aH \triangleq (a * ah : h \in H)$ is called a left coset of H; the set of elements is called a right coset of H.
- If the group G is commutative, then every left coset is identical to every right coset.

- Consider the additive group G={ 0,1,2,.,, .,15} under modulo-16. H={0,4,8,12} forms a subgroup of G.
- The coset $3 \boxplus H$ is

- Consider the additive group G={ 0,1,2,.,, .,15} under modulo-16. H={0,4,8,12} forms a subgroup of G.
- The coset $3 \boxplus H$ is
- $3 \boxplus H = \{3 \boxplus 0, 3 \boxplus 4, 3 \boxplus 8 3 \boxplus 12\}$ $3 \boxplus H = \{3, 7, 11, 15\}$

- Consider the additive group G={ 0,1,2,.,, .,15} under modulo-16. H={0,4,8,12} forms a subgroup of G.
- The coset $3 \boxplus H$ is
- $3 \boxplus H = \{3 \boxplus 0, 3 \boxplus 4, 3 \boxplus 83 \boxplus 12\}$ $3 \boxplus H = \{3, 7, 11, 15\}$
- The coset $7 \boxplus H$ is

- Consider the additive group G={ 0,1,2,.,, .,15} under modulo-16. H={0,4,8,12} forms a subgroup of G.
- The coset $3 \boxplus H$ is
- $3 \boxplus H = \{3 \boxplus 0, 3 \boxplus 4, 3 \boxplus 8 3 \boxplus 12\}$ $3 \boxplus H = \{3, 7, 11, 15\}$
- The coset $7 \boxplus H$ is
  $7 \boxplus H = \{7 \boxplus 0, 7 \boxplus 4, 7 \boxplus 8 7 \boxplus 12\}$

- Consider the additive group G={ 0,1,2,.,, .,15} under modulo-16. H={0,4,8,12} forms a subgroup of G.
- The coset $3 \boxplus H$ is
- $3 \boxplus H = \{3 \boxplus 0, 3 \boxplus 4, 3 \boxplus 8 3 \boxplus 12\}$ $3 \boxplus H = \{3, 7, 11, 15\}$
- The coset $7 \boxplus H$ is
  $7 \boxplus H = \{7 \boxplus 0, 7 \boxplus 4, 7 \boxplus 8 7 \boxplus 12\} 7 \boxplus H = \{7, 11, 15, 3\}$

- Consider the additive group G={ 0,1,2,.,, .,15} under modulo-16. H={0,4,8,12} forms a subgroup of G.
- The coset $3 \boxplus H$ is
- $3 \boxplus H = \{3 \boxplus 0, 3 \boxplus 4, 3 \boxplus 83 \boxplus 12\}$ $3 \boxplus H = \{3, 7, 11, 15\}$
- The coset $7 \boxplus H$ is
  $7 \boxplus H = \{7 \boxplus 0, 7 \boxplus 4, 7 \boxplus 87 \boxplus 12\} 7 \boxplus H = \{7, 11, 15, 3\}$
- We find that $3 \boxplus H = 7 \boxplus H$. There are only four distinct cosets of H Besides $3 \boxplus H$
- $0 \boxplus H = \{0, 4, 8, 12\}$

- Consider the additive group G={ 0,1,2,.,, .,15} under modulo-16. H={0,4,8,12} forms a subgroup of G.
- The coset $3 \boxplus H$ is
- $3 \boxplus H = \{3 \boxplus 0, 3 \boxplus 4, 3 \boxplus 83 \boxplus 12\}$ $3 \boxplus H = \{3, 7, 11, 15\}$
- The coset $7 \boxplus H$ is $7 \boxplus H = \{7 \boxplus 0, 7 \boxplus 4, 7 \boxplus 87 \boxplus 12\} 7 \boxplus H = \{7, 11, 15, 3\}$
- We find that $3 \boxplus H = 7 \boxplus H$. There are only four distinct cosets of H Besides $3 \boxplus H$
- $0 \boxplus H = \{0, 4, 8, 12\}$
- $1 \boxplus H = \{1, 5, 9, 13\}$

- Consider the additive group G={ 0,1,2,.,, .,15} under modulo-16. H={0,4,8,12} forms a subgroup of G.
- The coset $3 \boxplus H$ is
- $3 \boxplus H = \{3 \boxplus 0, 3 \boxplus 4, 3 \boxplus 83 \boxplus 12\}$ $3 \boxplus H = \{3, 7, 11, 15\}$
- The coset $7 \boxplus H$ is $7 \boxplus H = \{7 \boxplus 0, 7 \boxplus 4, 7 \boxplus 87 \boxplus 12\} 7 \boxplus H = \{7, 11, 15, 3\}$
- We find that $3 \boxplus H = 7 \boxplus H$. There are only four distinct cosets of H Besides $3 \boxplus H$
- $0 \boxplus H = \{0, 4, 8, 12\}$
- $1 \boxplus H = \{1, 5, 9, 13\}$
- $2 \boxplus H = \{2, 6, 10, 14\}$

- Consider the additive group G={ 0,1,2,.,, .,15} under modulo-16. H={0,4,8,12} forms a subgroup of G.
- The coset $3 \boxplus H$ is
- $3 \boxplus H = \{3 \boxplus 0, 3 \boxplus 4, 3 \boxplus 83 \boxplus 12\}$ $3 \boxplus H = \{3, 7, 11, 15\}$
- The coset $7 \boxplus H$ is
  $7 \boxplus H = \{7 \boxplus 0, 7 \boxplus 4, 7 \boxplus 87 \boxplus 12\}7 \boxplus H = \{7, 11, 15, 3\}$
- We find that $3 \boxplus H = 7 \boxplus H$. There are only four distinct cosets of H Besides $3 \boxplus H$
- $0 \boxplus H = \{0, 4, 8, 12\}$
- $1 \boxplus H = \{1, 5, 9, 13\}$
- $2 \boxplus H = \{2, 6, 10, 14\}$
- There are only four distinct cosets of H. The four distinct cosets of H are disjoint, and their union forms the entire group G.

- Theorem 2.4: Let H be a subgroup of a group G with binary operation $*$. No two elements in a coset of H are identical.
- The proof is based on the fact that all the elements in the subgroup H are distinct. Consider the coset $a * H = \{a * h :\in H\}$ with$a \in G$.
- Suppose two elements, say $a * h$ and $a * h'$, in a*H are identical, where h and h' are two distinct elements in H. Let a^{-1} denote the inverse of a with respect to the binary operation $*$. Then
- $$a^{-1} * (a * h) = a^{-1} * (a * h')$$
  $$(a^{-1} * a) * h = (a^{-1} * a) * h')$$
  $$e * h = e * h' h = h'$$
- This result is a contradiction to the fact that all the elements of H are distinct. Therefore, no two elements in a coset are identical.

2.5: No two elements in two different cosets of a subgroup H of a group G are identical. Proof: Let a*H and b*H be two distinct cosets of H, with a and b in G. Let a*h and b*h be two elements in a*H and b*H, respectively. Suppose $a * h = b * h'$. Let h^{-1} be the inverse of h.

$$(a * h) * h^{-1} = (b * b') * h^{-1}$$
$$a * (h * h^{-1}) = b * (b' * h^{-1})$$
$$a * e = b * h''$$
$$a = b * h''$$

where $(h'' = h * h^{-1})$ is an element in H. $a = b * h''$ implies that

$$\begin{aligned} a * H &= (b * b'') * H \\ &= \{(b * h'') * h : h \in H\} = \{b * (h'' * h) : h \in H\} \\ &= \{b * h''' : h''' \in H\} = b * H \end{aligned}$$

This result says that a*H and b*H are identical, which is a contradiction to the given condition that a*H and b*H are two distinct cosets of H. Therefore, no two elements in two distinct cosets of H are identical.

From Theorem 2.4 and 2.5, we obtain the following properties of cosets of a subgroup H of a group G:

i Every element in G appears in one and only one coset of H;

ii All the distinct cosets of H are disjoint;

iii The union of all the distinct cosets of H forms the group G.

All the distinct cosets of a subgroup H of a group G form a partition of G, denoted by G/H.

Lagranges Theorem: Let G be a group of order n, and let H be a subgroup of order m. Then m divides n, and the partition G/H consists of n/m cosets of H.

Proof: Every coset consists of m elements of G. Let i be the number of distinct cosets of H. Since n=im, m divides n and i=n/m.

Fields

- A field is a set of elements in which addition, subtraction, multiplication, and division is performed without leaving the set.

- A field is a set of elements in which addition, subtraction, multiplication, and division is performed without leaving the set.
- Addition and multiplication must satisfy the commutative, associative, and distributive laws.

- A field is a set of elements in which addition, subtraction, multiplication, and division is performed without leaving the set.
- Addition and multiplication must satisfy the commutative, associative, and distributive laws.
- Definition: Let F be a set of elements on which two binary operations, called addition "+" and multiplication "." are defined.

- A field is a set of elements in which addition, subtraction, multiplication, and division is performed without leaving the set.
- Addition and multiplication must satisfy the commutative, associative, and distributive laws.
- Definition: Let F be a set of elements on which two binary operations, called addition "+" and multiplication "." are defined. The set F together with the two binary operations "+" and "." is a field if the following conditions are satisfied:

- A field is a set of elements in which addition, subtraction, multiplication, and division is performed without leaving the set.
- Addition and multiplication must satisfy the commutative, associative, and distributive laws.
- Definition: Let F be a set of elements on which two binary operations, called addition "$+$" and multiplication "."are defined. The set F together with the two binary operations "$+$" and "." is a field if the following conditions are satisfied:
  1. F is a commutative group under addition $+$.
     The identity element with respect to addition is called the zero element i.e., 0.

- A field is a set of elements in which addition, subtraction, multiplication, and division is performed without leaving the set.
- Addition and multiplication must satisfy the commutative, associative, and distributive laws.
- Definition: Let F be a set of elements on which two binary operations, called addition "$+$" and multiplication "."are defined. The set F together with the two binary operations "$+$" and "." is a field if the following conditions are satisfied:
  1. F is a commutative group under addition $+$.
     The identity element with respect to addition is called the zero element i.e., 0.
  2. The set of nonzero elements in F is a commutative group under multiplication.
     The identity element with respect to multiplication is called the unit element i.e., 1.

- A field is a set of elements in which addition, subtraction, multiplication, and division is performed without leaving the set.
- Addition and multiplication must satisfy the commutative, associative, and distributive laws.
- Definition: Let F be a set of elements on which two binary operations, called addition "+" and multiplication "." are defined. The set F together with the two binary operations "+" and "." is a field if the following conditions are satisfied:
  1. F is a commutative group under addition +.
     The identity element with respect to addition is called the zero element i.e., 0.
  2. The set of nonzero elements in F is a commutative group under multiplication.
     The identity element with respect to multiplication is called the unit element i.e., 1.
  3. Multiplication is distributive over addition; that is, for any three elements a, b, and c in F,

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

- A field is a set of elements in which addition, subtraction, multiplication, and division is performed without leaving the set.
- Addition and multiplication must satisfy the commutative, associative, and distributive laws.
- Definition: Let F be a set of elements on which two binary operations, called addition "+" and multiplication "." are defined. The set F together with the two binary operations "+" and "." is a field if the following conditions are satisfied:
  1. F is a commutative group under addition +.
     The identity element with respect to addition is called the zero element i.e., 0.
  2. The set of nonzero elements in F is a commutative group under multiplication.
     The identity element with respect to multiplication is called the unit element i.e., 1.
  3. Multiplication is distributive over addition; that is, for any three elements a, b, and c in F,

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

- These properties can, be satisfied if the field size is any prime number or any integer power of a prime.

