Course: Cryptography and Network Security
Code: CS-34310
Branch: M.C.A - 4th Semester

Lecture – 8: MATHEMATICS OF CRYPTOGRAPHY
ALGEBRAIC STRUCTURES- Part-2 : Rings and Fields

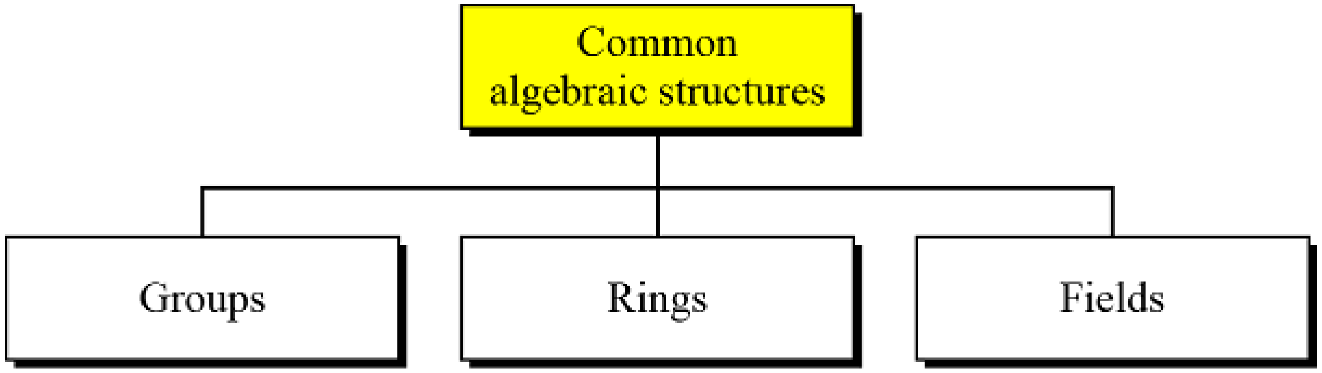
Faculty & Coordinator : Dr. J Sathish Kumar (JSK)

Department of Computer Science and Engineering

Motilal Nehru National Institute of Technology Allahabad,
Prayagraj-211004

ALGEBRAIC STRUCTURES

- Cryptography requires sets of integers and specific operations that are defined for those sets.
- The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure.
- Three common algebraic structures:
  - Groups
  - Rings, and
  - Fields.



Ring

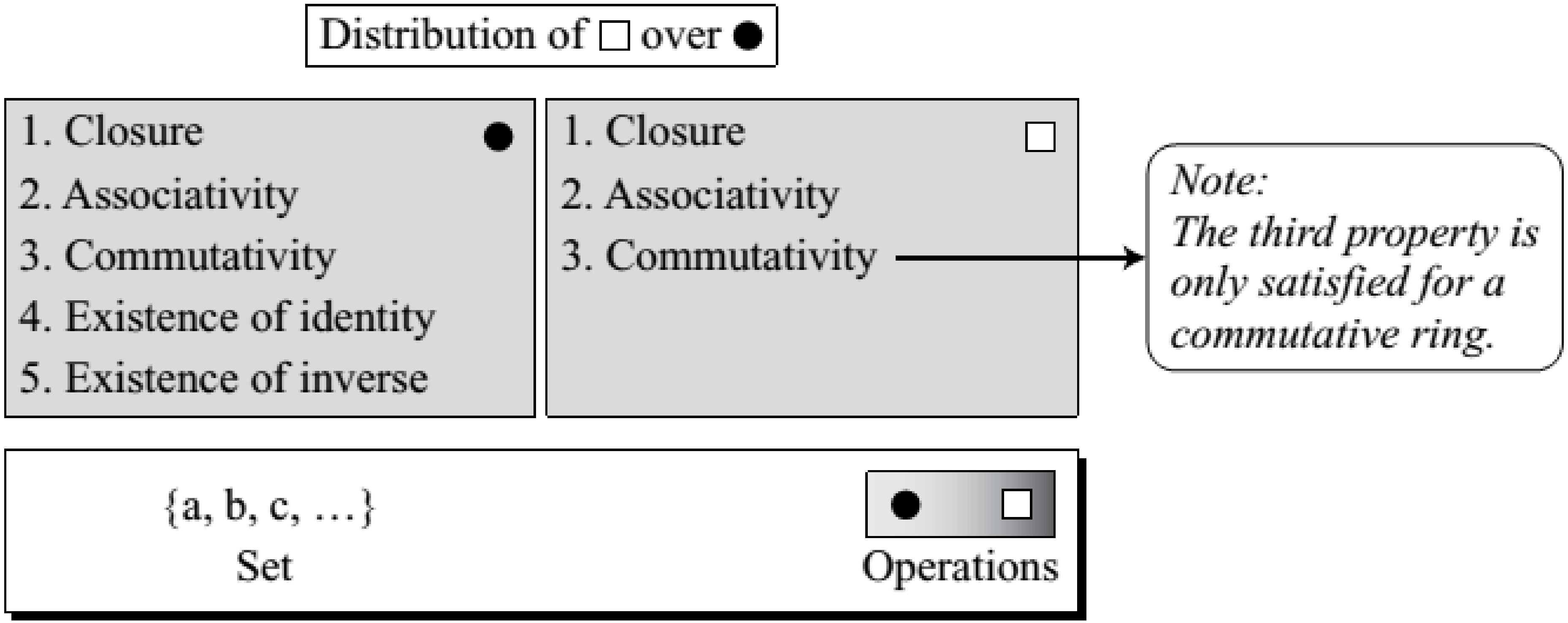
- A ring, R = <{…}, •, ■ >, is an algebraic structure with two operations.
- First operation must satisfy all five properties
- Second operation must satisfy only the first two
- In addition, second operation must be distributed over first

