Chapter 5

Finite Fields

1

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 ***axiom***s 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

2

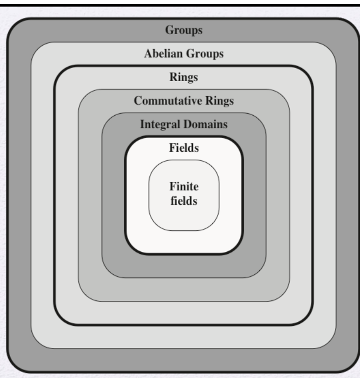


Figure 5.1 Groups, Rings, and Fields

3

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

4

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

6

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 $b = 0$

7

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

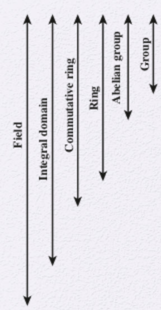
  (M7) Multiplicative inverse:

  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.

8



(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

9

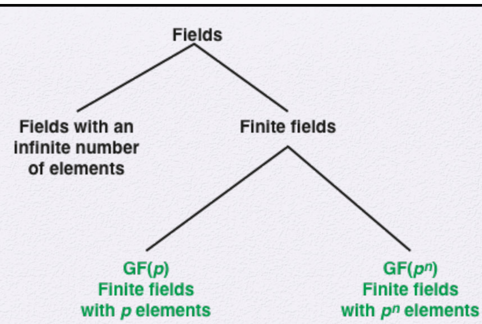


Figure 5.3 Types of Fields

10

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

11

Arithmetic Modulo 8

- Let's review the example from module 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 Z_8 have multiplicative inverses
- This implies that arithmetic modulo 8 does not produce a finite field

12

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

13

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

14

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

15

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

16

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

17

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

18

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)***

19

Table 5.1 Arithmetic Modulo 8 and Modulo 7

+	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

×	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

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

(c) Additive and multiplicative inverses modulo 8

+	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

×	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

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

(f) Additive and multiplicative inverses modulo 7

20

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

21

Finite Fields of the form *GF(2ⁿ)*

- 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

22

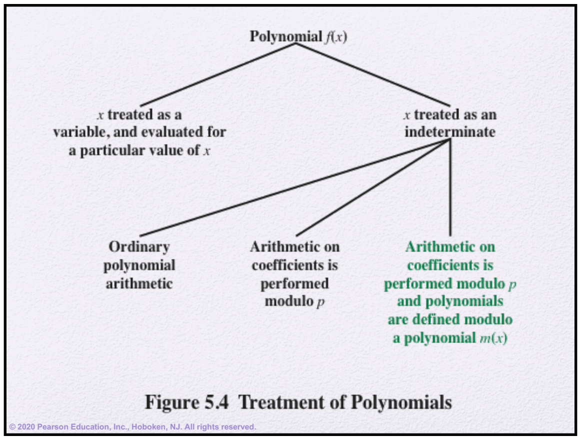


Figure 5.4 Treatment of Polynomials

23

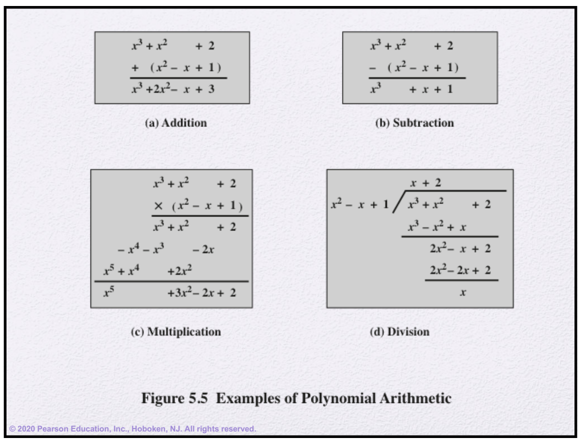


Figure 5.5 Examples of Polynomial Arithmetic

24

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

25

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**

26

Example of Polynomial Arithmetic with Coefficients in GF(2)

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

(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

(Figure 5.6 can be found on page 129 in the textbook)

27

Example of Polynomial Arithmetic with Coefficients in GF(2)

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

(c) Multiplication

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

(d) Division

(Figure 5.6 can be found on page 129 in the textbook)

28

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 **($x^3 + x + 1$)**

29

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

30

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

31

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

32

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)

33

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	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)

34

Arithmetic in GF(2^n)

- The ***Advanced Encryption Standard (AES)*** utilizes arithmetic in the finite field ***GF(2^8)***
- The prime polynomial chose by the designers, and it is in used is:
  - ($x^8 + x^4 + x^3 + x + 1$)

35

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)

36

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

37