Mathematics of Cryptography: Algebraic Structure

Dr. B C Dhara

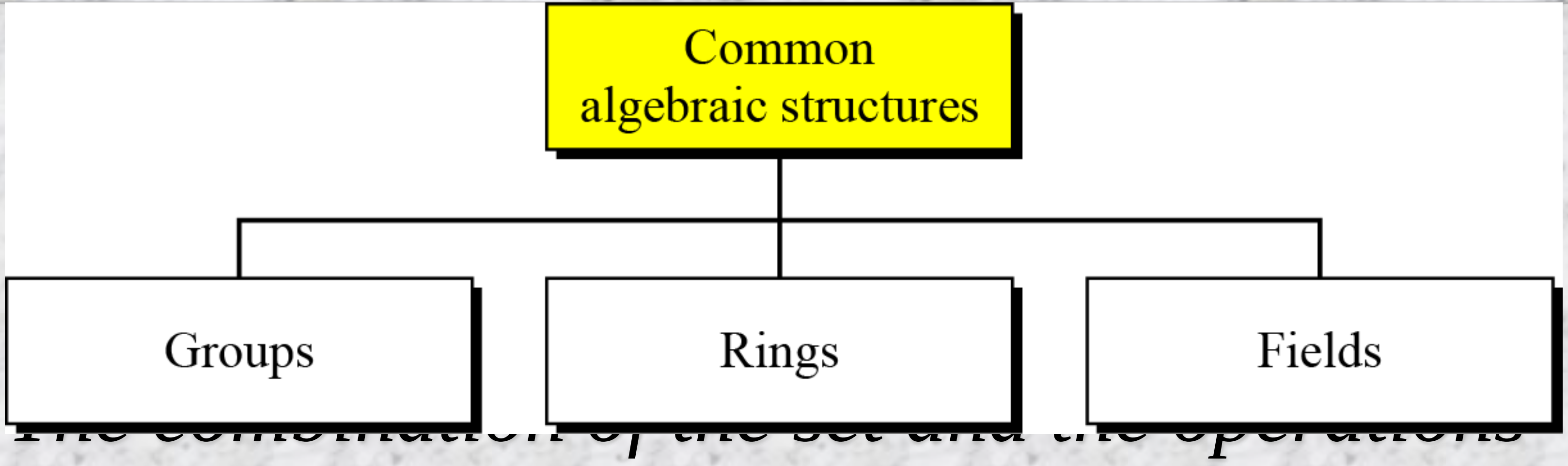
Department of Information Technology

Jadavpur University

Objectives

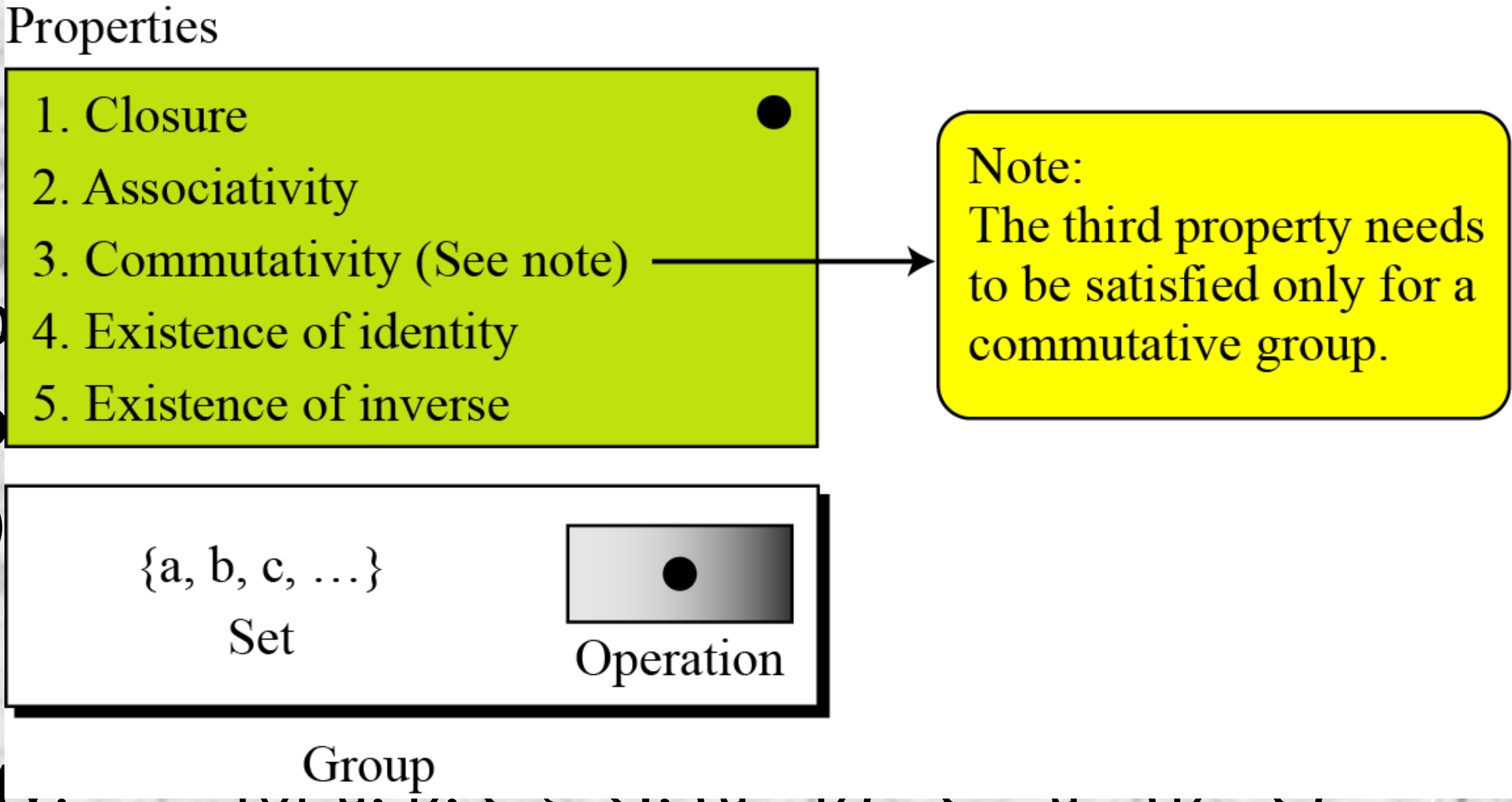
- Review the concept of algebraic structures
- Define and give some examples of groups
- Define and give some examples of rings
- Define and give some examples of fields
- Emphasize the finite fields of type GF(2^n) that make it possible to perform operations such as addition, subtraction, multiplication, and division on *n*-bit words in modern block ciphers

ALGEBRAIC STRUCTURES



- *The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure*
- *In this chapter, we will define three common algebraic structures: groups, rings, and fields.*

Groups



Properties

1. Closure ●
2. Associativity
3. Commutativity (See note)
4. Existence of identity
5. Existence of inverse

Note:
The third property needs to be satisfied only for a commutative group.

- A group
operatio
axioms)

Closure:

Associativity: for a, b, c ∈ G, (a • b) • c = a • (b • c)

Existence of identity: for all a ∈ G, there is e ∈ G such that a • e = e • a = a, e is the identity element

Existence of inverse: for all a ∈ G, there is b ∈ G such that a • b = b • a = e, b is inverse of a and vice versa

Groups (contd…)

- A group (G, •) is called commutative or abelian group if the operator '•' satisfies the commutative property
  - Commutative property: for all a, b $\in$ G, a • b = b • a

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: groups

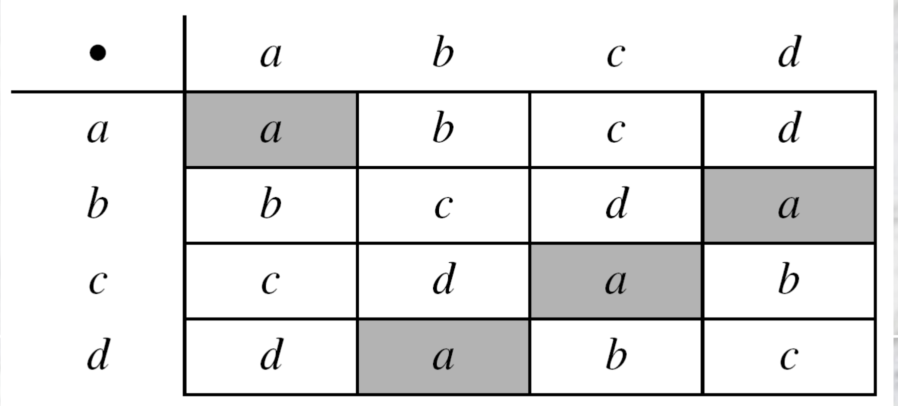
The set of residue integers with the addition operator,

$$G = < Z_n , +>,$$

is a commutative group. We can perform addition and subtraction on the elements of this set without moving out of the set.

The set Z_n* with the multiplication operator, G = <Z_n*, ×>, is also an abelian group.

