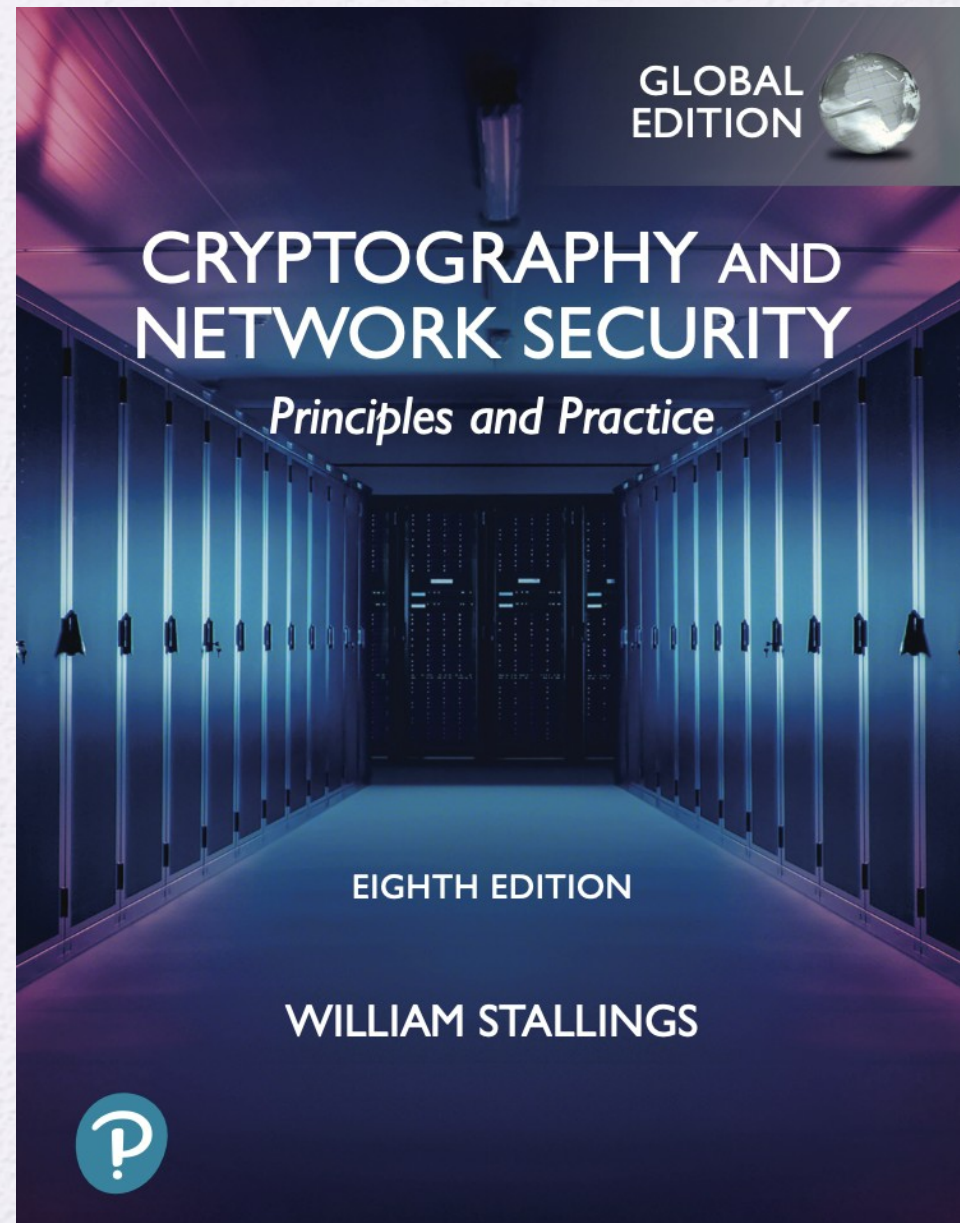


University of Nevada – Reno
Computer Science &
Engineering Department

CS454/654 Reliability and
Security of Computing
Systems - Fall 2024

Lecture 6

Dr. Batyr Charyyev
bcharyyev.com



FINITE FIELDS

5.1 Groups

- Groups
- Abelian Group
- Cyclic Group

5.2 Rings

5.3 Fields

5.4 Finite Fields of the Form $\text{GF}(p)$

- Finite Fields of Order p
- Finding the Multiplicative Inverse in $\text{GF}(p)$
- Summary

5.5 Polynomial Arithmetic

- Ordinary Polynomial Arithmetic
- Polynomial Arithmetic with Coefficients in \mathbb{Z}_p
- Finding the Greatest Common Divisor
- Summary

5.6 Finite Fields of the Form $\text{GF}(2^n)$

- Motivation
- Modular Polynomial Arithmetic
- Finding the Multiplicative Inverse
- Computational Considerations
- Using a Generator
- Summary

