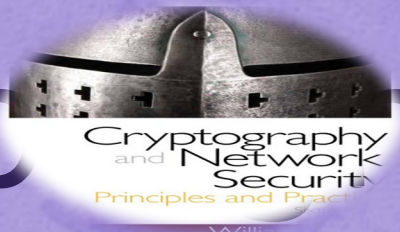
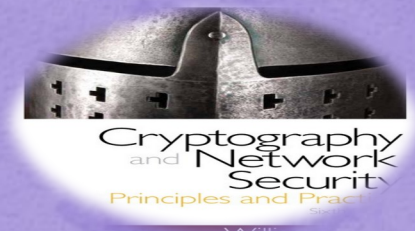
Cryptography and Network Security



Eighth Edition
by William Stallings



Chapter 5

Finite Fields

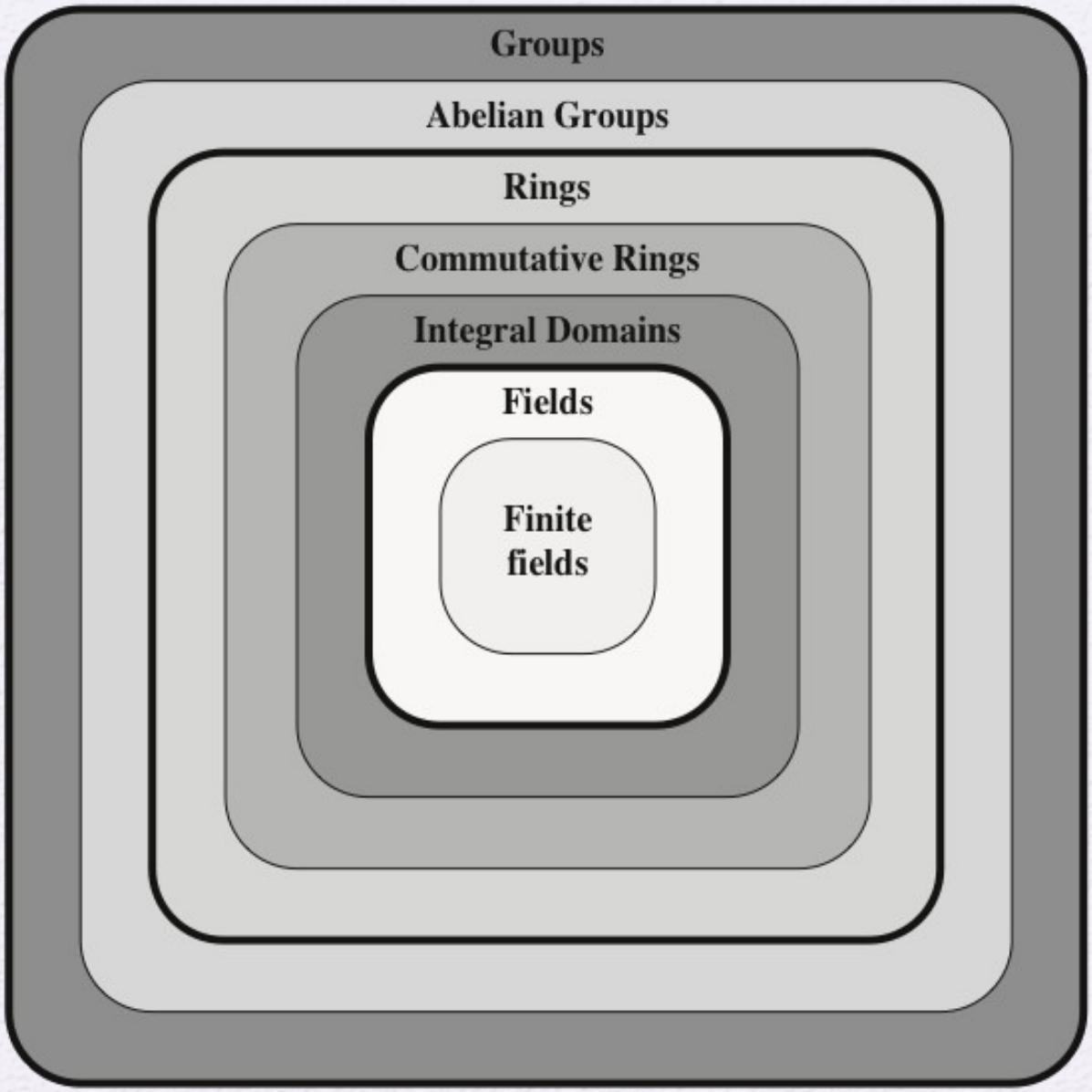
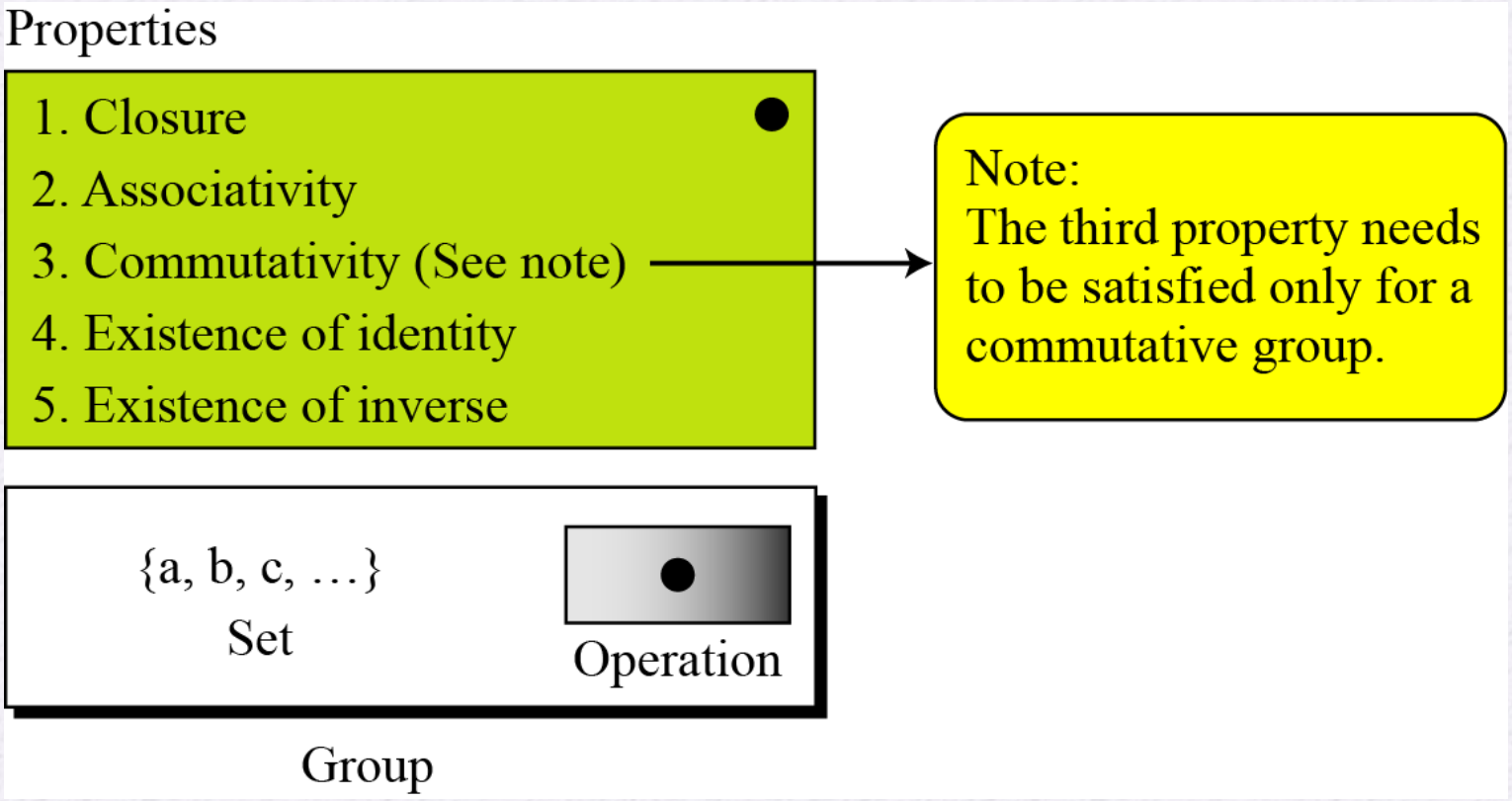


