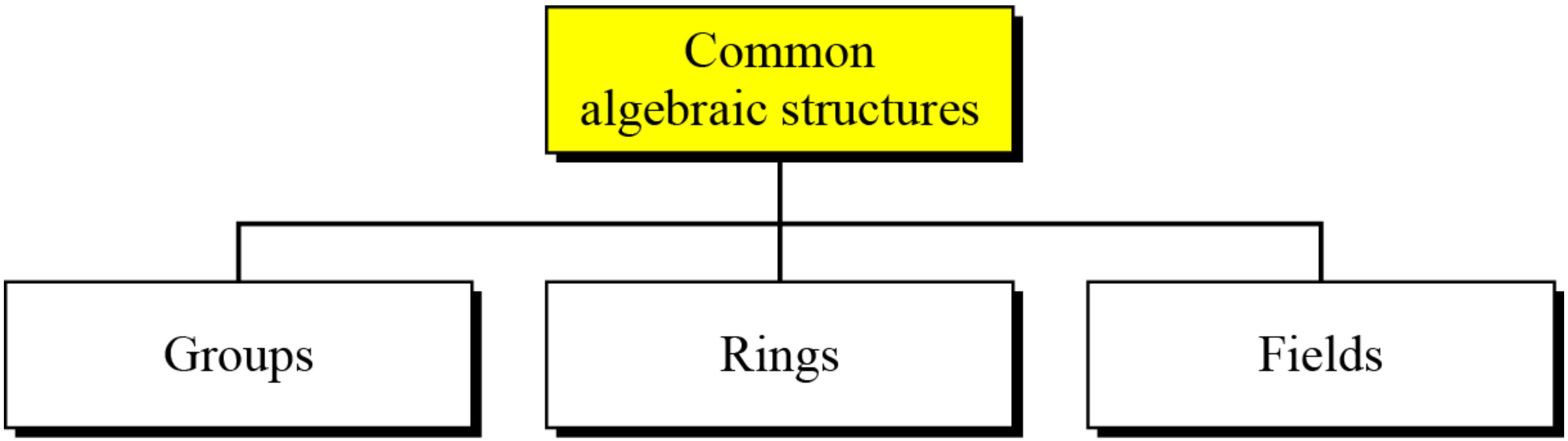
ALGEBRAIC STRUCTURES

Introduction

- Some sets of numbers, such as Z, Z_n, Z_n^*, Z_p, Z_p^*
- 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.

Introduction



Common algebraic structure

Group

- A group (G) is a set of elements with a binary operation (•) that satisfies four properties (or axioms).

- A commutative group satisfies an extra property, commutativity:

- Closure
- Associativity
- Commutativity
- Existence of identity
- Existence of inverse

Group

- Closure
  - If a and b are elements of G, then c = a•b is also an element of G.
- Associativity
  - If a, b and c are elements of G, then
    (a•b)•c=a•(b•c)
- Existence of identity
  - For all a in G, there exist an element e, called the identity element, such that e•a=a•e=a
- Existence of inverse
  - For each a in G, there exists an element a’, called the inverse of a, such that a•a’=a’•a=e

Group

- A Commutative group (Abelian group) is group in which the operator satisfies four properties plus an extra property that is commutativity.
  - For all a and b in G, we have $a \bullet b = b \bullet a$

Group

- Example:
- The set of residue integers with the addition operator,

$$G = < Z_n , +>,$$

- is a commutative group. We can perform addition and subtraction on the elements of this set without moving out of the set.

Group

- Application
  - Although a group involves a single operation, the properties imposed on the operation allow the use of a pair of operations!!!!

Group

- The set Z_n^* with the multiplication operator, $G = <Z_n^*, \times>$, is also an abelian group.

Group

- Finite Group
- Order of a Group
- Subgroups

Group

- Finite Group:
  - If the set has a finite number of elements; otherwise, it is an infinite group.

