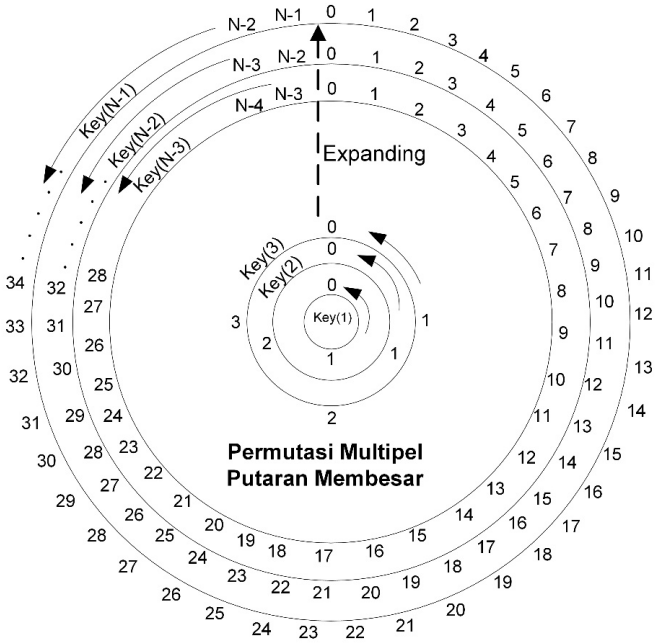


Dr. Yohan Suryanto, S.T, M.T

Semester Genap 2019/2020

MATHEMATICS OF CRYPTOGRAPHY

Algebraic Structures

source:

1. Behrouz Foroyzan, “Introduction to Cryptography and Network Security”
2. Stallings, William. "Cryptography and Network Security“

Outline

1. Algebraic Structures
2. $\mathrm{GF}(2^n)$ Fields

1 ALGEBRAIC STRUCTURES

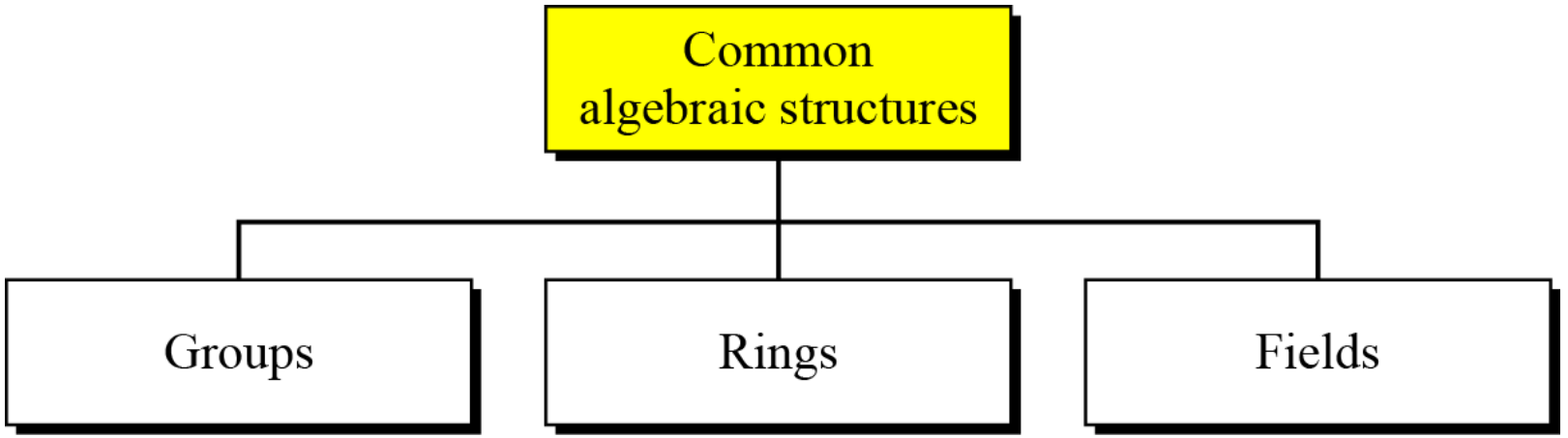
Algebraic Structures

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. In this chapter, we will define three common algebraic structues: groups, rings, and fields.