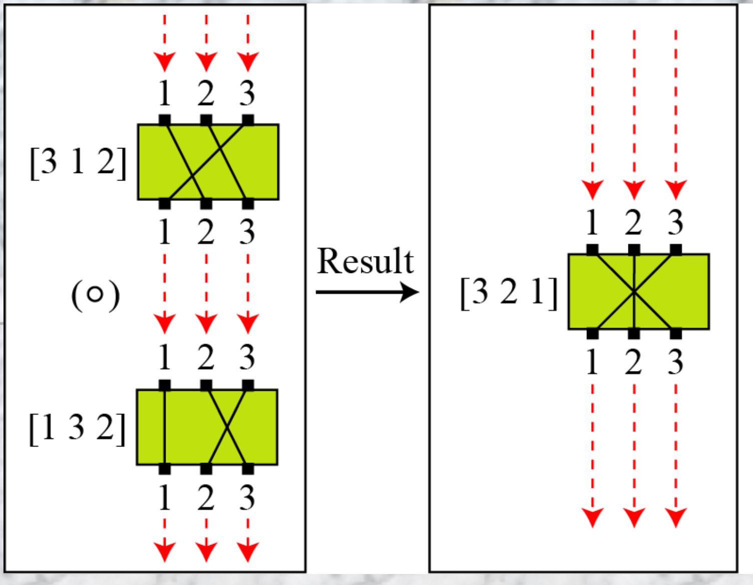
Let us define a set G = < {*a*, *b*, *c*, *d*}, •> and the operation as shown in following table



•	*a*	*b*	*c*	*d*
a	*a*	*b*	*c*	*d*
b	*b*	*c*	*d*	*a*
c	*c*	*d*	*a*	*b*
d	*d*	*a*	*b*	*c*

This is an abelian group

Permutation group



[3 2 1] = [3 1 2] ∘[1 3 2]

∘	[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]

Permutation group

- set of permutations with the composition operation is a group
  - This implies that using two permutations one after another cannot strengthen the security of a cipher
    - because we can always find a permutation that can do the same job because of the closure property

Groups (contd…)

- Finite Group: a group with finite elements; otherwise, infinite group
- Order of a Group: |G|, number of elements if finite; otherwise, infinite
- Subgroups: A subset H of G is a subgroup of G if H is a group under the operation of G

subgroups

- If a, b $\in$ G, H ➔ c = a • b $\in$ G, H
- e $\in$ G, H
- If a $\in$ G, H ➔ If $a^{-1} \in$ G, H
- ({e}, •) is subgroup of G, H
- G is a subgroup of itself

Example: subgroup

Is the group $H = <Z_{10}, +>$ a subgroup of the group $G = <Z_{12}, +>$?

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.

Cyclic Subgroups

- If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic subgroup

$$\boxed{a^n \rightarrow a \bullet a \bullet \ldots \bullet a \quad (n \text{ times})}$$

Example: cyclic subgroup

Four cyclic subgroups can be made from the group $G = <Z_6, +>$. They are $H_1 = <\{0\}, +>$, $H_2 = <\{0, 2, 4\}, +>$, $H_3 = <\{0, 3\}, +>$, and $H_4 = G$.

$0^0 \bmod 6 = 0$

$1^0 \bmod 6 = 0$
$1^1 \bmod 6 = 1$
$1^2 \bmod 6 = (1 + 1) \bmod 6 = 2$
$1^3 \bmod 6 = (1 + 1 +1) \bmod 6 = 3$
$1^4 \bmod 6 = (1 + 1 + 1 + 1) \bmod 6 = 4$
$1^5 \bmod 6 = (1 + 1 + 1 + 1+ 1) \bmod 6 = 5$

$2^0 \bmod 6 = 0$
$2^1 \bmod 6 = 2$
$2^2 \bmod 6 = (2 + 2) \bmod 6 = 4$

$3^0 \bmod 6 = 0$
$3^1 \bmod 6 = 3$

$4^0 \bmod 6 = 0$
$4^1 \bmod 6 = 4$
$4^2 \bmod 6 = (4 + 4) \bmod 6 = 2$

$5^0 \bmod 6 = 0$
$5^1 \bmod 6 = 5$
$5^2 \bmod 6 = 4$
$5^3 \bmod 6 = 3$
$5^4 \bmod 6 = 2$
$5^5 \bmod 6 = 1$

Example: cyclic subgroup

Three cyclic subgroups can be made from the group $G = \langle Z_{10}^{*}, \times \rangle$. G has only four elements: 1, 3, 7, and 9. The cyclic subgroups are $H_1 = \langle \{1\}, \times \rangle$, $H_2 = \langle \{1, 9\}, \times \rangle$, and $H_3 = G$.

$1^0 \bmod 10 = 1$

$3^0 \bmod 10 = 1$
$3^1 \bmod 10 = 3$
$3^2 \bmod 10 = 9$
$3^3 \bmod 10 = 7$

$7^0 \bmod 10 = 1$
$7^1 \bmod 10 = 7$
$7^2 \bmod 10 = 9$
$7^3 \bmod 10 = 3$

$9^0 \bmod 10 = 1$
$9^1 \bmod 10 = 9$

Cyclic Groups

- A cyclic group is a group that is its own cyclic subgroup.

$$\boxed{\{e, g, g^2, \ldots, g^{n-1}\}, \text{ where } g^n = e}$$

Cyclic Groups

Three cyclic subgroups can be made from the group $G = <Z_{10}^*, \times>$. G has only four elements: 1, 3, 7, and 9. The cyclic subgroups are $H_1 = <\{1\}, \times>$, $H_2 = <\{1, 9\}, \times>$, and $H_3 = G$.

a. The group $G = <Z_6, +>$ is a cyclic group with two generators, $g = 1$ and $g = 5$.

b. The group $G = < Z_{10}^*, \times>$ is a cyclic group with two generators, $g = 3$ and $g = 7$.

Subgroup property

Assume that G is a group, and H is a subgroup of G. If the order of G and H are |G| and |H|, respectively, then, based on this theorem, |H| divides |G|.

Order of an Element

The order of an element a, ord(a), is the smallest number n such that a^n =e

In other words, ord(a) is the order of the cyclic group generated by a

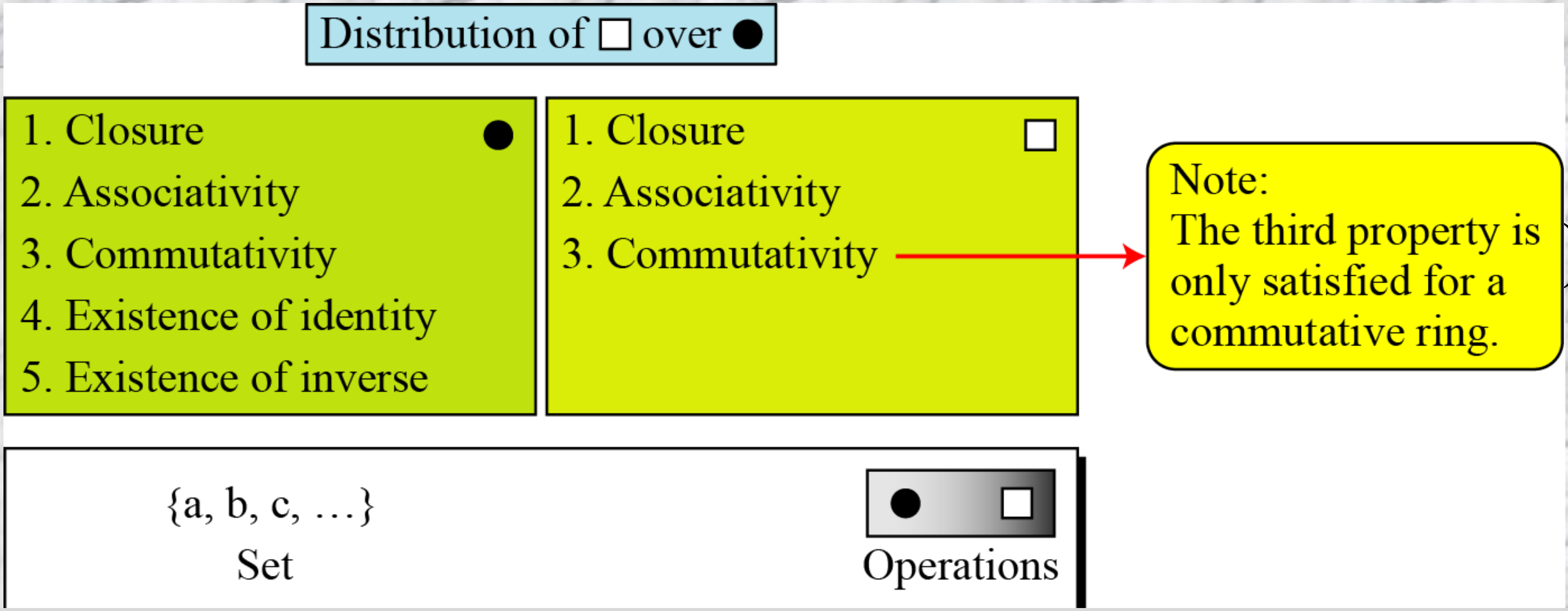
Example: ord(a)

a. In the group $G = \langle Z_6, + \rangle$, the orders of the elements are:

ord(0) = 1, ord(1) = 6, ord(2) = 3, ord(3) = 2, ord(4) = 3, ord(5) = 6.

b. In the group $G = \langle Z_{10}^*, \times \rangle$, the orders of the elements are: ord(1) = 1, ord(3) = 4, ord(7) = 4, ord(9) = 2.

Ring



Distribution of □ over ●

●
1. Closure
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse

□
1. Closure
2. Associativity
3. Commutativity

Note:
The third property is only satisfied for a commutative ring.