- Order of a Group $|G|$
  - The number of elements in the group.
  - If the group is finite, its order is finite

- Subgroups
  - A subset H of a group G is a subgroup of G if H itself is a group with respect to the operation on G

SubGroup

- Subgroups(cont.)
  - If G=<S, •> is a group, H=<T, •> is a group under the same operation, and T is a nonempty subset of S, then H is a subgroup of G
  - If a and b are members of both groups, then c=a•b is also member of both groups
  - The group share the same identity element
  - If a is a member of both groups, the inverse of a is also a member of both groups
  - The group made of the identity element of G, H=<{e}, •>, is a subgroup of G
  - Each group is a subgroup of itself

SubGroup

- Find all subgroups of Group $G = \langle Z_6, + \rangle$

SubGroup

- Find all subgroups of Group G = <Z_6, +>
- $Z_6 = \{0,1,2,3,4,5\}$ has subgroups
- {0}
- {0,3}
- {0,2,4}
- {0,1,2,3,4,5}
- {0,1,5} -> valid subgroup?

SubGroup

- Find all subgroups of Group $G = <Z_{10*}, X>$

SubGroup

- Find all subgroups of Group G = <Z_{10*}, X>
- Z_{10*} = {1,3,7,9} has subgroups
- {1}
- {1,9}
- {1,3,7,9}

SubGroup

- Is the group H = $\langle Z_{10}, +\rangle$ a subgroup of the group G = $\langle Z_{12}, +\rangle$?

SubGroup

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

- Solution: 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 Subgroups

- If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic subgroup.

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

Cyclic Subgroups

- Four cyclic subgroups can be made from the group G = <Z6, +>.

- $H_1 = \langle \{0\}, + \rangle$,
- $H_2 = \langle \{0, 2, 4\}, + \rangle$,
- $H_3 = \langle \{0, 3\}, + \rangle$,
- $H_4 = G$.

Cyclic Subgroups

- Four cyclic subgroups can be made from the group G = <Z6, +>. They are H1 = <{0}, +>, H2 = <{0, 2, 4}, +>, H_3 = <{0, 3}, +>, and H4 = G.

$0^0 \bmod 6 = 0$

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

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

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

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

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

Cyclic Subgroups

- Find all cyclic subgroups from the group $G = \langle Z_{10}^*, \times \rangle$.

Cyclic Subgroups

- Find all cyclic subgroups from the group G = <Z10*, ×>.

- G has only four elements: 1, 3, 7, and 9. The cyclic subgroups are H1 = <{1}, ×>, H2 = <{1, 9}, ×>, and H3 = G.

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

$$\begin{aligned} 3^0 \bmod 10 &= 1 \\ 3^1 \bmod 10 &= 3 \\ 3^2 \bmod 10 &= 9 \\ 3^3 \bmod 10 &= 7 \end{aligned}$$

$$\begin{aligned} 7^0 \bmod 10 &= 1 \\ 7^1 \bmod 10 &= 7 \\ 7^2 \bmod 10 &= 9 \\ 7^3 \bmod 10 &= 3 \end{aligned}$$

$$\begin{aligned} 9^0 \bmod 10 &= 1 \\ 9^1 \bmod 10 &= 9 \end{aligned}$$

Cyclic Groups

- A cyclic group is a group that is its own cyclic subgroup.

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

Cyclic Groups

- Three cyclic subgroups can be made from the group $G = \langle Z_{10}*, \times \rangle$.
- G has only four elements: 1, 3, 7, and 9. The cyclic subgroups are $H_1 = \langle \{1\}, \times \rangle$, $H_2 = \langle \{1, 9\}, \times \rangle$, and $H_3 = G$.

- The group $G = \langle Z_6, + \rangle$ is a cyclic group with two generators, $g = 1$ and $g = 5$.

- The group $G = \langle Z_{10}*, \times \rangle$ is a cyclic group with two generators, $g = 3$ and $g = 7$.

Cyclic Groups

- Lagrange's Theorem
- Assume that G is a group, and H is a subgroup of G. If the order of G and H are $|G|$ and $|H|$, respectively, then, based on this theorem, $|H|$ divides $|G|$.

- Order of an Element
- The order of an element is the order of the cyclic group it generates.

Cyclic Groups

- In the group G = <Z6, +>, the orders of the elements are:
- ord(0) = 1,
- ord(1) = 6,
- ord(2) = 3,
- ord(3) = 2,
- ord(4) = 3,
- ord(5) = 6.

