Finite Fields

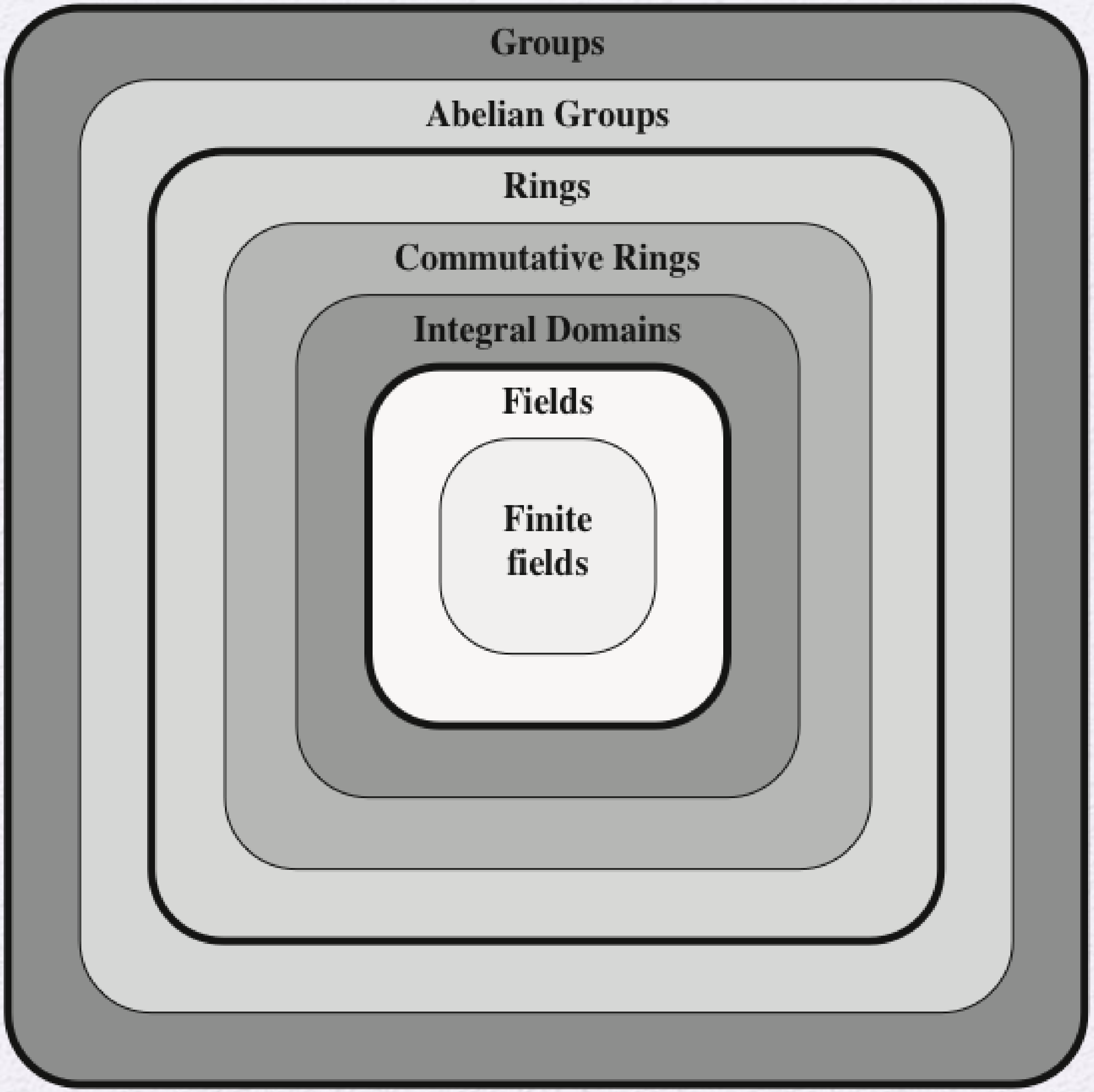


Figure 5.1 Groups, Rings, and Fields

Groups

- A set of elements **with a binary operation** denoted by • 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 $a \bullet a^1 = a^1 \bullet a = e$
  - (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 $a^{-n} = (a')^n$, where a' 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**

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)

