



Chapter 5

Finite Fields

Algebraic Structures

- In **abstract algebra**, an **algebraic structure** comprises the following three things:
 - A nonempty set of elements, **A**
 - A finite set of **operations** of finite arity that act on the elements of **A**
 - A finite set of **rules** or **axioms** that the operations must satisfy when operating on the elements of **A**
- Finite Fields are algebraic structures that are of great importance in Cryptography
- This module introduces finite fields
- However, as most algebraic structures are based on other algebraic structures we will also introduce Groups and Rings

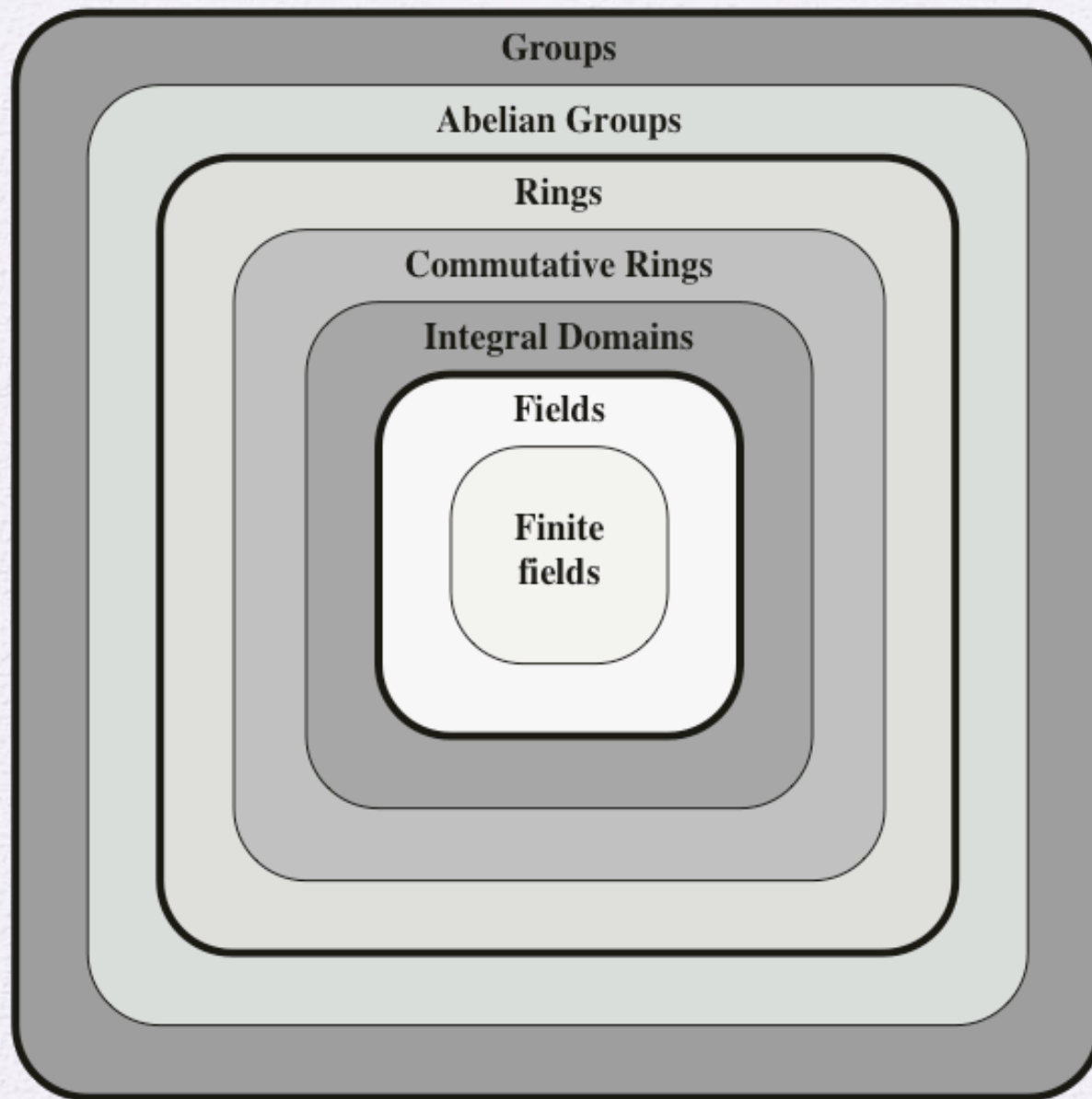


Figure 5.1 Groups, Rings, and Fields

Groups

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

If it is an **Abelian group**, it also satisfies A5.

 - (A5) Commutative:
 - $a \bullet b = b \bullet a$ for all a, b in G

Cyclic Group

- Exponentiation is defined within a group as a repeated application of **the group operator**, so that $a^3 = a \bullet a \bullet a$
- 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:

$$a(bc) = (ab)c \text{ for all } a, b, c \text{ in } R$$

(M3) Distributive laws:

$$a(b + c) = ab + ac \text{ for all } a, b, c \text{ in } R$$

$$(a + b)c = ac + bc \text{ for all } a, b, c \text{ in } R$$

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

Rings (cont.)

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

(M4) Commutativity of multiplication:

$$ab = ba \text{ for all } a, b \text{ in } R$$

- **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 the following rule: $a/b = a(b^{-1})$

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.

