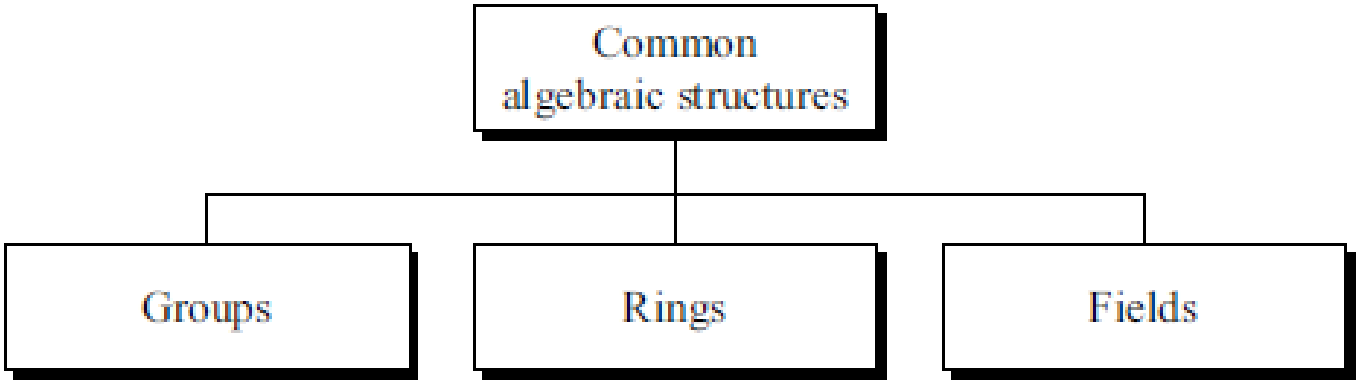
ALGEBRAIC STRUCTURES

- 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.
- three common algebraic structures: groups, rings, and fields



Group

- A group (G) is a set of elements with a binary operation "•" that satisfies four properties (or axioms). A commutative group, also called an abelian group, is a group in which the operator satisfies the four properties for groups plus an extra property, commutativity. The four properties for groups plus commutativity are defined as follows:
- **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).
- **Commutativity:** For all a and b in G, we have a • b = b • a. ---- to be satisfied only for a commutative group.
- **Existence of identity:** For all a in G, there exists 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.

- properties imposed on the operation allow the use of a pair of operations as long as they are inverses of each other.
- if the defined operation is addition, the group supports both addition and subtraction, because subtraction is addition using the additive inverse.
- This is also true for multiplication and division.
- However, a group can support only addition/subtraction or multiplication/division operations, but not the both at the same time.

Examples

- The set of residue integers with the addition operator, G = <Zn, + >, is a commutative group
- G = <Zn*, ×>,

Finite Group

- A group is called a finite group if the set has a finite number of elements; otherwise, it is an infinite group.
- **Order of a Group**
- The order of a group, |G|, is the number of elements in the group.
- If the group is not finite, its order is infinite; if the group is finite, the 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.
- 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.
- The above definition implies that:

1. If a and b are members of both groups, then c = a • b is also a member of both groups.
2. The group share the same identity element.
3. If a is a member of both groups, the inverse of a is also a member of both groups.
4. The group made of the identity element of G, H = <{e}, •>, is a subgroup of G.
5. Each group is a subgroup of itself.

- Is the group H = <Z10, +> a subgroup of the group G = <Z12, +>?
- 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.
- The term power here means repeatedly applying the group operation to the element:
- $a^n \rightarrow a \bullet a \bullet \ldots \bullet a$ (n times)
- The set made from this process is referred to as <a>.
- Note that the duplicate elements must be discarded.
- Note also that $a^0 = e$.

G = <Z6, +>.

$0^0 \bmod 6 = 0$ (stop: the process will be repeated)

$1^0 \bmod 6 = 0$
$1^1 \bmod 6 = 1$
$1^2 \bmod 6 = (1 + 1) \bmod 6 = 2$
$1^3 \bmod 6 = (1 + 1 + 1) \bmod 6 = 3$
$1^4 \bmod 6 = (1 + 1 + 1 + 1) \bmod 6 = 4$
$1^5 \bmod 6 = (1 + 1 + 1 + 1 + 1) \bmod 6 = 5$ (stop: the process will be repeated)

$2^0 \bmod 6 = 0$
$2^1 \bmod 6 = 2$
$2^2 \bmod 6 = (2 + 2) \bmod 6 = 4$ (stop: the process will be repeated)

