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

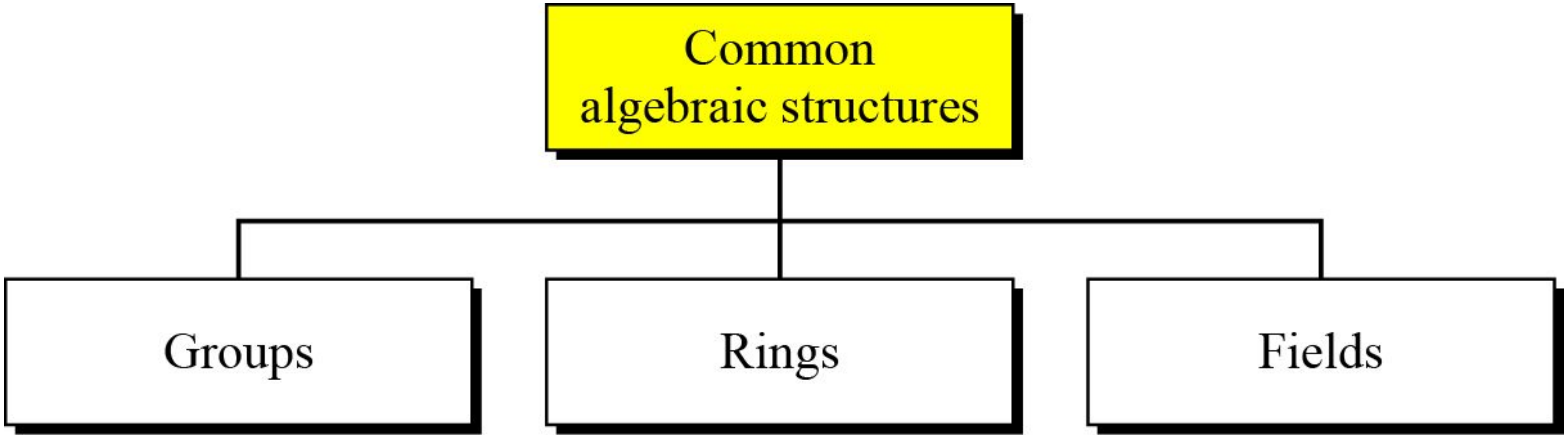
Cryptography requires sets of integers and specific operations that are defined for those sets. The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure. In this chapter, we will define three common algebraic structures: groups, rings,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