5.7 Key Terms, Review Questions, and Problems

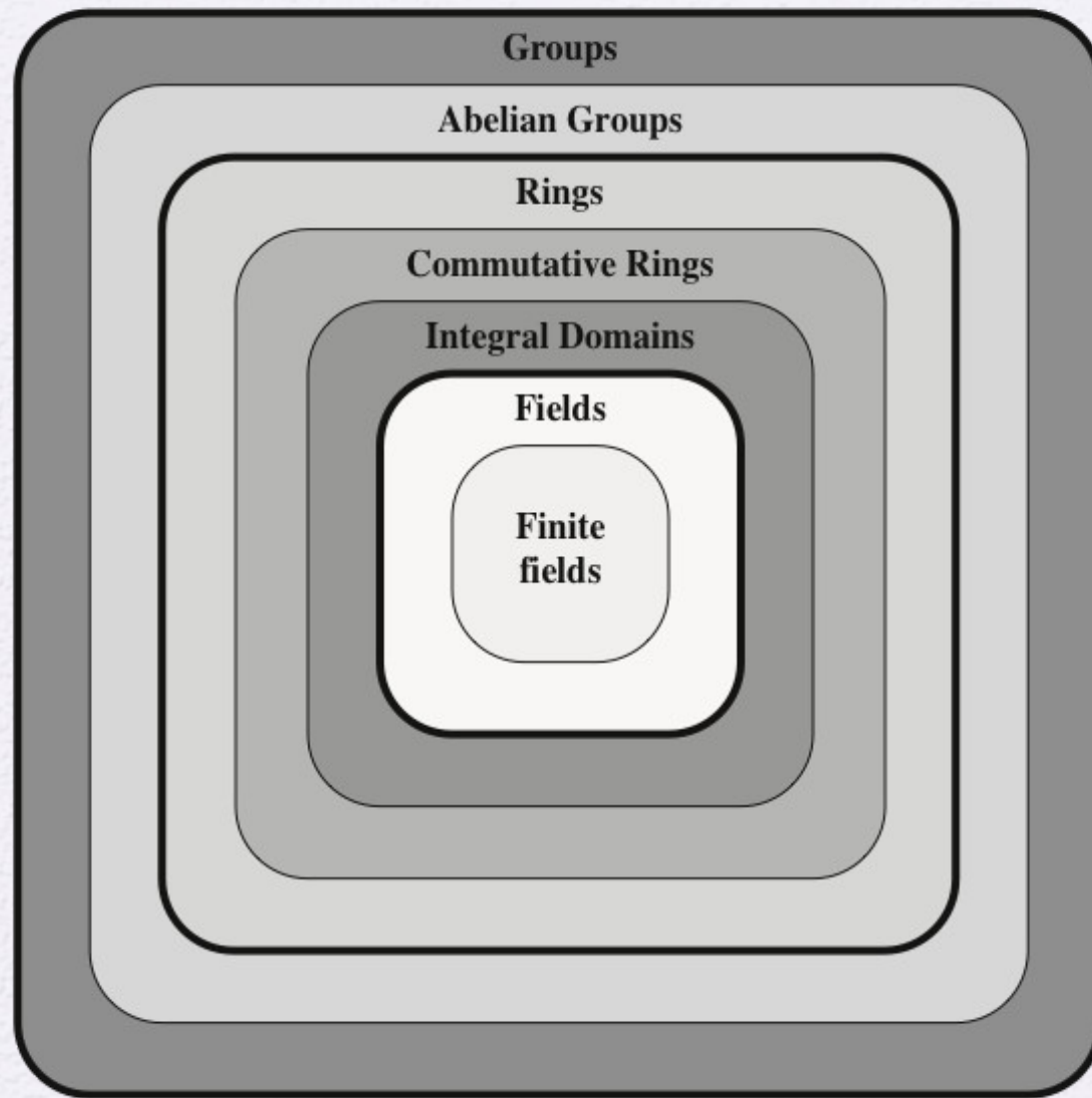


Figure 5.1 Groups, Rings, and Fields

Each successive subset (abelian group, ring, commutative ring, and so on) adds additional properties and is **thus**

Groups

- A group G is a set, together with binary operation $*$.
- $*$ often called multiplication but it can be any operation like addition.
- $*$ combines any element a and b to form $c=a*b$
- Group G must satisfy following properties.
 - (A1) Closure: If a and b belong to G , then $a*b$ is also in G
 - (A2) Associative: $a*(b*c) = (a*b)*c$ for all a, b, c in G
 - (A3) Identity element:
 - There is an element e in G such that $a+e = e+a = a$ for all a in G
 - (A4) Inverse element:
 - For each a in G , there is an element a^1 in G such that $a+a^1 = a^1 + a = e$

- Set of Integers (\mathbb{Z}) along with addition operation forms a group.
- The set consist of all integers $\mathbb{Z}=\{\dots,-2,-1,0,1,2,\dots\}$
- (A1) Closure –holds
 - If a and b belong to G , then $a + b$ is also in G
- (A2) Associative - holds
 - $a + (b+c) = (a+b)+c$ for all a, b, c in G
- (A3) Identity element - holds
 - There is an element e in G such that $a+ e = e+a = a$ for all a in G ,
 $e=0$
- (A4) Inverse element - holds
 - For each a in G , there is an element a^1 in G such that $a+a^1 = a^1 + a = e$
 - $7+(-7)=(-7)+7=0$

- Set of Natural Numbers (N) along with addition operation **doesn't form** a group.
- The set consist of integers $N=\{1,2,\dots\}$
- (A1) Closure –holds
 - If a and b belong to G , then $a + b$ is also in G
- (A2) Associative - holds
 - $a + (b+c) = (a+b)+c$ for all a, b, c in G
- (A3) Identity element – **doesn't hold**
 - There is an element e in G such that $a+ e = e+a = a$ for all a in G
- (A4) Inverse element - **doesn't hold**
 - For each a in G , there is an element a^1 in G such that $a+a^1 = a^1 + a = e$

Abelian Group

- (A1) Closure: If a and b belong to G , then $a \cdot b$ is also in G
- (A2) Associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c in G
- (A3) Identity element:
 - There is an element e in G such that $a \cdot e = e \cdot a = a$ for all a in G
- (A4) Inverse element:
 - For each a in G , there is an element a^{-1} in G such that $a \cdot a^{-1} = a^{-1} \cdot a = e$
- (A5) Commutative: $a \cdot b = b \cdot a$ for all a, b in G

- Set of Integers (\mathbb{Z}) along with addition operation forms a group.
- The set consist of all integers $\mathbb{Z}=\{\dots,-2,-1,0,1,2,\dots\}$
- (A1) Closure –holds
 - If a and b belong to G , then $a + b$ is also in G
- (A2) Associative - holds
 - $a + (b+c) = (a+b)+c$ for all a, b, c in G
- (A3) Identity element - holds
 - There is an element e in G such that $a+ e = e+a = a$ for all a in G ,
 $e=0$
- (A4) Inverse element - holds
 - For each a in G , there is an element a^1 in G such that $a+a^1 = a^1 + a = e$
 - $7+(-7)=(-7)+7=0$
- (A5) Commutative - holds