- The number of elements in a field is called the order of the field.

- The number of elements in a field is called the order of the field.
- A field with finite number of elements is called a finite field or Galois Field, denoted by GF(p), p can be a prime number or power of prime.

- The number of elements in a field is called the order of the field.
- A field with finite number of elements is called a finite field or Galois Field, denoted by GF(p), p can be a prime number or power of prime.
- In a field, the additive inverse of an element a is denoted by $-a$ and the multiplicative inverse of a is denoted by a^{-1} provided that $a \neq 0$.

- The number of elements in a field is called the order of the field.
- A field with finite number of elements is called a finite field or Galois Field, denoted by GF(p), p can be a prime number or power of prime.
- In a field, the additive inverse of an element a is denoted by $-a$ and the multiplicative inverse of a is denoted by a^{-1} provided that $a \neq 0$.
- Subtracting a field element b from another field element a is defined as adding the additive inverse $-b$ of b to a. $[a - b \triangleq a + (-b)]$.

- The number of elements in a field is called the order of the field.
- A field with finite number of elements is called a finite field or Galois Field, denoted by GF(p), p can be a prime number or power of prime.
- In a field, the additive inverse of an element a is denoted by $-a$ and the multiplicative inverse of a is denoted by a^{-1} provided that $a \neq 0$.
- Subtracting a field element b from another field element a is defined as adding the additive inverse $-b$ of b to a. $[a - b \triangleq a + (-b)]$.
- If b is a nonzero element, dividing a by b is defined as multiplying a by the multiplicative inverse b^{-1} of b . $[a \div b \triangleq a \cdot b^{-1})]$

- GF(2), p=2 GF(2)={0,1} is a binary set.
- Modulo-2 addition for GF(2), additive identity: 0

Table: Modulo-2 addition

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

Modulo-2 multiplication for GF(2),multiplicative identity: 1

Table: Modulo-2 multiplication

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

Consider GF(3), p=3 GF(3)={0,1,2}. additive identity is: 0, multiplicative identity is: 1
In GF(3), the additive inverse of 0 is 0, and the additive inverse of 1 is 2 and vice versa. The multiplicative inverse can be found by identifying from the table pairs of elements whose product is 1 . In the case of GF(3), we see that the multiplicative inverse of 1 is 1 and the multiplicative inverse of 2 is 2.
commutative, associative, and distributive
Additive a+b=b+a 1+2=2+1=0
Associative a+(b+c)=(a+b)+c=0+1+2=

Table: Modulo-3 addition

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

Table: Modulo-3 multiplication

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- GF(7), here p=7 GF(7)={0,1,2,3,4,5,6}. additive identity: 0, multiplicative identity: 1

Table: Modulo-7 addition

$\oplus$	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

Table: Modulo-7 multiplication

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

- The addition table shown above is used also for subtraction.
- For example , if we want to subtract 6 from 3 , we first use the addition table to find the additive inverse of 6, which is 1.
- Then we add 1 to 3 to obtain the result [i.e., 3-6=3+(-6)=3+1=4].
- For division, we use the multiplication table.
- Suppose that we divide 3 by 2. We first find the multiplicative inverse of 2, which is 4, and then we multiply 3 by 4 to obtain the result ,[i.e., $3 \div 2 = 3.(2^-1) = 3.4 = 5$].
- For any prime p, there exist a finite field of p elements.
- For any positive integer m it is possible to extend the prime field GF(p) to a field of p^m elements, which is called an extension field of GF(p) and is denoted by $GF(p^m)$

Def: Primitive

- In a finite field Gf(q), a nonzero element a is said to be primitive if the order of a is $q - 1$

Def: Primitive

- In a finite field Gf(q), a nonzero element a is said to be primitive if the order of a is $q - 1$
- The powers of a primitive element generate all the nonzero elements of GF(q).

Def: Primitive

- In a finite field Gf(q), a nonzero element a is said to be primitive if the order of a is $q - 1$
- The powers of a primitive element generate all the nonzero elements of GF(q).
- Every finite field has a primitive element.

Def: Primitive

- In a finite field Gf(q), a nonzero element *a* is said to be primitive if the order of *a* is $q-1$
- The powers of a primitive element generate all the nonzero elements of GF(q).
- Every finite field has a primitive element.
- Primitive elements are useful for constructing fields.

Def: Primitive

- In a finite field Gf(q), a nonzero element *a* is said to be primitive if the order of *a* is $q-1$
- The powers of a primitive element generate all the nonzero elements of GF(q).
- Every finite field has a primitive element.
- Primitive elements are useful for constructing fields.

Example. In GF(7) 3 is a primitive element.
$3^1 = 3$, $3^2 = 3.3 = 2$, $3^3 = 3.3^2 = 6$, $3^4 = 3.3^3 = 4$, $3^5 = 3.3^4 = 5$,
$3^6 = 3.3^5 = 1$
Therefore, the order of the integer 3 is 6, and the integer 3 is a primitive element of GF(7),
$4^1 = 4$, $4^2 = 4.4 = 2$, $4^3 = 4.4^2 = 1$
Clearly, the order of the integer 4 is 3, which is factor of 6.

Binary Field Arithmetic

Historical Notes

- Galois fields are named in honor of the French mathematician Evariste Galois (1811 1832) who was killed in a duel at the age of 20.

Historical Notes

- Galois fields are named in honor of the French mathematician Evariste Galois (1811 1832) who was killed in a duel at the age of 20.
- On the eve of his death, he wrote a letter to his friend in which he gave the results of his theory of algebraic equations, already presented to the Pairs Academy.

Remarks

1. Galois fields are important in the study of cyclic codes, a special class of block codes. In particular, they are used for constructing the well-known random error correcting BCH and Reed-Solomon Codes.

Remarks

1. Galois fields are important in the study of cyclic codes, a special class of block codes. In particular, they are used for constructing the well-known random error correcting BCH and Reed-Solomon Codes.
2. GF(2m) is an extension field of GF(2).

Remarks

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

In general, we can construct codes with symbols from any Galois field GF(q), where q is either a prime p or a power of p; however,codes with symbols from the binary field GF(2) or its extension $GF(2^m)$ are most widely used in digital data transmission and storage systems.

In binary arithmetic, we use modulo-2 addition and multiplication .

Sets of equations e.g. X+Y=1, X+Z=0, X+Y+Z=1 Solved by Cramers rule

$$\begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix} = 1\begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix} - 1\begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} + 0\begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}$$
$$= 1.1 - 1.0 + 0.1 = 1$$

$$x = \frac{\begin{vmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}}{\Delta} = \frac{0}{1} = 0$$

$$y = \frac{\begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}}{\Delta} = \frac{1}{1} = 1$$

$$z = \frac{\begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{vmatrix}}{\Delta} = \frac{0}{1} = 0$$

$g(x) = g_0 + g_1x + g_2x + ... + g_mx^m \qquad m \leq n$

Added (or subtracted)

$f(x)g(x) = (f_0 + g_0) + (f_1 + g_1)x + ...(f_m + g_m)x^m + f_{m+1}x_{m+1} + ...(f_n)x^n$

Multiplied

$f(x) \cdot g(x) = c_0 + c_1x + ... + c_{n+m}x^{n+m}$

$c_i = f_0g_i + f_1g_{i-1} + ... + f_ig_0(c_0 = f_0g_0 \quad c_{n+m} = f_ng_m)$

If g(x) = 0, then f(x) 0 = 0

i Commutative

$f(x) + g(x) = g(x) + f(x)$

$f(x) \cdot g(x) = g(x) \cdot f(x)$

ii Associative

$f(x) + [g(x) + h(x)] = [f(x) \cdot g(x)] + [f(x) \cdot h(x)]$

$f(x) \cdot [g(x) \cdot h(x)] = [f(x) \cdot g(x)] \cdot h(x)]$

iii Distributive

$f(x) \cdot [g(x) + h(x)] = [f(x) + g(x)] + h(x)]$

$f(x) \cdot [g(x) \cdot h(x)] = [f(x) \cdot g(x)] \cdot h(x)]$

- Polynomials over GF(2). We denote it GF(2).

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1x + f_2x^2 + \ldots + f_nx^n$

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1 x + f_2 x^2 + ... + f_n x^n$
- where $f_i = 0 \; or \; 1 \quad for \;\; 0 \leq i \leq n$

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1x + f_2x^2 + ... + f_nx^n$
- where $f_i = 0 \ or \ 1 \quad for \ \ 0 \leq i \leq n$
- The degree of a polynomial is the largest power of X with nonzero coefficient.

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1 x + f_2 x^2 + ... + f_n x^n$
- where $f_i = 0 \; or \; 1 \quad for \;\; 0 \leq i \leq n$
- The degree of a polynomial is the largest power of X with nonzero coefficient.
- if $f_n = 1$, $\deg[f(x)] = n$

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1x + f_2x^2 + ... + f_nx^n$
- where $f_i = 0 \ or \ 1 \quad for \ \ 0 \leq i \leq n$
- The degree of a polynomial is the largest power of X with nonzero coefficient.
- if $f_n = 1$, $\deg[f(x)] = n$

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1x + f_2x^2 + ... + f_nx^n$
- where $f_i = 0 \; or \; 1 \quad for \;\; 0 \leq i \leq n$
- The degree of a polynomial is the largest power of X with nonzero coefficient.
- if $f_n = 1$, $\deg[f(x)] = n$
- if $f_1 = ...f_n = 0, f_0 = 1 \; \deg[f(x)] = 0$

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1x + f_2x^2 + ... + f_nx^n$
- where $f_i = 0 \; or \; 1 \quad for \;\; 0 \leq i \leq n$
- The degree of a polynomial is the largest power of X with nonzero coefficient.
- if $f_n = 1$, $\deg[f(x)] = n$
- if $f_1 = ...f_n = 0, f_0 = 1 \; \deg[f(x)] = 0$
- A polynomial with coefficients from the binary field GF(2) is called a binary polynomial.

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1 x + f_2 x^2 + ... + f_n x^n$
- where $f_i = 0 \ or \ 1 \quad for \ \ 0 \leq i \leq n$
- The degree of a polynomial is the largest power of X with nonzero coefficient.
- if $f_n = 1$, $\deg[f(x)] = n$
- if $f_1 = ...f_n = 0, f_0 = 1 \ \deg[f(x)] = 0$
- A polynomial with coefficients from the binary field GF(2) is called a binary polynomial.
- e.g. $1 + x^2$ and $1 + x^3 + x^5$ are binary polynomials.

