Chapter 4

Mathematics of Cryptography

Part II: Algebraic Structures

Objectives

- To review the concept of algebraic structures
- To define and give some examples of groups
- To define and give some examples of rings
- To define and give some examples of fields
- To emphasize the finite fields of type GF(2^n) that make it possible to perform operations such as addition, subtraction, multiplication, and division on n-bit words in modern block ciphers

4-1 ALGEBRAIC STRUCTURES

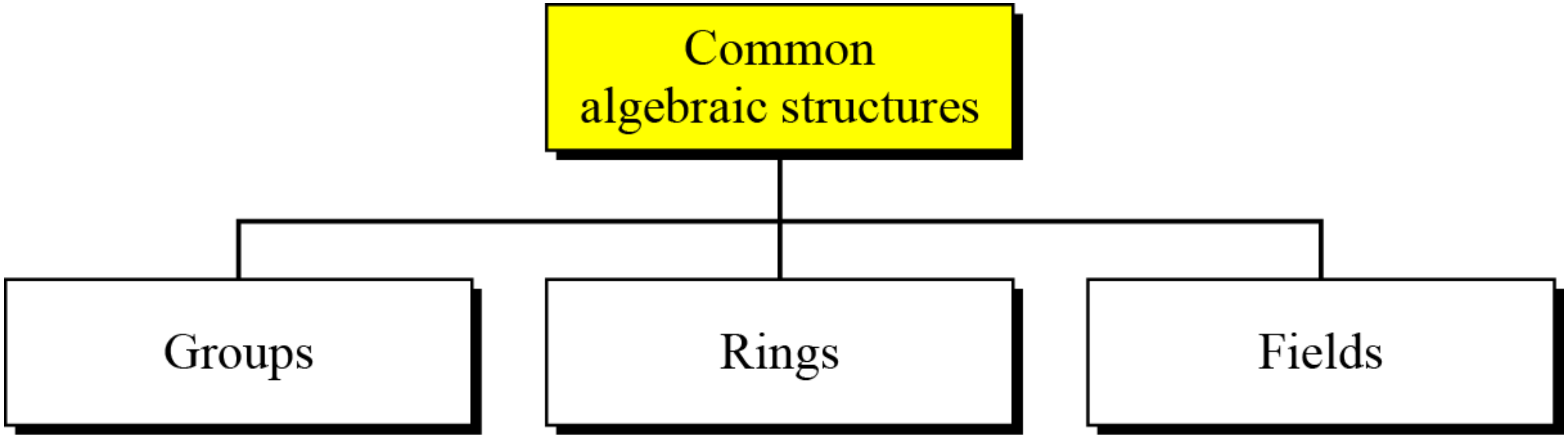
Cryptography requires sets of integers and specific operations that are defined for those sets. The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure. In this chapter, we will define three common algebraic structures: groups, rings, and fields.

Topics discussed in this section:

4.1.1 Groups
4.1.2 Rings
4.1.3 Fields

4.1 Continued

Figure 4.1 *Common algebraic structure*

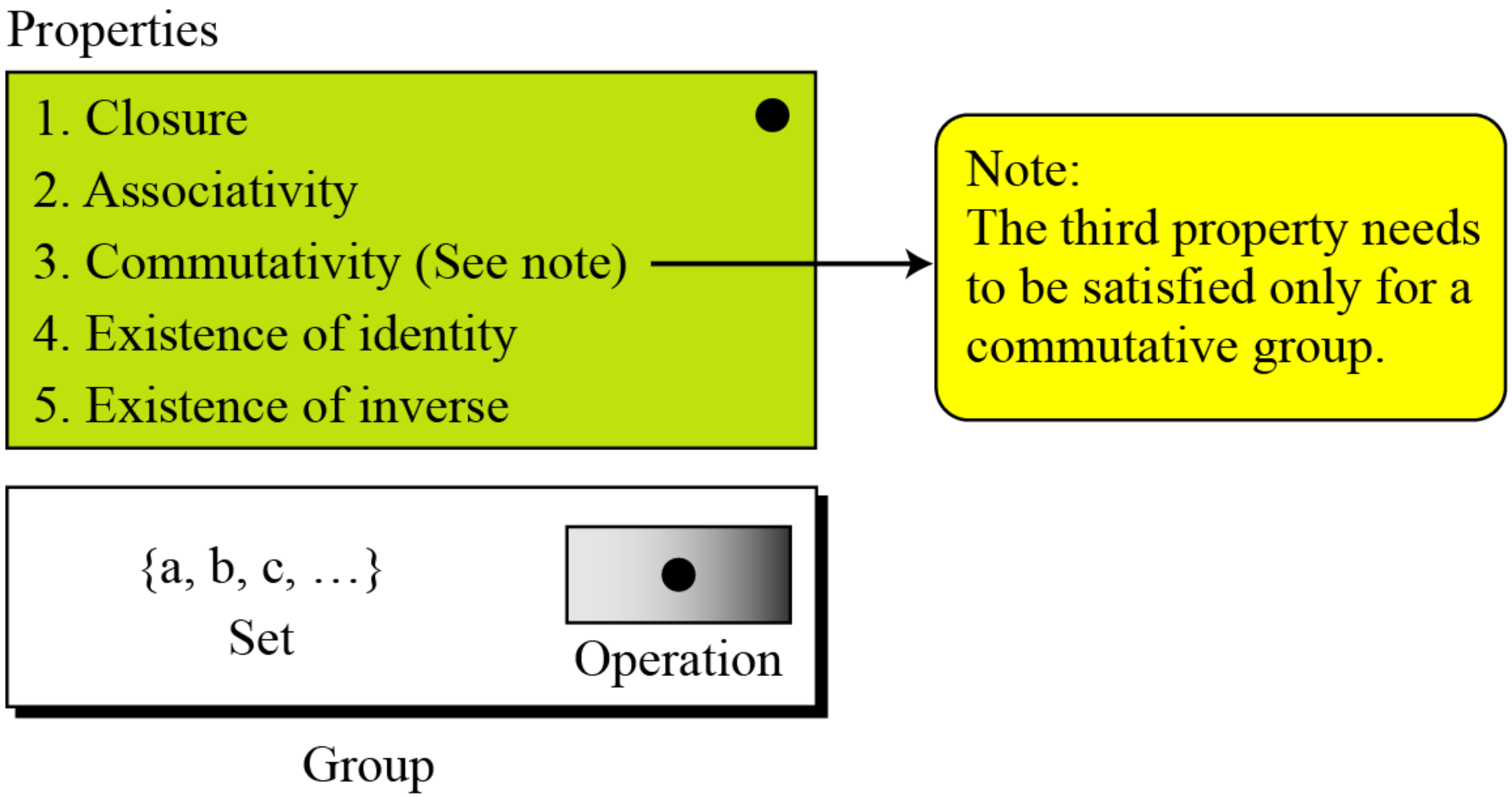


4.1.1 Groups

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:**

Figure 4.2 *Group*



Application

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 4.1

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.

Example 4.2

The set Z_n* with the multiplication operator, G = <Z_n*, ×>, is also an abelian group.

