Mathematics of Cryptography-II

Algebraic Structures

Tophan Kumar Jena
Assistant Professor, Dept. of CSE
Silicon Institute of Technology

Algebraic Structures

- Concept of algebraic structures :

  Groups

  Rings

  Fields

- To emphasize on finite fields of type GF(p) and GF(2^n) that play significant role in modern block cipher.

Groups

- A group (G) is a set of elements with a binary operation ($\bullet$) that satisfies four properties (or axioms).
  - ❑ **Closure**
  - ❑ **Associativity**
  - ❑ **Existence of identity**
  - ❑ **Existence of inverse**
- A commutative (abelian) group satisfies an extra property, i.e.
  - ❑ **Commutativity**

Groups (Contd…)

Although a group involves a single operation, the properties imposed on the operation allow the use of a pair of operations as long as they are inverses of each other.

Example 1

The set Z_n with the addition operator(+), $G = < Z_n , +>$, is a commutative group.

Example 2

The set Z_n* with the multiplication operator(x), $G = <Z_n{}^*, x>$, is also an abelian group.

More on Groups

- **Finite Group :** A group is finite if it has a finite no. of elements
- **Order of a Group:** It is the no. of elements in a group.

Subgroup

A subset **H** of a group **G** is a subgroup of G if H itself is a group w.r.t the operation on G.

That means:

1. For *a* and *b* elements of H, ***c* = *a* o *b*** is also an element of H.
2. Both G and H should have the same identity element.
3. The inverse of an element ***a*** in H is also the inverse of the element in G.

What are the subgroups of the group $G = <Z_8, +>$?

The subgroups are: H1={0, 4} and

H2={0, 2, 4, 6}

Subgroup(*Contd…)*

Example

Is the group $H = <Z_{10}, +>$ a subgroup of the group $G = <Z_{12}, +>$?

The answer is no.

- Although H is a subset of G, the operations defined for these two groups are different.
- The operation in H is addition modulo 10; the operation in G is addition modulo 12.

Cyclic Group

- A group G is cyclic if every element of G can be generated by using an element $g \in G$ and applying the group operator repeatedly on it.
- So, g is called the generator of the group.
- We can represent $g^0=e$ as an identity element.
- We also represent $g^{-n} = (g')^n$, where g' is the inverse element of g within the group.
- So, we represent all the elements as follows:

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

Cyclic Group(*Contd…)*

Example

How many generators are there for the cyclic group $G=<Z_6,+>$?

The group $G = <Z_6, +>$ is a cyclic group with two generators, $g = 1$ and $g = 5$.

Example:

Check whether group $G=<Z_{10}*,x>$ and $G=<Z_{12}*,x>$ are cyclic groups? If yes find out their generators.

Z_n*, the multiplicative group modulo n, is cyclic if and only if n is 1 or 2 or 4 or p^k or $2*p^k$ for an odd prime number p and $k \geq 1$.

Ring

- A ring is a set ***R*** having two binary operations (+) and (.) satisfying the following **<u>three sets of axioms</u>**:
- ***R*** is an **abelian group** under **<u>addition.</u>** That means:
  - For a, b in R, $a + b$ also in R *(i.e., **<u>closure</u>** under +*
  - $(a + b) + c = a + (b + c)$ for all a, b, c in R (*i.e., + is **<u>associative</u>***)
  - $a + b = b + a$ for all a, b in R (*i.e., + is **<u>commutative</u>***)
  - There is an element 0 in R such that $a + 0 = a$ for all a in R (*i.e., 0 is the **<u>additive identity</u>***)
  - For each a in R there exists $-a$ in R such that $a + (-a) = 0$ (*i.e., $-a$ is the **<u>additive inverse</u>** of a*).