Figure 5.1 Groups, Rings, and Fields

Groups

- A set of elements with a binary operation denoted by $\diamond$ that associates to each ordered pair (a,b) of elements in G an element $(a \diamond b)$ in G, such that the following axioms are obeyed:
  - (A1) Closure:
    - If a and b belong to G, then $a \diamond b$ is also in G
  - (A2) Associative:
    - $a \diamond (b \diamond c) = (a \diamond b) \diamond c$ for all a, b, c in G
  - (A3) Identity element:
    - There is an element e in G such that $a \diamond e = e \diamond a = a$ for all a in G
  - (A4) Inverse element:
    - For each a in G, there is an element a^{1} in G such that $a \diamond a^{1} = a^{1} \diamond a = e$
  - (A5) Commutative:
    - $a \diamond b = b \diamond a$ for all a, b in G

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 Zn^* with the multiplication operator, $G = \langle Zn^*, \times \rangle$, is also an abelian group.

Example 4.3

Let us define a set $G = \langle \{a, b, c, d\}, \bullet \rangle$ 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*

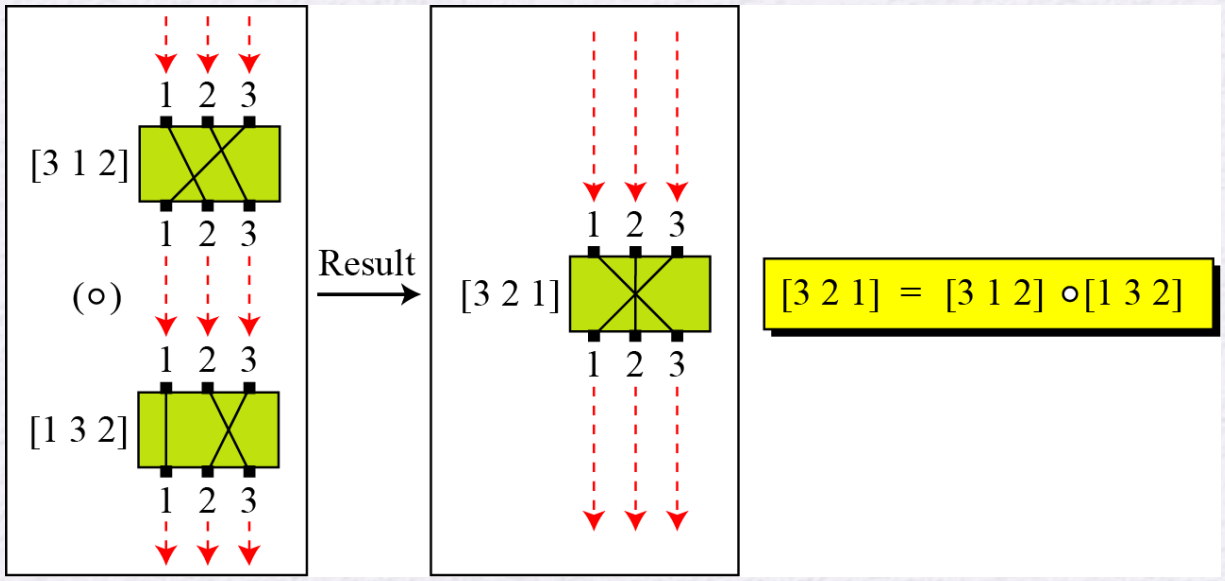
4.1.1 Continued

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)*



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]

Finite Group

A group is called a finite group if the set has a finite number of elements. Otherwise, the group is an infinite group.

Order of a Group

The order of a group 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.

Example 4.6

Is the group H = <Z10, +> a subgroup of the group G = <Z12, +>?

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.

H2 = <{0, 2, 4, 6, 8, 10}, +12> is a subgroup of G = <Z12, +12>.

Cyclic Group

- Exponentiation is defined within a group as a repeated application of the group operator, so that $a^3 = a \blacksquare a \blacksquare a$
- We define $a^0 = e$ as the identity element, and $a^{-n} = (a^{-1})^n$, where a^{-1} is the inverse element of a within the group
- A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element $a \in G$
- The element a is said to **generate** the group G or to be a **generator** of G
- A cyclic group is always abelian and may be finite or infinite

Rings

- A **ring** R , sometimes denoted by {R , + , * }, is a set of elements with two binary operations, called *addition* and *multiplication*, such that for all a , b , c in R the following axioms are obeyed:

(A1–A5)

R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5. For the case of an additive group, we denote the identity element as 0 and the inverse of a as $-a$

(M1) Closure under multiplication:

If a and b belong to R , then ab is also in R

(M2) Associativity of multiplication:

$a(bc) = (ab)c$ for all a , b , c in R

(M3) Distributive laws:

$a(b + c) = ab + ac$ for all a , b , c in R

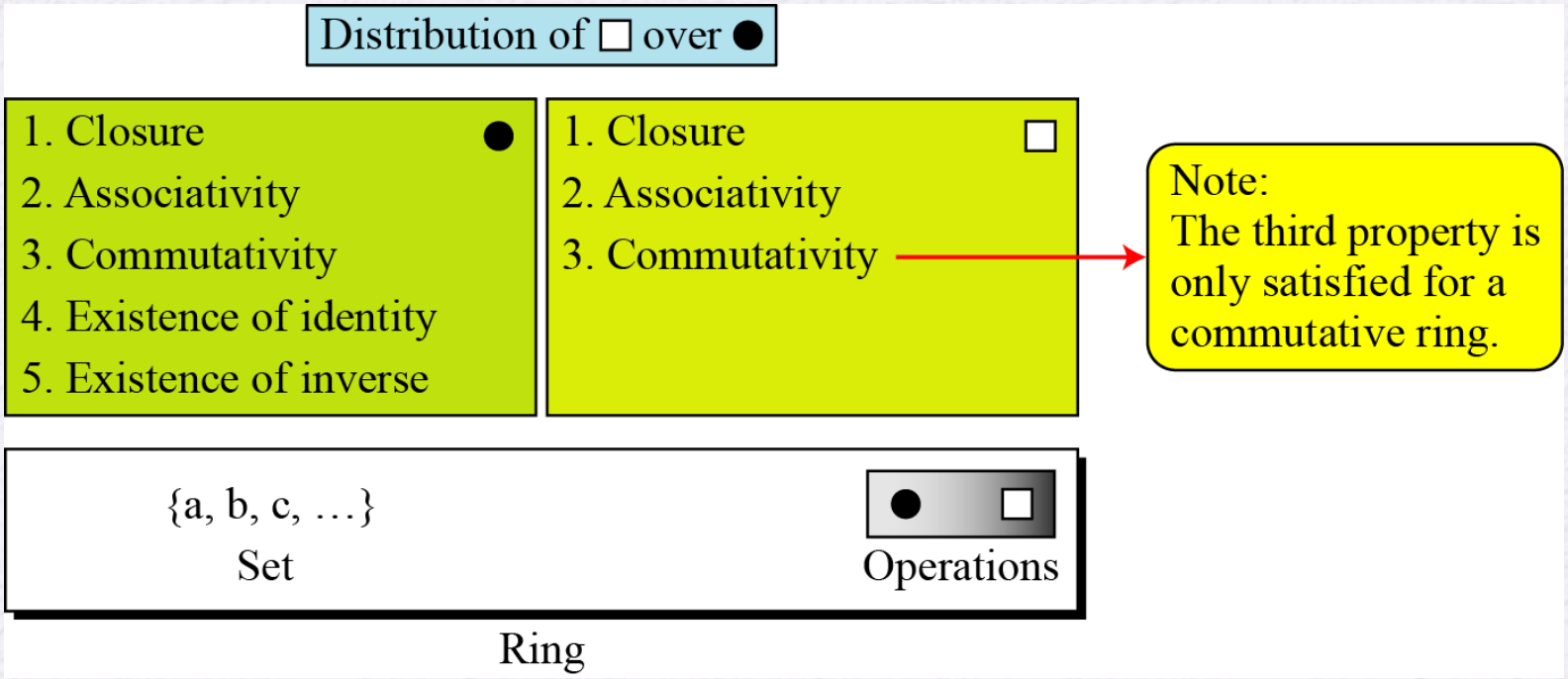
$(a + b)c = ac + bc$ for all a , b , c in R

- In essence, a ring is a set in which we can do addition, subtraction *[a - b = a + (-b)]*, and multiplication without leaving the set

4.1.2 Ring

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

Figure 4.4 *Ring*



distributive □ over • :

$a \square (b \bullet c) = a \square b \bullet a \square c$

Example 4.11

Definition.

A nonempty set R is called a ring, if it has two binary operations called addition denoted by $a + b$ and multiplication denoted by $a \times b$ for $a, b \in R$ satisfying the following axioms:

(1) $(R, +)$ is an abelian group.

(2) Multiplication is associative, i.e. $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$.

(3) Distributive laws hold: $a \times (b + c) = a \times b + a \times c$ and $(b + c) \times a = b \times a + c \times a$ for all $a, b, c \in R$.

Example 4.11

The set Z with two operations, addition and multiplication, is a commutative ring, denoted by $R = \langle Z, +, \times \rangle$.

Addition satisfies all of the five properties;

Multiplication satisfies only three properties.

The set Z_n with two operations, $+_n$ and $\times_n$ is a commutative ring, denoted by $R_n = \langle Z_n, +_n, \times_n \rangle$.

Rings (cont.)

- A ring is said to be commutative if it satisfies the following additional condition:

  (M4) Commutativity of multiplication:

  $ab = ba$ for all a, b in R

- An *integral domain* is a commutative ring that obeys the following axioms.

  (M5) Multiplicative identity:

  There is an element 1 in R such that $a1 = 1a = a$ for all a in R

  (M6) No zero divisors:

  If a , b in R and $ab = 0$, then either $a = 0$ or $b = 0$

Fields

- A **field** *F* , sometimes denoted by {F, +,* }, is a set of elements with two binary operations, called *addition* and *multiplication*, such that for all *a, b, c* in *F* the following axioms are obeyed:

(A1–M6)

F is an integral domain; that is, *F* satisfies axioms A1 through A5 and M1 through M6

(M7) Multiplicative inverse:

For each *a* in *F*, except 0, there is an element a^{-1} in *F* such that $aa^{-1} = (a^{-1})a = 1$

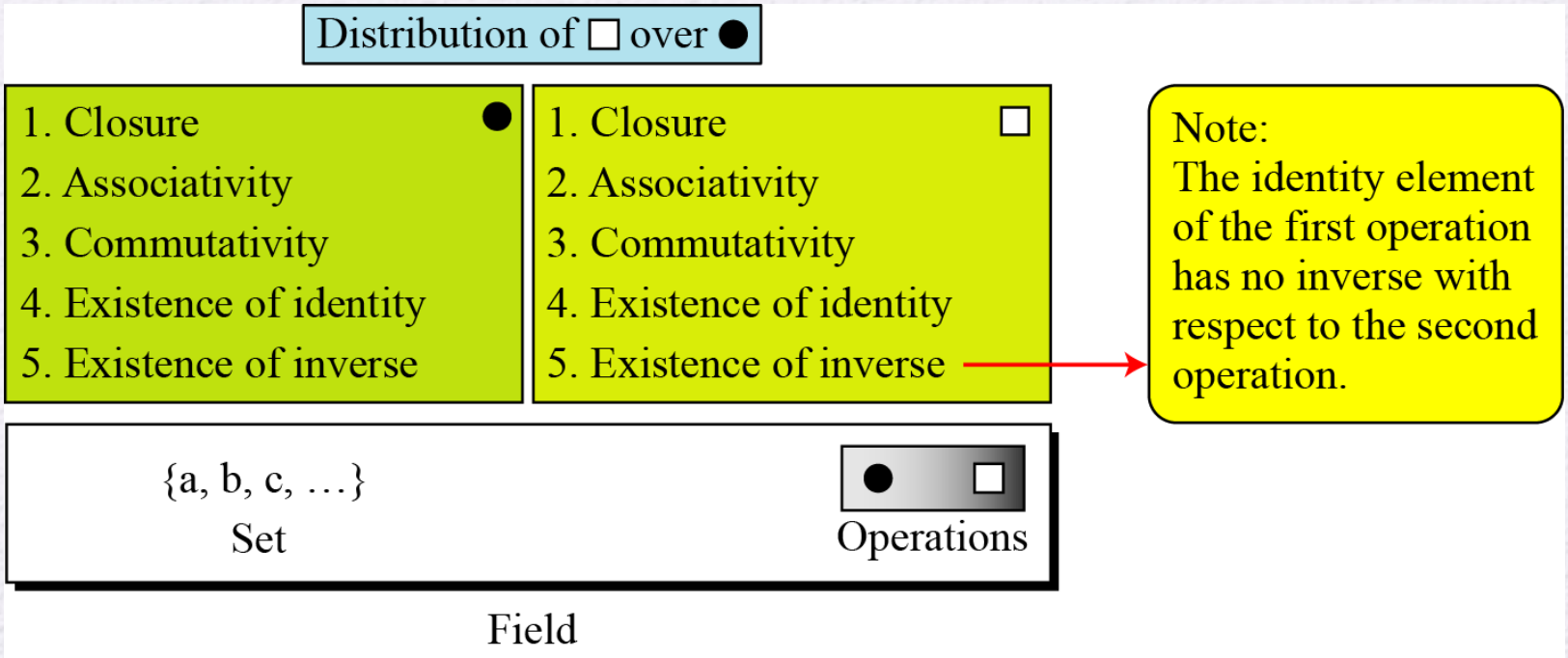
- In essence, a field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set. Division is defined with th

