Algebraic Structures

Dr. E.SURESH BABU

Assistant Professor

Computer Science and Engineering Department

National Institute of Technology, Warangal

Warangal

Algebraic Structures

Why Study Finite Fields?

- It is almost impossible to fully understand practically any feature of modern cryptography and several important aspects of general computer security

  ✓ if you do not know what is meant by a **Finite Field.**

Why Study Finite Fields?

❖ Without understanding the notion of a finite field,

- ✓ You will NOT be able to **understand AES**
- ✓ You will NOT be able to understand the **derivation of the RSA algorithm** for public-key cryptography.
- ✓ You will not be able to **understand the workings of several modern protocols** (like the SSH protocol)

Why Study Finite Fields?

- You will never understand the **up coming ECC algorithm.**
- **Finally,** if you do **not understand the concepts then** you might as **well give up on learning** computer and network security.

The starting point for learning finite fields is the concept of a group. That's where we begin in the next section.

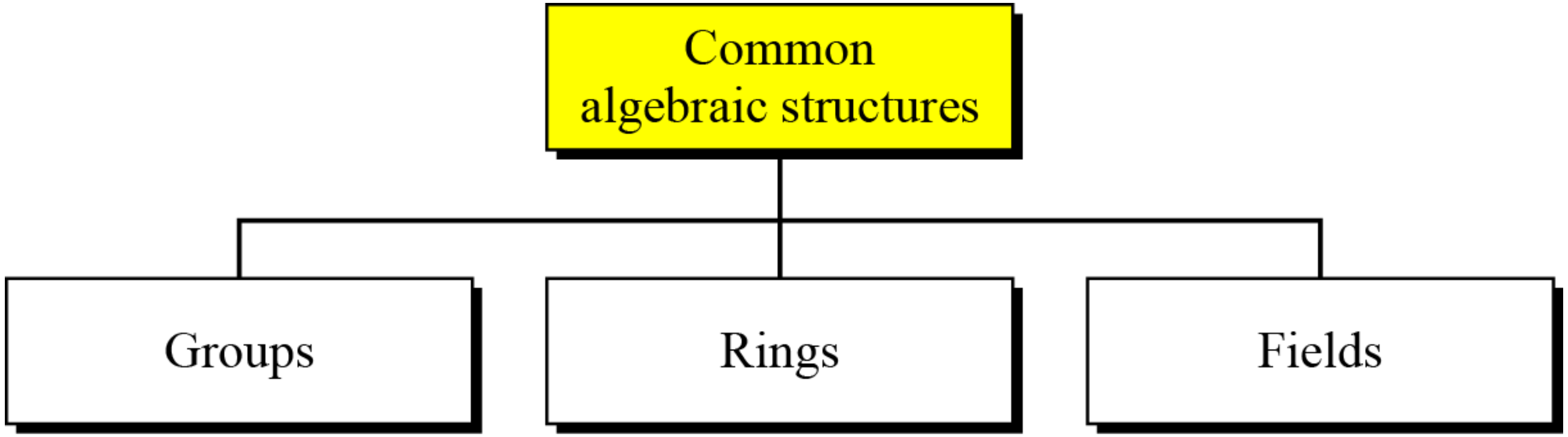
Algebraic Structures

- Cryptography requires **sets of integers** and **specific operations** that are defined for those sets.
- The combination of the **set and the operations** that are applied to the **elements of the set** is called an **Algebraic Structure**.

Algebraic Structures

- We will define **Three Common Algebraic Structures**:

1. **Groups,**
2. **Rings, and**
3. **Fields.**



Groups

Groups

- A **Group (G)** is a **set of elements with a binary operation** (•) that satisfies **four properties.**
  - ✓ **Closure**
  - ✓ **Associativity**
  - ✓ **Existence of identity**
  - ✓ **Existence of inverse**

Operations on Group

- If the operation is addition, we may refer to the group as an additive group or a group under addition.
  - ✓ Additive groups are normally **abelian(Supports Commutative).**
- If the operation is multiplication, we may refer to the group as a multiplicative group or a group under multiplication.
- We typically write G as **(G,+) and (G,X)**

Operations on Group

❖ The algebraic group properties of the combinations can be summarized as in the following table

	Addition	Multiplication
Closure	$a+b$ is an integer	$a*b$ is an integer
Associativity	$a+(b+c) = (a+b)+c$	$a*(b*c) = (a*b)*c$
Existence of an identity element	$a+0 = a$	$a*1 = a$
Existence of inverse elements	$a+(-a) = 0$	Only 1 and -1 have inverses: 1*1 = 1, -1*(-1) = 1
Commutativity	$a+b = b+a$	$a*b = b*a$

Operations on Group

❖ The operations are addition modulo n and Multiplication modulo n.