Topics discussed in this section:

1. Groups
2. Rings
3. Fields

Common algebraic structure

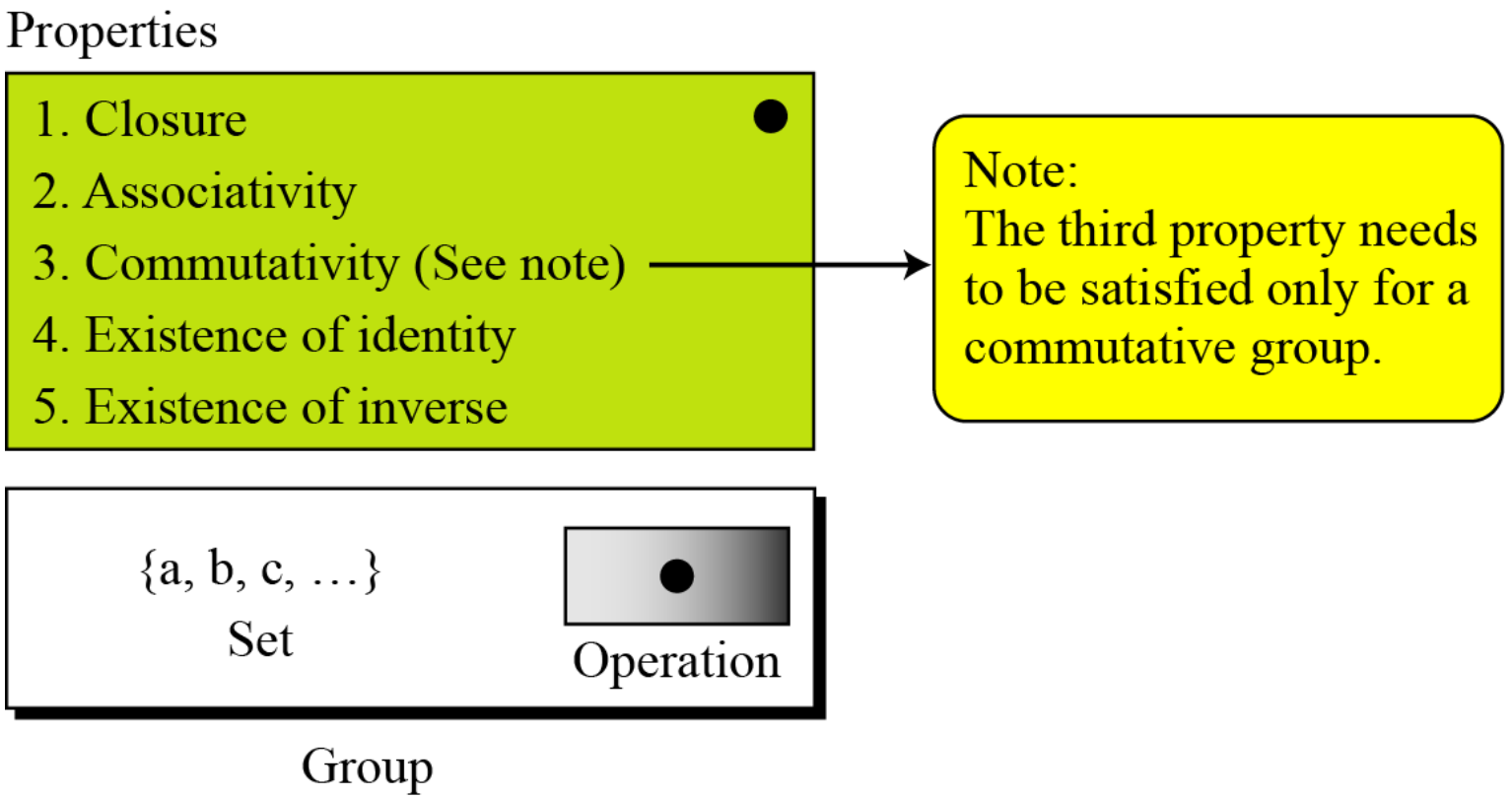


Groups

A group (G) is a set of elements with a binary operation (•) that satisfies four properties (or axioms). A commutative group satisfies an extra property, commutativity:

- Closure: If a and b belong to G, then $a \bullet b$ is also in G.
- Associativity: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all a, b, c in G.
- Commutativity: $a \bullet b = b \bullet a$ for all a, b in G.
- Existence of identity: There is an element e in G such that $a \bullet e = e \bullet a = a$ for all a in G.
- Existence of inverse: For each a in G there is an element a' in G such that $a \bullet a' = a' \bullet a = e$.

Groups Cont…


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, b, c, …}
Set
Operation
Group

Groups: Application

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 1:
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.

Example 2:
The set Z*n** with the multiplication operator, G = <Z*n**, ×>, is also an abelian group.
(Z*n** adalah set integer dalam modulus n yang memiliki inverse perkalian)

Groups: Application Cont…

Example 3:

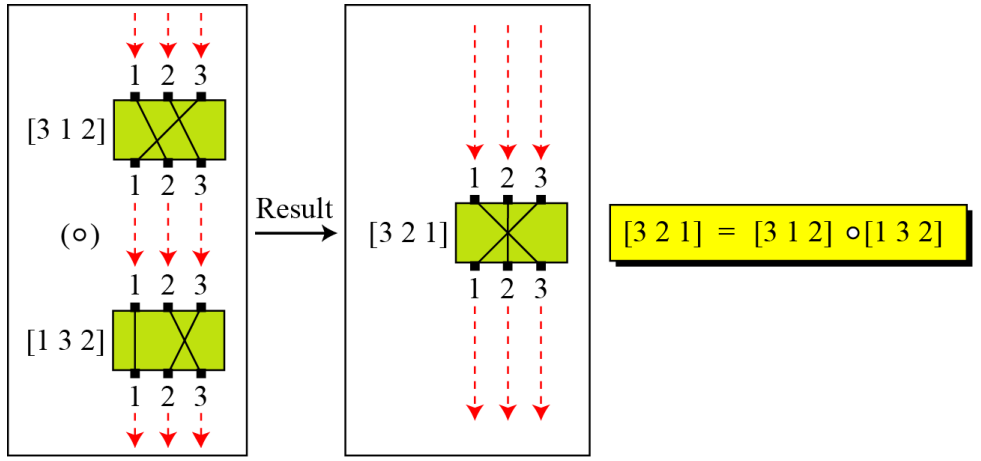
Let us define a set G = < {*a*, *b*, *c*, *d*}, •> and the operation as shown in the following Table:

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

Example 4:

A very interesting group is the permutation group. The set is the set of all permutations, and the operation is composition: applying one permutation after another.

Composition of permutation



Groups: Application Cont…

Operation table for permutation group

∘	[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]

In the previous example, we showed that a 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.

Finite and Infinite Groups

- Finite Group:
  A group is called a finite group if the set has a finite number of elements; otherwise, it is an infinite group.
- Infinite Group:
  A group with infinite number of elements;

The order of a group, |G|, is the number of elements in the group. If the group is not finite, its order is infinite; if the group is finite, the order is finite.

Subgroups

A subset H of a group G is a subgroup of G if H itself is a group with respect to the operation on G. In other words, if G = <S, • > is a group, H = <T, •> is a group under the same operation, and T is a nonempty subset of S, then H is a subgroup of G. The above definition implies that:

1. If a and b are members of both groups, then c = a • b is also a member of both groups.
2. The group share the same identity element.
3. If a is a member of both groups, the inverse of a is also a member of both groups.
4. The group made of the identity element of G, H = <{e}, •>, is a subgroup of G.
5. Each group is a subgroup of itself.