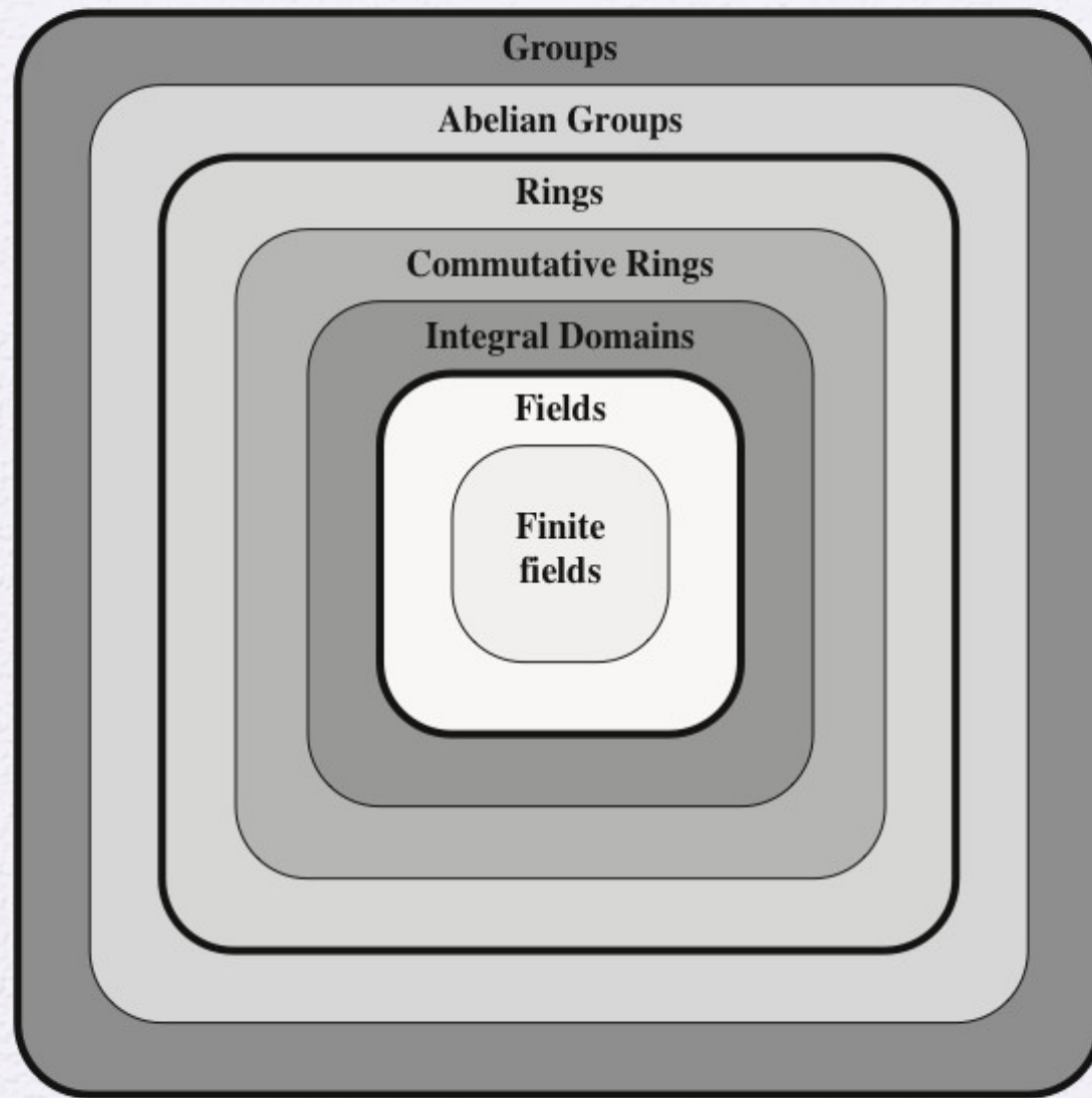


Figure 5.1 Groups, Rings, and Fields

Each successive subset (abelian group, ring, commutative ring, and so on) adds additional properties and is **thus**

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 rules are obeyed:

(A1–A5) : R is an abelian group with respect to addition; that is, R satisfies rules 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:

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

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

Commutative Rings

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

(M4) Commutativity of multiplication:

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

Set of Integers $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is a commutative ring.

Q: Example for abelian group but not commutative ring?

- Set of 2×2 matrices with real numbers as entries is abelian group but not **commutative ring**.
- $A \times B = B \times A$ doesn't hold where A, B are 2×2 matrices

Integral domain

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

(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 $b = 0$

Set of Integers $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is an integral domain.