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1 x + f_2 x^2 + ... + f_n x^n$
- where $f_i = 0 \ or \ 1 \quad for \ \ 0 \leq i \leq n$
- The degree of a polynomial is the largest power of X with nonzero coefficient.
- if $f_n = 1$, $\deg[f(x)] = n$
- if $f_1 = ... f_n = 0, f_0 = 1 \ \deg[f(x)] = 0$
- A polynomial with coefficients from the binary field GF(2) is called a binary polynomial.
- e.g. $1 + x^2$ and $1 + x^3 + x^5$ are binary polynomials.
- Polynomials over GF(2) with degree $= 1$ are $x, \ \ 1 + x$

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1 x + f_2 x^2 + ... + f_n x^n$
- where $f_i = 0 \ or \ 1 \quad for \ \ 0 \leq i \leq n$
- The degree of a polynomial is the largest power of X with nonzero coefficient.
- if $f_n = 1$, $\deg[f(x)] = n$
- if $f_1 = ...f_n = 0, f_0 = 1 \ \deg[f(x)] = 0$
- A polynomial with coefficients from the binary field GF(2) is called a binary polynomial.
- e.g. $1 + x^2$ and $1 + x^3 + x^5$ are binary polynomials.
- Polynomials over GF(2) with degree $= 1$ are $x, \ \ 1 + x$
- Polynomials over GF(2) with degree $= 2$ are

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1x + f_2x^2 + ... + f_nx^n$
- where $f_i = 0 \; or \; 1 \quad for \;\; 0 \leq i \leq n$
- The degree of a polynomial is the largest power of X with nonzero coefficient.
- if $f_n = 1$, $\deg[f(x)] = n$
- if $f_1 = ...f_n = 0, f_0 = 1 \; \deg[f(x)] = 0$
- A polynomial with coefficients from the binary field GF(2) is called a binary polynomial.
- e.g. $1 + x^2$ and $1 + x^3 + x^5$ are binary polynomials.
- Polynomials over GF(2) with degree $= 1$ are $x, \;\; 1 + x$
- Polynomials over GF(2) with degree $= 2$ are
- $x^2, \;\; 1 + x^2, \;\; x + x^2, \;\; 1 + x + x^2$

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1 x + f_2 x^2 + ... + f_n x^n$
- where $f_i = 0 \; or \; 1 \quad for \;\; 0 \leq i \leq n$
- The degree of a polynomial is the largest power of X with nonzero coefficient.
- if $f_n = 1$, $\deg[f(x)] = n$
- if $f_1 = ...f_n = 0, f_0 = 1 \; \deg[f(x)] = 0$
- A polynomial with coefficients from the binary field GF(2) is called a binary polynomial.
- e.g. $1 + x^2$ and $1 + x^3 + x^5$ are binary polynomials.
- Polynomials over GF(2) with degree = 1 are $x, \;\; 1 + x$
- Polynomials over GF(2) with degree = 2 are
- $x^2, \;\; 1 + x^2, \;\; x + x^2, \;\; 1 + x + x^2$
- In general, with degree = n we have 2^n polynomials.

- Polynomials over GF(2). We denote it GF(2).
- $f(x) = f_0 + f_1 x + f_2 x^2 + ... + f_n x^n$
- where $f_i = 0 \ or \ 1 \quad for \ \ 0 \leq i \leq n$
- The degree of a polynomial is the largest power of X with nonzero coefficient.
- if $f_n = 1$, $\deg[f(x)] = n$
- if $f_1 = ...f_n = 0, f_0 = 1 \deg[f(x)] = 0$
- A polynomial with coefficients from the binary field GF(2) is called a binary polynomial.
- e.g. $1 + x^2$ and $1 + x^3 + x^5$ are binary polynomials.
- Polynomials over GF(2) with degree $= 1$ are $x, \quad 1 + x$
- Polynomials over GF(2) with degree $= 2$ are
- $x^2, \quad 1 + x^2, \quad x + x^2, \quad 1 + x + x^2$
- In general, with degree = n we have 2^n polynomials.
- Polynomials over GF(2) can be added (or subtracted), multiplied, and divided in the usual way.

Add $a(x) = 1 + x + x^3 + x^5$ and $b(x) = 1 + x^2 + x^3 + x^4 + x^7$

Add $a(x) = 1 + x + x^3 + x^5$ and $b(x) = 1 + x^2 + x^3 + x^4 + x^7$

$$a(x) + b(x) = (1 + 1) + x + x^2 + (1 + 1)x^3 + x^4 + x^5 + x^7$$

For multiplication f(x) and g(x)

$$f(x).g(x) = c_0 + c_1X + c_2X^2 + \ldots + c_{n+m}X^{n+m}$$

Divide $f(x) = 1 + x + x^4 + x^5 + x^6$ by $f(x) = 1 + x + x^3$ using long division technique

Divide $f(x) = 1 + x + x^4 + x^5 + x^6$ by $f(x) = 1 + x + x^3$ using long division technique

$$
\begin{array}{r l}
 & x^3 + x^2 \\
x^3 + x + 1) & \overline{x^6 + x^5 + x^4 \qquad\qquad + x + 1} \\
 & x^6 + \qquad x^4 + x^3 \\
\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\cdots\cdots \\
 & \qquad x^5 \quad + x^3 \qquad\quad + x + 1 \\
 & \qquad x^5 \quad + x^3 \quad + x^2
\end{array}
$$

- Suppose the degree of *g(x)* is not zero, and *f(x)* is divided by g(x) then a pair of polynomials are obtained over GF(2)-q(x) called the quotient, and r(x) called the remainder.

- Suppose the degree of *g(x)* is not zero, and *f(x)* is divided by g(x) then a pair of polynomials are obtained over GF(2)-q(x) called the quotient, and r(x) called the remainder.
- $f(x)=q(x)g(x)+r(x)$

- Suppose the degree of *g(x)* is not zero, and *f(x)* is divided by g(x) then a pair of polynomials are obtained over GF(2)-q(x) called the quotient, and r(x) called the remainder.
- $f(x)=q(x)g(x)+r(x)$
- The degree of r(x) is less than that of g(x)

- Suppose the degree of *g(x)* is not zero, and *f(x)* is divided by g(x) then a pair of polynomials are obtained over GF(2)-q(x) called the quotient, and r(x) called the remainder.
- $f(x)=q(x)g(x)+r(x)$
- The degree of r(x) is less than that of g(x)
- When f(x) is divisible by g(x), if the remainder r(x) is identical to zero [r(x)=0] then it is said that f(x) is divisible by g(x) and g(x) is a factor of f(x)

- Suppose the degree of *g(x)* is not zero, and *f(x)* is divided by g(x) then a pair of polynomials are obtained over GF(2)-q(x) called the quotient, and r(x) called the remainder.
- $f(x)=q(x)g(x)+r(x)$
- The degree of r(x) is less than that of g(x)
- When f(x) is divisible by g(x), if the remainder r(x) is identical to zero [r(x)=0] then it is said that f(x) is divisible by g(x) and g(x) is a factor of f(x)
- $p(x) \in GF(2)$ [x] with deg[p(x)]=m is said to be irreducible over GF(2) if p(x) is not divisible by any polynomial over GF(2) of degree less than m but greater than zero.

- Suppose the degree of *g(x)* is not zero, and *f(x)* is divided by g(x) then a pair of polynomials are obtained over GF(2)-q(x) called the quotient, and r(x) called the remainder.
- *f(x)=q(x)g(x)+r(x)*
- The degree of r(x) is less than that of g(x)
- When f(x) is divisible by g(x), if the remainder r(x) is identical to zero [r(x)=0] then it is said that f(x) is divisible by g(x) and g(x) is a factor of f(x)
- $p(x) \in GF(2)$ [x] with deg[p(x)]=m is said to be irreducible over GF(2) if p(x) is not divisible by any polynomial over GF(2) of degree less than m but greater than zero.
- e.g. $1 + x + x^2$, $1 + x + x^3$, $1 + x^2 + x^5$ and $1 + x + x^5$ are irreducible polynomials.

- Suppose the degree of *g(x)* is not zero, and *f(x)* is divided by g(x) then a pair of polynomials are obtained over GF(2)-q(x) called the quotient, and r(x) called the remainder.
- $f(x)=q(x)g(x)+r(x)$
- The degree of r(x) is less than that of g(x)
- When f(x) is divisible by g(x), if the remainder r(x) is identical to zero [r(x)=0] then it is said that f(x) is divisible by g(x) and g(x) is a factor of f(x)
- $p(x) \in GF(2)$ [x] with deg[p(x)]=m is said to be irreducible over GF(2) if p(x) is not divisible by any polynomial over GF(2) of degree less than m but greater than zero.
- e.g. $1+x+x^2$, $1+x+x^3$, $1+x^2+x^5$ and $1+x+x^5$ are irreducible polynomials.
- For any positive integer $m \geq 1$, there exists at least one irreducible polynomial of degree m.

- Suppose the degree of *g(x)* is not zero, and *f(x)* is divided by g(x) then a pair of polynomials are obtained over GF(2)-q(x) called the quotient, and r(x) called the remainder.
- $f(x)=q(x)g(x)+r(x)$
- The degree of r(x) is less than that of g(x)
- When f(x) is divisible by g(x), if the remainder r(x) is identical to zero [r(x)=0] then it is said that f(x) is divisible by g(x) and g(x) is a factor of f(x)
- $p(x) \in GF(2)$ [x] with deg[p(x)]=m is said to be irreducible over GF(2) if p(x) is not divisible by any polynomial over GF(2) of degree less than m but greater than zero.
- e.g. $1+x+x^2$, $1+x+x^3$, $1+x^2+x^5$ and $1+x+x^5$ are irreducible polynomials.
- For any positive integer $m \geq 1$, there exists at least one irreducible polynomial of degree m.
- For a polynomial f(x), if the polynomial has an even number of terms, it is divisible by x+1

- Suppose the degree of *g(x)* is not zero, and *f(x)* is divided by g(x) then a pair of polynomials are obtained over GF(2)-q(x) called the quotient, and r(x) called the remainder.
- *f(x)=q(x)g(x)+r(x)*
- The degree of r(x) is less than that of g(x)
- When f(x) is divisible by g(x), if the remainder r(x) is identical to zero [r(x)=0] then it is said that f(x) is divisible by g(x) and g(x) is a factor of f(x)
- $p(x) \in GF(2)$ [x] with deg[p(x)]=m is said to be irreducible over GF(2) if p(x) is not divisible by any polynomial over GF(2) of degree less than m but greater than zero.
- e.g. $1+x+x^2$, $1+x+x^3$, $1+x^2+x^5$ and $1+x+x^5$ are irreducible polynomials.
- For any positive integer $m \geq 1$, there exists at least one irreducible polynomial of degree m.
- For a polynomial f(x), if the polynomial has an even number of terms, it is divisible by x+1

- For real numbers if a is root of a polynomial f(x) [f(a)=0]. f(x) is divisible by x-a [x+a]

- For real numbers if a is root of a polynomial f(x) [f(a)=0]. f(x) is divisible by x-a [x+a]

  Consider $f(x) = 1 + X^2 + X^3 + X^4$
  $f(1) = 1 + 1^2 + 1^3 + 1^4$=1+1+1+1=0 Thus f(x) has 1 as a root , and it should be divisible by x+1

- For real numbers if a is root of a polynomial f(x) [f(a)=0]. f(x) is divisible by x-a [x+a]

Consider $f(x) = 1 + X^2 + X^3 + X^4$
$f(1) = 1 + 1^2 + 1^3 + 1^4$=1+1+1+1=0 Thus f(x) has 1 as a root , and it should be divisible by x+1

$$\begin{array}{r}
x^3 + x^2 + 1 \\
x + 1\overline{)x^4 + x^3 + x^2 \qquad + 1} \\
x^4 + x^3 \qquad\qquad\qquad \\
\hline
x^2 \qquad + 1 \\
x^2 \quad + x \qquad \\
\hline
x + 1 \\
x + 1 \\
\hline
0
\end{array}$$

Primitive

- An irreducible polynomial p(x) of degree m is said to be primitive if the smallest positive integer n for which p(x) divides $x^n + 1$ is $n = 2^m - 1$.

