



**Virtual University of Pakistan**  
FEDERAL GOVERNMENT UNIVERSITY

COMPLETE SLIDES

# Sets and Logic

MTH104

**Order Your VU Books Now**

Get all Virtual University books in high-quality hard copy, delivered right to your doorstep. Visit [vubookshop.pk](http://vubookshop.pk)



Order Now

# Sets and Logic





# Introduction

- ▶ What is this course?
- ▶ Why do we study it?
- ▶ What is the relation between sets and logic?



# Introduction

In mathematics, a proof is a demonstration that, assuming certain axioms, some statement is necessarily true. That is, proof is a logical argument, not an empirical one. One must demonstrate that a proposition is true in all cases before it is considered a theorem of mathematics. An unproven proposition for which there is some sort of empirical evidence is a conjecture. Mathematical logic is the framework upon which rigorous proofs are built. It is the study of the principles and criteria of valid inference and demonstrations.



# Introduction

In set theory, we study sets, which are informally collection of objects. Although any type of object can be collected into a set, set theory is applied most often to objects that are relevant to mathematics. A rigorous analysis of set theory belongs to the foundations of mathematics and mathematical logic. A Set Theorist explores what is provable—and what is not provable—when one is allowed to use all of the usual tools of mathematical constructions and proofs (tools such as: creating



# Introduction

function spaces, completions of various kinds of objects, taking quotients, forming products, induction and recursion, etc.).



# Basic Concepts of Sets



# Sets and Elements

A fundamental concept in all branches of mathematics is that of a set. A set is any well-defined list, collection, or class of objects. The objects in sets, as we shall see from our examples, can be anything: numbers, people, letters, rivers, etc. These objects are called the elements or members of the set.



# Some Examples of Sets

- 1) The numbers 1, 3, 7 and 10.
- 2) The solution of the equation  $x^2 - 3x - 2 = 0$ .
- 3) The vowels of the english alphabet:  
a, e, i, o, u.
- 4) The people living on the earth.
- 5) The even integers 2, 4, 6, ....



# Notation

Sets will usually be denoted by capital letters

A, B, X, Y,...

The elements in our sets will usually be represented by lower case letters

a, b, x, y,...

If we define a particular set by actually listing its members, for example, let A consists of the numbers 1, 3, 7 and 10, then we write

$A = \{1, 3, 7, 10\}$   $1 \in A$   $2 \notin A$  belongs to

The statement “p belongs to A” is written as  $p \in A$ . The statement that p is not an element of A, is written  $p \notin A$



# Notation

that is, the elements are separated by commas and enclosed in brackets  $\{ \}$ . We call this the tabular form of a set.

But if we define a particular set by stating properties which its elements must satisfy, for example, let  $B$  be the set of all even numbers, then we use a letter, usually  $x$ , to represent an arbitrary element and we write

$$B = \{ \underline{x} \mid \underline{x \text{ is even}} \}$$

We call this the set-builder form of a set.



# Examples

1) Let  $E = \{x \mid x^2 - 3x + 2 = 0\} = \{1, 2\}$   
observe that  $1 \in E$ ,  $3 \notin E$ .

2)  $A = \{x \mid x \text{ is a vowel}\} = \{a, e, i, o, u\}$

3) Let  $F = \{x \mid x \in P, \underline{3 < x} < \underline{12}\}$   
where  $P = \{1, 2, 3, 4, \dots\}$

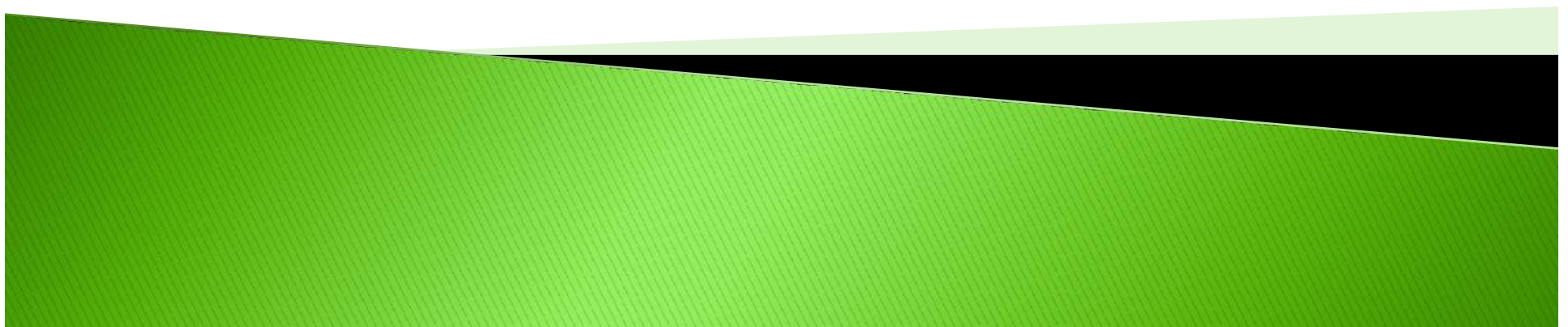
$$F = \{4, 5, 6, 7, 8, 9, 10, 11\}$$



# Examples



# Empty Set, Subsets and Universal Set



# Universal Set

All sets under investigation in any application of set theory are assumed to be contained in some large fixed set called the universal set or universe. We will denote the universal set by  $U$ .

Examples are given below:

- In plane geometry, the universal set consists of all points in the plane.
- In human population studies the universal set consists of all people in the world.



# Empty Set

It is convenient to introduce the concept of the empty set, that is, a set which contains no elements. This set is sometimes called the null set. We denote it by symbol  $\emptyset$ .



# Some Examples

1. Let  $A$  be the set of people in the world who are older than 200 years.
2. Let  $B = \{x \mid x^2 = 4, x \text{ is odd}\}$ . Then  $B$  is the empty set.
3. The set  $S = \{x : x \text{ is a positive integer, } x^2 = 3\}$  has no elements since no positive integer has the required property.

$$S = \emptyset$$



# Subsets

Suppose every element in a set  $A$  is also an element of a set  $B$  ; then  $A$  is called a subset of  $B$ . We also say that  $A$  is *contained in*  $B$  or  $B$  *contains*  $A$ . This relationship is written

$$A \subseteq B \quad \text{or} \quad B \supseteq A$$

$$A = \{1, 2\} , \quad B = \{1, 2, 3\}$$





# Examples

□ Consider the sets

$$\overset{\checkmark}{A} = \{1, 3, 5, 8, 9\}, \quad \overset{\checkmark}{B} = \{1, 2, 3, 5, 7\}, \quad \overset{\checkmark}{C} = \{1, 5\}$$

Then  $C \subseteq A$  and  $C \subseteq B$  . But  $B \not\subseteq A$ .

□ The set  $A = \{2, 3, 4, 5\}$  is not a subset of  $B = \{x : x \text{ is even}\}$   
since  $3 \in A$  but  $3 \notin B$ .

$$\Rightarrow \{2, 4, 6, \dots\}$$



# Properties of Sets

- Every set  $A$  is a subset of the universal set  $U$  since, by definition, all the elements of  $A$  belong to  $U$ . Also empty set  $\emptyset$  is a subset of  $A$ .
- Every set  $A$  is a subset of itself since, trivially, the elements of  $A$  belong to  $A$ .  $A \subseteq A$
- If  $A \subseteq B$  and  $B \subseteq C$ , then  $A \subseteq C$ .
- If  $A \subseteq B$  and  $B \subseteq A$ , then  $A = B$ .



# Proper Subset

If  $A \subseteq B$ , then it is still possible that  $A = B$ . When  $A \subseteq B$  but  $A \neq B$ , we say that  $A$  is a proper subset of  $B$ .

For example, suppose

$$A = \{1, 2\}, \quad B = \{1, 2, 3\}, \quad C = \{1, 3, 2\}$$


Then  $A$  and  $B$  are both subsets of  $C$ ; but  $A$  is a proper subset of  $C$ , whereas  $B$  is not a proper subset of  $C$ .



# Set Operations



# Set Operations

In this topic, we will study a number of set operations, including the basic operations of union, intersection, and difference of sets, where new sets will be assigned to pairs of sets  $A$  and  $B$ .



# Union and Intersection

The union of two sets  $A$  and  $B$ , denoted by  $A \cup B$ , is the set of all elements which belong to  $A$  or  $B$ ; that is

$$A \cup B = \{\underline{x} : x \in A \text{ or } x \in B\}$$

The intersection of two sets  $A$  and  $B$ , denoted by  $A \cap B$ , is the set of all elements which belong to both  $A$  and  $B$ ; that is

$$A \cap B = \{x : x \in A \text{ and } x \in B\}$$



# Example 1

Let  $A = \{1, \overset{\checkmark}{2}, \overset{\checkmark}{3}, 4\}$ ,  $B = \{3, 4, 5, 6, 7\}$ ,  $C = \{\overset{\checkmark}{2}, \overset{\checkmark}{3}, 8, 9\}$ .

Then

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7\}, \quad A \cap B = \{3, 4\}$$

$$A \cup C = \{1, 2, 3, 4, 8, 9\}, \quad A \cap C = \{2, 3\}$$

$$B \cup C = \{3, 4, 5, 6, 7, 2, 8, 9\}, \quad B \cap C = \{3\}$$
$$= \{2, 3, 4, 5, 6, 7, 8, 9\}$$



## Example 2

Let  $U$  denote the set of students at a university, and let  $M$  and  $F$  denote, respectively, the set of male and female students at the university. Then

$$M \cup F = U$$

since each student in  $U$  is either in  $M$  or in  $F$ . On the other hand,

$$\underline{M \cap F} = \underline{\emptyset}$$

since no students belong to both  $M$  and  $F$ .





# Some Properties of Union and Intersection

For any set A and B, we have

1)  $A \cap B \subseteq A$  and  $A \cap B \subseteq B$

2)  $A \subseteq A \cup B$  and  $B \subseteq A \cup B$

By combining the above two results, we can write

$$\underline{A \cap B \subseteq A} \subseteq A \cup B \text{ and } A \cap B \subseteq B \subseteq A \cup B$$



# Complement

Complement of a set  $A$ , denoted by  $A^c$ , is the set of elements which belong to  $U$  but which do not belong to  $A$ ; that is,

$$A^c = \{x : x \in U, x \notin A\}$$



## Example 3

Let  $U = \{a, b, c, \dots, y, z\}$  be the universal set, and let  
 $A = \{a, b, c, d, e\}$ ,  $B = \{e, f, g\}$ ,  $V = \{a, e, i, o, u\}$

Then

$$A^c = \{f, g, h, \dots, v, z\}$$

$$B^c = \{a, b, c, d, h, i, \dots, v, z\}$$

$$V^c = \text{consonants}$$



## Example 4

Suppose the set R of real numbers is the universal set.  
 $\mathbb{Q}$  denotes the set of rational numbers. Hence  $\mathbb{Q}^c$  will  
denote the set of irrational numbers.

$$\mathbb{Q} = \left\{ \frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0 \right\} \quad \left\{ \sqrt{2}, \sqrt{3} \right\}$$

*irrational*

$$\mathbb{Q}^c = ?$$



# Difference of Sets

Let  $A$  and  $B$  be sets. The difference of  $A$  and  $B$ , denoted by  $A/B$ , is the set of elements which belong to  $A$  but which do not belong to  $B$  ; that is,

$$A / B = \{x : x \in A, x \notin B\}$$

Many texts denote  $A/B$  by  $A-B$ .



## Example 5

Consider the sets

$$A = \{1, 2, 3, 4\}, \quad B = \{3, 4, 5, 6, 7\}, \quad C = \{6, 7, 8, 9\}$$

Then

$$A/B = \{1, 2\} \checkmark$$

$$B/C = \{3, 4, 5\}$$

$$B/A = \{5, 6, 7\} \checkmark$$

$$C/B = \{8, 9\}$$



# Symmetric Difference

The symmetric difference of the sets  $A$  and  $B$ , denoted by

$$A \oplus B = (A \cup B) / (A \cap B)$$

or

$$A \oplus B = \underline{(A / B)} \cup \underline{(B / A)}$$



## Example 6

Consider the sets

$$A = \{1, 2, 3, 4\}, \quad B = \{3, 4, 5, 6, 7\}, \quad C = \{6, 7, 8, 9\}$$

Then

$$A \oplus B = (A \cup B) / (A \cap B) = \{1, 2, 3, 4, 5, 6, 7\} / \{3, 4\} \\ = \{1, 2, 5, 6, 7\}$$

$$B \oplus C = \{3, 4, 5, 6, 7, 8, 9\} / \{6, 7\} \\ = \{3, 4, 5, 8, 9\}$$



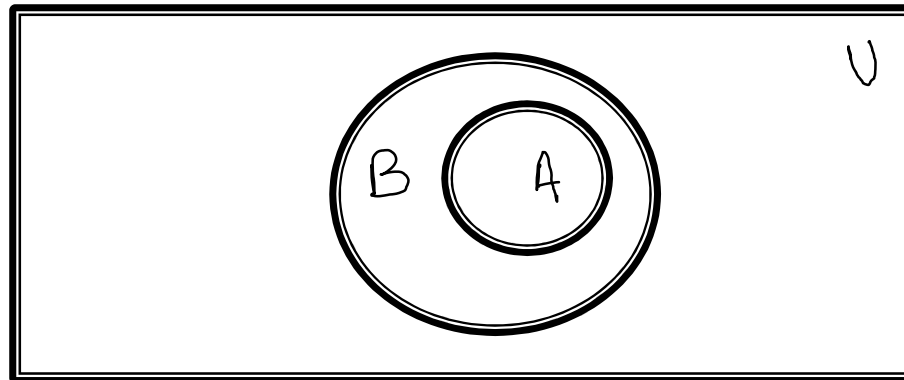


# Venn Diagrams



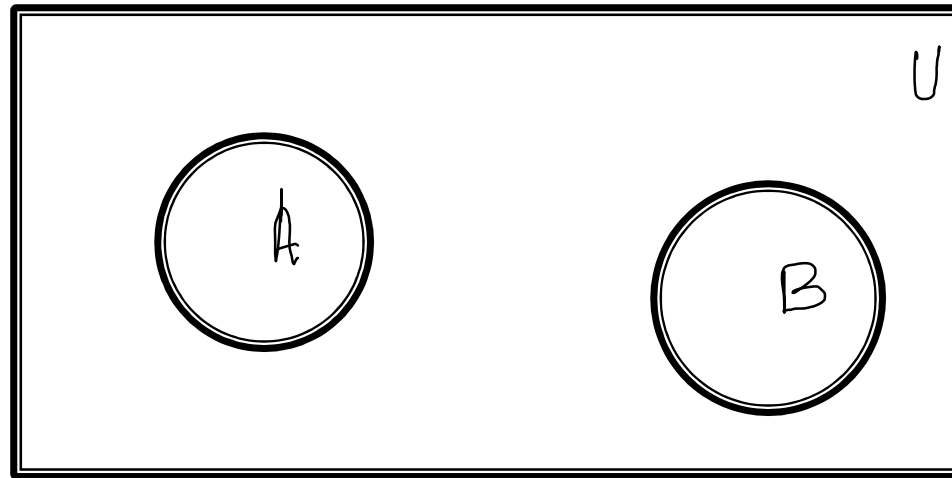
# Venn Diagrams

A Venn diagram is a pictorial representation of sets where sets are represented by enclosed areas in the plane. The universal  $U$  represented by the points in a rectangle, and other sets are represented by disks lying within the rectangle. If  $A \subseteq B$ , then the disks representing  $A$  will entirely within the disk representing  $B$ , as shown in the following figure.



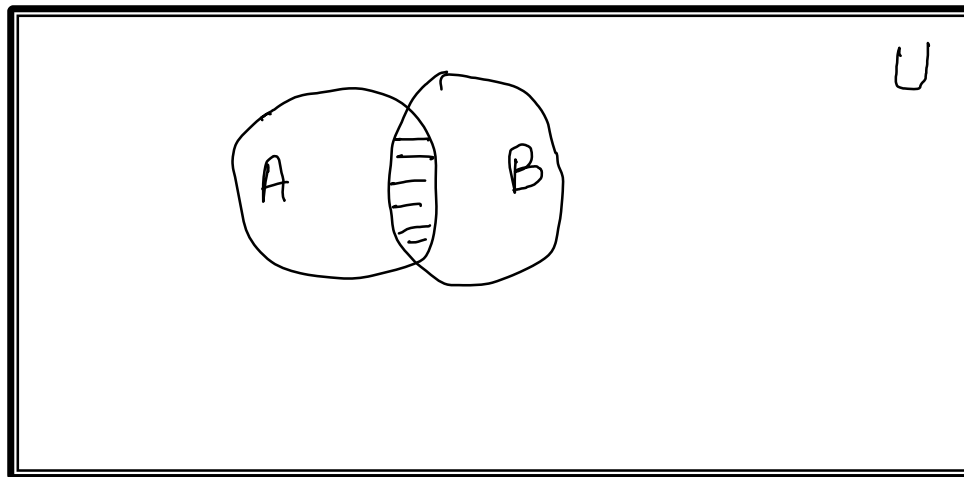
# Venn Diagrams

If  $A$  and  $B$  are disjoint, then the disk representing  $A$  will be separated from the disk representing  $B$ , as in the following figure.



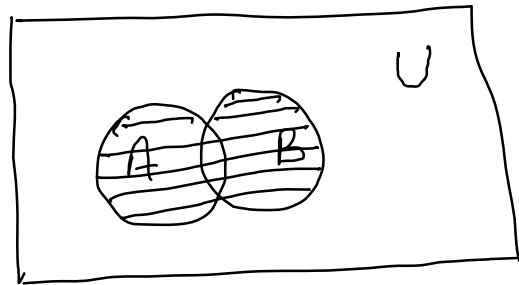
# Venn Diagrams

On the other hand, if  $A$  and  $B$  are two arbitrary sets, it is possible that some elements are in  $A$  but not in  $B$ , some elements are in  $B$  but not in  $A$ , some are in both  $A$  and  $B$ , and some are in neither  $A$  nor  $B$ ; hence, in general, we represent  $A$  and  $B$  as in the following way.

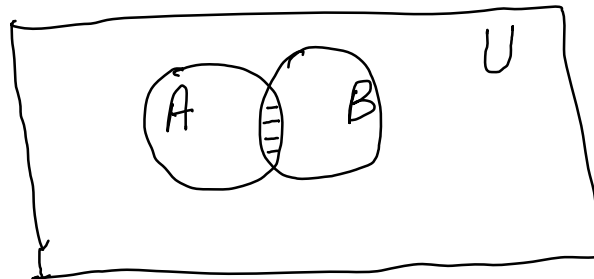


# Some Examples

1) Union of  $A$  and  $B$

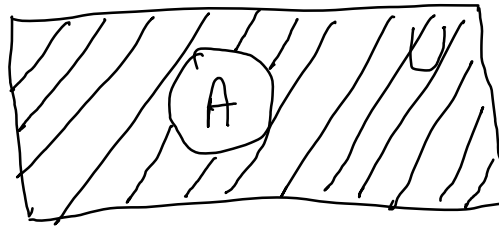


2) Intersection of  $A$  and  $B$



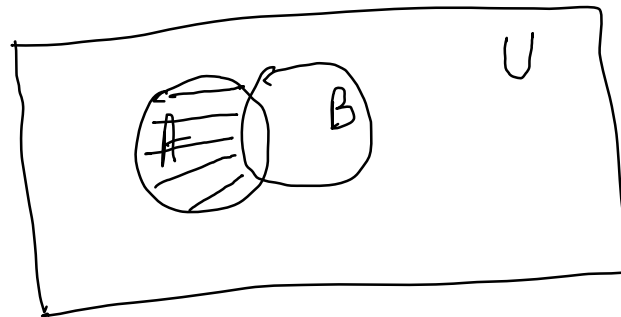
# Examples

## 3) Complement of $A$



$$A^c = U - A$$

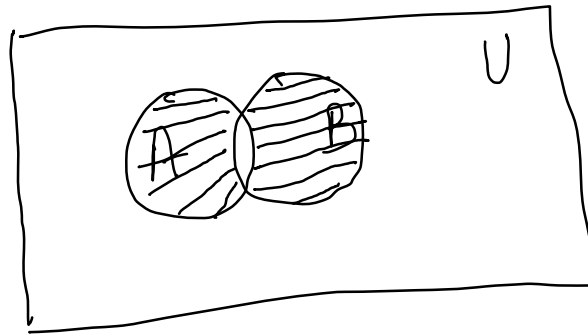
## 4) Difference of $A$ and $B$



$$A - B = \{x \mid x \in A, x \notin B\}$$

# Examples

7) Symmetric difference of  $A$  and  $B$



$$A \oplus B = (A \cup B) \setminus (A \cap B)$$



# Algebra of Sets, Duality





# Laws of the Algebra of Sets

Sets under the operations of union, intersection and complement satisfy various laws(identities). Which are listed below one by one.

## ❖ Idempotent Laws

$$A \cup A = A \text{ and } A \cap A = A$$

$$\underline{A \cup A = A}$$

$$\begin{aligned} \text{L.H.S} &= A \cup A \\ &= \{x: \underline{x \in A} \text{ or } \underline{x \in A}\} \\ &= \{x: x \in A\} = A \end{aligned}$$

$$\underline{A \cap A = A}$$

$$\begin{aligned} \text{L.H.S} &= A \cap A \\ &= \{x: \underline{x \in A} \text{ and } \underline{x \in A}\} \\ &= \{x: x \in A\} = A \end{aligned}$$



# Laws of the Algebra of Sets

## ❖ Associative Laws

$$A \cup (B \cup C) = (A \cup B) \cup C$$

and

$$A \cap (B \cap C) = (A \cap B) \cap C$$

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$\begin{aligned} \text{L.H.S.} &= A \cup (B \cup C) \\ &= \{x : x \in A \text{ or } x \in (B \cup C)\} \\ &= \{x : \underline{x \in A} \text{ or } \underline{x \in B} \text{ or } x \in C\} \\ &= \{x : x \in A \cup B \text{ or } x \in C\} = (A \cup B) \cup C \end{aligned}$$


# Laws of the Algebra of Sets

## ❖ Commutative Laws

$$A \cup B = B \cup A$$

and

$$A \cap B = B \cap A$$

$$\begin{aligned} A \cup B &= \{x: x \in A \text{ or } x \in B\} \\ &= \{x: x \in B \text{ or } x \in A\} \\ &= B \cup A \end{aligned}$$

$$\begin{aligned} A \cap B &= \{x: x \in A \text{ and } x \in B\} \\ &= \{x: x \in B \text{ and } x \in A\} \\ &= B \cap A \end{aligned}$$



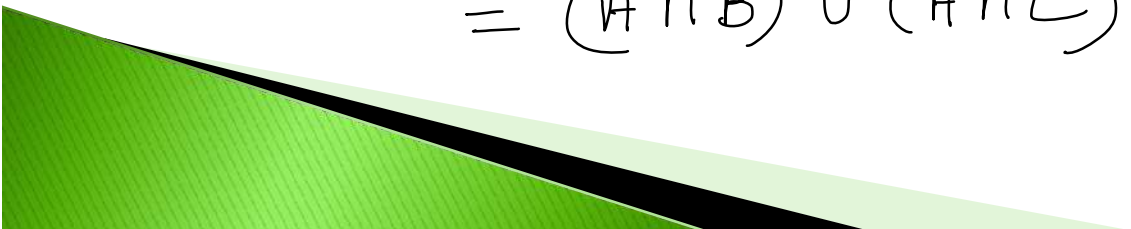
# Laws of the Algebra of Sets

## ❖ Distributive Laws

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

and

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$\begin{aligned} \text{L.H.S.} &= A \cap (B \cup C) \\ &= \{x : x \in A \text{ and } x \in B \cup C\} \\ &= \{x : \underline{x \in A \text{ and } x \in B} \text{ or } x \in A \text{ and } x \in C\} \\ &= \{x : x \in (A \cap B) \text{ or } x \in (A \cap C)\} \\ &= (A \cap B) \cup (A \cap C) \end{aligned}$$


# Laws of the Algebra of Sets

## ❖ Identity Laws

$$A \cup \phi = A, \quad A \cap U = A$$

and

$$A \cup \underline{U} = U, \quad A \cap \underline{\phi} = \underline{\phi}$$

$$\text{L.H.S} = A \cup \phi = \{x : x \in A\} = A = \text{R.H.S}$$

$$\begin{aligned} \text{R.H.S} = A &= \{x : x \in A\} = \{x : x \in A \text{ and } x \in U\} \\ &= \underline{A \cap U} \end{aligned}$$



# Laws of the Algebra of Sets

## ❖ Involution Law

$$(A^c)^c = A$$

Note that  $A^c = \{x : x \in U, x \notin A\}$

$$\begin{aligned}\text{so, } (A^c)^c &= \{x : x \in U, x \notin A^c\} \\ &= \{x : x \in U, x \in A\} \\ &= A\end{aligned}$$



# Laws of the Algebra of Sets

## ❖ Complement Laws

$$A \overset{\vee}{\cup} A^c = U, \quad \underline{A \overset{\vee}{\cap} A^c} = \phi$$

and

$$\overset{\vee}{U}^c = \phi, \quad \phi^c = \overset{\vee}{U}$$

$$\begin{aligned} 1) \text{ L.H.S} &= A \overset{\vee}{\cup} A^c \\ &= \{x : x \in A \text{ or } x \in A^c\} \\ &= \{x : x \overset{x}{\in} A \text{ or } x \in U, x \notin A\} \\ &= \{x : x \in U\} = U = \text{R.H.S} \end{aligned}$$

$$\begin{aligned} 2) \text{ L.H.S} &= A \overset{\vee}{\cap} A^c \\ &= \{x : x \in A \text{ and } x \in A^c\} \\ &= \{x : x \overset{\vee}{\in} A \text{ and } \\ &\quad x \in U, x \overset{\vee}{\notin} A\} \\ &= \phi = \text{R.H.S} \end{aligned}$$



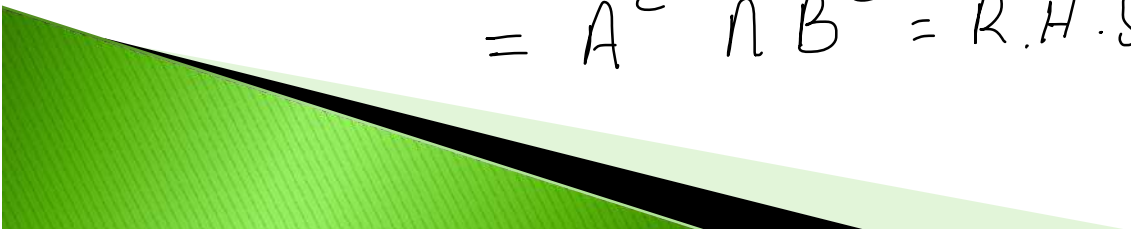
# Laws of the Algebra of Sets

## ❖ DeMorgan's Laws

$$1) (A \cup B)^c = A^c \cap B^c$$

and

$$2) (A \cap B)^c = A^c \cup B^c$$

$$\begin{aligned} 1) \text{ L.H.S} &= (A \cup B)^c \\ &= \{x : x \notin (A \cup B)\} \\ &= \{x : x \notin A \text{ and } x \notin B\} \\ &= \{x : x \in A^c \text{ and } x \in B^c\} \\ &= A^c \cap B^c = \text{R.H.S} \end{aligned}$$




# Duality

The identities that we have discussed above are arranged in pairs. We now consider the principle behind this arrangement. Let  $E$  be an equation of set algebra. The dual  $E^*$  of  $E$  is the equation obtained by replacing each occurrence of  $\cup, \cap, U, \emptyset$  in  $E$  by  $\cap, \cup, \emptyset, U$ , respectively.

For example, the dual of

$$\underbrace{(U \cap A) \cup (B \cap A) = A}_{\text{dual of}} \text{ is } \boxed{(\emptyset \cup A) \cap (B \cup A) = A}.$$



# Example

Question. Write the dual  $(A \cap U)^c \cap A = \emptyset$ .

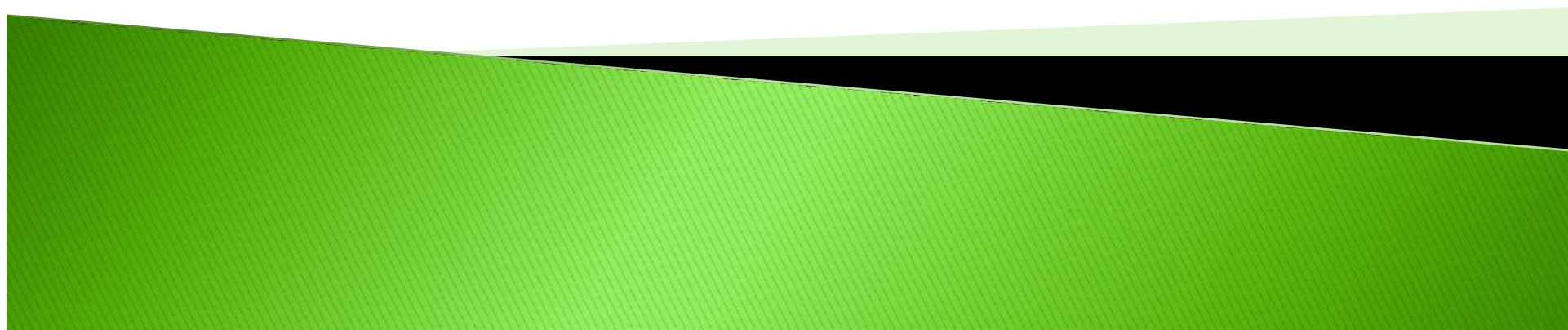
Solution.

The dual is

$$(A \cup \emptyset)^c \cup A = U$$



# Finite Sets, Counting Principles



# Finite Sets

A set is said to be finite if it contains exactly  $m$  distinct elements where  $m$  denotes some nonnegative integer. Otherwise set is said to be infinite. For example, the empty set  $\emptyset$  and the set of letters of the English alphabet are finite sets, whereas the set of even positive integers  $\{2, 4, 6, \dots\}$  is infinite.

## Notation

The notation  $\underline{n(A)}$  or  $\underline{|A|}$  will denote the number of elements in a finite set  $A$ .



