

# CSCI 124/224

## Discrete Structures II: Groups – Definition and Examples

Poorvi L. Vora

In this module, we attempt to look at the similarities between the affine and shift ciphers using the notion of a group

### 1 A Group

**Definition 2:** A *group* is a set  $G$  with an associated operation  $\diamond$ , such that the following hold:

- *Closure*  
 $G$  is closed under the operation, i.e.  $x, y \in G \Rightarrow x \diamond y \in G$ .
- *Associativity*  
The operation is associative, i.e.  $(x \diamond y) \diamond z = x \diamond (y \diamond z)$
- *Identity*  
There is an element  $e \in G$  such that  $x \diamond e = e \diamond x = x$ . The element  $e$  is known as the *identity*
- *Inverses exist*  
Every element has an inverse in  $G$ , i.e.  $\forall g \in G, \exists \bar{g} \in G$  such that  $\bar{g} \diamond g = g \diamond \bar{g} = e$ .

Notice that the operation is very much like addition, however, it is not always commutative. Examples of a group include:  $\mathbb{R}$ , the real numbers, with addition as the operation;  $\mathbb{Q}$ , the rational numbers with addition as the operation;  $\mathbb{Z}$  the integers, with addition as the operation;  $\mathcal{R}/\{0\}$  (the real numbers without the number 0) under multiplication;  $n \times m$  matrices for any integers  $m, n$ , under addition; any vector space under vector addition (including, for example, the integer lattice); the complex  $n^{\text{th}}$  roots of one under multiplication. All the above examples are *abelian* groups, that is the operation  $\diamond$  is also commutative ( $a \diamond b = b \diamond a$ ). The set of invertible  $n \times n$  matrices is a non-abelian group under multiplication.

### 2 An Example

To see that  $\mathcal{R}$  with  $\diamond = +$  is a group, we check each of the requirements of a group:

- *Closure*  
Suppose  $x, y \in \mathcal{R}$ , i.e.  $x$  and  $y$  are real numbers. Their sum,  $x + y$  is also real, i.e.  $x + y \in \mathcal{R}$ . Hence the closure condition holds.

- *Associativity*  
Addition is associative, i.e.  $(x + y) + z = x + (y + z)$  so associativity holds.
- *Identity*  
Consider the element 0.  $0 \in \mathcal{R}$ , and  $x + 0 = 0 + x = x$ . Hence the identity exists.
- *Inverses exist*  
Given  $r \in R$ , consider  $\bar{r} = -r$ . It is a member of  $\mathcal{R}$  too, and  $\bar{r} \diamond r = (-r) + r = 0 = e$ . Hence inverses exist.

You should similarly show that the other examples above are groups.

### 3 $\mathbb{Z}_m$ as a group under addition mod $m$

An example of a group is the set of remainders mod  $m$ ,  $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$  under addition modulo  $m$ . For  $a, b \in \mathbb{Z}_m$ ,  $a \diamond b = (a + b) \text{ MOD } m$ .

To see that it is a group, we check each of the requirements of a group:

- *Closure*  
Suppose  $x, y \in \mathbb{Z}_m$ . Their sum,  $x + y \text{ MOD } m$  is also in  $\mathbb{Z}_m$ . Hence the closure condition holds.
- *Associativity*  
Addition over the integers is associative, i.e.  $(x + y) + z = x + (y + z)$ , and hence it is also associative modulo  $m$ , and so associativity holds.
- *Identity*  
Consider the element  $0 \in \mathbb{Z}_m$ , and  $x + 0 \text{ MOD } m = 0 + x \text{ MOD } m = x \text{ MOD } m$ . Hence the identity exists.
- *Inverses exist*  
Given  $x \in \mathbb{Z}_m$ , consider  $\bar{x} = m - x \text{ MOD } m$ . It is a member of  $\mathbb{Z}_m$ , and  $\bar{x} \diamond x = m \text{ MOD } m = 0 \text{ MOD } m = e$ . Hence inverses exist.

The shift cipher now is as follows:

$$e_K : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$$

$$e_K(g) = g \diamond K$$

$$d_K : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$$

$$d_K(g) = g \diamond \bar{K}$$

### 4 $\mathbb{Z}_m$ as a group under multiplication mod $m$ ?

Consider the set of remainders modulo  $m$  under multiplication. Is this a group?