Ring (contd…)

- ***R*** *has following* properties under **multiplication**:
  - For a, b in R, $a \,.\, b$ also in R *(i.e.,* ***closure*** *under .)*
  - $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$ for all a, b, c in R (*i.e.*, ***associative*** *under .*)
  - ***distributive*** with respect to addition. That means:

    $a \,.\, (b + c) = (a \,.\, b) + (a \,.\, c)$ for all a, b, c in R (*left distributivity*)

    $(b + c) \,.\, a = (b \,.\, a) + (c \,.\, a)$ for all a, b, c in R (*right distributivity*)
- A ring ***R*** is said to be commutative if it satisfies the ***commutative*** property. ($a.b = b.a$ *for all* a, b *in* R)

Ring(*Contd…)*

Example

- The set **Z** of integers with two operations, addition and multiplication, is a commutative ring.
- The set **R** of real numbers with two operations, addition and multiplication, is also a commutative ring
- The set of all **square matrices** of a fixed size, with real elements, using the matrix addition and multiplication

Integral domain

- It is a commutative ring with two extra properties as follows:
  - There is an element 1 in **R** such that $a.1 = 1.a = a$ for all a in R (***Multiplicative identity***)
  - If a, b in R and $a.b = 0$, then either $a = 0$ or $b = 0$ (***No zero divisors***)

Field

- A field ***F*** denoted by **{*F*, +, .}** is a set of elements with two binary operations (+) and (.) often called addition and multiplication respectively satisfy the following axioms:
- F is an integral domain; that is, F satisfies axioms:
  - Closure w.r.t addition and multiplication
  - Associative w.r.t addition and multiplication
  - Commutative w.r.t. addition and multiplication
  - Additive identity and Additive inverse exist
  - Distributivity of multiplication over addition
  - multiplicative identity exists
  - No zero divisor
- and also Multiplicative inverse exists

Examples: **Field**

- The set of all real numbers under the operations of arithmetic addition and multiplication is a field.
- The set of all rational numbers under the operations of arithmetic addition and multiplication is a field.
- The set of all complex numbers under the operations of complex arithmetic addition and multiplication is a field.
- What about Z_n and Z_n^* ?
- What about Z_p and Z_p^* ?

Examples: **NOT a Field**

- The set of all integers under the operations of arithmetic addition and multiplication is NOT a field.
- The set of all even integers, positive, negative, and zero, under the operations arithmetic addition and multiplication is NOT a field.

Finite Fields

Galois showed that for a field to be finite, the number of elements should be p^n, where p is a prime and n is a positive integer.

Note

A Galois field, GF(p^n), is a finite field with p^n elements.

Field: GF(p)

- When $n = 1$, we have GF(p) field.
- This is also called a Prime field
- This field is consisting of the set $Z_p = \{0, 1, 2, \ldots, p-1\}$, having p elements.
- The binary operations + and . are defined over the set. Therefore, addition, subtraction, multiplication, and division can be performed in the set.
- Each element of the set other than 0 has a multiplicative inverse.

Field: GF(2)

Example

- A very common field in this category is GF(2)
- It can be denoted as GF(2)={0, 1} with two operations, addition(+) and multiplication(×)

GF(2)

{0, 1} + ×

+	0	1
0	0	1
1	1	0

Addition

×	0	1
0	0	0
1	0	1

Multiplication

a	0	1
−a	0	1

a	0	1
a^{-1}	—	1

Inverses

Field: GF(5)

Example

- We can define GF(5) on the set Z_5 (5 is a prime) with addition and multiplication operations as shown below.

GF(5)

$\{0, 1, 2, 3, 4\}$ $\boxed{+ \ \times}$

GF(2^n) FIELDS

- In cryptography, we often need to use four operations(addition, subtraction, multiplication, and division).
- In other words, we need to use fields.
- The finite field GF(2^n) is also called binary extension field and it has a set of 2^n elements.
- Each element in this set is an **n-bit words**.

Example

- Let us define a **GF(2^2)** field.
- The set has four **2-bit words**: {00, 01, 10, 11}.
- We can redefine addition and multiplication for this field in such a way that all properties of these operations are satisfied.

Addition

⊕	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Identity: 00

So, multiplication under GF(2^n) may need a division with a predefined irreducible polynomial to get the result as an n-bit word.