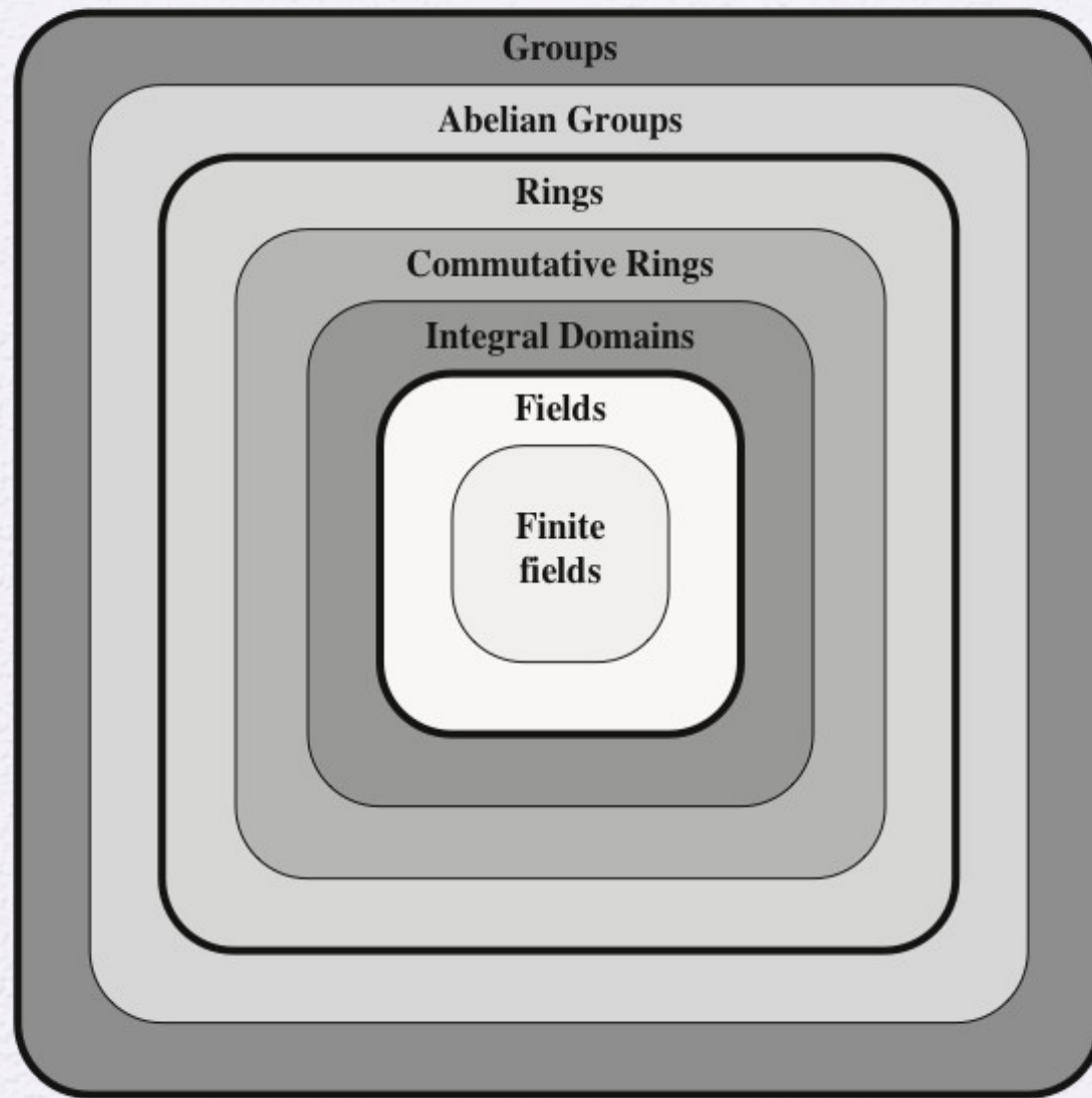


Figure 5.1 Groups, Rings, and Fields

Each successive subset (abelian group, ring, commutative ring, and so on) adds additional properties and is **thus**

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 holds:

(A1–M6): F is an integral domain; that is, F satisfies rules 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.

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. (Ex: 2, $\frac{1}{2}$)



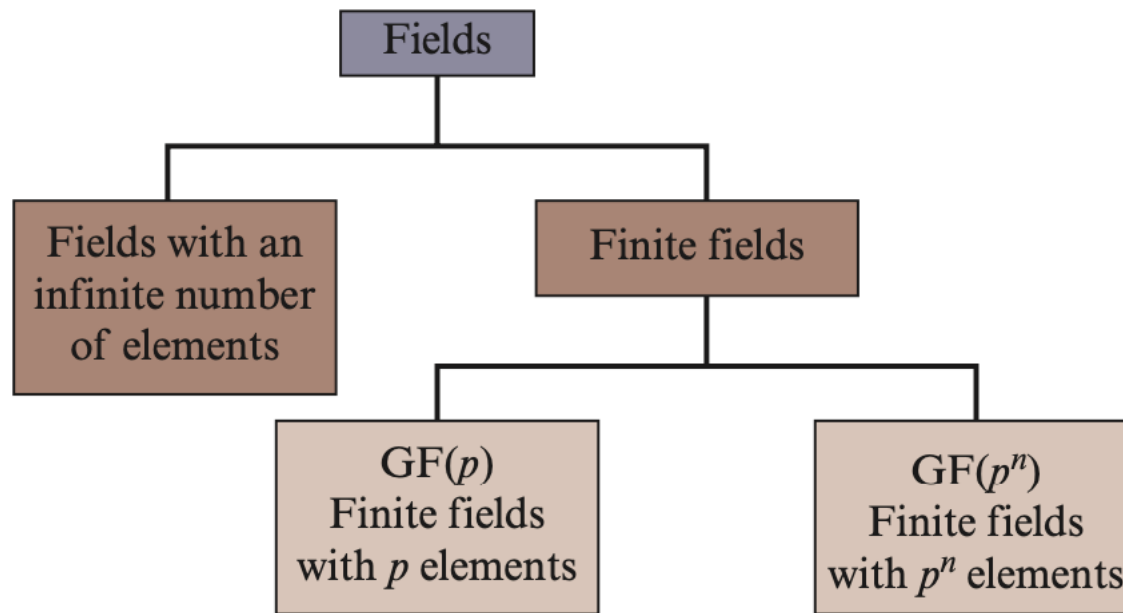


Figure 5.3 Types of Fields

- A finite field (also known as a Galois field) is a field with a **finite number of elements**. The number of elements in a finite field is called the order of the field.
- Finite fields play a crucial role in many cryptographic algorithms
- For a given **prime, p** , we define the **finite field of order p** , $GF(p)$, as the set Z_p of integers $\{0, 1, \dots, p - 1\}$ together with the arithmetic operations **modulo p** .

- For a given **prime, p** , we define the **finite field of order p** , $GF(p)$, as the set Z_p of integers $\{0, 1, \dots, p - 1\}$ together with the arithmetic operations **modulo p** .
- $GF(5)$ where p is prime 5. $\Rightarrow Z_p = \{0, 1, 2, 3, 4\}$
- Addition performed as follows $3+4=7$ then $7 \bmod 5 = 2$
- Multiplication $3*4=12$ then $12 \bmod 5 = 2$

- GF(5) where p is prime 5. $\Rightarrow \mathbb{Z}_p = \{0, 1, 2, 3, 4\}$
- Addition performed as follows $3+4=7$ then $7 \bmod 5 = 2$
- Multiplication $3*4=12$ then $12 \bmod 5 = 2$

Closure under addition / multiplication (A1, M1), easy to see associative of addition/multiplication (A2, M2), commutativity of addition/multiplication (A5, M4).

+	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

\times	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

~~(A1) Closure under addition:~~

~~(A2) Associativity of addition:~~

~~(A3) Additive identity:~~

(A4) Additive inverse:

~~(A5) Commutativity of addition:~~

~~(M1) Closure under multiplication:~~

~~(M2) Associativity of multiplication:~~

~~(M3) Distributive laws:~~

~~(M4) Commutativity of multiplication:~~

(M5) Multiplicative identity:

(M6) No zero divisors:

(M7) Multiplicative inverse:

If a and b belong to S , then $a + b$ is also in S

$a + (b + c) = (a + b) + c$ for all a, b, c in S

There is an element 0 in R such that

$a + 0 = 0 + a = a$ for all a in S

For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$

$a + b = b + a$ for all a, b in S

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

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

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

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

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

There is an element 1 in S such that

$a1 = 1a = a$ for all a in S

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

$a = 0$ or $b = 0$

If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

- GF(5) where p is prime 5. $\Rightarrow \mathbb{Z}_p = \{0, 1, 2, 3, 4\}$
- Addition performed as follows $3+4=7$ then $7 \bmod 5 = 2$
- Multiplication $3*4=12$ then $12 \bmod 5 = 2$

Additive identity (A3): 0 serves as additive identity because $a+0=a$ for all a in GF(5). Similarly, 1 serves as multiplicative identity (M5)

Additive identity (A3): 0 serves as additive identity because $a+0=a$ for all a in GF(5). Similarly, 1 serves as multiplicative identity (M5)

(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 $aa^{-1} = a^{-1}a = 1$

- GF(5) where p is prime 5. $\Rightarrow \mathbb{Z}_p = \{0, 1, 2, 3, 4\}$
- Addition performed as follows $3+4=7$ then $7 \bmod 5 = 2$
- Multiplication $3*4=12$ then $12 \bmod 5 = 2$

Looking at closure under multiplication matrix we can see that No Zero Divisors (M6) also hold.

