

## **Lecture 4: Finite Fields (PART 1)**

### **PART 1: Groups, Rings, and Fields**

#### **Theoretical Underpinnings of AES and ECC**

#### **Lecture Notes on “Computer and Network Security”**

by Avi Kak (kak@purdue.edu)

January 30, 2009

©2009 Avinash Kak, Purdue University

Goal of this part:

- To review groups, rings, and fields as the fundamental elements of modern algebra.

Goals for the next part:

- To review modular arithmetic.
- To review the algorithms for finding the Greatest Common Divisor of two integers.

## 4.1: What Does It Take for a Set of Objects to Form a Group

We need four properties to be satisfied by a set of objects (along with an operation on the objects) to form a group:

1. **Closure** with respect to the operation. Closure means that if  $a$  and  $b$  are in the set, then the element  $a \circ b = c$  is also in the set. The symbol  $\circ$  denotes the operation.
2. **Associativity** with respect to the operation. Associativity means that  $(a \circ b) \circ c = a \circ (b \circ c)$ .
3. Guaranteed existence of a unique **identity element** with regard to the operation. An element  $i$  would be called an identity element if for every  $a$  in the set, we have  $a \circ i = a$ .
4. The existence of an **inverse element** for each element with regard to the operation. That is, for every  $a$  in the set, the set must also contain an element  $b$  such that  $a \circ b = i$  assuming that  $i$  is the identity element.

In general, a group is denoted by  $\{G, \circ\}$  where  $G$  is the set of objects and  $\circ$  the operation.

## 4.2: Example of a Group

- Let  $L_n = \{1, 2, \dots, n\}$  denote a set of labels for  $n$  objects. [Note that this is NOT the set that we will turn into a group. The set that we will turn into a group is the set of permutations of the labels in  $L_n$ , as explained below.]
- Let's now consider the set of all permutations of the labels in the set  $L_n$ . Denote this set by  $S_n$ . Each element of the set  $S_n$  stands for a permutation  $(p_1, p_2, p_3, \dots, p_n)$  where each  $p_i \in L_n$  and  $p_i \neq p_j$  whenever  $i \neq j$ . [What is the size of the set  $S_n$ ? Answer:  $n!$ ]
- Now consider the following binary operation on any two elements  $\rho$  and  $\pi$  of the set  $S_n$ :  $\pi \circ \rho$  **means that we want to permute the elements of  $\rho$  according to the elements of  $\pi$ .**
- To explain the above operation, consider the example on the next page.

### 4.3: An Example That Explains the Operation 'o' on the Elements of the Set $S_n$

- Let's say we have  $L_3 = \{1, 2, 3\}$  as the set of labels for some three objects.
- We will now construct a set  $S_3$  whose each element will be a distinct permutation of the set of three labels in  $L_3$ . That is,

$$S_3 = \{ (p_1, p_2, p_3) \mid p_1, p_2, p_3 \in L_3 \text{ with } p_1 \neq p_2 \neq p_3 \}$$

- Now consider the following two elements  $\pi$  and  $\rho$  in the set  $S_3$  of permutations:

$$\pi = (3, 2, 1)$$

$$\rho = (1, 3, 2)$$

- Let's now consider the following operation between the elements  $\pi$  and  $\rho$ :

$$\pi \circ \rho = (3, 2, 1) \circ (1, 3, 2)$$

To permute  $\rho$  according to the elements of  $\pi$  means that we first choose the third element of  $\rho$ , followed by the second element of  $\rho$ , and followed by the first element of  $\rho$ . The result is, of course, the permutation  $\{2, 3, 1\}$ . So we say

$$\pi \circ \rho = (3, 2, 1) \circ (1, 3, 2) = (2, 3, 1)$$

- Clearly,  $\pi \circ \rho \in S_3$ .
- This shows that  $S_3$  **closed** with respect to the operation 'o'.

#### 4.4: Going Back to Our Group Example ....

- Since it is a small enough set, we can also easily demonstrate that  $S_3$  obeys the associativity property with respect to the 'o' operator. This we can do by showing that for any three elements  $\rho_1$ ,  $\rho_2$ , and  $\rho_3$  of the set  $S_3$ , the following will always be true

$$\rho_1 \circ (\rho_2 \circ \rho_3) = (\rho_1 \circ \rho_2) \circ \rho_3$$

- The set  $S_3$  obviously contains a special element  $(1, 2, 3)$  that can serve as the identity element with respect to the operation 'o'. It is definitely the case that for any  $\rho \in S_3$  we have

$$(1, 2, 3) \circ \rho = \rho \circ (1, 2, 3) = \rho$$

- Again, because  $S_3$  is a small sized set, we can easily demonstrate that for every  $\rho \in S_3$  there exists another unique element  $\pi \in S_3$  such that

$$\rho \circ \pi = \pi \circ \rho = \textit{the identity element}$$

For each  $\rho$ , we may refer to such a  $\pi$  as  $\rho$ 's inverse. For the sake of convenience, we may use the notation  $-\rho$  for such a  $\pi$ .

- Obviously, then,  $S_3$  along with the operation 'o' is a group.

## 4.5: More about Groups

- Note that the set  $S_n$  of all permutations of the labels in the set  $L_n$  can only be finite. As a result,  $S_n$  along with the operation 'o' forms a **finite group**.
- However, a group can also be infinite. The set of *all* integers, positive, negative and zero, along with the operation of arithmetic addition is an **infinite group**.
- If the operation on the set elements is **commutative**, the group is called an **abelian group**. An operation  $\circ$  is commutative if  $a \circ b = b \circ a$ .
- Is  $\{S_n, \circ\}$  an abelian group? If not for  $n$  in general, is  $\{S_n, \circ\}$  an abelian group for any particular value of  $n$ ? [ $S_n$  is abelian for only  $n = 2$ .]
- Is the set of all integers, positive, negative, and zero, along with the operation of arithmetic addition an abelian group? [The answer is yes.]