Familiar examples of fields are the rational numbers, the real numbers, and the complex numbers. Note that the set of all integers is not a field, because not every element of the set has a multiplicative inverse.

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*



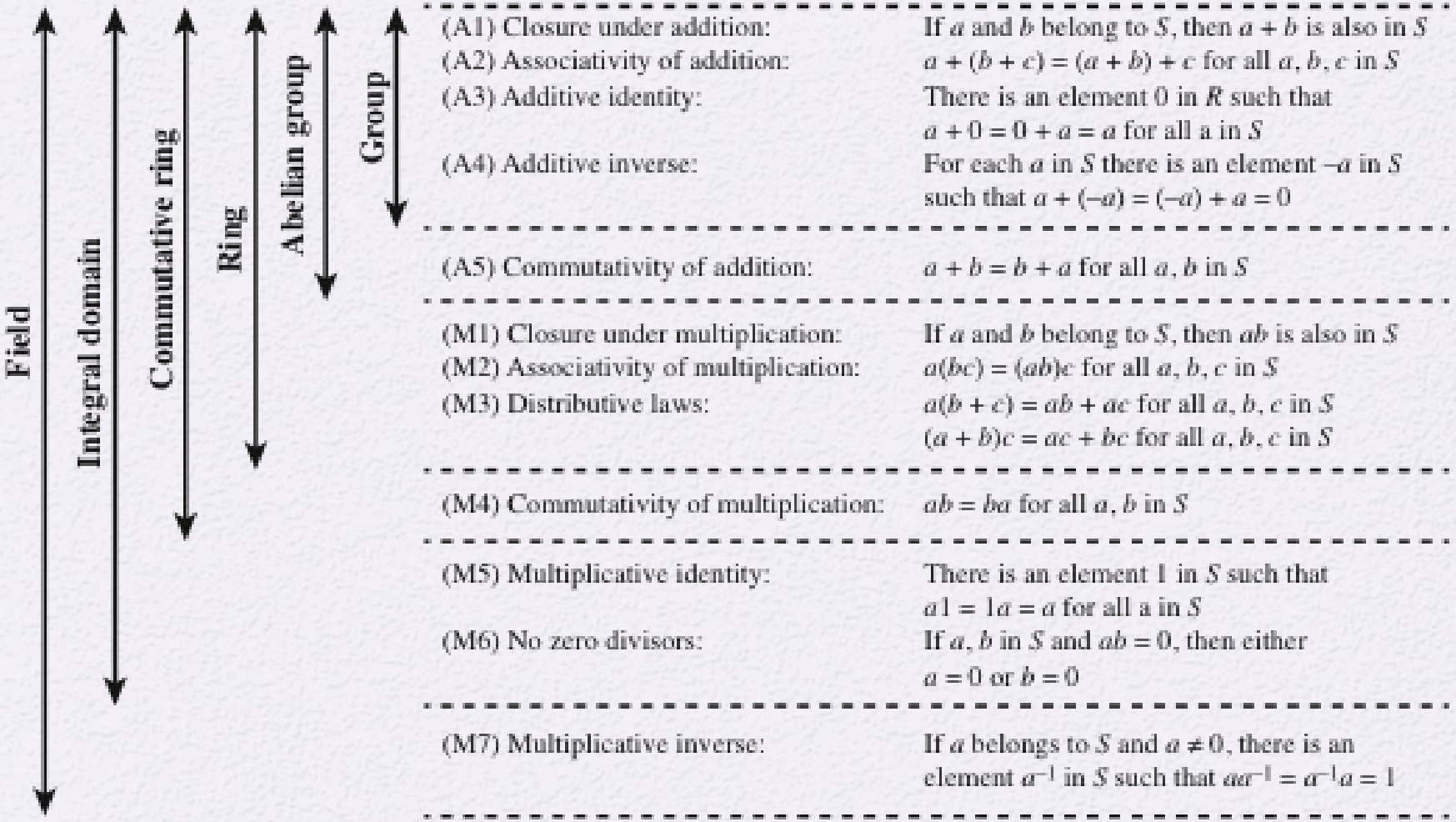


Figure 5.2 Properties of Groups, Rings, and Fields

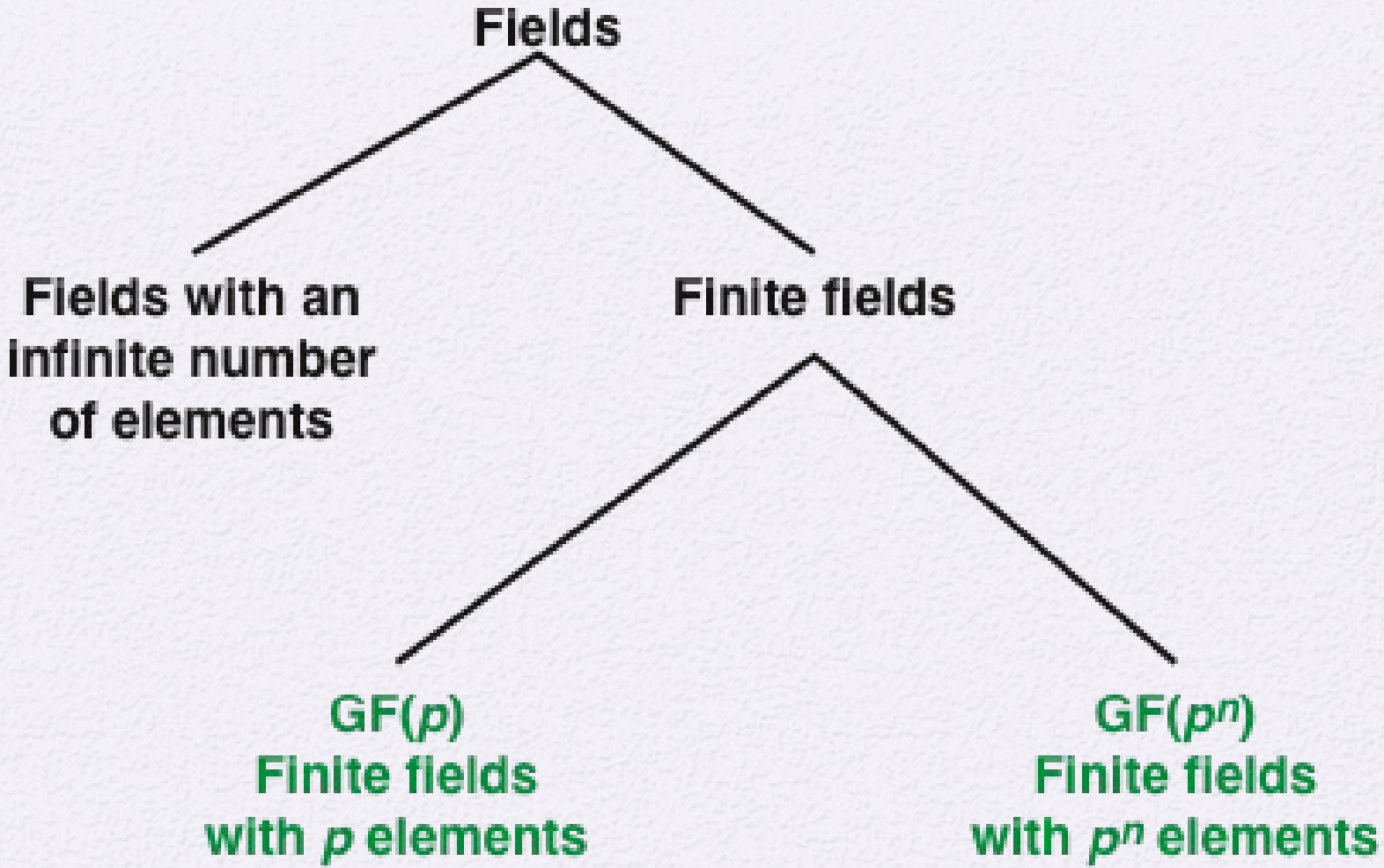


Figure 5.3 Types of Fields

Finite Fields of the Form GF(*p*)

- Finite fields play a crucial role in many cryptographic algorithms
- It can be shown that the order of a finite field must be a power of a prime p^n, where n is a positive integer
  - The finite field of order p^n is generally written GF(p^n)
  - GF stands for Galois field, in honor of the mathematician who first studied finite fields

Table 5.1(a)

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

Table 5.1(b)

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

Table 5.1(c)

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