\times	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

~~(A1) Closure under addition:~~

~~(A2) Associativity of addition:~~

~~(A3) Additive identity:~~

(A4) Additive inverse:

~~(A5) Commutativity of addition:~~

~~(M1) Closure under multiplication:~~

~~(M2) Associativity of multiplication:~~

~~(M3) Distributive laws:~~

~~(M4) Commutativity of multiplication:~~

~~(M5) Multiplicative identity:~~

~~(M6) No zero divisors:~~

(M7) Multiplicative inverse:

If a and b belong to S , then $a + b$ is also in S

$a + (b + c) = (a + b) + c$ for all a, b, c in S

There is an element 0 in R such that

$a + 0 = 0 + a = a$ for all a in S

For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$

$a + b = b + a$ for all a, b in S

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

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

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

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

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

There is an element 1 in S such that

$a1 = 1a = a$ for all a in S

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

$a = 0$ or $b = 0$

If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

- GF(5) where p is prime 5. $\Rightarrow \mathbb{Z}_p = \{0, 1, 2, 3, 4\}$
- Addition performed as follows $3+4=7$ then $7 \bmod 5 = 2$
- Multiplication $3*4=12$ then $12 \bmod 5 = 2$

Distributive law $a=2, b=3, c=4$

$$a(b+c)=2*2=4 ==$$

$$ab+ac=2*3 +2*4=1+3=4$$

$$(a+b)c=0*4=0 ==$$

$$ac+bc=3+2=0$$

Note, mod 5 is taken whenever possible

(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 $aa^{-1} = a^{-1}a = 1$

- GF(5) where p is prime 5. $\Rightarrow Z_p = \{0, 1, 2, 3, 4\}$
- Addition performed as follows $3+4=7$ then $7 \bmod 5 = 2$
- Multiplication $3*4=12$ then $12 \bmod 5 = 2$

Additive inverse (A4): for each a in $Z_p \{0,1,2,3,4\}$ there is $-a$ such that $a+(-a)=0$

Note: $a=2$ doesn't mean $-a=-2$

a	0	1	2	3	4
$-a$	0	4	3	2	1

Multiplicative inverse (M7): for each a in $Z_p \{0,1,2,3,4\}$ there is a^{-1} such that $aa^{-1} = a^{-1}a = 1$

a	1	2	3	4
a^{-1}	1	3	2	4

(A1) Closure under addition:

(A2) Associativity of addition:

(A3) Additive identity:

(A4) Additive inverse:

(A5) Commutativity of addition:

(M1) Closure under multiplication:

(M2) Associativity of multiplication:

(M3) Distributive laws:

(M4) Commutativity of multiplication:

(M5) Multiplicative identity:

(M6) No zero divisors:

(M7) Multiplicative inverse:

If a and b belong to S , then $a + b$ is also in S

$a + (b + c) = (a + b) + c$ for all a, b, c in S

There is an element 0 in R such that

$a + 0 = 0 + a = a$ for all a in S

For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$

$a + b = b + a$ for all a, b in S

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

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

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

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

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

There is an element 1 in S such that

$a1 = 1a = a$ for all a in S

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

$a = 0$ or $b = 0$

If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

POLYNOMIAL ARITHMETIC

A polynomial of degree n (integer $n \geq 0$) is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^n a_i x^i$$

where the a_i are elements of some designated set of numbers S , called the **coefficient** set, and $a_n \neq 0$.

Polynomial arithmetic includes the operations of addition, subtraction, multiplication, and division. To perform **division** the coefficient set S should be a **field**.

$$f(x) = \sum_{i=0}^n a_i x^i, \quad g(x) = \sum_{i=0}^m b_i x^i, \quad n \geq m$$

then addition is defined as

$$f(x) + g(x) = \sum_{i=0}^m (a_i + b_i) x^i + \sum_{i=m+1}^n a_i x^i$$

and multiplication is defined as

$$f(x) \times g(x) = \sum_{i=0}^{n+m} c_i x^i$$

where

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0$$

In the last formula, we treat a_i as zero for $i > n$ and b_i as zero for $i > m$. Note that the degree of the product is equal to the sum of the degrees of the two polynomials.

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

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

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

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

To perform division coefficient set S should be field. Examples real numbers, rational numbers, and \mathbb{Z}_p for prime p .

- For a given prime, p , we define the finite field of order p , $\text{GF}(p)$, as the set \mathbb{Z}_p of integers $\{0, 1, \dots, p - 1\}$ together with the arithmetic operations modulo p .
- $\text{GF}(5)$ where p is prime 5. $\Rightarrow \mathbb{Z}_p = \{0, 1, 2, 3, 4\}$
- Addition performed as follows $3+4=7$ then $7 \bmod 5 = 2$
- Multiplication $3*4=12$ then $12 \bmod 5 = 2$

POLYNOMIAL ARITHMETIC

Polynomial Arithmetic with Coefficients in \mathbb{Z}_p

When polynomial arithmetic is performed on polynomials over a **field**, then **division** is **possible**.

However, even if the coefficient set is a **field**, polynomial division is **not necessarily exact**. In general, division will produce a **quotient** and a **remainder**.