Example 4.3

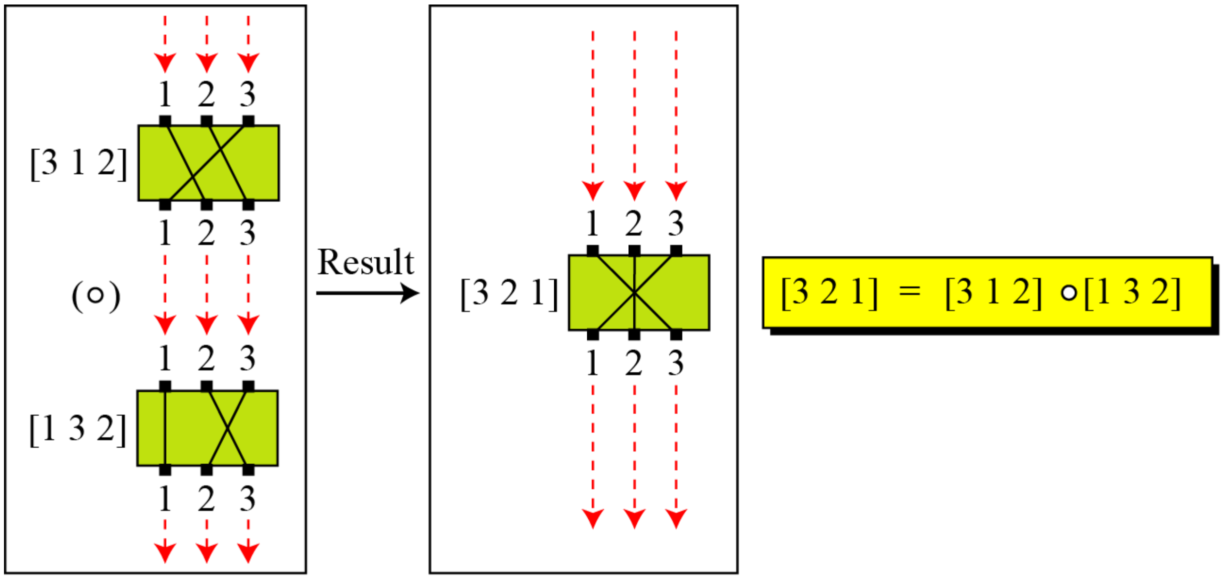
Let us define a set G = < {*a*, *b*, *c*, *d*}, •> and the operation as shown in Table 4.1.

•	*a*	*b*	*c*	*d*
a	*a*	*b*	*c*	*d*
b	*b*	*c*	*d*	*a*
c	*c*	*d*	*a*	*b*
d	*d*	*a*	*b*	*c*

Example 4.4

A very interesting group is the permutation group. The set is the set of all permutations, and the operation is composition: applying one permutation after another.

Figure 4.3 *Composition of permutation (Exercise 4.4)*



4.1.1 Continued

Example 4.4 *Continued*

Table 4.2 *Operation table for permutation group*

∘	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 2 3]	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 3 2]	[1 3 2]	[1 2 3]	[2 3 1]	[2 1 3]	[3 2 1]	[3 1 2]
[2 1 3]	[2 1 3]	[3 1 2]	[1 2 3]	[3 2 1]	[1 3 2]	[2 3 1]
[2 3 1]	[2 3 1]	[3 2 1]	[1 3 2]	[3 1 2]	[1 2 3]	[2 1 3]
[3 1 2]	[3 1 2]	[2 1 3]	[3 2 1]	[1 2 3]	[2 3 1]	[1 3 2]
[3 2 1]	[3 2 1]	[2 3 1]	[3 1 2]	[1 3 2]	[2 1 3]	[1 2 3]

4.1.1 Continued

Example 4.5

In the previous example, we showed that a set of permutations with the composition operation is a group. This implies that using two permutations one after another **cannot strengthen** the security of a cipher, because we can always find a permutation that can do the same job because of the closure property.

4.1.1 Continued

Finite Group

A group is called a finite group if the set has a finite number of element.

Order of a Group

The order of a group, |G|, is the number of elements in the group.

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.

In the other words, 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.

4.1.1 Continued

Example 4.6

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

Solution

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.

4.1.1 Continued

Cyclic Subgroups

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

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

Note that the term power here means repeatedly applying the group operation to the element.

4.1.1 Continued

Example 4.7

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.

$0^0 \bmod 6 = 0$

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

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

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

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

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

Example 4.8

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 $H_3 = G$.

$1^0 \bmod 10 = 1$

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

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

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

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:

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

4.1.1 Continued

Example 4.9

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 $H_3 = G$.

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

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

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

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

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 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 (i.e. the No. of elements in the group).

4.1.1 Continued

Example 4.10

a. In the group G = <Z_6, +>, the orders of the elements are: ord(0) = 1, ord(1) = 6, ord(2) = 3, ord(3) = 2, ord(4) = 3, ord(5) = 6.

b. In the group G = <Z_{10}*, ×>, the orders of the elements are: ord(1) = 1, ord(3) = 4, ord(7) = 4, ord(9) = 2.