In GF(2^2), it is 111

Polynomials

A polynomial of degree $n - 1$ is an expression of the form

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0$$

where x^i is called the ith term and a_i is called coefficient of the ith term.

Continued

Example

Represent 8-bit word (10011001) by a *polynomial.*

8-bit word	1	0	0	1	1	0	0	1

Polynomial: $1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 0x^1 + 1x^0$

First simplification: $1x^7 + 1x^4 + 1x^3 + 1x^0$

Second simplification: $x^7 + x^4 + x^3 + 1$

Continued

Example

Find the bits of a 8bit word whose polynomial is given by: $x^5 + x^2 + x$

To find the 8-bit word related to the polynomial $x^5 + x^2 + x$, we first supply the omitted terms.

Since $n = 8$, it means the polynomial is of degree 7. The expanded polynomial is

$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0$$

This is related to the 8-bit word **00100110**.

GF(2^n) Fields

Note

Polynomials representing n-bit words use two fields: GF(2) and GF(2^n).

Modulus in GF(2^n) Fields

- For the sets of polynomials in GF(2^n), a group of polynomials of degree n is defined as the modulus.
- Such polynomials are referred to as irreducible polynomials.

List of irreducible polynomials

Degree	*Irreducible Polynomials*
1	$(x+1)$, (x)
2	(x^2+x+1)
3	(x^3+x^2+1), (x^3+x+1)
4	$(x^4+x^3+x^2+x+1)$, (x^4+x^3+1), (x^4+x+1)
5	(x^5+x^2+1), $(x^5+x^3+x^2+x+1)$, $(x^5+x^4+x^3+x+1)$, $(x^5+x^4+x^3+x^2+1)$, $(x^5+x^4+x^2+x+1)$

Addition and Subtraction in GF(2^n)

Note

Addition and subtraction operations on polynomials are the same operation.

Example

Perform $(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1)$ in $GF(2^8)$.

The symbol $\oplus$ denotes polynomial addition.

It is the Exclusive-OR operation.

$$
\begin{array}{ll}
0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 & \oplus \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 & \\
\hline
0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 & \rightarrow \quad x^5 + x^3 + x + 1
\end{array}
$$

Multiplication in GF(2^n)

1. The coefficient multiplication is done in GF(2).
2. Multiplying x^i by x^j results in x^{i+j}.
3. The multiplication may create terms with degree more than $n - 1$, which means the result needs to be reduced using a modulus (irreducible) polynomial.

Example

Find the result of $(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$.

1. Do the normal multiplication of polynomials
2. Then reduce the resulting higher degree polynomial by dividing the modulus and taking the remainder.

$$
\begin{aligned}
P_1 \otimes P_2 &= x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x) \\
&= x^{12} + x^9 + x^8 + x^7 + x^6 + x^9 + x^6 + x^5 + x^4 + x^3 + x^8 + x^5 + x^4 + x^3 + x^2 \\
&= (x^{12} + x^7 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x^5 + x^3 + x^2 + x + 1
\end{aligned}
$$

Continued

Polynomial division with coefficients in GF(2)

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\hline
x^8 + x^4 + x^3 + x + 1 & x^{12} + x^7 + x^2 \\
 & x^{12} + x^8 + x^7 + x^5 + x^4 \\
\cline{2-2}
 & x^8 + x^5 + x^4 + x^2 \\
 & x^8 + x^4 + x^3 + x + 1 \\
\cline{2-2}
\text{Remainder} & \boxed{x^5 + x^3 + x^2 + x + 1}
\end{array}
$$

Example

How many elements are there in GF(2^3)? Show the addition and multiplication tables for the irreducible polynomial ($x^3 + x^2 + 1$)

The GF(2^3) field has 8 elements.

Note that there are two irreducible polynomials for degree 3. The other one, ($x^3 + x + 1$), yields a totally different table for multiplication.