Example:
Is the group H = <Z_{10}, +> a subgroup of the group G = <Z12, +>?

Solution:
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.

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

Example 1:

Four cyclic subgroups can be made from the group G = $<Z_6, +>$. They are H1 = $<\{0\}, +>$, $H_2 = <\{0, 2, 4\}, +>$, $H_3 = <\{0, 3\}, +>$, and H_4 = G.

$0^0 \bmod 6 = 0$

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

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

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

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

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

Cyclic Subgroups Cont…

Example 2:

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 Cyclic Groups

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

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

Example:
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 $H_3 = G$.

a. The group $G = \langle Z_6, + \rangle$ is a cyclic group with two generators, $g = 1$ and $g = 5$.

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

Lagrange's Theorem

Lagrange's theorem relates the order of a group to the order of its subgroup. 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|.

In Example G = <Z6, +>, |G| = 6. The order of the subgroups are $|H_1| = 1$, $|H_2| = 3$, $|H_3| = 2$, and $|H_4| = 6$. Obviously all of these orders divide 6.

Lagrange's theorem has a very interesting application. Given a group G of order |G|, the orders of the potential subgroups can be easily determined if the divisors of |G| can be found.

For example, the order of the group G = <Z17, +> is 17. The only divisors of 17 are 1 and 17. This means that this group can have only two subgroups, H1 with the identity element and H2 = G.

Order of an Element

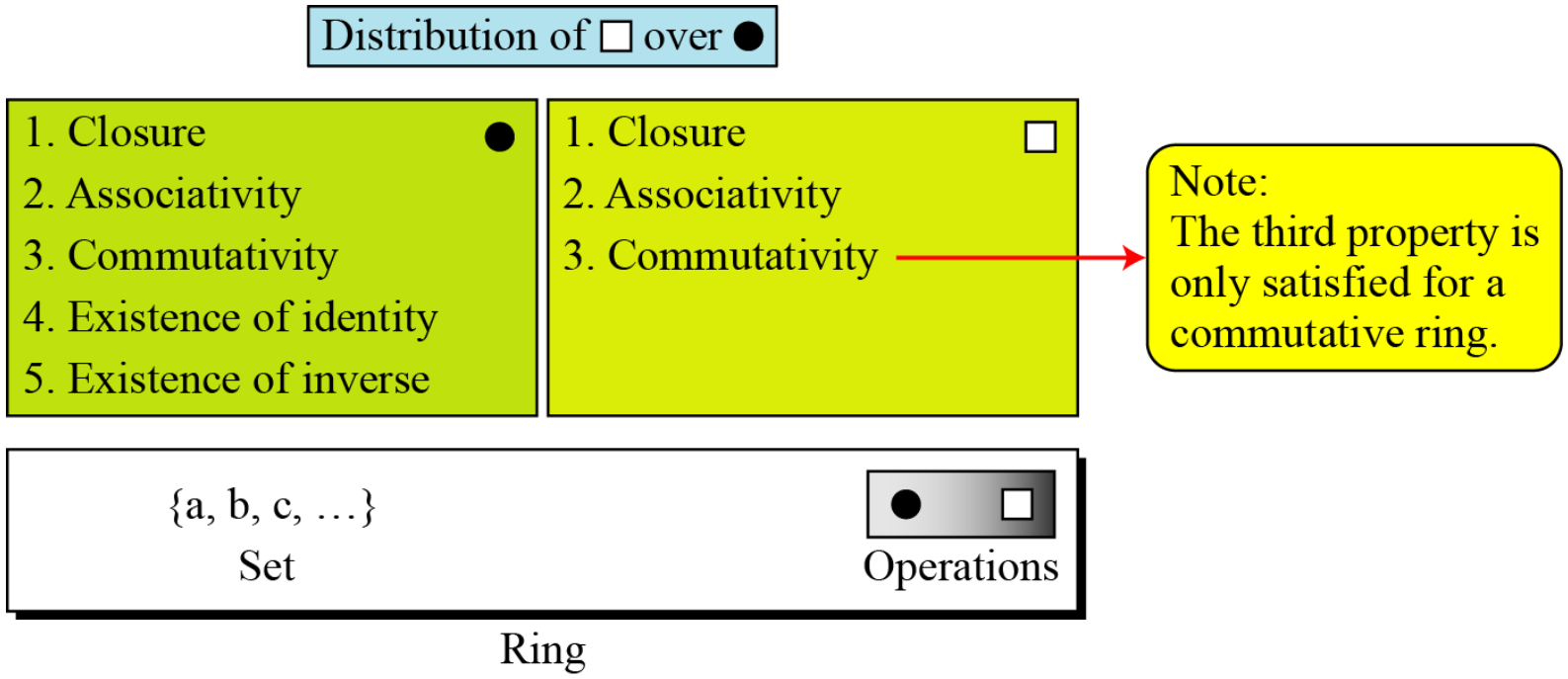
The order of an element is the order of the cyclic group it generates.