{a, b, c, …}
Set

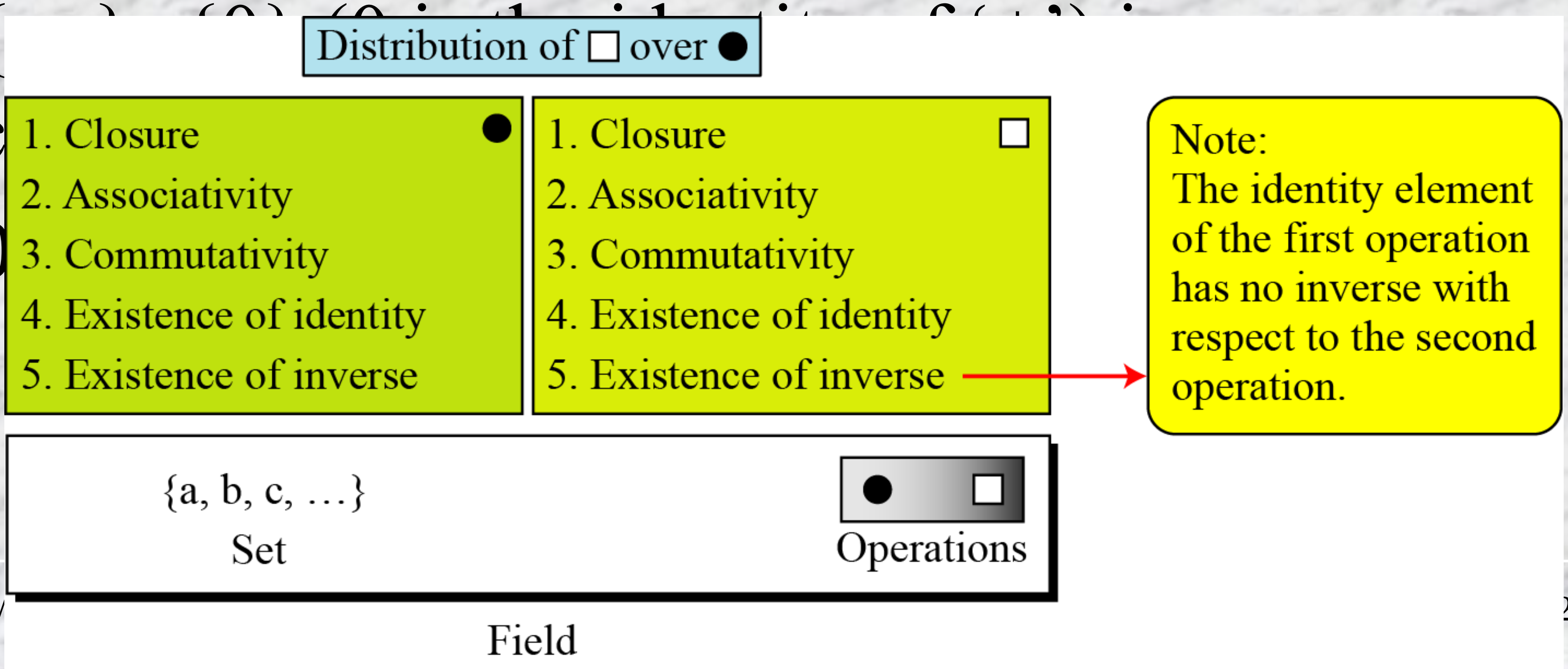
● □
Operations

The set Z with two operations, addition and multiplication, is a commutative ring. We show it by R = <Z, +, ×>. Addition satisfies all of the five properties; multiplication satisfies only three properties.

If '*' is commutative, R is commutative ring

Field

- A field, denoted by F = <{…}, +, *> is
- {…} is a commutative group respect to the first operation '+'
- {
  c
- 0



Distribution of □ over ●

1. Closure ●
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse

1. Closure □
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse

Note:
The identity element of the first operation has no inverse with respect to the second operation.

{a, b, c, …}
Set

● □
Operations

Field

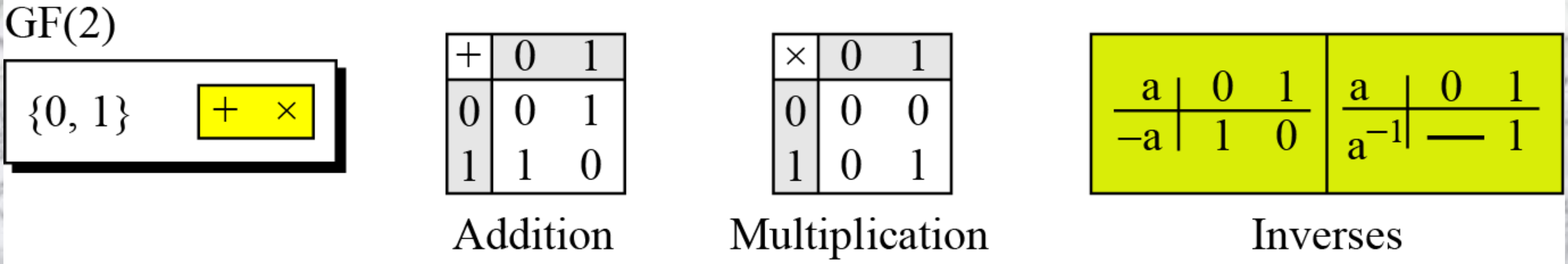
Finite field

- Finite field is important in cryptography
- A field with finite number is called finite field
- Galois showed that for a field to be finite, the number of elements should be p^n, where p is a prime and n is a positive integer

Galois field GF(p)

- When n = 1, we have GF(p) field. This field can be the set Z_p, {0, 1, …, p − 1}, with two arithmetic operations

A very common field in this category is GF(2) with the set {0, 1} and two operations, addition and multiplication, as shown in Figure 4.6.



+	0	1
0	0	1
1	1	0

Addition

×	0	1
0	0	0
1	0	1

Multiplication

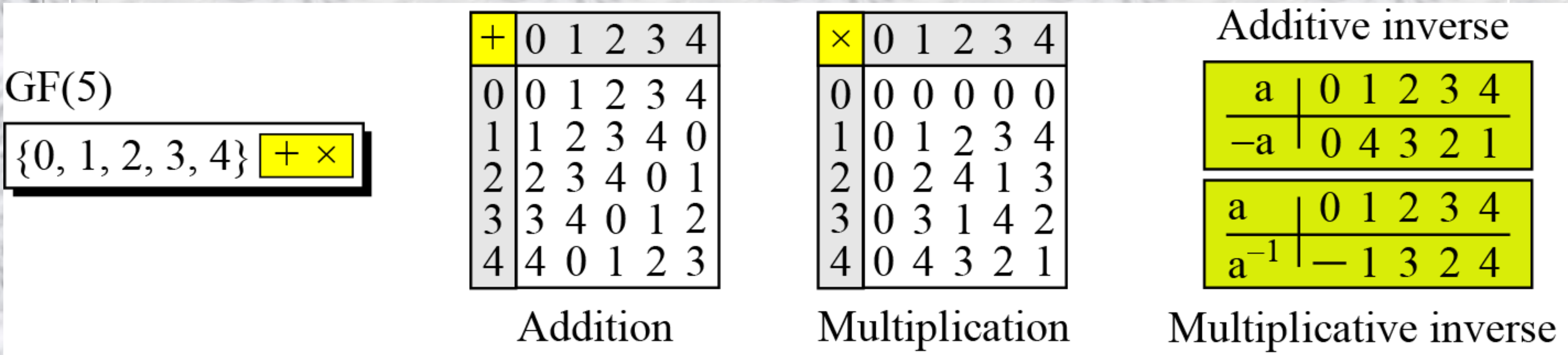
a	0	1
−a	1	0

a	0	1
a^{-1}	—	1

Inverses

Galois field GF(p) (contd…)

We can define GF(5) on the set Z_5 (5 is a prime) with addition and multiplication operators as shown below



GF(5)