# Lemma 1

Suppose  $A$  and  $B$  are finite disjoint sets. Then  $A \cup B$  is finite and

$$n(A \cup B) = n(A) + n(B)$$

For example,

$$A = \{1, 2, 3\} \quad \text{and} \quad B = \{a, b, c\}$$

Then,

$$A \cup B = \{1, 2, 3, a, b, c\}$$

$$n(A \cup B) = 6 = n(A) + n(B) = 3 + 3 = 6$$



# Theorem 1

Let  $A$  be any set in a finite universal set  $U$ . Then

$$n(A^c) = \underline{n(U)} - \underline{n(A)}$$

For example, if there are 20 male students in a class of 35 students, then there are  $35-20=15$  female students.

$$n(\overline{U}) - \overset{\wedge}{n(A)}$$



## Theorem 2

Suppose  $A$  and  $B$  are finite sets. Then

$$n(\underline{A \setminus B}) = n(A) - n(A \cap B)$$

For example, suppose an archery class  $A$  contains 35 students, and 15 of them are also in a bowling class  $B$ .

Then

$$n(A \setminus B) = n(A) - n(A \cap B) = \underline{35} - 15 = \underline{20}$$

That is, there are 20 students in the class  $A$  who are not in class  $B$ .



# Theorem 3

Suppose  $A$  and  $B$  are finite sets. Then

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

For example,

$$A = \{2, 4, 6, 8\}, B = \{6, 8, 10, 12\}$$

$$\text{Then, } A \cup B = \{2, 4, 6, 8, 10, 12\}$$

$$n(A \cup B) = 6$$

$$= n(A) + n(B) - n(A \cap B)$$

$$= 4 + 4 - 2 = 6$$

$$A \cap B = \{6, 8\}$$





# Corollary 1

Suppose  $A, B, C$  are finite sets. Then  $A \cup B \cup C$  is finite and

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C).$$



# Example

Consider the following data among 110 students in a college dormitory:

30 students are on a list A (taking Accounting),  
35 students are on a list B (taking Biology),  
20 students are on both lists.

Find the number of students:

- (a) On list A or B
- (b) On exactly one of the two lists,
- (c) On neither list.



## Example

$$\begin{aligned} a) \quad n(A \cup B) &= n(A) + n(B) - n(A \cap B) \\ &= 30 + 35 - 20 = 45 \checkmark \end{aligned}$$

$$\begin{aligned} b) \quad n(A/B) &= n(A) - n(A \cap B) \\ &\Rightarrow 30 - 20 = 10 \end{aligned}$$

$$\begin{aligned} n(B/A) &= n(B) - n(A \cap B) \\ &= 35 - 20 = 15 \end{aligned}$$

$$\begin{aligned} c) \quad n(A^c \cap B^c) &= n((A \cup B)^c) \\ &= n(U) - n(A \cup B) \\ &= 110 - 45 \\ &= 65 \end{aligned} \quad \left| \begin{array}{l} (A \cup B)^c = A^c \cap B^c \\ \therefore n(A^c) \\ = n(U) - n(A) \end{array} \right.$$

# Classes of Sets, Power Sets



# Classes of Sets

Given a set  $S$ , we may wish to talk about some of its subsets. Thus we would be considering a “set of sets”. Whenever such a situation arises, to avoid confusion, we will speak of *class* of sets or a *collection* of sets. If we wish to consider some of the sets in a given class of sets, then we will use the term *subclass* or *subcollection*.



# Classes of Sets

To understand this concept, we consider the set  $S = \{1, 2, 3, 4\}$ . Let  $A$  be the class of subsets of  $S$  which contain exactly three elements of  $S$ . Then

$$A = \left[ \{1, \check{2}, 3\}, \{1, \check{2}, 4\}, \{1, 3, 4\}, \{2, \check{3}, 4\} \right]$$

Let  $B$  be the class of subsets of  $S$  which contain 2 and two other elements of  $S$ . Then

$$B = \left[ \{2, \check{1}, 3\}, \{2, \check{1}, 4\}, \{2, 3, \check{4}\} \right]$$

Here we can see that  $B$  is a subclass of  $A$ .



# Power Sets

For a given set  $S$ , we may speak about the class of all subsets of  $S$ . This class is called the power set of  $S$ , and it will be denoted by  $\underline{P(S)}$ . If  $S$  is finite, then so is  $\underline{P(S)}$ .

Also

$$\underline{n(P(S))} = 2^{n(S)}$$



# Power Sets

Suppose  $S = \{1, 2, 3\}$ . Then

$$P(S) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} \}$$

Note that

$$2^{n(S)} = 2^3 = 8 \text{ elements}$$



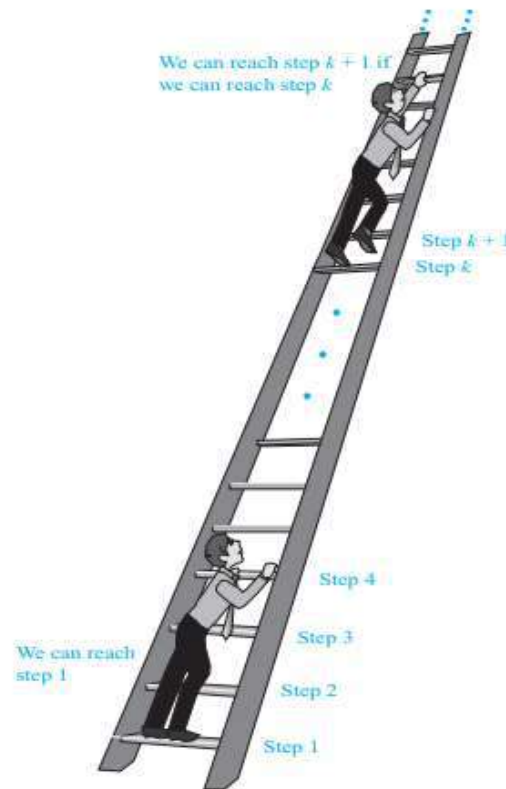


# Mathematical Induction



# Introduction

Suppose we have an infinite ladder, as shown in Figure 1.



**FIGURE 1** Climbing an Infinite Ladder.

# Introduction

We want to know whether we can reach every step on this ladder. We know two things:

1. We can reach the first step of the ladder.
2. If we can reach a particular step of the ladder, then we can reach the next step.

Can we conclude that we can reach every step?

Answer is yes. Something we can verify using an important proof technique called mathematical induction.



# Mathematical Induction

In general, mathematical induction can be used to prove statements that assert that  $P(n)$  is true for all positive integers  $n$ , where  $P(n)$  is a proposition. A proof by mathematical induction has two parts, a basis step, where we show that  $P(1)$  is true, and an inductive step, where we show that for all positive integers  $k$ , if  $P(k)$  is true, then  $P(k+1)$  is true.



# Principle of Mathematical Induction

To prove that  $P(n)$  is true for all positive integers  $n$ ,  
where  $P(n)$  is a proposition, we complete two steps:

*Basis Step:* We verify that  $P(1)$  is true.

*Inductive Step:* We show that the conditional statement  
 $P(k) \longrightarrow P(k+1)$  is true for all positive integers  $k$ .

If  $\underline{P(k)}$  is true then we will prove that  
 $P(k+1)$  is true.



# Example 1

Show that if  $n$  is a positive integer, then

$$1 + 2 + \dots + n = \frac{n(n+1)}{2} \qquad 1 + 2 + 3 = \frac{3(3+1)}{2} \\ = \frac{12}{2} = 6$$

Let  $P(n)$  be the proposition. First we show that  $P(1)$  is true and then conditional statement  $P(k)$  implies  $P(k+1)$  is true for  $k=1, 2, 3, \dots$ .

Base Step. / / /

$$P(1) \text{ is true: } 1 = \frac{1(1+1)}{2} \\ 1 = \frac{2}{2} = 1$$



# Example 1

Inductive step: Assume that  $P(k)$  is true for an arbitrary positive integer  $k$

$$1 + 2 + \dots + k = \frac{k(k+1)}{2} \checkmark$$

Under this assumption it must be shown that  $P(k+1)$  is true, namely

$$\frac{1 + 2 + \dots + k + (k+1)}{2} = \frac{(k+1)[(k+1)+1]}{2} = \frac{(k+1)(k+2)}{2}$$

Now,  $1 + 2 + \dots + k = \frac{k(k+1)}{2}$

$$\begin{aligned} 1 + 2 + \dots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \end{aligned}$$

## Example 1

$$\begin{aligned} &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

Thus last equation shows that  $P(k+1)$  is true under the assumption that  $P(k)$  is true





## Example 2

Let  $P(n)$  be the assertion that the sum of the first  $n$  odd integers is  $n^2$ ; that is,

$$P(n): 1+3+5+\dots+(2n-1)=n^2.$$

$1+3+5 = 3^2$   
 $9 = 9$

Base Step:  $P(1)$  is true, because

$$1 = 1^2$$

Inductive Step: Assume that  $P(k)$  is true. That is,

$$1+3+5+\dots+(2k-1) = k^2$$

Next odd number after  $2k-1$  is  $2k+1$ . ✓

## Example 2

$$1 + 3 + \dots + (2k-1) = k^2 \checkmark$$

$$\begin{aligned} 1 + 3 + \dots + (2k-1) + (2k+1) &= k^2 + (2k+1) \\ &= \cancel{k^2 + 2k + 1} \\ &= (k+1)^2 \checkmark \end{aligned}$$

That is,  $P(k+1)$  is true whenever  $P(k)$  is true.

P moved



# Example 2



## Example 3

Use mathematical induction to show that

$$P(n): 1 + 2^1 + 2^2 + \dots + 2^n = 2^{n+1} - 1$$

for all nonnegative integers  $n$ .

$$\begin{aligned} & 2^{(k+1)+1} - 1 \\ &= 2^{k+2} - 1 \end{aligned}$$

Basis Step: Let  $P(n)$  be the statement.  
 $P(0)$  is true, because

$$2^0 = 2^{0+1} - 1$$

$$1 = 2^1 - 1$$

$$\boxed{1 = 1}$$

Inductive Step: Assume that  
 $P(k)$  is true. That

$$1 + 2 + 2^2 + \dots + 2^k = 2^{k+1} - 1 \quad \checkmark$$

# Example 3



# Axiomatic Development of Set Theory



# What is axiom and axiomatic development?

Any axiomatic development of a branch of mathematics begins with the following:

- 1) undefined terms,  $\neq$
- 2) Undefined relations,
- 3) Axioms relating the undefined terms and undefined relations.

Then one develops theorems based upon the axioms and definitions.



# Axiomatic Development of Euclidean Geometry

Consider, for example, the axiomatic development of plane Euclidean geometry. It begins with the following :

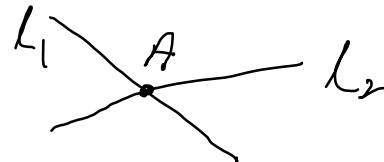
- 1) “points” and “lines” are undefined terms;
- 2) “point on a line” is an undefined relation.

Two of many axioms of Euclidean geometry follow:

**Axiom 1:** Two distinct points are on one and only one line.



**Axiom 2:** Two distinct lines cannot contain more than one point in common.





# Axiomatic Development of Set Theory

The axiomatic development of set theory begins with the following:

- 1) “element<sup>✓</sup>” and “set<sup>✓</sup>” are undefined terms;
- 2) “elements belong to a set” is the undefined relation.

Two of the axioms of set theory follow:

**Principle of Extension:** Two sets  $A$  and  $B$  are equal if and only if they have the same elements.



# Axiomatic Development of Set Theory

**Principle of Abstraction:** Given any set  $U$  and any property  $P$ , there is a set  $A$  such that the elements of  $A$  are exactly those elements in  $U$  which have the property  $P$ .

$$U = \{Nauman, Sara, Aleekha, Mansoor\}$$

$$A = \{Nauman, Mansoor\}$$



# Real Number System



# Real Number System

The notation  $\underline{R}$  will be used to denote the real numbers.

These are the numbers one uses in basic arithmetic and algebra.  $\underline{R}$  together with its properties is called the real number system.

The set  $R$  of real numbers includes the following sets of numbers:

$\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, 3, \dots \} = \text{set of integers}$

$\mathbb{Z}^+ = \mathbb{P} = \{ 1, 2, 3, \dots \} = \text{set of positive integers}$

$\mathbb{N} = \{ 0, 1, 2, 3, \dots \} = \text{set of nonnegative integers}$

$\mathbb{Q} = \text{set of rational numbers i.e. numbers which are ratios of integers}$   $\frac{2}{3}, -\frac{1}{2}, \frac{2}{1} = 2$

# Real Number System

## Irrational Numbers

Those real numbers which cannot be represented as the ratio of integers, are called irrational numbers.

For example,  $\pi = 3.14\dots \neq \frac{22}{7}$

$$\sqrt{2}$$

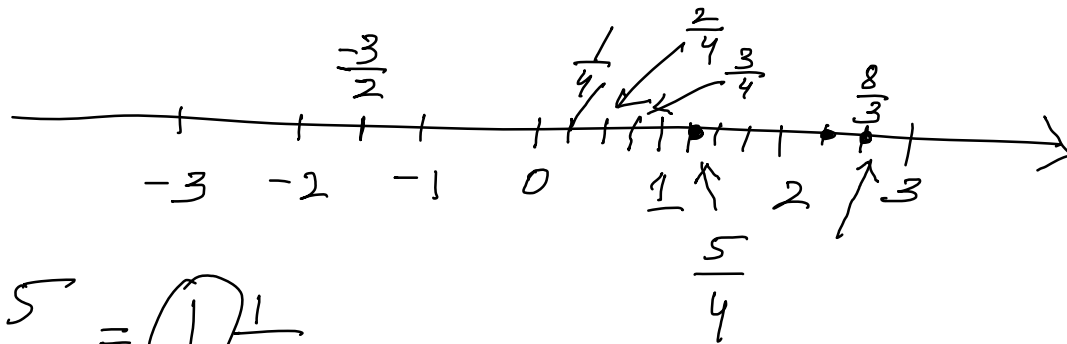
$$\sqrt{3}$$

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{Q}'$$



# Real Line $R$ , Decimal Expansion

One of the most important properties of the real numbers is that they can be represented graphically by points on a straight line.



$$\frac{1}{4} \checkmark$$

$$\frac{5}{4} = 1 \frac{1}{4} \checkmark$$

$$\frac{8}{3} = 2 \frac{2}{3} \checkmark$$

$$\begin{array}{r} 4 \overline{) 5} \\ \underline{4} \phantom{0} \\ 1 \phantom{0} \end{array}$$

$$\begin{array}{r} 3 \overline{) 8} \\ \underline{6} \phantom{0} \\ 2 \phantom{0} \end{array}$$

# Decimal Expansion

Real numbers can also be represented by decimals. The decimal expansion of a rational number will either stop as in  $\frac{3}{4} = 0.75$  or will have a pattern that repeats indefinitely, such as  $\frac{17}{11} = 1.\overline{545454}\dots$ . Even when the decimal expansion stops, it can be rewritten using repeated 9's, for example,  $\frac{3}{4} = 0.74999\dots$

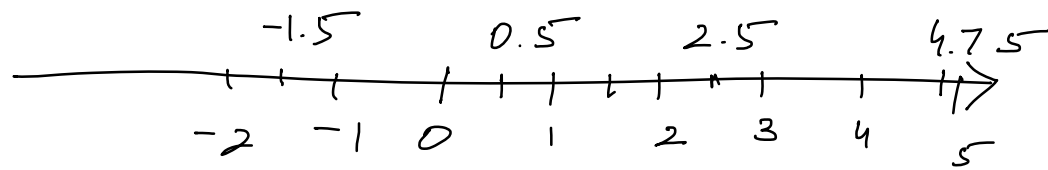
$$= 0.75, 0.3 = 0.2999\dots$$

The decimal expansion of an irrational number never stops nor does it have a repeating pattern. The points representing the decimal 2.5 and 4.75 are indicated below on real line.

$$\pi = 3.14\dots$$



# Decimal Expansion



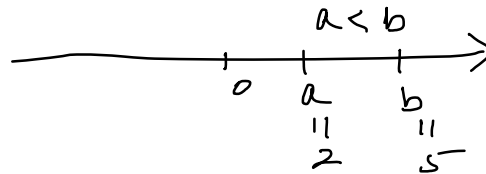


# Order and Inequalities



# Order Relation of Real Numbers

Let  $a$  and  $b$  be real numbers. We say  $a$  is less than  $b$ , written  $a < b$  if the difference  $b-a$  is positive.  $2 < 5$   
 $5-2$  is positive  
Geometrically,  $a < b$  if and only if the point  $a$  lies to the left of the point  $b$  on the real line  $R$ .



Observe that we define order in  $R$  in terms of the positive real numbers denoted by  $R^+$ .



# Main Properties of Positive Real Number

There are two main properties of the positive real numbers  $R^+$ :

- 1) If  $a$  and  $b$  are positive, then  $a+b$  and  $ab$  are positive.
- 2) For any real number  $a$ , either  $a$  is positive,  $a = 0$ , or  $-a$  is positive.

$$\begin{array}{ll} a = 2 & -a = -(-2) = 2 \\ a = -2 & a = 0 \end{array}$$

The following additional notation and terminology are used:

$\checkmark$   
 $\underline{a} > b$ , means  $\checkmark$   
 $b < a$

$a \leq b$ , means  $a < b$  or  $a = b$   $\checkmark$   
 $2 \lesseqgtr 2$  or  $2 = 2$

$a \geq b$ , means  $b \leq a$   $2 \leq 5$  or  $5 \geq 2$ .



# Inequality

Any statement of the form  $\underline{a < b}$ ,  $\underline{a \leq b}$ ,  $\underline{a > b}$ , or  $\underline{a \geq b}$  is called inequality; and any statement of the form  $\overline{a < b}$  or  $a > b$  is sometimes called a strict inequality.

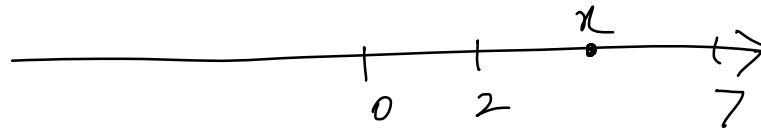
$2 < 7$  ✓ strict inequality

$a \geq b$  ✗ not strict inequality



# Example 1

- a)  $2 < 5$  ;  $-6 < -3$  ,  $4 \leq 4$  ,  $5 > -8$  ,  $6 \geq 0$  ,  $-7 \leq 0$
- b) A real number  $a$  is positive iff  $a > 0$ ,  
and  $a$  is negative iff  $a < 0$ .
- c) The statement  $2 < \overset{\vee}{x} < 7$  means  $2 < x$   
and  $x < 7$ .



# Properties of Inequality

Basic properties of the inequality relation follow.

1) Let  $a, b, c$  be real numbers. Then:

(i)  $a \leq a$      $2 \leq 2$

(ii) If  $a \leq b$  and  $b \leq a$ , then  $a = b$ .     $3 \leq 3, \Rightarrow 3 = 3$

(iii) If  $a \leq b$  and  $b \leq c$ , then  $a \leq c$ .     $2 \leq 5, 5 \leq 7 \Rightarrow 2 \leq 7$

2) For any real numbers  $a$  and  $b$ , exactly one of the following holds:

$$a < b, \quad a = b \quad \text{or} \quad a > b$$



# Properties of Inequality

3) Let  $a, b, c$  be real numbers such that  $\overline{a} \leq \overline{b}$ . Then

(i)  $\overline{a+c} \leq \overline{b+c}$ .

(ii)  $ac \leq bc$  when  $\underline{c} > 0$ ; but  $ac \geq bc$  when  $\underline{c} < 0$ .

$$a = 2, b = 5, c = 2$$

$$a < b$$

$$\begin{array}{rcl} a+c & = & b+c \\ 4 & < & 7 \end{array}$$

$$a < b$$

$$ac < bc$$

$$4 < 10$$

$$\text{Let } c = -2$$

$$ac > bc$$

$$-4 > -10$$



# Properties of Inequality

Q. Prove that if  $a \leq b$  and  $b \leq c$ , then  $a \leq c$ .

P proof. If  $a = b$  and  $b = c$ , then  $a = c$ .

If  $a < b$  and  $b < c$ , then  $b - a$  is positive and  $c - b$  is positive.

Now,  $(b - a) + (c - b)$  is positive.

$$= -a + c$$

$$= c - a \text{ is positive}$$

$$\Rightarrow a < c$$

Hence,  $a \leq c$ . P proved



# Properties of Inequality

Q. Let  $a, b, c$  be real numbers. <sup>and suppose  $a \leq b$</sup>  Then prove that

(i)  $a + c \leq b + c$ .

(ii)  $ac \leq bc$  when  $c > 0$ ; but  $ac \geq bc$  when  $c < 0$ .

Do it yourself as assignment.

If  $a = b$ , then  $ac = bc$

If  $a < b$ , then  $b - a$  is positive

$c(b - a)$  is also positive.

$$= bc - ac \text{ is } // \quad //$$

$$\Rightarrow ac < bc$$

$$\text{Hence } ac \leq bc$$

# Absolute Value, Distance



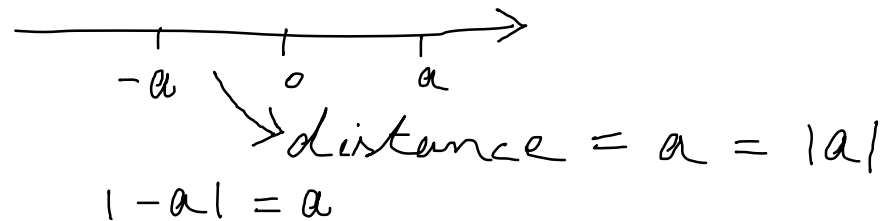
# Absolute value of a Number

The absolute value of a real number  $a$ , denoted by  $|a|$ , may be viewed as the distance between  $a$  and the 0 on the real line  $R$ . Formally,  $|a| = a$  or  $-a$  according as  $a$  is positive or negative, and  $|0| = 0$ . That is:

$$|a| = \begin{cases} a, & \text{if } a \geq 0 \\ -a, & \text{if } a < 0 \end{cases}$$

Accordingly,  $|a|$  is always positive when  $a \neq 0$ .

Geometrically,  $|a|$  is:



# Example 1

$$|-3| = -(-3) = 3, \quad |2| = 2, \quad |-3.5| = -(-3.5) \\ = 3.5$$

$$|4.5| = 4.5$$



# The Distance Between Two Numbers

The distance  $d$  between two points  $a$  and  $b$  is denoted by  $d(a, b)$  and is obtained from the formula

$$d = d(a, b) = |a - b| = |b - a|$$

For example,

$$2, 5$$

$$d(2, 5) = |2 - 5| = |-3| = 3$$

$$-3, 11$$

$$d(-3, 11) = |-3 - 11| = |-14| = 14$$



# Properties of Absolute Value Function

Let  $a$  and  $b$  be any real numbers.

1)  $|a| \geq 0$ , and  $|a| = 0$  iff  $a = 0$ .

2)  $\underline{-|a| \leq a \leq |a|}$ .

3)  $|ab| = |a||b|$ . ✓

4)  $|a \pm b| \leq |a| + |b|$ . ✓

5)  $\underline{||a| - |b|| \leq |a \pm b|}$ . ✓

$a = -5$ ,  $|a| = 5$ ,  $a = 2$ ,  $b = -3$

$\Rightarrow a \leq |a|$

$-|a| = -5 \leq a$

$\Rightarrow -|a| \leq a$

$ab = -6$

$|ab| = 6$

$|a| = 2, |b| = 3$

$|a||b| = 6$

Let  $a = 5$ ,  $b = -2$

$|a + b| = |5 - 2| = 3$  ✓

$|a| = 5, |b| = 2$

$|a| + |b| = 7$

$3 < 7$

$|a + b| < |a| + |b|$

# Properties of Absolute Value Function

Q. Prove that  $|ab| = |a||b|$ . where  $a$  and  $b$  are real nos.

Proof. 1) Suppose  $a=0$  and  $b=0$ , then  $|ab|=0=|a||b|$

2) Suppose  $a>0$ ,  $b>0$ , then  $ab>0$   
 $\Rightarrow |a|=a$ ,  $|b|=b$ ,  $|ab|=ab$   
 $\Rightarrow |ab|=ab=|a||b|$

3) Suppose  $a>0$  and  $b<0$ , then  $ab<0$ .  
 $\Rightarrow |a|=a$ ,  $|b|=-b$ ,  $|ab|=-ab$   
 $\Rightarrow |ab|=-ab=a(-b)=|a||b|$

4) Suppose  $a<0$ ,  $b>0$  (Do it yourself)

5) Suppose  $a<0$  and  $b<0$ , then  $ab>0$ .  
 $\Rightarrow |a|=-a$ ,  $|b|=-b$ ,  $|ab|=ab$   
 $\Rightarrow |ab|=ab=(-a)(-b)=|a||b|$

# Properties of Absolute Value Function

Q. Prove that  $|a \pm b| \leq |a| + |b|$ .

P proof: 1)  $|a+b| \leq |a| + |b|$  2)  $|a-b| \leq |a| + |b|$  ✓

$$\begin{aligned}(a+b)^2 &= a^2 + 2ab + b^2 \leq \frac{a^2 + 2|a||b| + b^2}{= |a|^2 + 2|a||b| + |b|^2} \\ &= (|a| + |b|)^2 \\ \Rightarrow (a+b)^2 &\leq (|a| + |b|)^2 \\ \Rightarrow \sqrt{(a+b)^2} &\leq \sqrt{(|a| + |b|)^2} \\ \Rightarrow |a+b| &\leq |a| + |b| \text{ Proved}\end{aligned}$$

Note that  
 $ab \leq |ab| = |a||b|$   
 $= |a||b|$   
 $\Rightarrow ab \leq |a||b|$   
 $\Rightarrow 2ab \leq 2|a||b|$

$$\therefore \sqrt{x^2} = |x|$$

Also,  $|a-b| = |a + (-b)|$   
 $\leq |a| + |-b|$   
 $= |a| + |b|$



# Intervals



# Intervals

Let  $a$  and  $b$  be distinct real numbers with, say,  $a < b$ . The intervals with endpoints  $a$  to  $b$  are denoted and defined as follows:

$(a, b) = \{x: a < x < b\}$ , open interval from  $a$  to  $b$

$[a, b] = \{x: a \leq x \leq b\}$ , *closed* interval from  $a$  to  $b$

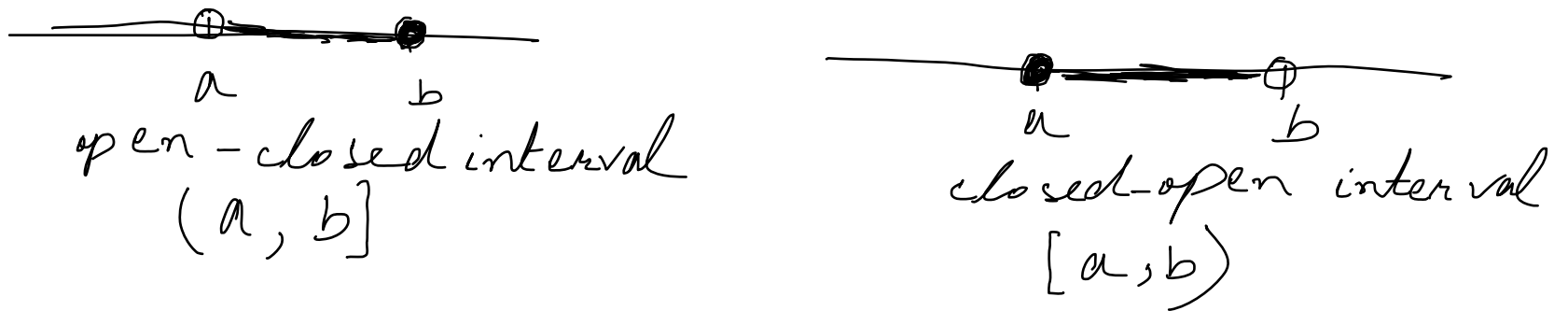
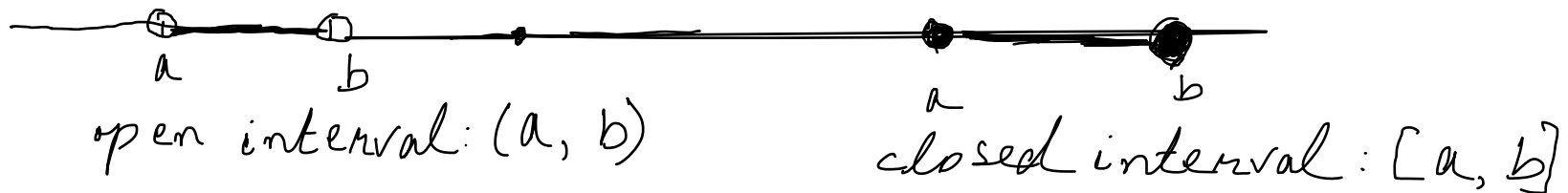
$[a, b) = \{x: a \leq x < b\}$ , *closed-open* interval from  $a$  to  $b$

$(a, b] = \{x: a < x \leq b\}$ , *open-closed* interval from  $a$  to  $b$



# Intervals

- How do we represent these intervals on a real line?



# Example 1

Find the interval satisfying each inequality, i.e., rewrite the inequality in terms of  $x$  alone:

1)  $2 \leq x-5 \leq 8$

Add 5 throughout the inequality:

$$2 + 5 \leq x - 5 + 5 \leq 8 + 5$$

$$7 \leq x \leq 13$$

$$[7, 13]$$

2)  $6 \leq -2x \leq 4$

Multiply  $-\frac{1}{2}$  throughout the inequality

$$-\frac{1}{2} \times 6 \geq -\frac{1}{2} \times -2x \geq -\frac{1}{2} \times 4$$

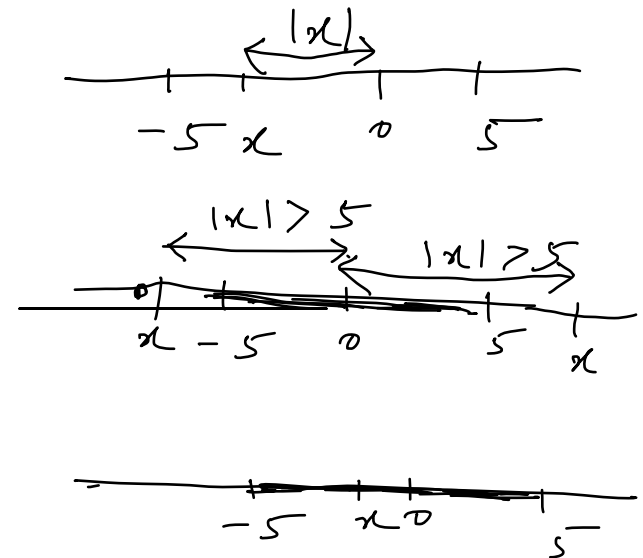
$$-3 \geq x \geq -2$$

$$\text{or } -2 \leq x \leq -3 \quad \text{or } [-3, -2]$$

## Example 2

The inequality  $|x| < 5$  may be interpreted to mean that the distance between  $x$  and the origin 0 is less than 5; hence  $x$  must lie between -5 and 5 on the real line  $R$ . How?

$$\begin{aligned} |x| &< a \\ \Rightarrow -a &< x < a \\ |x| &< 10 \\ \Rightarrow -10 &< x < 10 \end{aligned}$$



## Example 3

Q. Rewrite  $|x-5| < 5$  without the absolute value sign.

Sol.

$$|x-5| < 5$$

$$\Rightarrow -5 < x-5 < 5$$

$$\Rightarrow -5 + 5 < x-5+5 < 5+5$$

$$\Rightarrow 0 < x < 10 \quad \text{Ans.}$$

$$(0, 10)$$



# Definition

A set  $A$  of real numbers is said to be dense in  $R$  if every open interval contains a point of  $A$ .