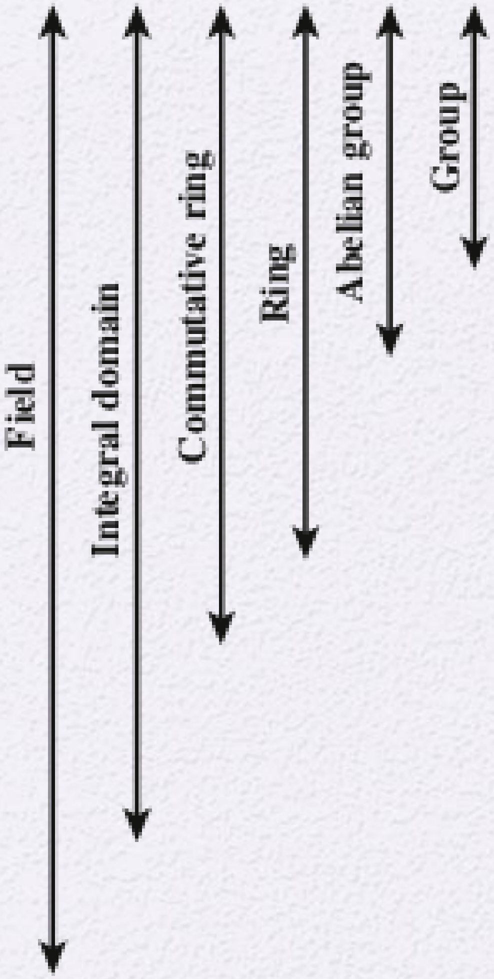
  F is an **integral domain**; that is, *F* satisfies axioms A1 through A5 and M1 through M6

  (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 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.



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Figure 5.2 Properties of Groups, Rings, and Fields