Given polynomials $f(x)$ of degree n and $g(x)$ of degree (m) , ($n \geq m$), if we divide $f(x)$ by $g(x)$, we get a quotient $q(x)$ and a remainder $r(x)$ that obey the relationship

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

with polynomial degrees:

$$\text{Degree } f(x) = n$$

$$\text{Degree } g(x) = m$$

$$\text{Degree } q(x) = n - m$$

$$0 \leq \text{Degree } r(x) \leq m - 1$$

For the preceding example [$f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$], $f(x)/g(x)$ produces a quotient of $q(x) = x + 2$ and a remainder $r(x) = x$, as shown in Figure 5.5d. This is easily verified by noting that

$$\begin{aligned} q(x)g(x) + r(x) &= (x + 2)(x^2 - x + 1) + x = (x^3 + x^2 - x + 2) + x \\ &= x^3 + x^2 + 2 = f(x) \end{aligned}$$

Handwritten polynomial division on a grid background. The dividend $f(x) = x^3 + x^2 + 2$ is written on the left, and the divisor $g(x) = x^2 - x + 1$ is written on the right. The division process shows subtracting $x^3 - x^2 + x$ from $x^3 + x^2 + 2$ to get $2x^2 - x + 2$. Then, $2x^2 - 2x + 2$ is subtracted from $2x^2 - x + 2$ to get the remainder x . The quotient $q(x) = x + 2$ is written to the right of the division line. Arrows point from labels $f(x)$, $g(x)$, $q(x)$, and $r(x)$ to their respective parts in the calculation.

POLYNOMIAL ARITHMETIC

Polynomial Arithmetic with Coefficients in \mathbb{Z}_p

Consider polynomials over $\text{GF}(2)$

Figure 5.6 shows an example of polynomial arithmetic over $\text{GF}(2)$. For $f(x) = (x^7 + x^5 + x^4 + x^3 + x + 1)$ and $g(x) = (x^3 + x + 1)$, the figure shows $f(x) + g(x)$; $f(x) - g(x)$; $f(x) \times g(x)$; and $f(x)/g(x)$. Note that $g(x) \mid f(x)$.

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 greater than 0 and lower than that of $f(x)$. By analogy to integers, an irreducible polynomial is also called a prime polynomial.:

The polynomial⁶ $f(x) = x^4 + 1$ over $\text{GF}(2)$ is reducible, because $x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1)$.

↑
irreducible

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

Figure 5.6 Examples of Polynomial Arithmetic over $\text{GF}(2)$

FINITE FIELDS OF THE FORM $\text{GF}(2^n)$

Virtually all encryption algorithms, both symmetric and asymmetric, involve arithmetic operations on integers.

Also, integers should **fit exactly into a given number of bits** with no wasted bit patterns. That is, we wish to work with integers in the **range 0 through $2^n - 1$** , which fit into an **n-bit word**.

Suppose algorithm needs to operate with 8-bit data.

With **8 bits** we can represent integers in the range $[0, 255]$. However, **256 is not prime** thus $[0, 255]$ **will not be field** thus we **can't do division**. Closest prime is 251 but integers $[251, 255]$ will be wasted.

Let's assume we don't need division.

Integer	1	2	3	4	5	6	7
Occurrences in \mathbb{Z}_8	4	8	4	12	4	8	4

With \mathbb{Z}_8 , occurrence of non-zero elements under multiplication is non-uniform (may lead to attack

\times	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

FINITE FIELDS OF THE FORM $\text{GF}(2^n)$

$\text{GF}(2)$ is a base field with 2 elements $\{0, 1\}$

$\text{GF}(2^n)$ is extension field with 2^n elements.

The elements of $\text{GF}(2^n)$ is **irreducible** polynomial of **degree less than n** with **coefficients in $\text{GF}(2)$** .

- Each element in $\text{GF}(2^n)$ can be represented as:

$$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0$$

where $a_i \in \text{GF}(2)$ (i.e., a_i is either 0 or 1).

Addition/subtraction is performed by adding/subtracting corresponding coefficients module 2.

Example:

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

(Since $x^2 + x^2 = 0$ and $1 + 1 = 0$ in $\text{GF}(2)$).

Multiplication: If multiplication results in a polynomial of **degree greater than $n - 1$** , then the **polynomial is reduced modulo some irreducible polynomial $m(x)$ of degree n** .

That is, **we divide by $m(x)$ and keep the remainder**. For a polynomial $f(x)$, the remainder is expressed as $r(x) = f(x) \bmod m(x)$.

- 1. Multiply the Polynomials:** Multiply the two polynomials as you would in regular polynomial arithmetic.
- 2. Reduce the Result:** Reduce the resulting polynomial modulo the **chosen irreducible** polynomial to ensure the result is still within the field.

Polynomials in $\text{GF}(2^3)$

Elements of $\text{GF}(2^3)$ can be represented as polynomials of degree less than 3 with coefficients in $\text{GF}(2)$:

$\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$

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 greater than 0 and lower than that of $f(x)$. By analogy to integers, an irreducible polynomial is also called a prime polynomial.:

The polynomial⁶ $f(x) = x^4 + 1$ over $\text{GF}(2)$ is reducible, because
$$x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1).$$

↑
irreducible

Let's use the irreducible polynomial $f(x) = x^3 + x + 1$ to construct $\text{GF}(2^3)$.

- Each element in $\text{GF}(2^n)$ can be represented as:

$$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0$$

where $a_i \in \text{GF}(2)$ (i.e., a_i is either 0 or 1).

1. **Multiply the Polynomials:** Multiply the two polynomials as you would in regular polynomial arithmetic.
2. **Reduce the Result:** Reduce the resulting polynomial modulo the **chosen irreducible** polynomial to ensure the result is still within the field.

Polynomials in $\text{GF}(2^3)$

Elements of $\text{GF}(2^3)$ can be represented as polynomials of degree less than 3 with coefficients in $\text{GF}(2)$:

$$\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$$

Let's use the irreducible polynomial $f(x) = x^3 + x + 1$ to construct $\text{GF}(2^3)$.

$$(x^2 + x) \cdot (x + 1) = x^2 \cdot x + x^2 \cdot 1 + x \cdot x + x \cdot 1 = x^3 + x^2 + x^2 + x = x^3 + 2x^2 + x$$

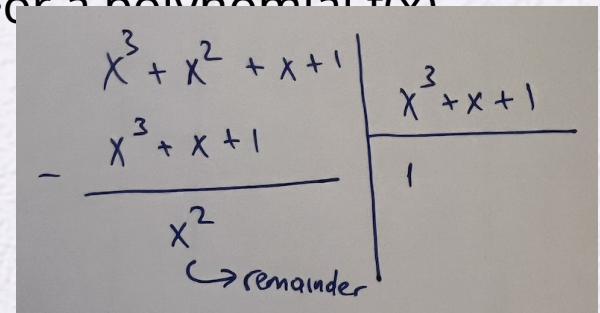
Degree greater than $n-1$ (3-1)

If multiplication results in a polynomial of **degree greater** than $n - 1$, then the **polynomial is reduced modulo some irreducible polynomial $m(x)$ of degree n** .