	Addition modulo n	**Multiplication modulo n**
Closure	$a+b \equiv c \bmod n,\ 0 \le c \le n-1$	$a*b \equiv c \bmod n,\ 0 \le c \le n-1$
Associativity	$a+(b+c) \equiv (a+b)+c \ mod\ n$	$a*(b*c) \equiv (a*b)*c \ mod\ n$
Existence of an identity element	$a+0 \equiv a \ mod\ n$	$a*1 \equiv a \ mod\ n$
Existence of inverse elements	$a+(n-a) \equiv 0 \ mod\ n$	a has the inverse only when a is coprime to n
Commutativity	$a+b \equiv b+a \ mod\ n$	$a*b \equiv b*a \ mod\ n$

Additive Group

- ❖ Consider the set **Z_5 = { 0, 1, 2, 3, 4} of integers modulo 5.** This has the **group table for addition modulo 5 below:**

Multiplicative Group

- Consider the set $Z_6 = \{0, 1, 2, 3, 4, 5\}$, together with **multiplication modulo 6.**

Multiplicative Group

- Consider the set $\mathbf{Z_5} = \{0, 1, 2, 3, 4\}$, together with **multiplication modulo 5.**

Cyclic Group

Cyclic Groups

- A **Cyclic Group is a group** that is its **Own Cyclic Subgroup**.

$$\boxed{\{e, g, g^2, \ldots, g^{n-1}\}, \text{ where } g^n = e}$$

- The subgroup of group can be **generated** using the **power of an element** then such a subgroup is called the **Cyclic Subgroup.**

$$\boxed{a^n \to a \bullet a \bullet \ldots \bullet a \quad (n \text{ times})}$$

- Note : The Term Power is used here, to repeatedly applying the group operation to the element

Cyclic Groups Generator

- The exponentiation as **repeated application of operator**

$$a^{-3} = a.a.a$$

and the **Identity Element** can be :

$$a^{0} = e$$

Cyclic Groups Generator

- A **group is cyclic** if every element is a power of some fixed element

$$b = a^k$$

For some **'a' and every 'b' in group**

- **'a'** is said to be a **generator of the group**

Cyclic Groups Generator

- The **element** that generates the **Cyclic Subgroup** and which can **generate the group itself,** then such a **element** is called as **Group Generator**

- Note : The Cyclic Group can have Many **GENERATOR**

Order of a Group

- What is the **Order of a Group**
  - ✓ The order of the group is the cardinality of the group
  - ✓ In other words the number of elements in the group.

Order of a Group

❖ What is the order of an element in a group;

✓ The **order of an element a ∈ G** is the **smallest value t** such that

- $a^t \equiv a \circ a \circ \ldots (t \text{ times}) \ldots \circ a$ = group identity element
- where $\circ$ is the **group operator.**

Order of a Group

- What is the **purpose of notation Z^*_p**
  - In the given notation p is a prime p,
  - The set **$\{1, 2, 3, \cdots, p - 1\}$ constitutes a group** with the group operator being **modulo p multiplication.**

Order of a Group

- The group Z^*_p is merely a set of **p −1 integers (1 through p − 1.)**
  - ✓ Example : Z^*_7 contains only the **6 integers from 1 through 6**
- Z^*_p is also frequently referred to as a **multiplicative group of order p − 1** with **1 being the group identity element.**

Cyclic Groups

- When will be Z^*_p is in cyclic group
  - The group Z^*_p is a cyclic group if all the elements of **group Z^*_p** can be expressed as

    α^i mod p for all $i = 0, 1, 2, \cdots$ and for some element $\alpha \in Z^*_p$
  - The **group Z^*_p** is a cyclic group for certain values of p.