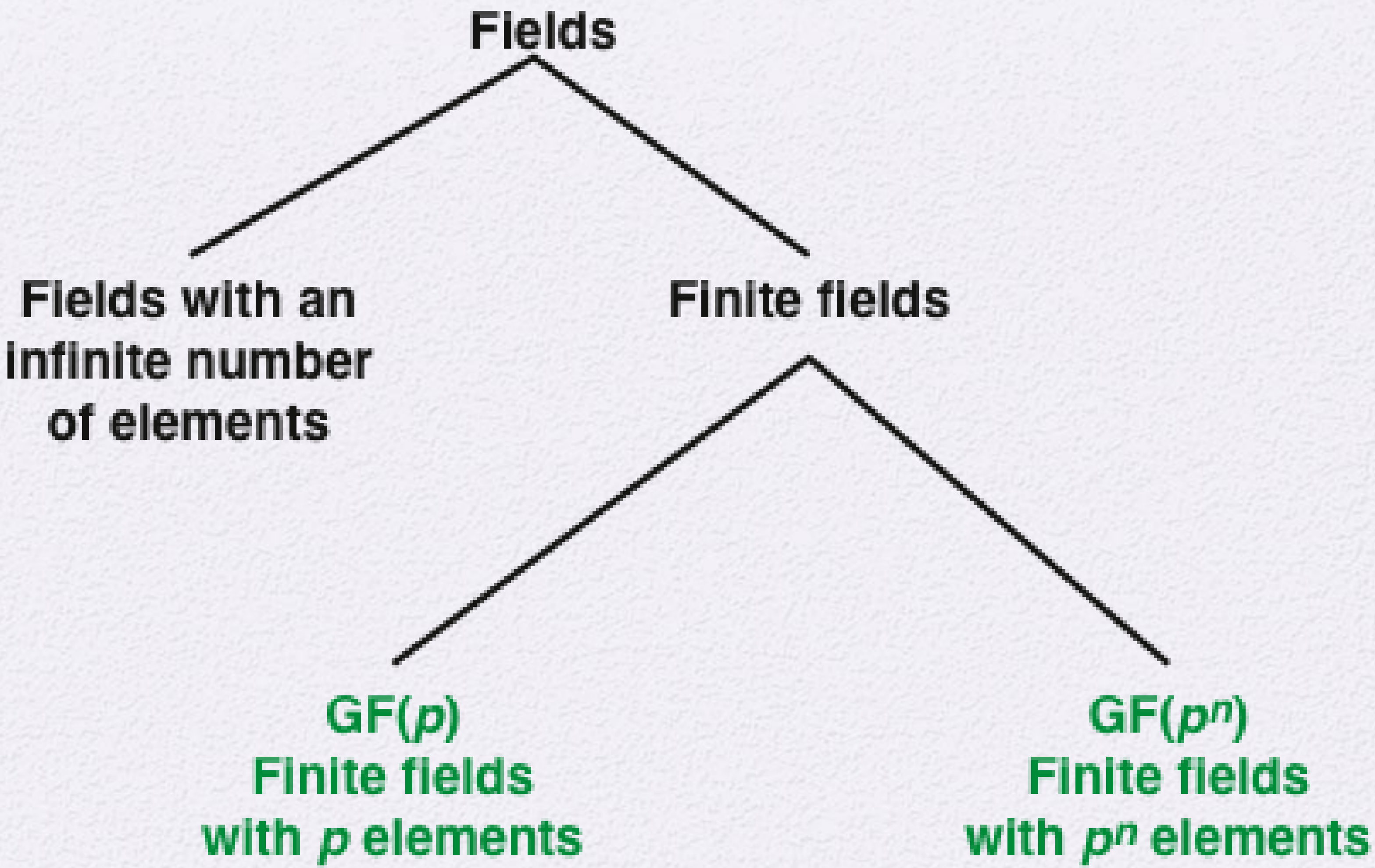


Figure 5.3 Types of Fields

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

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, . . . , $p - 1$} and that the arithmetic operations are addition and multiplication mod *p*