Table 5.1(d)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(d) Addition modulo 7

Table 5.1(e)

×	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

(e) Multiplication modulo 7

Table 5.1(f)

w	$-w$	w^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

(f) Additive and multiplicative inverses modulo 7

have shown how to construct a finite field of order p, where p is prime.

GF(p) is defined with the following properties:

- 1. GF(p) consists of p elements
- 2. The binary operations + and * are defined over the set. The operations of addition, subtraction, multiplication, and division can be performed without leaving the set. Each element of the set other than 0 has a multiplicative inverse
- We have shown that the elements of GF(p) are the integers $\{0, 1, \ldots, p - 1\}$ and that the arithmetic operations are addition and multiplication mod p

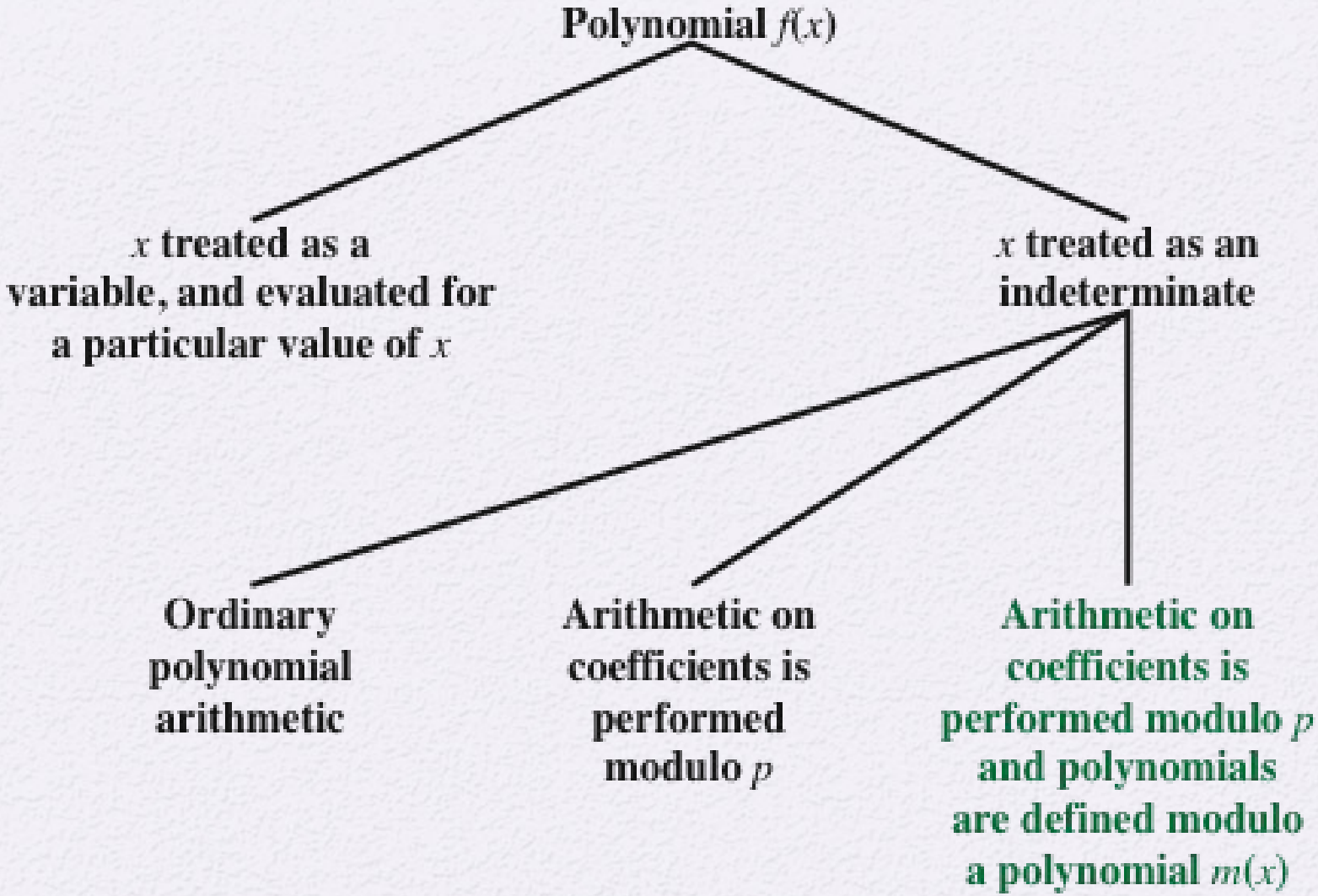
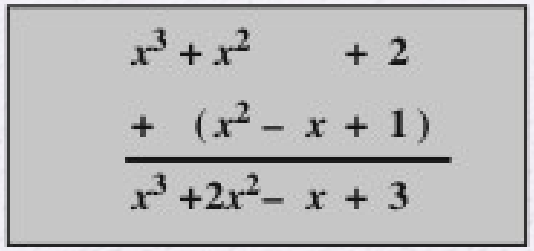
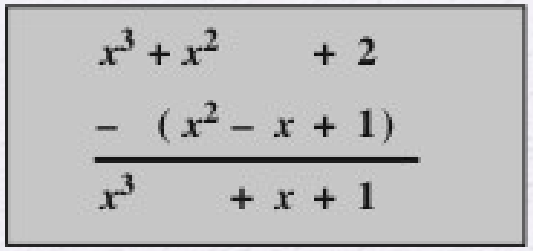