i.e. for all a, b, and c elements of R, we have,

a ■ (b • c) = (a ■ b) • (a ■ c) and

(a • b) ■ c = (a ■ c) • (a ■ c)

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

Ring

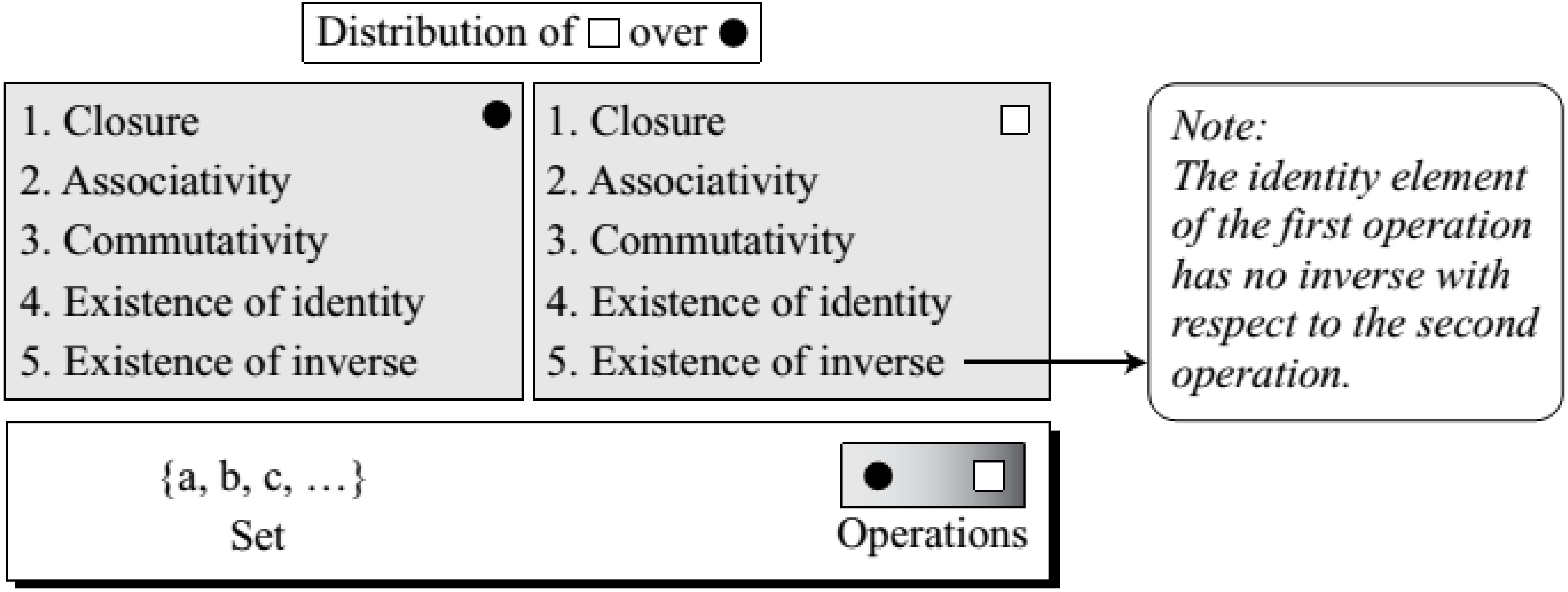
Ring

- 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.
- For example,
  - $5 \times (3 + 2) = (5 \times 3) + (5 \times 2) = 25$.
  - Although, we can perform addition and subtraction on this set, we can perform only multiplication, but not division.
  - Division is not allowed in this structure because it yields an element out of the set.
  - The result of dividing 12 by 5 is 2.4, which is not in the set.

Field

- A field, denoted by F = <{…}, •, ■ > is a commutative ring in which the second operation satisfies all five properties defined for the first operation except that the identity of the first operation has no inverse.
- Application
  - A field is a structure that supports two pairs of operations that we have used in mathematics: addition/subtraction and multiplication/division.
  - There is one exception: division by zero is not allowed.

Field



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

Fields

- Finite Fields
  - 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.

A Galois field, GF(p^n), is a finite field with p^n elements.

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

Fields

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

GF(2)

{0, 1} + ·

+	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

Addition/subtraction in GF(2) is the same as the XOR operation; multiplication/division is the same as the AND operation.

Fields

- We can define GF(5) on the set Z_5 (5 is a prime) with addition and multiplication operators.

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

GF(5) field

Summary

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

GF(2^n) FIELDS

- In cryptography, we often need to use four operations (addition, subtraction, multiplication and division).
- In other words, we need to use fields.
- However, when we work with computers, the positive integers are stored in the computers as n-bit words in which n is usually 8, 16, 32 and so on.
- Range of integers is 0 to $2^n – 1$
- Hence, the modulus is 2^n.
- So we have two choices if we want to use a field!!!!

GF(2^n) FIELDS