Cyclic Groups : Example

- For illustration, Z^*_7 is a cyclic group with **α = 3.** That is,
  - if you **compute 3^i mod 7** for all i = 0, 1, 2, · · ·

3^1 mod 7	=	$3^0 \times 3$	=	1×3	=	3	≡	3 mod		7
3^2 mod 7	=	$3^1 \times 3$	=	3×3	=	9	≡	2 mod		7
3^3 mod 7	=	$3^2 \times 3$	=	2×3	=	6	≡	6	mod	7
3^4 mod 7	=	$3^3 \times 3$	=	6×3	=	18	≡	4 mod		7
3^5 mod 7	=	$3^4 \times 3$	=	4×3	=	12	≡	5	mod	7
3^6 mod 7	=	$3^5 \times 3$	=	5×3	=	15	≡	1	mod	7

- you will get the **6 numbers {2,3,6,4,5,1}** in the multiplicative group Z^*_7

Another Example of Z^*_{17}

- if we use **2 as a generator element**, we get the cyclic **subgroup** **{1, 2, 4, 8, 16, 15, 13, 9}** whose **order is 8.**
- All of the elements in this subgroup are given by **2^i mod 17 for all i = 0, 1, 2, ……**

Cyclic Groups Generator : Addition

- The group **$G = \langle Z_6, + \rangle$ is a cyclic group** with **two generators**

$g = 1$ and $g = 5$.

Cyclic Groups Generator - Examples: Addition

- Let the **Group G = $<Z_6, +>$.** Then we can form **Four cyclic subgroups** They are

  $H_1 = < \{0\}, + >$

  $H_2 = < \{0, 2, 4\}, + >$

  $H_3 = < \{0, 3\}, + >$

  $H_4 = G.$

Examples: $H_1 = < \{0\}, + >$: Element = 0

$$\boxed{0^0 \bmod 6 = 0}$$

Stop : The Process will be repeated

Examples: $H_2 = G$. Element = '1'

$$1^0 \bmod 6 = 0$$
$$1^1 \bmod 6 = 1$$
$$1^2 \bmod 6 = (1 + 1) \bmod 6 = 2$$
$$1^3 \bmod 6 = (1 + 1 + 1) \bmod 6 = 3$$
$$1^4 \bmod 6 = (1 + 1 + 1 + 1) \bmod 6 = 4$$
$$1^5 \bmod 6 = (1 + 1 + 1 + 1 + 1) \bmod 6 = 5$$

1 is a Group Generator

Stop : The Process will be repeated

Examples: $H_3 = < \{0, 3\}, + >$, Element ='3'

$$3^0 \bmod 6 = 0$$
$$3^1 \bmod 6 = 3$$

Stop : The Process will be repeated

Examples: $H_4 = <\{0, 2, 4\}, + >$, Element ='2'

$$2^0 \bmod 6 = 0$$
$$2^1 \bmod 6 = 2$$
$$2^2 \bmod 6 = (2 + 2) \bmod 6 = 4$$

Stop : The Process will be repeated

Examples: $H_4 = <\{0, 2, 4\}, + >$; Element ='4'

$$4^0 \bmod 6 = 0$$
$$4^1 \bmod 6 = 4$$
$$4^2 \bmod 6 = (4 + 4) \bmod 6 = 2$$

Stop : The Process will be repeated

Note : This is not a New Group

Examples: $H_5 = G$; Element ='5'

$$5^0 \bmod 6 = 0$$
$$5^1 \bmod 6 = 5$$
$$5^2 \bmod 6 = 4$$
$$5^3 \bmod 6 = 3$$
$$5^4 \bmod 6 = 2$$
$$5^5 \bmod 6 = 1$$

5 is a Group Generator

Stop : The Process will be repeated

Note : This is not a New Group

Cyclic Groups Generator : Multiplications

❖ The group **G = <Z_{10}^{*}, ×> is a cyclic group** with **two generators**

g = 3 and g = 7.

Examples: Multiplication

- Let the **Group G = $<Z_{10^*}, \times>$.** Then we can form **Four elements 1,3,7, and 9.** The cyclic subgroups are

$$H_1 = < \{1\}, \times >$$

$$H_2 = < \{1, 9\}, \times >$$

$$H_3 = G.$$

Examples: H1 = < {1}, × > , Element = 1

$$1^0 \bmod 10 = 1$$

Stop : The Process will be repeated

Examples: Element = ‘3’

$$3^0 \bmod 10 = 1$$
$$3^1 \bmod 10 = 3$$
$$3^2 \bmod 10 = 9$$
$$3^3 \bmod 10 = 7$$

3 is a Group Generator

Stop : The Process will be repeated

Examples: Element ='7'

$$7^0 \bmod 10 = 1$$
$$7^1 \bmod 10 = 7$$
$$7^2 \bmod 10 = 9$$
$$7^3 \bmod 10 = 3$$

7 is a Group Generator

Stop : The Process will be repeated

Examples: Element ='9'

$$9^0 \bmod 10 = 1$$
$$9^1 \bmod 10 = 9$$

Stop : The Process will be repeated

Thank U