Example 1: The rational numbers  $Q$  are dense in  $R$ .

like  $(2, 4)$ , let's say  $3 \in (2, 4)$  and  $3 \in Q$   
 $(\frac{1}{3}, \frac{1}{2})$ , here  $\frac{1}{4} \in (\frac{1}{3}, \frac{1}{2})$  and  $\frac{1}{4} \in Q$

Example 2: The integers  $Z$  is not dense in  $R$ .

For example, Take  $(\frac{1}{3}, \frac{1}{2})$   
we cannot find, point on  $(\frac{1}{3}, \frac{1}{2})$   
such that it is a member of  $Z$ .

# Infinite Intervals

Let  $a$  be any real number. Then the set of real numbers  $x$  satisfying  $x < a$ ,  $x \leq a$ ,  $x > a$ , or  $x \geq a$ , is called an infinite interval with endpoint  $a$ . The interval is said to be closed or open according as the endpoint  $a$  does or does not belong to the interval. The four infinite intervals may also be denoted and defined as follows:

$$\begin{array}{l} \text{open} \\ \text{interval} \end{array} \left\{ \begin{array}{l} \checkmark x < a : (-\infty, a) \\ \checkmark x > a : (a, +\infty) \end{array} \right. ; \left\{ \begin{array}{l} \checkmark x \leq a : (-\infty, a] \\ \checkmark x \geq a : [a, +\infty) \end{array} \right.$$

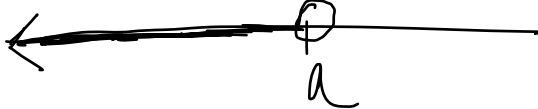
↖ closed intervals





# Infinite Intervals

These infinite intervals are pictured as:

$$(-\infty, a) :$$


A horizontal number line with an arrow pointing left from a point labeled 'a'. The point 'a' is marked with an open circle.

$$(a, \infty) :$$


A horizontal number line with an arrow pointing right from a point labeled 'a'. The point 'a' is marked with an open circle.

$$(-\infty, a]$$

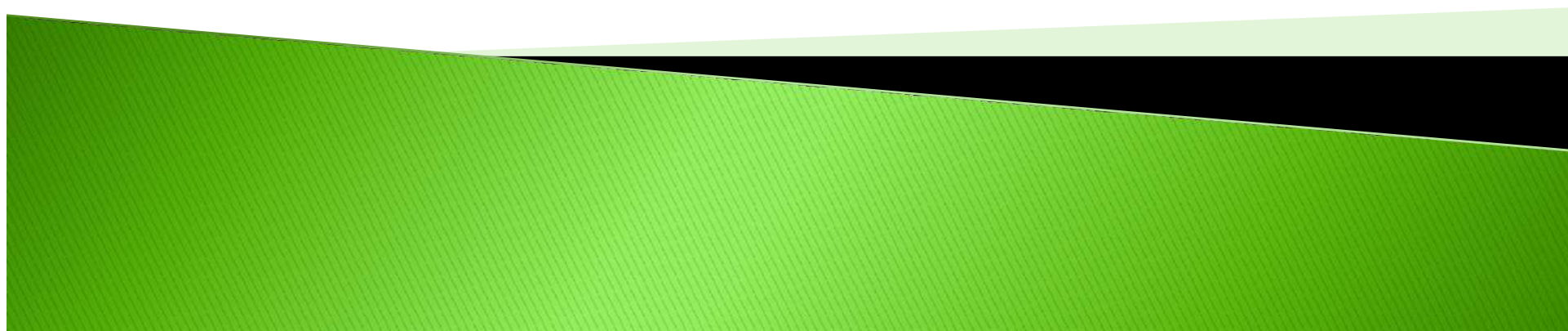

A horizontal number line with an arrow pointing left from a point labeled 'a'. The point 'a' is marked with a closed circle.

$$[a, \infty)$$


A horizontal number line with an arrow pointing right from a point labeled 'a'. The point 'a' is marked with a closed circle.



# Bounded Sets, Completion Property



# Bounded Set

Let  $A$  be a set of real numbers. Then  $A$  is said to be bounded according as there exists a real number  $M$  such that, for every  $x \in A$ , we have  $|x| \leq M$ .  $-M \leq x \leq M$

The number  $M$  is called a bound. Note that  $A$  is bounded if and only if  $A$  is a subset of some finite interval. Specifically  $M$  is a bound of  $A$  if and only if  $A$  is a subset of  $[-M, M]$ . ✓

For example,

$A = \{1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}, \dots\}$  is bounded.

Set ~~for~~  $A$  is a subset of the closed unit interval  $I = [0, 1]$ . i.e.  $A \subseteq [0, 1]$ .

$$|x| \leq a \\ \Rightarrow -a \leq x \leq a$$

# Bounded From Above

Let  $A$  be a set of real numbers. Then  $A$  is said to be bounded from above according as there exists a real number  $M$  such that, for every  $x \in A$ , we have  $x \leq \underline{M}$ .

The number  $M$  is called an upper bound.

For example,  $C = \{\dots, -5, -3, -1\}$  is bounded from above. Here upper bound is  $M = -1$ . since for all  $x \in C$ , we have  $x \leq M = -1$ .



# Bounded From Below

Let  $A$  be a set of real numbers. Then  $A$  is said to be bounded from below according as there exists a real number  $M$  such that, for every  $x \in A$ , we have  $x \geq M$ .

The number  $M$  is called a lower bound.

For example,  $B = \{2, 4, 6, \dots\}$  is bounded from below. Here lower bound is 2 since for all  $x \in B$ ,  $x \geq 2 = M$ .

Note: Finite sets are always bounded.



# Exercise

State whether each set of real numbers is bounded or unbounded:

a)  $A = \{x : x \leq \sqrt{5}\}$

$A$  is unbounded.  $A$  is bounded from above.

b)  $B = \{\dots, -10, -5, 0, 5, 10, \dots\}$

Unbounded. No lower or upper bound is present.

c)  $C = \{2^{18}, \underline{3^{-7}}, 7, 0, \underline{8^{35}}\}$

Bounded.

d)  $D = \{\underline{2}, 4, 8, \dots, 2^n, \dots\}$

$D$  is unbounded.  $D$  is bounded from below.

## Exercise

e)  $E = \{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots, (\frac{1}{2})^n, \dots\}$

$f_t$  is bounded because  $E \subseteq I = \underline{[0, 1]}$ .

f)  $F = \{1, -1, \frac{1}{2}, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{3}, \dots\}$

$f_t$  is bounded because  $F \subseteq [-1, 1]$ .



Note Let  $A = \{\dots, -10, -5, 0, 5, 10\}$

upper bound  $(A) = 10$

Any number greater than 10 is also an upper bound of  $A$ . upper bound of  $A = \{x : x \geq \underline{10}\}$

Least upper bound or supremum of  $A = 10$

Let  $B = \{2, 4, 6, \dots\}$

lower bound is  $\textcircled{2} \rightarrow$  greatest lower bound  
so any real number less than 2 is also a lower bound of  $B$ .

Infimum





# Supremum

Let  $A$  be a set of real numbers. A number  $M$  is called the least upper bound or supremum of  $A$ , written  $M = \sup(A)$  if  $M$  is an upper bound of  $A$  but any number less than  $M$  is not an upper bound of  $A$ , that is, for any positive number  $\epsilon$ , there exist  $a \in A$  such that,  $M - \epsilon < a$ .

For example, consider the set  $\{ \dots, -5, -10, 0, \underline{5} \} = A$

$$\text{Here } \sup(A) = 5$$

$$\text{let } \epsilon = 0.1$$

$5 - 0.1 = 4.9$  is not an upper bound of  $A$ .



# Completion Property of $\mathbb{R}$

If a set of real numbers is bounded from above, then  $\sup(A)$  exists.

The real numbers  $\mathbb{R}$  are said to be complete since it satisfies the above property. For example, consider the set:

$$B = \{ \dots, -2, -1, 0, 1, 2, 3, 4 \}$$

$$\text{Here } \sup(B) = 4$$



# $\mathbb{Q}$ is not Complete

Let  $A$  be the following subset of the rational numbers  $\mathbb{Q}$ :

$$A = \{x \in \mathbb{Q} : \underline{x} > 0, x^2 < 3\}$$
$$= (0, \sqrt{3})$$

This set is bounded. Upper bound is  $\sqrt{3}$ .  
We cannot let  $\sup(A) = \sqrt{3}$  since  $\sqrt{3}$   
is not a rational number



# Greatest Common Divisor



# Definition

Suppose  $a$  and  $b$  are integers, not both 0. An integer  $d$  is called a common divisor of  $a$  and  $b$  if  $d$  divides both  $a$  and  $b$ , that is, if  $d|a$  and  $d|b$ . If  $d$  is largest then it is denoted by  $\gcd(a, b)$  and it is called the greatest common divisor of  $a$  and  $b$ .



## Example 1

a) The common divisors of 12 and 18 are  $\pm 1, \pm 2, \pm 3, \pm 6$

Thus  $\gcd(12, 18) = 6$ . Similarly,

$$\gcd(12, -18) = 6, \quad \gcd(12, -16) = 4,$$

$$\gcd(29, 15) = 1, \quad \gcd(14, 49) = 7$$

b) For any integer  $a$ , we have  $\gcd(1, a) = 1$ .



## Example 2

a) For any prime  $p$ , we have  $\gcd(p, a) = p$   
if  $\underline{p \mid a}$ . Similarly  $\gcd(p, a) = 1$  if  $\underline{p \nmid a}$ .  
For example,  $\gcd(5, 10) = 5$ ,  
and  $\gcd(5, 11) = 1$



# Important Result

Suppose  $d = \gcd(a, b)$ . Then there exist integers  $x$  and  $y$  such that  $d = \underline{ax+by}$ .

For example,  $\gcd(12, 18) = 6 = d$   
So,

$$d = ax + by$$

$$6 = \underline{12}x + \underline{18}y$$

$$6 = 12(-1) + 18(1)$$

$$\text{Hence, } x = -1, y = \underline{1}$$





# Theorem

A positive integer  $d = \gcd(a, b)$  if and only if  $d$  has the following properties:

- 1)  $d$  divides both  $a$  and  $b$ .
- 2) If  $c$  divides both  $a$  and  $b$ , then  $\underline{c|d}$ .

$$\gcd(12, 18) = 6$$

Here  $d = 6$  divides both 12 & 18.

Also 3 divides both 12 & 18.

Hence 3 divides 6.



# Properties of the Greatest Common Divisor

1)  $\gcd(a, b) = \gcd(b, a)$

2) If  $x > 0$ , then  $\gcd(\underline{ax}, \underline{bx}) = x \cdot \gcd(a, b)$ .

$$\begin{aligned}\gcd(12, 18) &= \gcd(3 \cdot 4, 3 \cdot 6) \\ &= 3 \cdot \gcd(4, 6) \\ &= 3 \cdot 2 = 6\end{aligned}$$

3) If  $d = \gcd(a, b)$ , then  $\gcd(a/d, b/d) = 1$ .

$$\gcd(12, 18) = \gcd\left(\frac{12}{6}, \frac{18}{6}\right) = \gcd(2, 3) = 1$$

4) For any integer  $x$ ,  $\gcd(a, b) = \gcd(a, b + ax)$ .

$$\begin{aligned}\gcd(12, 18) &= \gcd(12, 18 + 12(2)) \\ &= \gcd(12, 42) = 6\end{aligned}$$



# Fundamental Theorem of Arithmetic



# Theorem

Every integer  $n > 1$  can be expressed uniquely as a product of primes.

$$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

where  $m_i$  are positive and  $p_1 < p_2 < \cdots < p_r$ .



# Example 1

Find the unique factorization of each number:

a) 135      (b) 1330      (c) 211

Sol: (a)

$$135 = 5 \times 3 \times 3 \times 3 = 3^3 \times 5.$$

$$b) \quad 1330 = 2^1 \times 5^1 \times 7^1 \times 19^1$$

c) 211 is a prime, so it cannot be factored.

|   |     |
|---|-----|
| 5 | 135 |
| 3 | 27  |
| 3 | 9   |
| 3 | 3   |
|   | 1   |

|    |      |
|----|------|
| 2  | 1330 |
| 5  | 665  |
| 7  | 133  |
| 19 | 19   |
|    | 1    |



## Example 1

Let  $a = \underline{2}^3 \cdot 3^5 \cdot \underline{5}^4 \cdot \underline{11}^6 \cdot \underline{17}^3$  and  $b = \underline{2}^5 \cdot \underline{3}^5 \cdot 7^2 \cdot \underline{11}^4 \cdot \underline{13}^2$

Find  $\gcd(a, b)$  and  $\text{lcm}(a, b)$ .

Sol:  $\gcd(a, b) = 2^3 \cdot \cancel{3}^5 \cdot 11^4 = ?$

$$\begin{aligned} \text{lcm}(a, b) &= 2^5 \cdot 3^5 \cdot 5^4 \cdot 7^2 \cdot 11^6 \cdot 13^2 \cdot \cancel{17}^3 \\ &= ? \end{aligned}$$

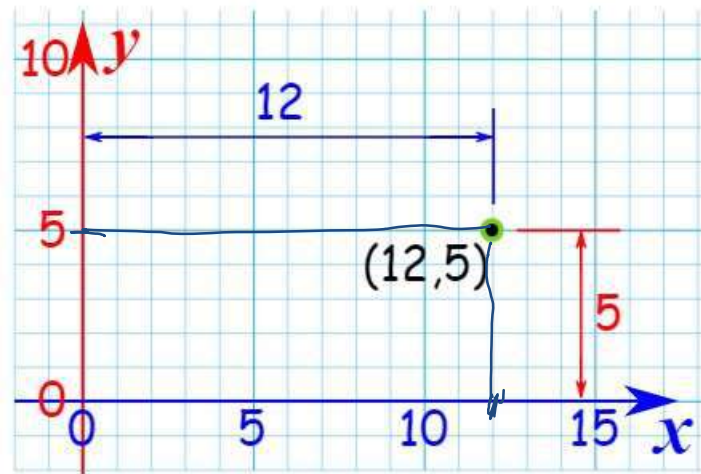


# Product Sets



# Ordered Pairs

Two numbers written in a certain order. Usually written in parentheses like  $(12, 5)$  which can be used to show position on a graph, where the “ $x$ ”(horizontal) value is first and the “ $y$ ”(vertical) value is second. So  $(12, 5)$  is 12 units along, and 5 units up.



$$(a, b) \neq (b, a)$$

$$(a, b) = (c, d)$$

$$\text{iff } a = c, b = d$$



# Product Sets

Let  $A$  and  $B$  be two sets. The product set or cartesian product of  $A$  and  $B$ , written  $A \times B$  is the set of all ordered pairs  $(a, b)$  such that  $a \in A$  and  $b \in B$ . Namely

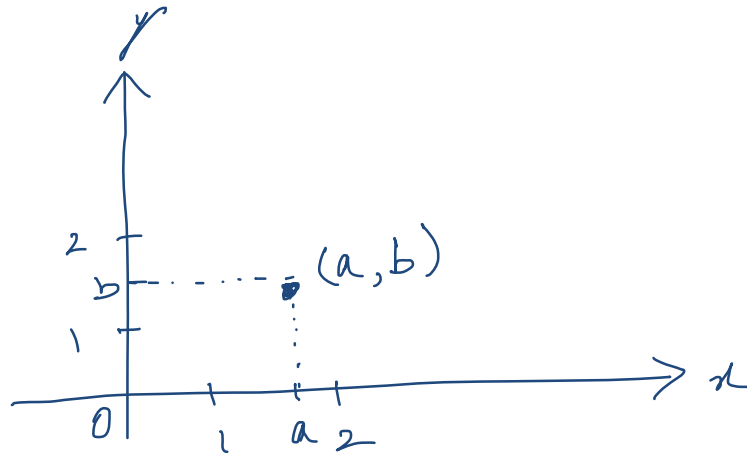
$$A \times B = \{(\underline{a, b}) : a \in A, b \in B\}$$

One usually writes  $A^2$  instead of  $A \times A$ .



# Example 1

$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$  is the set of all ordered pairs of real numbers. In  $xy$ -plane, each point  $P$  represents an ordered pair  $(a, b)$  of real numbers and vice versa.  $\mathbb{R}^2$  is also called the Cartesian plane.



## Example 2

Let  $A = \{1, 2\}$  and  $B = \{a, b, c\}$ . Then

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

$$B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

$$A^2 = A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$$

$$A \times B \neq B \times A$$

$$n(A \times B) = 6 = n(A) \cdot n(B)$$



# Product of Three or More Sets

The idea of a product of sets can be extended to any finite number of sets. Specifically, for any sets  $A_1, A_2, \dots, A_m$  the set of all  $m$ -element lists  $(a_1, a_2, \dots, a_m)$  where each  $a_i \in A_i$  is called the cartesian product of the sets  $A_1, A_2, \dots, A_m$ . It is denoted by  $A_1 \times A_2 \times \dots \times A_m$ .



## Example 3

Let  $A = \{1, 2\}$ ,  $B = \{x, y, z\}$ ,  $C = \{3, 4\}$ . Find  $A \times B \times C$ .

$$A \times B \times C = \{(a, b, c) : a \in A, b \in B, c \in C\}$$

$$A \times B \times C = \{(1, x, 3), (1, x, 4), (1, y, 3), (1, y, 4), \\ (1, z, 3), (1, z, 4), (2, x, 3), (2, x, 4), \\ (2, y, 3), (2, y, 4), (2, z, 3), (2, z, 4)\}$$

$$\therefore n(A \times B \times C) = 12 = n(A) \cdot n(B) \cdot n(C)$$



## Example 4

Let  $A = \{1, 2\}$ ,  $B = \{a, b, c\}$ ,  $C = \{c, d\}$ . Find  $A \times (B \cap C)$ .

Sol.  $B \cap C = \{c\}$

$$\begin{aligned} A \times (B \cap C) &= \{1, 2\} \times \{c\} \\ &= \{(1, c), (2, c)\} \end{aligned}$$

Exercise:  $A \times B = ?$   
 $B \times A = ?$



# Relations



# Definitions

Let  $A$  and  $B$  be sets. A binary relation or, simply, a relation from  $A$  to  $B$  is a subset of  $A \times B$ . Suppose  $R$  is a relation from  $A$  to  $B$ . Then  $R$  is a set of ordered pairs where each first element comes from  $A$  and each second element comes from  $B$ . That is, *for each  $a \in A$  and  $b \in B$ ,*

*(i)  $(a, b) \in R$ , we say " $a$  is related to  $b$ " written  $a R b$ .*

*(ii)  $(a, b) \notin R$ , we say " $a$  is not related to  $b$ ,  $a \not R b$ .*





# Domain and Range

The domain of a relation  $R$  from  $A$  to  $B$  is the set of all first elements of the ordered pairs which belong to  $R$ , and so it is subset of  $A$ ; and the range of  $R$  is the set of all second elements, and so it is a subset of  $B$ .

**Note:** Sometimes  $R$  is a relation from a set  $A$  to itself, that is,  $R$  is a subset of  $A^2 = \underline{A \times A}$ . In such a case, we say that  $R$  is a relation on  $A$ .



# Example 1

- a) Let  $A = \{1, 2, 3\}$  and  $B = \{x, y, z\}$ , and let  $R = \{(1, y), (1, z), (3, y)\}$ . This is a relation from  $A$  to  $B$ .  
 $1Ry, 1Rz, 3Ry$  but  
 $1Rx, 2Rx, 2Ry, 2Rz, 3Rx, 3Rz$

- b) Suppose we say that two countries are adjacent if they have some part of their boundaries in common. Then “is adjacent to” is a relation  $R$  on the countries of the earth. Thus:

$(\text{India}, \text{Pakistan}) \in R$  but  $(\text{Pakistan}, \text{Bangladesh}) \notin R$   
 $(\text{Iran}, \text{Pakistan}) \in R$

# Example 1

- c) Set inclusion  $\subseteq$  is a relation on any collection of sets.

For, given any pair of sets  $A$  and  $B$ , either  $A \subseteq B$  or  $A \not\subseteq B$ .

- d) A familiar relation on the set  $Z$  of integers is “ $m$  divides  $n$ ”. We write  $m|n$  when  $m$  divides  $n$ .

$(m, n) \in R$ . Here  $(6, 30) \in R$  because  $6|30$ .  
But  $(7, 25) \notin R$  because  $7 \nmid 25$ .



# Universal, Empty and Equality Relation

Let  $A$  be any set. Then  $A \times A$  and  $\emptyset$  are subsets of  $A \times A$  and hence are relations on  $A$  called the universal relation and empty relation, respectively. Thus

$$\emptyset \subseteq R \subseteq A \times A$$

An important relation on the set  $A$  is that of equality, that is, the relation

$$\{(a, a) : a \in A\}$$

$A = \{1, 2, 3\}$   
 $R = \{(1, 1), (2, 2), (3, 3)\}$

which is usually denoted by  $=$ .



# Inverse Relation

Let  $R$  be any relation from a set  $A$  to a set  $B$ . The inverse of  $R$ , denoted by  $R^{-1}$  is the relation from  $B$  to  $A$ . That is

$$R^{-1} = \{ (b, a) : (a, b) \in R \}$$

For example if  $R = \{(1, y), (1, z), (3, y)\}$  is the relation from  $A = \{1, 2, 3\}$  to  $B = \{x, y, z\}$ , then

$$R^{-1} = \{ (y, 1), (z, 1), (y, 3) \}$$

Note:  $\underline{(R^{-1})^{-1}} = R$ . Also domain of  $R^{-1}$  is the range of  $R$ , and vice versa.



## Example 2

Let  $A = \{1, 2, 3, 4, 5, 6\}$ , and let  $R$  be the relation on  $A$  defined by “ $x$  divides  $y$ ”, written  $x|y$ .

- a) Write  $R$  as a set of ordered pairs.
- b) Find the inverse relation  $R^{-1}$  of  $R$ .

Sol (a)  $\begin{array}{l} 1|1, 1|2, 1|3, 1|4, 1|5, 1|6, \\ 2|2, 2|4, 2|6, 3|3, 3|6, 4|4, 5|5, 6|6 \end{array}$

Hence,  $R = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6),$   
 $(2,2), (2,4), (2,6), (3,3), (3,6), (4,4),$   
 $(5,5), (6,6)\}$

(b)  $R^{-1} = \{(1,1), (2,1), (3,1), \dots, (5,5), (6,6)\}$

# Representation of Relations on Finite Sets



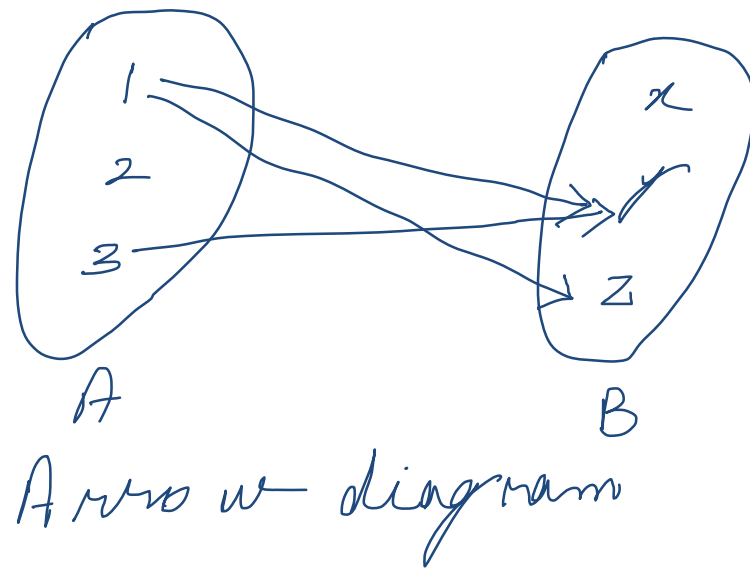
Consider, for example, the following relation  $R$  from  $A = \{1, 2, 3\}$  to  $B = \{x, y, z\}$ :

$$R = \{(1, y), (1, z), (3, y)\}$$

We can represent this relation  $R$  in two ways as follows:

|   |   | B |   |   |
|---|---|---|---|---|
|   |   | x | y | z |
| A | 1 | 0 | 1 | 1 |
|   | 2 | 0 | 0 | 0 |
|   | 3 | 0 | 1 | 0 |

matrix of the relation



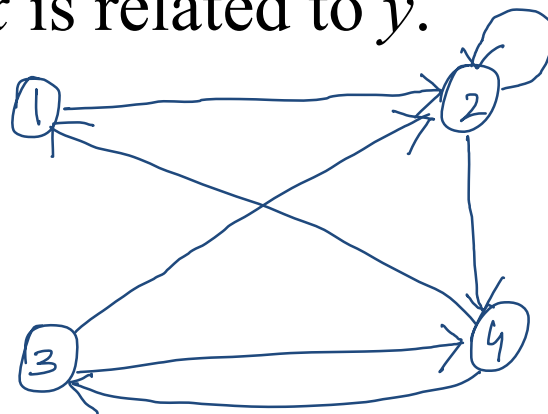


# Directed Graphs of Relations on Sets

There is another way of picturing a relation  $R$  when  $R$  is a relation from a finite set  $A$  to itself. Consider the set  $A = \{1, 2, 3, 4\}$  and the following relation  $R$ :

$$R = \{(\underline{1}, \underline{2}), (\underline{2}, \underline{2}), (\underline{2}, \underline{4}), (\underline{3}, \underline{2}), (\underline{3}, \underline{4}), (\underline{4}, \underline{1}), (\underline{4}, \underline{3})\}$$

First we write down the elements of the set  $A$ , and then we draw an arrow from each element  $x$  to each element  $y$  whenever  $x$  is related to  $y$ .

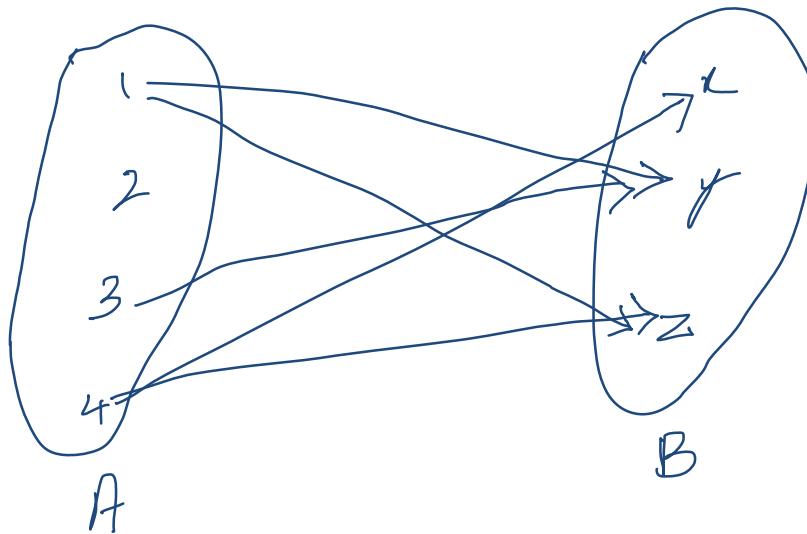


# Example 1

Given  $A = \{1, 2, 3, 4\}$  and  $B = \{x, y, z\}$ . Let  $R$  be the following relation from  $A$  to  $B$ :

$$R = \{(1, y), (1, z), (3, y), (4, x), (4, z)\}$$

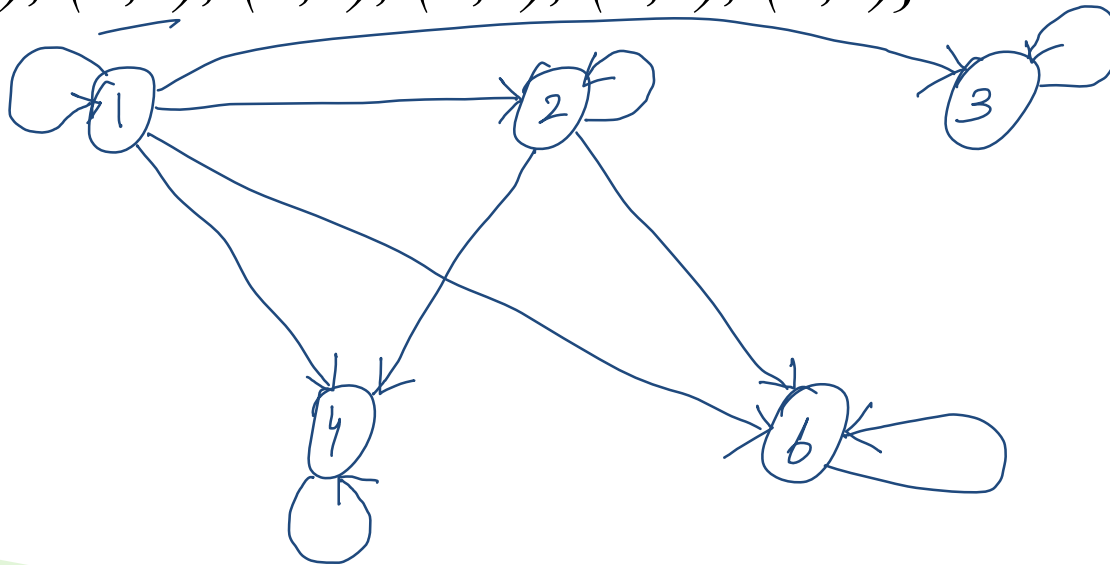
Draw the arrow diagram of  $R$ .



## Example 2

Given  $A = \{1, 2, 3, 4, 6\}$  and let  $R$  be the relation on  $A$  defined by “ $x$  divides  $y$ ”, written  $x|y$ . Draw its directed graph.