$1^0 \bmod 10 = 1$

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

$3^4 = 81 \pmod{10} = 1 = e$

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

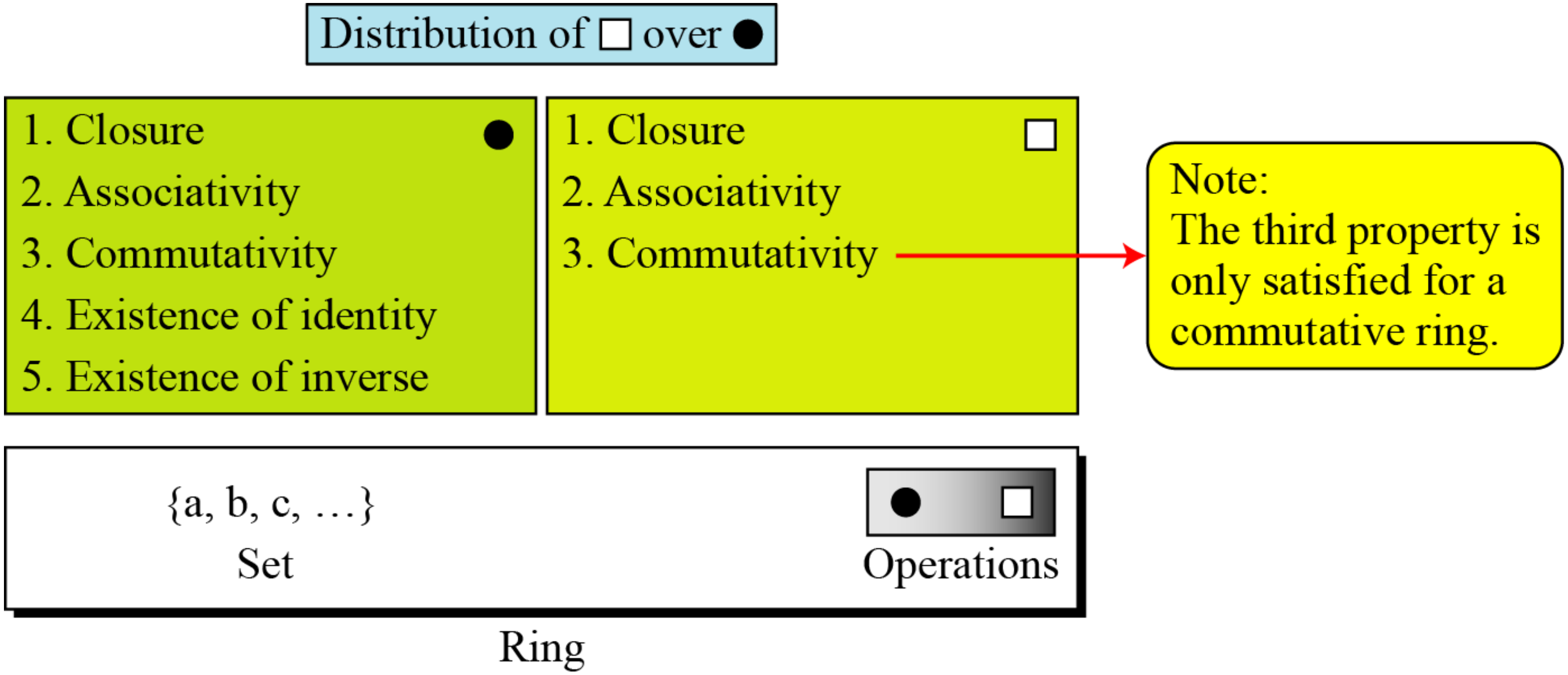
$7^4 = 2401 \pmod{10}$
$= 1 = e$

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

4.1.2 Ring

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

Figure 4.4 *Ring*



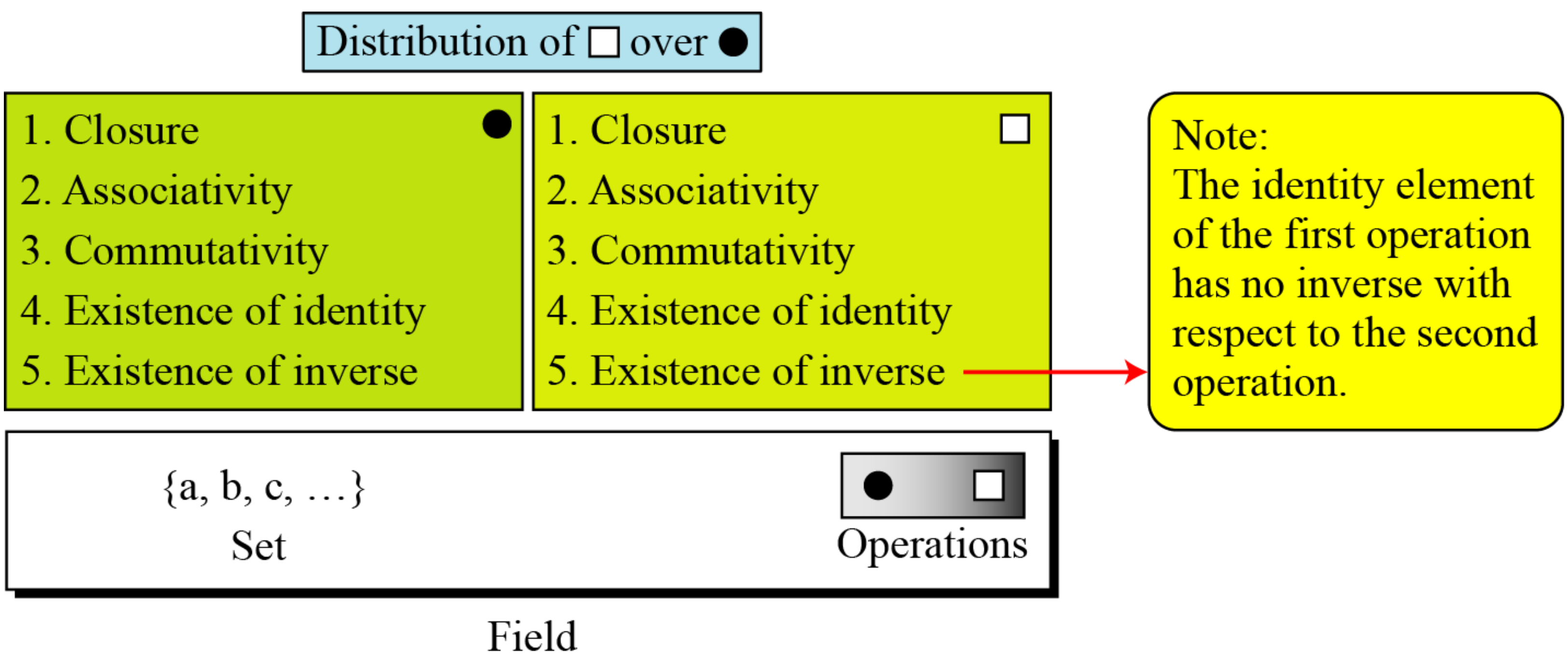
Example 4.11

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.

4.1.3 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.

Figure 4.5 *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.

4.1.3 Continued

GF(*p*) Fields

When $n = 1$, we have GF(p) field. This field can be the set Z_p, {0, 1, …, p − 1}, with two arithmetic operations.

4.1.2 Continued

Example 4.12

A very common field in this category is GF(2) with the set {0, 1} and two operations, addition and multiplication, as shown in Figure 4.6.

Figure 4.6 *GF(2) field*

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

4.1.2 Continued

Example 4.13

We can define GF(5) on the set Z_5 (5 is a prime) with addition and multiplication operators as shown in Figure 4.7.

Figure 4.7 *GF(5) field*

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

Summary

Table 4.3 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 (× ÷)	$\mathbf{Z}_p$

4-2 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. We can work in GF(2^n) and uses a set of 2^n elements. The elements in this set are n-bit words.