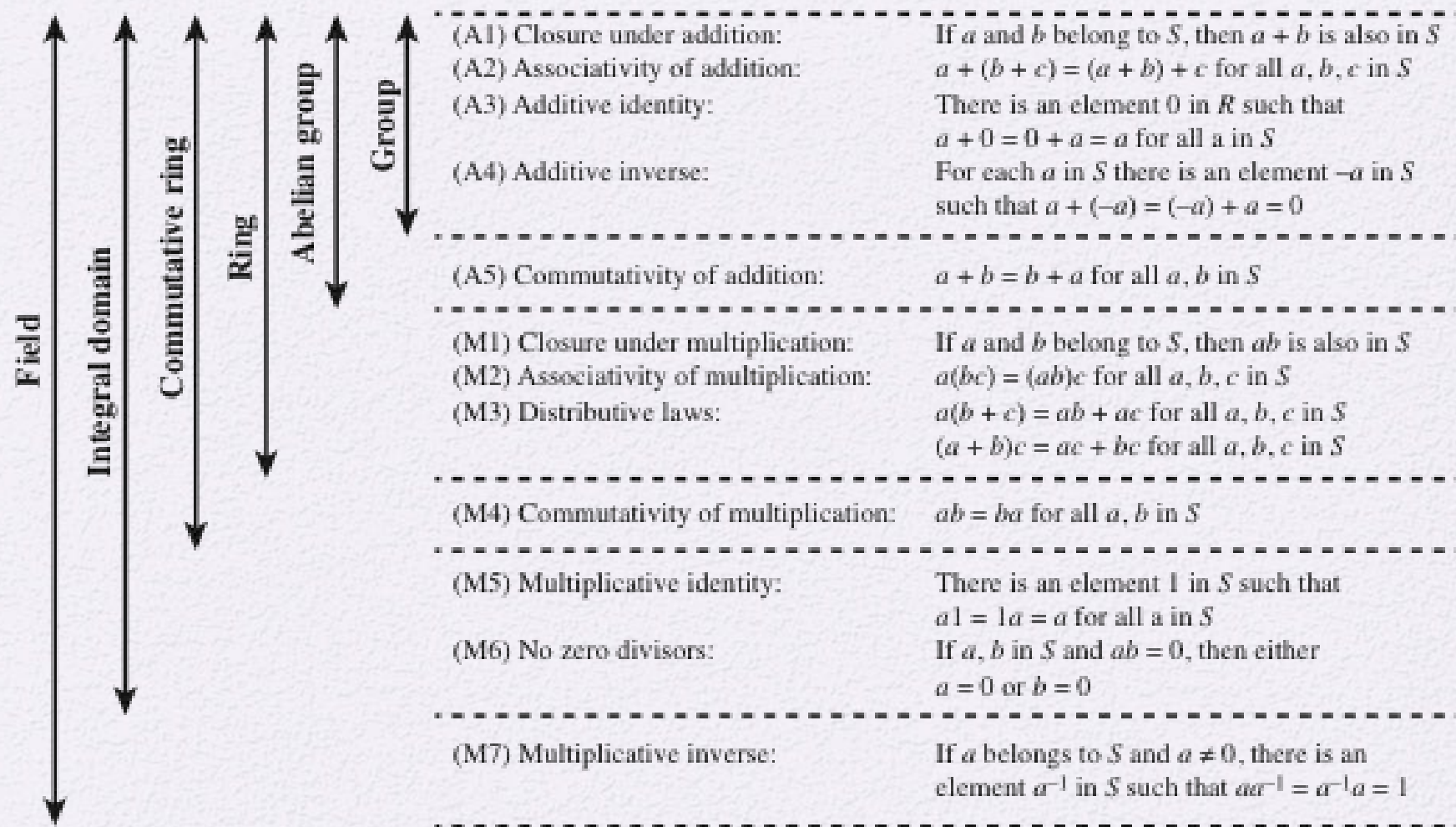


Figure 5.2 Properties of Groups, Rings, and Fields

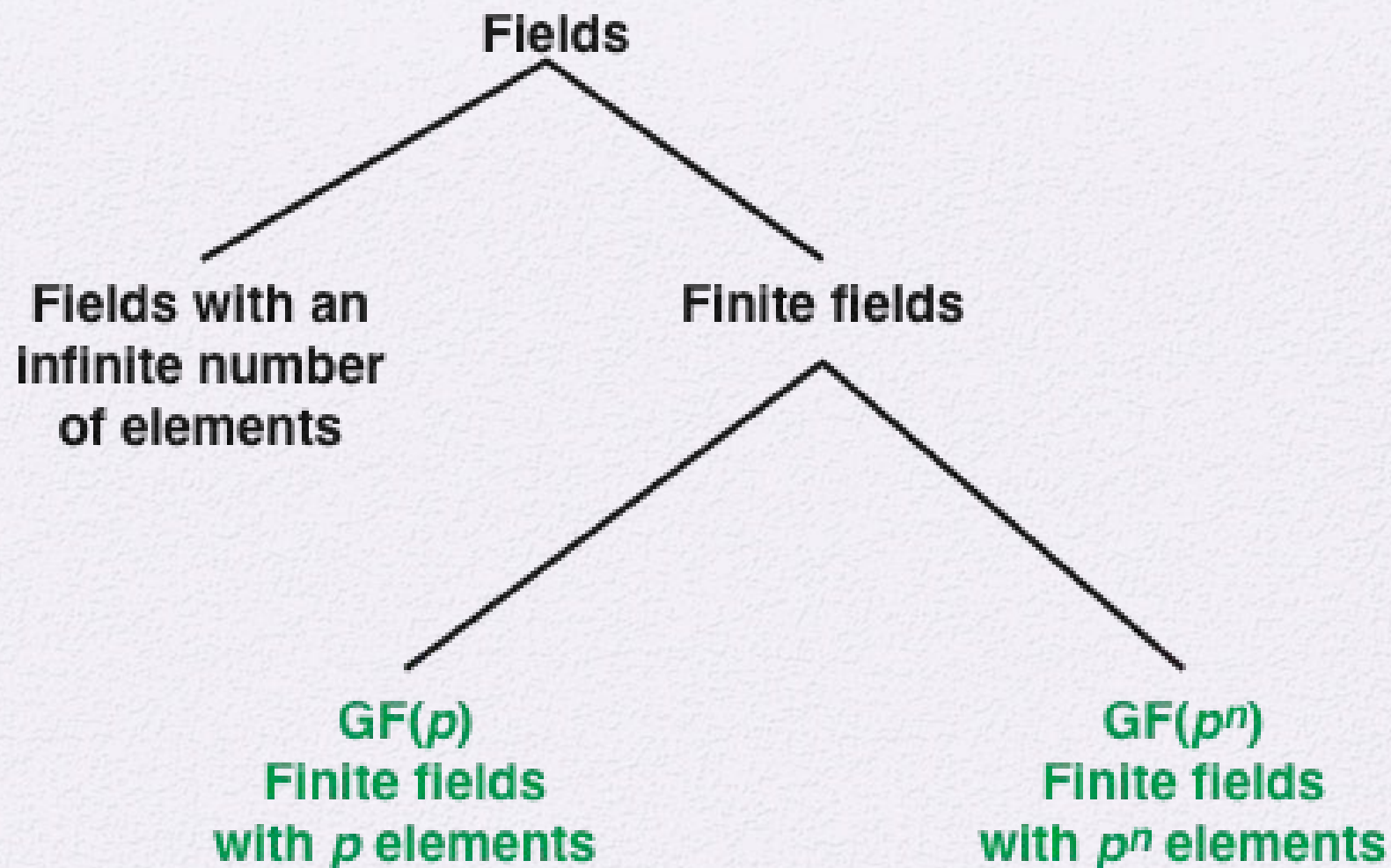


Figure 5.3 Types of Fields

Finite Fields of the Form $GF(p)$

- Finite fields play a crucial role in many cryptographic algorithms
- The order of a finite field is the number of elements in its set
- 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

Arithmetic Modulo 8

- Let's review the example from chapter 2 of arithmetic modulo 8
- Recall that arithmetic modulo 8 results in the inability to perform certain division operations
 - Due to the fact that not all elements of \mathbf{Z}_8 have multiplicative inverses
- This implies that arithmetic modulo 8 does not produce a finite field.

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)

x	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)

x	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

Arithmetic Modulo 7

- Arithmetic modulo 7 produces a finite field.
- All elements of \mathbf{Z}_7 have additive and multiplicative inverses. All elements of \mathbf{Z}_7 are relatively prime to 7
 - This is because 7 is a prime number.
- They create a finite field of form **GF(7)**
- Arithmetic modulo **p**, where p is a prime number produces a finite field of form **GF(p)**

In this section,
we 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 $\{0, 1, \dots, p - 1\}$ and that the arithmetic operations are addition and multiplication mod p

Finite Fields of the form $GF(2^n)$

- Finite fields of this form involve binary numbers
 - They are therefore easy to implement using computer algorithms
- The binary numbers in the set are treated as polynomials and the arithmetic is polynomial arithmetic
- We will look at the polynomial arithmetic required for finite fields of the form $GF(2^n)$ in the next few slides, starting with conventional polynomial arithmetic