{0, 1, 2, 3, 4} + ×

+	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

Addition

×	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

Multiplication

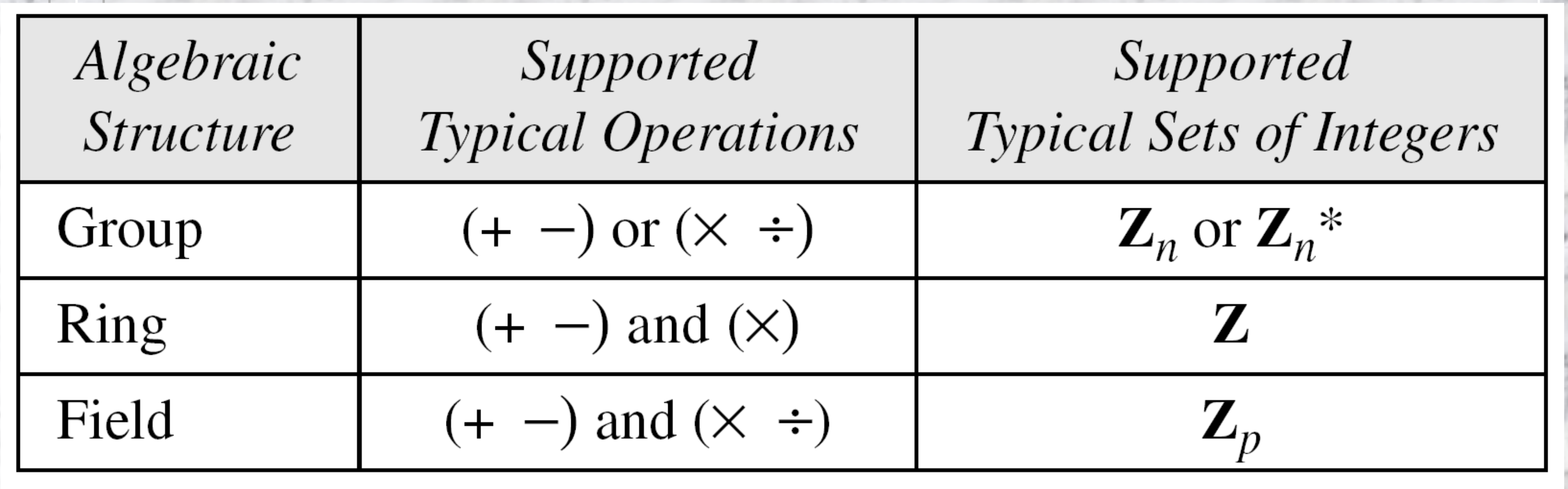
Additive inverse

a	0	1	2	3	4
−a	0	4	3	2	1

a	0	1	2	3	4
a^{-1}	—	1	3	2	4

Multiplicative inverse

Summary



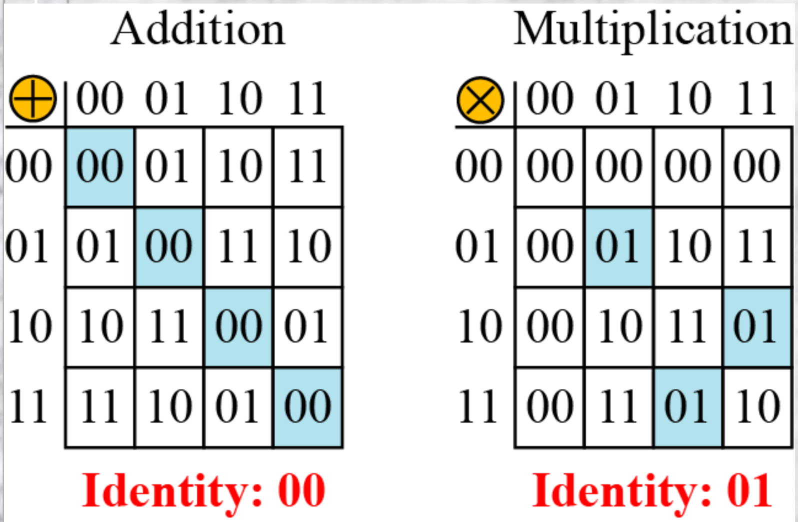
Algebraic Structure	*Supported Typical Operations*	*Supported Typical Sets of Integers*
Group	(+ −) or (× ÷)	$\mathbf{Z}_n$ or $\mathbf{Z}_n{}^*$
Ring	(+ −) and (×)	$\mathbf{Z}$
Field	(+ −) and (× ÷)	$\mathbf{Z}_p$

GF(2^n)

- *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(p) where p is the largest number less than 2^n*
  - *But, numbers between p and 2^n -1 cannot be handled*
- *In GF(2^n), we have a set of 2^n elements*
  - *The elements in this set are n-bit words*

GF(2^n) (contd…)

Let us define a GF(2^2) field in which the set has four 2-bit words: {00, 01, 10, 11}. We can redefine addition and multiplication for this field in such a way that all properties of these operations are satisfied



Addition

⊕	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Identity: 00

Multiplication

⊗	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Identity: 01

00, 01,…, 11 cannot be considered as integer from 0 to 3

Addition and multiplication are defined in terms of polynomial

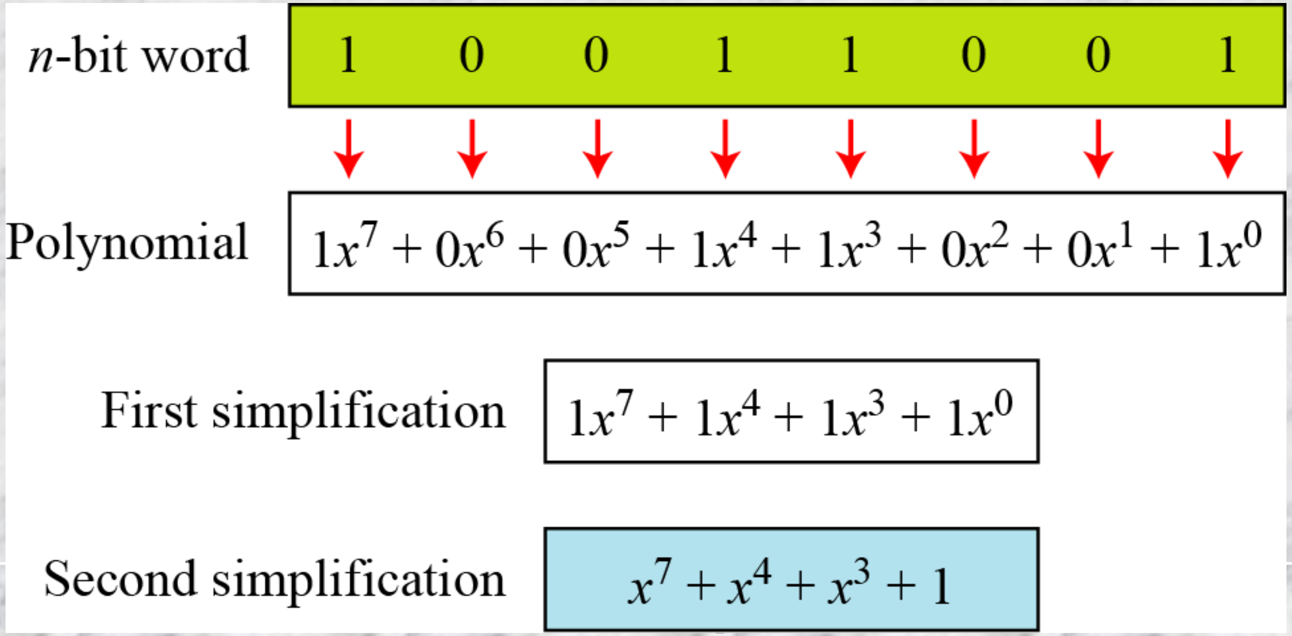
Polynomials

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

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

where a_i is called coefficient of the i^{th} term.

- 8-bit word 10011001 represents as



n-bit word: 1 0 0 1 1 0 0 1

Polynomial: $1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 0x^1 + 1x^0$

First simplification: $1x^7 + 1x^4 + 1x^3 + 1x^0$

Second simplification: $x^7 + x^4 + x^3 + 1$

Polynomials (contd…)

- 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

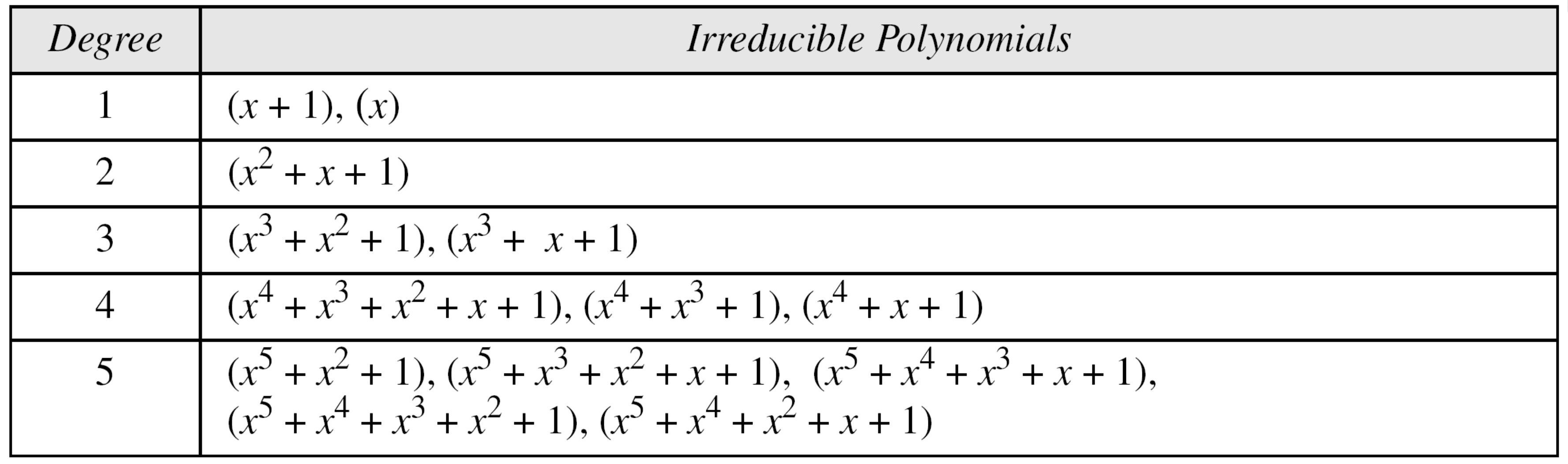
$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0$$

  - Related 8-bit word is 00100110

Operations on polynomials

- Any operation on polynomial involves two operations:
  - operation on coefficients and
  - operations on two polynomials
- Operations on coefficients (0/1) use GF(2)
- For operations on polynomials need GF(2^n)