Primitive

- An irreducible polynomial p(x) of degree m is said to be primitive if the smallest positive integer n for which p(x) divides $x^n + 1$ is $n = 2^m - 1$.
- $p(x) = x^4 + x + 1$ divides $x^{15} + 1$ but does not divide any $x^n + 1$ for $1 \leq n \leq 15$. Hence $p(x) = x^4 + x + 1$ is primitive polynomial.

Primitive

- An irreducible polynomial p(x) of degree m is said to be primitive if the smallest positive integer n for which p(x) divides $x^n + 1$ is $n = 2^m - 1$.
- $p(x) = x^4 + x + 1$ divides $x^{15} + 1$ but does not divide any $x^n + 1$ for $1 \leq n \leq 15$. Hence $p(x) = x^4 + x + 1$ is primitive polynomial.
- For a given $m > 0$, there may be more than one primitive polynomials of degree n.

Primitive

- An irreducible polynomial p(x) of degree m is said to be primitive if the smallest positive integer n for which p(x) divides $x^n + 1$ is $n = 2^m - 1$.
- $p(x) = x^4 + x + 1$ divides $x^{15} + 1$ but does not divide any $x^n + 1$ for $1 \leq n \leq 15$. Hence $p(x) = x^4 + x + 1$ is primitive polynomial.
- For a given $m > 0$, there may be more than one primitive polynomials of degree n.
- 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 $n = 2^4 - 1 = 15$

Primitive

- An irreducible polynomial p(x) of degree m is said to be primitive if the smallest positive integer n for which p(x) divides $x^n + 1$ is $n = 2^m - 1$.
- $p(x) = x^4 + x + 1$ divides $x^{15} + 1$ but does not divide any $x^n + 1$ for $1 \leq n \leq 15$. Hence $p(x) = x^4 + x + 1$ is primitive polynomial.
- For a given $m > 0$, there may be more than one primitive polynomials of degree n.
- 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 $n = 2^4 - 1 = 15$

m	Primitive Polynomial
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	$1 + x + x^9$
10	$1 + x + x^{10}$
11	$1 + x^2 + x^{11}$
12	$1 + x + x^4 + x^6 + x^{12}$
13	$1 + x + x^3 + x^4 + x^{13}$

Any irreducible polynomial over GF(2) of degree m, divides $x^{2^m-1} + 1$

Any irreducible polynomial over GF(2) of degree m, divides $x^{2^m-1}+1$
x^3+x+1 divides $x^{2^3-1}+1=x^7+1$

Any irreducible polynomial over GF(2) of degree m, divides $x^{2^m-1}+1$
x^3+x+1 divides $x^{2^3-1}+1=x^7+1$

$$
\begin{array}{r}
x^4+x^2+x+1 \\
x^3+x+1)\overline{x^7 \qquad\qquad\qquad +1} \\
x^7 \quad +x^5 \quad +x^4 \qquad\qquad \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
x^5 \quad +x^4 \qquad\quad +1 \\
x^5 \quad +x^3+x^2 \qquad \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
x^4 \ +x^3+x^2+1 \\
x^4 \ + \quad x^2+x \quad \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
x^3+x+1 \\
x^3+x+1 \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
0
\end{array}
$$

Construction of Galois Field $GF(2^m)$

- Consider two elements 0 and 1 from GF(2) and a new symbol α
- Define multiplication "."
- $$\begin{aligned} 0.0 &= 0 \\ 0.1 &= 0 \\ 1.0 &= 0 \\ 1.1 &= 1 \\ 0.\alpha &= \alpha.0 = 0 \\ 1.\alpha &= \alpha.1 = \alpha \\ \alpha^2 &= \alpha.\alpha \\ \alpha^3 &= \alpha.\alpha.\alpha \\ &\vdots \\ \alpha^3 &= \alpha.\alpha.\ldots.\alpha(j\ times) \end{aligned}$$
- $$\begin{aligned} 0.\alpha^j &= \alpha^j.0 \\ 1.\alpha^j &= \alpha^j.1 = \alpha^j \\ \alpha^i.\alpha^j &= \alpha^j.\alpha^i = \alpha^{i+j} \end{aligned}$$

The set of elements on which a multiplication "." is

$$F = (0, 1, \alpha, \alpha^2 \ldots \alpha^j \ldots)$$

Let p(X) be positive polynomial of degree m over GF(2). Assume that $p(\alpha) = 0$ where $p(\alpha)$ is root of p(X)
Then p(X) divides $X^{2^m-1} + 1$

$$X^{2^m-1} + 1 = q(x)p(x) \tag{6}$$

Replace X with α

$$\alpha^{2^m-1} + 1 = q(\alpha)p(\alpha)$$

and $p(\alpha) = 0$

$$\alpha^{2^m-1} + 1 = q(\alpha).0$$

If we regard $q(\alpha)$ as a polynomial of over α over $GF(2)$ $q(\alpha).0 = 0$

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

Adding 1 on both sides

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

Therefore, under the condition that $p(\alpha) = 0$ the set F becomes finite and contains the following elements:

$$F^* = (0, 1, \alpha, \alpha^2, \vdots \alpha^{2^m-2})$$

The nonzero elements of F^* are closed under the multiplication operation "."

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, $\alpha^4 = 1 + \alpha$. Using this relation $GF(2^4)$ is constructed.

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, $\alpha^4 = 1 + \alpha$. Using this relation $GF(2^4)$ is constructed.

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

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, $\alpha^4 = 1 + \alpha$. Using this relation $GF(2^4)$ is constructed.

$\alpha^5 = \alpha.\alpha^4 = \alpha(1 + \alpha) = \alpha + \alpha^2$,$\alpha^6 = \alpha.\alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$,

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, $\alpha^4 = 1 + \alpha$. Using this relation $GF(2^4)$ is constructed.

$\alpha^5 = \alpha.\alpha^4 = \alpha(1 + \alpha) = \alpha + \alpha^2$,$\alpha^6 = \alpha.\alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$,$\alpha^7 = \alpha.\alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3$,

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, $\alpha^4 = 1 + \alpha$. Using this relation $GF(2^4)$ is constructed.

$\alpha^5 = \alpha.\alpha^4 = \alpha(1 + \alpha) = \alpha + \alpha^2$,$\alpha^6 = \alpha.\alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$,$\alpha^7 = \alpha.\alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3$,To multiply two elements $\alpha^i * \alpha^j$ their exponents are added.

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, $\alpha^4 = 1 + \alpha$. Using this relation $GF(2^4)$ is constructed.

$\alpha^5 = \alpha.\alpha^4 = \alpha(1 + \alpha) = \alpha + \alpha^2$,$\alpha^6 = \alpha.\alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$,$\alpha^7 = \alpha.\alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3$,To multiply two elements $\alpha^i * \alpha^j$ their exponents are added.$\alpha^5 * \alpha^7 = \alpha^{12}$,
$\alpha^{12} * \alpha^7 = \alpha^{19}$

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, $\alpha^4 = 1 + \alpha$. Using this relation $GF(2^4)$ is constructed.

$\alpha^5 = \alpha.\alpha^4 = \alpha(1 + \alpha) = \alpha + \alpha^2$,$\alpha^6 = \alpha.\alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$,$\alpha^7 = \alpha.\alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3$,To multiply two elements $\alpha^i * \alpha^j$ their exponents are added.$\alpha^5 * \alpha^7 = \alpha^{12}$, $\alpha^{12} * \alpha^7 = \alpha^{19}$For division α^j, by α^i, multiply α^j by the multiplicative inverse α^{15-i}.

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, $\alpha^4 = 1 + \alpha$. Using this relation $GF(2^4)$ is constructed.

$\alpha^5 = \alpha.\alpha^4 = \alpha(1 + \alpha) = \alpha + \alpha^2$,$\alpha^6 = \alpha.\alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$,$\alpha^7 = \alpha.\alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3$,To multiply two elements $\alpha^i * \alpha^j$ their exponents are added.$\alpha^5 * \alpha^7 = \alpha^{12}$, $\alpha^{12} * \alpha^7 = \alpha^{19}$For division α^j, by α^i, multiply α^j by the multiplicative inverse α^{15-i}.Example. $\alpha^4/\alpha^{12} = \alpha^4 * \alpha^3 = \alpha^7$

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, $\alpha^4 = 1 + \alpha$. Using this relation $GF(2^4)$ is constructed.

$\alpha^5 = \alpha.\alpha^4 = \alpha(1 + \alpha) = \alpha + \alpha^2$,$\alpha^6 = \alpha.\alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$,$\alpha^7 = \alpha.\alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3$,To multiply two elements $\alpha^i * \alpha^j$ their exponents are added.$\alpha^5 * \alpha^7 = \alpha^{12}$,

$\alpha^{12} * \alpha^7 = \alpha^{19}$For division α^j, by α^i, multiply α^j by the multiplicative inverse α^{15-i}.Example. $\alpha^4/\alpha^{12} = \alpha^4 * \alpha^3 = \alpha^7$

$\alpha^{12}/\alpha^5 = \alpha^{12} * \alpha^{10} = \alpha^{22} = \alpha^7$

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, $\alpha^4 = 1 + \alpha$. Using this relation $GF(2^4)$ is constructed.

$\alpha^5 = \alpha.\alpha^4 = \alpha(1 + \alpha) = \alpha + \alpha^2$,$\alpha^6 = \alpha.\alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$,$\alpha^7 = \alpha.\alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3$,To multiply two elements $\alpha^i * \alpha^j$ their exponents are added.$\alpha^5 * \alpha^7 = \alpha^{12}$,

$\alpha^{12} * \alpha^7 = \alpha^{19}$For division α^j, by α^i, multiply α^j by the multiplicative inverse α^{15-i}.Example. $\alpha^4/\alpha^{12} = \alpha^4 * \alpha^3 = \alpha^7$

$\alpha^{12}/\alpha^5 = \alpha^{12} * \alpha^{10} = \alpha^{22} = \alpha^7$

To add α^i and α^j polynomial representation given in table is used.

Construction of Galois Field

Let m=4. The polynomial $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2).

Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, $\alpha^4 = 1 + \alpha$. Using this relation $GF(2^4)$ is constructed.

$\alpha^5 = \alpha.\alpha^4 = \alpha(1 + \alpha) = \alpha + \alpha^2$,$\alpha^6 = \alpha.\alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$,$\alpha^7 = \alpha.\alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3$,To multiply two elements $\alpha^i * \alpha^j$ their exponents are added.$\alpha^5 * \alpha^7 = \alpha^{12}$,

$\alpha^{12} * \alpha^7 = \alpha^{19}$For division α^j, by α^i, multiply α^j by the multiplicative inverse α^{15-i}.Example. $\alpha^4/\alpha^{12} = \alpha^4 * \alpha^3 = \alpha^7$

$\alpha^{12}/\alpha^5 = \alpha^{12} * \alpha^{10} = \alpha^{22} = \alpha^7$

To add α^i and α^j polynomial representation given in table is used.