Topics discussed in this section:

4.2.1 Polynomials
4.2.2 Using A Generator
4.2.3 Summary

Example 4.14

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, as shown in Figure 4.8.

Figure 4.8 *An example of $GF(2^2)$ field*

Modulus: $x^2 + x + 1$

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

4.2.1 Polynomials

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

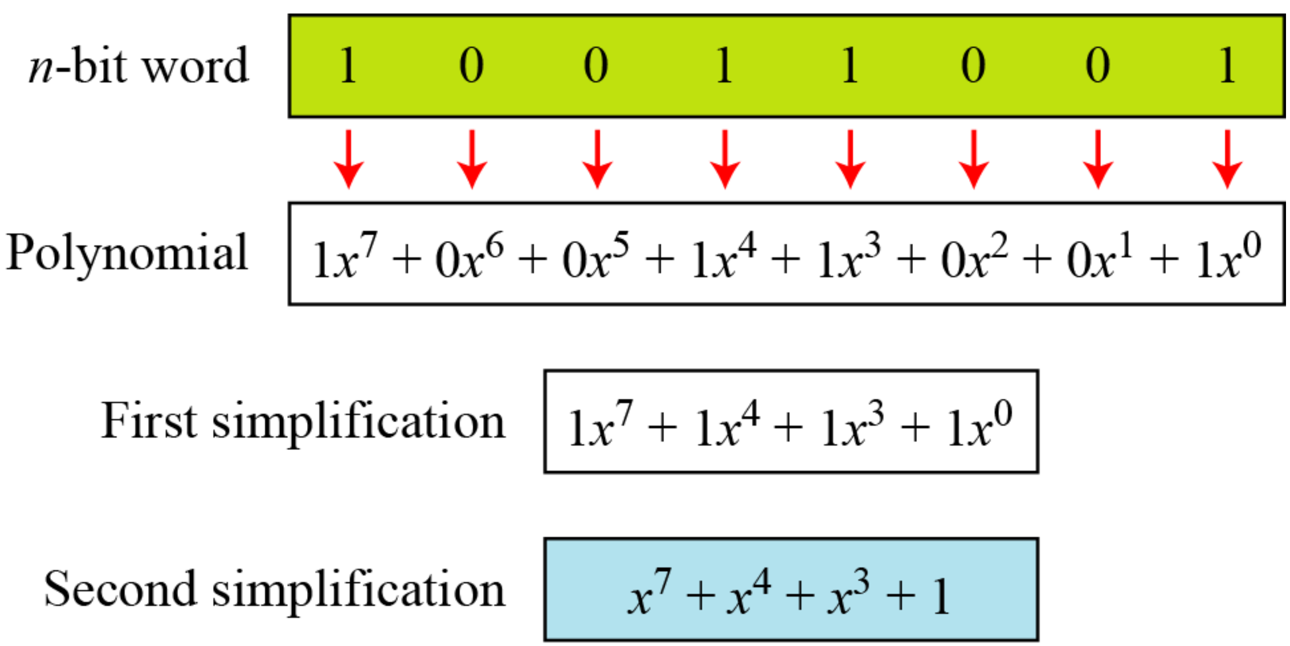
$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0$$

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

Example 4.15

Figure 4.9 show how we can represent the 8-bit word (10011001) using a polynomials.

Figure 4.9 *Representation of an 8-bit word by a polynomial*



4.2.1 Continued

Example 4.16

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.

4.2.1 Continued

GF(2^n) Fields

Note

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

4.2.1 Continued

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.

Table 4.9 *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	$(x^5 + x^2 + 1)$, $(x^5 + x^3 + x^2 + x + 1)$, $(x^5 + x^4 + x^3 + x + 1)$, $(x^5 + x^4 + x^3 + x^2 + 1)$, $(x^5 + x^4 + x^2 + x + 1)$

4.2.1 Continued

Addition

Note

Addition and subtraction operations on polynomials are the same operation.

4.2.1 Continued

Example 4.17

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:

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

4.2.1 Continued

Example 4.18

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 $x^5 + x^3 + x + 1$.