Modulus respect to polynomial

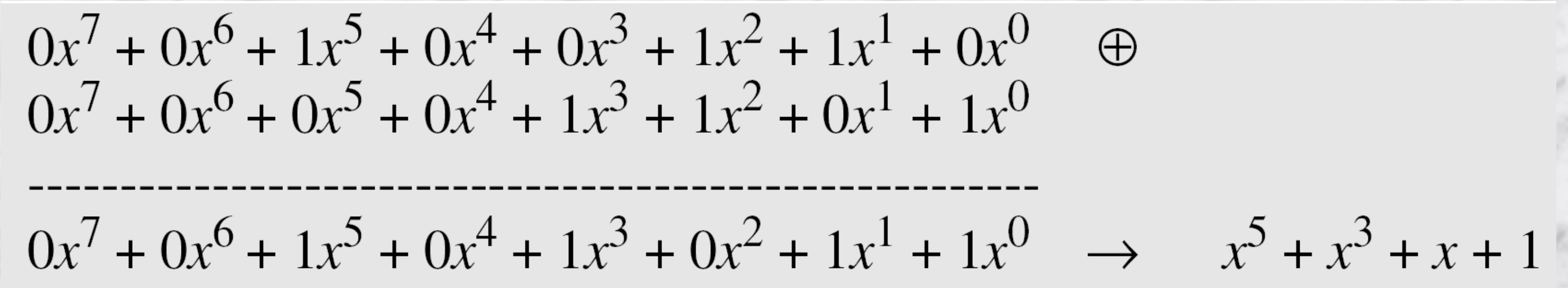


Degree	*Irreducible Polynomials*
1	$(x + 1), (x)$
2	$(x^2 + x + 1)$
3	$(x^3 + x^2 + 1), (x^3 + x + 1)$
4	$(x^4 + x^3 + x^2 + x + 1), (x^4 + x^3 + 1), (x^4 + x + 1)$
5	$(x^5 + x^2 + 1), (x^5 + x^3 + x^2 + x + 1), (x^5 + x^4 + x^3 + x + 1),$ $(x^5 + x^4 + x^3 + x^2 + 1), (x^5 + x^4 + x^2 + x + 1)$

- We need a polynomial of degree n, respect to which we have to take remainder
- The modulus polynomial takes as prime polynomial
- Prime polynomial is irreducible, i.e., no polynomial can divides it

Addition operation

- Addition (or subtraction) over GF(2)
- $(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1)$ in $GF(2^8)$, the symbol $\oplus$ to show that we mean polynomial addition



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

Additive identity: zero polynomial

Additive inverse: polynomial itself

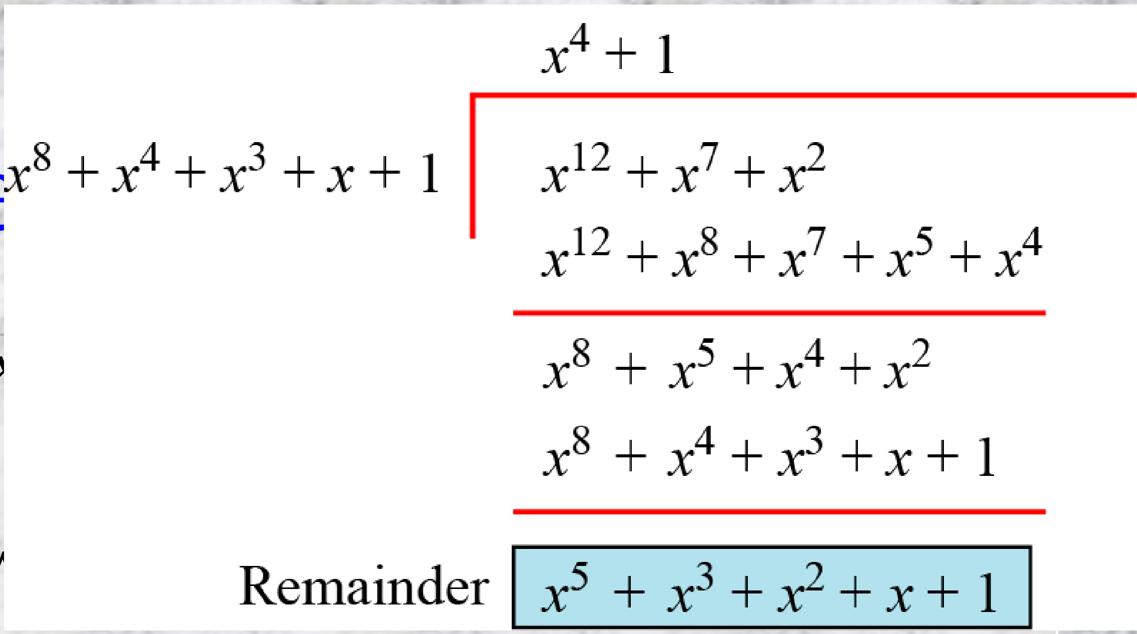
Multiplication

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.

Multiplication: e



$$x^4 + 1$$

$$x^8 + x^4 + x^3 + x + 1 \;\big|\; x^{12} + x^7 + x^2$$

$$x^{12} + x^8 + x^7 + x^5 + x^4$$

$$x^8 + x^5 + x^4 + x^2$$

$$x^8 + x^4 + x^3 + x + 1$$

Remainder $\boxed{x^5 + x^3 + x^2 + x + 1}$

Find the result of (x^5 + x^2 + x

irreducible polynomial (x^8

represent multiplication of tw

Solution

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

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

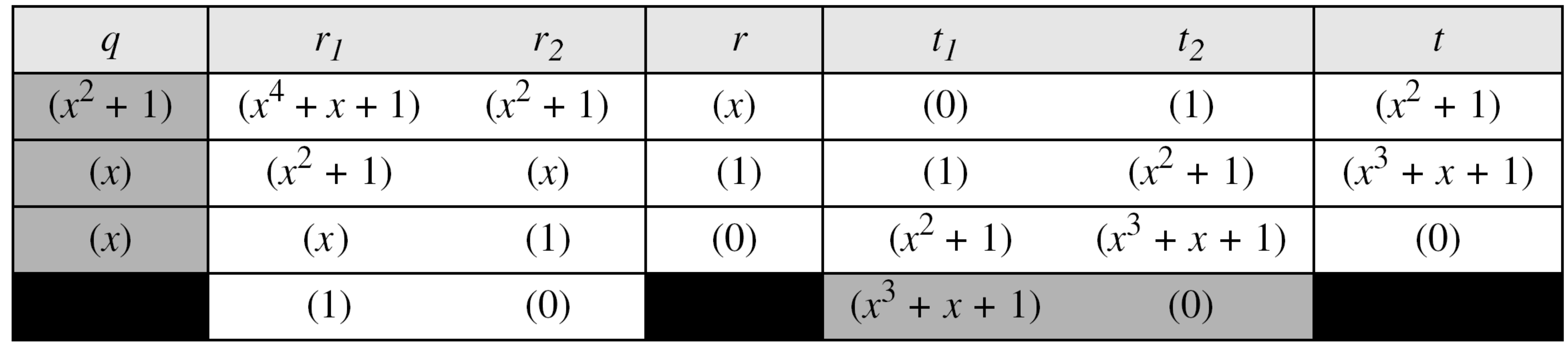
$$P_1 \otimes P_2 = (x^{12} + x^7 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x^5 + x^3 + x^2 + x + 1$$

To find the final result, divide the polynomial of degree 12 by the polynomial of degree 8 (the modulus) and keep only the remainder

Multiplication

- Multiplicative identity: 1 i.e., 00000…0001
- Multiplicative inverse: extended Euclidean algorithm on the given polynomial and modulus polynomial

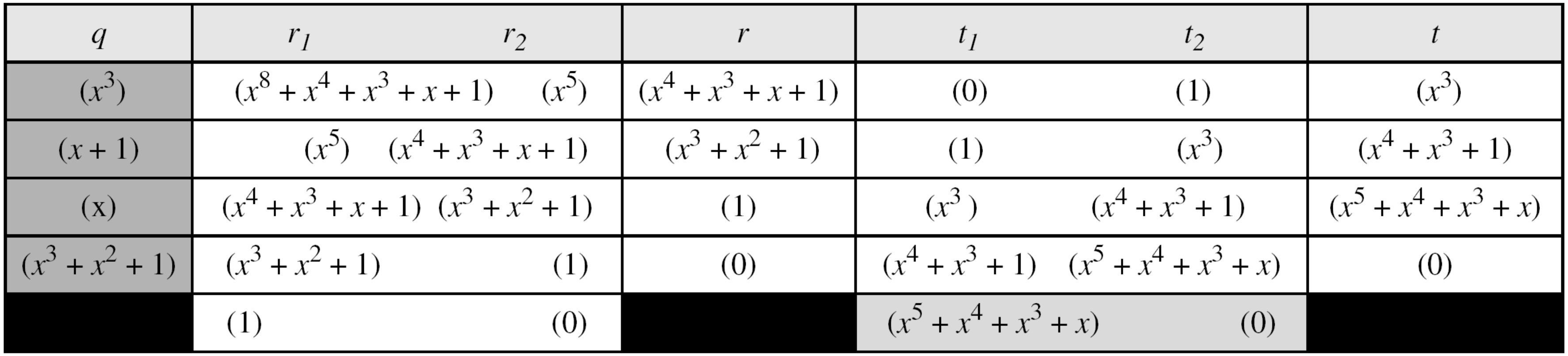
In GF (2^4), find the inverse of $(x^2 + 1)$ modulo $(x^4 + x + 1)$.



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)	

Multiplicative inverse

In GF(2^8), find the inverse of (x^5) modulo ($x^8 + x^4 + x^3 + x + 1$).