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

$1 + \alpha^5 + \alpha^{10} = 1 + (\alpha + \alpha^2) + (1 + \alpha + \alpha^2) = 0$

Power representation	*Polynomial representation*	*4 − Tuple representation*
0	0	(0000)
1	1	(1000)
α	α	(0100)
α^2	α^2	(0010)
α^3	α^3	(0001)
α^4	$1+\alpha$	(1100)
α^5	$\alpha+\alpha^2$	(0110)
α^6	$\alpha^2+\alpha^3$	(0011)
α^7	$1+\alpha+\alpha^3$	(1101)
α^8	$1+\alpha^2$	(1010)
α^9	$\alpha+\alpha^3$	(0101)
α^{10}	$1+\alpha^2+\alpha^3$	(1110)
α^{11}	$\alpha+\alpha^2+\alpha^3$	(0111)
α^{12}	$1+\alpha+\alpha^2+\alpha^3$	(1111)
α^{13}	$1+\alpha^2+\alpha^3$	(1011)
α^{14}	$1+\alpha^3$	(1001)

Basic Properies of a Galois Field $GF(2^m)$

In ordinary algebra a polynomial with real coefficients has roots not from the field of real numbers but from the field of complex numbers

$$X^2 + 6X + 25$$

does not have roots from the real numbers but has two complex conjugate roots

$$\frac{-6 \pm \sqrt{36 - 100}}{2}$$

-3+4i and -3-4i
In case of polynomial with coefficients from $GF(2)$ may not have roots from $GF(2)$ but has roots from an extension field of $GF(2)$.
Consider $X^4 + X^4 + 1$ is irreducible over $GF(2)$ and therefore it does not have roots from $GF(2)$
It has four roots which are α^7, α^{11}, α^{13}, and α^{14}

$$(\alpha^7)^4 + (\alpha^7)^3 + 1 = (1 + \alpha^2 + \alpha^3) + (\alpha^2 + \alpha^3) + 1 = 0$$

$\alpha^7, \alpha^{11}, \alpha^{13}$ *and* α^{14} are the other roots of $f(x)$

$$(X+\alpha^7)(X+\alpha^{11})(X+\alpha^{13})(X+\alpha^{14})$$

$$\begin{aligned}
&= [X^2+(\alpha^7+\alpha^{11})X+\alpha^{18}][X^2+(\alpha^{13}+\alpha^{14})X+\alpha^{27}] \\
&= (X^2+\alpha^8X+\alpha^3)(X^2+\alpha^2X+\alpha^{12}] \\
&= X^4+(\alpha^8+\alpha^2)X^3+(\alpha^{12}+\alpha^{10}+\alpha^3)X^2+(\alpha^{20}X+\alpha^5)X+\alpha^{15} \\
&= X^4+X^3+1
\end{aligned}$$

$$(X+\alpha^7)(X+\alpha^{11})(X+\alpha^{13})(X+\alpha^{14}) =$$

Theorem: Let f(x) be a polynomial with coefficients from GF(2). Let β be an element in an extension field of GF(2). If β is a root of f(x), then for any $l \geq 0$ β^{2^l} is also root of f(x)

$f(X) = 1+X^3+X^4+X^5+X^6$ has α^4

The conjugates of α^4 are

$$(\alpha^4)^2 = \alpha^8, \;\; (\alpha^4)^{2^2} = \alpha^{16} = \alpha, \;\; (\alpha^4)^{2^3} = \alpha^{32} = \alpha^2$$

Theorem 2.18 Let $\phi(X)$ be the minimal polynomial of an element β in $GF(2^m)$. Let e be the smallest integer such that $\beta^{2^e} = \beta$. Then

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

Consider a primitive polynomial $f(x) = x^3 + x + 1 \in GF(2)[x]$ and let α be a root of f(x). Then the elements of GF(8) 0=0, $\alpha^0 = 1$, $\alpha^1 = \alpha$, $\alpha^2 = \alpha^2$ $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$ $\alpha^5 = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha^2 + 1$ $(X - \alpha)(X - \alpha^2)(X - \alpha^4)$

$$\begin{aligned}
&= (X^2 - X(\alpha + \alpha^2) + \alpha^3)(X - \alpha^4) \\
&= X^3 - X^2(\alpha + \alpha^2) + X\alpha^3 - X^2\alpha^4 - X(\alpha + \alpha^2)\alpha^4 - \alpha^7 \\
&= X^3 - X^2(\alpha + \alpha^2 + \alpha^4) - X(\alpha^5 + \alpha^6 + \alpha^3) - \alpha^7 \\
&= X^3 - X^2(\alpha + \alpha^2 + \alpha^4) - X(\alpha^5 + \alpha^6 + \alpha^3) - \alpha^7 \\
&= X^3 - X^2(\alpha + \alpha^2 + \alpha^2 + \alpha) - X(\alpha^2 + \alpha + 1 + \alpha^2 + 1 + \alpha + 1) - \alpha^7 \\
&= X^3 + X + 1
\end{aligned}$$

Table: Minimal polynomial of the elements in $GF(2^3)$ generated by $f(x) = X^4 + X + 1$

Conjugate roots	Minimal polynomial
0	M.(x) = x-0 = x
$\alpha^0 = 1$	$M_0(x)$ = x -1 = x + 1
$\alpha, \alpha^2, \alpha^4 = 1$	$M_1(x)= (x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1$
$\alpha^3, \alpha^6, \alpha^5 = 1$	$M_3(x)= (x - \alpha^3)(x - \alpha^6)(x - \alpha^5) = x^3 + x^2 + 1$

Consider a primitive polynomial $f(x) = X^4 + X + 1$ and Galois Field $GF(2^4)$ let $\beta = \alpha^3$. The conjugates of β are $\beta^2 = \alpha^6$, $\beta^{2^2}=\alpha^{12}$, $\beta^{2^3}=\alpha^{24} = \alpha^9$
The minimal polynomial polynomial of $\beta = \alpha^3$ is then

$$\begin{aligned}
&= (X+\alpha^3)(X+\alpha^6)(X+\alpha^{12})(X+\alpha^9) \\
&= [X^2 + (\alpha^3+\alpha^6)X + \alpha^9][X^2 + (\alpha^{12}+\alpha^9)X + \alpha^{21}] \\
&= [X^2 + \alpha^2 X + \alpha^9][X^2 + \alpha^8 X + \alpha^6] \\
&= X^4 + (\alpha^2+\alpha^8)X^3 + (\alpha^6+\alpha^{10}+\alpha^9)X^2 + (\alpha^{17}+\alpha^8)X + \alpha^{15} \\
&= X^4 + X^3 + X^2 + X + 1
\end{aligned}$$

Table: Minimal polynomial of the elements in $GF(2^4)$ generated by $f(x) = X^4 + X + 1$

Conjugate roots	Minimal polynomial
0	M.(x) = x-0 = x
$\alpha^0 = 1$	$M_0(x)$ = x -1 = x + 1
$\alpha, \alpha^2, \alpha^4, \alpha^8 = 1$	$M_1(x)= (x-\alpha)(x-\alpha^2)(x-\alpha^4) = x^4 + x + 1$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12} = 1$	$M_3(x)= (x-\alpha^3)(x-\alpha^6)(x-\alpha^5) = x^4 + x^3 + x^2 + x + 1$
α^5, α^{10}	$x^2 + x + 1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$x^4 + x^3 + 1$

Theorem 2.20 If β is primitive element of $GF(2^m)$, all its conjugates β^2, β^{2^2} are also primitive elements of $GF(2^m)$

Vector Space

- V be a set of elements with a binary operation '$+$' is defined.

- V be a set of elements with a binary operation '$+'$ is defined.
- F be a field. A multiplication operator $'\cdot'$ between the elements in F and elements in V is also defined.

- V be a set of elements with a binary operation '$+'$ is defined.
- F be a field. A multiplication operator $'\cdot'$ between the elements in F and elements in V is also defined.
- The V is called a vector space over the field F if it satisfies the following conditions:

  i V is a commutative group under addition.

- V be a set of elements with a binary operation '$+'$ is defined.
- F be a field. A multiplication operator $'\cdot'$ between the elements in F and elements in V is also defined.
- The V is called a vector space over the field F if it satisfies the following conditions:

  i V is a commutative group under addition.

  ii For any element in v in V a.v is an element in V.

- V be a set of elements with a binary operation '$+'$ is defined.
- F be a field. A multiplication operator $'\cdot'$ between the elements in F and elements in V is also defined.
- The V is called a vector space over the field F if it satisfies the following conditions:

  i V is a commutative group under addition.

  ii For any element in v in V a.v is an element in V.

  iii (Distributive law) For any elements in u and v in V and any elements a and b in F.

- V be a set of elements with a binary operation '$+$' is defined.
- F be a field. A multiplication operator $'\cdot'$ between the elements in F and elements in V is also defined.
- The V is called a vector space over the field F if it satisfies the following conditions:

   i V is a commutative group under addition.

   ii For any element in v in V a.v is an element in V.

   iii (Distributive law) For any elements in u and v in V and any elements a and b in F.
   $a \cdot (u + v) = a \cdot u + a \cdot v$

- V be a set of elements with a binary operation '$+'$ is defined.
- F be a field. A multiplication operator $'\cdot'$ between the elements in F and elements in V is also defined.
- The V is called a vector space over the field F if it satisfies the following conditions:

    i V is a commutative group under addition.

    ii For any element in v in V a.v is an element in V.

    iii (Distributive law) For any elements in u and v in V and any elements a and b in F.
    $a \cdot (u + v) = a \cdot u + a \cdot v$
    $(a + b) \cdot v = a \cdot v + b \cdot v$

- V be a set of elements with a binary operation '+' is defined.
- F be a field. A multiplication operator '·' between the elements in F and elements in V is also defined.
- The V is called a vector space over the field F if it satisfies the following conditions:

  i V is a commutative group under addition.

  ii For any element in v in V a.v is an element in V.

  iii (Distributive law) For any elements in u and v in V and any elements a and b in F.
  $a \cdot (u + v) = a \cdot u + a \cdot v$
  $(a + b) \cdot v = a \cdot v + b \cdot v$

  iv (Associative Law) For any v in V and any element a and b in F

- V be a set of elements with a binary operation '$+'$ is defined.
- F be a field. A multiplication operator $'\cdot'$ between the elements in F and elements in V is also defined.
- The V is called a vector space over the field F if it satisfies the following conditions:

  i V is a commutative group under addition.

  ii For any element in v in V a.v is an element in V.

  iii (Distributive law) For any elements in u and v in V and any elements a and b in F.
  $a \cdot (u + v) = a \cdot u + a \cdot v$
  $(a + b) \cdot v = a \cdot v + b \cdot v$

  iv (Associative Law) For any v in V and any element a and b in F
  $(a \cdot b) \cdot v = a \cdot (b \cdot v)$

- V be a set of elements with a binary operation '$+$' is defined.
- F be a field. A multiplication operator $'\cdot'$ between the elements in F and elements in V is also defined.
- The V is called a vector space over the field F if it satisfies the following conditions:

  i V is a commutative group under addition.

  ii For any element in v in V a.v is an element in V.

  iii (Distributive law) For any elements in u and v in V and any elements a and b in F.
  $a \cdot (u + v) = a \cdot u + a \cdot v$
  $(a + b) \cdot v = a \cdot v + b \cdot v$

  iv (Associative Law) For any v in V and any element a and b in F
  $(a \cdot b) \cdot v = a \cdot (b \cdot v)$

  v Let 1 be the unit element of F Then for nay v in $V \cdot 1 \cdot v = v$

- The elements of V are called vectors and the elements of the field F are called scalars.

- The elements of V are called vectors and the elements of the field F are called scalars.
- The addition on V is called a vector addition and the multiplication that combines a scalar in F and a vector in V is referred to as scalar multiplication (or product)
- The additive identity of V is denoted by 0.

- The elements of V are called vectors and the elements of the field F are called scalars.
- The addition on V is called a vector addition and the multiplication that combines a scalar in F and a vector in V is referred to as scalar multiplication (or product)
- The additive identity of V is denoted by 0.
- Property I. Let 0 be the zero element of the field F. For any vector v in V, $0 \cdot v = 0$.