Addition table for GF(2^3)

$\oplus$	000 (0)	001 (1)	010 (x)	011 ($x+1$)	100 (x^2)	101 x^2+1	110 (x^2+x)	111 (x^2+x+1)
000 (0)	000 (0)	001 (1)	010 (x)	011 ($x+1$)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
001 (1)	001 (1)	000 (0)	011 ($x+1$)	010 (x^2)	101 (x^2+1)	100 (x^2+x)	111 (x^2+x+1)	110 (x^2+x)
010 (x)	010 (x)	011 ($x+1$)	000 (0)	001 (1)	110 (x^2+x)	111 (x^2+x+1)	100 (x^2+x)	101 (x^2+1)
011 ($x+1$)	011 ($x+1$)	010 (x)	001 (1)	000 (0)	111 (x^2+x+1)	110 (x^2+x)	101 (x^2+1)	100 (x^2)
100 (x^2)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)	000 (0)	001 (1)	010 (x)	011 ($x+1$)
101 (x^2+1)	101 (x^2+1)	100 (x^2)	111 (x^2+x+1)	110 (x^2+x)	001 (1)	000 (0)	011 ($x+1$)	010 (x)
110 (x^2+x)	110 (x^2+x)	111 (x^2+x+1)	100 (x^2)	101 (x^2+1)	010 (x)	011 ($x+1$)	000 (0)	001 (1)
111 (x^2+x+1)	111 (x^2+x+1)	110 (x^2+x)	101 (x^2+1)	100 (x^2)	011 ($x+1$)	010 (x)	001 (1)	000 (0)

Multiplication table for $GF(2^3)$

$\otimes$	000 $(\mathbf{0})$	001 $(\mathbf{1})$	010 $(\mathbf{x})$	011 $(\mathbf{x+1})$	100 $(\mathbf{x^2})$	101 $(\mathbf{x^2+1})$	110 $(\mathbf{x^2+x})$	111 $(\mathbf{x^2+x+1})$
000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)
001 (1)	000 (0)	001 (1)	010 (x)	011 $(x+1)$	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
010 (x)	000 (0)	010 (x)	100 (x)	110 (x^2+x)	101 (x^2+1)	111 (x^2+x+1)	001 (1)	011 $(x+1)$
011 $(x+1)$	000 (0)	011 $(x+1)$	110 (x^2+x)	101 (x^2+1)	001 (1)	010 (x)	111 (x^2+x+1)	100 (x)
100 (x^2)	000 (0)	100 (x^2)	101 (x^2+1)	001 (1)	111 (x^2+x+1)	011 $(x+1)$	010 (x)	110 (x^2+x)
101 (x^2+1)	000 (0)	101 (x^2+1)	111 (x^2+x+1)	010 (x)	011 $(x+1)$	110 (x^2+x)	100 (x^2)	001 (1)
110 (x^2+x)	000 (0)	110 (x^2+x)	001 (1)	111 (x^2+x+1)	010 (x)	100 (x^2)	011 $(x+1)$	101 (x^2+1)
111 (x^2+x+1)	000 (0)	111 (x^2+x+1)	011 $(x+1)$	100 (x^2)	110 (x^2+x)	001 (1)	101 (x^2+1)	010 (x)

Finding inverse in GF(2^n) Field

Example

In GF (2^4), find the inverse of ($x^2 + 1$) modulo ($x^4 + x + 1$).

The answer is ($x^3 + x + 1$) as shown in following Table after applying Extended Euclidean algorithm (EEA).

q	r_1	r_2	r	t_1	t_2	t
$(x^2 + 1)$	$(x^4 + x + 1)$	$(x^2 + 1)$	(x)	(0)	(1)	$(x^2 + 1)$
(x)	$(x^2 + 1)$	(x)	(1)	(1)	$(x^2 + 1)$	$(x^3 + x + 1)$
(x)	(x)	(1)	(0)	$(x^2 + 1)$	$(x^3 + x + 1)$	(0)
	(1)	(0)		$(x^3 + x + 1)$	(0)	

Using a Generator

Sometimes it is easier to define the elements of the GF(2^n) field using a generator.

$$\boxed{\{0, 1, g, g^2, \ldots, g^N\}, \text{ where } N = 2^n - 2}$$

Example

Generate the elements of the field $GF(2^4)$ using the irreducible polynomial $f(x) = x^4 + x + 1$.