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

A ring, R = <{…}, •, □>, is an algebraic structure with two operations.

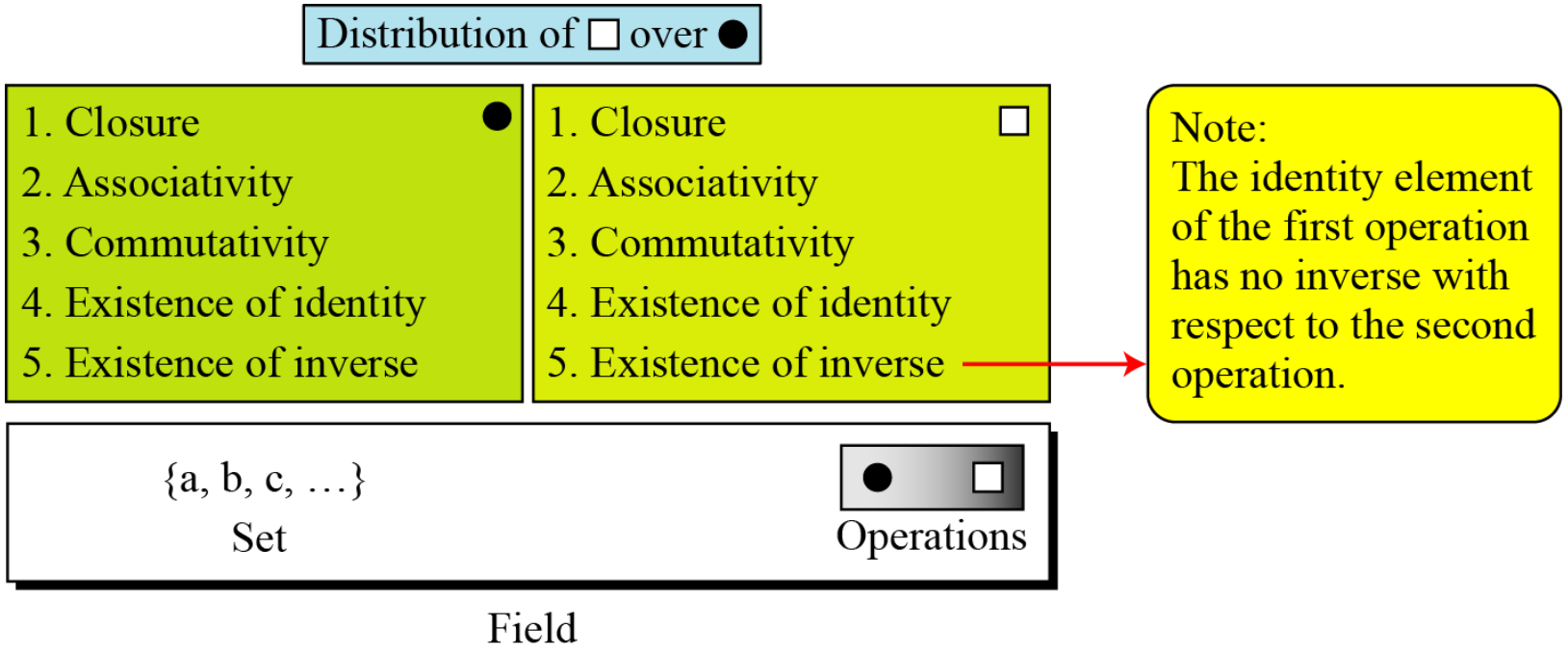


Example:

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.

Field

A ring, 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.



Finite Field: Galois

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.

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

Finite Field: Galois Cont

Example 1:

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

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

Example 2:

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

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 $(\times \ \div)$	$\mathbf{Z}_n$ or $\mathbf{Z}_n^*$