- A group is also denoted  $\{G, +\}$ , where  $G$  denotes the set and '+' the operation.
- Note that the name of the operation, *addition*, used in the context of defining a group may have nothing to do with your usual arithmetic definition of addition.

## 4.6: If the Group Operation is referred to as Addition, then a Group also Allows for Subtraction

- A group is guaranteed to have a special element, the identity element. The identity element of a group is frequently denoted by the symbol 0.

- For every element  $\rho_1$ , the group must contain its inverse element  $\rho_2$  such that

$$\rho_1 + \rho_2 = 0$$

where the operator '+' is the group operator.

- So if we maintain the illusion that we want to refer to this operation as addition, we can think of  $\rho_2$  is the additive inverse of  $\rho_1$  and even denote it by  $-\rho_1$ . We can therefore write

$$\rho_1 + (-\rho_1) = 0$$

or more compactly as  $\rho_1 - \rho_1 = 0$ .

- In general

$$\rho_1 - \rho_2 = \rho_1 + (-\rho_2)$$

where  $-\rho_2$  is the additive inverse of  $\rho_2$  with respect to the group operator  $+$ . **We may now refer to an expression of the sort  $\rho_1 - \rho_2$  as representing subtraction.**

## 4.7: Rings

- If we can define one more operation on an **abelian group**, we have a **ring**, provided the elements of the set satisfy some properties with respect to this new operation also.
- Just to set it apart from the operation defined for the abelian group, we will refer to the new operation as *multiplication*. **Note that the use of the name 'multiplication' for the new operation is merely a notational convenience.**
- A ring is typically denoted  $\{R, +, \times\}$  where  $R$  denotes the set of objects, '+' the operator with respect to which  $R$  is an abelian group, the '×' the additional operator needed for  $R$  to form a ring.

#### 4.8: Rings: Properties of the Elements with Respect to the Other Operator

- $R$  must be **closed** with respect to the additional operator ' $\times$ '.
- $R$  must exhibit **associativity** with respect to the additional operator ' $\times$ '.
- The additional operator (that is, the “multiplication operator”) must **distribute** over the group addition operator. That is

$$\begin{aligned} a \times (b + c) &= a \times b + a \times c \\ (a + b) \times c &= a \times c + b \times c \end{aligned}$$

- The “multiplication” operation is frequently shown by just concatenation in such equations:

$$\begin{aligned} a(b + c) &= ab + ac \\ (a + b)c &= ac + bc \end{aligned}$$

## 4.9: Examples of a Ring

- For a given value of  $N$ , the set of all  $N \times N$  square matrices over the real numbers under the operations of **matrix addition** and **matrix multiplication** constitutes a **ring**.
- The set of all **even integers**, positive, negative, and zero, under the operations arithmetic addition and multiplication is a **ring**.
- The set of **all integers** under the operations of arithmetic addition and multiplication is a **ring**.
- The set of **all real numbers** under the operations of arithmetic addition and multiplication is a **ring**.

## 4.10: Commutative Rings

- A **ring** is **commutative** if the **multiplication operation** is commutative for all elements in the ring. That is, if all  $a$  and  $b$  in  $R$  satisfy the property

$$ab = ba$$

- Examples of a **commutative ring**:
  - The set of all **even integers**, positive, negative, and zero, under the operations arithmetic addition and multiplication.
  - The set of **all integers** under the operations of arithmetic addition and multiplication.
  - The set of **all real numbers** under the operations of arithmetic addition and multiplication.

## 4.11: Integral Domain

An **integral domain**  $\{R, +, \times\}$  is a **commutative ring** that obeys the following two additional properties:

- **ADDITIONAL PROPERTY 1:** The set  $R$  must include an **identity element** for the **multiplicative operation**. That is, it should be possible to symbolically designate an element of the set  $R$  as '1' so that for every element  $a$  of the set we can say

$$a1 = 1a = a$$

- **ADDITIONAL PROPERTY 2:** Let 0 denote the identity element for the **addition operation**. If a multiplication of any two elements  $a$  and  $b$  of  $R$  results in 0, that is if

$$ab = 0$$

then either  $a$  or  $b$  **must be** 0.

- Examples of an **integral domain**:
  - The set of **all integers** under the operations of arithmetic addition and multiplication.
  - The set of **all real numbers** under the operations of arithmetic addition and multiplication.

## 4.12: Fields

A **field**, denoted  $\{F, +, \times\}$ , is an **integral domain** whose elements satisfy the following additional property:

- For **every element**  $a$  in  $F$ , except the element designated 0 (the identity element for the '+' operator), there must also exist in  $F$  its **multiplicative inverse**. That is, if  $a \in F$  and  $a \neq 0$ , then there must exist an element  $b \in F$  such that

$$ab = ba = 1$$

where '1' symbolically denotes the element which serves as the identity element for the multiplication operation. For a given  $a$ , such a  $b$  is often designated  $a^{-1}$ .

### 4.13: Positive and Negative Examples of Fields

- The set of **all real numbers** under the operations of arithmetic addition and multiplication **is a field**.
- The set of **all rational numbers** under the operations of arithmetic addition and multiplication **is a field**.
- The set of **all complex numbers** under the operations of complex arithmetic addition and multiplication **is a field**.
- The set of all **even integers**, positive, negative, and zero, under the operations arithmetic addition and multiplication **is NOT a field**.
- The set of **all integers** under the operations of arithmetic addition and multiplication **is NOT a field**.