$3^0 \bmod 6 = 0$
$3^1 \bmod 6 = 3$ (stop: the process will be repeated)

$4^0 \bmod 6 = 0$
$4^1 \bmod 6 = 4$
$4^2 \bmod 6 = (4 + 4) \bmod 6 = 2$ (stop: the process will be repeated)

$5^0 \bmod 6 = 0$
$5^1 \bmod 6 = 5$
$5^2 \bmod 6 = 4$
$5^3 \bmod 6 = 3$
$5^4 \bmod 6 = 2$
$5^5 \bmod 6 = 1$ (stop: the process will be repeated)

Four cyclic subgroups can be made from the group G = $<Z_6, +>$.
They are $H_1 = <\{0\}, +>$, $H_2 = <\{0, 2, 4\}, +>$, $H_3 = <\{0, 3\}, +>$, and $H_4 = G$.

$G = \langle Z_{10}^*, \times \rangle$

G has only four elements:1, 3, 7, and 9.

The cyclic subgroups are $H1 = \langle \{1\}, \times \rangle$, $H2 = \langle \{1, 9\}, \times \rangle$, and $H3 = G$.

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

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

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

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

Cyclic Groups

- A cyclic group is a group that is its own cyclic subgroup.
- The element that generates the cyclic subgroup can also generate the group itself.
- This element is referred to as a generator. If g is a generator, the elements in a finite cyclic group can be written as
- $\{e, g, g^2, \ldots, g^{n-1}\}$, where $g^n = e$
- Note that a cyclic group can have many generators.
- The group G = <Z6, +> is a cyclic group with two generators, g = 1 and g = 5.
- The group G = $<Z10^*, \times>$ is a cyclic group with two generators, g = 3 and g = 7.

Lagrange's Theorem

- Lagrange's theorem relates the order of a group to the order of its subgroup
- 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|
- The order of the subgroups are |H1| = 1, |H2| = 3, |H3| = 2, and |H4| = 6. Obviously all of these orders divide 6.
- Given a group G of order |G|, the orders of the potential subgroups can be easily determined if the divisors of |G| can be found.
- For example, the order of the group G = <Z17, +> is 17. The only divisors of 17 are 1 and 17.
- This means that this group can have only two subgroups, H1 with the identity element and H2 = G.

Order of an Element

- The order of an element a in a group, ord(a), is the smallest integer n such that $a^n = e$.
- the order of an element is the order of the cyclic group it generates.
- 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.
- In the group G = <Z10*, ×>, the orders of the elements are: ord(1) = 1, ord(3) = 4, ord(7) = 4, ord(9) = 2.