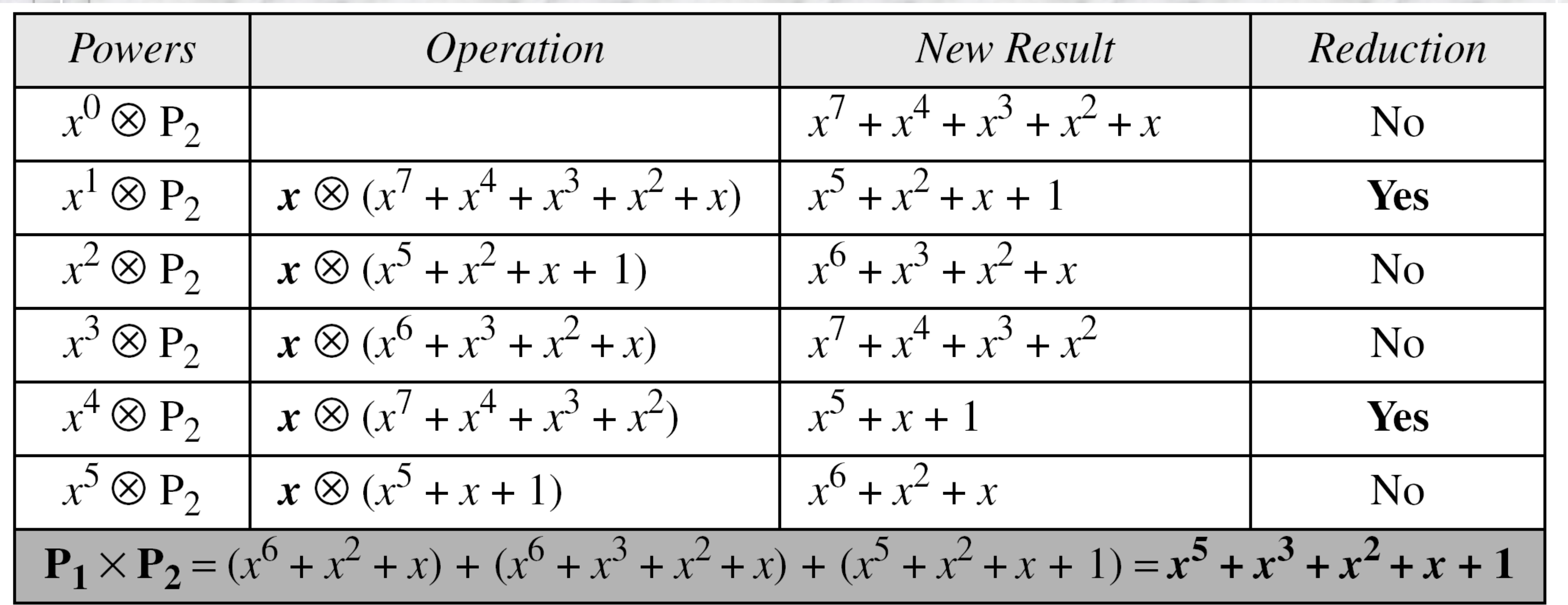
q	r_1	r_2	r	t_1	t_2	t
(x^3)	$(x^8 + x^4 + x^3 + x + 1)$	(x^5)	$(x^4 + x^3 + x + 1)$	(0)	(1)	(x^3)
$(x + 1)$	(x^5)	$(x^4 + x^3 + x + 1)$	$(x^3 + x^2 + 1)$	(1)	(x^3)	$(x^4 + x^3 + 1)$
(x)	$(x^4 + x^3 + x + 1)$	$(x^3 + x^2 + 1)$	(1)	(x^3)	$(x^4 + x^3 + 1)$	$(x^5 + x^4 + x^3 + x)$
$(x^3 + x^2 + 1)$	$(x^3 + x^2 + 1)$	(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)	

Algorithm for multiplication

Find the result of multiplying $P_1 = (x^5 + x^2 + x)$ by $P_2 = (x^7 + x^4 + x^3 + x^2 + x)$ in GF(2^8) with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$

$x^5P_2 + x^2P_2 + xP_2$ mod IRP

Multiply P_2 by x, x^2, x^3,…



Powers	*Operation*	*New Result*	*Reduction*
$x^0 \otimes P_2$		$x^7 + x^4 + x^3 + x^2 + x$	No
$x^1 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x^5 + x^2 + x + 1$	**Yes**
$x^2 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x^2 + x + 1)$	$x^6 + x^3 + x^2 + x$	No
$x^3 \otimes P_2$	$\boldsymbol{x} \otimes (x^6 + x^3 + x^2 + x)$	$x^7 + x^4 + x^3 + x^2$	No
$x^4 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2)$	$x^5 + x + 1$	**Yes**
$x^5 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x + 1)$	$x^6 + x^2 + x$	No
$\mathbf{P_1} \times \mathbf{P_2} = (x^6 + x^2 + x) + (x^6 + x^3 + x^2 + x) + (x^5 + x^2 + x + 1) = \boldsymbol{x^5 + x^3 + x^2 + x + 1}$			

- Multiplication by *x* can be achieved by one bit left shift of P_2
- Need to be reduced after multiplication if degree greater than n-1
  - i.e., previously degree was n-1 (leading bit was 1)
  - Reduction, after multiplication result is XOR-ed with IRP

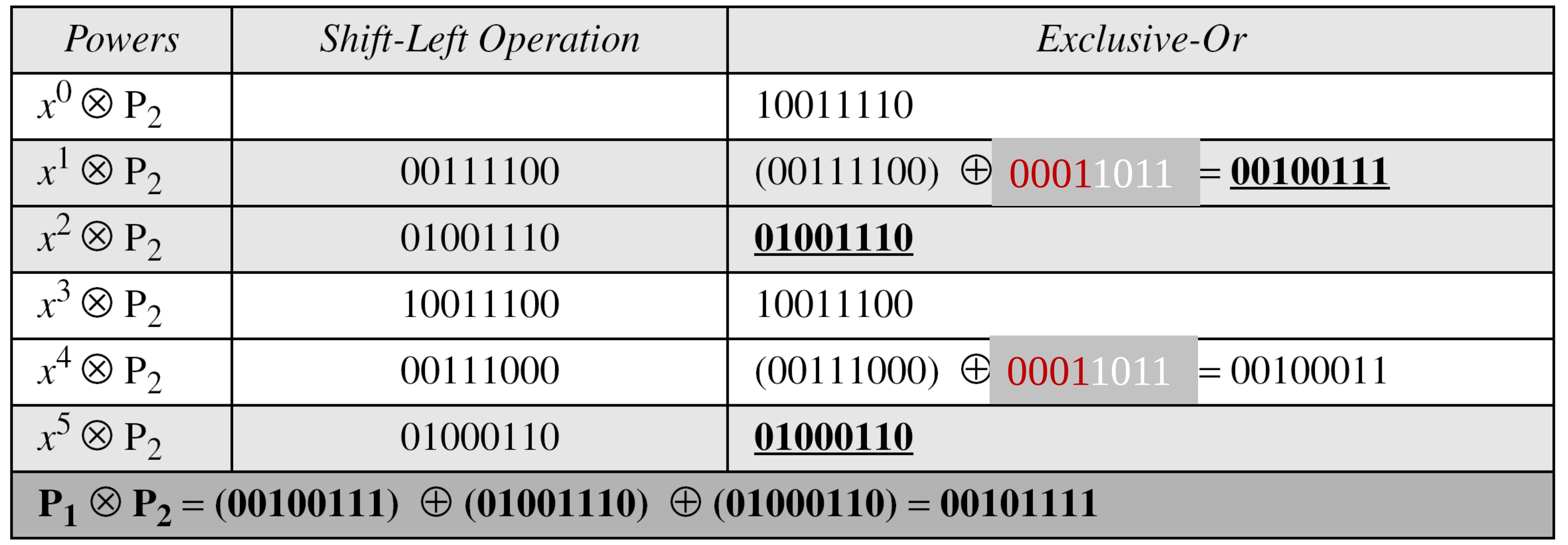
Algorithm

- if leading bit of previous result ‘0’
  - One left shift
- if leading bit of previous result ‘1’
  - One left shift
  - XOR the result with least n-1 bits of IRP
    - (note: IRP is with degree n

P1 = 00100110,

P2 = 10011110,

modulus = 100011011



Powers	*Shift-Left Operation*	*Exclusive-Or*
$x^0 \otimes P_2$		10011110
$x^1 \otimes P_2$	00111100	(00111100) $\oplus$ 00011011 = **00100111**
$x^2 \otimes P_2$	01001110	**01001110**
$x^3 \otimes P_2$	10011100	10011100
$x^4 \otimes P_2$	00111000	(00111000) $\oplus$ 00011011 = 00100011
$x^5 \otimes P_2$	01000110	**01000110**
$P_1 \otimes P_2$ = (00100111) $\oplus$ (01001110) $\oplus$ (01000110) = 00101111		

Note

- A filed GF(2^n) may have more than one irreducible polynomials
- In addition no role of irreducible polynomial where as the result of multiplication highly depends on irreducible polynomial (like mod p)