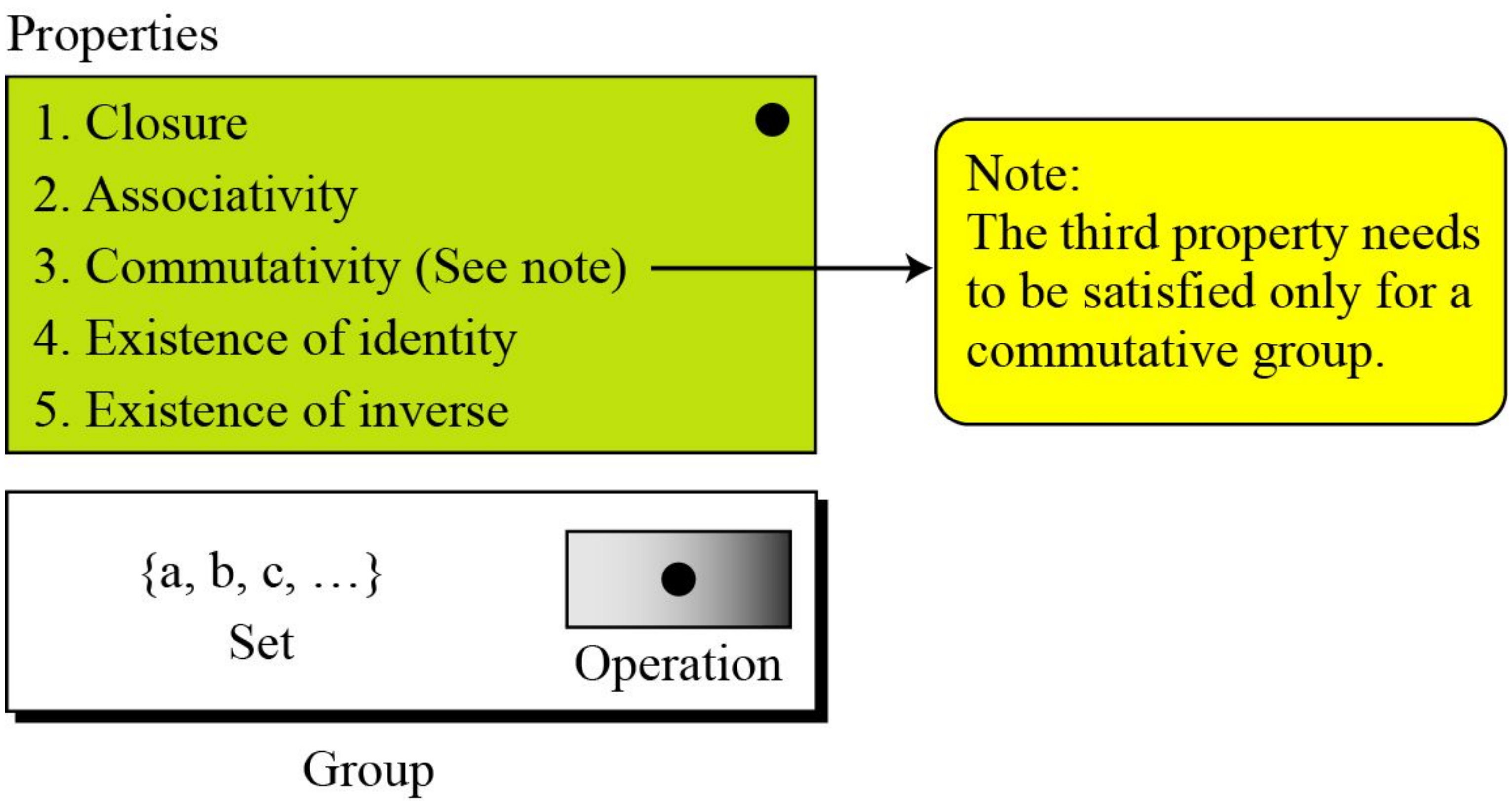
4.1.1 Groups

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:

4.1.1 Continued

Figure 4.2 ***Group***



Properties

Closure:

For all a, b in G, the result of the operation, $a \cdot b$, is also in G.

Associativity:

For all a, b and c in G, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Identity element:

There exists an element e in G such that, for every element a in G, the equation $e \cdot a = a \cdot e = a$ holds. Such an element is unique, and thus one speaks of *the* identity element.

Inverse element:

For each a in G, there exists an element b in G, commonly denoted a^{-1} (or $-a$, if the operation is denoted "+"), such that $a \cdot b = b \cdot a = e$, where e is the identity element.

4.1.1 Continued

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.
Eg: a + b = b + a for any two integers

4.1.1 Continued

Example 4.2

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

Groups for which the commutativity equation a · b = b · a always holds are called abelian groups