Here  $R = \{(1,1), (1, 2), (1, 3), (1, 4), \text{~~(1, 5)~~, (1, 6), (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (6,6)}\}$



# Composition of Relations



# Definition

Let  $A, B, C$  be sets, and let  $R$  be a relation from  $A$  to  $B$  and let  $S$  be a relation from  $B$  to  $C$ . Then  $R$  and  $S$  give rise to a relation from  $A$  to  $C$  denoted by  $R \circ S$  and defined as follows:

$$R \circ S = \{(a, c) : \text{there exist } b \in B \text{ for which } (a, b) \in R \text{ and } (b, c) \in S\}$$

That is,

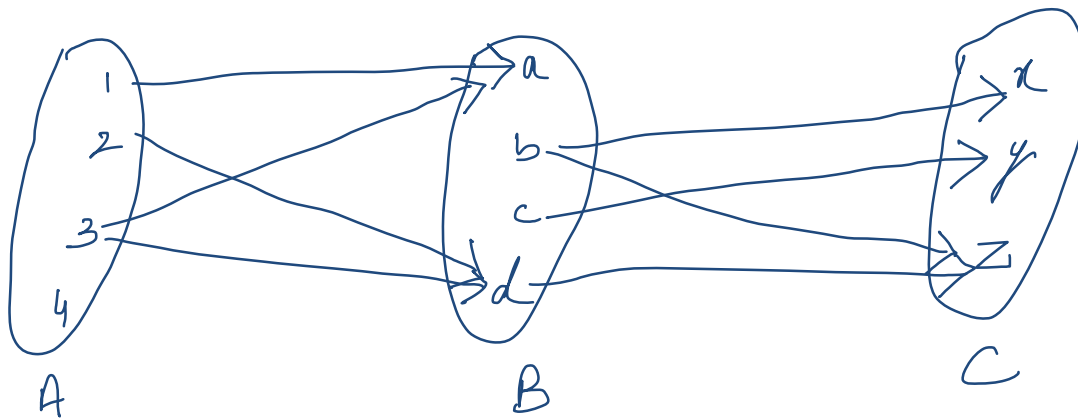
$a(R \circ S)c$  whenever there exist  $b \in B$  such that  $aRb$  and  $bSc$ .

This relation  $R \circ S$  is called the composition of  $R$  and  $S$ ; it is sometimes denoted by  $RS$ .



# Example 1

Let  $A = \{1, 2, 3, 4\}$ ,  $B = \{a, b, c, d\}$ ,  $C = \{x, y, z\}$ , and let  $R = \{(1, a), (2, d), (3, a), (3, d)\}$  and  $S = \{(b, x), (b, z), (c, y), (d, z)\}$ . Then find  $R \circ S$ .



$S \circ R = ?$

$$R \circ S = \{(2, z), (3, z)\}$$

# Note

Suppose  $R$  is a relation on a set  $A$ . Then  $R \circ R$ , the composition of  $R$  with itself, is always defined, and  $R \circ R$  is sometimes denoted by  $R^2$ . Similarly  $R^3 = \underline{R^2 \circ R} = R \circ R \circ R$ . Thus  $R^n$  is defined for all positive  $n$ .

$$R^4 = R^3 \circ R$$

$$R^n = R^{n-1} \circ R = R \circ R \circ \dots \circ R \text{ (n times)}$$



# Composition of Relations





# Definition

Let  $A, B, C$  be sets, and let  $R$  be a relation from  $A$  to  $B$  and let  $S$  be a relation from  $B$  to  $C$ . Then  $R$  and  $S$  give rise to a relation from  $A$  to  $C$  denoted by  $R \circ S$  and defined as follows:

$$R \circ S = \{(a, c) : \text{there exist } b \in B \text{ for which } (a, b) \in R \text{ and } (b, c) \in S\}$$

That is,

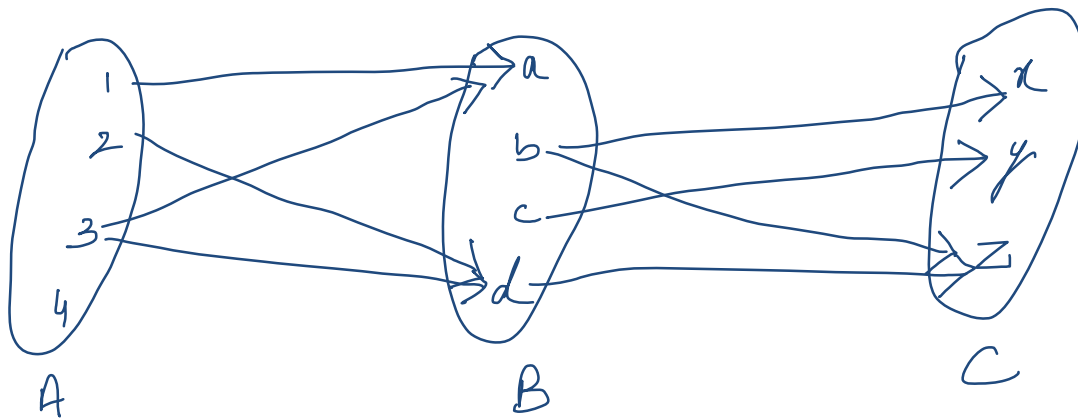
$a(R \circ S)c$  whenever there exist  $b \in B$  such that  $aRb$  and  $bSc$ .

This relation  $R \circ S$  is called the composition of  $R$  and  $S$ ; it is sometimes denoted by  $RS$ .



# Example 1

Let  $A = \{1, 2, 3, 4\}$ ,  $B = \{a, b, c, d\}$ ,  $C = \{x, y, z\}$ , and let  $R = \{(1, a), (2, d), (3, a), (3, d)\}$  and  $S = \{(b, x), (b, z), (c, y), (d, z)\}$ . Then find  $R \circ S$ .



$S \circ R = ?$

$$R \circ S = \{(2, z), (3, z)\}$$

# Note

Suppose  $R$  is a relation on a set  $A$ . Then  $R \circ R$ , the composition of  $R$  with itself, is always defined, and  $R \circ R$  is sometimes denoted by  $R^2$ . Similarly  $R^3 = \underline{R^2 \circ R} = R \circ R \circ R$ . Thus  $R^n$  is defined for all positive  $n$ .

$$R^4 = R^3 \circ R$$

$$R^n = R^{n-1} \circ R = R \circ R \circ \dots \circ R \text{ (n times)}$$



# Types of Relations



# Reflexive Relation

Consider a given set  $A$ . A relation  $R$  on a set  $A$  is reflexive if  $a R a$  for every  $a \in A$ , that is,  $(a, a) \in R$  for every  $a \in A$ .

For example, let  $A = \{1, 2, 3, 4\}$  and consider the relation  $R = \{(\underline{1}, \underline{1}), (1, 2), (2, 1), (\underline{2}, 2), (\underline{3}, 3), (\underline{4}, 4)\}$ .

$S = \{ (1,1), (1,2), (2,2), (3,3) \}$  non reflexive



# Symmetric Relation

A relation  $R$  on a set  $A$  is symmetric if whenever  $a R b$  then  $b R a$ , that is, if whenever  $(\underline{a}, \underline{b}) \in R$ , then  $(\underline{b}, \underline{a}) \in R$ .

For example, let  $A = \{1, 2, 3, 4\}$  and consider the relation  $R = \{(\underline{1}, \underline{1}), (\underline{1}, \underline{2}), (\underline{2}, \underline{1}), (2, 2), (3, 3), (4, 4)\}$ .



# Antisymmetric Relation

A relation  $R$  on a set  $A$  is antisymmetric if whenever  $a R b$  and  $b R a$  then  $a = b$ , that is, if whenever  $(a, b) \in R$ , and  $(b, a) \in R$ , then  $a = b$  or if  $(a, b) \in R$  with  $a \neq b$ , then  $(b, a)$  should not belong to  $R$ .

For example, let  $A = \{1, 2, 3, 4\}$  and consider the relation  $R = \{(1, 1), (\underline{1}, 2), (\underline{2}, 3), (\underline{1}, 3), (4, 4)\}$ .



# Transitive Relation

A relation  $R$  on a set  $A$  is transitive if whenever  $a R b$  and  $b R c$  then  $a R c$ , that is, if whenever  $\underline{(a, b)} \in R$ , and  $(b, c) \in R$ , then  $(a, c) \in R$ .

For example, let  $A = \{1, 2, 3, 4\}$  and consider the relation  $R = \{(1, 3), (2, 1)\}$  and  $S = \{(1, 1), \underline{(1, 2)}, \underline{(2, 3)}, \underline{(1, 3)}, (4, 3)\}$ .

$$S^2 = S \circ S \subseteq S$$





# Example 1

Consider the following relations:

- a) Relation  $\leq$  on the set  $\mathbb{Z}$  of integers.
- b) Set inclusion  $\subseteq$  on a collection of sets.
- c) Relation  $|$  of divisibility on the set  $\mathbb{P}$  of positive integers.

Reflexive  $a \leq a$  for all  $a \in \mathbb{Z}$ ,  $2 \leq 2$ ,  $-2 \leq 2$  etc  
Relation (a) is reflexive.

Relation (b) is reflexive

Relation (c) is reflexive.

$$A \subseteq A$$

$$A \subseteq A$$

$$2|2, 3|3$$

# Example 1

symmetric  $3 \leq 4$ , but  $4 \not\leq 3$ , so relation (a) is not symmetric.

$\nexists A \subseteq B$ , then  $B \not\subseteq A$ .  $\{1, 2\} \subseteq \{1, 2, 3\}$  but  $\{1, 2, 3\} \not\subseteq \{1, 2\}$ . so relation (b) is not symmetric.

$2 \mid 6$  but  $6 \nmid 2$ . so relation (c) is not symmetric.

Antisymmetric

$\nexists a \leq b$  and  $b \leq a$ , then  $a = b$ . so relation (a) is antisymmetric.

$\nexists A \subseteq B$  and  $B \subseteq A$ , then  $A = B$ . so relation

(b) is antisymmetric.

$\nexists m \mid n$  and  $n \mid m$ , then  $n = m$ . so relation (c) is also antisymmetric.

Transitive (a)  $\nexists a \leq b$  and  $b \leq c$ , then  $a \leq c$ . <sup>then</sup>  $2 \mid 4, 4 \mid 8$

(b)  $\nexists A \subseteq B$  and  $B \subseteq C$ , then  $A \subseteq C$   $2 \mid 8$ .

(c)  $\nexists a \mid b$ , and  $b \mid c$ , then  $a \mid c$ .

## Remark

The properties of being symmetric and antisymmetric are not negative of each other. For example, the relation  $\checkmark R = \{(1, 3), (3, 1), (2, 3)\}$  is neither symmetric and antisymmetric. On the other hand, the relation  $S = \{(1, 1), (2, 2)\}$  is both symmetric and antisymmetric.

$(a, b)$

② A relation  $R$  is transitive iff  $R^n \subseteq R$  for every  $n \geq 1$ .

$$R^2 = R \circ R$$

$$R^2 \subseteq R, R^3 \subseteq R, \dots$$

## Example 2

Let  $A = \{1, 2, 3, 4\}$ . Consider the following relation  $R$  on  $A$ :

$$R = \{(1, 1), (2, 2), (2, 3), (3, 2), (\underline{4}, 2), (4, 4)\}.$$

Reflexive:  $R$  is not reflexive because  $3 \in A$  but  $(3, 3) \notin R$ .

Symmetric:  $R$  is not symmetric because  $(4, 2) \in R$  but  $(2, 4) \notin R$ .

Antisymmetric:  $R$  is not antisymmetric because  $(2, 3) \in R$  and  $(3, 2) \in R$  but  $2 \neq 3$ .

Transitive: Here  $(4, 2) \in R$  and  $(2, 3) \in R$  but  $(4, 3) \notin R$  so  $R$  is not transitive.



# Closure of Relations



# Definition

Consider a relation  $R$  on a set  $A$ .  $R$  may or may not have property  $P$ , such as reflexivity, symmetry, or transitivity.

If there is a relation  $P(R)$  with property  $P$  containing  $R$  such that  $P(R)$  is the subset of every relation with property  $P$  containing  $R$ , then  $P(R)$  is called the closure of  $R$  with respect to  $P$ .

$$R \subseteq P(R)$$



# Notation

The reflexive, symmetric and transitive closures of a relation  $R$  will be denoted respectively by:

$\text{reflexive}(R)$ ,  $\text{symmetric}(R)$ ,  $\text{transitive}(R)$

The next theorem tells us how to easily obtain the reflexive and symmetric closures of a relation.



# Theorem 1

Let  $R$  be a relation on a set  $A$ . Then:

- (i)  $RU\Delta_A$  is the reflexive closure of  $R$ .
- (ii)  $\underline{RUR}^{-1}$  is the symmetric closure of  $R$ .

here  $\Delta_A = \{(a, a) : a \in A\}$  is the equality relation on  $A$ .





# Example 1

Consider the following relation  $R$  on a set  $A = \{1, 2, 3, 4\}$ :

$$R = \{(1,1), (1,3), (2,4), (3,1), (3,3), (4,3)\}$$

Then  $\text{reflexive}(R) = R \cup \Delta_A$

$$= R \cup \{(2,2), (4,4)\}$$
$$= \{(1,1), (1,3), (2,4), (3,1), (3,3), (4,3), (2,2), (4,4)\}$$

$$\text{Symmetric}(R) = R \cup R^{-1}$$
$$= R \cup \{(4,2), (3,4)\}$$
$$= \{(1,1), (1,3), (2,4), (3,1), (3,3), (4,3), (4,2), (3,4)\}$$

## Theorem 2

Let  $R$  be a relation on a set  $A$  with  $n$  elements. Then

$$\text{transitive}(R) = R \cup R^2 \cup \dots \cup R^n$$

Here  $R^2 = R \circ R$ ,  $R^3 = R^2 \circ R$ , ...,  $R^n = R^{n-1} \circ R$

Example 2: Consider the following relation on  $A = \{1, 2, 3\}$ :

$$R = \{(1,2), (2,3), (3,3)\}$$

Then

$$\text{transitive}(R) = R \cup R^2 \cup R^3$$

Here  $R^2 = R \circ R = \{(1,2), (2,3), (3,3)\} \circ \{(1,2), (2,3), (3,3)\}$   
 $= \{(1,3), (2,3), (3,3)\}$   
 $R^3 = R^2 \circ R = \{(1,3), (2,3), (3,3)\} \circ \{(1,2), (2,3), (3,3)\}$

So,

$$\text{transitive}(R) = R \cup R^2 \cup R^3$$
$$= \{(1,2), (2,3), (3,3), (1,3)\}$$



# Partitions



# Definition

Let  $S$  be a nonempty set. A partition of  $S$  is a subdivision of  $S$  into nonoverlapping, nonempty subsets. Precisely, a partition of  $S$  is a collection  $P = \{\underline{A_i}\}$  of nonempty subsets of  $S$  such that

- (i) Each  $a \in S$  belongs to one of the  $A_i$
- (ii) The sets  $\{A_i\}$  are mutually disjoint; that is,

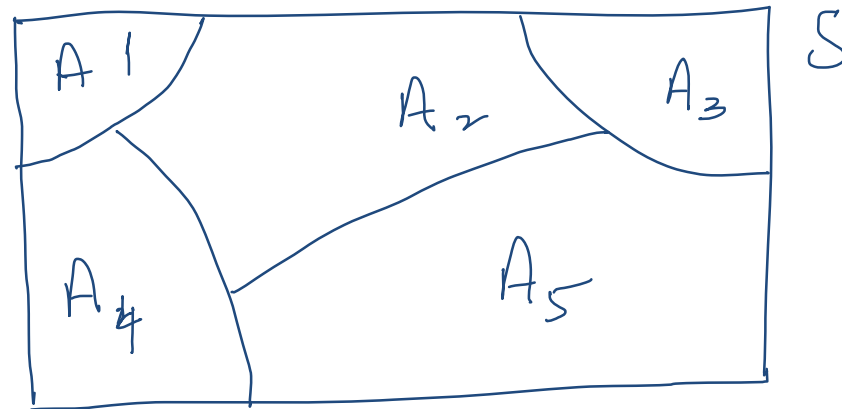
$$\text{If } i \neq j, \text{ then } A_i \cap A_j = \emptyset$$

The subsets in a partition are called cells. Thus each  $a \in S$  belongs to exactly one of the cells.



# Venn Diagram of Partition

Following figure is a Venn diagram of a partition of the rectangular set  $S$  of points into five cells:



# System of Representative

Given a partition  $P = \{A_i\}$  of a set  $S$ , any element  $b \in A_i$  is called a representative of the cell  $A_i$  and a subset  $B$  of  $S$  is called a system of representatives if  $B$  contains exactly one element of each of the cells of  $P$ .



# Example 1

Consider the following collections of subsets of  $S = \{1, 2, \dots, 9\}$ :

- (i)  $P_1 = [\{1, 3, 5\}, \{2, 6\}, \{4, 8, 9\}]$  Not a partition
- (ii)  $P_2 = [\{1, 3, 5\}, \{2, 4, 6, 8\}, \{5, 7, 9\}]$  Not a partition
- (iii)  $P_3 = [\{1, 3, 5\}, \{2, 4, 6, 8\}, \{7, 9\}]$  This is a partition

Note that  $B = \{1, 2, 7\}$  is a system of representative of the partition given in (iii).

$B = \{3, 2, 9\}$  is also system of representative.





## Example 2

Find all partition of the set  $S = \{a, b, c\}$ .

Sol. Note that we can make partitions of  $S$  containing 1, 2 or 3 cells.

(1)  $[S]$  ✓

(2)  $[\underbrace{\{a\}, \{b, c\}}], [\underbrace{\{b\}, \{a, c\}}], [\underbrace{\{c\}, \{a, b\}}]$  ✓

(3)  $[\{a\}, \{b\}, \{c\}]$  ✓



# Equivalence Relations



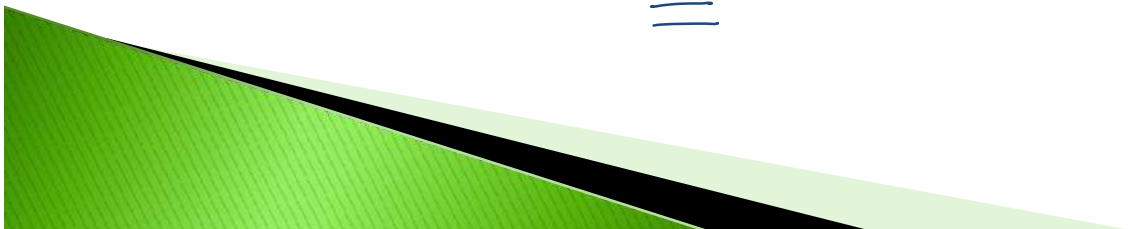
# Definition

Let  $S$  be a nonempty set. A relation  $R$  on  $S$  is an equivalence relation if  $R$  is reflexive, symmetric and transitive. That is,  $R$  is an equivalence relation on  $S$  if it has the following three properties:

- 1) For every  $a \in S$ ,  $aRa$
- 2) If  $aRb$ , then  $bRa$ .
- 3) If  $aRb$  and  $bRc$ , then  $aRc$ .

The general idea behind an equivalence relation is that it is a classification of objects which are in some way alike. We use  $\sim$  or  $\equiv$  to denote the equivalence relation.

$\equiv$



# Example 1

The relation  $=$  of equality on any set  $S$  is an equivalence relation. How?

(1)  $a = a$  for every  $a \in S$ .

(2) If  $a = b$ , then  $b = a$ .

(3) If  $a = b$  and  $b = c$ , then  $a = c$ .



## Example 2

The relation  $\subseteq$  of set inclusion is not an equivalence relation. It is reflexive and transitive, but it is not symmetric since

$$A \subseteq A, \checkmark$$

$$\text{If } A \subseteq B, B \subseteq C, \text{ then } A \subseteq C. \checkmark$$

$$\text{If } A \subseteq B, \text{ then } B \not\subseteq A.$$



## Example 3

Let  $m$  be a fixed positive integer. Two integers  $a$  and  $b$  are said to be congruent modulo  $m$  written  $a \equiv b \pmod{m}$

If  $m$  divides  $a - b$ . For example, if  $m = 4$ , then  $11 \equiv 3 \pmod{4}$  since  $4 \mid 11 - 3$ ,  $22 \equiv 6 \pmod{4}$

We claim that this relation of congruence modulo  $m$  is an equivalence relation.

(1)  $a \equiv a \pmod{m}$  for every  $a \in \mathbb{Z}$ . because  $m \mid a - a = 0$ .

(2) If  $a \equiv b \pmod{m}$ , then  $m \mid a - b \Rightarrow m \mid -(a - b) \Rightarrow m \mid b - a \Rightarrow b \equiv a \pmod{m}$

### Example 3

(3) If  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ ,  
then we will show that  $a \equiv c \pmod{m}$

Here  $m$  divides  $a - b$  and  $m$  divides  $b - c$ .

So,  $m$  divides  $(a - b) + (b - c)$ .

$$\parallel \parallel a - c.$$

Hence,  $a \equiv c \pmod{m}$ .



# Equivalence Relations and Partition





# Equivalence Class and Quotient Set

Suppose  $R$  is an equivalence relation on a set  $S$ . For each  $a$  in  $S$ , let  $\underline{[a]}$  denote the set of elements of  $S$  to which  $a$  is related under  $R$ ; that is,

$$\underline{[a]} = \{x: (a, x) \in R\}$$

We call  $\underline{[a]}$  the equivalence class of  $a$  in  $S$  under  $R$ . The collection of all such equivalence classes is denoted by  $\underline{S/R}$ , that is,

$$\underline{S/R} = \{\underline{[a]} : a \in S\}$$

It is called the quotient set of  $S$  by  $R$ .



# Theorem 1

Let  $R$  be an equivalence relation on a set  $S$ . Then the quotient set  $S/R$  is a partition of  $S$ . Conversely, suppose  $P = \{A_i\}$  is a partition of a set  $S$ . Then there is an equivalence relation  $\sim$  on  $S$  such that the set  $S/\sim$  of equivalence classes is the same as the partition  $P = \{A_i\}$ .



# Example 1

Consider the relation  $R = \{(1, \check{1}), (2, \check{2}), (1, \check{3}), (3, \check{1}), (3, \check{3}), (4, 4)\}$  on  $S = \{1, 2, 3, 4\}$ .

Observe that  $R$  is an equivalence relation.

$$[\underline{1}] = \{1, 3\}, [\underline{2}] = \{2\}, [\overset{x}{\underline{3}}] = \{1, 3\}, [\underline{\check{4}}] = \{4\}$$

Note that  $[1] = [3]$ . Now,

$S/R = \{[\underline{1}], [\underline{2}], [\overset{x}{\underline{3}}], [\underline{\check{4}}]\}$  is a partition of  $S$ .

System of representative  
 $\{1, 2, 4\}$  or  $\{2, 3, 4\}$



## Example 2

$$3 \equiv 0 \pmod{3}$$

$$3 \equiv 6 \pmod{3}$$

Let  $R_3$  be the relation on the set  $Z$  of integers defined by

$$x \equiv y \pmod{3}$$

Here  $x \equiv y \pmod{3}$  is an equivalence relation.  
It means  $x - y$  is divisible by 3.

$$[0] = \{ \dots, -6, -3, 0, 3, 6, 9, \dots \}$$

$$[1] = \{ \dots, -5, -2, 1, 4, 7, 10, \dots \}$$

$$[2] = \{ \dots, -7, -4, -1, 2, 5, 8, 11, \dots \}$$

$$[3] = \{ \dots, -6, -3, 0, 3, 6, 9, \dots \}$$

$$Z/R_3 = \{ [0], [1], [2] \}$$

is a partition of  $Z$ .

$$2 \equiv -1 \pmod{3}$$

$$2 \equiv -4 \pmod{3}$$

$$0 \equiv 3 \pmod{3}$$

$$0 \equiv 6 \pmod{3}$$

$$0 \equiv -3 \pmod{3}$$

$$1 \equiv 4 \pmod{3}$$

$$1 \equiv 7 \pmod{3}$$

$$1 \equiv -2 \pmod{3}$$

$$1 \equiv -5 \pmod{3}$$

$$2 \equiv 5 \pmod{3}$$

$$2 \equiv 8 \pmod{3}$$

## Example 2

$$\mathbb{Z} = [0] \cup [1] \cup [2]$$

$$\mathbb{Z}/R_3 = \mathbb{Z}/_3\mathbb{Z} = \mathbb{Z}_3$$

$\{0, 1, 2\}$  is a system of representatives of the equivalence classes.



# Proof of Theorem 1

For the first part, we want to prove that

- (i) For each  $a \in S$ , we have  $a \in [a]$ .
- (ii)  $[a] = [b]$  if and only if  $(a, b) \in R$ .
- (iii) If  $[a] \neq [b]$ , then  $[a]$  and  $[b]$  are disjoint.



# Proof of Theorem 1



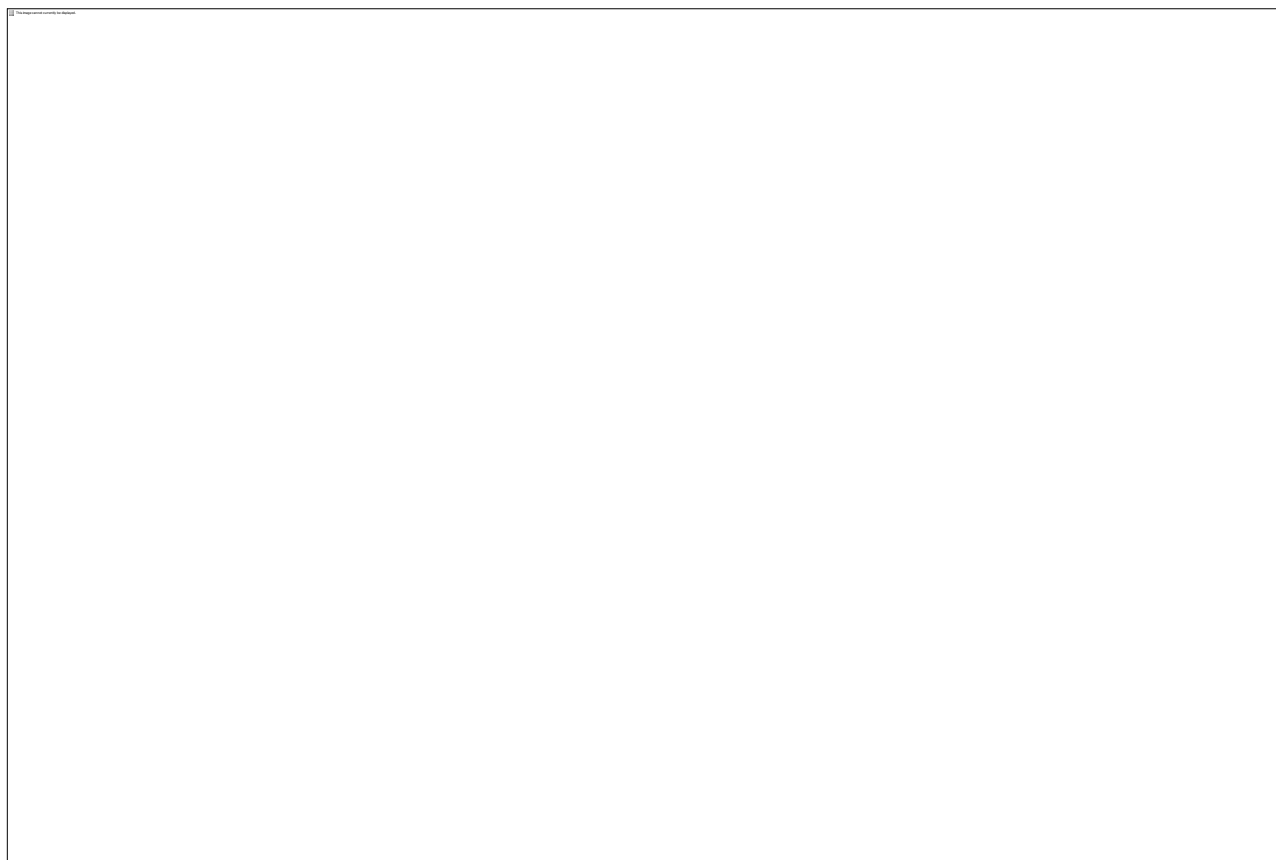
# Proof of Theorem 1

For the 2<sup>nd</sup> part, let  $a, b \in S$  and define  $a \sim b$  if  $a$  and  $b$  belong to the same cell  $A_k$  in  $P$ . We need to show that  $\sim$  is reflexive, symmetric and transitive.





# Proof of Theorem 1

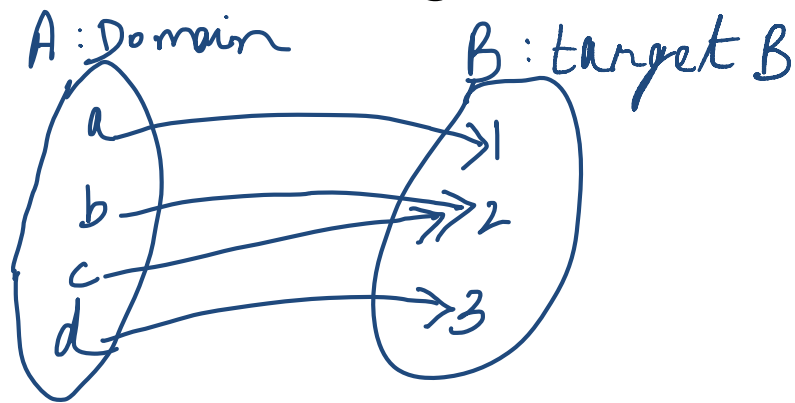


# Functions



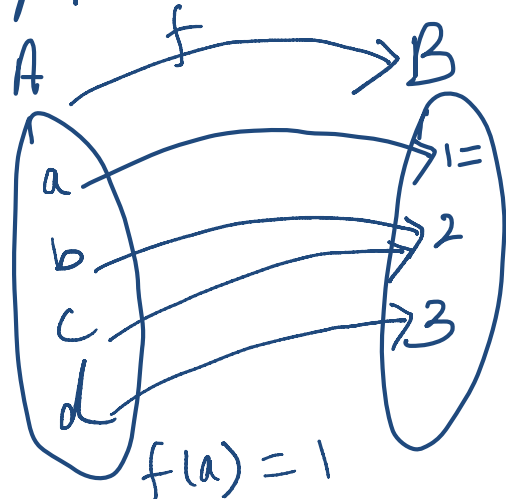
# Functions

Suppose that to each element of a set  $A$  we assign a unique element of a set  $B$ ; the collection of such assignments is called a function from  $A$  into  $B$ . The set  $A$  is called the domain of the function, and the set  $B$  is called the target set.



# Notation

Suppose  $f: A \rightarrow B$  and  $a \in A$ . Then  $f(a)$  will denote the unique element of  $B$  which  $f$  assigns to  $a$ .