Ring	$(+ \ -)$ and $(\times)$	$\mathbf{Z}$
Field	$(+ \ -)$ and $(\times \ \div)$	$\mathbf{Z}_p$

2 GF(2^n) FIELDS

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. We can work in GF(2^n) and uses a set of 2^n elements. The elements in this set are n-bit words.

Topics discussed in this section:

1. Polynomials
2. Using A Generator
3. Summary

GF(2^n) FIELDS Example

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, as shown in the following Figure.

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

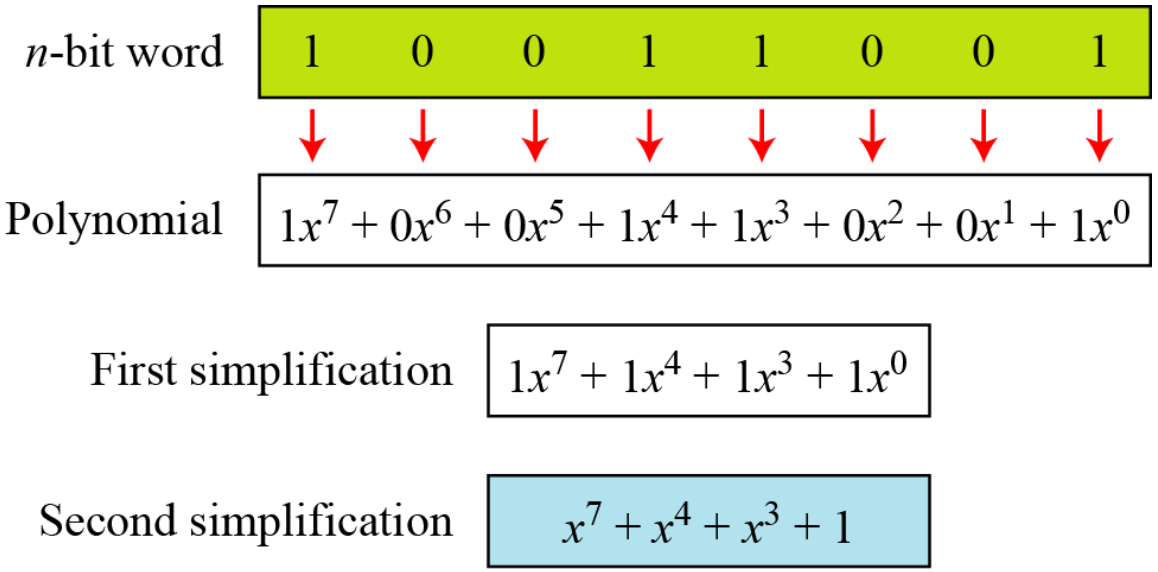
Polynomials

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 ith term and a_i is called coefficient of the ith term.