Example 4.3

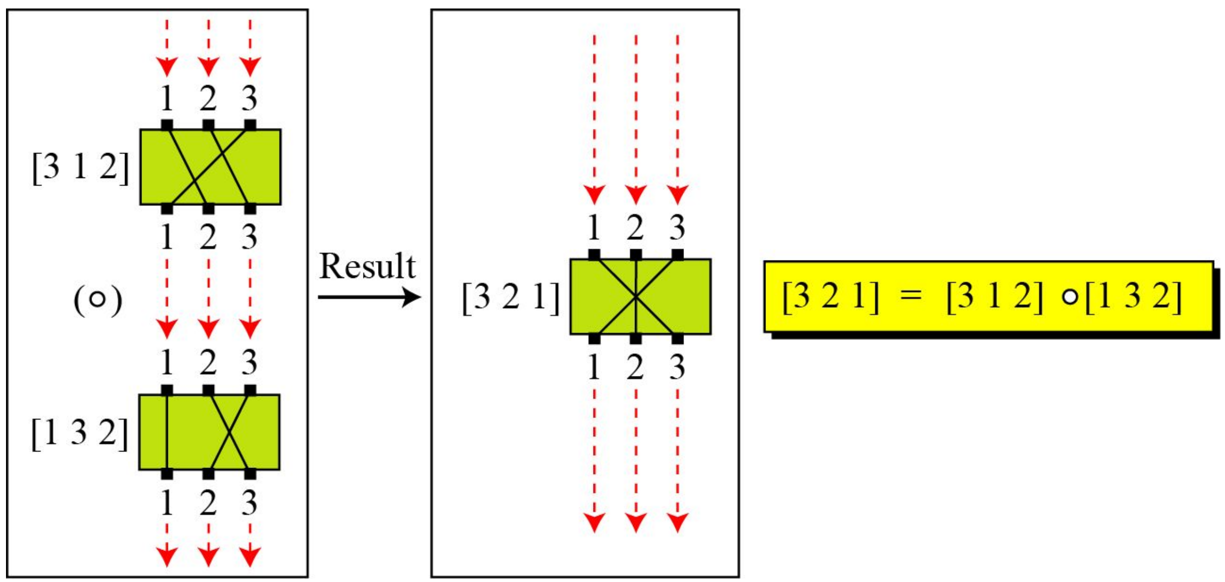
Let us define a set G = < {*a*, *b*, *c*, *d*}, •> and the operation as shown in Table 4.1.

•	*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**

- **Order of a Group**

- **Subgroups**

4.1.1 Continued

Example 4.6

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

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.

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

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.

$0^0 \bmod 6 = 0$

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

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

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

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

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

4.1.1 Continued

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 $H_3 = G$.

$1^0 \bmod 10 = 1$

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

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

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

4.1.1 Continued

Cyclic Groups

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

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

Example 4.9

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

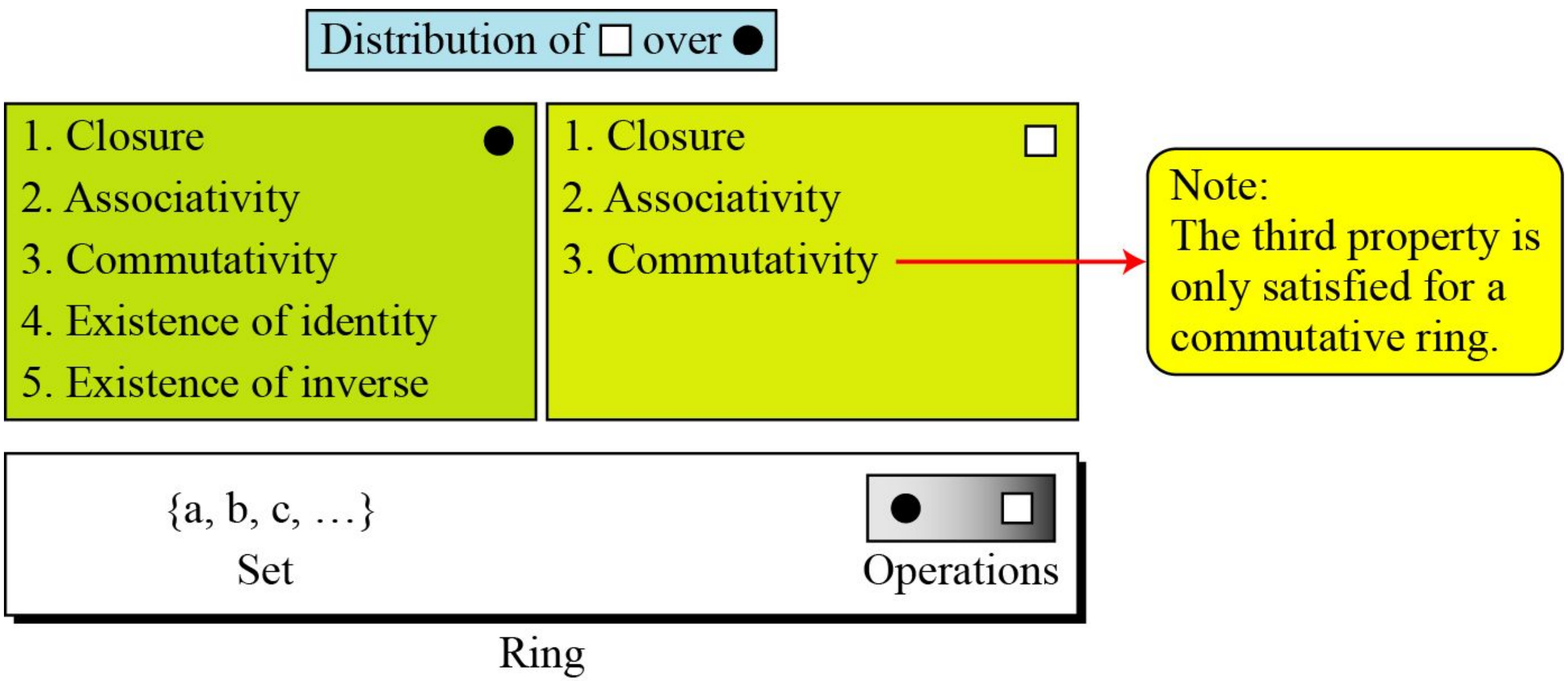
a. The group $G = <Z_6, +>$ is a cyclic group with two generators, $g = 1$ and $g = 5$.