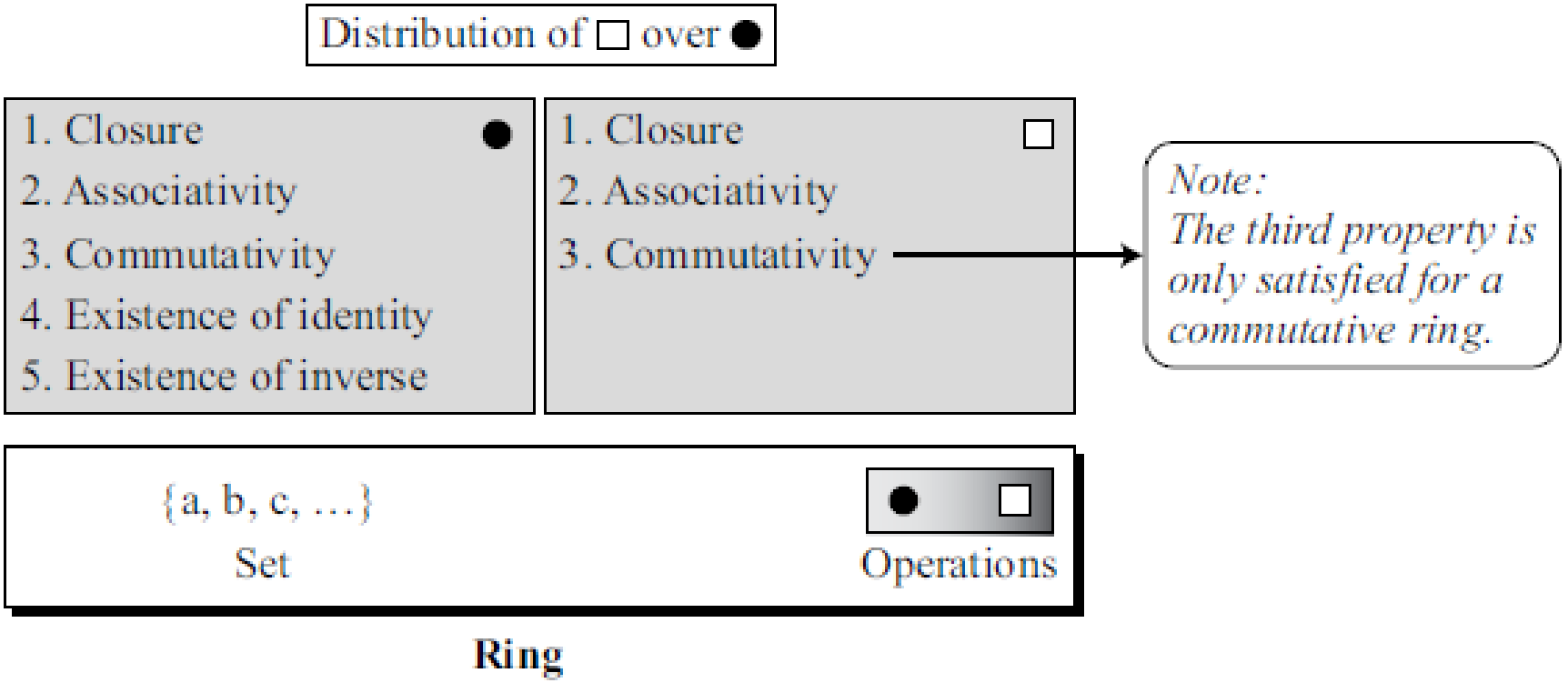
Ring

- A ring, denoted as R = <{…}, •, □ >, is an algebraic structure with two operations.
- The first operation must satisfy all five properties required for an abelian group.
- The second operation must satisfy only the first two.
- In addition, the second operation must be distributed over the first.
- Distributivity means that for all a, b, and c elements of R, we have

$$a \square (b \bullet c) = (a \square b) \bullet (a \square c) \text{ and } (a \bullet b) \square c = (a \square c) \bullet (b \square c)$$

- A commutative ring is a ring in which the commutative property is also satisfied for the second the operation.
- Figure shows a ring and a commutative ring.