- The elements of V are called vectors and the elements of the field F are called scalars.
- The addition on V is called a vector addition and the multiplication that combines a scalar in F and a vector in V is referred to as scalar multiplication (or product)
- The additive identity of V is denoted by 0.
- Property I. Let 0 be the zero element of the field F. For any vector v in V, $0 \cdot v = 0$.
- Property II. For any scalar c in F, $c \cdot 0 = 0$.

- The elements of V are called vectors and the elements of the field F are called scalars.
- The addition on V is called a vector addition and the multiplication that combines a scalar in F and a vector in V is referred to as scalar multiplication (or product)
- The additive identity of V is denoted by 0.
- Property I. Let 0 be the zero element of the field F. For any vector v in V, $0 \cdot v = 0$.
- Property II. For any scalar c in F, $c \cdot 0 = 0$.
- Property III. For any scalar c in F and any vector v in V,

- The elements of V are called vectors and the elements of the field F are called scalars.
- The addition on V is called a vector addition and the multiplication that combines a scalar in F and a vector in V is referred to as scalar multiplication (or product)
- The additive identity of V is denoted by 0.
- Property I. Let 0 be the zero element of the field F. For any vector v in V, $0 \cdot v = 0$.
- Property II. For any scalar c in F, $c \cdot 0 = 0$.
- Property III. For any scalar c in F and any vector v in V, $(-c) \cdot v = c \cdot (-v) = -(c \cdot v)$ i.e., $(-c) \cdot v$ or $c \cdot (-v)$ is the additive inverse of the vector $c \cdot v$.

- Consider an ordered sequence of n components, $(a_0, a_1, a_2, ...a_{n-1})$, where each component a_i is an element from the binary field GF(2) (i.e., $a_i = 0$ or 1).

- Consider an ordered sequence of n components, $(a_0, a_1, a_2, ...a_{n-1})$, where each component a_i is an element from the binary field GF(2) (i.e., $a_i = 0$ or 1).
- This sequence is called an n-tuple over GF(2).

- Consider an ordered sequence of n components, $(a_0, a_1, a_2, ...a_{n-1})$, where each component a_i is an element from the binary field GF(2) (i.e., $a_i = 0$ or 1).
- This sequence is called an n-tuple over GF(2).
- Since there are two choices for each a_i, we can construct distinct n-tuples.
- Let V_n denote this set. Now we define an addition $+$ on as following : For any

- Consider an ordered sequence of n components, $(a_0, a_1, a_2, ...a_{n-1})$, where each component a_i is an element from the binary field GF(2) (i.e., $a_i = 0$ or 1).
- This sequence is called an n-tuple over GF(2).
- Since there are two choices for each a_i, we can construct distinct n-tuples.
- Let V_n denote this set. Now we define an addition $+$ on as following : For any $u = (u_0, u_1, u_2, ...u_{n-1})$, and $v = (v_0, v_1, v_2, ...v_{n-1})$

- Consider an ordered sequence of n components, $(a_0, a_1, a_2, ...a_{n-1})$, where each component a_i is an element from the binary field GF(2) (i.e., $a_i = 0$ or 1).
- This sequence is called an n-tuple over GF(2).
- Since there are two choices for each a_i, we can construct distinct n-tuples.
- Let V_n denote this set. Now we define an addition $+$ on as following : For any $u = (u_0, u_1, u_2, ...u_{n-1})$, and $v = (v_0, v_1, v_2, ...v_{n-1})$

$$u + v = (u_0 + v_0, u_1 + v_1, u_2 + v_2, ...u_{n-1} + v_{n-1})$$

- Consider an ordered sequence of n components, $(a_0, a_1, a_2, ...a_{n-1})$, where each component a_i is an element from the binary field GF(2) (i.e., $a_i = 0$ or 1).
- This sequence is called an n-tuple over GF(2).
- Since there are two choices for each a_i, we can construct distinct n-tuples.
- Let V_n denote this set. Now we define an addition $+$ on as following : For any $u = (u_0, u_1, u_2, ...u_{n-1})$, and $v = (v_0, v_1, v_2, ...v_{n-1})$

$$u + v = (u_0 + v_0, u_1 + v_1, u_2 + v_2, ...u_{n-1} + v_{n-1})$$

- where $u_i + v_i$ is carried out in modulo-2 addition.

- Consider an ordered sequence of n components, $(a_0, a_1, a_2, ...a_{n-1})$, where each component a_i is an element from the binary field GF(2) (i.e., $a_i = 0$ or 1).
- This sequence is called an n-tuple over GF(2).
- Since there are two choices for each a_i, we can construct distinct n-tuples.
- Let V_n denote this set. Now we define an addition $+$ on as following : For any $u = (u_0, u_1, u_2, ...u_{n-1})$, and $v = (v_0, v_1, v_2, ...v_{n-1})$

$$u + v = (u_0 + v_0, u_1 + v_1, u_2 + v_2, ...u_{n-1} + v_{n-1})$$

- where $u_i + v_i$ is carried out in modulo-2 addition.
- $u + v$ is also an n-tuple over GF(2). Closed under addition.

- Consider an ordered sequence of n components, $(a_0, a_1, a_2, ...a_{n-1})$, where each component a_i is an element from the binary field GF(2) (i.e., $a_i = 0$ or 1).
- This sequence is called an n-tuple over GF(2).
- Since there are two choices for each a_i, we can construct distinct n-tuples.
- Let V_n denote this set. Now we define an addition $+$ on as following : For any $u = (u_0, u_1, u_2, ...u_{n-1})$, and $v = (v_0, v_1, v_2, ...v_{n-1})$
$$u + v = (u_0 + v_0, u_1 + v_1, u_2 + v_2, ...u_{n-1} + v_{n-1})$$
- where $u_i + v_i$ is carried out in modulo-2 addition.
- $u + v$ is also an n-tuple over GF(2). Closed under addition.
- We can readily verify that is a commutative group under the addition defined by.

- Consider an ordered sequence of n components, $(a_0, a_1, a_2, ...a_{n-1})$, where each component a_i is an element from the binary field GF(2) (i.e., $a_i = 0$ or 1).
- This sequence is called an n-tuple over GF(2).
- Since there are two choices for each a_i, we can construct distinct n-tuples.
- Let V_n denote this set. Now we define an addition $+$ on as following : For any $u = (u_0, u_1, u_2, ...u_{n-1})$, and $v = (v_0, v_1, v_2, ...v_{n-1})$

$$u + v = (u_0 + v_0, u_1 + v_1, u_2 + v_2, ...u_{n-1} + v_{n-1})$$

- where $u_i + v_i$ is carried out in modulo-2 addition.
- $u + v$ is also an n-tuple over GF(2).Closed under addition.
- We can readily verify that is a commutative group under the addition defined by.
- we see that allzero n-tuple $0 = (0, 0, ..., 0)$ is the additive identity. For any v in,

- Consider an ordered sequence of n components, $(a_0, a_1, a_2, ...a_{n-1})$, where each component a_i is an element from the binary field GF(2) (i.e., $a_i = 0$ or 1).
- This sequence is called an n-tuple over GF(2).
- Since there are two choices for each a_i, we can construct distinct n-tuples.
- Let V_n denote this set. Now we define an addition + on as following : For any $u = (u_0, u_1, u_2, ...u_{n-1})$, and $v = (v_0, v_1, v_2, ...v_{n-1})$
$$u + v = (u_0 + v_0, u_1 + v_1, u_2 + v_2, ...u_{n-1} + v_{n-1})$$
- where $u_i + v_i$ is carried out in modulo-2 addition.
- $u + v$ is also an n-tuple over GF(2).Closed under addition.
- We can readily verify that is a commutative group under the addition defined by.
- we see that allzero n-tuple $0 = (0, 0, ..., 0)$ is the additive identity. For any v in, V_n
$$v + v = (v_0 + v_0, v_1 + v_1, ...v_{n-1} + v_{n-1}) = (0, 0, 0, ...0) = 0$$

- Hence, the additive inverse of each n-tuples in is itself.

- Hence, the additive inverse of each n-tuples in is itself.
- Since modulo-2 addition is commutative and associative, the addition is also commutative and associative.

- Hence, the additive inverse of each n-tuples in is itself.
- Since modulo-2 addition is commutative and associative, the addition is also commutative and associative.
- Therefore, is a commutative group under the addition.

- Hence, the additive inverse of each n-tuples in is itself.
- Since modulo-2 addition is commutative and associative, the addition is also commutative and associative.
- Therefore, is a commutative group under the addition.
- We defined scalar multiplication of an n-tuple v in n V

- Hence, the additive inverse of each n-tuples in is itself.
- Since modulo-2 addition is commutative and associative, the addition is also commutative and associative.
- Therefore, is a commutative group under the addition.
- We defined scalar multiplication of an n-tuple v in n V
- by an element a from GF(2) as follows :

- Hence, the additive inverse of each n-tuples in is itself.
- Since modulo-2 addition is commutative and associative, the addition is also commutative and associative.
- Therefore, is a commutative group under the addition.
- We defined scalar multiplication of an n-tuple v in n V
- by an element a from GF(2) as follows :
- $a.(v_0, v_1, v_2, ...v_{n-1}) = (a.v_0, a.v_1, a.v_2, ...a.v_{n-1})$

- Hence, the additive inverse of each n-tuples in is itself.
- Since modulo-2 addition is commutative and associative, the addition is also commutative and associative.
- Therefore, is a commutative group under the addition.
- We defined scalar multiplication of an n-tuple v in n V
- by an element a from GF(2) as follows :
- $a.(v_0, v_1, v_2, ...v_{n-1}) = (a.v_0, a.v_1, a.v_2, ...a.v_{n-1})$
- where $a.v_i$ is carried out in modulo-2 multiplication.
- Clearly, $a.(v_0, v_1, v_2, ...v_{n-1})$ is also an n-tuple in V_n.

- Hence, the additive inverse of each n-tuples in is itself.
- Since modulo-2 addition is commutative and associative, the addition is also commutative and associative.
- Therefore, is a commutative group under the addition.
- We defined scalar multiplication of an n-tuple v in n V
- by an element a from GF(2) as follows :
- $a.(v_0, v_1, v_2, ...v_{n-1}) = (a.v_0, a.v_1, a.v_2, ...a.v_{n-1})$
- where $a.v_i$ is carried out in modulo-2 multiplication.
- Clearly, $a.(v_0, v_1, v_2, ...v_{n-1})$ is also an n-tuple in V_n.
- If a = 1, $1.(v_0, v_1, v_2, ...v_{n-1}) = (1.v_0, 1.v_1, 1.v_2, ...1.v_{n-1})$

- Hence, the additive inverse of each n-tuples in is itself.
- Since modulo-2 addition is commutative and associative, the addition is also commutative and associative.
- Therefore, is a commutative group under the addition.
- We defined scalar multiplication of an n-tuple v in n V
- by an element a from GF(2) as follows :
- $a.(v_0, v_1, v_2, ...v_{n-1}) = (a.v_0, a.v_1, a.v_2, ...a.v_{n-1})$
- where $a.v_i$ is carried out in modulo-2 multiplication.
- Clearly, $a.(v_0, v_1, v_2, ...v_{n-1})$ is also an n-tuple in V_n.
- If a = 1, $1.(v_0, v_1, v_2, ...v_{n-1}) = (1.v_0, 1.v_1, 1.v_2, ...1.v_{n-1})$
- $= (v_0, v_1, v_2, ...v_{n-1})$

- Hence, the additive inverse of each n-tuples in is itself.
- Since modulo-2 addition is commutative and associative, the addition is also commutative and associative.
- Therefore, is a commutative group under the addition.
- We defined scalar multiplication of an n-tuple v in n V
- by an element a from GF(2) as follows :
- $a.(v_0, v_1, v_2, ...v_{n-1}) = (a.v_0, a.v_1, a.v_2, ...a.v_{n-1})$
- where $a.v_i$ is carried out in modulo-2 multiplication.
- Clearly, $a.(v_0, v_1, v_2, ...v_{n-1})$ is also an n-tuple in V_n.
- If a $= 1$, $1.(v_0, v_1, v_2, ...v_{n-1}) = (1.v_0, 1.v_1, 1.v_2, ...1.v_{n-1})$
- $= (v_0, v_1, v_2, ...v_{n-1})$
- Vector addition and scalar multiplication satisfy the distributive and associative laws.
- Therefore the set V_n of all n tuples over GF(2)forms a vector space over over GF(2)

Let n=5. The vector space V_5 of all 5 tuples over GF(2) consists of the following 32 vectors.