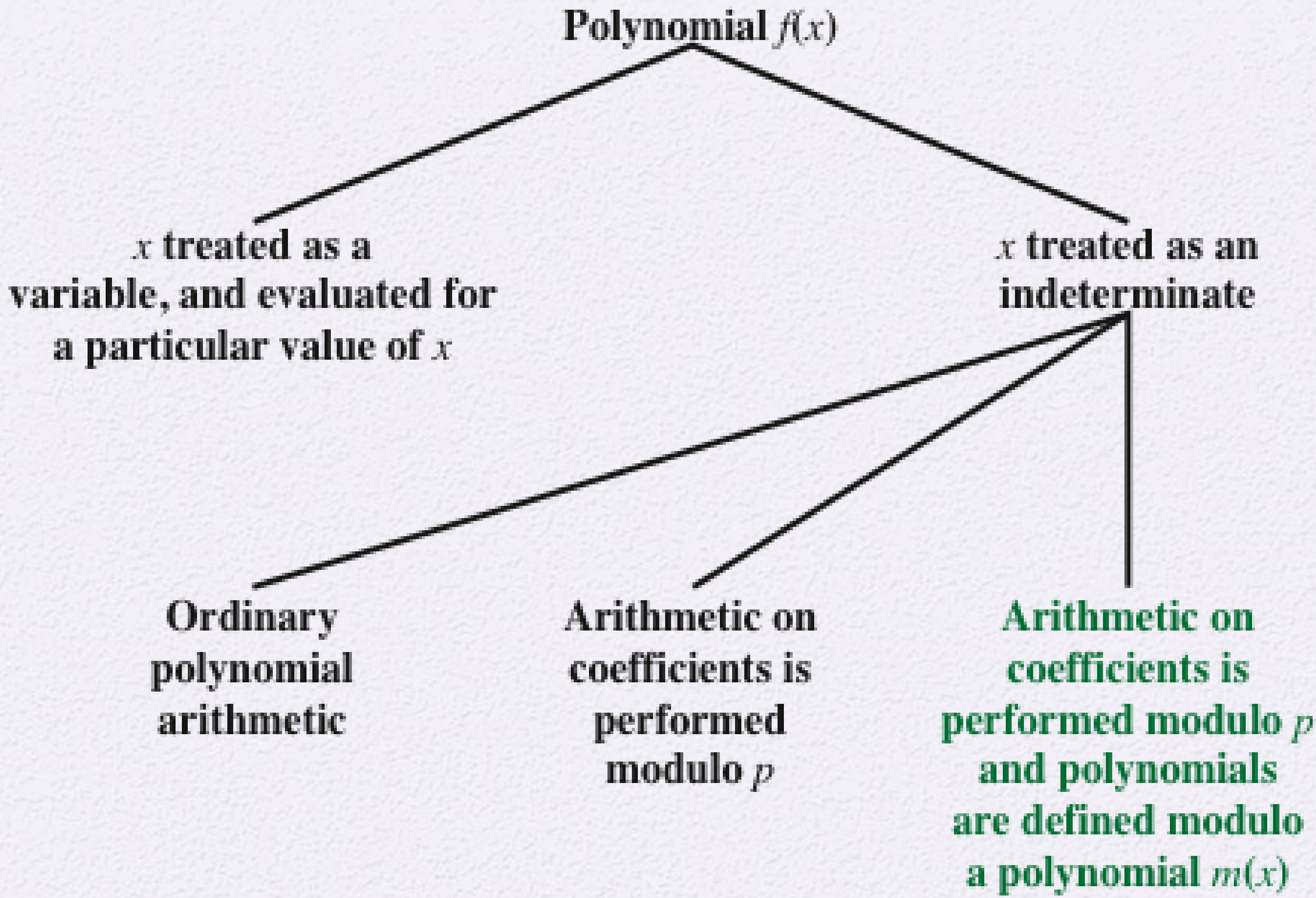


Figure 5.4 Treatment of Polynomials

$$\begin{array}{rrrrr}
 & x^3 & +\,x^2 & & +\,2 \\
+ & (& x^2 & -\,x & +\,1) \\ \hline
 & x^3 & +2x^2 & -\,x & +\,3
\end{array}$$

(a) Addition

$$\begin{array}{rrrrr}
 & x^3 & +\,x^2 & & +\,2 \\
- & (& x^2 & -\,x & +\,1) \\ \hline
 & x^3 & & +\,x & +\,1
\end{array}$$

(b) Subtraction

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

(c) Multiplication

$$\begin{array}{r|rrrr}
 & & & x & +\,2 \\ \cline{2-5}
x^2 - x + 1 & x^3 & +\,x^2 & & +\,2 \\
 & x^3 & -\,x^2 & +\,x & \\ \cline{2-5}
 & & 2x^2 & -\,x & +\,2 \\
 & & 2x^2 & -\,2x & +\,2 \\ \cline{3-5}
 & & & x &
\end{array}$$

(d) Division

Figure 5.5 Examples of Polynomial Arithmetic

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 $r(x) = f(x) \bmod g(x)$

- 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**

Example of Polynomial Arithmetic Over GF(2)

(Figure 5.6 can be found on page 137 in the textbook)

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\hline
x^3 + x + 1 & x^7 + x^5 + x^4 + x^3 + x + 1 \\
 & x^7 + x^5 + x^4 \\
\cline{2-2}
 & \qquad\qquad x^3 + x + 1 \\
 & \qquad\qquad x^3 + x + 1 \\
\cline{2-2}
\end{array}
$$

(d) Division

Figure 5.6 Examples of Polynomial Arithmetic over GF(2)

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)

		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

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

		000	001	010	011	100	101	110	111
	×	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

Table 5.3 (page 144 in textbook)

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

		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	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 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	$q_4(x) = \mathrm{x}$; $r_4(x) = 0$ $v_4(x) = x^7 + x + 1$; $w_4(x) = x^8 + x^4 + x^3 + x + 1$
Result	$d(x) = r_3(x) = \gcd(a(x), b(x)) = 1$ $\mathrm{w}(x) = w_3(x) = (x^7 + x + 1)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1) = x^7$

(Table 5.4 can be found on page 146 in 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)

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 5.5

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 (page 150 in textbook)

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	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

		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

Summary

- Groups
  - Abelian group
  - Cyclic group
- Finite fields of the form GF(p)
  - Finite fields of Order p
  - Finding the multiplicative inverse in GF(p)
- Polynomial arithmetic
  - Ordinary polynomial arithmetic
  - Polynomial arithmetic with coefficients in Z_p
  - Finding the greatest common divisor

- Rings
- fields
- Finite fields of the form GF(2^n)
  - Motivation
  - Modular polynomial arithmetic
  - Finding the multiplicative inverse
  - Computational considerations
  - Using a generator