How we can represent the 8-bit word (10011001) using a polynomials:



Polynomials Cont…

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

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

This is related to the 8-bit word 00100110.

Polynomials representing *n*-bit words use two fields: GF(2) and 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.

List of irreducible polynomials

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: Addition and Subtraction

Addition and subtraction operations on polynomials are the same operation.

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:

$$
\begin{array}{ll}
0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 & \oplus \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 & \\
\text{---------- (50 dashes) ----------} & \\
0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 & \rightarrow \quad x^5 + x^3 + x + 1
\end{array}
$$

There is also another short cut. Because the 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

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.

Polynomials: Multiplication 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 ($x^8 + x^4 + x^3 + x + 1$). Note that we use the symbol $\otimes$ to show the multiplication of two polynomials.

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. Next slide (polynomial division) shows the process of division.

Polynomials: Polynomial division with coefficients in GF(2)

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

Polynomials: Inverse

Example 1:

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

Solution

The answer is ($x^3 + x + 1$) as shown in following Table:

Euclidean algorithm example 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: Inverse Cont…

Example 2:

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

Solution

The answer is ($x^5 + x^4 + x^3 + x$) as shown in following Table:

Euclidean algorithm for Example 2:

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: Multiplication using Computer

The computer implementation uses a better algorithm, repeatedly multiplying a reduced polynomial by x.

Example 1:

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 $(x^8 + x^4 + x^3 + x + 1)$ using the algorithm described above.

Solution

The process is shown in following Table. 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 $x^m \otimes P_2$ for m from 0 to 5 because each calculation depends on the previous result.

Polynomials: Multiplication using Computer Cont..

A Multiplication efficient algorithm for example 1

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
$\mathbf{P_1 \times P_2} = (x^6 + x^2 + x) + (x^6 + x^3 + x^2 + x) + (x^5 + x^2 + x + 1) = \boldsymbol{x^5 + x^3 + x^2 + x + 1}$			

Polynomials: Multiplication using Computer Cont..

Example 2:

Repeat Example 4.22 using bit patterns of size 8.

Solution

We have P1 = 000100110, P2 = 10011110, modulus = 100011010 (nine bits). We show the exclusive or operation by ⊕.

An efficient algorithm for multiplication using n-bit words

Powers	*Shift-Left Operation*	*Exclusive-Or*
$x^0 \otimes P_2$		10011110
$x^1 \otimes P_2$	00111100	(00111100) ⊕ (00011010) = **00100111**
$x^2 \otimes P_2$	01001110	**01001110**
$x^3 \otimes P_2$	10011100	10011100
$x^4 \otimes P_2$	00111000	(00111000) ⊕ (00011010) = 00100011
$x^5 \otimes P_2$	01000110	**01000110**
$P_1 \otimes P_2$ = (00100111) ⊕ (01001110) ⊕ (01000110) = 00101111		

Polynomials: Multiplication Table

The GF(2^3) field has 8 elements. We use the irreducible polynomial ($x^3 + x^2 + 1$) and show the addition and multiplication tables for this field. We show both 3-bit words and the polynomials. Note that there are two irreducible polynomials for degree 3. The other one, ($x^3 + x + 1$), yields a totally different table for multiplication.