(00000),(00001),(00010),(00011),
(00100),(00101),(00110),(00111),
(01000),(01001),(01010),(01011),
(01100),(01101),(01110),(01111),
(10000),(10001),(10010),(10011),
(10100),(10101),(10110),(10111),
(11000),(11001),(11010),(11011),
(11100),(11101),(11110),(11111)

- The vector sum of (10111)and (11001) is

- The vector sum of (10111)and (11001) is
- (10111)+(11001)=(1+1,0+1,1+0,1+0,1+1)=(01110)

- The vector sum of (10111)and (11001) is
- (10111)+(11001)=(1+1,0+1,1+0,1+0,1+1)=(01110)
- The scalar multiplication is

- The vector sum of (10111)and (11001) is
- (10111)+(11001)=(1+1,0+1,1+0,1+0,1+1)=(01110)
- The scalar multiplication is
- 0.(11010)=(0.1, 0.1, 0.0, 0.1, 0.0)=(00000)
- 1.(11010)=(1.1, 1.1, 1.0, 1.1, 1.0)=(11010)

Theorem 2.18

- Let S be a nonempty subset of a vector space V over a field F. Then S is a subspace of V if the following conditions are satisfied :

Theorem 2.18

- Let S be a nonempty subset of a vector space V over a field F. Then S is a subspace of V if the following conditions are satisfied :
  i For any two vectors u and v in S, u + v is also a vector in S.

Theorem 2.18

- Let S be a nonempty subset of a vector space V over a field F. Then S is a subspace of V if the following conditions are satisfied :
  i For any two vectors u and v in S, u + v is also a vector in S.
  ii For an element a in F and any vector u in S, a u is also in S.

Theorem 2.18

- Let S be a nonempty subset of a vector space V over a field F. Then S is a subspace of V if the following conditions are satisfied :
  - i For any two vectors u and v in S, u + v is also a vector in S.
  - ii For an element a in F and any vector u in S, a u is also in S.
- Conditions (i) and (ii) says that S is closed under vector addition and scalar multiplication of V.

Theorem 2.18

- Let S be a nonempty subset of a vector space V over a field F. Then S is a subspace of V if the following conditions are satisfied :
  - i For any two vectors u and v in S, u + v is also a vector in S.
  - ii For an element a in F and any vector u in S, a u is also in S.
- Conditions (i) and (ii) says that S is closed under vector addition and scalar multiplication of V.
- Condition (ii) ensures that, for any vector v in S, its additive inverse (-1).v is also in S. Then, v + (-1).v = 0 is also in S.

Theorem 2.18

- Let S be a nonempty subset of a vector space V over a field F. Then S is a subspace of V if the following conditions are satisfied :
  - i For any two vectors u and v in S, u + v is also a vector in S.
  - ii For an element a in F and any vector u in S, a u is also in S.
- Conditions (i) and (ii) says that S is closed under vector addition and scalar multiplication of V.
- Condition (ii) ensures that, for any vector v in S, its additive inverse (-1).v is also in S. Then, v + (-1).v = 0 is also in S.
- Therefore, S is a subgroup of V. Since the vectors of S are also vectors of V, the associative and distributive laws must hold for S.

Theorem 2.18

- Let S be a nonempty subset of a vector space V over a field F. Then S is a subspace of V if the following conditions are satisfied :
  - i For any two vectors u and v in S, u + v is also a vector in S.
  - ii For an element a in F and any vector u in S, a u is also in S.
- Conditions (i) and (ii) says that S is closed under vector addition and scalar multiplication of V.
- Condition (ii) ensures that, for any vector v in S, its additive inverse (-1).v is also in S. Then, v + (-1).v = 0 is also in S.
- Therefore, S is a subgroup of V. Since the vectors of S are also vectors of V, the associative and distributive laws must hold for S.
- Hence, S is a vector space over F and is a subspace of V.

Theorem 2.18

- Let S be a nonempty subset of a vector space V over a field F. Then S is a subspace of V if the following conditions are satisfied :
  - i For any two vectors u and v in S, u + v is also a vector in S.
  - ii For an element a in F and any vector u in S, a u is also in S.
- Conditions (i) and (ii) says that S is closed under vector addition and scalar multiplication of V.
- Condition (ii) ensures that, for any vector v in S, its additive inverse (-1).v is also in S. Then, v + (-1).v = 0 is also in S.
- Therefore, S is a subgroup of V. Since the vectors of S are also vectors of V, the associative and distributive laws must hold for S.
- Hence, S is a vector space over F and is a subspace of V.

Consider the vector space V_5 of all 5-tuples over GF(2)

Theorem 2.18

- Let S be a nonempty subset of a vector space V over a field F. Then S is a subspace of V if the following conditions are satisfied :
  - i For any two vectors u and v in S, u + v is also a vector in S.
  - ii For an element a in F and any vector u in S, a u is also in S.
- Conditions (i) and (ii) says that S is closed under vector addition and scalar multiplication of V.
- Condition (ii) ensures that, for any vector v in S, its additive inverse (-1).v is also in S. Then, v + (-1).v = 0 is also in S.
- Therefore, S is a subgroup of V. Since the vectors of S are also vectors of V, the associative and distributive laws must hold for S.
- Hence, S is a vector space over F and is a subspace of V.

Consider the vector space V_5 of all 5-tuples over GF(2)The set {(00000),(00111),(11010),(11101)}

Theorem 2.18

- Let S be a nonempty subset of a vector space V over a field F. Then S is a subspace of V if the following conditions are satisfied :
  - i For any two vectors u and v in S, u + v is also a vector in S.
  - ii For an element a in F and any vector u in S, a u is also in S.
- Conditions (i) and (ii) says that S is closed under vector addition and scalar multiplication of V.
- Condition (ii) ensures that, for any vector v in S, its additive inverse (-1).v is also in S. Then, v + (-1).v = 0 is also in S.
- Therefore, S is a subgroup of V. Since the vectors of S are also vectors of V, the associative and distributive laws must hold for S.
- Hence, S is a vector space over F and is a subspace of V.

Consider the vector space V_5 of all 5-tuples over GF(2)The set
{(00000),(00111),(11010),(11101)}
satisfies the conditions of Theorem so it is a subspace of V_5

- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.

- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- Let $a_1, a_2, \ldots, a_k$ be k scalars from F. The sum

- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- Let $a_1, a_2, \ldots, a_k$ be k scalars from F. The sum
- $$a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$$

- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- Let $a_1, a_2, \ldots, a_k$ be k scalars from F. The sum
- $$a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$$
- is called a linear combination of $v_1, v_2, \ldots, v_k$. Clearly, the sum of two linear combinations of $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$,

- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- Let $a_1, a_2, \ldots, a_k$ be k scalars from F. The sum
- $$a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$$
- is called a linear combination of $v_1, v_2, \ldots, v_k$. Clearly, the sum of two linear combinations of $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$,
- $(a_1 v_1 + a_2 v_2 + \ldots + a_k v_k) + (b_1 v_1 + b_2 v_2 + +b_k v_k)$

- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- Let $a_1, a_2, \ldots, a_k$ be k scalars from F. The sum
- $$a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$$
- is called a linear combination of $v_1, v_2, \ldots, v_k$. Clearly, the sum of two linear combinations of $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$,
- $(a_1 v_1 + a_2 v_2 + \ldots + a_k v_k) + (b_1 v_1 + b_2 v_2 + +b_k v_k) =$ $(a_1 + b_1)v_1 + (a_2 + b_2)v_2 + \ldots + (a_k + b_k)v_k$
- is also a linear combination of $v_1, v_2, \ldots, v_k$, and the product of a scalar c in F and a linear combination of $v_1, v_2, \ldots, v_k$,

- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- Let $a_1, a_2, \ldots, a_k$ be k scalars from F. The sum
- $$a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$$
- is called a linear combination of $v_1, v_2, \ldots, v_k$. Clearly, the sum of two linear combinations of $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$,
- $(a_1 v_1 + a_2 v_2 + \ldots + a_k v_k) + (b_1 v_1 + b_2 v_2 + +b_k v_k) =$ $(a_1 + b_1)v_1 + (a_2 + b_2)v_2 + \ldots + (a_k + b_k)v_k$
- is also a linear combination of $v_1, v_2, \ldots, v_k$, and the product of a scalar c in F and a linear combination of $v_1, v_2, \ldots, v_k$,
- $c.(a_1 v_1 + a_2 v_2 + \ldots + a_k v_k) = (c.a_1)v_1 + (c.a_2)v_2 + \ldots (c.a_k)v_k$

- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- Let $a_1, a_2, \ldots, a_k$ be k scalars from F. The sum
- $$a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$$
- is called a linear combination of $v_1, v_2, \ldots, v_k$. Clearly, the sum of two linear combinations of $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$,
- $(a_1 v_1 + a_2 v_2 + \ldots + a_k v_k) + (b_1 v_1 + b_2 v_2 + +b_k v_k) = (a_1 + b_1)v_1 + (a_2 + b_2)v_2 + \ldots + (a_k + b_k)v_k$
- is also a linear combination of $v_1, v_2, \ldots, v_k$, and the product of a scalar c in F and a linear combination of $v_1, v_2, \ldots, v_k$,
- $c.(a_1 v_1 + a_2 v_2 + \ldots + a_k v_k) = (c.a_1)v_1 + (c.a_2)v_2 + \ldots (c.a_k)v_k$
- is also a linear combination of $v_1, v_2, \ldots, v_k$

- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- Let $a_1, a_2, \ldots, a_k$ be k scalars from F. The sum
- $$a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$$
- is called a linear combination of $v_1, v_2, \ldots, v_k$. Clearly, the sum of two linear combinations of $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$,
- $(a_1 v_1 + a_2 v_2 + \ldots + a_k v_k) + (b_1 v_1 + b_2 v_2 + +b_k v_k) =$ $(a_1 + b_1)v_1 + (a_2 + b_2)v_2 + \ldots + (a_k + b_k)v_k$
- is also a linear combination of $v_1, v_2, \ldots, v_k$, and the product of a scalar c in F and a linear combination of $v_1, v_2, \ldots, v_k$,
- $c.(a_1 v_1 + a_2 v_2 + \ldots + a_k v_k) = (c.a_1)v_1 + (c.a_2)v_2 + \ldots (c.a_k)v_k$
- is also a linear combination of $v_1, v_2, \ldots, v_k$

- Consider the vector space V_5 of all 5 tuples over GF(2). The linear combination of (00111) and (11101) are

$$0.(00111)+0.(11101)=(00000)$$
$$0.(00111)+1.(11101)=(11101)$$
$$1.(00111)+0.(11101)=(00111)$$
$$1.(00111)+1.(11101)=(11010)$$

- Theorem 2.23
- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.