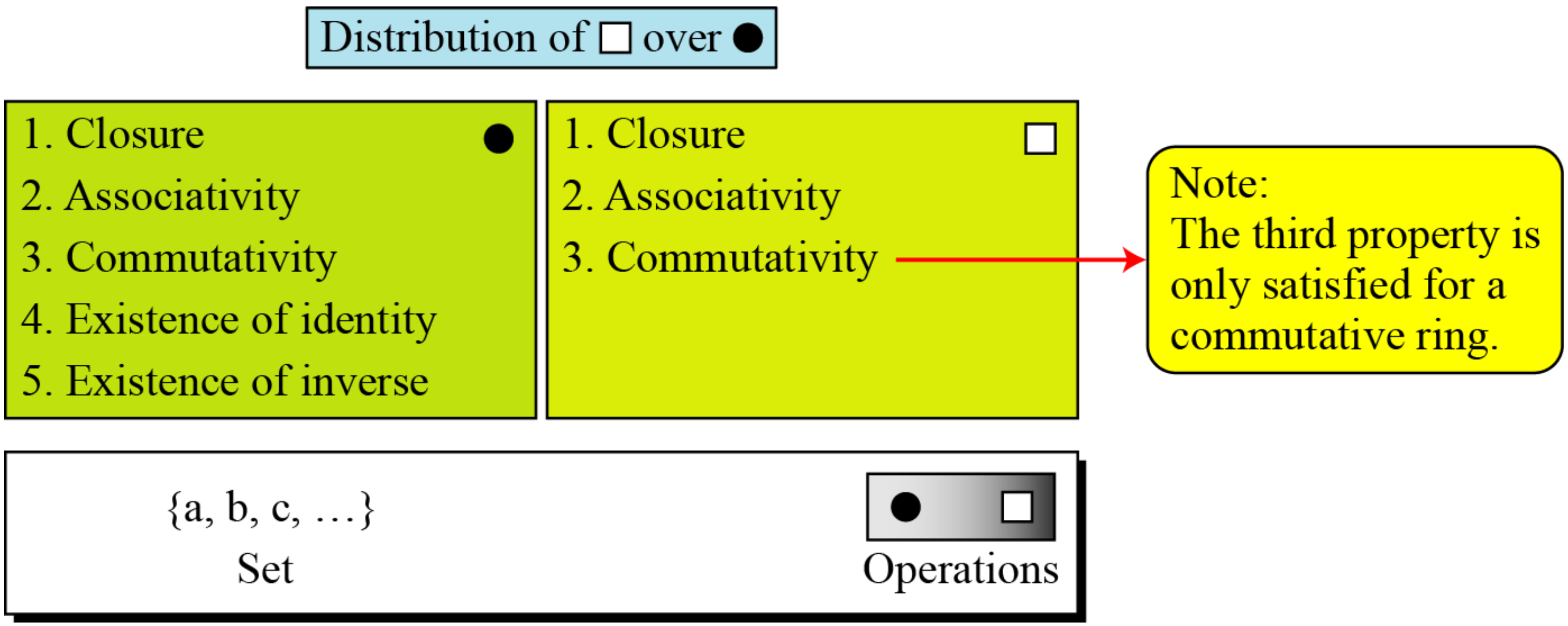
Cyclic Groups

- In the group $G = <Z_{10}^*, \times>$, the orders of the elements are:

  $ord(1) = 1$, $ord(3) = 4$, $ord(7) = 4$, $ord(9) = 2$.

Ring

- A ring, R = <{…}, •, >, is an algebraic structure with two operations.