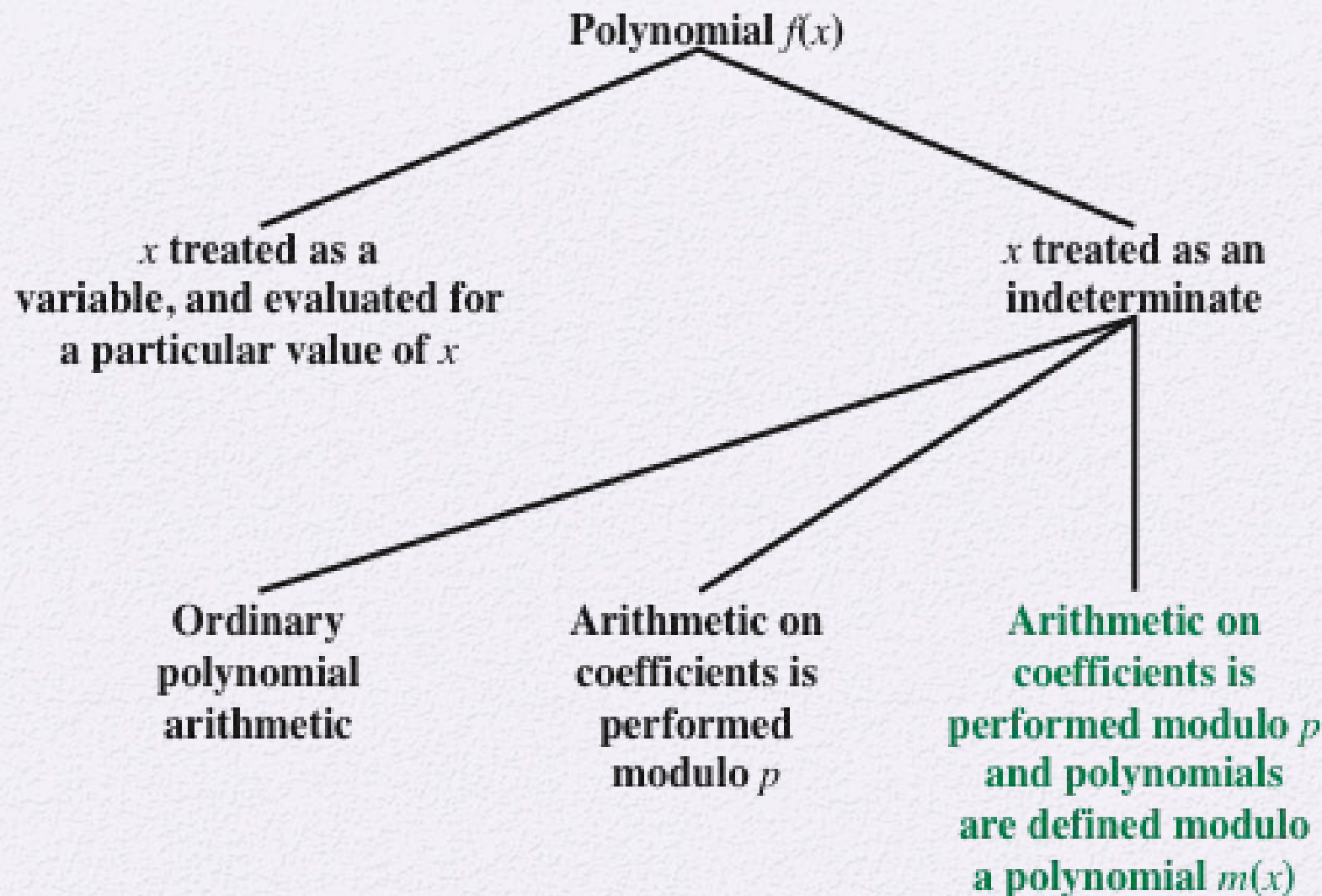


Figure 5.4 Treatment of Polynomials

Ordinary Polynomial Arithmetic:

$a_i \in \mathbb{R}$
 $f(x) = \underline{a_n}x^n + \underline{a_{n-1}}x^{n-1} + \dots + a_1x + a_0$

$\text{constant} = a_0$
 $d = n$ leading coefficient = a_n

$f(x) = 3x^3 + 5x^2 - 10x + 4$
 $d = 3$ constant = 4

$f(x) = x^3 + x^2 + 2$
 $g(x) = x^2 - x + 1$

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

$f(x) \cdot g(x) = (x^3 + x^2 + 2)(x^2 - x + 1) = x^5 - x^4 + x^3 + x^4 - x^3 + x^2 + 2x^2 - 2x + 2$
 $= x^5 + 3x^2 - 2x + 2$