4.2.1 Continued

Multiplication

1. The coefficient multiplication is done in GF(2).

2. The 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 polynomial.

4.2.1 Continued

Example 4.19

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.

Solution

$$P_1 \otimes P_2 = x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x)$$

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

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

To find the final result, divide the polynomial of degree 12 by the polynomial of degree 8 (the modulus) and keep only the remainder. Figure 4.10 shows the process of division.

4.2.1 Continued

Figure 4.10 *Polynomial division with coefficients in GF(2)*

Divisor: $x^8 + x^4 + x^3 + x + 1$

Quotient: $x^4 + 1$

$$
\begin{array}{r}
x^{12} + x^7 + x^2 \\
x^{12} + x^8 + x^7 + x^5 + x^4 \\
\hline
x^8 + x^5 + x^4 + x^2 \\
x^8 + x^4 + x^3 + x + 1 \\
\hline
\end{array}
$$

Remainder $x^5 + x^3 + x^2 + x + 1$

4.2.1 Continued

Example 4.20

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

Solution

The answer is ($x^3 + x + 1$) as shown in Table 4.5.

Table 4.5 *Euclidean algorithm for Exercise 4.20*

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)	

Example 4.21

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

Solution

The answer is ($x^5 + x^4 + x^3 + x$) as shown in Table 4.6.

Table 4.6 *Euclidean algorithm for Exercise 4.21*

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)	

4.2.1 Continued

Multtliplication Using Computer

The computer implementation uses a better algorithm, repeatedly multiplying a reduced polynomial by *x*.

Example 4.22

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 $(x^8 + x^4 + x^3 + x + 1)$ using the algorithm described above.

Solution

The process is shown in Table 4.7. 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.

Example 4.22 Continued

$P_1 = (x^5 + x^2 + x) \times P_2 = (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$

Table 4.7 *An efficient algorithm (Example 4.22)*

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

Example 4.23

Repeat Example 4.22 using bit patterns of size 8.

Solution

We have P1 = 000100110, P2 = 10011110, modulus = 100011010 (nine bits). We show the exclusive or operation by ⊕.

Table 4.8 *An efficient algorithm for multiplication using n-bit words*

Powers	*Shift-Left Operation*	*Exclusive-Or*
$x^0 \otimes P_2$		10011110
$x^1 \otimes P_2$	00111100	(00111100) ⊕ (00011010) = **<u>00100111</u>**
$x^2 \otimes P_2$	01001110	**<u>01001110</u>**
$x^3 \otimes P_2$	10011100	10011100
$x^4 \otimes P_2$	00111000	(00111000) ⊕ (00011010) = 00100011
$x^5 \otimes P_2$	01000110	**<u>01000110</u>**
$P_1 \otimes P_2$ = (00100111) ⊕ (01001110) ⊕ (01000110) = 00101111		

Example 4.24

The GF(2^3) field has 8 elements. We use the irreducible polynomial ($x^3 + x^2 + 1$) and show the addition and multiplication tables for this field. We show both 3-bit words and the polynomials. Note that there are two irreducible polynomials for degree 3. The other one, ($x^3 + x + 1$), yields a totally different table for multiplication.

4.2.1 Continued

Example 4.24 Continued

Table 4.9 *Addition table for GF(2³)*

⊕	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)

Example 4.24 Continued

Table 4.10 *Multiplication table for GF(2^3)*

⊗	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)	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)

4.2.2 Using a Generator

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

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

Example 4.25

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

Solution

The elements 0, g^0, g^1, $g2$, and g^3 can be easily generated, because they are the 4-bit representations of 0, 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, the relation $f(g) = g^4 + g + 1 = 0$ can be used therefore $g^4 = g + 1$.

(See next slide)

4.2.1 Continued

Example 4.25 Continued

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

4.2.1 Continued

Example 4.26

The following show the results of addition and subtraction operations:

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

4.2.1 Continued

Example 4.27

The following show the result of multiplication and division operations:.

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

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

4.2.3 Summary

The finite field $GF(2^n)$ can be used to define four operations of addition, subtraction, multiplication and division over *n*-bit words. The only restriction is that division by zero is not defined.