- We can use GF(p) with the set Z_p, where p is the largest prime number less than 2^n.
- Although this scheme works, it is inefficient because we cannot use the integers from p to $2^n - 1$.
- For example,
  - if n = 4, the largest prime less than 2^4 is 13. This means that we cannot use integers 13, 14, and 15.
  - If n = 8, the largest prime less than 2^8 is 251, so we cannot use 251, 252, 253, 254, and 255.
- We can work in GF(2^n) and uses a set of 2^n elements.
- The elements in this set are n-bit words.
- For example,
  - if n = 3, the set is {000, 001, 010, 011, 100, 101, 110, 111}
- 2^n is not prime. So, we need to define a set of n-bit words and two new operations that satisfies the properties defined for a field.

GF(2^n) FIELDS

- 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

$\oplus$	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

$\otimes$	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

An example of a GF(2^2) field

Polynomials

- A polynomial of degree $n - 1$ is an expression of the form

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

where x^i is called the i[th] term and a_i is called coefficient of the i^{th} term.

- We can represent the 8-bit word (10011001) using a polynomial.

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

- 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,

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

- This is related to the 8-bit word 00100110.

Polynomials Operations

- Operations on polynomials
  - Actually involves two operations
- Operation on coefficients and operation on polynomials
- Hence, need to define two fields for each
- What for coefficient??
  - Coefficients are made of 0 or 1; we can use the GF(2) field for this purpose.
- What for polynomials???
  - For the polynomials we need the field GF(2^n).

Polynomials

- Modulus
  - For the sets of polynomials in GF(2^n), a group of polynomials of degree *n* is defined as the modulus.
  - Such polynomials are referred to as irreducible polynomials.
- Irreducible polynomials.
  - Prime Polynomial: No polynomial in the set can divide this polynomial
  - Can not be factored into a polynomial with degree of less than n

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), $(x^5+x^3+x^2+x+1)$, $(x^5+x^4+x^3+x+1)$, $(x^5+x^4+x^3+x^2+1)$, $(x^5+x^4+x^2+x+1)$