⊕	000 (0)	001 (1)	010 (x)	011 (x + 1)	100 (x^2)	101 $x^2 + 1$	110 (x^2 + x)	111 ($x^2 + x + 1$)
000 (0)	000 (0)	001 (1)	010 (x)	011 (x + 1)	100 (x^2)	101 ($x^2 + 1$)	110 ($x^2 + x$)	111 ($x^2 + x + 1$)
001 (1)	001 (1)	000 (0)	011 (x + 1)	010 (x^2)	101 ($x^2 + 1$)	100 (x^2 + x)	111 ($x^2 + x + 1$)	110 ($x^2 + x$)
010 (x)	010 (x)	011 (x + 1)	000 (0)	001 (1)	110 ($x^2 + x$)	111 ($x^2 + x + 1$)	100 ($x^2 + x$)	101 ($x^2 + 1$)
011 (x + 1)	011 (x + 1)	010 (x)	001 (1)	000 (0)	111 ($x^2 + x + 1$)	110 ($x^2 + x$)	101 ($x^2 + 1$)	100 (x^2)
100 (x^2)	100 (x^2)	101 ($x^2 + 1$)	110 (x^2 + x)	111 ($x^2 + x + 1$)	000 (0)	001 (1)	010 (x)	011 (x + 1)
101 ($x^2 + 1$)	101 ($x^2 + 1$)	100 (x^2)	111 ($x^2 + x + 1$)	110 ($x^2 + x$)	001 (1)	000 (0)	011 (x + 1)	010 (x)
110 ($x^2 + x$)	110 (x^2 + x)	111 ($x^2 + x + 1$)	100 (x^2)	101 ($x^2 + 1$)	010 (x)	011 (x + 1)	000 (0)	001 (1)
111 ($x^2 + x + 1$)	111 ($x^2 + x + 1$)	110 ($x^2 + x$)	101 ($x^2 + 1$)	100 (x^2)	011 (x + 1)	010 (x)	001 (1)	000 (0)

Polynomials: Multiplication Table Cont..

Multiplication table for GF(2^3) using irreducible polynomial ($x^3 + x + 1$)

⊗	000 **(0)**	001 **(1)**	010 (x)	011 $(x+1)$	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)
001 (1)	000 (0)	001 (1)	010 (x)	011 $(x+1)$	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
010 (x)	000 (0)	010 (x)	100 (x)	110 (x^2+x)	101 (x^2+1)	111 (x^2+x+1)	001 (1)	011 $(x+1)$
011 $(x+1)$	000 (0)	011 $(x+1)$	110 (x^2+x)	101 (x^2+1)	001 (1)	010 (x)	111 (x^2+x+1)	100 (x)
100 (x^2)	000 (0)	100 (x^2)	101 (x^2+1)	001 (1)	111 (x^2+x+1)	011 $(x+1)$	010 (x)	110 (x^2+x)
101 (x^2+1)	000 (0)	101 (x^2+1)	111 (x^2+x+1)	010 (x)	011 $(x+1)$	110 (x^2+x)	100 (x^2)	001 (1)
110 (x^2+x)	000 (0)	110 (x^2+x)	001 (1)	111 (x^2+x+1)	010 (x)	100 (x^2)	011 $(x+1)$	101 (x^2+1)
111 (x^2+x+1)	000 (0)	111 (x^2+x+1)	011 $(x+1)$	100 (x^2)	110 (x^2+x)	001 (1)	101 (x^2+1)	010 (x)

Using a Generator

Sometimes it is easier to define the elements of the GF(2^n) field using a generator.

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

Example:

Generate the elements of the field GF(2^4) using the irreducible polynomial $f(x) = x^4 + x + 1$.

Solution

The elements 0, g^0, g^1, $g2$, and g^3 can be easily generated, because they are the 4-bit representations of 0, 1, x^2, and x^3. Elements g^4 through g^{14}, which represent x^4 though x^{14} need to be divided by the irreducible polynomial. To avoid the polynomial division, the relation $f(g) = g^4 + g + 1 = 0$ can be used (See next slide).

Using a Generator Cont…

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)

Addition and Multiplication using Generator

The following show the results of addition and subtraction 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. $g^3 - g^6 = g^3 + g^6 = g^3 + (g^3 + g^2) = g^2 \rightarrow (0100)$

The following show the result of multiplication and division operations:.

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

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

Summary

The finite field GF(2^n) can be used to define four operations of addition, subtraction, multiplication and division over *n*-bit words. The only restriction is that division by zero is not defined.

Lifelong Learning

THANKS YOU