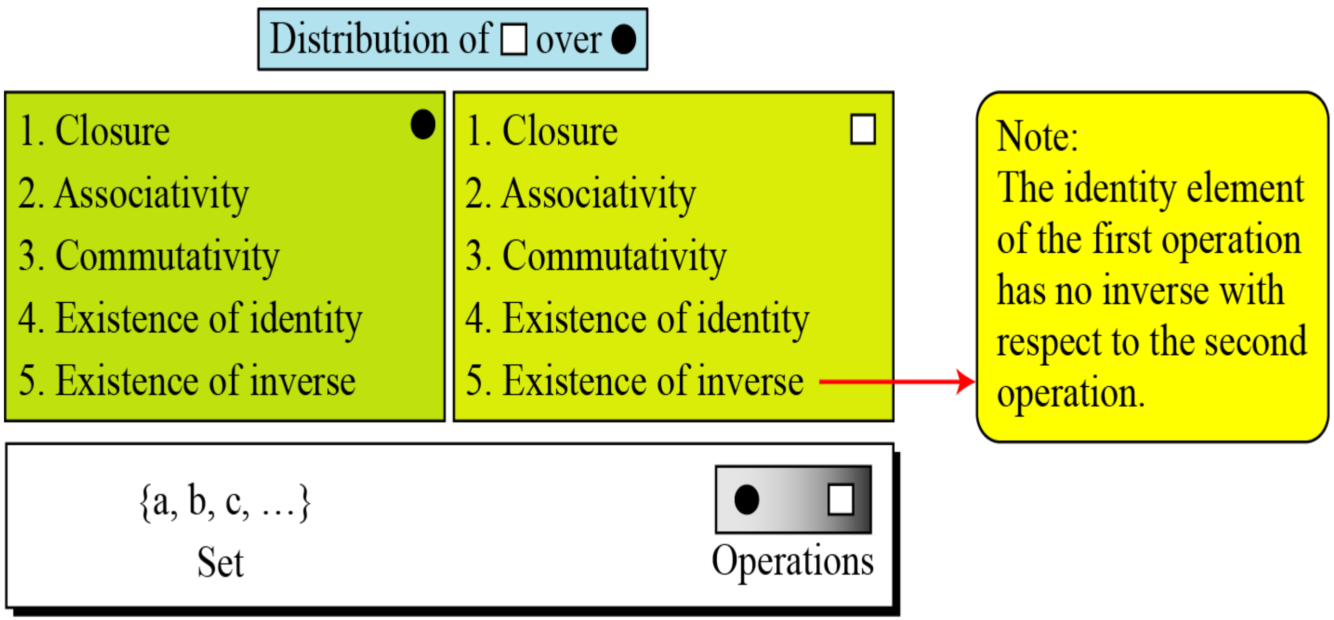
Ring

Ring

- The set Z with two operations, addition and multiplication, is a commutative ring.
- We show it by R = <Z, +, ×>. Addition satisfies all of the five properties; multiplication satisfies only three properties.

Field

- A field, denoted by F = <{…}, •, □ > is a commutative ring in which the second operation satisfies all five properties defined for the first operation except that the identity of the first operation has no inverse.



Field

Finite Field

- Finite Field: A field with a finite number of elements
- 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.

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

Finite Field

- When n = 1, we have GF(p) field.

- This field can be the set Z_p, {0, 1, …, p − 1}, with two arithmetic operations. Addition and multiplication

- In this set, each element has an additive inverse and that all nonzero elements have a multiplicative inverse (no multiplicative inverse for 0).

Finite Field

- A very common field in this category is GF(2) with the set {0, 1} and 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
$-a$	1	0

a	0	1
a^{-1}	—	1

Inverses

GF(2) field

Addition/Subtraction in GF(2) is the same as XOR operation;
Multiplication/division is the same as the AND Operation.

Finite Field

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

GF(5)

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

$+$	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

Addition

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication

Additive inverse

a	0	1	2	3	4
$-a$	0	4	3	2	1

a	0	1	2	3	4
a^{-1}	—	1	3	2	4

Multiplicative inverse

GF(5) field

Summary

Algebraic Structure	*Supported Typical Operations*	*Supported Typical Sets of Integers*
Group	(+ −) or (× ÷)	$\mathbf{Z}_n$ or $\mathbf{Z}_n{}^*$
Ring	(+ −) and (×)	$\mathbf{Z}$
Field	(+ −) and (× ÷)	$\mathbf{Z}_p$

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.
- However, when we work with computers, the positive integers are stored in the computers as n-bit words in which n is usually 8,16,32,64 and so on.
- Range of integers is 0 to $2^n - 1$
- Hence modulus is ???
  - 2^n
- What if we want to use field????