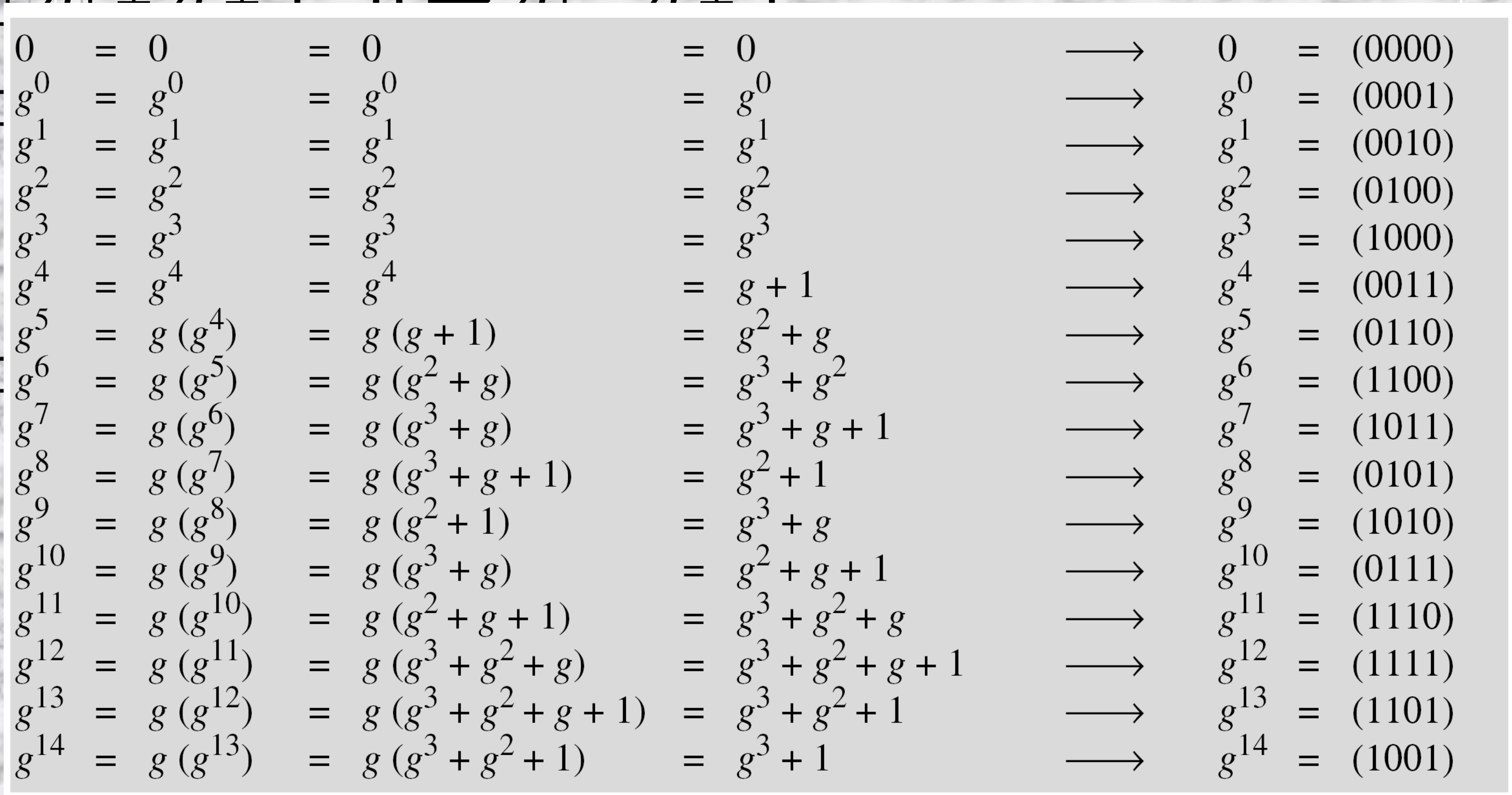
Using generator

- It is easier to define the elements of GF(2^n) using a generator
- Generator is ‘g’ where f(g)=0 for an irreducible polynomial of GF(2^n)
- Using the generator, the elements of GF(2^n) are

$$\boxed{\{0, g, g, g^2, \ldots, g^N\}, \text{ where } N = 2^n - 2}$$

Elements of GF(2^4): $x^4 + x + 1$

$g^4 + g + 1 = 0$ ➔ $g^4 = g + 1$



0	$=$	0	$=$	0	$=$	0	$\longrightarrow$	0	$=$	(0000)
g^0	$=$	g^0	$=$	g^0	$=$	g^0	$\longrightarrow$	g^0	$=$	(0001)
g^1	$=$	g^1	$=$	g^1	$=$	g^1	$\longrightarrow$	g^1	$=$	(0010)
g^2	$=$	g^2	$=$	g^2	$=$	g^2	$\longrightarrow$	g^2	$=$	(0100)
g^3	$=$	g^3	$=$	g^3	$=$	g^3	$\longrightarrow$	g^3	$=$	(1000)
g^4	$=$	g^4	$=$	g^4	$=$	$g + 1$	$\longrightarrow$	g^4	$=$	(0011)
g^5	$=$	$g\,(g^4)$	$=$	$g\,(g + 1)$	$=$	$g^2 + g$	$\longrightarrow$	g^5	$=$	(0110)
g^6	$=$	$g\,(g^5)$	$=$	$g\,(g^2 + g)$	$=$	$g^3 + g^2$	$\longrightarrow$	g^6	$=$	(1100)
g^7	$=$	$g\,(g^6)$	$=$	$g\,(g^3 + g)$	$=$	$g^3 + g + 1$	$\longrightarrow$	g^7	$=$	(1011)
g^8	$=$	$g\,(g^7)$	$=$	$g\,(g^3 + g + 1)$	$=$	$g^2 + 1$	$\longrightarrow$	g^8	$=$	(0101)
g^9	$=$	$g\,(g^8)$	$=$	$g\,(g^2 + 1)$	$=$	$g^3 + g$	$\longrightarrow$	g^9	$=$	(1010)
g^{10}	$=$	$g\,(g^9)$	$=$	$g\,(g^3 + g)$	$=$	$g^2 + g + 1$	$\longrightarrow$	g^{10}	$=$	(0111)
g^{11}	$=$	$g\,(g^{10})$	$=$	$g\,(g^2 + g + 1)$	$=$	$g^3 + g^2 + g$	$\longrightarrow$	g^{11}	$=$	(1110)
g^{12}	$=$	$g\,(g^{11})$	$=$	$g\,(g^3 + g^2 + g)$	$=$	$g^3 + g^2 + g + 1$	$\longrightarrow$	g^{12}	$=$	(1111)
g^{13}	$=$	$g\,(g^{12})$	$=$	$g\,(g^3 + g^2 + g + 1)$	$=$	$g^3 + g^2 + 1$	$\longrightarrow$	g^{13}	$=$	(1101)
g^{14}	$=$	$g\,(g^{13})$	$=$	$g\,(g^3 + g^2 + 1)$	$=$	$g^3 + 1$	$\longrightarrow$	g^{14}	$=$	(1001)