That is, **we divide by $m(x)$ and keep the remainder**. For a polynomial $f(x)$ the remainder is expressed as $r(x) = f(x) \bmod m(x)$.

In our case $m(x) = x^3 + x + 1$

So result of $(x^2 + 1)(x + 1)$ in $\text{GF}(2^3)$ is x^2



$$\begin{array}{r|l}
 x^3 + x^2 + x + 1 & x^3 + x + 1 \\
 - (x^3 + x + 1) & \\
 \hline
 & x^2 \\
 & \text{remainder}
 \end{array}$$

The Advanced Encryption Standard (AES) uses arithmetic in the finite field $\text{GF}(2^8)$, with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Consider the two polynomials $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$. Then

$$\begin{aligned} f(x) + g(x) &= x^6 + x^4 + x^2 + x + 1 + x^7 + x + 1 \\ &= x^7 + x^6 + x^4 + x^2 \end{aligned}$$

$$\begin{aligned} f(x) \times g(x) &= x^{13} + x^{11} + x^9 + x^8 + x^7 \\ &\quad + x^7 + x^5 + x^3 + x^2 + x \\ &\quad + x^6 + x^4 + x^2 + x + 1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \end{aligned}$$

$$\begin{array}{r}
 x^8 + x^4 + x^3 + x + 1 \sqrt{\begin{array}{l} x^5 + x^3 \\ x^{13} + x^{11} + x^9 + x^8 \end{array}} \quad \begin{array}{l} + x^6 + x^5 + x^4 + x^3 + 1 \\ + x^6 + x^5 \end{array} \\
 \hline
 \begin{array}{l} x^{11} \\ x^{11} \end{array} \quad \begin{array}{l} + x^4 + x^3 \\ + x^7 + x^6 \end{array} \quad \begin{array}{l} + x^4 + x^3 \\ + x^4 + x^3 \end{array} \\
 \hline
 \begin{array}{l} x^7 + x^6 \\ x^7 + x^6 \end{array} \quad \begin{array}{l} + 1 \\ + 1 \end{array}
 \end{array}$$

Therefore, $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$.

Arithmetic operations are lightweight in $G(2^n)$, if they are represented in binary format

Consider the two polynomials in $\text{GF}(2^8)$ from our earlier example:

$$f(x) = x^6 + x^4 + x^2 + x + 1 \text{ and } g(x) = x^7 + x + 1.$$

$$\begin{aligned} (x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) &= x^7 + x^6 + x^4 + x^2 \text{ (polynomial notation)} \\ (01010111) \oplus (10000011) &= (11010100) \text{ (binary notation)} \\ \{57\} \oplus \{83\} &= \{\text{D4}\} \text{ (hexadecimal notation)}^7 \end{aligned}$$

We will use $m(x) = x^8 + x^4 + x^3 + x + 1$, which is the finite field used in AES.

$$x^8 \bmod m(x) = [m(x) - x^8] = (x^4 + x^3 + x + 1) \quad \text{Equation 5.4}$$

Handwritten polynomial long division:

$$\begin{array}{r} x^4 + x^3 + x + 1 \\ x^8 \\ \hline x^8 + x^4 + x^3 + x + 1 \\ \hline 0 \end{array}$$

Since we are operating on $GF(2^n)$

Now, consider a polynomial in $GF(2^8)$, which has the form $f(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$. If we multiply by x , we have

$$x \times f(x) = (b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \bmod m(x) \quad (5.5)$$

If $b_7 = 0$ in Equation (5.5), then the result is a polynomial of **degree less than 8**, which is **already in reduced** form and no further computation is necessary.

If $b_7 = 1$, then reduction modulo $m(x)$ is achieved using Equation (5.4):

$$x \times f(x) = (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) + (x^4 + x^3 + x + 1)$$

We will use $m(x) = x^8 + x^4 + x^3 + x + 1$, which is the finite field used in AES.

$$x^8 \bmod m(x) = [m(x) - x^8] = (x^4 + x^3 + x + 1) \quad \text{Equation 5.4}$$

Now, consider a polynomial in $GF(2^8)$, which has the form $f(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$. If we multiply by x , we have

$$x \times f(x) = (b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \bmod m(x) \quad (5.5)$$

If $b_7 = 0$ in Equation (5.5), then the result is a polynomial of **degree less than 8**, which is **already in reduced** form and no further computation is necessary. If $b_7 = 1$, then reduction modulo $m(x)$ is achieved using Equation (5.4):

$$x \times f(x) = (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) + (x^4 + x^3 + x + 1)$$

It follows that multiplication by x (i.e., 00000010) can be implemented as a 1-bit left shift followed by a conditional bitwise XOR with (00011011), which represents $(x^4 + x^3 + x + 1)$. To summarize,

$$x \times f(x) = \begin{cases} (b_6b_5b_4b_3b_2b_1b_00) & \text{if } b_7 = 0 \\ (b_6b_5b_4b_3b_2b_1b_00) \oplus (00011011) & \text{if } b_7 = 1 \end{cases} \quad (5.6)$$

Multiplication by a higher power of x can be achieved by repeated application of Equation (5.6). By adding intermediate results, multiplication by any constant in $GF(2^8)$ can be achieved.