- *Closure*  
Suppose  $x, y \in \mathbb{Z}_m$ . Their product,  $x \times y \text{ MOD } m$  is also in  $\mathbb{Z}_m$ . Hence the closure condition holds.
- *Associativity*  
Multiplication over the integers is associative, i.e.  $(x \times y) \times z = x \times (y \times z)$ , and hence it is also associative *modulo*  $m$ , and so associativity holds.
- *Identity*  
Consider the element  $1 \in \mathbb{Z}_m$ , and  $x \times 1 \text{ MOD } m = 1 \times x \text{ MOD } m = x \text{ MOD } m$ . Hence the identity exists.
- *Inverses?*  
Given  $x \in \mathbb{Z}_m$ ,  $\bar{x}$  is that integer,  $0 \leq \bar{x} < m$ , such that  $x\bar{x} = 1$ . Such a value does not always exist.

If it were a group, the affine cipher for  $b = 0$  could be expressed as:

$$e_K : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$$

$$e_K(g) = g \diamond K$$

$$d_K : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$$

$$d_K(g) = g \diamond \bar{K}$$

where  $\diamond$  is multiplication *MOD*  $m$ .

## 5 When does $x \in \mathbb{Z}_m$ have a multiplicative inverse?

Consider the encryption function:

$$f : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$

$$f(x) = 3x \text{ MOD } 26$$

Its inverse  $g$  would be such that

$$g : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$$

$$3g(x) = x \text{ MOD } 26$$

We have seen that  $g(x) \neq \frac{x}{3}$  because that might not always be an element of  $\mathbb{Z}_{26}$ . However, as mentioned by one of the students in the class in the Fall 2006 semester, maybe we could get an element in  $\mathbb{Z}_{26}$  if we added multiples of 26 to  $x$  before dividing by 3.

For example, if  $x = 10$ ,  $f(x) = 30 \text{ MOD } 26 = 4$ , and  $g(4) \neq \frac{4}{3}$ . However,  $g(4) = \frac{4+26}{3} = 10$ .

We use the same idea when determining if  $x \in \mathbb{Z}_m$  has a multiplicative inverse. If  $x$  has an inverse, we denote it as  $\bar{x}$ . Then:

$$x\bar{x} = 1 \text{ MOD } m$$

and

$$\bar{x} \neq \frac{1}{x} \text{ MOD } m$$

However,  $\exists k \in \mathbb{Z}$  such that

$$x\bar{x} = 1 + mk$$

and

$$\bar{x} = \frac{1 + mk}{x} \text{ MOD } m$$

This idea leads to the following more formal statement.

**Theorem**  $x$  is invertible modulo  $m$  if and only if  $\exists a, b \in \mathbb{Z}$  such that  $ax + bm = 1$ .

*Proof:* We need to show that  $\bar{x}$  exists  $\Leftrightarrow \exists a, b \in \mathbb{Z}$  s.t.  $ax + bm = 1$ .

$\Rightarrow$ :

$\bar{x}$  exists

$$\Rightarrow \exists \bar{x} \in \mathbb{Z}_m \text{ s.t. } x\bar{x} = 1 \text{ MOD } m$$

$$\Rightarrow \exists \bar{x}, k \in \mathbb{Z} \text{ s.t. } x\bar{x} = 1 + km$$

$$\Rightarrow \exists \bar{x}, k \in \mathbb{Z} \text{ s.t. } x\bar{x} - km = 1$$

$$\Rightarrow \exists a = \bar{x} \in \mathbb{Z}, \text{ and } b = -k \in \mathbb{Z} \text{ s.t. } ax + bm = 1$$

$\Leftarrow$ :

$$\exists a, b \in \mathbb{Z} \text{ s.t. } ax + bm = 1$$

$$\Rightarrow \exists a, b \in \mathbb{Z} \text{ s.t. } (a \text{ MOD } m)x + lmx + bm = 1 \text{ (where } a = (a \text{ MOD } m) + lm)$$

$$\Rightarrow \exists \bar{x} = (a \text{ MOD } m) \in \mathbb{Z}_m \text{ s.t. } \bar{x}x = 1 \text{ MOD } m$$

If we had a means of determining whether such values of  $a$  and  $b$  exist, we could answer questions such as: how many keys for the affine cipher exist for a particular value of  $m$ ? In the next section, we address an algorithm for determining if such  $a$  and  $b$  exist.