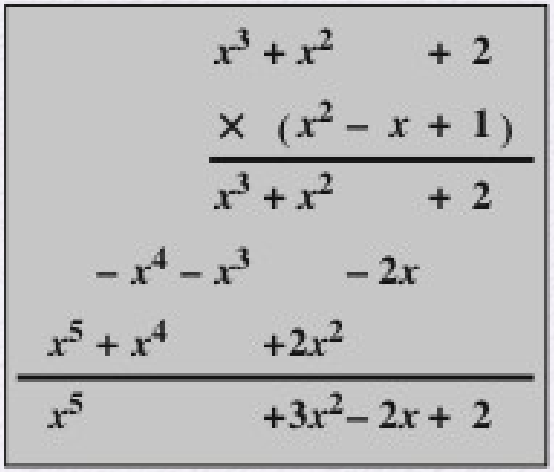
Figure 5.4 Treatment of Polynomials



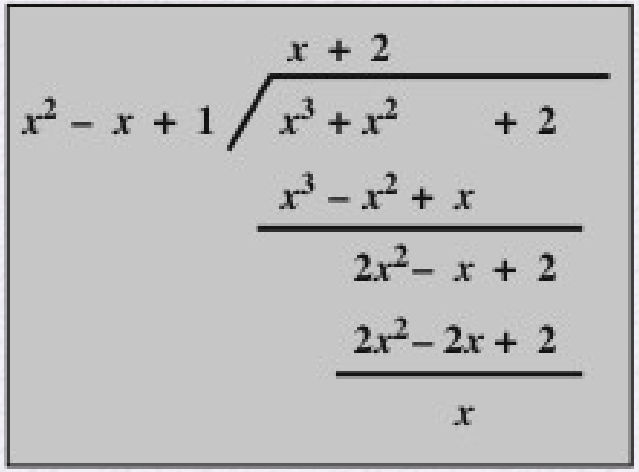
(a) Addition



(b) Subtraction



(c) Multiplication



(d) Division

Figure 5.5 Examples of Polynomial Arithmetic

Addition

Note

Addition and subtraction operations on polynomials are the same operation.

Polynomial Arithmetic With Coefficients in Z_p

- If each distinct polynomial is considered to be an element of the set, then that set is a ring
- When polynomial arithmetic is performed on polynomials over a field, then division is possible
  - Note: this does not mean that *exact division* is possible
- If we attempt to perform polynomial division over a coefficient set that is not a field, we find that division is not always defined
  - Even if the coefficient set is a field, polynomial division is not necessarily exact
  - With the understanding that remainders are allowed, we can say that polynomial division is possible if the coefficient set is a field

Polynomial Division

- We can write any polynomial in the form:

  $f(x) = q(x)\, g(x) + r(x)$

  - $r(x)$ can be interpreted as being a remainder
  - *So* $r(x) = f(x)$ mod $g(x)$

- If there is no remainder we can say $g(x)$ **divides** $f(x)$
  - Written as $g(x) \mid f(x)$
  - We can say that $g(x)$ is a **factor** of $f(x)$
  - *Or* g(x) is a **divisor** of $f(x)$

- A polynomial $f(x)$ over a field F is called **irreducible** if and only if $f(x)$ cannot be expressed as a product of two polynomials, both over F, and both of degree lower than that of $f(x)$
  - An irreducible polynomial is also called a **prime polynomial**

Example of Polynomial Arithmetic Over GF(2)

$$
\begin{array}{rrr}
x^7 & + x^5 + x^4 + x^3 & + x + 1 \\
 & + (x^3 & + x + 1) \\
\hline
x^7 & + x^5 + x^4 &
\end{array}
$$

(a) Addition

$$
\begin{array}{rrr}
x^7 & + x^5 + x^4 + x^3 & + x + 1 \\
 & - (x^3 & + x + 1) \\
\hline
x^7 & + x^5 + x^4 &
\end{array}
$$

(b) Subtraction

(Figure 5.6 can be found on page 129 in the t

Example of Polynomial Arithmetic Over GF(2)

$$
\begin{array}{rrrrrrrrrrr}
 & & & & x^7 & +x^5 & +x^4 & +x^3 & & +x & +1 \\
 & & & & & & & \times\,(x^3 & & +x & +1) \\
\hline
 & & & & x^7 & +x^5 & +x^4 & +x^3 & & +x & +1 \\
 & & & x^8 & & +x^6 & +x^5 & +x^4 & +x^2 & +x & \\
 & x^{10} & & +x^8 & +x^7 & +x^6 & & +x^4 & +x^3 & & \\
\hline
 & x^{10} & & & & & & +x^4 & +x^2 & & +1
\end{array}
$$

(c) Multiplication

$$
\begin{array}{r}
x^4 + 1 \\
\hline
x^3 + x + 1 \;\big/\; x^7 + x^5 + x^4 + x^3 + x + 1 \\
\quad x^7 + x^5 + x^4 \\
\hline
\qquad\qquad x^3 + x + 1 \\
\qquad\qquad x^3 + x + 1 \\
\hline
\end{array}
$$