$f$  sends or maps  $a$  into  $f(a) = 1$ .

$$\begin{aligned} \text{Im}(f) &= \text{image of } f \\ &= \{1, 2, 3\} = \text{range of } f. \end{aligned}$$

Here  $f(b) = 2$

$f(c) = 2$

$f(d) = 3$

$$\text{Im}(f) = \{b \in B : \text{there exists } a \in A \text{ for which } f(a) = b\}$$

Note:  $\text{Im}(f)$  is a subset of target set  $B$ .

# Functions

Mathematical Formula:

$$\overline{f(x) = x^2},$$

or  $x \mapsto x^2$

↓  
goes to

Let  $f(x) = y$ , then  $y = x^2 \rightarrow$  independent variable  
dependent variable

Domain

$$f : A \rightarrow B$$

↓  
domain

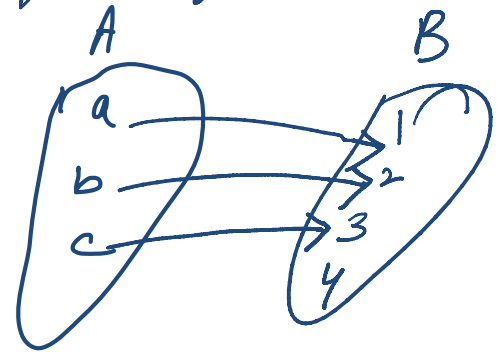
→ target set



# Functions

Remark: Suppose  $f: A \rightarrow B$ . If  $A'$  is a subset of  $A$ , then  $f(A')$  = set of images of elements in  $A'$ .

And if  $B'$  is a subset of  $B$ , then  $f^{-1}(B')$  = set of elements of  $A$  each whose image belongs to  $B'$ .



We call  $f(A')$  the image of  $A'$ ,  
and  $f^{-1}(B')$  the inverse image  
or preimage of  $B'$ .

$A' \subseteq A$ , means  $A' = \{a, b\}$

$$f(A') = \{1, 2\}$$

$$\text{Let } B' = \{1, 3\}$$

$$\text{so } f^{-1}(B') = \{a, c\}$$

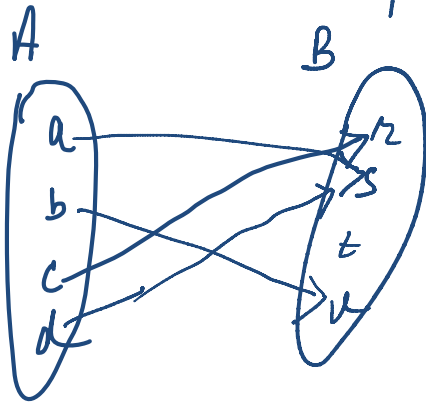
# Examples

a) Let  $f(x) = x^3$

The image of 2 is 8,  $f(2) = 8$ . Similarly  $f(-3) = -27$ .

b) Let  $A = \{a, b, c, d\}$ ,  $B = \{r, s, t, u\}$ . Define a function from  $A$  to  $B$  as:

$$f(a) = s, f(b) = u, f(c) = r, f(d) = s$$



The image of  $f = \{r, s, u\} = \text{range}$

# Examples





# Identity Function

Consider any set  $A$ . Then there is a function from  $A$  into  $A$  which sends each element <sup>of  $A$</sup>  into itself. It is called the identity function on  $A$  and it is usually denoted by

$\mathbb{I}_A: A \rightarrow A$  defined by

$\mathbb{I}_A(a) = a$  for every element  
 $a \in A$ .



# Functions as Relations



# Functions as Relations

Every function  $f: A \rightarrow B$  give rise to a relation from  $A$  to  $B$  called the graph of  $f$  and defined by

$$\text{Graph of } f = \{(\underline{a}, \underline{b}); a \in A, b = f(a)\}$$

This ordered pair  $(a, b)$  is unique.

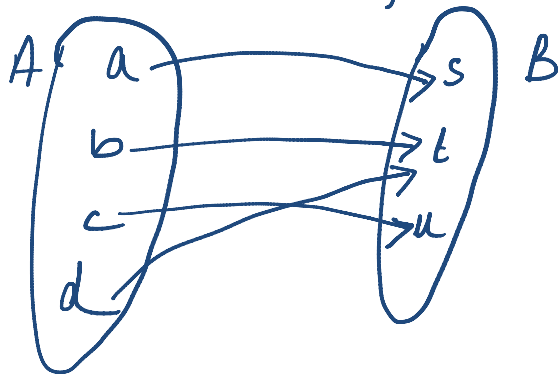
For example, consider the function  $f(x) = x^2$  . We can represent this function as a relation and draw its graph as follows:

$$\begin{aligned} f(1) &= 1, f(2) = 4, f(3) = 9, f(4) = 16 \\ \text{graph of } f &= \{(1, 1), (2, 4), (3, 9), (4, 16)\} \\ &= \{(x, y) : y = x^2\} \end{aligned}$$

# Functions as Relations

Set  $A = \{a, b, c, d\}$ ,  $B = \{s, t, u\}$

Define a function from  $A$  to  $B$  as:



graph of  $f = \{(a, s), (b, t), (c, u), (d, t)\}$   
 $(b, s)$

Here  $f(a) = s$ ,  $f(b) = t$ ,  
 $f(c) = u$ ,  $f(d) = t$



## Example 1

$$A = \{a, b, c, d\}, \quad B = \{s, u, r, s\}$$

Let  $f: A \rightarrow B$  be the function defined as follows:

$$f(a) = s, \quad f(b) = u, \quad f(c) = r, \quad f(d) = s$$

$$\text{graph of } f = \{ (a, s), (b, u), (c, r), (d, s) \}.$$

Then the graph of  $f$  is the following set of ordered pairs:



## Example 2

Consider the following relations on the set  $A = \{1, 2, 3\}$ .

$$f = \{(\overset{\checkmark}{1}, 3), (\overset{\checkmark}{2}, 3), (\overset{\checkmark}{3}, 1)\}, \quad g = \{(1, 2), (3, 1)\},$$

$$h = \{(\overset{\checkmark}{1}, 3), (2, 1), (\overset{\checkmark}{1}, 2), (3, 1)\}$$

Here  $f$  is a function. Here  $f(1) = 3, f(2) = 3, f(3) = 1$ .

\*  $g$  is not a function, since  $2 \in A$  is not the first coordinate of any pair in  $g$ .

\*  $h$  is not a function, since  $1 \in A$  appears as the first coordinate of two distinct ordered pairs.



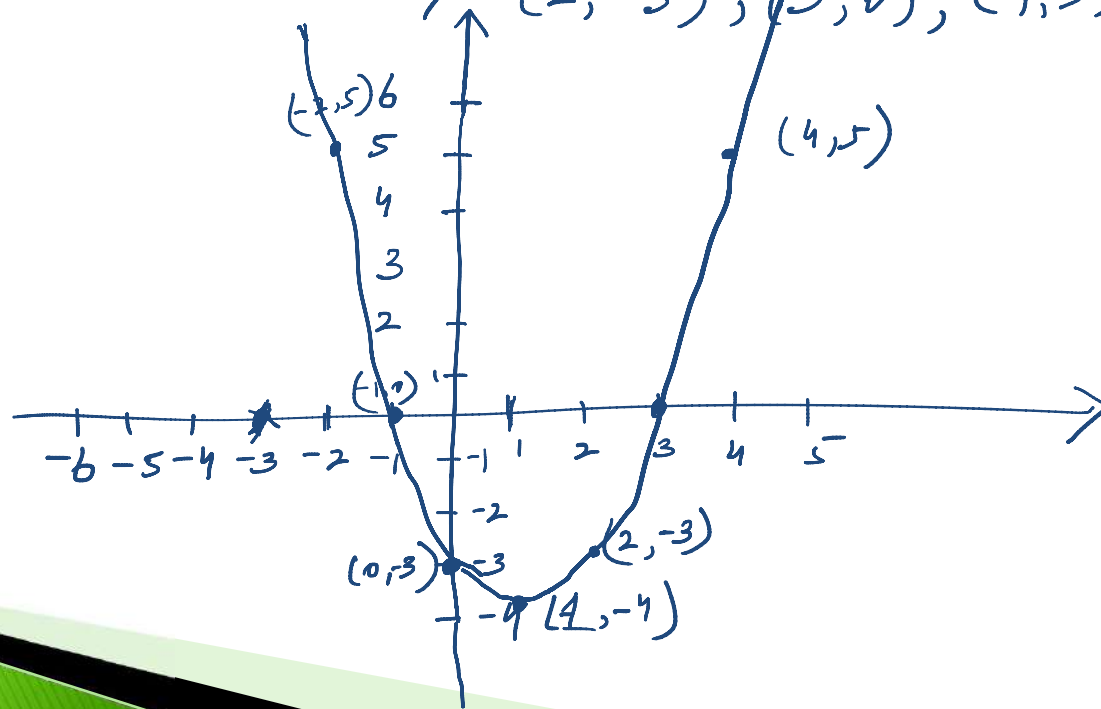
# Example 3

Sketch the graph of  $f(x) = x^2 - 2x - 3$ .

| $x$ | $f(x)$ |
|-----|--------|
| -2  | 5      |
| -1  | 0      |
| 0   | -3 ✓   |
| 1   | -4     |
| 2   | -3     |
| 3   | 0      |
| 4   | 5      |

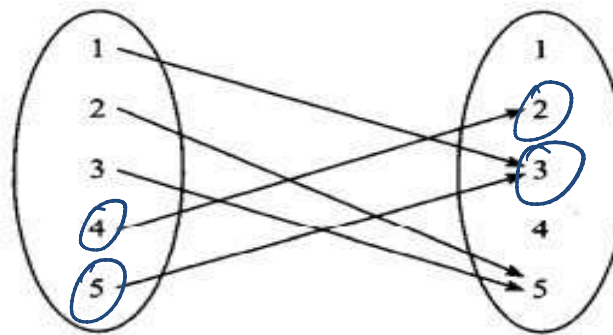
$$f(-2) = (-2)^2 - 2(-2) - 3 \\ = 4 + 4 - 3 = -5$$

graph of  $f : \{(-2, 5), (-1, 0), (0, -3), (1, -4), (2, -3), (3, 0), (4, 5)\}$



## Example 4

Let  $A = \{1, 2, 3, 4\}$  and let  $f: A \rightarrow A$  be defined by the following diagram.



- Find the graph of  $f$ .  $\{(1, 3), (2, 5), (3, 5), (4, 2), (5, 2)\}$
- Find  $f(A)$ , the image of  $f$ .  $f(A) = \{3, 5, 2\} = \{2, 3, 5\}$
- Find  $f(S)$  where  $S = \{1, 3, 5\}$ .  $f(S) = \{3, 5\}$
- Find  $f^{-1}(T)$  where  $T = \{2, 3\}$ .  $f^{-1}(T) = \{1, 4, 5\}$



# Composition of Functions



# Definition

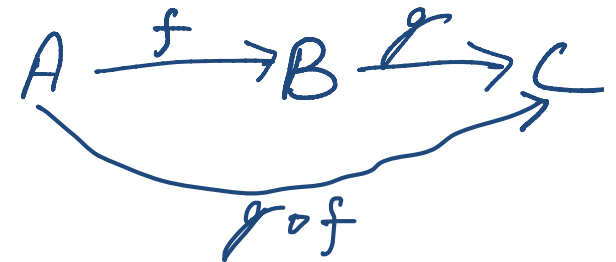
Considers functions  $f:A \rightarrow B$  and  $g:B \rightarrow C$ , that is, where the target set  $B$  of  $f$  is the domain of  $g$ . This relationship can be pictured by the following diagram:

$$\begin{array}{c} a \in A \xrightarrow{f} B \xrightarrow{g} C \\ \text{Let } a \in A, \text{ then } f(a) \in B, \underline{g(f(a))} \in C \end{array}$$

This new function is called the composition of  $f$  and  $g$ , and it is denoted by  $g \circ f$ .

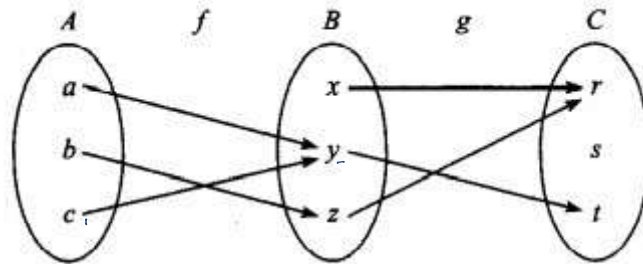
More briefly, if  $f:A \rightarrow B$  and  $g:B \rightarrow C$ , then we define a new function  $g \circ f: A \rightarrow C$  by

$$\underline{(g \circ f)(a)} = g(f(a))$$



# Example 1

Let  $f:A \rightarrow B$  and  $g:B \rightarrow C$  be the functions defined in the diagram.



We compute  $g \circ f: A \rightarrow C$  by its definition:

$$\checkmark (g \circ f)(a) = g(f(a)) = g(x) = r,$$

$$\checkmark (g \circ f)(b) = g(f(b)) = g(y) = t,$$

$$\checkmark (g \circ f)(c) = g(f(c)) = g(z) = s$$

## Example 2

Let  $f: \mathbf{R} \rightarrow \mathbf{R}$  and  $g: \mathbf{R} \rightarrow \mathbf{R}$  be defined by  $\underline{f(x)} = x^2$ ,  $\underline{g(x)} = x + 3$ .

$$\checkmark (g \circ f)(2) = g(f(2)) = g(4) = 4 + 3 = 7$$

$$\checkmark (f \circ g)(2) = f(g(2)) = f(5) = 5^2 = 25$$

We compute general formula for these functions.

$$(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 3$$

$$(f \circ g)(x) = f(g(x)) = f(x + 3) = (x + 3)^2 = x^2 + 6x + 9$$

$$f(2) = 4$$

$$g(2) = 2 + 3 = 5$$



### Example 3

Consider any function  $f:A\rightarrow B$ . Then *one can easily show*

that  $f \circ \underline{1}_A = f$  and  $\underline{1}_B \circ f = f$   
 $\downarrow$   
 identity function

check:

Let  $f(a) = \underline{b}$ . Then

$$\begin{array}{l|l} (f \circ 1_A)(a) = f(1_A(a)) & (1_B \circ f)(a) \\ \hline \quad \quad \quad = \underline{f(a)} & = 1_B(f(a)) \\ & = 1_B(b) = b = \underline{f(a)} \end{array}$$

$\mathbb{I}_A : A \rightarrow A$   
such that  
 $\mathbb{I}_A(a) = a$

# Theorem

Let  $f:A \rightarrow B$ ,  $g:B \rightarrow C$  and  $h:C \rightarrow D$ . Then prove that  $(f \circ g) \circ h = f \circ (g \circ h)$ .

Proof. Let  $a \in A$ . Then :

$$\overset{h(a)}{((f \circ g) \circ h)(a)} = (f \circ g)(\underline{h(a)}) = f(g(h(a))) \checkmark$$

$$\begin{aligned} ((f \circ (g \circ h))(a) &= f((g \circ h)(a)) \\ &= f(g(h(a))) \checkmark \end{aligned}$$

Thus  ~~$((f \circ g) \circ h)(a)$~~   $((f \circ g) \circ h)(a) = (f \circ (g \circ h))(a)$   
for every  $a \in A$ ,

# One to one, Onto and Invertible function



# One-to-One Function

A function  $f:A \rightarrow B$  is said to be one-to-one (injective) if different elements in the domain  $A$  have distinct images. Another way of saying the same things follows:

*$f$  is one-to-one if  $f(a) = f(b)$  implies  $a = b$ . ✓*

For example, let  $f:\mathbf{R} \rightarrow \mathbf{R}$  be defined by  $f(x) = \underline{2x-3}$  is one-to-one. But  $f(x) = x^2$  is not one-to-one.

$$f(2) = 4$$

$$f(-2) = 4$$

*Here  $f(2) = f(-2)$  but  $2 \neq -2$ .*





# Onto Function

A function  $f:A \rightarrow B$  is said to be onto (surjective) function if every element of  $B$  is the image of some element in  $A$  or, in other words, if the image of  $f$  is the entire target set  $B$ . In such a case we say that  $f$  is a function of  $A$  onto  $B$  or that maps  $A$  onto  $B$ . That is:

$f$  maps  $A$  onto  $B$  if  $\forall b \in B, \exists a \in A$  such that  $f(a) = b$ .

For example,  $f:\mathbf{R} \rightarrow \mathbf{R}$  be defined by  $f(x) = 2x-3$  is onto.

But  $f(x) = 1+x^2$  not onto since  $0 \in \mathbf{R}$  but there is no real number  $x$  such that  $f(x) = 0$ .

$$\begin{aligned} f(x) &= 0 \\ 1 + x^2 &= 0 \\ x^2 &= -1 \\ x &= \sqrt{-1} = i \end{aligned}$$



# Invertible Function

A function  $f:A \rightarrow B$  is said to be invertible if its inverse relation  $f^{-1}$  is a function from  $B$  to  $A$ . Equivalently,  $f:A \rightarrow B$  is invertible if there exists a function  $f^{-1}:B \rightarrow A$  called the inverse of  $f$ , such that

$$\underline{f^{-1} \circ f} = 1_A \quad \text{and} \quad \underline{f \circ f^{-1}} = 1_B$$



# Theorem

A function  $f: A \rightarrow B$  is invertible if and only if  $f$  is both one-to-one and onto.

For example, let  $f: \mathbf{R} \rightarrow \mathbf{R}$  be defined by  $f(x) = \underline{2x-3}$ . Now  $f$  is one-to-one and onto; hence  $f$  has an inverse function.

We can find the inverse of  $f$  as follows:

$$\begin{aligned} y &= 2x - 3 \\ \Rightarrow y + 3 &= 2x \\ \Rightarrow \frac{y+3}{2} &= x \\ \text{Now interchange } x \text{ and } y: \\ y &= \frac{x+3}{2} \\ \Rightarrow f^{-1}(x) &= \frac{x+3}{2} \end{aligned} \quad \left| \begin{aligned} f \circ f^{-1}(x) &= x \\ f^{-1} \circ f(x) &= x \\ \text{verify } f \circ f^{-1} &= ? \end{aligned} \right.$$

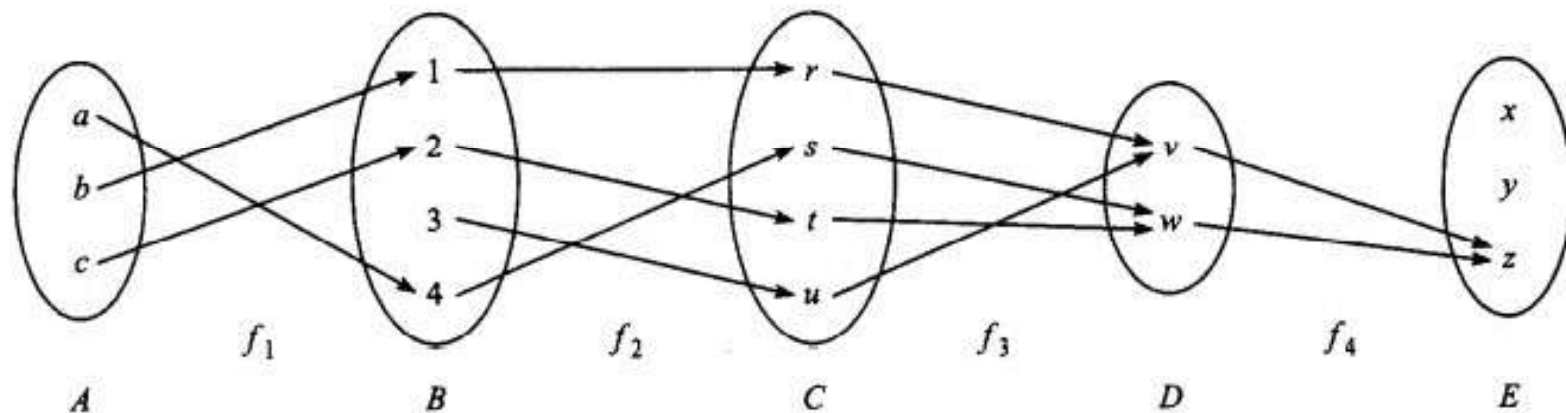
# One-to-One Correspondence

If  $f: A \rightarrow B$  is both one-to-one and onto, then  $f$  is called a one-to-one correspondence (bijective) between  $A$  and  $B$ . This terminology comes from the fact that each element of  $A$  will correspond to a unique element of  $B$  and vice versa. For example,  $f(x) = 2x - 3$  is a bijective function.



# Example 1

Consider functions  $f_1, f_2, f_3$  and  $f_4$  defined in the following figure.



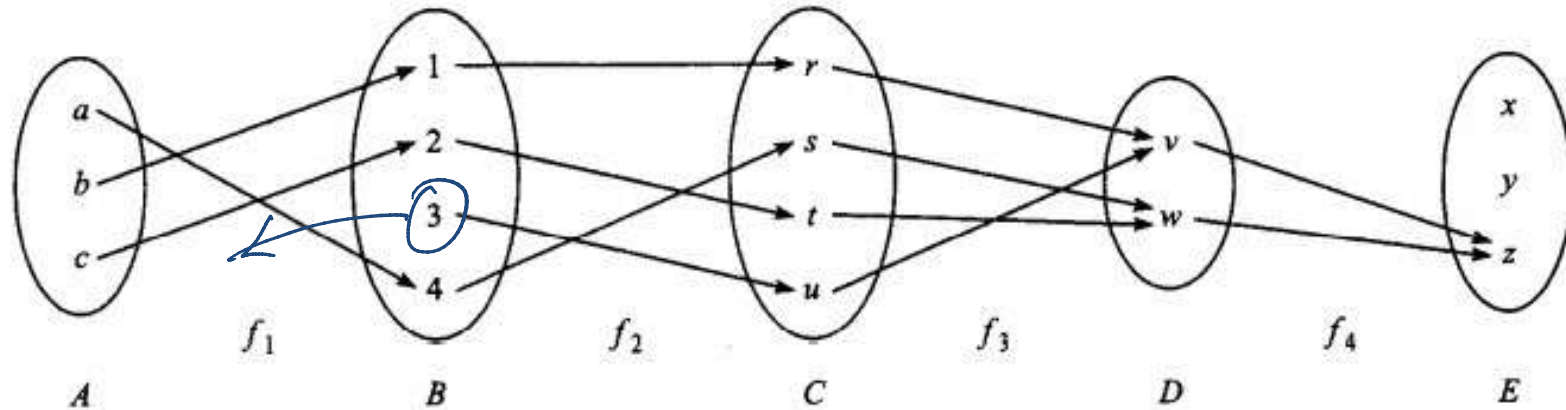
One-to-One

Here  $f_1$  is one-to-one.  $f_2$  is one-to-one.

Since  $f_3(s) = f_3(t) = w$ , so  $f_3$  is not one-to-one.

Since  $f_4(v) = f_4(w) = z$ , so  $f_4$  is not one-to-one.

# Example 1



Onto Since  $3 \in B$  is not the image under  $f_1$  of any element of  $A$ , so  $f_1$  is not onto.

image of  $f_1 = \{1, 2, 4\} \neq$  target set  $B$

Here  $f_2$  is onto. Here  $f_3$  is also onto.

Since image of  $f_4 = \{z\} \neq$  target set  $E$ .

so  $f_4$  is not onto. We can say that

$f_2$  is invertible.

## Example 2

Consider functions  $f: A \rightarrow B$  and  $g: B \rightarrow C$ . Prove that if  $f$  and  $g$  are one-to-one, then the composition function  $g \circ f$  is one-to-one.

Proof: Suppose  $(g \circ f)(x) = (g \circ f)(y) \mid \begin{array}{l} \text{if } f(x) = f(y) \\ \text{then } x = y. \end{array}$

$$\begin{aligned} &\Rightarrow g(f(x)) = g(f(y)) \\ &\Rightarrow f(x) = f(y) \\ &\Rightarrow x = y \quad \checkmark \end{aligned}$$

Also you can prove that  $g \circ f$  is onto.



# Mathematical Functions





# Integer Value Function

Let  $x$  be any real number. The integer value of  $x$ , written  $\text{INT}(x)$ , converts  $x$  into an integer by deleting the fractional part of the number. Thus

$$\text{INT}(3.14) = 3, \quad \text{INT}(7) = 7, \quad \text{INT}(\sqrt{5}) = 2,$$

$$\text{INT}(-8.5) = -8, \quad \text{INT}(-3.33) = -3$$



# Remainder Function: Modular Arithmetic

Let  $k$  be any integer and let  $M$  be a positive integer. Then

$$\overset{\checkmark}{k}(\text{mod } \overset{\checkmark}{M}) = \overset{\checkmark}{r}$$

(read  $k$  modulo  $M$ ) will denote the integer remainder when  $k$  is divided by  $M$ . More exactly,  $k(\text{mod } M)$  is the unique integer  $r$  such that

$$k = Mq + r \text{ where } 0 \leq r < M$$

When  $k$  is positive, simply divide  $k$  by  $M$  to obtain remainder  $r$ . Thus

$$\begin{aligned} 25(\text{mod } 7) &= 4, & 25(\text{mod } 5) &= 0, \\ \text{Here } k &= 25, M = 7 & 35(\text{mod } 11) &= 2, \\ 3(\text{mod } 8) &= 3 \end{aligned}$$

$$\begin{array}{r} 3 \\ 7 \overline{) 25} \\ \underline{21} \phantom{0} \\ 4 \end{array}$$

# Remainder Function: Modular Arithmetic

When  $k$  is negative, divide  $|k|$  by the modulus  $M$  to obtain the remainder  $s$ . Then, when  $s \neq 0$ ,  $k(\text{mod } M) = M - s$ . Thus:

$$-26(\text{mod } 7) = \textcircled{7} - 5 = \textcircled{2}, \quad -371(\text{mod } 8) = 8 - \textcircled{3} = \textcircled{5}$$

$$|-26| = 26$$

$$\begin{array}{r} 46 \\ 8 \overline{) 371} \\ \underline{368} \\ 3 = s \end{array}$$

$$\begin{array}{r} 3 \\ 7 \overline{) 26} \\ \underline{21} \\ 5 = s \\ -4 \\ 7 \overline{) -26} \\ \underline{-28} \\ 2 \end{array}$$



# Remainder Function: Modular Arithmetic

The term “mod” is also used for the mathematical congruence relation, which is denoted and defined as follows:

$a \equiv b \pmod{M}$  if and only if  $M$  divides  $b - a$

$M$  is called the modulus, and  $a \equiv b \pmod{M}$  is read “ $a$  is congruent to  $b$  modulo  $M$ ”

$5 \equiv 5 \pmod{5}$  because  $\frac{5-5}{5} = \frac{0}{5} = 0$

$8 \equiv 16 \pmod{2}$  because  $\frac{8-16}{2} = \frac{-8}{2} = -4$

$5 \not\equiv 1 \pmod{3}$

Note: ①  $a \equiv a \pmod{M}$

②  $a \pm M \equiv a \pmod{M}$

$$\left\{ \begin{array}{l} 8 \equiv 16 \pmod{2} \\ 8+2 \equiv 16 \pmod{2} \\ 8-2 \equiv 16 \pmod{2} \end{array} \right.$$

# Arithmetic Operations with Modulo

Arithmetic modulo M refers to the arithmetic operations of addition, multiplication, and subtraction. It is quite simple: calculate as in ordinary arithmetic and reduce the result to the smallest positive remainder by dividing the modulus. For example,

$$12+9 \equiv 21 \equiv 1 \pmod{5}$$

$$35 \times 7 \equiv 245 \equiv 0 \pmod{5}$$

$$12-9 \equiv 3 \pmod{5}$$

$$12+3 \equiv 0 \pmod{5}$$

$$15-23 \equiv -8 \equiv 2 \pmod{5} \text{ because } \frac{-8-2}{5} = -2$$



# Exponential and Logarithmic functions



# Exponential Function

An exponential function is a mathematical in form as follows:

$$f(x) = a^x$$

where  $x$  is a variable and  $a$  is a constant which is called the base of the function and it should be greater than 0.

For example,  $f(x) = 2^x$ ,  $f(x) = 5^x$  etc are all exponential functions.  $f(x) = 0.5^x$

$f(x) = -2^x$ . Take  $x = \frac{1}{2}$ , then  $f(x) = (-2)^{\frac{1}{2}} = \sqrt{-2}$   
= undefined!



# Logarithmic Function

Logarithms are related to exponent as follows. Let  $b$  be a positive number. The logarithm of any positive number  $x$  to the base  $b$ , written

$$\log_b x$$

represents the exponent to which  $b$  must be raised to obtain  $x$ . That is,

$$x = \log_b b^x \quad \text{and} \quad b^x = x$$

are equivalent statements.

Note:  $x$  cannot be negative and 0.





# Examples

$$\log_2 8 = 3 \text{ since } 2^3 = 8, \quad \log_{\textcircled{10}} 100 = 2 \text{ since } 10^2 = 100$$

$$\log_2 64 = 6 \text{ since } 2^6 = 64, \quad \log_{10} 0.001 = -3$$

since  $10^{-3} = 0.001$ .