Ring

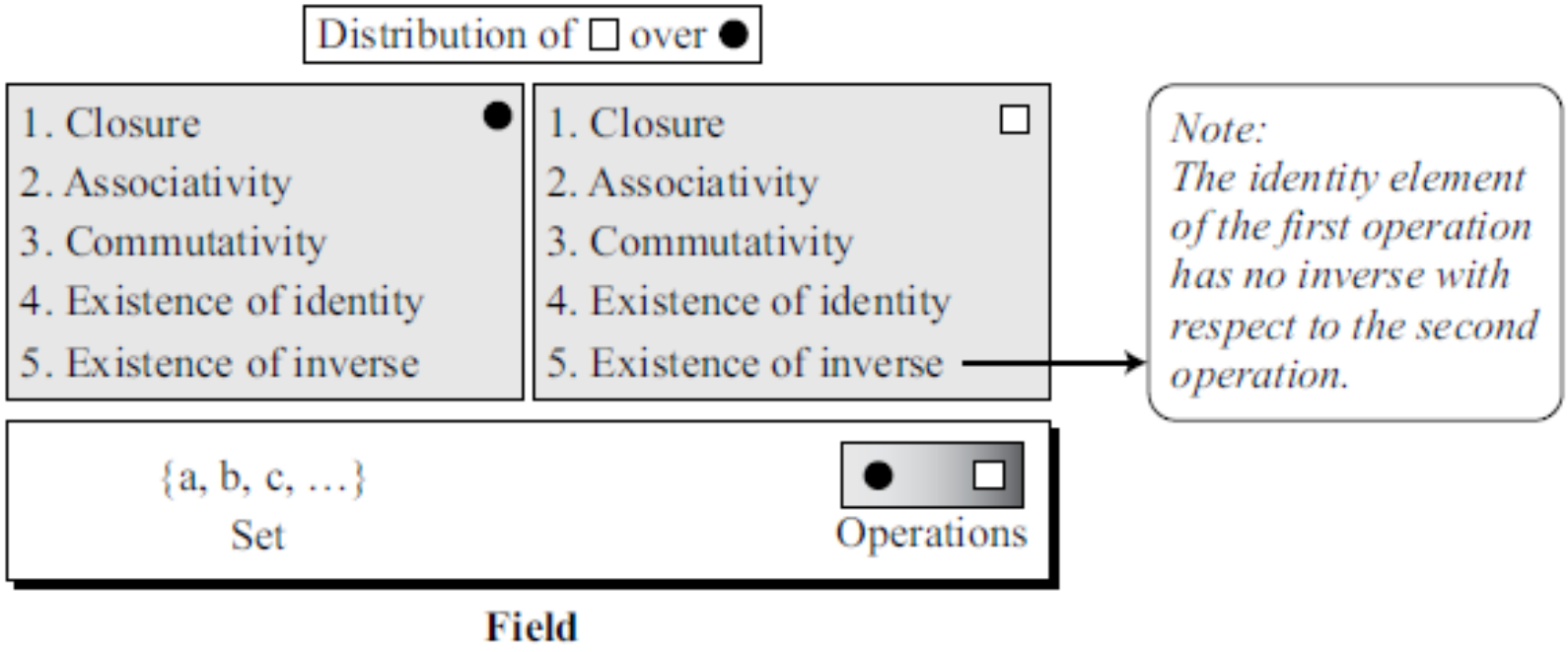

Distribution of □ over ●
1. Closure ●
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse
1. Closure □
2. Associativity
3. Commutativity
Note:
The third property is only satisfied for a commutative ring.
{a, b, c, …}
Set
● □
Operations
Ring

Ring

- The set Z with two operations, addition and multiplication, is a commutative ring. R = <Z, +, × >.
- Addition satisfies all of the five properties; multiplication satisfies only three properties. Multiplication also distributes over addition.
- For example, 5 × (3 + 2) = (5 × 3) + (5 × 2) = 25. Although, we can perform addition and subtraction on this set, we can perform only multiplication, but not division.
- Division is not allowed in this structure because it yields an element out of the set.

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 (sometimes called the zero element) has no inverse.



- all encryption algorithms, both symmetric and public key, involve arithmetic operations on integers. l
- f one of the operations that is used in the algorithm is division, then we need to work in arithmetic defined over a field.
- For convenience and for implementation efficiency, we would also like to work with integers that fit exactly into a given number of bits with no wasted bit patterns. T
- we wish to work with integers in the range 0 through , which fit into an *n*-bit word.

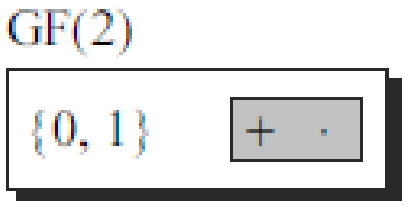
- Suppose we wish to define a conventional encryption algorithm that operates on data 8 bits at a time, and we wish to perform division.
- With 8 bits, we can represent integers in the range 0 through 255.
- However, 256 is not a prime number, so that if arithmetic is performed in Z 256(arithmetic modulo 256), this set of integers will not be a field.
- The closest prime number less than 256 is 251. Thus, the set Z251,using arithmetic modulo 251, is a field.
- However, in this case the 8-bit patterns representing the integers 251 through 255 would not be used, resulting in inefficient use of storage.

Finite Fields

- 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.
- The finite fields - called Galois fields-denoted as GF(p^n)
- **GF(p) Fields**
- When n = 1, we have GF(p) field. This field can be the set Zp, {0, 1, …, p − 1}, with two arithmetic operations (addition and multiplication).
- In this set each element has an additive inverse and that nonzero elements have a multiplicative inverse (no multiplicative inverse for 0).

GF(2)

- A very common field in this category is GF(2) with the set {0, 1} and two operations, addition and multiplication,



+	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(5)

GF(5)

{0, 1, 2, 3, 4} + ×

+	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

×	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

Example GF(7)

×	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

(b) Multiplication modulo 7

GF(2^n) FIELDS- GF(2^2)

set has four 2-bit words: {00, 01, 10, 11}.