$GF(2^n)$ FIELDS

- Solution 1
  - Use $GF(p)$, with the set Z_p, where p is the largest prime number less than 2^n
  - But the problem ???
    - It is inefficient because we cannot use the integers from p to 2^n-1.
    - For example, if $n=4$, the largest prime less than $2^4(=16)$ is 13.
      - Means, we cannot use integers 13, 14, and 15.
    - If $n=8$, the largest prime less than 2^8 is 251.
      - Means, we cannot use 251, 252, 253, 254, and 255.

GF(2^n) FIELDS

- Solution 2
  - Use GF(2^n)
  - Use a set of 2^n words
  - The elements in this set are n-bit words
  - E.g. for n=3, the set is {000,001,010,011,100,101,110,111}

- Problem:
  - We cannot interpret each element as an integer between 0 to 7. because regular four operations cannot be applied
  - Modulus 2^n is not prime
  - Need to define operations on the set of elements in GF(2^n)

GF(2^n) FIELDS

- Let us define a GF(2^2) field in which 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

$\oplus$	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

Multiplication

$\otimes$	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Identity: 01

An example of GF(2^2) field

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 *i*th term.

Polynomials

- represent the 8-bit word (10011001) using a polynomials.

Polynomials

- we can represent the 8-bit word (10011001) using a polynomials.

n-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	$x^7 + x^4 + x^3 + 1$

Polynomials

- find the 8-bit word related to the polynomial $x^5 + x^2 + x$

Polynomials

- 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.

Polynomials

- Operations on polynomials
  - Actually involves two operations
  - Operation on coefficients and operation on polynomials
- Hence, need to define two fields
  - What for coefficient??
  - What for polynomials???
- GF(2) and GF(2^n) is the answer….

Polynomials

- Polynomial Addition

Addition and subtraction operations on polynomials are the same operation.

Polynomial Addition - Example

- Let us do $(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1)$ in $GF(2^8)$.
- We use the symbol $\oplus$ to show that we mean polynomial addition.

Polynomial Addition - Example

- Let us do $(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1)$ in $GF(2^8)$.
- We use the symbol $\oplus$ to show that we mean polynomial addition.
- The following shows the procedure:

$$
\begin{array}{l}
0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 \quad \oplus \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 \\
\text{---} \\
0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 \quad \rightarrow \quad x^5 + x^3 + x + 1
\end{array}
$$

Polynomial Addition - Example

- There is also another short cut.
- Because the addition in GF(2) means the exclusive-or (XOR) operation.
- So we can exclusive-or the two words, bits by bits, to get the result.
- In the previous example, $x^5 + x^2 + x$ is 00100110 and $x^3 + x^2 + 1$ is 00001101.
- The result is 00101011 or in polynomial notation $x^5 + x^3 + x + 1$.

Polynomials

- Modulus
  - 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.

Polynomials

- irreducible polynomials.
  - No polynomial in the set can divide this polynomial
  - Can not be factored into a polynomial with degree of less than n

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	$(x^5 + x^2 + 1), (x^5 + x^3 + x^2 + x + 1), (x^5 + x^4 + x^3 + x + 1),$ $(x^5 + x^4 + x^3 + x^2 + 1), (x^5 + x^4 + x^2 + x + 1)$

Exercise

- Prove that (x^2+x+1) is an irreducible polynomial of degree 2.

Exercise

- Prove that (x^2+x+1) is an irreducible polynomial of degree 2.
- Solution:
  - A polynomial f(x) of degree n is reducible if f(x) = g(x) × h(x), where g and h are two polynomials, each with the degree greater than zero and degree less than the highest degree of f(x) .
  - According to this definition we have **degree (f) = degree (g) + degree (h).**
  - Based on this, a reducible polynomial of degree 2 can be factored only as two polynomials of degree 1 (2 = 1 + 1).
  - In other words, a factors of a reducible polynomial of degree 2 can be only x or (x+ 1) (the only two polynomials of degree 1).