$\frac{f(x)}{g(x)}$

$\frac{x^7}{x^2} = x^5$

$(x^2 - x + 1) \overline{) x^3 + x^2 + 2}$
 $\underline{x^3 - x^2 + x}$
 $\underline{2x^2 - x + 2}$
 $\underline{-2x^2 + 2x + 2}$
 \underline{x}

$4 \overline{) 15}$
 $\underline{12}$
 3
 $15 = 4 \cdot 3 + 3$

$(x^3 + x^2 + 2) = (x^2 - x + 1)(x + 2) + x$

$f(x)$ $g(x)$ $q(x)$ $r(x)$
 $d = n$ $d = m$ $d = n - m$ $0 \leq d \leq m - 1$

if $r(x) = 0$ $g(x) | f(x)$ $f(x) = g(x)q(x)$ $g(x)$ Factor of $f(x)$

if $a_i \in \frac{\mathbb{I}}{2}$

$\frac{3}{2}x$
 $2x + 1 \overline{) 3x^2 - 1}$
 $\underline{3x^2 + \frac{3}{2}x}$

$(\mathbb{I}, +, *)$

**Ordinary
Polynomial
Arithmetic:**

$$\begin{array}{r} x^3 + x^2 \quad + 2 \\ + (x^2 - x + 1) \\ \hline x^3 + 2x^2 - x + 3 \end{array}$$

(a) Addition

$$\begin{array}{r} x^3 + x^2 \quad + 2 \\ - (x^2 - x + 1) \\ \hline x^3 \quad + x + 1 \end{array}$$

(b) Subtraction

$$\begin{array}{r} x^3 + x^2 \quad + 2 \\ \times (x^2 - x + 1) \\ \hline x^3 + x^2 \quad + 2 \\ - x^4 - x^3 \quad - 2x \\ \hline x^5 + x^4 \quad + 2x^2 \\ \hline x^5 \quad + 3x^2 - 2x + 2 \end{array}$$

(c) Multiplication

$$\begin{array}{r} x + 2 \\ x^2 - x + 1 \overline{) x^3 + x^2 \quad + 2} \\ \underline{x^3 - x^2 + x} \\ 2x^2 - x + 2 \\ \underline{2x^2 - 2x + 2} \\ x \end{array}$$

(d) Division

Figure 5.5 Examples of Polynomial Arithmetic

As an example, let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$, where S is the set of integers. Then

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

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

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

Figures 5.5a through 5.5c show the manual calculations. We comment on division subsequently.

Polynomial Arithmetic With Coefficients in \mathbb{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 $r(x) = f(x) \bmod g(x)$
- 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**

polynomials over \mathbb{Z}_p : The coefficients are from \mathbb{Z}_p

$$\text{GF}(2) = \mathbb{Z}_2$$

polynomials over $\text{GF}(2)$: The coefficients $a_i \in \{0, 1\}$

$$\text{Ex: } x+1$$

$$x^2+x+1$$

$$x^3+1$$

$$x^{1000}+x+1$$

Ex: Addition in \mathbb{Z}_3 : $a_i \in \{0, 1, 2\}$

$$2x^2+1$$

$$+ x^2+2x$$

$$\hline 3x^2+2x+1 \rightarrow 2x+1$$

$$5x^3+4x+1 \rightarrow 2x^3+x+1$$

The set of polynomials over \mathbb{Z}_p forms a ring.

