CS 4450

Coding and Information Theory

Mathematical Fundamentals (A)

Dr. Xuejun Liang

1

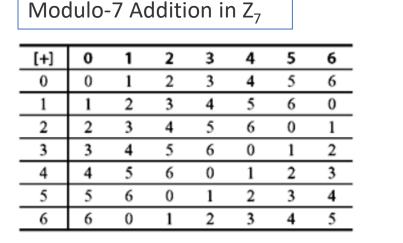
Mathematical Fundamentals

- 1. Modular Arithmetic
- 2. Group and Examples
- 3. Field and Examples
- 4. Extension Field
- 5. Linear (Vector) Space
- 6. Matrix and Groups of Linear Equations

Modular Arithmetic

Definition 1: Suppose *a* and *b* are integers, and *m* is positive integer. Then we write $a \equiv b \pmod{m}$ if *m* divides *b*-*a*.

- $a \equiv b \mod m$ if and only if $(a-b) = k \times m$ for some k
- Z_m the equivalence class under mod m
- Canonical form $Z_m = \{0, 1, 2, ..., m-1\}$, we use the positive remainder as the standard representation.
- -a mod m = m (a mod m)



 $5 + 13 \equiv 5 + 1 \equiv 6 \mod 12$

 $5 \times 13 \equiv 5 \times 1 \equiv 5 \mod 12$

Group

Definition 2: A set *G* on which a binary operation * is defined is called a *group* if the following conditions are satisfied:

- 1. The binary operation * is associative.
- 2. G contains an element *e*, called an *identity element* on *G*, such that, for any *a* in *G*

$$a * e = e^* a = a$$

3. For any element a in G, there exists another element a', called an inverse of a in G, such that

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

a * b = b * a

Two important properties of groups:

- 1. The inverse of a group element is unique.
- 2. The identity element in a group *G* is unique.

Group examples

• (Z₂, +, 0) is a group

• (Z₇, +, 0) is a group

[+]	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

Order of Group: The number of elements in a group is known as the order of the group

- (Z_m, +, 0) is a group
 - + is closed
 - Associative: (a + b) + c = a + (b + c)
 - Commutative: a + b = b + a (abelian group)
 - 0 is the identity for +: a + 0 = a + 0 = a
 - Additive inverse: (-a) + a = a + (-a) = 0

Group examples

Let p be a prime (e.g., p = 2, 3, 5, 7, 11, 13, 17, ...). Then (Zp-{0}, ×, 1) = ({1, 2, ..., p-1}, ×, 1) is a multiplicative (modulo-p) group.

Proof: Let $a \in Z_p$ -{0}, Since a < p and p is a prime, a and p must be relatively prime. By Euclidean theorem, there exist two integers i and j such that

$$i \cdot a + j \cdot p = 1$$
 \longrightarrow $i \cdot a = -j \cdot p + 1 = 1 \pmod{p}$ $a^{-1} = i \pmod{p}$

• (Z₇-{0}, ×, 1) is a group

[•]	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Field

- A set *F* is a Field
 - At least two elements 0, $1 \in F$
 - Two operations + and × on F
 - Associative and commutative
 - Operation × distributes over +
 - 0 is the identity for + and 1 for \times
 - Additive inverse and multiplicative inverse

Order of Field: The number of elements in a field is known as the *order* of the field. A field having finite number of elements is called a *finite field*.

Property 1: For every element *a* in a field, $a \times 0 = 0 \times a = 0$.

Property 2: For any two nonzero elements *a* and *b* in a field, $a \times b \neq 0$.

Property 3: For $a \neq 0$, $a \times b = a \times c$ implies that b = c.

Finite Field Examples

(Z₇, +, ×, 0, 1) is a Field

Example: Evaluate $((2 - 4) \times 4)/3$ in the field Z_7

[+]	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

[•]	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

- $(Z_p, +, \times, 0, 1)$ is a Field (when p is a prime number.)
 - +, × are closed
 - +, × are associative and commutative
 - Operation × distributes over +
 - 0 is the identity for + and 1 for ×
 - Additive inverse and multiplicative inverse