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

Each word is the additive inverse of itself. Every word (except 00) has a multiplicative inverse. The multiplicative inverse pairs are (01, 01) and (10, 11). Addition and multiplication are defined in terms of polynomials

Galois Fields

- finite fields play a key role in cryptography
- can show number of elements in a finite field **must** be a power of a prime p^n
- known as Galois fields
- denoted GF(p^n)
- in particular often use the fields:
  - GF(p)
  - GF(2^n)

Polynomial Arithmetic

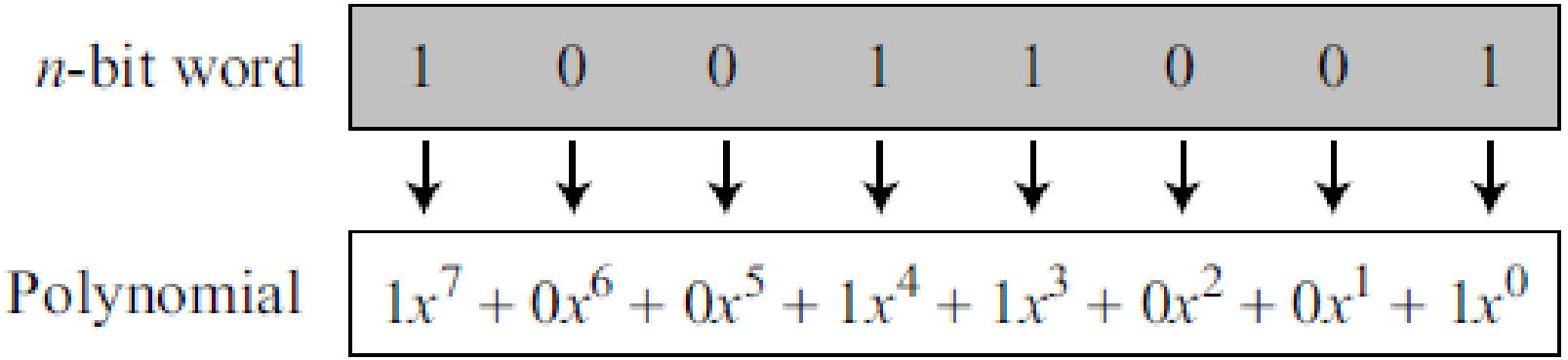
- can compute using polynomials

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

- several alternatives available
  - ordinary polynomial arithmetic
  - poly arithmetic with coords mod p
  - poly arithmetic with coords mod p and polynomials mod M(x)
- To represent an n-bit word by a polynomial follow some rules:
  - The power of x defines the position of the bit in the n-bit word. This means the leftmost bit is at position zero (related to x0); the rightmost bit is at position n − 1(related to xn−1).
  - The coefficients of the terms define the value of the bits. Because a bit can have only a value of 0 or 1, our polynomial coefficients can be either 0 or 1.

Example

Representation of an 8-bit word by a polynomial



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

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

- Any operation on polynomials actually involves two operations: operations on coefficients and operations on two polynomials.
- In other words, we need to define two fields:
  - one for the coefficients- made of 0 or1; can use GF(2)
  - one for the polynomials. - GF(2^n),

Ordinary Polynomial Arithmetic

- add or subtract corresponding coefficients
- multiply all terms by each other
- eg
  - let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

  $f(x) + g(x) = x^3 + 2x^2 - x + 3$

  $f(x) - g(x) = x^3 + x + 1$

  $f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$

Modulus

- Addition of two polynomials never creates a polynomial out of the set.
- Multiplication of two polynomials may create a polynomial with degrees more than n − 1.
- This means we need to divide the result by a modulus and keep only the remainder, as we did in modular arithmetic.
- For the sets of polynomials in GF(2^n), a group of polynomials of degree n is defined as the modulus.
- The modulus in this case acts as a prime polynomial, which means that no polynomials in the set can divide this polynomial.
- A prime polynomial cannot be factored into a polynomial with degree of less than n.
- 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	$(x^5 + x^2 + 1), (x^5 + x^3 + x^2 + x + 1), (x^5 + x^4 + x^3 + x + 1),$ $(x^5 + x^4 + x^3 + x^2 + 1), (x^5 + x^4 + x^2 + x + 1)$

Modular Polynomial Arithmetic

- can write any polynomial in the form:
  - $f(x) = q(x)\, g(x) + r(x)$
  - can interpret $r(x)$ as being a remainder
  - $r(x) = f(x) \bmod g(x)$
- if have no remainder say $g(x)$ divides $f(x)$
- if $g(x)$ has no divisors other than itself & 1 say it is **irreducible** (or prime) polynomial
- arithmetic modulo an irreducible polynomial forms a field

Addition

- add the coefficients of the corresponding terms in GF(2).
- Note that adding two polynomials of degree n − 1 always create a polynomial with degree n − 1, which means that we do not need to reduce the result using the modulus.

$$(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1) \text{ in } GF(2^8)$$

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

Addition in GF(2) means the exclusive-or (XOR)operation
example, $x^5 + x^2 + x$ → 00100110 and
$x^3 + x^2 + 1$ is → 00001101.
The result is 00101011 or in polynomial notation $x^5 + x^3 + x + 1$.