For any base  $b$ ,

①  $\log_b 1 = 0$  since  $b^0 = 1$

②  $\log_b b = 1$  since  $b^1 = b$ ;  $\log_2 2 = 1$

Common logarithms if it has base 10

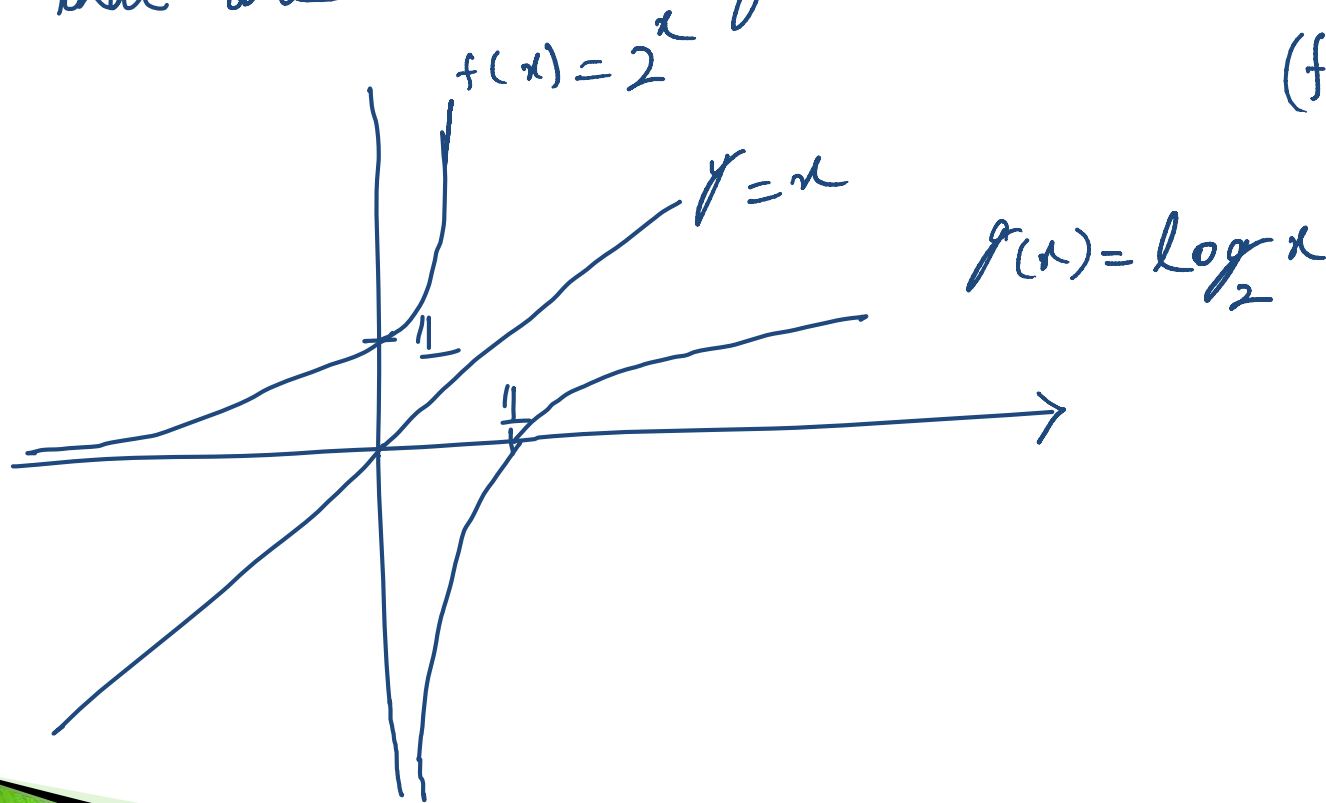
Natural logarithms  $\log_e x = \ln x$

# Relationship Between the Exponential and Logarithmic Function

$$f(x) = b^x \text{ and } g(x) = \log_b x$$

is that are inverses of each other.

$$(f \circ g)(x) = x$$



# Recursively Defined Functions



# Definition

A recursive or inductive definition of a function consists of two steps.

- 1) Basis Step: Specify the value of the function at initial values. (e.g.  $f(0)$  defined.)
- 2) Recursive Step: Give a rule for finding its values at an integer from its values at smaller integers. (For  $n > 0$ , define  $f(n)$  in terms of  $f(0), f(1), \dots, f(n-1)$ )



# Example 1: Fibonacci Sequence

- a) If  $n = 0$  or  $n = 1$ , then  $F_n = n$       $F_0 = 0$ ,  $F_1 = 1$
- b) If  $n > 1$ , then  $F_n = F_{n-2} + F_{n-1}$ .

Here the base values are 0 and 1. Hence, the sequence can be found as:

$$\begin{aligned} F_2 &= F_0 + F_1 = 0 + 1 = 1 \checkmark \\ F_3 &= F_1 + F_2 = 1 + 1 = 2 \\ F_4 &= F_2 + F_3 = 1 + 2 = 3 \\ F_5 &= F_3 + F_4 = 2 + 3 = 5 \\ &\vdots \end{aligned}$$

0, 1, 1, 2, 3, 5, 8, 13, ...



## Example 2:

Find  $f(1)$ ,  $f(2)$ ,  $f(3)$  and  $f(4)$  if  $f(n)$  is defined recursively by  $\underline{f(0) = 1}$  and  $\underline{f(n+1) = f(n) + 2}$  for  $n = 0, 1, 2, \dots$

Sol.  $f(n+1) = f(n) + 2$

put  $n = 0$ ,  $f(1) = f(0) + 2 = 1 + 2 = 3$

put  $n = 1$ ,  $f(2) = f(1) + 2 = 3 + 2 = 5$

put  $n = 2$ ,  $f(3) = f(2) + 2 = 5 + 2 = 7$

put  $n = 3$ ,  $f(4) = f(3) + 2 = 7 + 2 = 9$



$\{a, b, c, d\}$  ,  $\{2, 3, 5, 7\}$ ,  $\{x, y, z, t\}$

## Equipotent Sets

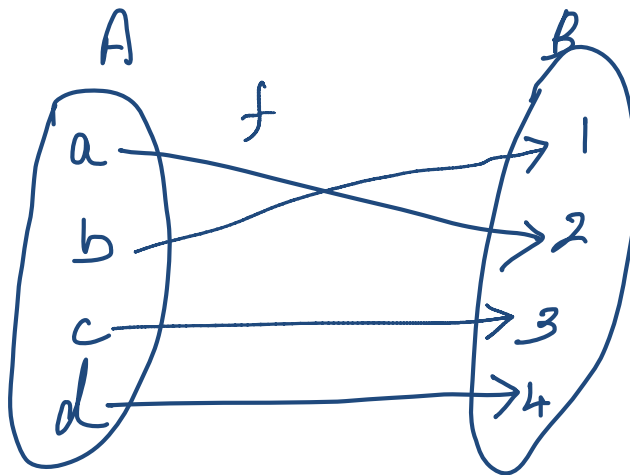


# Definition

Sets  $A$  and  $B$  are said to have the same cardinality or the same number of elements, or to be equipotent, written

$$A \cong B$$

if there is a function  $f: A \rightarrow B$  which is bijective.



Here  $f$  is one-to-one  
 $f$  is onto.

$\therefore f$  is bijective.  
or  $f$  is one-to-one  
correspondence.



# Theorem 1

The relation  $\approx$  of being equipotent is an equivalence relation in any collection of sets. That is,

- i)  $A \approx A$  for any set  $A$ .
- ii) If  $A \approx B$ , then  $B \approx A$ .
- iii) If  $A \approx B$  and  $B \approx C$ , then  $A \approx C$ .

Proof.

(i) Let  $\overset{\checkmark}{\Pi}_A: \overset{\checkmark}{A} \rightarrow \overset{\checkmark}{A}$  is a bijective mapping.  
It is defined as  $\overset{\checkmark}{\Pi}_A(a) = a, \forall a \in A$ .  
one-to-one  $\overset{\checkmark}{\Pi}_A(a_1) = \overset{\checkmark}{\Pi}_A(a_2) \mid \text{so } A \approx A.$   
 $\Rightarrow a_1 = a_2$

# Theorem 1

(ii) If  $A \approx B$ , there exists a bijective mapping  $f: A \rightarrow B$ . Hence  $f^{-1}: B \rightarrow A$  is also a bijection. Therefore,  $B \approx A$ .

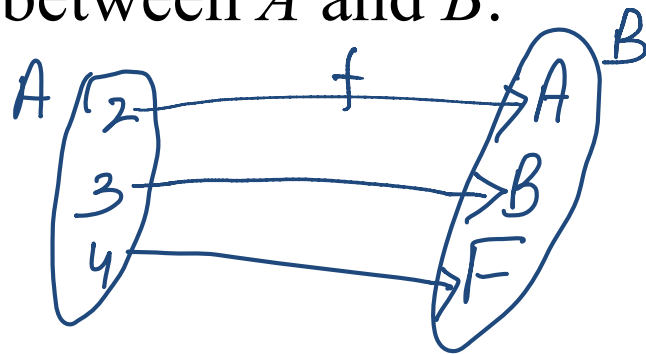
(iii) If  $A \approx B$ ,  $B \approx C$ , then  $f: A \rightarrow B$  and  $g: B \rightarrow C$  are both bijective. Now, the composition  $g \circ f: A \rightarrow C$  is also bijective. Hence  $A \approx C$ .



# Example 1

Let  $A$  and  $B$  be sets with exactly three elements, say,  $A = \{2, 3, 4\}$  and  $B = \{\text{Anum}, \text{Bilal}, \text{Fahad}\}$ .

Then clearly we can find the one-to-one correspondence between  $A$  and  $B$ .

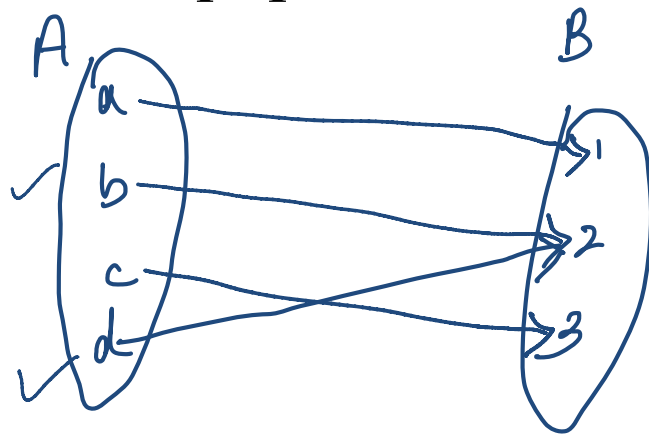


Hence  $A \approx B$   
 $f(2) = \text{Anum}, f(3) = \text{Bilal},$   
 $f(4) = \text{Fahad}$

Remark: The same idea may be used to show that any two finite sets with the same number of elements are equipotent.

## Example 2

Let  $A = \{a, b, c, d\}$  and  $B = \{1, 2, 3\}$ . Then  $A$  and  $B$  are not equipotent.



*This is not one-to-one.*

Remark: In a similar way, we can say that any two finite sets with different number of elements are not equipotent.

# Example 3

$$\begin{aligned} I &= [0, 1] \checkmark & [1, 2] \\ S &= [a, b] \checkmark & \text{and } [3, 5] \\ & & \text{are equipotent} \end{aligned}$$

Let  $I = [0, 1]$ , the closed unit interval, and let  $S$  be any other closed interval, say  $[a, b]$  where  $a < b$ . The function  $f: I \rightarrow S$  defined by

$$f(x) = (b - a)x + a$$

$$\begin{aligned} f(0) &= a \\ f(1) &= (b - a) + a = b \end{aligned}$$

is one-to-one and onto. Thus  $I$  and  $S$  are equipotent.

Remark: Any two closed intervals are equipotent by theorem 1.

$$g(x) = (d - c)x + c$$

Reason: Since  $f: I \rightarrow S$  bijective so  $f: S \rightarrow I$  is also bijective.

Consider another closed interval  $T$ , say  $[c, d]$ . We can define bijective function  $g: I \rightarrow T$  as in the above example. So by transitivity we can define another bijective function from  $S$  to  $T$ . Hence  $S$  and  $T$  are equipotent.

$$f: S \rightarrow I, \quad g: I \rightarrow T$$

$g \circ f: S \rightarrow T$  is also bijective.

$$\begin{aligned} f(x_1) &= f(x_2) \\ (b - a)x_1 + a &= (b - a)x_2 + a \\ \Rightarrow x_1 &= x_2 \end{aligned}$$

## Example 3

Remark: Any two closed intervals are equipotent by theorem 1.

Reason: Since  $f: I \rightarrow S$  bijective so  $f: S \rightarrow I$  is also bijective. Consider another closed interval  $T$ , say  $[c, d]$ . We can define bijective function  $g: I \rightarrow T$  as in the above example. So by transitivity we can define another bijective function from  $S$  to  $T$ . Hence  $S$  and  $T$  are equipotent.



## Example 4

Consider the set  $P = \{1, 2, 3, \dots\}$  of positive integers and the set  $E = \{2, 4, 6, \dots\}$  of even positive integers. The following defines a one-to-one correspondence between  $P$  and  $E$ :

$$\begin{array}{ccc} P = \{1, 2, 3, \dots\} & & f(1) = 2(1) = 2 \\ & \downarrow \downarrow \downarrow & \\ E = \{2, 4, 6, \dots\} & & f(2) = 2(2) = 4 \end{array}$$

In other words, the function  $f: P \rightarrow E$  defined by  $f(n) = 2n$  is one-to-one and onto. Thus  $P$  and  $E$  have the same cardinality.

Note: What does this example show us?

$$E \subseteq P$$



# Definition

A set  $S$  is infinite if it has the same cardinality as a proper subset of itself. Otherwise  $S$  is finite.

For example, the counting numbers  $\check{P}$ , the natural numbers (nonnegative integers)  $N$ , the integers  $\check{Z}$ , the rational numbers  $Q$ , and the real numbers  $R$ .

$$A = \{1, 2, 3, 4\}$$

$$B = \{1, 2, 3\}$$

$$B \subset A$$





# Denumerable and Countable Sets Part 1



# Denumerable Set

A set  $D$  is said to be denumerable or countably infinite if

$D$  has the same cardinality as  $P = \{1, 2, 3, \dots\}$ .

i.e.  $f: D \rightarrow P$  is bijective.

$\mathbb{E}$  and  $P$   
 $f: P \rightarrow \mathbb{E}$  defined by  $f(n) = 2n$   
is bijective.

## Countable Set

A set is countable if it is finite or denumerable, and a set is nondenumerable if it is not countable.

Note: Thus a set  $S$  is nondenumerable if  $S$  is infinite and  $S$  does not have the same cardinality as  $P$ .



# Example 1

Any infinite sequence

$$S = \{a_1, a_2, a_3, \dots\}$$

of distinct elements is countably infinite. *or denumerable.*

Let  $f: P \rightarrow S$  defined by  $f(n) = a_n$ .  
 Here  $f(1) = a_1, f(2) = a_2, f(3) = a_3, \dots$

Similarly all the following sets are countably infinite.

$$\left\{ 1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}, \dots \right\}, \quad \left\{ 1, -2, 3, -4, \dots, (-1)^{n-1} n, \dots \right\}$$

$\downarrow \quad \downarrow \quad \downarrow \quad \dots \quad \downarrow \quad \dots$   
 $1 \quad 2 \quad 3 \quad \dots \quad n \quad \dots$

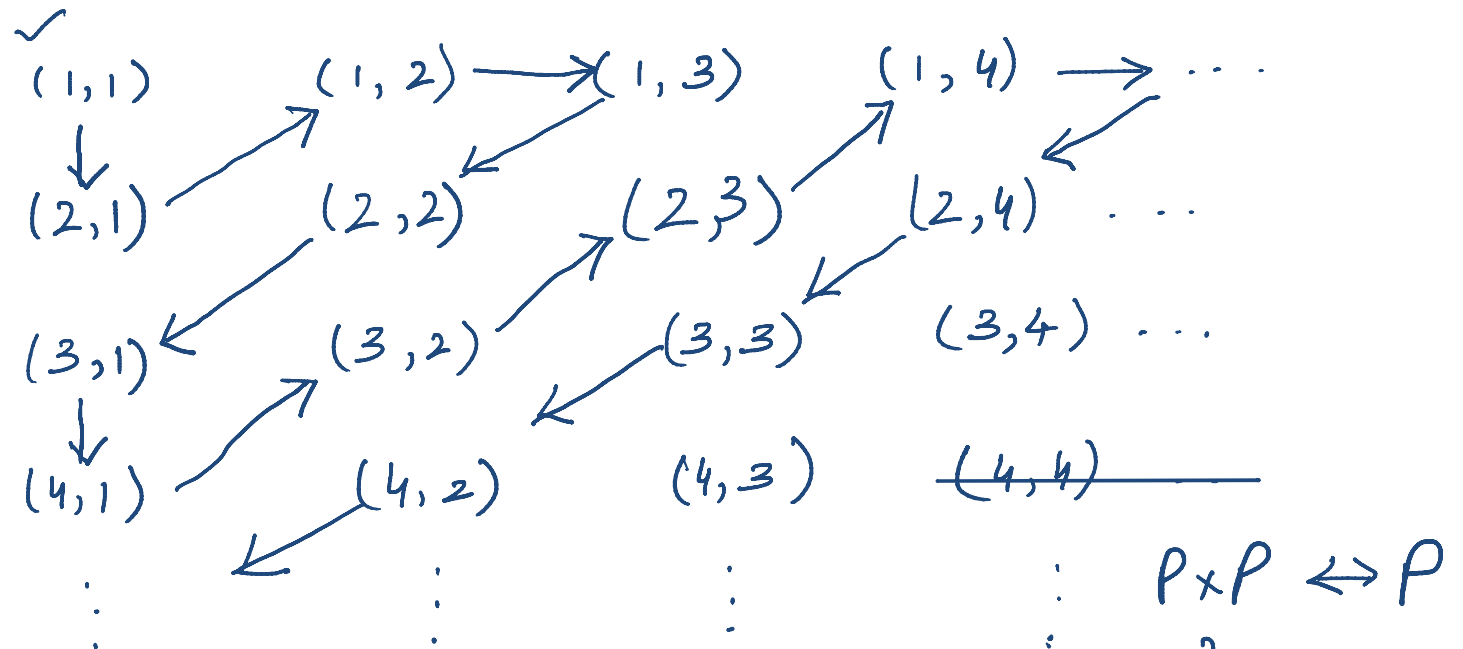
$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \dots \quad \downarrow$   
 $P = \{1 \quad 2 \quad 3 \quad 4 \quad \dots \quad n \quad \dots\}$

$$\left\{ (1, 1), (4, 8), (9, 27), \dots, (n^2, n^3), \dots \right\}$$

$\downarrow \quad \downarrow \quad \downarrow \quad \dots \quad \downarrow$   
 $P = \{1 \quad 2 \quad 3 \quad \dots \quad n \quad \dots\}$

## Example 2

Consider the product set  $\check{P} \times \check{P}$ . The set  $P \times P$  can be written as an infinite sequence as follows:



$$P \times P = \{ (1,1), (2,1), (1,2), (1,3), (2,2), (3,1), \dots \}$$

$$P = \{ 1, 2, 3, 4, 5, 6, \dots \} \checkmark$$

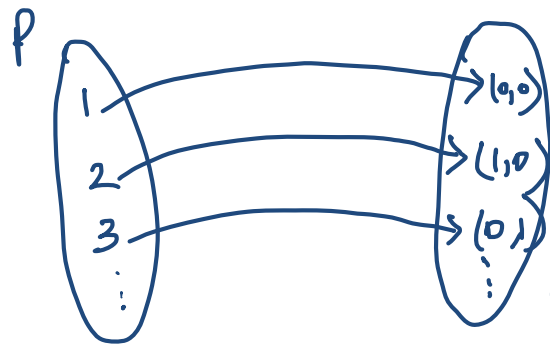
# Example 3

$$P = \{1, 2, \dots\}$$

Recall that  $N = \{0, 1, 2, \dots\}$  is the set of natural numbers or nonnegative numbers. Now each positive integer  $a \in P$  can be written uniquely in the form

$$\checkmark a = 2^r (2s+1), \quad r, s \in N$$

consider the function  $f: P \rightarrow \underline{N \times N}$   
defined by  $f(a) = (r, s)$ .



This  $f$  is one-to-one and onto. Thus  $N \times N$  is denumerable.

$N \times N$  has the same cardinality as  $P$ .

Note:  $P \times P$  is a subset of  $N \times N$ .

$$\begin{aligned} \text{put } r=0, s=0, \quad a &= 2^0(2 \cdot 0 + 1) \\ &= 1(0+1) \\ &= 1 \checkmark \end{aligned}$$

$$\begin{aligned} \text{put } r=1, s=0, \\ a &= 2^1(2 \cdot 0 + 1) = 2 \end{aligned}$$

$$\begin{aligned} \text{put } r=0, s=1, \\ a &= 2^0(2 \cdot 1 + 1) \\ &= 1(3) = 3 \end{aligned}$$

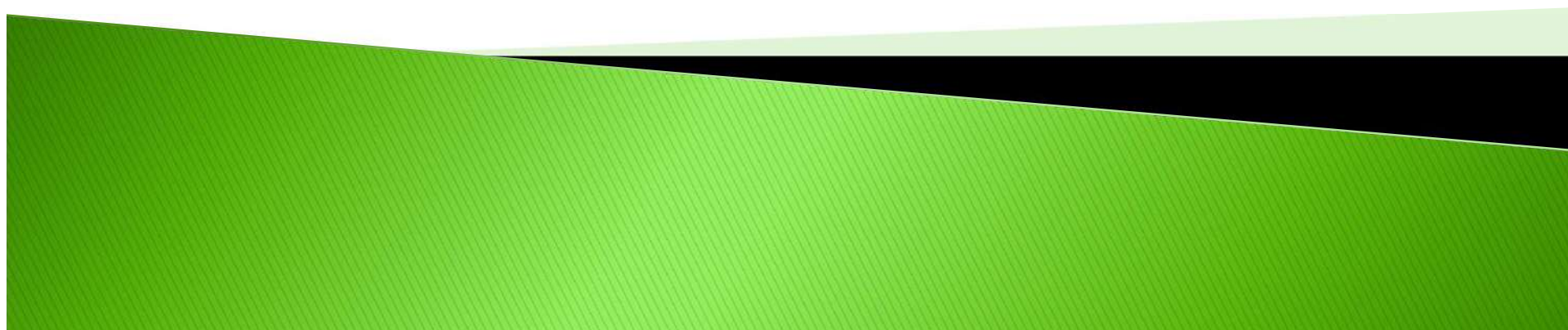
## Example 4

The set  $Z$  of integers can be put into a one-to-one correspondence with  $P = \{1, 2, 3, \dots\}$  as follows:

The formula for the function  $f: P \rightarrow Z$  is given by:



# Denumerable and Countable Sets Part 2



# Theorem 1

Every infinite set contains a subset which is denumerable.

Proof. Let  $A$  be an infinite set. Suppose  $f: P(A) \rightarrow A$ . Consider the following sequence.

$$\checkmark a_1 = f(A)$$

$$\checkmark a_2 = f(A \setminus \{a_1\})$$

$$\checkmark a_3 = f(A \setminus \{a_1, a_2\})$$

$$\vdots$$
$$\checkmark a_n = f(A \setminus \{a_1, a_2, \dots, a_{n-1}\})$$
$$\vdots$$

Therefore,  
 $D = \{a_1, a_2, \dots\}$

Here,  
 $D \subseteq A$

Also  $D$  is  
denumerable.

Since  $A$  is infinite,  $A \setminus \{a_1, \dots, a_{n-1}\}$  is not empty for every  $n \in \mathbb{P}$ . Furthermore  $a_n \neq a_i$  for  $i < n$ .



## Theorem 2

$P$  is denumerable  
and  $E$  is a subset of  $P$ .  
Also  $E \approx P$ , means?

A subset of a denumerable set is finite or denumerable.

Proof: Let  $A = \{a_1, a_2, \dots\}$  is a denumerable set.

Let  $B \subseteq A$ . If  $B = \emptyset$ , then  $B$  is finite.

Suppose  $B \neq \emptyset$ . Let  $b_1 \in B$  and  $b_1$  be the first element in the sequence in  $A$ . Let  $b_2 \in B$  and  $b_2$  be the first element follows  $b_1$  in the sequence  $A$ , so on. Then  $B = \{\cancel{b_1}, \cancel{b_2}, \cancel{b_3}, \dots\}$ .

$B = \{b_1, b_2, b_3, \dots\}$ . If the sequence  $b_1, b_2, \dots$  ends, then  $B$  is finite. Otherwise  $B$  is denumerable.

# Corollary

A subset of a countable set is countable.

Proof. Proof is obvious from theorem 2.



# Theorem 3

$$T = \bigcup D_j = \{ \check{a}_{11}, \check{a}_{12}, \check{a}_{21}, \check{a}_{13}, \check{a}_{22}, \check{a}_{31}, \dots \}$$

Let  $A_1, A_2, A_3, \dots$  be a sequence of pairwise disjoint denumerable sets. Then the union

$$A_1 \cup A_2 \cup A_3 \cup \dots = \bigcup (A_i : i \in P)$$

is denumerable.

Proof: Suppose  $A_1 = \{a_{11}, a_{12}, a_{13}, \dots\}$ ,  $A_2 = \{a_{21}, a_{22}, a_{23}, \dots\}$

$$A_3 = \{a_{31}, a_{32}, a_{33}, \dots\}, \dots$$

$$\text{Then } S = A_1 \cup A_2 \cup A_3 \cup \dots = \{ \check{a}_{11}, \check{a}_{12}, \check{a}_{13}, \dots, \check{a}_{21}, \check{a}_{22}, \check{a}_{23}, \dots, \check{a}_{31}, \check{a}_{32}, \check{a}_{33}, \dots \}$$

Define  $D_n = \{ a_{ij} : i+j=n, n > 1 \}$ . For example,  
 $i=1, j=1, n=2, D_2 = \{a_{11}\}$ ,  $D_3 = \{a_{12}, a_{21}\}$ ,  $D_4 = \{a_{13}, a_{22}, a_{31}\}, \dots$

Note that each  $D_n$  is finite. Let  $T = \bigcup \{D_j : j > 1\}$   
~~is~~ Here  $T$  is countable. Also  $T = A_1 \cup A_2 \cup A_3 \dots$

## Theorem 4

$$f(2/3) = (2, 3)$$

The set  $Q$  of rational numbers is denumerable.

Proof. Note that  $Q = \check{Q}^+ \cup \{0\} \cup \check{Q}^-$ . Let  $f: Q^+ \rightarrow P \times P$  defined by  $f(p/q) = (p, q)$

where  $p/q \in Q^+$  expressed as the ratio of two relatively prime positive integers. Then  $f$  is one-to-one correspondence. Hence  $|Q^+| \approx P \times P$ . As we know  $|P \times P| \approx P$ . So  $Q^+ \approx P$ . Similarly,  $Q^-$  is denumerable. The set  $Q$  of rational numbers, the union of  $Q^+$ ,  $\{0\}$ , and  $Q^-$  is also denumerable.

# Theorem 5

The set  $\mathbb{Z}$  of integers is denumerable.

Proof: Let  $f: \mathbb{P} \rightarrow \mathbb{Z}$  defined by

$$f(n) = \begin{cases} -\frac{n}{2} + \frac{1}{2} & \text{if } n \text{ is odd} \\ \frac{n}{2} & \text{if } n \text{ is even.} \end{cases}$$

For example,

$$f(1) = -\frac{1}{2} + \frac{1}{2} = 0$$

$$f(2) = \frac{2}{2} = 1$$

$$f(3) = -\frac{3}{2} + \frac{1}{2} = -\frac{3-1}{2} = -1$$

$$f(4) = \frac{4}{2} = 2$$

$\vdots$

$$\begin{array}{cccccc} \mathbb{P} = \{ & 1 & 2 & 3 & 4 & 5 \dots \} \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \mathbb{Z} = \{ & 0 & 1 & -1 & 2 & -2 \dots \} \end{array}$$

Here  $f$  is one-to-one.  
and  $f$  is onto. So  $f$  is  
bijective. Hence  $\mathbb{Z}$  is denumerable.

# Ordering of Cardinal Numbers

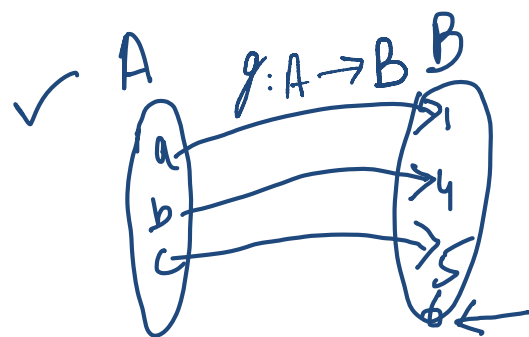


A

# Definition

Let  $A$  and  $B$  be two sets. We say that  $|\overset{\checkmark}{A}| \leq |\overset{\checkmark}{B}|$  if there exists a one-to-one (injective) function  $f: A \rightarrow B$ .

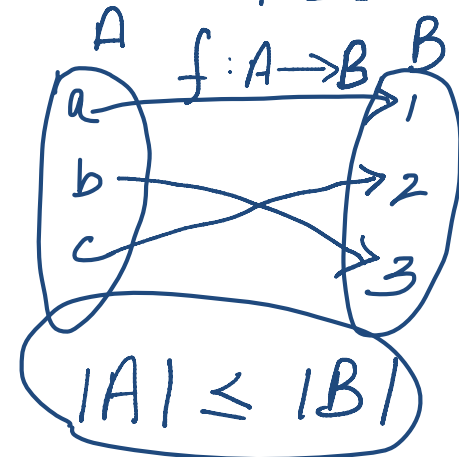
The above relation between cardinal numbers are well defined, that is, the relations are independent of the particular sets involved. Namely, if  $A \approx A'$  and  $B \approx B'$ ,



$$|A| < |B|$$

Here  $g$  is one-to-one.  
but  $g$  is not onto.

$$|A| \leq |B| \not\leftrightarrow |A'| \leq |B'| \quad |A| \equiv |B|$$



### Example 1

Let ~~A~~<sup>B</sup> be a proper subset of a finite set ~~B~~<sup>A</sup>.

For example,  $A = \{1, 2, 3, 4\}$ , then  $B = \{1, 2\}$

Here  $|B| < |A|$ .

### Example 2

Let  $n$  be a finite cardinal. Let  $A$  be a finite subset of  $P = \{1, 2, 3, \dots\}$ . Then  $|A| \neq |P|$ . Thus  $|A| < |P|$ .

We may write

$$0 < 1 < 2 < \dots < \underbrace{N_0}_{\text{circled}}$$

$$\underline{n < N_0}$$





### Example 3

Consider the set  $P$  of positive integers and the unit interval  $I$ , that is, consider the sets

$$P = \{1, 2, 3, \dots\} \quad \text{and} \quad \check{I} = [0, 1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$$

The function  $f : P \rightarrow I$  defined by  $f(n) = 1/n$  is one-to-one. (prove it.)

$$\text{Let } f(n_1) = f(n_2)$$

$$\Rightarrow 1/n_1 = 1/n_2$$

$$\Rightarrow n_1 = n_2$$

$$\begin{array}{l|l} \text{proved} & \begin{array}{l} f(1) = 1/1 = 1 \in I \\ f(2) = 1/2 = 0.5 \in I \\ f(3) = 1/3 = 0.333 \dots \in I \\ f(4) = \text{different} \end{array} \end{array}$$



$$|P| = \aleph_0, \quad |I| = c$$

Therefore,  $|P| \leq |I|$ . ✓

On the other hand  $|P| \neq |I|$ . Therefore  $|P| < |I|$ .