(d) Division

(Figure 5.6 can be found on page 129 in the t

Polynomial GCD

- The polynomial *c(x)* is said to be the greatest common divisor of *a(x)* and *b(x)* if the following are true:
  - *c(x)* divides both *a(x)* and *b(x)*
  - Any divisor of *a(x)* and *b(x)* is a divisor of *c(x)*
- An equivalent definition is:
  - gcd*[a(x), b(x)]* is the polynomial of maximum degree that divides both *a(x)* and *b(x)*
- The Euclidean algorithm can be extended to find the greatest common divisor of two polynomials whose coefficients are elements of a field

Table 5.2(a) Arithmetic in GF(2^3)

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

Table 5.2(b) Arithmetic in GF(2^3)

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

Table 5.2(c)

Arithmetic in GF(2^3)

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses

Table 5.3
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

(Table is on page 136 in the textbook)

Table 5.3
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	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

(Table is on page 136 in the textbook)

$$(x^2 + x + 1)*(x^2 + x + 1)$$
$$= x^2 * (x^2 + x + 1) + x * (x^2 + x + 1) + (x^2 + x + 1)$$
$$= x^4 + x^3 + x^2$$
$$\quad\; x^3 + x^2 + x$$
$$\quad\quad\; x^2 + x + 1$$
$$= x^4 \quad + x^2 \quad + 1$$

$$\begin{array}{r|l} x^3 + x + 1 & x^4 + x^2 + 1 \\ & x^4 + x^2 + x \\ \hline & x + 1 \end{array}$$

$$(x^2 + 1)*(x^2 + 1)$$
$$= x^2 * (x^2 + 1) + (x^2 + 1)$$
$$= x^4 \quad + x^2$$
$$\quad\quad + x^2 \quad + 1$$
$$= x^4 \quad\quad + 1$$

$$\begin{array}{r|l} x^3 + x + 1 & x^4 + 1 \\ & x^4 + x^2 + x \\ \hline & x^2 + x + 1 \end{array}$$

Table 5.4

Extended Euclid [$(x^8 + x^4 + x^3 + x + 1), (x^7 + x + 1)$]

Initialization	$a(x) = x^8 + x^4 + x^3 + x + 1; v_{-1}(x) = 1; w_{-1}(x) = 0$ $b(x) = x^7 + x + 1; v_0(x) = 0; w_0(x) = 1$
Iteration 1	$q_1(x) = x; r_1(x) = x^4 + x^3 + x^2 + 1$ $v_1(x) = 1; w_1(x) = x$
Iteration 2	$q_2(x) = x^3 + x^2 + 1; r_2(x) = x$ $v_2(x) = x^3 + x^2 + 1; w_2(x) = x^4 + x^3 + x + 1$
Iteration 3	$q_3(x) = x^3 + x^2 + x; r_3(x) = 1$ $v_3(x) = x^6 + x^2 + x + 1; w_3(x) = x^7$
Iteration 4	$q_4(x) = x; r_4(x) = 0$ $v_4(x) = x^7 + x + 1; w_4(x) = x^8 + x^4 + x^3 + x + 1$
Result	$d(x) = r_3(x) = \gcd(a(x), b(x)) = 1$ $w(x) = w_3(x) = (x^7 + x + 1)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1) = x^7$

(Table 5.4 can be found on page 138 in textbook)

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

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

of the form

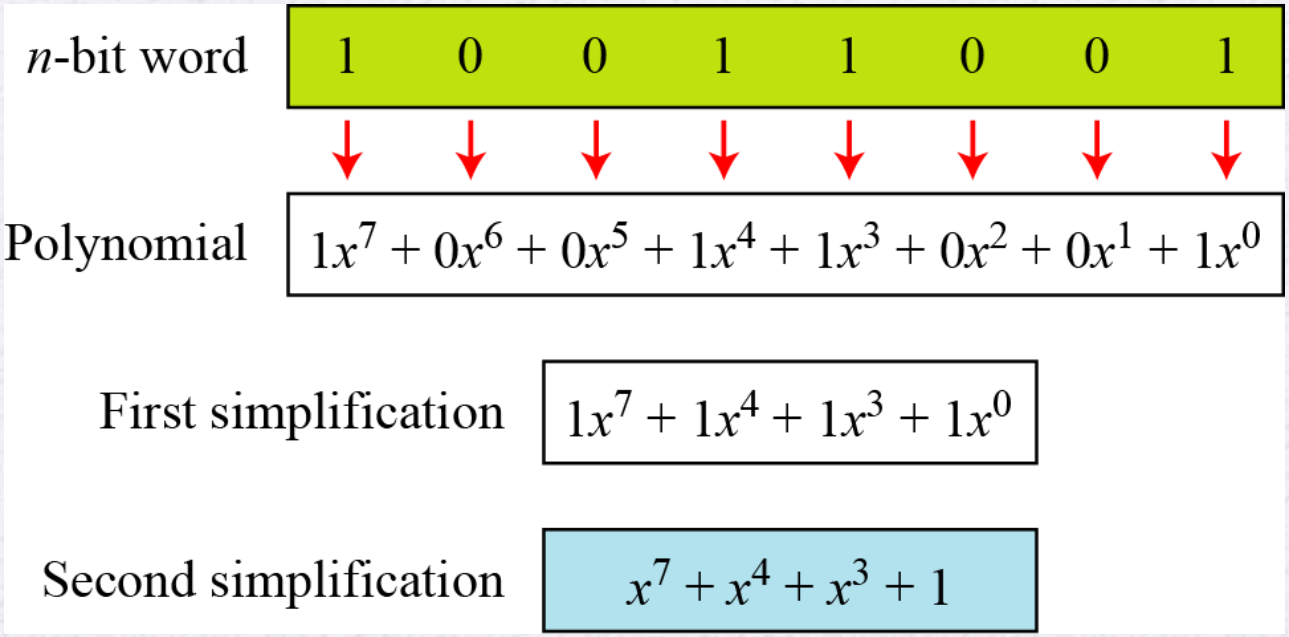
$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0$$

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

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*



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.

GF(2^n) Fields

Note

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

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

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:

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

4.2.1 Continued

Example 4.18

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

Multliplication

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.