- Theorem 2.23
- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- The set of all linear combinations of $v_1, v_2, \ldots, v_k$ forms a subspace of V.

- Theorem 2.23
- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- The set of all linear combinations of $v_1, v_2, \ldots, v_k$ forms a subspace of V.
- A set of vectors $v_1, v_2, \ldots, v_k$ in a vector space V over a field F is said to be linearly dependent if and only if there exit k scalars $a_1, a_2, \ldots, a_k$ from F, not all zeros, such that

- Theorem 2.23
- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- The set of all linear combinations of $v_1, v_2, \ldots, v_k$ forms a subspace of V.
- A set of vectors $v_1, v_2, \ldots, v_k$ in a vector space V over a field F is said to be linearly dependent if and only if there exit k scalars $a_1, a_2, \ldots, a_k$ from F, not all zeros, such that
- $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k = 0$

- Theorem 2.23
- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- The set of all linear combinations of $v_1, v_2, \ldots, v_k$ forms a subspace of V.
- A set of vectors $v_1, v_2, \ldots, v_k$ in a vector space V over a field F is said to be linearly dependent if and only if there exit k scalars $a_1, a_2, \ldots, a_k$ from F, not all zeros, such that
- $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k = 0$
- A set of vectors $v_1, v_2, \ldots, v_k$ is said to be linearly independent if it is not linearly dependent. That is, if $v_1, v_2, \ldots, v_k$ are linearly independent, then

- Theorem 2.23
- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- The set of all linear combinations of $v_1, v_2, \ldots, v_k$ forms a subspace of V.
- A set of vectors $v_1, v_2, \ldots, v_k$ in a vector space V over a field F is said to be linearly dependent if and only if there exit k scalars $a_1, a_2, \ldots, a_k$ from F, not all zeros, such that
- $a_1v_1 + a_2v_2 + \ldots + a_kv_k = 0$
- A set of vectors $v_1, v_2, \ldots, v_k$ is said to be linearly independent if it is not linearly dependent. That is, if $v_1, v_2, \ldots, v_k$ are linearly independent, then
- $a_1v_1 + a_2v_2 + \ldots + a_kv_k \neq 0$

- Theorem 2.23
- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- The set of all linear combinations of $v_1, v_2, \ldots, v_k$ forms a subspace of V.
- A set of vectors $v_1, v_2, \ldots, v_k$ in a vector space V over a field F is said to be linearly dependent if and only if there exit k scalars $a_1, a_2, \ldots, a_k$ from F, not all zeros, such that
- $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k = 0$
- A set of vectors $v_1, v_2, \ldots, v_k$ is said to be linearly independent if it is not linearly dependent. That is, if $v_1, v_2, \ldots, v_k$ are linearly independent, then
- $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k \neq 0$

EX. The vectors (1 0 1 1 0), (0 1 0 0 1), and (1 1 1 1 1) are linearly dependent since

- Theorem 2.23
- Let $v_1, v_2, \ldots, v_k$ be k vectors in a vector space V over a field F.
- The set of all linear combinations of $v_1, v_2, \ldots, v_k$ forms a subspace of V.
- A set of vectors $v_1, v_2, \ldots, v_k$ in a vector space V over a field F is said to be linearly dependent if and only if there exit k scalars $a_1, a_2, \ldots, a_k$ from F, not all zeros, such that
- $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k = 0$
- A set of vectors $v_1, v_2, \ldots, v_k$ is said to be linearly independent if it is not linearly dependent. That is, if $v_1, v_2, \ldots, v_k$ are linearly independent, then
- $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k \neq 0$

EX. The vectors (1 0 1 1 0), (0 1 0 0 1), and (1 1 1 1 1) are linearly dependent since
1.(1 0 1 1 0) + 1.(0 1 0 0 1) + 1.(1 1 1 1 1) = (0 0 0 0 0) However, (1 0 1 1 0), (0 1 0 0 1), and (1 1 1 1 1) are linearly independent.

- A set of vectors is said to span a vector space V if every vector in V is a linear combination of the vectors in the set.

- A set of vectors is said to span a vector space V if every vector in V is a linear combination of the vectors in the set.
- In any vector space or subspace there exits at least one set B of linearly independent vectors which span the space.

- A set of vectors is said to span a vector space V if every vector in V is a linear combination of the vectors in the set.
- In any vector space or subspace there exits at least one set B of linearly independent vectors which span the space.
- This set is called a basis (or base) of the vector space.

- A set of vectors is said to span a vector space V if every vector in V is a linear combination of the vectors in the set.
- In any vector space or subspace there exits at least one set B of linearly independent vectors which span the space.
- This set is called a basis (or base) of the vector space.
- The number of vectors in a basis of a vector space is called the dimension of the vector space. (Note that the number of vectors in any two bases are the same.)

- A set of vectors is said to span a vector space V if every vector in V is a linear combination of the vectors in the set.
- In any vector space or subspace there exits at least one set B of linearly independent vectors which span the space.
- This set is called a basis (or base) of the vector space.
- The number of vectors in a basis of a vector space is called the dimension of the vector space. (Note that the number of vectors in any two bases are the same.)

$$0.(10110)+0.(01001)+0.(11011)=(00000)$$
$$0.(10110)+0.(01001)+1.(11011)=(11011)$$
$$0.(10110)+1.(01001)+0.(11011)=(01001)$$
$$0.(10110)+1.(01001)+1.(11011)=(10010)$$
$$1.(10110)+0.(01001)+0.(11011)=(10110)$$
$$1.(10110)+0.(01001)+1.(11011)=(01101)$$
$$1.(10110)+1.(01001)+0.(11011)=(11111)$$
$$1.(10110)+1.(01001)+1.(11011)=(00100)$$

- Consider the vector space V_5 of 5 tuples over GF(2) given. The following eight vectors form a three dimensional subspace S of V_5

- Consider the vector space V_5 of 5 tuples over GF(2) given. The following eight vectors form a three dimensional subspace S of V_5
- (00000), (11100),(01010),(10001),

- Consider the vector space V_5 of 5 tuples over GF(2) given. The following eight vectors form a three dimensional subspace S of V_5
- (00000), (11100),(01010),(10001),
- (10110),(01101),(11011),(00111)
- The null space S_d of S consists of the following four vectors

- Consider the vector space V_5 of 5 tuples over GF(2) given. The following eight vectors form a three dimensional subspace S of V_5
- (00000), (11100),(01010),(10001),
- (10110),(01101),(11011),(00111)
- The null space S_d of S consists of the following four vectors
- (00000),(10101),(01110),(11011)

- Consider the vector space V_5 of 5 tuples over GF(2) given. The following eight vectors form a three dimensional subspace S of V_5
- (00000), (11100),(01010),(10001),
- (10110),(01101),(11011),(00111)
- The null space S_d of S consists of the following four vectors
- (00000),(10101),(01110),(11011)
- is spanned by (10101) and (01110) which are linearly independent. Thus the dimension of S_d is 2

- Consider the vector space of all n-tuples over GF(2). Let us form the following n n-tuples: $e_0 = (1000\ldots00)$
  $e_1 = (0100\ldots00)$
  $\vdots$
  $e_{n-1} = (0000\ldots01)$
- where the n-tuple ei has only nonzero component at ith position.
- Then every n-tuple $(a_0, a_1, \ldots, an-1)$ in $V-n$ can be expressed as a linear combination of $e_0, e_1 \ldots, en-1$ as follows:
  $(a_0, a_1 \ldots, an-1) = (a_0e_0 + a_1e_1 + \ldots, +an-1en-1)$
- Therefore, $e_0, e_1, \ldots, e_{n-1}$ span the vector space of all n-tuples over GF(2). We also see that $e_0, e_1, \ldots, e_{n-1}$ linearly independent.

- Let $u = (u_0, u_1, \ldots, u_{n-1})$ and $v = (v_0, v_1, \ldots, v_{n-1})$ be two n-tuples in V_n).
- We define the inner product (or dot product) of u and v as $u.v = (u_0.v_0, u_1.v_1, \ldots, u_{n-1}.v_{n-1})$ where $u_i.v_i$ and $u_i.v_i + u_{i+1}.v_{i+1}$ are carried out in modulo-2 multiplication and addition.
- Hence the inner product $u.v$ is a scalar in GF(2). If $u.v = 0$, u and v are said to be orthogonal to each other.
- The inner product has the following properties :
    - i $u.v = v.u$
    - ii $u.(v + w) = u.v + u.w$
    - iii $(au).v = a(u.v)$

- Let S be a k-dimension subspace of V_n and let S_d be the set of vectors in such that, for any u in S and v in S_d, $u.v = 0$. The set S_d contains at least the all-zero n-tuple $0 = (0, 0, \ldots, 0)$, since for any u in S, $0.u = 0$. Thus, S_d is nonempty. For any element a in GF(2) and any v in S_d,
$$a.v = \begin{cases} 0 & \text{if} \quad \mathrm{a} = 0 \\ 1 & \text{if} \quad \mathrm{a} = 1 \end{cases}$$
- Therefore, a.v is also in S_d . Let v and w be any two vectors in S_d. For any vector u in S, $u.(v + w) = u.v + u.w = 0 + 0 = 0$.
- This says that if v and w are orthogonal to u, the vector sum v + w is also orthogonal to u.
- Consequently, v + w is a vector in Sd. It follows from Theorem 2.18 that Sd is also a subspace of . This subspace is called the null (or dual) space of S. Conversely, S is also the null space of S_d.

Matrices

- A matrix $k \times n$ over GF(2) is a rectangular array with k rows and n columns

$$\begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_0 n-1 \\ g_{10} & g_{11} & g_{12} & \cdots & g_1 n-1 \\ \vdots & & & & \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

where each entry $g_{i,j}$ with $0 \leq i \leq k$ and $0 \leq i \leq n$ is an element from the binary i indicates the row and j indicates the column.

- Each row of G is an n-tuple over GF(2) and each column is k-tuple over GF(2).
- The matrix G can also be represented by its k rows as follows

$$G = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix}$$

- If the $k(k \leq n)$ rows of G are linearly independent then the 2^k linear combinations of these rows form a k-dimensional subspace of the vector space V_n of all the n-tuples over.
- This subpace is called the row space over G. Interchange rows of G or add one row to another. These are called elementary row operations.
- Consider a 3x6 matrix G over GF(2)

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Adding the third tow to the first row and interchanging the second and third rows

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$H = \begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{k-1} \end{bmatrix} = \begin{bmatrix} h_{00} & h_{01} & h_{02} & \dots & h_0 n-1 \\ h_{10} & h_{11} & h_{12} & \dots & h_1 n-1 \\ \vdots & & & & \\ h_{k-1,0} & h_{k-1,1} & h_{k-1,2} & \dots & h_{k-1,n-1} \end{bmatrix}$$

Consider the following 3x6 matrix over

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

The row space of this matrix is the null space

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Two matrices can be added if they have the same number of rows and the same number of columns. To add two kxn $A = [a_{ij}]$ and $B = [b_{ij}]$ two matrices we simply add their corresponding entries a_{ij} and b_{ij}

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}]$$

Thank You

References

S. Lin and J. Daniel J. Costello, *Error Control Coding*, 2nd ed. Pearson/Prentice Hall, 2004.