Polynomials

- Polynomial addition
  - ***Addition and subtraction operations on polynomials are the same operation***
  - Adding two polynomials of degree n − 1 always create a polynomial with degree n − 1, which means that we do not need to reduce the result using the modulus.
- Example:
  - Let us do $(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1)$ in $GF(2^8)$.
  - We use the symbol $\oplus$ to show that we mean polynomial addition. The following shows the procedure:

$$
\begin{array}{ll}
0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 & \oplus \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 & \\
\hline
0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 & \rightarrow \quad x^5 + x^3 + x + 1
\end{array}
$$

Polynomials

- Short cut method
  - Addition in GF(2) means the exclusive-or (XOR) operation.
  - So we can exclusive-or the two words, bits by bits, to get the result.
  - In the previous example, $x^5 + x^2 + x$ is 00100110 and $x^3 + x^2 + 1$ is 00001101.
  - The result is 00101011 or in polynomial notation $x^5 + x^3 + x + 1$.

Polynomials

- Multiplication
  - The coefficient multiplication is done in GF(2).
  - The multiplying x^i by x^j results in x^{i+j}.
  - The multiplication may create terms with degree more than $n - 1$, which means the result needs to be reduced using a modulus polynomial.
- For example
  - Find the result of $(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$.

$$P_1 \otimes P_2 = x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x)$$
$$P_1 \otimes P_2 = x^{12} + x^9 + x^8 + x^7 + x^6 + x^9 + x^6 + x^5 + x^4 + x^3 + x^8 + x^5 + x^4 + x^3 + x^2$$
$$P_1 \otimes P_2 = (x^{12} + x^7 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x^5 + x^3 + x^2 + x + 1$$

Polynomials

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

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\hline
x^8 + x^4 + x^3 + x + 1 & x^{12} + x^7 + x^2 \\
 & x^{12} + x^8 + x^7 + x^5 + x^4 \\
\cline{2-2}
 & x^8 + x^5 + x^4 + x^2 \\
 & x^8 + x^4 + x^3 + x + 1 \\
\cline{2-2}
\text{Remainder} & \boxed{x^5 + x^3 + x^2 + x + 1}
\end{array}
$$

Polynomial division
with
coefficients in GF(2)

Polynomials

- Example:
  - In GF (2^4), find the inverse of (x^2 + 1) modulo (x^4 +x + 1).
- Solution
  - The answer is (x^3 + 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)	

Polynomials

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

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)	

Polynomials

- A better algorithm: Obtain the result by repeatedly multiplying a reduced polynomial by *x*.
- For example, instead of finding the result of ($x^2 \otimes$ P2), the program finds the result of ($x \otimes$ ($x \otimes$ P2)).

- Example:
  - Find the result of multiplying P1 = ($x^5 + x^2 + x$) by P_2 = ($x^7 + x^4 + x^3 + x^2 + x$) in GF($2^8$) with irreducible polynomial ($x^8 + x^4 + x^3 + x + 1$)
- Solution
  - We first find the partial result of multiplying x^0, x^1, x^2, x^3, x^4, and x^5 by P_2.
  - Note that although only three terms are needed, the product of $x^m \otimes$ P2 for *m* from 0 to 5 because each calculation depends on the previous result

Polynomials

Powers	*Operation*	*New Result*	*Reduction*
$x^0 \otimes \mathrm{P}_2$		$x^7 + x^4 + x^3 + x^2 + x$	No
$x^1 \otimes \mathrm{P}_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x^5 + x^2 + x + 1$	**Yes**
$x^2 \otimes \mathrm{P}_2$	$\boldsymbol{x} \otimes (x^5 + x^2 + x + 1)$	$x^6 + x^3 + x^2 + x$	No
$x^3 \otimes \mathrm{P}_2$	$\boldsymbol{x} \otimes (x^6 + x^3 + x^2 + x)$	$x^7 + x^4 + x^3 + x^2$	No
$x^4 \otimes \mathrm{P}_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2)$	$x^5 + x + 1$	**Yes**
$x^5 \otimes \mathrm{P}_2$	$\boldsymbol{x} \otimes (x^5 + x + 1)$	$x^6 + x^2 + x$	No
$\mathbf{P_1} \times \mathbf{P_2} = (x^6 + x^2 + x) + (x^6 + x^3 + x^2 + x) + (x^5 + x^2 + x + 1) = \boldsymbol{x^5 + x^3 + x^2 + x + 1}$			