Example of Polynomial Arithmetic with Coefficients in GF(2)

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

(a) Addition

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

(b) Subtraction

Example of Polynomial Arithmetic with Coefficients in GF(2)

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

(c) Multiplication

$$\begin{array}{r}
 \begin{array}{r}
 x^4 + 1 \\
 \hline
 x^3 + x + 1 \overline{) x^7 \quad + x^5 + x^4 + x^3 \quad + x + 1} \\
 \underline{x^7 \quad + x^5 + x^4} \\
 x^3 \quad + x + 1 \\
 \underline{x^3 \quad + x + 1} \\
 0
 \end{array}
 \end{array}$$

(d) Division

Arithmetic in $GF(2^n)$

- Please note a prime polynomial is needed to complete some of the arithmetic operations in finite fields of type **$GF(2^n)$**
- When the result of an operation goes outside of the range of acceptable values, it is divided by the prime polynomial and the remainder value of the division operation is taken as the answer
- The prime polynomial chosen must of the same order as **n**
- For the examples in the proceeding slides the prime polynomial used is **$(x^3 + x + 1)$**

$f(x)$ over $GF(2^n)$ mod $m(x)$

$$a_i \in \{0, 1\} \quad d = n-1 \quad a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_0$$

$= (a_{n-1}, a_{n-2}, \dots, a_0) \rightarrow$ binary string

$$\begin{array}{c} 0 \ 1 \ 1 \\ \downarrow \ \downarrow \ \downarrow \\ a_2 \ a_1 \ a_0 \end{array} \quad 0x^2 + x + 1 = x + 1$$

$m(x)$ is a prime polynomial \rightarrow cannot be factored

Ex: 8 polynomials in $GF(2^3)$ mod $x^3 + x + 1$:

0	\longrightarrow	000	
1	\longrightarrow	001	
x	\longrightarrow	010	
$x+1$	\longrightarrow	100	
x^2	\longrightarrow	011	\longrightarrow represented by bit string
x^2+1	\longrightarrow	101	
x^2+x	\longrightarrow	110	
x^2+x+1	\longrightarrow	111	

The set of polynomials over $GF(2^n)$ on mod $m(x)$

where $m(x)$ is prime polynomial degree n forms a field.

Arithmetic in $GF(2^3)$

		000	001	010	011	100	101	110	111
	+	0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

(a) Addition

Arithmetic in $GF(2^3)$

		000	001	010	011	100	101	110	111
	\times	0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

(b) Multiplication

Table 5.2(c)

Arithmetic
in $GF(2^3)$

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

(c) Additive and multiplicative inverses

Addition in $GF(2^3)$: bitwise XOR

$$4 \rightarrow 100$$

$$7 \rightarrow 111$$

$$1 \oplus 1 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$0 \oplus 0 = 0$$

$$7 + 4 = 111 \oplus 100 = 011 = 3$$

$$100 \rightarrow x^2$$

$$111 \rightarrow x^2 + x + 1$$

$$a_i \in \mathbb{Z}_2$$

$$100 \oplus 111 = (x^2) + (x^2 + x + 1) = 2x^2 + x + 1 \xrightarrow{a_i \in \mathbb{Z}_2} x + 1 \rightarrow 011$$

Additive inverse:

each element is the inverse of itself.

$$a_i \in \mathbb{Z}_2$$

$$101 \oplus 101 = 000$$

$$x^3 + 1 + x^3 + 1 = 2x^3 + 2 \xrightarrow{a_i \in \mathbb{Z}_2} 0$$

Multiplication in $GF(2^3)$ mod $x^3 + x + 1$

$$\hookrightarrow x^3 = x + 1$$

$$4 \rightarrow 100$$

$$7 \rightarrow 111$$

$$100 : x^2$$

$$111 : x^2 + x + 1$$

$$\begin{array}{r} x \ 111 \\ 100 \\ \hline 000 \\ \oplus \ 111 \\ \hline 11100 \end{array}$$

$$\begin{aligned} &\rightarrow x^4 + x^3 + x^2 = x(x+1) + (x+1) + x^2 \\ &= x^2 + x + x + 1 + x^2 \\ &= 2x^2 + 2x + 1 \\ &= 1 \pmod{x^3 + x + 1} \text{ over } \end{aligned}$$

Thus 100 is the inverse of 111.

OR x^2 is the inverse of $x^2 + x + 1$

Table 5.3

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

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

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 polynomial (also shift and XOR)

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