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

4.1.2 Ring

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

Figure 4.4 *Ring*



4.1.2 Continued

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.

A ring is a set R equipped with two binary operations + and · satisfying the following three sets of axioms, called the ring

Properties

1. R is an abelian group under addition, meaning that:

- $(a + b) + c = a + (b + c)$ for all a, b, c in R (that is, $+$ is associative).
- $a + b = b + a$ for all a, b in R (that is, $+$ is commutative).
- There is an element 0 in R such that $a + 0 = a$ for all a in R (that is, 0 is the additive identity).
- For each a in R there exists $-a$ in R such that $a + (-a) = 0$ (that is, $-a$ is the additive inverse of a).

Properties

2. R is a <u>monoid</u> under multiplication, meaning that:

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c in R (that is, $\cdot$ is associative).
- There is an element 1 in R such that $a \cdot 1 = a$ and $1 \cdot a = a$ for all a in R (that is, 1 is the <u>multiplicative identity</u>).

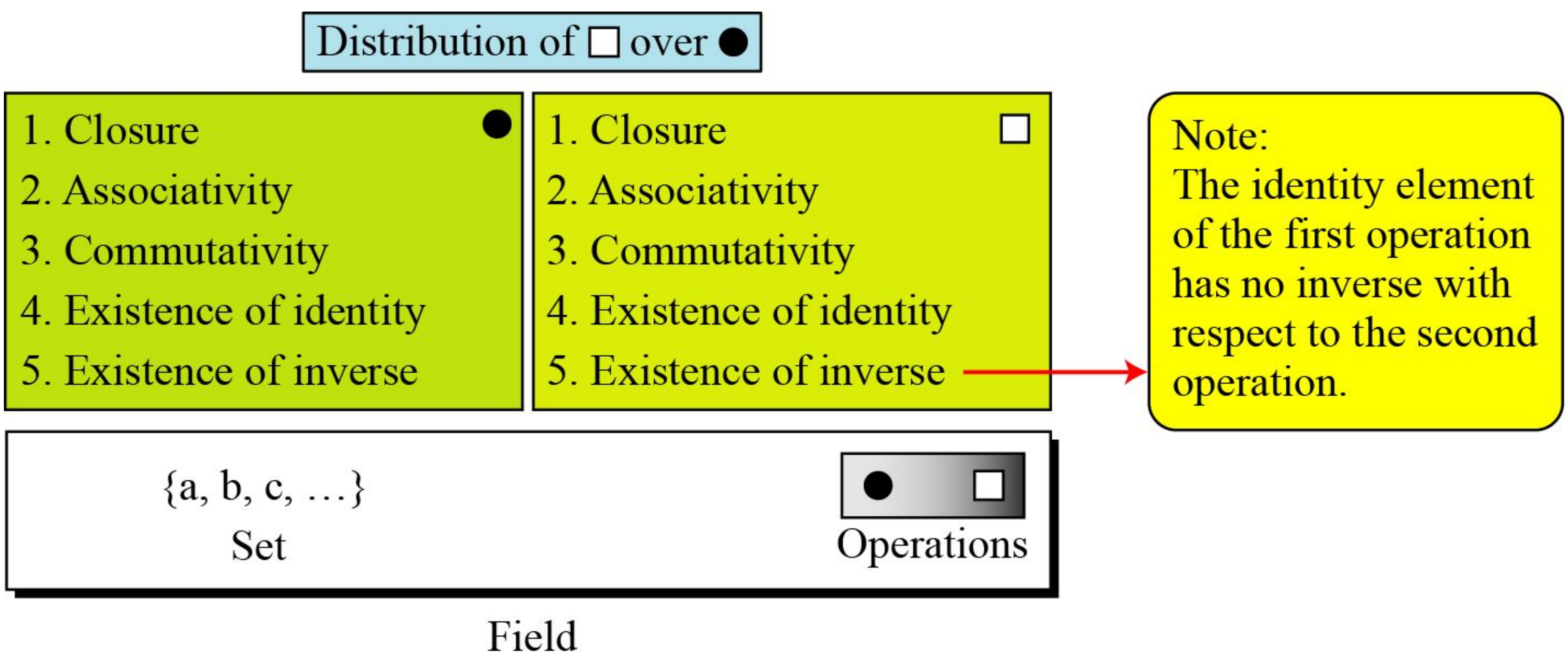
3. Multiplication is <u>distributive</u> with respect to addition, meaning that:

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

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***



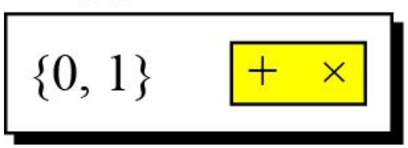
4.1.2 Continued

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	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

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

4.1.3 *Continued*

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

Formally, a field is a set F together with two binary operations on F called addition and multiplication. A binary operation on F is a mapping $F \times F \rightarrow F$, that is, a correspondence that associates with each ordered pair of elements of F a uniquely determined element of F.

The result of the addition of a and b is called the sum of a and b, and is denoted $a + b$.

Similarly, the result of the multiplication of a and b is called the product of a and b, and is denoted ab or $a \cdot b$.

Properties

1. Associativity of addition and multiplication: $a + (b + c) = (a + b) + c$, and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. Commutativity of addition and multiplication: $a + b = b + a$, and $a \cdot b = b \cdot a$.
3. AdditiveAdditive and multiplicative identity: there exist two different elements 0 and 1 in F such that $a + 0 = a$ and $a \cdot 1 = a$.
4. Additive inverses: for every a in F, there exists an element in F, denoted $-a$, called the *additive inverse* of a, such that $a + (-a) = 0$.
5. Multiplicative inverses: for every $a \neq 0$ in F, there exists an element in F, denoted by a^{-1} or $1/a$, called the *multiplicative inverse* of a, such that $a \cdot a^{-1} = 1$.
6. Distributivity of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

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:

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

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

$$\mathrm{P}_1 \otimes \mathrm{P}_2 = x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x)$$
$$\mathrm{P}_1 \otimes \mathrm{P}_2 = x^{12} + x^9 + x^8 + x^7 + x^6 + x^9 + x^6 + x^5 + x^4 + x^3 + x^8 + x^5 + x^4 + x^3 + x^2$$
$$\mathrm{P}_1 \otimes \mathrm{P}_2 = (x^{12} + x^7 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x^5 + x^3 + x^2 + x + 1$$

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)*

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

4.2.1 Continued

Multliplication 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.

4.2.1 Continued

Example 4.22 Continued

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

4.2.1 Continued

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) = **00100111**
$x^2 \otimes P_2$	01001110	**01001110**
$x^3 \otimes P_2$	10011100	10011100
$x^4 \otimes P_2$	00111000	(00111000) ⊕ (00011010) = 00100011
$x^5 \otimes P_2$	01000110	**01000110**
$P_1 \otimes P_2$ = (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)*

Example 4.24 *Continued*

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

$\otimes$	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.

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

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 (See next slide).

Example 4.25 Continued

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

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

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.