Accordingly we may write

$$\Rightarrow \aleph_0 < c.$$

$$0 < 1 < 2 < \dots < \aleph_0 < c.$$



## Example 4

Let  $A$  be any infinite set. So  $A$  contains a subset which is denumerable. Accordingly, for any infinite set  $A$ , we always have

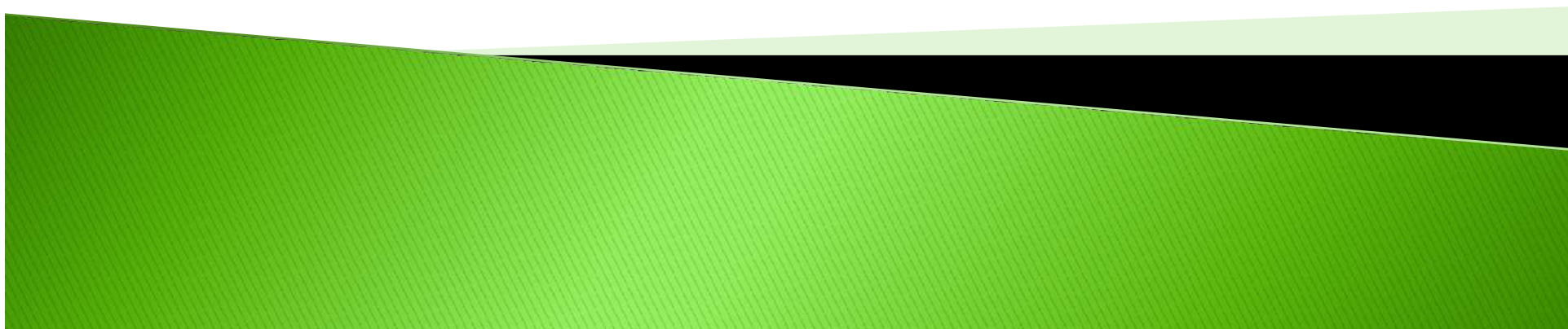
$$\begin{aligned} \underline{\aleph_0} &\leq |A|. \\ \left\{ \begin{array}{l} P = \{1, 2, 3, \dots\} \\ E \subseteq P. \end{array} \right. \\ \downarrow \\ |P| &= |E| \\ \underline{\aleph_0} &= \underline{\aleph_0} \end{aligned}$$

$R =$  infinite set,  
 $P \subseteq R$ .

Here  $P$  is denumerable.

$$\begin{aligned} \cancel{\aleph_0} |P| &\neq |R| \\ \aleph_0 &\not\leq c. \end{aligned}$$

# Cantor's Theorem



# Theorem 1

If  $A$  has 3 elements,  
then  $P(A)$  has 8 elements.  $2^3 = 8$

For any set  $A$ , we have  $|A| < |P(A)|$ .

Proof. Let  $f: A \rightarrow P(A)$  defined  
by  $f(x) = \{x\}$ ,  $\forall x \in A$ .

We need to prove that  $f$  is one-to-one  
but not onto.

$$\text{Let } f(x_1) = f(x_2)$$

$$\Rightarrow \{x_1\} = \{x_2\}$$

$$\Rightarrow x_1 = x_2$$

Hence  $f$  is one-to-one.

$$|P| < |P(P)|$$

$$\aleph_0 < \underline{2^{\aleph_0}}$$

$$|\mathbb{R}| < |P(\mathbb{R})|$$

$$c < \underline{2^c}$$

# Theorem 1

Suppose  $f: A \rightarrow P(A)$  is onto. Now consider the set

$$\underline{B} = \{ \underline{x} \in A : x \notin f(x) \}$$

For example, if  $A = \{1, 2, 3\}$ , then

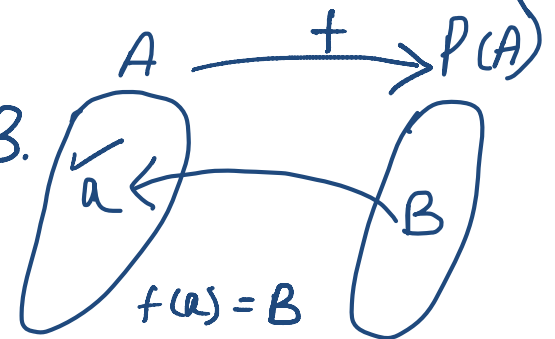
$$1 \rightarrow \emptyset, 2 \rightarrow \{1, 3\}, 3 \rightarrow \underline{\{2\}}$$

clearly  $B$  is a subset of  $A$ , so  $\underline{B} \in P(A)$ . Also

since  $f$  is onto, so there exists  $\underline{a} \in A$  such that

$f(a) = B$ . Now we have two

possibilities, either  $a \in B$  or  $a \notin B$ .



# Theorem 1

- 1) If  $a \in B$ , then  $a \in f(a)$ . Then, by the definition of set  $B$ , we have  $a \notin B$ , which is a contradiction.
- 2) If  $a \notin B$ , then  $a \notin f(a)$ . Then  $a \in B$ , which is a contradiction.

Hence, our assumption that  $f$  is onto is wrong.  
Thus  $f$  is not onto. Therefore,

$$|A| < |P(A)|.$$



# Theorem 2

~~Prove that~~  $2^{\aleph_0} = \underline{c}$ .





# Theorem 2

$$2^{\aleph_0} = c$$



# Continuum Hypothesis

There exists no cardinal  
number  $\beta$  such that

$$\aleph_0 < \beta < c.$$

$$\left. \begin{array}{l} \aleph_0, c \\ \neg \aleph_0 < c. \\ \neg \aleph_0 < \frac{\aleph_0}{2} = c. \end{array} \right\} \begin{array}{l} \text{same} \end{array}$$



# Cardinal Arithmetic Part 1



# Cardinal Addition

Addition and multiplication of the counting numbers  $N$  are sometimes treated from the point of view of set theory. The interpretation of  $2+3 = 5$ , for example, is the union of two disjoint sets, one having two elements and the other having three elements, is a set with five elements. This idea leads to a completely general definition of addition of cardinal numbers.



# Cardinal Addition

**Definition:** Let  $\alpha$  and  $\beta$  be cardinal numbers and let  $A$  and  $B$  be disjoint sets with  $\alpha = |A|$  and  $\beta = |B|$ . Then the sum of  $\alpha$  and  $\beta$  is denoted and defined by

$$\alpha + \beta = |(A \cup B)|$$

For example, let  $A = \{1, 2, 3\}$ ,  $B = \{a, b, c\}$ .

Here  $|A| = 3$ ,  $|B| = 3$ . Now,  $A \cup B = \{1, 2, 3, a, b, c\}$ ,  $|A \cup B| = 6$

**Note:**(1) This definition is well-defined.

$$= |A| + |B|$$

Let  $A'$  and  $B'$  with same cardinal numbers.

means  $|A'| = \alpha$ ,  $|B'| = \beta$ . Then  $|A' \cup B'| = |A \cup B|$

(2) If  $A$  and  $B$  are any two sets, then

$A \times \{1\}$  and  $B \times \{2\}$  are disjoint sets.

# Examples

(a) Let  $\underline{m}$  and  $\underline{n}$  be finite cardinal numbers. Then  $m + n$  corresponds to the usual addition in  $N$ .

(b) Let  $n$  be a finite cardinal number.

Let  $A = \{1, 2, 3, \dots, n\}$ . Then  $|A| = n$

$B = \{n+1, n+2, n+3, \dots\}$ . Then  $|B| = \aleph_0$

Here  $B \approx P$

Now,  $A \cup B = \{1, 2, 3, \dots, n, n+1, n+2, \dots\}$ . Then  $|A \cup B| = \underline{\aleph_0}$

But  $|A \cup B| = n + \aleph_0$

$$\Rightarrow \boxed{\aleph_0 = n + \aleph_0}$$

## Examples

c) Let  $C = [0, \frac{1}{2}]$ ,  $D = (\frac{1}{2}, 1]$

Here  $C \approx I$  and  $D \approx I = [0, 1]$ .

So,  $|C| = c$ ,  $|D| = c$ .

Now,  $C \cup D = [0, \frac{1}{2}] \cup (\frac{1}{2}, 1] = [0, 1]$

$$\Rightarrow |C \cup D| = c.$$

Thus,  $\boxed{|C + C| = c}$

d) Let  $E = \{2, 4, 6, \dots\}$  and  $F = \{1, 3, 5, \dots\}$

$$\Rightarrow |E| = \aleph_0 \text{ and } |F| = \aleph_0$$

Now,  $E \cup F = \{1, 2, 3, 4, 5, 6, \dots\} = \mathbb{P}$

$$|E \cup F| = \underline{\aleph_0}$$

$$\boxed{\aleph_0 + \aleph_0 = \aleph_0}$$

# Cardinal Arithmetic Part 2





# Cardinal Multiplication

Let  $\alpha$  and  $\beta$  be cardinal numbers and let  $A$  and  $B$  be sets with  $\alpha = |A|$  and  $\beta = |B|$ . Then the product  $\alpha$  and  $\beta$  is denoted and defined by

$$\underline{\alpha\beta} = \underline{|A \times B|} \checkmark$$

For example, let  $A = \{2, 3, 4\}$ ,  $B = \{4, 5\}$ .

Here  $|A| = 3$  and  $|B| = 2$ .

Now,  $A \times B = \{(2, 4), (2, 5), (3, 4), (3, 5), (4, 4), (4, 5)\}$

$$\therefore \underline{|A \times B|} = 6 = 2 \times 3 = |A| \times |B| = \alpha\beta$$



# Examples

(a) Let  $m$  and  $n$  be finite cardinal numbers. Then  $mn$  corresponds to the usual multiplication in  $N$ .

(b) Since  $N \times N$  is denumerable, so  $|N \times N| = \aleph_0$   
 $N \times N \approx P$  or  $|N \times N| = |P| \Rightarrow \boxed{\aleph_0 \times \aleph_0 = \aleph_0}$  ✓

(c) The Cartesian plane  $R^2 = R \times R$  has the same cardinality as  $R$ . That is,  $\mathfrak{c} \mathfrak{c} = \mathfrak{c}$ .

$$|R \times R| = R$$

$$\mathfrak{c} \mathfrak{c} = \mathfrak{c}$$



# Theorem 1

Let  $\alpha$  and  $\beta$  be nonzero cardinal numbers such that  $\beta$  is infinite and  $\alpha \leq \beta$ . Then

$$\underline{\alpha + \beta} = \alpha \underline{\beta} = \underline{\beta}$$

We know that  $\aleph_0 < c$ .

It means,  $\aleph_0 + c = c$ .

and  $\aleph_0 c = c$



# Ordered Sets



# Definition

Suppose  $R$  is a relation on a set  $S$  satisfying the following three properties:

- 1) (Reflexive) For any  $a \in S$ , we have  $a R a$ .
- 2) (Antisymmetric) If  $a R b$  and  $b R a$ , then  $a = b$ .
- 3) (Transitive) If  $a R b$  and  $b R c$ , then  $a R c$ .

Then  $R$  is called a partial order or, simply an order relation, and  $R$  is said to define a partial ordering of  $S$ . The set  $S$  with partial ordering  $R$  is called a partially ordered set or, simply an ordered set. *Poset*



## Notation

1)  $\forall a \in P$ , then  $a \leq a$ .

2)  $\nexists a \leq b$  and  $b \leq a$ , then  $a = b$ .

3)  $\nexists a \leq b$  and  $b \leq c$ , then  $a \leq c$ .

The most familiar order relation, called the usual order, is the relation  $\leq$  on the positive integers  $P$  or, more generally on any subset of the real numbers  $R$ . For this reason, a partial ordering relation is frequently denoted by  $\leq = R$

With this notation, the above three properties of a partial order appear in the following usual form:

- 1) (Reflexive) For any  $a \in S$ , we have  $a \leq a$  or  $a R a$ .
- 2) (Antisymmetric)  $\nexists a \leq b$  and  $b \leq a$ , then  $a = b$ .
- 3) (Transitive)  $\nexists a \leq b$  and  $b \leq c$ , then  $a \leq c$ .

# Notation

Although an ordered set consists of two things, a set  $S$  and the partial ordering  $R$ , one usually simply write  $S$  to denote the ordered sets as long as the partial ordering is fixed in the context of the discussion; otherwise the ordered set is denoted by the pair  $(S, \leq)$

Suppose  $S$  is an ordered set. Then the statement  $a \leq b$  is read "a precedes b".

In this context we also write:

$a < b$  means  $a \leq b$  and  $a \neq b$ . (a strictly precedes b)  
 $b > a$  means  $b \leq a$  and  $b \neq a$ . (b strictly succeeds a)  
 $b > a$  means  $b < a$  and  $a \neq b$ . (b strictly succeeds a)

$$3) \text{ If } A \subseteq B, B \subseteq C, \text{ then } A \subseteq C.$$

## Example 1

- 1) Let  $C$  be any collection of sets. The relation of set  $\subseteq$  inclusion is a partial ordering of  $C$ . Specifically,

$$1) \text{ For any } A \in C, A \subseteq A \text{ or } A R A.$$

$$2) \text{ For any } A, B \in C, \text{ we have } A \subseteq B \text{ or } B \subseteq A \text{ or } A = B \text{ and } B \subseteq A, \text{ then } A = B.$$

- 2) Consider the set  $P$  of positive integers. We say " $a$  divides  $b$ ", written  $a|b$ , if there exists an integer  $c$  such that  $ac = b$ . For example,  $2|4$ ,  $3|12$ ,  $7|21$ , and so on. This relation of divisibility is a partial ordering of  $P$ .

$$1) \text{ If } a \in P, a|a \text{ or } a R a.$$

$$2) \text{ If } a|b \text{ and } b|a, \text{ then } a = b.$$

$$3) \text{ If } a|b, b|c, \text{ then } a|c. \quad \begin{array}{l} 3|12, 12|24 \\ \Rightarrow 3|24. \end{array}$$



# Example 1

- 3) The relation “ $|$ ” of divisibility is not an ordering of the set  $Z$  of integers. Specifically, the relation is not antisymmetric. For instance,

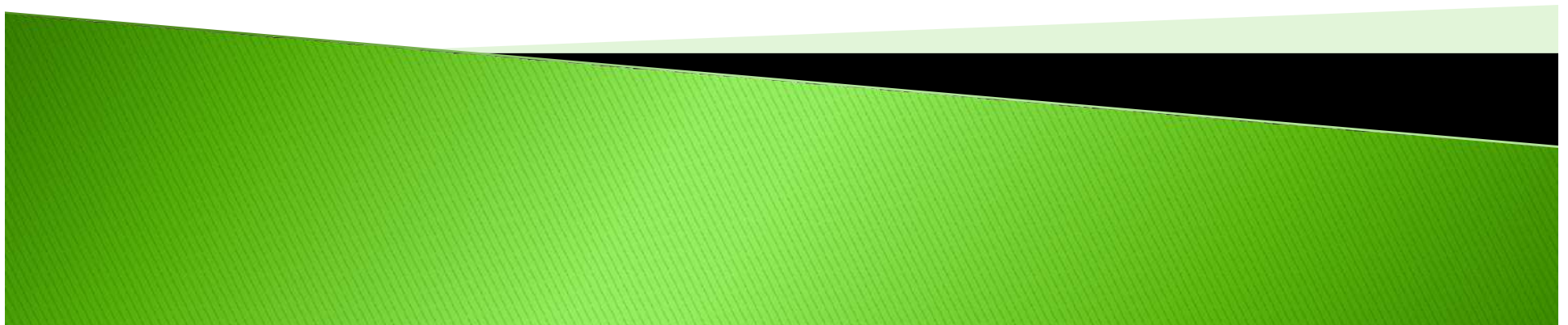
For example,  $\overset{a}{2} | \overset{b}{-2}$  and  $-2 | 2$   
but  $2 \neq -2$ .



# Example 1



# Comparability and Linearly Ordered Sets



# Comparability

Suppose  $a$  and  $b$  are distinct elements in a partially ordered set  $S$ . We say  $a$  and  $b$  are comparable if

$$a \leq b \text{ or } b < a.$$

Thus  $a$  and  $b$  are noncomparable written

$$\text{if } a \not\leq b \text{ or } \frac{a \not\geq b}{b \not\leq a}.$$



# Linearly Ordered Sets and Chain

Suppose that every pair of elements of  $S$  are comparable.

Then  $S$  is said to be linearly or totally ordered.

Although an ordered set  $S$  may not be linearly ordered, it is still possible for a subset  $A$  of  $S$  to be linearly ordered. Such a linearly ordered subset  $A$  of an ordered set  $S$  is called a chain in  $S$ .



# Example 1

- a) Consider the set  $P$  of positive integers ordered by divisibility. Then 21 and 7 are comparable since  $7|21$ . Here 3 and 5 are non comparable because neither  $3|5$  nor  $5|3$ . Thus  $P$  is not linearly ordered by divisibility. Observe that  $A = \{2, 6, 12, 36\}$  is a chain.
- b) The set  $P$  of positive integers with the usual order  $\leq$  is linearly ordered and hence every ordered subset of  $P$  is also linearly ordered.  $P = \{1, 2, 3, \dots\}$ , Now  $B = \{2, 5, 7\}$



# Example 1

- c) The power set  $P(A)$  of a set  $A$  with 2 or more elements is not linearly ordered by set inclusion. For example,  $a, b \in A$ , then  $\{a\}$  and  $\{b\}$  are non comparable. Let  $B \subseteq P(A)$  such that  $B = \{\emptyset, \{a\}, A\}$ . Here  $\emptyset < \{a\} < A$  or  $\emptyset = \{a\} = A$  so set  $B$  is a chain.
- d) Consider the set  $A = \{1, 2, \underline{3}, \underline{4}, 6, 12, 24\}$  ordered by divisibility. Then clearly  $A$  is not linearly ordered as for instance, 3 and 4 are not comparable. Observe that the sets  $\{1, 2, \underline{4}, 12, 24\}$ ,  $\{1, 2, 6, 12, 24\}$  and  $\{1, 3, 6, 12, 24\}$  are all chains.



## Example 2

Let  $\underline{P} = \{1, 2, 3, \dots\}$  be ordered by divisibility. State whether each of the following is a chain in  $P$ .

- a)  $A = \{24, 2, 6\}$ , it is a chain.  
Here  $2 < 6 < 24$  or  $2 | 6 | 24$
- b)  $B = \{3, 15, 5\}$ , so it is not a chain.  
Here  $3 \nmid 5$
- c)  $C = \{2, 8, 32, 4\}$ , it is a chain.  
 $2 < 4 < 8 < 32$
- d)  $D = \{7\}$ , it is a chain.





# Partially Ordered Sets and Hasse Diagrams



# Immediate Predecessor and Immediate Successor

Let  $S$  be a partially ordered set, and suppose  $a, b \in S$ . We say that  $a$  is an immediate predecessor of  $b$ , or that  $b$  is an immediate successor of  $a$ , or that  $b$  is a cover of  $a$ , written  $a \lessdot b$ , if  $a < b$  but no element in  $S$  lies between  $a$  and  $b$ , that is, there exists no element  $c$  in  $S$  such that  $a < c < b$ .✕

For example, consider the set  $P = \{1, 2, \underline{3}, 4, \dots\}$  with the order  $<$ . Then we can see that  $\underline{1 \lessdot 2}$ ,  $2 \lessdot 3$ , and so on.



# Immediate Predecessor and Immediate Successor

Suppose  $S$  is a finite partially ordered set. Then the order on  $S$  is completely known once we know all pairs  $a, b$  in  $S$  such that  $a << b$ . This follows from the fact that  $x < y$  if and only if  $x << y$  or there exists elements

$$x << a_1 << a_2 << \dots << a_m << y$$

For example, consider the set  $A = \{1, 2, 3, 4, 6, 12, 24\}$  ordered by the relation “ $x$  divides  $y$ ”. Then we can write

$$\underline{2 << 4}, \underline{2 << 6}, 3 << 6, 4 << 12, 6 << 12, 12 << 24.$$

Also  $1 << 2 << \check{4} << \check{12} << \check{24}$  or  $1 << 2 << 6 << 12 << 24$  or  $1 << 3 << 6 << 12 << 24$ .

$$2 \not<< 3 \not<< 4$$

# Hasse Diagrams



The Hasse diagram of a finite partially ordered set  $S$  is a graphical representation of  $S$  as follows. The elements of  $S$  are represented by points in the plane and there is a directed line segment (arrow) drawn from  $a$  to  $b$  whenever  $a << b$  in  $S$ . Instead of drawing an arrow from  $a$  to  $b$ , we sometimes place  $b$  higher than  $a$  and draw a line between them.

The Hasse diagram of an ordered set  $S$  is a picture of  $S$ . Sometimes we define a partially ordered set by simply presenting its Hasse diagram.

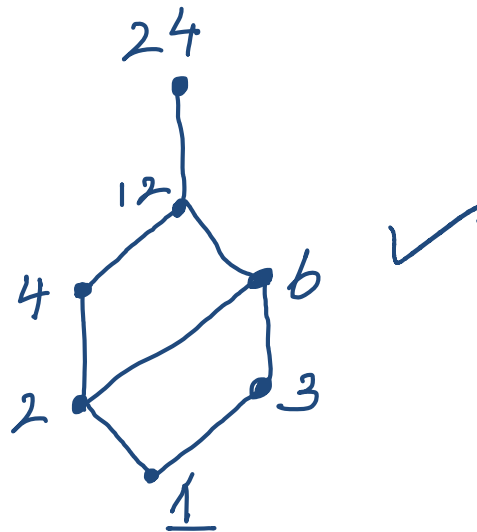


# Example 1

Draw the Hasse diagram representing the divisibility relation on set  $A = \{1, 2, 3, 4, 6, 12, 24\}$ . ✓

Solution. As we saw ✓  $1 \ll 2 \ll 4 \ll 12 \ll 24$  or  $1 \ll \cancel{2} \ll 6 \ll 12 \ll 24$  or  $1 \ll 3 \ll 6 \ll 12 \ll 24$ . We can draw its Hasse diagram as follows:

Here  $1 \ll 24$



## Example 2

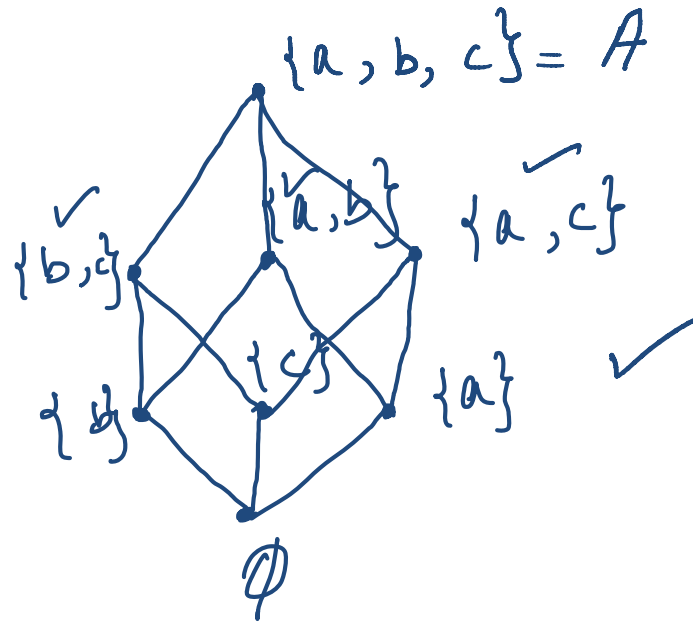
Let  $A = \{a, b, c\}$ . Draw the Hasse diagram representing the subset relation  $\subseteq$  on the power set  $P(A)$ .

- ▶ Solution. The power set  $P(A)$  contains all subsets of  $A$ :
- ▶  $P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$ .  $2^3 = 8$
- ▶ We place the empty set  $\emptyset$  at the bottom of the diagram. The subsets with one element  $\{a\}, \{b\}, \{c\}$  are placed on the first level, and the subsets with two elements  $\{a, b\}, \{b, c\}, \{a, c\}$  are placed on the next level. The element  $\{a, b, c\}$  occupies the top of the diagram. Finally we connect the subsets with their immediate successor with respect to the inclusion relation. The resulting diagram is shown in the next slide.



## Example 2

Here  $\{b\} \leq \{b, c\}$  because  $\{b\} \subseteq \{b, c\}$   
 $\{b\} < \{a, b\}$ ,  $\{c\} < \{b, c\}$ ,  $\{c\} < \{a, c\}$   
 $\{a\} < \{a, b\}$ ,  $\{a\} < \{a, c\}$



## Example 3

Let  $A = \{1, 2, 3, 4, 5\}$  and  $R = \{(1, 1), (1, 3), (1, 4), (1, 5), (2, 2), (2, 3), (2, 4), (2, 5), (3, 3), (3, 4), (3, 5), (4, 4), (5, 5)\}$ . Show that the relation  $R$  is a partial order and draw its Hasse diagram.

Solution.

- ▶ The relation  $R$  is reflexive since it contains all reflexive pairs:  $(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)$ . ✓
- ▶  $R$  is antisymmetric since all non-reflexive elements do not have the corresponding inverse pairs:  
 $(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5)$ .





## Example 3

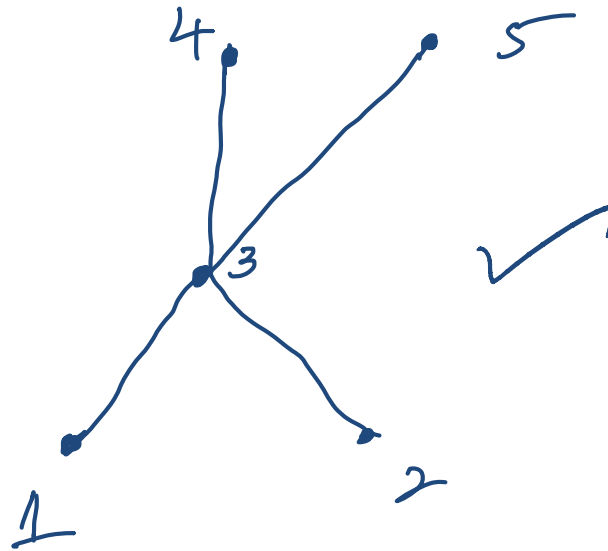
- ▶  $R$  is transitive:
- ▶  $(1,3) \in R, (3,4) \in R \rightarrow (1,4) \in R;$
- ▶  $(1,3) \in R, (3,5) \in R \rightarrow (1,5) \in R; \checkmark$
- ▶  $(2,3) \in R, (3,4) \in R \rightarrow (2,4) \in R; \checkmark$
- ▶  $(2,3) \in R, (3,5) \in R \rightarrow (2,5) \in R. \checkmark$

Hence, the relation  $R$  is a partial order and we can draw its Hasse diagram, which is represented below.



### Example 3

$$R = \{(1,3), (1,4), (1,5), (2,\overset{\checkmark}{3}), (2,4), \\ (\underline{2},\underline{5}), (\underline{3},\underline{4}), (3,5)\}$$



# Minimal and Maximal Elements



# Minimal Element

Let  $S$  be a partially ordered set. An element  $a \in S$  is called a minimal element of  $S$  if no element of  $S$  strictly precedes (is less than)  $a$ ; that is, if

$$x \leq a \text{ implies } x = a$$

For example, let  $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$  be ordered by divisibility. Then we can see that  $A$  has only one minimal element, 1.

# Maximal Element

Let  $S$  be a partially ordered set. An element  $b \in S$  is called a maximal element of  $S$  if no element of  $S$  strictly succeeds (is greater than)  $b$ ; that is, if

$$x \geq b \text{ implies } x = b$$

For example, let  $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$  be a set ordered by divisibility. Then we can see that  $A$  has two maximal elements, 18 and 24.

# Geometrical Meaning

Geometrically speaking,  $a$  is a minimal element of  $S$  if no edge enters  $a$  (from below), and  $b$  is a maximal element of  $S$  if no edge leaves  $b$  (in an upward direction).

**Note:**  $S$  can have more than one minimal and more than one maximal element. Hasse diagram of divisibility relation on set  $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$  is given below:

# Minimal and Maximal Element of an Infinite and Finite Set

If  $S$  is infinite, then  $S$  may have no minimal and maximal element. For instance, the set  $Z$  of integers with the usual order  $\leq$  has no minimal and maximal element. On the other hand, if  $S$  is finite, then  $S$  has at least one minimal and one maximal element.

# First and Last Element

An element  $a \in S$  is called a first element of  $S$  if  $a \leq x$  for every  $x \in S$ , that is, if  $a$  precedes every other element in  $S$ .

Similarly, an element  $b \in S$  is called a last element of  $S$  if  $y \leq b$  for every  $y \in S$ , that is,  $b$  succeeds every other element in  $S$ .

For example, let  $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$  be a set ordered by divisibility. 1 is minimal element of  $A$  which is also the first element of  $A$ . Set  $A$  has two maximal element and neither is a last element.





# First and Last Element

**Note:** We note that  $S$  can have at most one first element which must be a minimal element of  $S$ , and  $S$  can have at most one last element which must be a maximal element of  $S$ . Generally speaking,  $S$  may have neither a first nor a last element, even when  $S$  is finite.

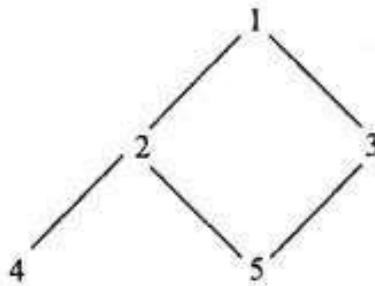


# Examples

- a) Consider the set  $P = \{1, 2, 3, \dots\}$  with the usual order  $\leq$ .
- b) Let  $A$  be any nonempty set and let  $P(A)$  be the power set of  $A$  ordered by set inclusion.

# Examples

- c) Consider the ordered set  $A$  in the figure below:



- 1) Find all minimal and maximal elements of  $A$ .
- 2) Does  $A$  have a first element or a last element?

# Supremum and Infimum



# Upper Bound and Supremum

Let  $S$  be a partially ordered set, and let  $A$  be a subset of  $S$ .

An element  $m$  in  $S$  is called an upper bound of  $A$  if  $m$  succeeds every element of  $A$ , that is, for every  $x \in A$ , we have

$$x \leq m$$

If an upper bound of  $A$  precedes every other upper bound of  $A$ , then it is called the supremum of  $A$  and it is denoted by  $\sup(A)$ .



# Lower Bound and Infimum

Let  $S$  be a partially ordered set, and let  $A$  be a subset of  $S$ .

An element  $n$  in  $S$  is called a lower bound of  $A$  if  $n$  precedes every element of  $A$ , that is, for every  $y \in A$ , we have

$$y \geq n$$

If a lower bound of  $A$  succeeds every other lower bound of  $A$ , then it is called the infimum of  $A$  and it is denoted by  $\inf(A)$ .



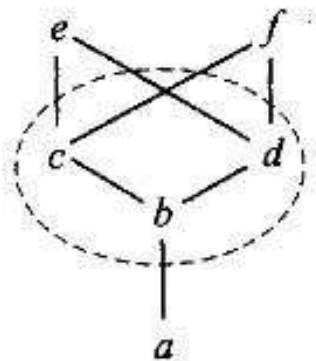
# Bounded Above and Bounded Below

If  $A$  has an upper bound we say  $A$  is bounded above, and if  $A$  has a lower bound we say  $A$  is bounded below. In particular,  $A$  is bounded if  $A$  has an upper and lower bound.