The elements 0, g^0, g^1, g^2, and g^3 can be easily generated, because they are the 4-bit representations of 0, 1, x^1, x^2, and x^3.

Elements g^4 through g^{14}, which represent x^4 though x^{14} need to be divided by the irreducible polynomial.

To avoid the polynomial division, we can take, $f(g)=0$

Then we get, $g^4 + g + 1 = 0 \Rightarrow g^4 = g + 1$

Generating all the elements of GF(2^4)

$$
\begin{array}{lclclclcclcl}
0 & = & 0 & = & 0 & = & 0 & \longrightarrow & 0 & = & (0000) \\
g^0 & = & g^0 & = & g^0 & = & g^0 & \longrightarrow & g^0 & = & (0001) \\
g^1 & = & g^1 & = & g^1 & = & g^1 & \longrightarrow & g^1 & = & (0010) \\
g^2 & = & g^2 & = & g^2 & = & g^2 & \longrightarrow & g^2 & = & (0100) \\
g^3 & = & g^3 & = & g^3 & = & g^3 & \longrightarrow & g^3 & = & (1000) \\
g^4 & = & g^4 & = & g^4 & = & g+1 & \longrightarrow & g^4 & = & (0011) \\
g^5 & = & g\,(g^4) & = & g\,(g+1) & = & g^2+g & \longrightarrow & g^5 & = & (0110) \\
g^6 & = & g\,(g^5) & = & g\,(g^2+g) & = & g^3+g^2 & \longrightarrow & g^6 & = & (1100) \\
g^7 & = & g\,(g^6) & = & g\,(g^3+g) & = & g^3+g+1 & \longrightarrow & g^7 & = & (1011) \\
g^8 & = & g\,(g^7) & = & g\,(g^3+g+1) & = & g^2+1 & \longrightarrow & g^8 & = & (0101) \\
g^9 & = & g\,(g^8) & = & g\,(g^2+1) & = & g^3+g & \longrightarrow & g^9 & = & (1010) \\
g^{10} & = & g\,(g^9) & = & g\,(g^3+g) & = & g^2+g+1 & \longrightarrow & g^{10} & = & (0111) \\
g^{11} & = & g\,(g^{10}) & = & g\,(g^2+g+1) & = & g^3+g^2+g & \longrightarrow & g^{11} & = & (1110) \\
g^{12} & = & g\,(g^{11}) & = & g\,(g^3+g^2+g) & = & g^3+g^2+g+1 & \longrightarrow & g^{12} & = & (1111) \\
g^{13} & = & g\,(g^{12}) & = & g\,(g^3+g^2+g+1) & = & g^3+g^2+1 & \longrightarrow & g^{13} & = & (1101) \\
g^{14} & = & g\,(g^{13}) & = & g\,(g^3+g^2+1) & = & g^3+1 & \longrightarrow & g^{14} & = & (1001)
\end{array}
$$

Example

Compute the following under the field GF(2^4) :

a. $g^3 + g^{12} + g^7$

b. $g^3 - g^6$

a. $g^3 + g^{12} + g^7 = g^3 + (g^3 + g^2 + g + 1) + (g^3 + g + 1) = g^3 + g^2 \rightarrow (1100)$

b. $g^3 - g^6 = g^3 + g^6 = g^3 + (g^3 + g^2) = g^2 \rightarrow (0100)$

Example

Compute the following under the field GF(2^4) :

a. g^9 x g^{11}

b. g^3 / g^8

a. $g^9 \times g^{11} = g^{20} = g^{20 \bmod 15} = g^5 = g^2 + g \rightarrow (0110)$

b. $g^3 / g^8 = g^3 \times g^7 = g^{10} = g^2 + g + 1 \rightarrow (0111)$

Note: For multiplication of two elements in the field, use the equality $\mathbf{g^k = g^{k \bmod (2^n-1)}}$ for any integer k.