The Advanced Encryption Standard (AES) uses arithmetic in the finite field $GF(2^8)$, with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Consider the two polynomials $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$. Then

$$\begin{aligned} f(x) + g(x) &= x^6 + x^4 + x^2 + x + 1 + x^7 + x + 1 \\ &= x^7 + x^6 + x^4 + x^2 \\ f(x) \times g(x) &= x^{13} + x^{11} + x^9 + x^8 + x^7 \\ &\quad + x^7 + x^5 + x^3 + x^2 + x \\ &\quad + x^6 + x^4 + x^2 + x + 1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \end{aligned}$$

$$\begin{array}{r} x^5 + x^3 \\ x^8 + x^4 + x^3 + x + 1 \overline{) x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1} \\ \underline{x^{13} \phantom{+ x^{11}} + x^9 + x^8 + x^5} \\ x^{11} + x^4 + x^3 \\ \underline{x^{11} + x^7 + x^6 + x^3} \\ x^7 + x^6 + 1 \end{array}$$

Therefore, $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$.

$$\begin{aligned} x \times f(x) &= (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \\ &\quad + (x^4 + x^3 + x + 1) \end{aligned}$$

It follows that multiplication by x (i.e., 00000010) can be implemented as a 1-bit left shift followed by a conditional bitwise XOR with (00011011), which represents $(x^4 + x^3 + x + 1)$. To summarize,

$$x \times f(x) = \begin{cases} (b_6b_5b_4b_3b_2b_1b_0) & \text{if } b_7 = 0 \\ (b_6b_5b_4b_3b_2b_1b_0) \oplus (00011011) & \text{if } b_7 = 1 \end{cases} \tag{5.6}$$

Multiplication by a higher power of x can be achieved by repeated application of Equation (5.6). By adding intermediate results, multiplication by any constant in $GF(2^8)$ can be achieved.

$f(x) * x^2$, $b_7 = 1$, so left shift
And xor with $m(x) = 00011011$

In an earlier example, we showed that for $f(x) = x^6 + x^4 + x^2 + x + 1$, $g(x) = x^7 + x + 1$, and $m(x) = x^8 + x^4 + x^3 + x + 1$, we have $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$. Redoing this in binary arithmetic, we need to compute $(01010111) \times (10000011)$. First, we determine the results of multiplication by powers of x :

$$\begin{aligned} (01010111) \times (00000010) &= (10101110) && f(x) * x \quad b_7=0 \text{ so just left shift} \\ (01010111) \times (00000100) &= (01011100) \oplus (00011011) = (01000111) \\ (01010111) \times (00001000) &= (10001110) \\ (01010111) \times (00010000) &= (00011100) \oplus (00011011) = (00000111) \\ (01010111) \times (00100000) &= (00001110) \\ (01010111) \times (01000000) &= (00011100) \\ (01010111) \times (10000000) &= (00111000) && f(x) * x^7. \quad b_7=0 \text{ so just left shift} \end{aligned}$$

So,

$$\begin{aligned} (01010111) \times (10000011) &= (01010111) \times [(00000001) \oplus (00000010) \oplus (10000000)] \\ &= (01010111) \oplus (10101110) \oplus (00111000) = (11000001) \end{aligned}$$

which is equivalent to $x^7 + x^6 + 1$. $*1$ $*x$ $*x^7$

Suppose we wish to use 3-bit blocks in our encryption algorithm and use only the operations of addition and multiplication. Then arithmetic modulo 8 is well defined, as shown in Table 5.1. However, note that in the multiplication table, the nonzero integers do not appear an equal number of times. For example, there are only four occurrences of 3, but twelve occurrences of 4. On the other hand, as was mentioned, there are finite fields of the form $\text{GF}(2^n)$, so there is in particular a finite field of order $2^3 = 8$. Arithmetic for this field is shown in Table 5.2. In this case, the number of occurrences of the nonzero integers is uniform for multiplication. To summarize,

Integer	1	2	3	4	5	6	7
Occurrences in \mathbb{Z}_8	4	8	4	12	4	8	4
Occurrences in $\text{GF}(2^3)$	7	7	7	7	7	7	7

$\text{GF}(2^n)$ consists of 2^n elements.

The binary operations $+$ and $*$ are defined over the set. The operations of addition, subtraction, multiplication, and division can be performed without leaving the set.

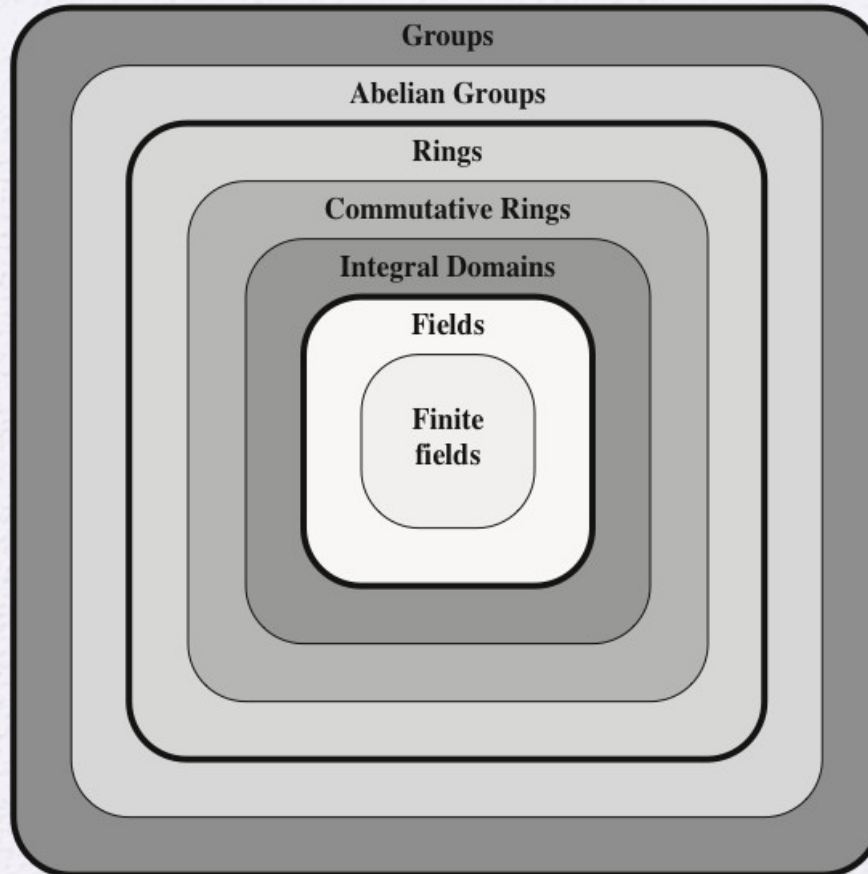


Figure 5.1 Groups, Rings, and Fields

5.4 FINITE FIELDS OF THE FORM $\text{GF}(p)$

5.5 POLYNOMIAL ARITHMETIC

5.6 FINITE FIELDS OF THE FORM $\text{GF}(2^n)$