Inverse

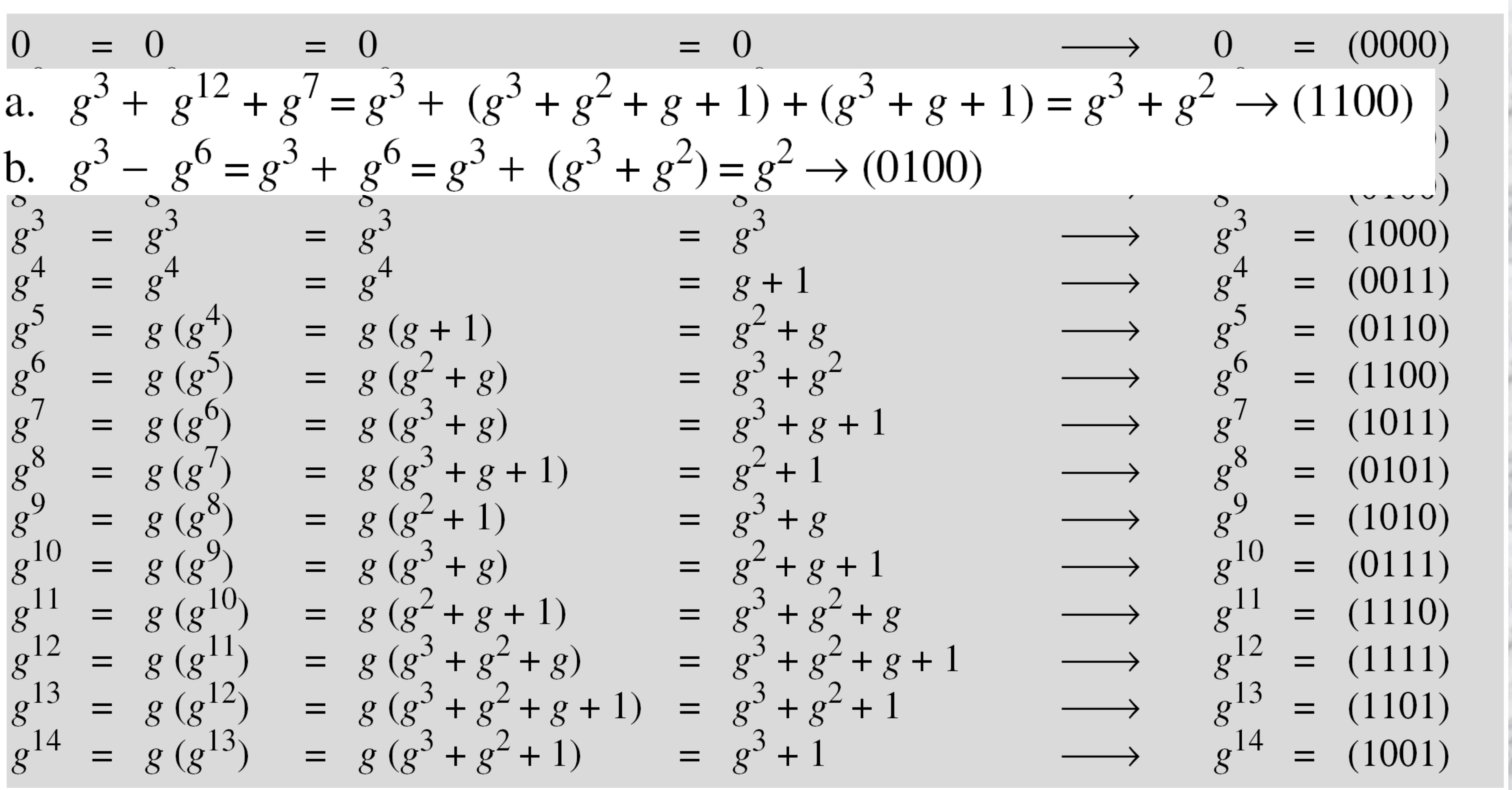
- Additive inverse: the element itself

- Multiplicative inverse: for g^i, it is g^{-i} where $-i \equiv k \bmod 2^n -1$

Operations

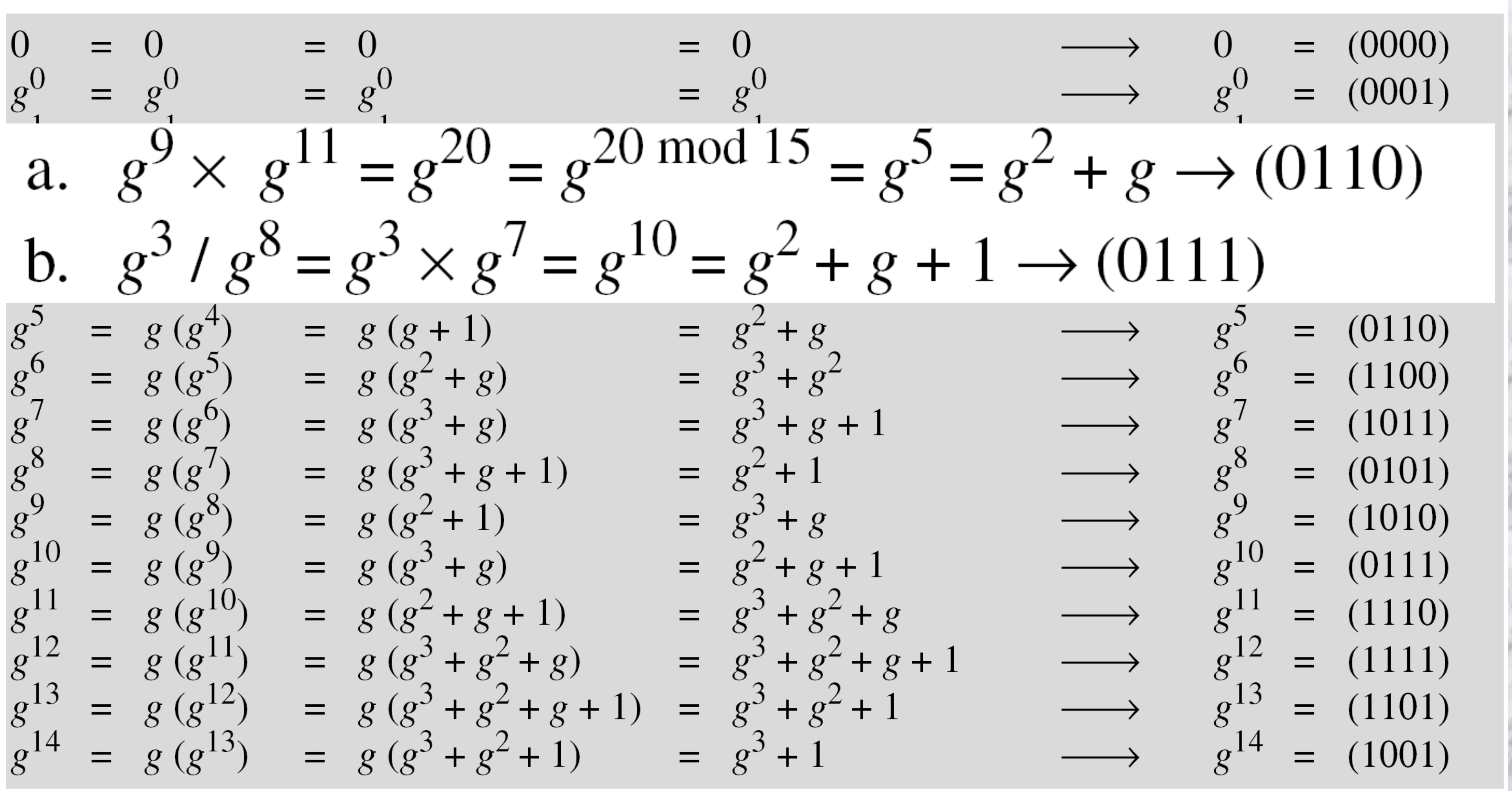
a. $g^3 + g^{12} + g^7 = g^3 + (g^3 + g^2 + g + 1) + (g^3 + g + 1) = g^3 + g^2 \rightarrow (1100)$

b. $g^3 - g^6 = g^3 + g^6 = g^3 + (g^3 + g^2) = g^2 \rightarrow (0100)$



0	$=$	0	$=$	0	$=$	0	$\longrightarrow$	0	$=$	(0000)
g^3	$=$	g^3	$=$	g^3	$=$	g^3	$\longrightarrow$	g^3	$=$	(1000)
g^4	$=$	g^4	$=$	g^4	$=$	$g + 1$	$\longrightarrow$	g^4	$=$	(0011)
g^5	$=$	$g\,(g^4)$	$=$	$g\,(g + 1)$	$=$	$g^2 + g$	$\longrightarrow$	g^5	$=$	(0110)
g^6	$=$	$g\,(g^5)$	$=$	$g\,(g^2 + g)$	$=$	$g^3 + g^2$	$\longrightarrow$	g^6	$=$	(1100)
g^7	$=$	$g\,(g^6)$	$=$	$g\,(g^3 + g)$	$=$	$g^3 + g + 1$	$\longrightarrow$	g^7	$=$	(1011)
g^8	$=$	$g\,(g^7)$	$=$	$g\,(g^3 + g + 1)$	$=$	$g^2 + 1$	$\longrightarrow$	g^8	$=$	(0101)
g^9	$=$	$g\,(g^8)$	$=$	$g\,(g^2 + 1)$	$=$	$g^3 + g$	$\longrightarrow$	g^9	$=$	(1010)
g^{10}	$=$	$g\,(g^9)$	$=$	$g\,(g^3 + g)$	$=$	$g^2 + g + 1$	$\longrightarrow$	g^{10}	$=$	(0111)
g^{11}	$=$	$g\,(g^{10})$	$=$	$g\,(g^2 + g + 1)$	$=$	$g^3 + g^2 + g$	$\longrightarrow$	g^{11}	$=$	(1110)
g^{12}	$=$	$g\,(g^{11})$	$=$	$g\,(g^3 + g^2 + g)$	$=$	$g^3 + g^2 + g + 1$	$\longrightarrow$	g^{12}	$=$	(1111)
g^{13}	$=$	$g\,(g^{12})$	$=$	$g\,(g^3 + g^2 + g + 1)$	$=$	$g^3 + g^2 + 1$	$\longrightarrow$	g^{13}	$=$	(1101)
g^{14}	$=$	$g\,(g^{13})$	$=$	$g\,(g^3 + g^2 + 1)$	$=$	$g^3 + 1$	$\longrightarrow$	g^{14}	$=$	(1001)

Operations (contd…)



0	=	0	=	0	=	0	$\longrightarrow$	0	=	(0000)
g^0	=	g^0	=	g^0	=	g^0	$\longrightarrow$	g^0	=	(0001)
g^5	=	$g\,(g^4)$	=	$g\,(g+1)$	=	g^2+g	$\longrightarrow$	g^5	=	(0110)
g^6	=	$g\,(g^5)$	=	$g\,(g^2+g)$	=	g^3+g^2	$\longrightarrow$	g^6	=	(1100)
g^7	=	$g\,(g^6)$	=	$g\,(g^3+g)$	=	g^3+g+1	$\longrightarrow$	g^7	=	(1011)
g^8	=	$g\,(g^7)$	=	$g\,(g^3+g+1)$	=	g^2+1	$\longrightarrow$	g^8	=	(0101)
g^9	=	$g\,(g^8)$	=	$g\,(g^2+1)$	=	g^3+g	$\longrightarrow$	g^9	=	(1010)
g^{10}	=	$g\,(g^9)$	=	$g\,(g^3+g)$	=	g^2+g+1	$\longrightarrow$	g^{10}	=	(0111)
g^{11}	=	$g\,(g^{10})$	=	$g\,(g^2+g+1)$	=	g^3+g^2+g	$\longrightarrow$	g^{11}	=	(1110)
g^{12}	=	$g\,(g^{11})$	=	$g\,(g^3+g^2+g)$	=	g^3+g^2+g+1	$\longrightarrow$	g^{12}	=	(1111)
g^{13}	=	$g\,(g^{12})$	=	$g\,(g^3+g^2+g+1)$	=	g^3+g^2+1	$\longrightarrow$	g^{13}	=	(1101)
g^{14}	=	$g\,(g^{13})$	=	$g\,(g^3+g^2+1)$	=	g^3+1	$\longrightarrow$	g^{14}	=	(1001)

a. $g^9 \times g^{11} = g^{20} = g^{20 \bmod 15} = g^5 = g^2 + g \rightarrow (0110)$

b. $g^3 / g^8 = g^3 \times g^7 = g^{10} = g^2 + g + 1 \rightarrow (0111)$