

CS 5319  
Advanced Discrete Structure

Lecture 11:  
Introduction to Group Theory I

# Outline

- Introduction
- Groups and Subgroups
- Generators
- Cosets (and Lagrange's Theorem)
- Permutation Group (and Burnside's Theorem)
- Group Codes

# Introduction

# Introduction

- Let  $A$  and  $B$  be two sets. A function of the form  $A \times A \rightarrow B$  is called a **binary operation on  $A$**

Ex : Consider a vending machine which delivers

coke            if we insert two \$10 coins

water          if we insert \$5 + \$10 coins

gum            if we insert two \$5 coins

The operations of the machine is a **binary operation on  $\{ \$5, \$10 \}$**

# Introduction

- Intuitively, a binary operation specifies how two elements are combined to get an output
- Let  $f$  denote a binary operation on  $A$
- For easier understanding, we usually write

$$a_1 f a_2 \text{ instead of } f(a_1, a_2)$$

- We also usually use “operator symbols” such as  $+$ ,  $\times$ ,  $\oplus$ ,  $\star$ ,  $\cdot$ ,  $\cup$ ,  $\cap$ ,  $\dots$  as names of binary operations

Ex : We may use  $+$  to name the previous operation.

Then we have  $+(\$5, \$10) = \$5 + \$10 = \text{water}$

# Introduction

- In this lecture, we shall encounter mostly binary operations of the form  $A \times A \rightarrow A$
- Such binary operation is said to be **closed**

Ex : Suppose the hair color of a child is determined by the hair colors of its parents :

	Mother		
Father	light	dark	
light	light	dark	
dark	dark	dark	
			Child

This is a **closed**  
binary operation

# Introduction

- A binary operation  $\star$  on a set  $A$  is said to be **associative** if for any  $a, b, c$  in  $A$

$$(a \star b) \star c = a \star (b \star c)$$

- It follows that we can write  $(a \star b) \star c$  as  $a \star b \star c$  without any possible confusion

Ex : Let  $A =$  a set of people with distinct height

$\Delta =$  a binary operation on  $A$ , such that

$a \Delta b =$  the taller one of  $a$  and  $b$

Then  $\Delta$  is an associative operation

# Introduction

- The notion of binary operation can be extended immediately
  - A **ternary** operation on a set  $A$  is a function from  $(A \times A) \times A$  to some set  $B$
  - An  **$m$ -ary** operation on a set  $A$  is a function from  $A^m$  to some set  $B$



# Introduction

- A set, together with a number of operations on the set, is called an **algebraic system**
- We denote  $(A, \oplus, \star, \cdot)$  for an algebraic system, where  $A$  is a set and  $\oplus, \star, \cdot$  are operations on  $A$

Ex : Let  $A = \{ \$5, \$10 \}$ , and  $+$  be a binary operation such that

$$\$5 + \$5 = \text{gum}, \quad \$10 + \$10 = \text{coke},$$

$$\$5 + \$10 = \$10 + \$5 = \text{water}$$

Then  $(A, +)$  is an algebraic system

# Introduction

Ex :  $(N, +, \times)$  is an algebraic system,

where  $N$  = natural numbers, and

$+, \times$  = usual addition and multiplication

Ex : Let  $\oplus$  be a binary operation such that

$$(a, b) \oplus = (a + b) \text{ rem } 2$$

Let  $\Delta$  be a ternary operation such that

$$\Delta(a, b, c) = \max \text{ of } a, b, c$$

Then  $(N, \oplus, \Delta)$  is an algebraic system

# Groups and Subgroups

# Groups and Subgroups

- Let  $(A, \star)$  be an algebraic system, where  $\star$  is a binary operation on  $A$

Definition:  $(A, \star)$  is called a **semigroup** if

1.  $\star$  is a closed operation ; and
2.  $\star$  is an associative operation

Ex :  $(\mathbb{N}, +)$  is a semigroup

Ex : Let  $S =$  all binary strings,  $\cdot =$  concatenation

$(S, \cdot)$  is a semigroup

# Groups and Subgroups

- Let  $(A, \star)$  be an algebraic system, where  $\star$  is a binary operation on  $A$