Exercise

- Prove that (x^2+x+1) is an irreducible polynomial of degree 2.
- Solution:

$$(x^2) = (x) \times (x) \quad \rightarrow \quad (x^2) \text{ is reducible}$$

$$(x^2 + 1) = (x + 1) \times (x + 1) \quad \rightarrow \quad (x^2 + 1) \text{ is reducible}$$

$$(x^2 + x) = (x) \times (x + 1) \quad \rightarrow \quad (x^2 + x) \text{ is reducible}$$

$$(x^2 + x + 1) \text{ cannot be factored.} \quad \rightarrow \quad (x^2 + x + 1) \text{ is irreducible}$$

Polynomial Multiplication

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

Polynomial Multiplication - 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 $(x^8 + x^4 + x^3 + x + 1)$.

Polynomial Multiplication - 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 $(x^8 + x^4 + x^3 + x + 1)$.
- Note that we use the symbol $\otimes$ to show the multiplication of two polynomials.

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

- To find the final result, divide the polynomial of degree 12 by the polynomial of degree 8 (the modulus) and keep only the remainder.

Polynomial Multiplication - Example

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

Polynomial division with coefficients in GF(2)

GF(2^n) FIELDS

- Let us define a GF(2^2) field in which 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

Multiplication

⊗	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Identity: 01

An example of GF(2^2) field

Inverse of Polynomial

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

Inverse of Polynomial

- In GF (2^4), find the inverse of $(x^2 + 1)$ modulo $(x^4 + x + 1)$.
- **Solution:**
  - The answer is - $(x^3 + x + 1)$.

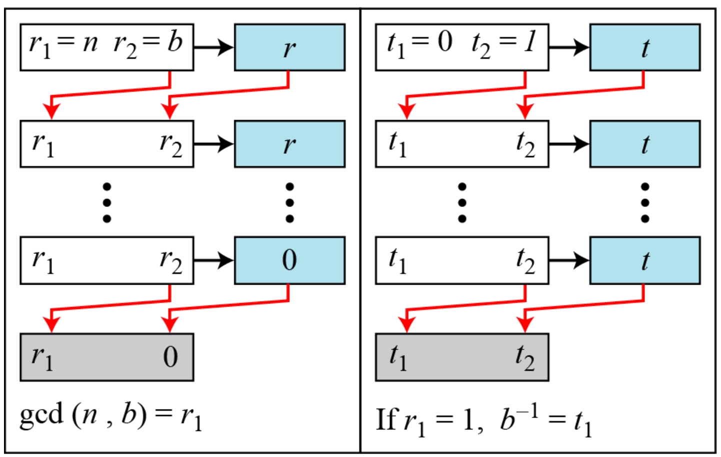
q	r_1	r_2	r	t_1	t_2	t
(x^2+1)	(x^4+x+1)	(x^2+1)	(x)	(0)	(1)	(x^2+1)
(x)	(x^2+1)	(x)	(1)	(1)	(x^2+1)	(x^3+x+1)
(x)	(x)	(1)	(0)	(x^2+1)	(x^3+x+1)	(0)
	(1)	(0)		(x^3+x+1)	(0)	

Euclidean algorithm

Inverse of Polynomial

- In $GF(2^8)$, find the inverse of (x^5) modulo $(x^8 + x^4 + x^3 + x + 1)$.

Multiplicative Inverse



a. Process

$r_1 \leftarrow n; \qquad r_2 \leftarrow b;$

$t_1 \leftarrow 0; \qquad t_2 \leftarrow 1;$

while $(r_2 > 0)$

{

$q \leftarrow r_1 \,/\, r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2; \qquad r_2 \leftarrow r;$

$t \leftarrow t_1 - q \times t_2;$

$t_1 \leftarrow t_2; \qquad t_2 \leftarrow t;$

}

if $(r_1 = 1)$ then $b^{-1} \leftarrow t_1$

b. Algorithm

Using extended Euclidean algorithm to find multiplicative inverse

Multiplicative Inverse

- Find the multiplicative inverse of 11 in Z_{26}.

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	−2
2	11	4	3	1	−2	5
1	4	3	1	−2	5	−7
3	3	1	0	5	−7	26
	1	0		−7	26	

The gcd (26, 11) is 1; the inverse of 11 is -7 or 19.