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

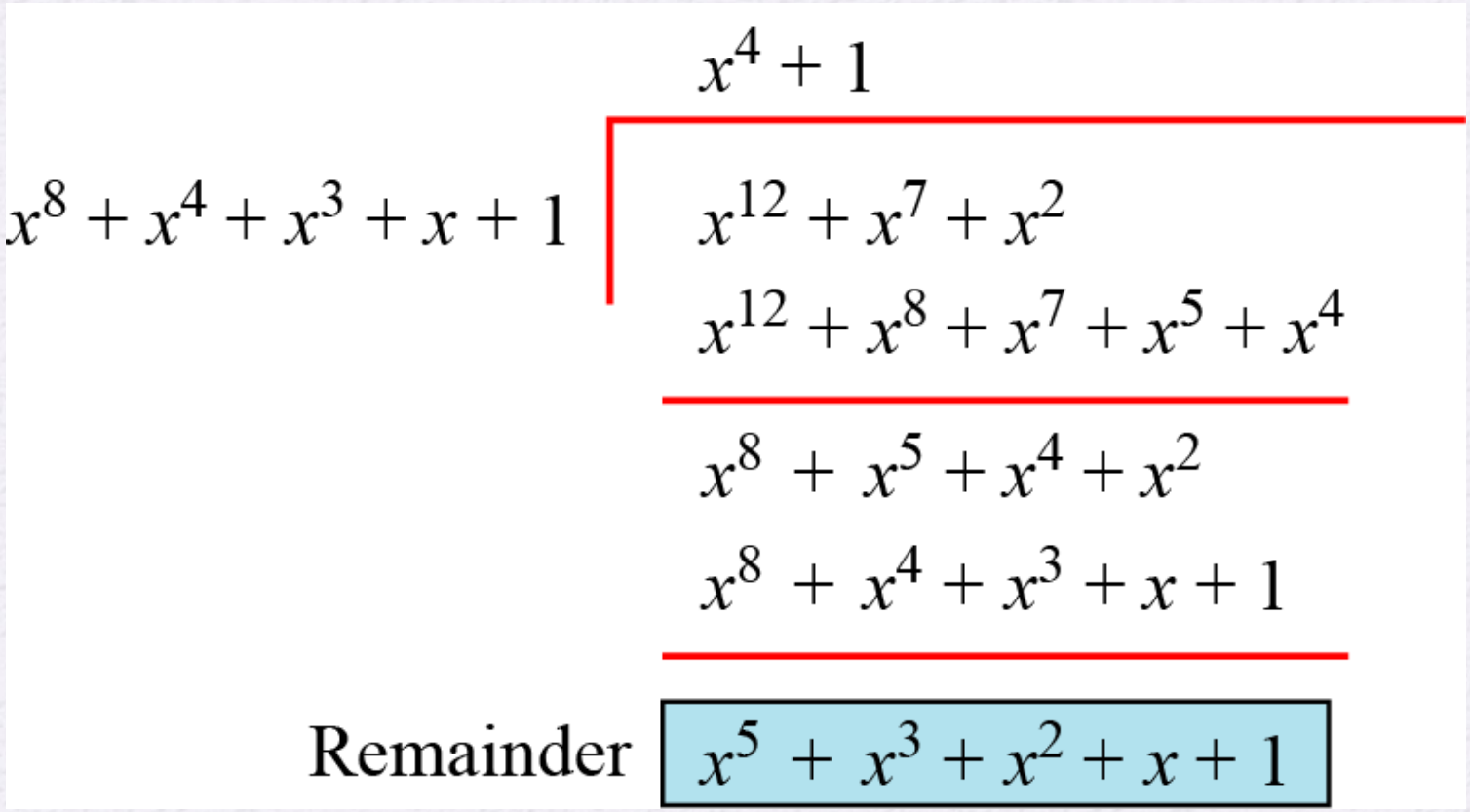
$$P_1 \otimes P_2 = x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x)$$

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

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

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.

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



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)	

4.2.1 Continued

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)	

Computational Considerations

- Since coefficients are 0 or 1, they can represent any such polynomial as a bit string
- Addition becomes XOR of these bit strings
- Multiplication is shift and XOR
  - cf long-hand multiplication
- Modulo reduction is done by repeatedly substituting highest power with remainder of irreducible

Using a Generator

- A **generator** *g* of a finite field F of order *q* (contains *q* elements) is an element whose first *q*-1 powers generate all the nonzero elements of F
  - The elements of F consist of 0, g^0, g^1, ..., g^{q-2}
- Consider a field F defined by a polynomial *fx*
  - An element b contained in F is called a **root** of the polynomial if *f(b) = 0*
- Finally, it can be shown that a root *g* of an irreducible polynomial is a generator of the finite field defined on that polynomial

Table 3.3

Generator for GF(2^3) using $x^3 + x + 1$

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	000	0
$g^0 (= g^7)$	1	001	1
g^1	g	010	2
g^2	g^2	100	4
g^3	$g + 1$	011	3
g^4	$g^2 + g$	110	6
g^5	$g^2 + g + 1$	111	7
g^6	$g^2 + 1$	101	5

Table 5.6

GF(2^3) Arithmetic Using Generator for the Polynomial ($x^3 + x + 1$)

	+	000 0	001 1	010 G	100 g^2	011 g^3	110 g^4	111 g^5	101 g^6
000	0	0	1	G	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1
001	1	1	0	$g+1$	g^2+1	g	g^2+g+1	g^2+g	g^2
010	g	g	$g+1$	0	g^2+g	1	g^2	g^2+1	g^2+g+1
100	g^2	g^2	g^2+1	g^2+g	0	g^2+g+1	g	$g+1$	1
011	g^3	$g+1$	g	1	g^2+g+1	0	g^2+1	g^2	g^2+g
110	g^4	g^2+g	g^2+g+1	g^2	g	g^2+1	0	1	$g+1$
111	g^5	g^2+g+1	g^2+g	g^2+1	$g+1$	g^2	1	0	g
101	g^6	g^2+1	g^2	g^2+g+1	1	g^2+g	$g+1$	g	0

(a) Addition

(Table is on page 142 in the textbook)

Table 5.6

GF(2^3) Arithmetic Using Generator for the Polynomial ($x^3 + x + 1$)

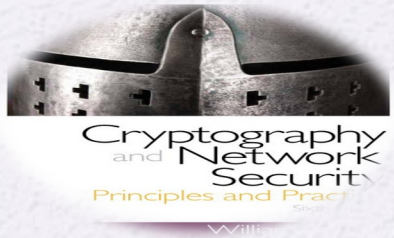
		000	001	010	100	011	110	111	101
	×	0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	0	0	0	0	0	0	0
001	1	0	1	G	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1
010	g	0	g	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1	1
100	g^2	0	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1	1	g
011	g^3	0	$g+1$	g^2+g	g^2+g+1	g^2+1	1	g	g^2
110	g^4	0	g^2+g	g^2+g+1	g^2+1	1	g	g^2	$g+1$
111	g^5	0	g^2+g+1	g^2+1	1	g	g^2	$g+1$	g^2+g
101	g^6	0	g^2+1	1	g	g^2	$g+1$	g^2+g	g^2+g+1

(b) Multiplication

(Table is on page 142 in the textbook)

Summary

- Distinguish among groups, rings, and fields
- Define finite fields of the form GF(*p)*
- Define finite fields of the form GF(2^n)



- Explain the differences among ordinary polynomial arithmetic, polynomial arithmetic with coefficients in $Z_{p,}$ and modular polynomial arithmetic in GF(2^n)
- Explain the two different uses of the mod operator