Definition: An element  $e$  in  $A$  is said to be a **left identity**, if for every  $x$  in  $A$

$$e \star x = x$$

An element  $e$  in  $A$  is said to be a **right identity**, if for every  $x$  in  $A$

$$x \star e = x$$

# Groups and Subgroups

Ex : In the algebraic system  $(N, \times)$ , the element 1 is both a left identity and a right identity

Ex :

$\star$	$\alpha$	$\beta$	$\gamma$	$\delta$
$\alpha$	$\delta$	$\alpha$	$\beta$	$\gamma$
$\beta$	$\alpha$	$\beta$	$\gamma$	$\delta$
$\gamma$	$\alpha$	$\beta$	$\gamma$	$\gamma$
$\delta$	$\alpha$	$\beta$	$\gamma$	$\delta$

- In this algebraic system, both  $\beta$  and  $\delta$  are left identities
- There are no right identities

# Groups and Subgroups

- Let  $(A, \star)$  be an algebraic system, where  $\star$  is a binary operation on  $A$

Definition: If  $e$  in  $A$  is both a left identity and a right identity, then we say  $e$  is an **identity**

- Suppose  $e_1$  is a left identity,  $e_2$  is a right identity

$$\rightarrow e_1 = e_1 \star e_2 = e_2$$

This implies that there is at most one identity

# Groups and Subgroups

- Let  $(A, \star)$  be an algebraic system, where  $\star$  is a binary operation on  $A$

Definition:  $(A, \star)$  is called a **monoid** if

1.  $\star$  is a closed operation ;
2.  $\star$  is an associative operation ; and
3. There is an identity

Ex :  $(N, \times)$  is a monoid, but  $(N, +)$  is not

Here, we assume  $N = \{ 1, 2, 3, \dots \}$



# Groups and Subgroups

- Let  $(A, \star)$  be an algebraic system with identity  $e$

Definition: An element  $a$  in  $A$  is said to be a **left inverse** of an element  $b$  if

$$a \star b = e$$

An element  $a$  in  $A$  is said to be a **right inverse** of an element  $b$  if

$$b \star a = e$$

# Groups and Subgroups

Ex : In the algebraic system  $(\mathbb{Z}, +)$ , 0 is the identity.  
 For each integer  $x$ ,  $-x$  is both a left inverse  
 and a right inverse

Ex :

$\star$	$\alpha$	$\beta$	$\gamma$	$\delta$
$\alpha$	$\alpha$	$\beta$	$\gamma$	$\delta$
$\beta$	$\beta$	$\delta$	$\alpha$	$\gamma$
$\gamma$	$\gamma$	$\beta$	$\beta$	$\alpha$
$\delta$	$\delta$	$\alpha$	$\gamma$	$\delta$

- In this algebraic system,  $\alpha$  is the identity
- $\Rightarrow \beta$  is a left inverse of  $\gamma$
- $\Rightarrow \delta$  is a right inverse of  $\gamma$

# Groups and Subgroups

- Let  $(A, \star)$  be an algebraic system with an identity

Definition: If an element  $a$  in  $A$  is both a left inverse and a right inverse of an element  $b$ , then we say  $a$  is an **inverse** of  $b$

Ex : In  $(\mathbb{Z}, +)$ ,  $-3$  is an inverse of  $3$ .

Clearly,  $3$  is an inverse of  $-3$ .

# Groups and Subgroups

- Let  $(A, \star)$  be an algebraic system, where  $\star$  is a binary operation on  $A$

Definition:  $(A, \star)$  is called a **group** if

1.  $\star$  is a closed operation ;
2.  $\star$  is an associative operation ;
3. There is an identity ; and
4. Every element in  $A$  has a left inverse

Ex :  $(\mathbb{Z}, +)$  is a group, but  $(\mathbb{N}, \times)$  is not

# Groups and Subgroups

Lemma 1:

Let  $(A, \star)$  be a group. A left inverse of an element  $a$  is also a right inverse of  $a$

Proof:

Let  $b =$  left inverse of  $a$

$c =$  left inverse of  $b$

$e =$  identity

# Groups and Subgroups

Proof (cont) :

First, we have :

$$(c \star (b \star a) \star b) = c \star e \star b = e$$

Also, we have :

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

$$\rightarrow a \star b = e$$

$\rightarrow b$  is also a right inverse of  $a$

# Groups and Subgroups

Lemma 2:

Let  $(A, \star)$  be a group. The inverse of an element  $a$  is unique. We denote this inverse by  $a^{-1}$

Proof:

Suppose  $b$  and  $c$  are both inverses of  $a$

Then we have :

$$b = (b \star a) \star b = (c \star a) \star b = c$$

# Some Examples of Groups

Ex :  $G = \{ 0, 1 \}$ ,  $a \oplus b = (a + b) \text{ rem } 2$

→  $(G, \oplus)$  is a group

Ex :  $Z_n = \{ 0, 1, \dots, n - 1 \}$ ,  $a \oplus_n b = (a + b) \text{ rem } n$

→  $(Z_n, \oplus_n)$  is a group

Ex :  $R = \{ 0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ \}$ ,

$a \star b =$  overall angular rotation to successive rotations by  $a$  and then  $b$

→  $(R, \star)$  is a group



# Groups and Subgroups

- Let  $(A, \star)$  be a group

Definition: If  $\star$  is commutative, that is,

$$a \star b = b \star a \quad \text{for any } a \text{ and } b,$$

then we say  $(A, \star)$  is a commutative group, or an abelian group

Ex :  $(\mathbb{Z}, +)$  is an abelian group

Let  $M =$  all non-singular  $n \times n$  matrixes

$\rightarrow (M, \times)$  is not abelian

# Groups and Subgroups

- Let  $(A, \star)$  be a group

Definition: If  $A$  is finite, then  $(A, \star)$  is called a **finite group** (otherwise,  $A$  is an infinite group)

The size of  $A$  is called the **order** of the group

Ex :  $(\mathbb{Z}, +)$  is an infinite group

$(\mathbb{Z}_n, \oplus_n)$  is a finite group, whose order is  $n$

# Groups and Subgroups

- Let  $(A, \star)$  be a group. Let  $B$  be a subset of  $A$

Definition: If  $(B, \star)$  is also a group, we call it a **subgroup** of  $(A, \star)$

Ex : Let  $E$  denote all even integers.

Then  $(E, +)$  is a subgroup of  $(\mathbb{Z}, +)$

Ex : Let  $R$  and  $\star$  be as defined on Page 24.

Then  $(\{0^\circ, 180^\circ\}, \star)$  is a subgroup of  $(R, \star)$

# Groups and Subgroups

- To check whether  $(B, \star)$  is a subgroup of  $(A, \star)$ , we should test :
  1. Whether  $\star$  is a closed operation on  $B$  ;
  2. Whether the identity element is in  $B$  ;
  3. Whether each element in  $B$  has an inverse.

We can skip the checking of associative property of  $\star$  since we know  $(A, \star)$  is a group, so that it must be associative

# Groups and Subgroups

- In fact, if  $B$  is finite, we have a easier checking for whether  $(B, \star)$  is a subgroup of  $(A, \star)$

Theorem 1:

Let  $(A, \star)$  be a group, and  $B$  be a subset of  $A$ .

If  $B$  is finite, then

$(B, \star)$  is a subgroup of  $(A, \star)$

if  $\star$  is a closed operation on  $B$

# Groups and Subgroups

Proof : Let  $a$  be an element of  $B$ .

Consider the elements  $a, a^2, a^3, \dots$ . By pigeonhole principle, there exist  $j < k$  such that  $a^j = a^k$

- $a^{k-j}$  = identity of  $(A, \star)$ , since  $a^j = a^{k-j} \star a^j$ , so that it must also be the identity  $e$  of  $(B, \star)$

- If  $k - j > 1$  :  $a \star a^{k-j-1} = a^{k-j} = e$

Else  $k - j = 1$  :  $a \star a = e \star e = e$

➔ In both cases the inverse of  $a$  exists