Inverse of Polynomial

- In GF(2^8), find the inverse of (x^5) modulo ($x^8 + x^4 + x^3 + x + 1$).
- Solution:
  - The answer is - ($x^5 + x^4 + x^3 + x$)

q	r_1	r_2	r	t_1	t_2	t
(x^3)	$(x^8+x^4+x^3+x+1)$	(x^5)	(x^4+x^3+x+1)	(0)	(1)	(x^3)
$(x+1)$	(x^5)	(x^4+x^3+x+1)	(x^3+x^2+1)	(1)	(x^3)	(x^4+x^3+1)
(x)	(x^4+x^3+x+1)	(x^3+x^2+1)	(1)	(x^3)	(x^4+x^3+1)	$(x^5+x^4+x^3+x)$
(x^3+x^2+1)	(x^3+x^2+1)	(1)	(0)	(x^4+x^3+1)	$(x^5+x^4+x^3+x)$	(0)
	(1)	(0)		$(x^5+x^4+x^3+x)$	(0)	

Euclidean algorithm

Polynomial Multiplication

- A better algorithm: Obtain the result by repeatedly multiplying a reduced polynomial by x.
- Find the result of multiplying $P_1 = (x^5 + x^2 + x)$ by $P_2 = (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$

Polynomial Multiplication

- Solution:

- We first find the partial result of multiplying x^0, x^1, x^2, x^3, x^4, and x^5 by P_2.
- Note that although only three terms are needed, the product of $x^m \otimes P_2$ for m from 0 to 5 because each calculation depends on the previous result.

Polynomial Multiplication

Powers	*Operation*	*New Result*	*Reduction*
$x^0 \otimes P_2$		$x^7 + x^4 + x^3 + x^2 + x$	No
$x^1 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x^5 + x^2 + x + 1$	**Yes**
$x^2 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x^2 + x + 1)$	$x^6 + x^3 + x^2 + x$	No
$x^3 \otimes P_2$	$\boldsymbol{x} \otimes (x^6 + x^3 + x^2 + x)$	$x^7 + x^4 + x^3 + x^2$	No
$x^4 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2)$	$x^5 + x + 1$	**Yes**
$x^5 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x + 1)$	$x^6 + x^2 + x$	No
$\mathbf{P_1} \times \mathbf{P_2} = (x^6 + x^2 + x) + (x^6 + x^3 + x^2 + x) + (x^5 + x^2 + x + 1) = \boldsymbol{x^5 + x^3 + x^2 + x + 1}$			

An efficient algorithm

Exercise

- Find the result of multiplying P1 = $(x^3 + x^2 + x + 1)$ by P2 = $(x^2 + 1)$ in GF(2^4) with irreducible polynomial $(x^4 + x^3 + 1)$

Exercise

- Which of the following is a valid Galois Field?
  - GF(12)
  - GF(13)
  - GF(16)
  - GF(17)

- For following n-bit words, find the polynomial that represent that word:
  - 10010
  - 00011
  - 100001

Exercise

- Find the n-bit word that is represented by each of the following polynomials:
  - X^2+1 in $GF(2^4)$
  - X^7 in $GF(2^8)$
  - $X+1$ in $GF(2^3)$

- In the field GF(7), find the result of
  - 5+3
  - 5-4
  - 5X3
  - 5/3

Exercise

- In the filed $GF(2^3)$, perform the following operation with irreducible polynomial (x^3+x^2+1).
  - (100)/(010)
  - (100)/(000)
  - (101)/(011)
  - (000)/(111)

Exercise

- In the filed GF(2^3), perform the following operation with irreducible polynomial (x^3+x^2+1).
  - (100)/(010)
    - Solution: (100)X$(010)^{-1}$ = (100)X(110) = (010)
  - (100)/(000)
    - Solution: operation is impossible because (000) has no inverse
  - (101)/(011)
  - (000)/(111)

Exercise

- Find the result of multiplying (10101) by (10000) in $GF(2^5)$ using $(x^5 + x^2 + 1)$ as modulus.