- ***Additive Identity*** in a polynomial is a zero polynomial (a polynomial with all coefficients set to zero) because adding a polynomial with itself results in a zero polynomial.
- ***Additive Inverse*** The additive inverse of a polynomial with coefficients in GF(2) is the polynomial itself.
- This means that the subtraction operation is the same as the addition operation.

Multiplication

- Multiplication in polynomials is the sum of the multiplication of each term of the first polynomial with each term of the second polynomial
- the coefficient multiplication is done in GF(2). multiplying
- x^i by x^j results in x^{i+j}
- multiplication may create terms with degree more than n − 1, which means the result needs to be reduced using a modulus polynomial

$(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$ in GF(2^8)

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

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

- ***Multiplicative identity*** is always 1.
- For example, in GF(2^8), the multiplicative identity is the bit pattern 00000001.
- ***Multiplicative Inverse*** -The extended Euclidean algorithm must be applied to the modulus and the polynomial.
- The process is exactly the same as for integers.

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

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)	

$$(x^2 + 1)^{-1} \text{ modulo } (x^4 + x + 1) \text{ is } (x^3 + x + 1)$$

$$[(x^2 + 1) \otimes (x^3 + x + 1)] \bmod (x^4 + x + 1) = 1$$

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

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

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
$\mathbf{P_1 \times P_2} = (x^6 + x^2 + x) + (x^6 + x^3 + x^2 + x) + (x^5 + x^2 + x + 1) = \boldsymbol{x^5 + x^3 + x^2 + x + 1}$			

multiplication of a polynomial by x can be easily achieved by one-bit shifting of the n-bit word;

Second, the result needed to be reduced only if the polynomial maximum power is n − 1.

In this case, reduction can be easily done by an XOR operation with the modulus because the highest power in the result is only 8

Algorithm

1. If the most significant bit of the previous result is 0, just shift the previous result one bit to the left.

2. If the most significant bit of the previous result is 1,

a. shift it one bit to the left, and

b. exclusive-or it with the modulus without the most significant bit

Example

P1 = 000100110, P2 = 10011110, modulus = 100011010

Powers	*Shift-Left Operation*	*Exclusive-Or*
$x^0 \otimes P_2$		10011110
$x^1 \otimes P_2$	00111100	(00111100) $\oplus$ (00011010) = **00100111**
$x^2 \otimes P_2$	01001110	**01001110**
$x^3 \otimes P_2$	10011100	10011100
$x^4 \otimes P_2$	00111000	(00111000) $\oplus$ (00011010) = 00100011
$x^5 \otimes P_2$	01000110	**01000110**
$\mathbf{P_1 \otimes P_2 = (00100111) \oplus (01001110) \oplus (01000110) = 00101111}$		

a maximum of n − 1 shift-left operations and 2n exclusive-or operations are needed to multiply two polynomial of degree n − 1.

Example GF(2^3)

Table 4.6 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

	+	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
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

	×	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	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

Using a Generator

- Sometimes it is easier to define the elements of the GF(2n) field using a generator.
- In this field with the irreducible polynomial $f(x)$, an element in the field, a, must satisfy the relation $f(a) = 0$.
- In particular, if g is a generator of the field, then $f(g) = 0$. It can be proved that the elements of the field can be generated as

  $\{0, g, g, g2, \ldots, g^N\}$, where $N = 2^n - 2$

Generate the elements of the field GF(2^4) using the irreducible polynomial $f(x) = x4 + x + 1$

The elements 0, g0, g1, g2, and g3 can be easily generated, because they are the 4-bit representations of 0, 1, x2, and x3

- Elements g4 through g14, which represent x4 though x14 need to be divided by the irreducible polynomial
- To avoid division, $f(g) = g4 + g + 1 = 0$ can be used

$g4 = -g - 1$

$g4 = g + 1.$

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

Reference

- Behrouz A. Forouzan and Debdeep Mukhopadhyay, “Cryptography and Network Security”, McGraw Hill, 2nd Edition, 2008