# Example 1

Let  $S = \{a, b, c, d, e, f\}$  be ordered as in the Hasse diagram below and let  $A = \{b, c, d\}$ .





## Example 2

Let  $S = \{1, 2, 3, \dots, 8\}$  be ordered as in the Hasse diagram below and let  $A = \{4, 5, 7\}$ .

## Example 3

Consider the set  $Q$  of rational numbers, and its subset



# Similar Ordered Sets



# Similar Mapping

Suppose  $X$  and  $Y$  are partially ordered sets. A one-to-one(injective) function  $f : X \rightarrow Y$  is called a similar mapping from  $X$  into  $Y$  if  $f$  preserves the order relation, that is, if the following conditions holds for any pair  $a, b \in X$ :

$$a \leq b \text{ in } X \text{ if and only if } f(a) \leq f(b) \text{ in } Y$$

The above condition is equivalent to the following two conditions:



# Similar Ordered Sets

Two ordered sets  $X$  and  $Y$  are said to be order-isomorphic or isomorphic or similar, written

if there exists a one-to-one correspondence  $f : X \rightarrow Y$  which preserves the order relations. Such a function  $f$  is then called an order-isomorphism or isomorphism from  $X$  onto  $Y$ .



# Example 1

Suppose  $S = \{a, b, c, d\}$  is ordered by the diagram below  
and suppose  $T = \{1, 2, 6, 8\}$  is ordered by divisibility.  
Determine whether S

## Example 2

The set of positive integers  $P = \{1, 2, 3, \dots\}$  is order-isomorphic to the set of even positive integers  $E = \{2, 4, 6, \dots\}$  since the function  $f: P \rightarrow E$  defined by  $f(x) = 2x$  is an isomorphism between  $P$  and  $E$ .

## Example 3

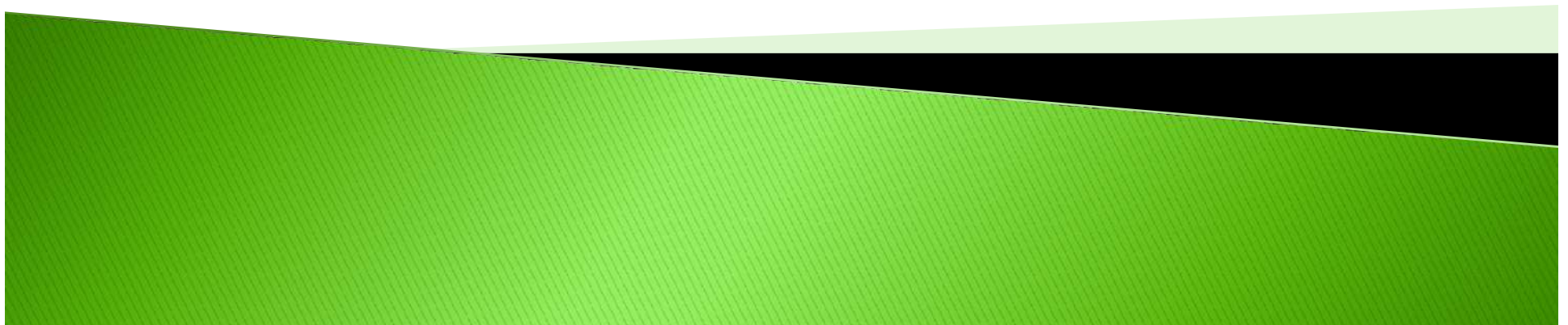
Consider the usual ordering  $\leq$  of the positive integers  $P = \{1, 2, 3, \dots\}$  and the negative integers  $A = \{-1, -2, -3, \dots\}$ . Then  $P$  is not order-isomorphic to  $A$ .

Proof.





# Well Ordered Sets and Initial Segment



# Definition

Let  $A$  be an ordered set. Then  $A$  is said to be well-ordered if every subset of  $A$  contains a first element.

**Note:** Any well-ordered set  $A$  is linearly ordered. ✓

Proof. Let  $A$  be a well ordered set. Also, let  $\underline{a, b} \in A$ , then the subset  $\underline{\{a, b\}}$  of  $A$  has a first, which, therefore, must precede the other. Hence any two elements of  $A$  are comparable.



# Theorem 1

Let  $A$  be a well-ordered set. Then:

- (i) Every subset of  $A$  is well-ordered.
- (ii) If  $\underline{B}$  is similar to  $\underline{A}$ , then  $B$  is well-ordered.



# Example 1

Consider the following two subsets of well-ordered set  $\overline{P}$ :

$$A_1 = \{1, 3, 5, \dots\} \quad \text{and} \quad A_2 = \{2, 4, 6, \dots\}$$

Then  $A_1$  and  $A_2$  are also well-ordered.

Suppose the union

$$S = A_1 \cup A_2 = \{1, 3, 5, \dots; 2, 4, 6, \dots\}$$

is ordered from left to right. Then  $S$  is also well-ordered.



# Initial Segments

Let  $A$  be a well-ordered set. The initial segment  $s(a)$  of an element  $\underline{a} \in A$  consists of all elements in  $A$  which strictly precedes  $a$ . In other words,

$$\underline{s(a)} = \{x : x \in A, x < a\}$$

Consider the well-ordered set  $S$  as in previous example, that is,

$$S = \{1, 3, 5, \dots; \underline{2}, 4, 6, \dots\} \checkmark$$

$$\text{Then } s(1) = \emptyset, s(5) = \{1, 3\},$$

$$s(2) = \{1, 3, 5, \dots\}$$

$$s(8) = \{1, 3, 5, \dots, 2, 4, 6\}$$



## Theorem 2

Let  $\underline{S(A)}$  denote the collection of all initial segments of elements in a well-ordered set  $A$ , and let  $\underline{S(A)}$  be ordered by set inclusion  $\subseteq$ . Then  $A$  is similar to  $\underline{S(A)}$  and, in particular, the function  $\underline{f}: A \rightarrow \underline{S(A)}$  defined by  $\underline{f(x)} = \underline{s(x)}$  is a similarity mapping between  $A$  and  $\underline{S(A)}$ .

Consider the set  $A = \{1, 2, 3\}$  with usual ordering.

Here  $\underline{s(1)} = \underline{\emptyset}$ ,  $\underline{s(2)} = \underline{\{1\}}$ ,  $\underline{s(3)} = \underline{\{1, 2\}}$

Now  $\underline{S(A)} = \{\underline{\emptyset}, \underline{\{1\}}, \underline{\{1, 2\}}\}$  ✓

Let  $\underline{f}: A \rightarrow \underline{S(A)}$  defined by  $\underline{f(x)} = \underline{s(x)}$ .

Means  $\underline{f(1)} = \underline{s(1)} = \underline{\emptyset}$ ,  $\underline{f(2)} = \underline{s(2)} = \underline{\{1\}}$ ,  
 $\underline{f(3)} = \underline{s(3)} = \underline{\{1, 2\}}$ .

## Theorem 2

$$A = \{1, 2, 3\}, \quad \mathcal{S}(A) = \{\emptyset, \{1\}, \{1, 2\}\}$$

Here  $1 < 2 \Rightarrow f(1) < f(2)$

$$\emptyset < \{1\}$$

$$2 < 3 \Rightarrow f(2) < f(3)$$

$$\Rightarrow \{1\} \subseteq \{1, 3\}$$

$$1 < 3 \Rightarrow f(1) < f(3)$$

$$\Rightarrow \emptyset \subseteq \{1, 3\}$$



# Transfinite Induction and Limit Elements





# Principle of Transfinite Induction

Let  $S$  be a subset of a well-ordered set  $A$  with the following two properties:



# Limit Elements

An element  $a$  in a well-ordered set  $A$  is called a limit element if it does not have an immediate predecessor and if it is not the first element.

Consider two finite well-ordered sets:



# Comparison of Well-Ordered Sets

Suppose  $A$  and  $B$  are well-ordered sets, and suppose  $A$  is similar to an initial segment of  $B$ . Then  $A$  is said to be shorter than  $B$ , and  $B$  is said to be longer than  $A$ .



# Comparison of Well-Ordered Sets



# Ordinal Numbers



Consider a collection  $C$  of well-ordered sets. Each well-ordered set  $A$  in  $C$  is assigned a symbol in such a way that any two well-ordered sets  $A$  and  $B$  are assigned the same symbol if and only if  $A$  and  $B$  are similar. This symbol is called the ordinal number of  $A$ . We will write

$$\lambda = \text{ord}(A)$$

to indicate that  $\lambda$  is the ordinal number of  $A$ .



# Finite Ordinal Numbers

The ordinal number of each of the well-ordered sets

$$\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}, \dots$$

is denoted by 0, 1, 2, 3, ... respectively, and is called a finite ordinal numbers. All other ordinals are called transfinite numbers.

**Note:** Since any two finite well-ordered sets with the same number of elements are similar, 0, 1, 2, 3, ... are the only finite ordinal numbers.



# Ordinal Number of $P$

The ordinal number of the set  $P$  of counting numbers is denoted by  $\omega$ .



# Inequalities and Ordinal Numbers

Let  $\lambda$  and  $\mu$  be ordinal numbers and let  $A$  and  $B$  be two well-ordered sets such that  $\lambda = \text{ord}(A)$  and  $\mu = \text{ord}(B)$ .  
Then

$$\lambda < \mu$$

if  $A$  is similar to an initial segment of  $B$ . Accordingly,

# Examples



# Choice Function and Axiom of Choice



# Choice Function

Let  $C$  be a non-empty set of non-empty sets. A function  $f: \underline{C} \rightarrow \underline{\cup C}$  is called a choice function for  $C$  if  $\underline{f(A)} \in \underline{A}$  for all  $\underline{A} \in C$ .



# Example 1

Let  $C$  be the set of countries on earth, thinking of each country as a collection of cities. Then  $\bigcup C$  is the set of all cities on earth, and the function  $f$  that assigns to each country its capital city is an example of a choice function for  $C$ .

$$f : \underline{C} \rightarrow \bigcup C$$

For example,

let  $\underline{A} \in C$  denotes Pakistan, then  $f(\underline{A}) = \text{Islamabad} \in A$ .

$A = \text{Pakistan}$

Here  $f(A) \in A$



## Example 2

$$f : \mathcal{C} \rightarrow \cup \mathcal{C}$$

Let  $\mathcal{C}$  be the collection of all pairs of shoes in the world.

Then the function that picks the left shoe out of each

pair is a choice function for  $\mathcal{C}$ . *Let  $A = \text{pair of shoes}$*

$$f(A) = \text{left shoe} \in A$$

**Example 3**  $\mathcal{N} = \{1, 2, 3, \dots\}$

Let  $\mathcal{C} = P(\mathcal{N}) \setminus \{\emptyset\}$ . The function  $f(A) = \min(A)$  is a choice function on  $\mathcal{C}$ .

$$A = \{1, 2, 3\}$$

$$\text{then } f(A) = 1 \in A$$

$$\text{so } f(A) \in A$$



Notice that in these examples, and in most other examples the reader might think of, the choice function  $f$  is defined by some rule: “choose the left shoe”, “choose the least element”, “choose the capital city”, and so on. In all of these we simply define the choice function.

What the axiom of choice does is guarantee that there always exist choice functions, even in the absence of such a rule for defining one easily.



# Axiom of Choice

Let  $C$  be a non-empty set of non-empty sets. There exists a choice function for  $C$ .

The statement seems simple, but this is a subtle idea. To a non-mathematician, we might summarize the statement as, “If you have a bunch of choices, each of which is possible to make, then you can make all of them.”





# Well Ordering Theorem



Recall that the set of positive numbers with the order  $\leq$  is well-ordered. In general, a set with some order is called well-ordered if any nonempty subset has a least element. The set of even numbers and the set  $\{1, 5, 17, 12\}$  with usual order on numbers are two examples of well-ordered sets and you can check this. However, the set of integers with our usual ordering on it is not well-ordered, neither is the set of rational numbers, nor the set of all positive rational numbers.

Whether a set is well-ordered or not depends on how you define the order on the set.



# Well Ordering Theorem

Every set can be well-ordered.

Although  $\mathbb{Z}$  with our usual  $\leq$  is not well-ordered, we can define another kind of order on it which does make it well-ordered. Let's call this order  $\lessdot$  instead  $<$ . We define it as follows:

$\lessdot a < b$  whenever  $|a| < |b|$  or if  $|a| = |b|$  and  $a$  is negative and  $b$  is a positive number. As an example, we have :

$$|-9| < |-20| \text{ so } -9 < -20, \quad |-2| = |2| \text{ so } -2 < 2$$

$$|0| < |5| \text{ so } 0 < 5$$

$$|-1| < |-5| \text{ so } -1 < -5$$

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

# Zorn's Lemma

Let  $X$  be a nonempty partially ordered set in which every chain (linearly ordered subset) has an upper bound in  $X$ . Then  $X$  contains at least one maximal element.

Consider the partially ordered set  $\overline{X} = \{1, 2, 3, 4, 6, 12, 24\}$  ordered by divisibility. It has three chains  $\{1, 2, 4, 12, 24\}$ ,  $\{1, 2, 6, 12, 24\}$  and  $\{1, 3, 6, 12, 24\}$ . All chains has an upper bound 24. Also maximal element of  $X$  is 24.



# Theorem

The following are equivalent:

- 1) Axiom of choice;
- 2) Well ordering theorem;
- 3) Zorn's lemma.

↖

↖



# Propositions and Compound Propositions



# Propositions

A proposition is a declarative sentence which is true or false, but not both. Consider, for example, the following eight sentences:

- (i) Paris is in France.
- (ii)  $1+1=2$
- (iii)  $2+2=3$
- (iv) Islamabad is in Sri lanka.
- (v)  $9 < 6$
- (vi)  $x = 2$  is a solution of  $x^2 = 4$ .
- (vii) Where are you going?
- (viii) Do your homework.



# Notation

We use letters to denote propositional variables, that is, variables that represent propositions, just as letters are used to denote numerical variables. The conventional letters used for propositional variables are  $p, q, r, s, \dots$

The **truth value** of proposition is true, denoted by T, if it is a true proposition, and the truth value of a proposition is false, denoted by F, if it is a false proposition.





# Compound Proposition

Many mathematical statements are constructed by combining one or more propositions. New propositions, called compound propositions, are formed from existing propositions using logical operators.

Example:

- 1) “Roses are red and violets are blue” is a compound proposition.
- 2) John is intelligent or studies every night.



# Basic Logical Operations



# Conjunction $p \wedge q$

Any two propositions can be combined by the word “and” to form a compound proposition called the conjunction of the original propositions. Symbolically,  $p \wedge q$  read “ $p$  and  $q$ ” denotes the conjunction of  $p$  and  $q$ .

## Truth Value:

Since  $p \wedge q$  is a proposition it has a truth value, and this truth value depends on the truth values of  $p$  and  $q$ . Specifically:

If  $\check{p}$  and  $\check{q}$  are true, then  $\underline{p \wedge q}$  is true; otherwise  $p \wedge q$  is false.



# Conjunction $p \wedge q$

Any two propositions can be combined by the word “and” to form a compound proposition called the conjunction of the original propositions. Symbolically,  $p \wedge q$  read “ $p$  and  $q$ ” denotes the conjunction of  $p$  and  $q$ .

## Truth Value:

Since  $p \wedge q$  is a proposition it has a truth value, and this truth value depends on the truth values of  $p$  and  $q$ . Specifically:

If  $p$  and  $q$  are true, then  $p \wedge q$  is true; otherwise  $p \wedge q$  is false.



# Truth Table of $p \wedge q$ and Examples

| $p$ | $q$ | $p \wedge q$ |
|-----|-----|--------------|
| T   | T   | T            |
| - T | F   | F            |
| - F | T   | F            |
| - F | F   | F            |

Examples:

- 1) Paris is in France and  $2+2=4$ . True
- 2) Paris is in England and  $2+2=4$ . False.
- 3) Paris is in France and  $2+2=5$ . False.
- 4) Paris is in England and  $2+2=5$ . False.

# Disjunction $p \vee q$

Any two propositions can be combined by the word “or” to form a compound proposition called the disjunction of the original propositions. Symbolically,  $p \vee q$  read “ $p$  or  $q$ ”, denotes the disjunction of  $p$  and  $q$ .

## Truth Value:

The truth value of  $p \vee q$  depends only on the truth values of  $p$  and  $q$  as follows:

If  $p$  and  $q$  are false, then  $p \vee q$  is false; otherwise  $p \vee q$  is true.



# Truth Table of $p \vee q$ and Examples

| $p$ | $q$ | $p \vee q$ |
|-----|-----|------------|
| T   | T   | T          |
| T   | F   | T          |
| F   | T   | T          |
| F   | F   | F          |

- 1) Paris is in France or  $2+2=4$ . T
- 2) Paris is in England or  $2+2=4$ . T
- 3) Paris is in France or  $2+2=5$ . T
- 4) Paris is in England or  $2+2=5$ . F



# Negation

Let  $p$  be a proposition. The negation of  $p$ , denoted by  $\sim p$ , is the statement “It is not the case that  $p$ ” The proposition  $\sim p$  is read “not  $p$ ”.

## **Truth Value:**

The truth value of the negation of  $p$  is the opposite of the truth value of  $p$ .





# Truth Table of $\sim p$ and Examples

| $p$ | $\sim p$ |
|-----|----------|
| T   | F        |
| F   | T        |

Examples :

1) Paris is in France.

Negation is "Paris is not in France".

2)  $2 + 2 = 5$ .

Negation is " $2 + 2 \neq 5$ ".



# More Logical Operations



# Conditional Statement

Let  $p$  and  $q$  be propositions. The conditional statement  $p \rightarrow q$  is the proposition “if  $p$  then  $q$ ”. The conditional statement  $p \rightarrow q$  is false when  $p$  is true and  $q$  is false, and true otherwise. In the conditional statement  $p \rightarrow q$ ,  $p$  is called the hypothesis and  $q$  is called the conclusion.

Useful Way to Understand the Truth Value:

Consider a statement that a professor might make:

“If you get 100% on the final, then you will get A.”

*If you manage to get 100% on the final, then you would expect to receive an A. If you do not get 100% you may or may not receive an A. However, if you do get 100%, but the professor does not give you an A, you will feel cheated.*

# Different Form of Conditional Statement

Because conditional statements play such an essential role in mathematical reasoning, a variety of terminology is used to express  $p \rightarrow q$ . You will encounter most if not all of the following ways to express this conditional statement:

“if  $p$ , then  $q$ ”

“ $p$  implies  $q$ ”

“ $p$  implies  $q$ ” ✓

“ $q$  whenever  $p$ ” ✓

“ $p$  is sufficient for  $q$ ”

“ $q$  if  $p$ ”

“ $q$  when  $p$ ”



# Truth Table of $p \rightarrow q$ and $\sim p \vee q$

1)  $p \rightarrow q$

| $p$ | $q$ | $p \rightarrow q$ |
|-----|-----|-------------------|
| T   | T   | T                 |
| T   | F   | F                 |
| F   | T   | T                 |
| F   | F   | T                 |

2)  $\sim p \vee q$

| $p$ | $q$ | $\sim p$ | $\sim p \vee q$ |
|-----|-----|----------|-----------------|
| T   | T   | F        | T               |
| T   | F   | F        | F               |
| F   | T   | T        | T               |
| F   | F   | T        | T               |

$$p \rightarrow q \equiv \sim p \vee q$$



Observe that the truth tables of  $p \rightarrow q$  and  $\sim p \vee q$  are identical. Accordingly,  $p \rightarrow q$  and  $\sim p \vee q$  are logically equivalent.

*In other words, the conditional statement “If  $p$  then  $q$ ” is logically equivalent to the statement “Not  $p$  or  $q$ ”*

$$\sim p \vee q$$



# Example 1

Let  $p$  be the statement “Maria learns discrete mathematics” and  $q$  the statement “Maria will find a job.” Express the statement  $p \rightarrow q$  as a statement in English.

Solution: If Maria learns discrete mathematics, then she will find a good job.

There are other ways to express this conditional statement in English.

Maria will find a good job when she learns discrete mathematics.

*q when p*



# Biconditional Statement

Let  $p$  and  $q$  be propositions. The biconditional statement  $p \Leftrightarrow q$  is the proposition “ $p$  if and only if  $q$ .” The biconditional statement  $p \Leftrightarrow q$  is true when  $p$  and  $q$  have the same truth values, and is false otherwise.

Truth table is given below:

|   | $p$ | $q$ | $p \Leftrightarrow q$ |
|---|-----|-----|-----------------------|
| → | T   | T   | T                     |
| → | T   | F   | F                     |
| → | F   | T   | F                     |
| → | F   | F   | T                     |





# Truth table of $(p \rightarrow q) \wedge (q \rightarrow p)$ and $p \leftrightarrow q$

| $p$ | $q$ | $p \rightarrow q$ | $q \rightarrow p$ | $(p \rightarrow q) \wedge (q \rightarrow p)$ | $p \leftrightarrow q$ |
|-----|-----|-------------------|-------------------|----------------------------------------------|-----------------------|
| T   | T   | T                 | T                 | T                                            | T                     |
| T   | F   | F                 | T                 | F                                            | F                     |
| F   | T   | T                 | F                 | F                                            | F                     |
| F   | F   | T                 | T                 | T                                            | T                     |

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$



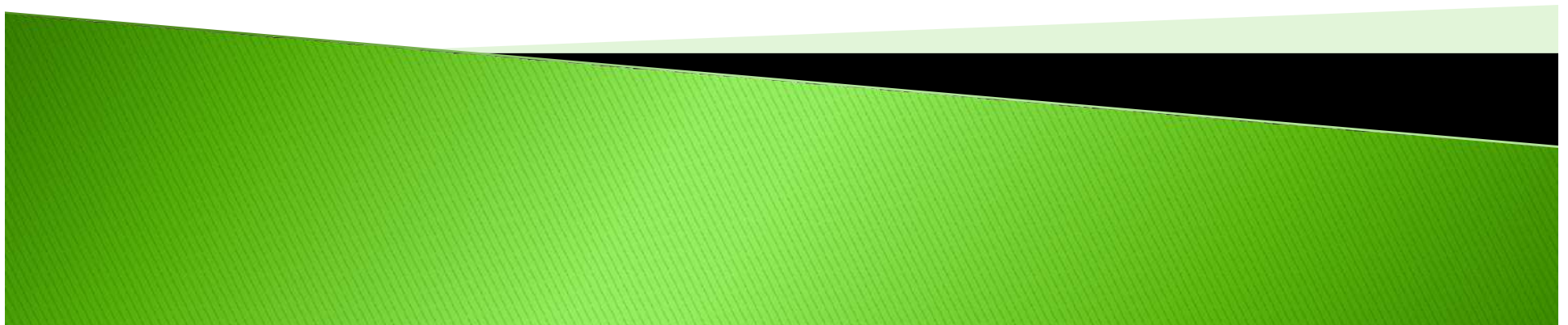
## Example 2

Let  $p$  be the statement “You can take the flight,” and let  $q$  be the statement “You buy a ticket.” Then  $p \leftrightarrow q$  is the statement

✓ “You can take the flight if and only if you buy a ticket.”



# Truth Tables of Compound Propositions



We have now introduced four important logical connectives– conjunctions, disjunctions, conditional statements, and biconditional statements– as well as negations. We can use these connectives to build up complicated compound propositions involving any number of propositional variables. We can use truth tables to determine the truth values of these compound propositions.



# Example 1

Construct the truth table of the compound proposition  $(p \vee \sim q) \rightarrow (p \wedge q)$ .

| $p$ | $q$ | $\sim q$ | $p \vee \sim q$ | $\overline{p \wedge q}$ | $(p \vee \sim q) \rightarrow (p \wedge q)$ |
|-----|-----|----------|-----------------|-------------------------|--------------------------------------------|
| T   | T   | F        | T               | T                       | T                                          |
| T   | F   | T        | T               | F                       | F                                          |
| F   | T   | F        | F               | F                       | T                                          |
| F   | F   | T        | T               | F                       | F                                          |



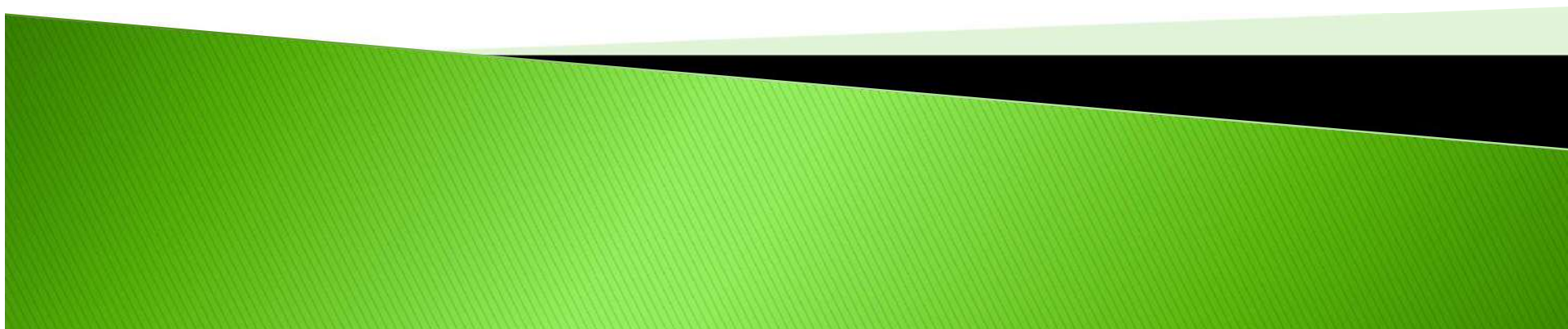
## Example 2

Construct the truth table of the compound proposition  $(p \rightarrow q) \vee (\sim p \rightarrow r)$ .

| $p$ | $q$ | $r$ | $\sim p$ | $p \rightarrow q$ | $\sim p \rightarrow r$ | $(p \rightarrow q) \vee (\sim p \rightarrow r)$ |
|-----|-----|-----|----------|-------------------|------------------------|-------------------------------------------------|
| T   | T   | T   | F        | T                 | T                      | T                                               |
| T   | T   | F   | F        | T                 | T                      | T                                               |
| T   | F   | T   | F        | F                 | T                      | T                                               |
| T   | F   | F   | F        | F                 | T                      | T                                               |
| F   | T   | T   | T        | T                 | T                      | T                                               |
| F   | T   | F   | T        | T                 | F                      | T                                               |
| F   | F   | T   | T        | T                 | T                      | T                                               |
| F   | F   | F   | T        | T                 | F                      | T                                               |



# Real Numbers and the Power of Continuum Part 1



# Theorem 1

The unit interval  $I = [0, 1]$  is nondenumerable.

*Proof.* Let  $I$  is denumerable. Then

$$\checkmark I = \{x_1, x_2, x_3, \dots\}$$

That is, the elements of  $I$  can be written in a sequence. So

$$x_1 = 0.\overset{\checkmark}{a_{11}} a_{12} a_{13} \dots a_{1n} \dots$$

$$x_2 = 0.a_{21} \overset{\checkmark}{a_{22}} a_{23} \dots a_{2n} \dots$$

$$x_3 = 0.a_{31} a_{32} a_{33} \dots a_{3n} \dots$$

$$\vdots$$

$$x_n = 0.a_{n1} a_{n2} a_{n3} \dots a_{nn} \dots$$

Here

$$a_{ij} \in \{0, 1, 2, \dots, 9\}$$

$$\left. \begin{array}{l} 0 = 0.000\dots \\ 0.1 = 0.\underline{0}\underline{9}99\dots \\ 0.5 = 0.4999\dots \\ 1 = 0.\overline{9}99\dots \end{array} \right\}$$



# Theorem 1

Now construct the real number

$$\sqrt{x} = 0.b_1 b_2 b_3 \dots b_n \dots$$

→ which will belong to  $I$  in the following way:

choose  $b_1$  so  $b_1 \neq a_{11}$  and  $b_1 \neq 0$

choose  $b_2$  so  $b_2 \neq a_{22}$  and  $b_2 \neq 0$

choose  $b_3$  so  $b_3 \neq a_{33}$  and  $b_3 \neq 0$  and so on.

Note that  $\sqrt{x} \neq x_1$  since  $b_1 \neq a_{11}$ .

and  $\sqrt{x} \neq x_2$  since  $b_2 \neq a_{22}$  and so on.

That is  $\sqrt{x} \neq x_n$  for all  $n \in \mathbb{P}$ .

Thus  $\sqrt{x} \notin I$ , which contradicts the fact that  $\sqrt{x} \in I$ . Thus the assumption that  $I$  is denumerable is wrong. Hence  $I$  is nondenumerable.

# Power of the Continuum

A set  $A$  is said to have the power of the continuum if  $A$  has the same cardinality as the unit interval  $I = [0, 1]$ .

For example,  $[a, b] \approx [0, 1]$ .

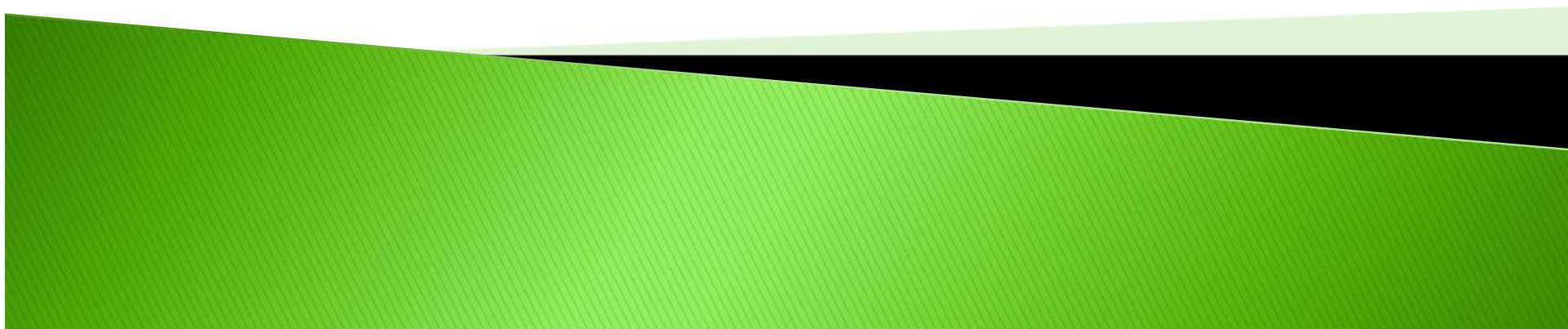
Hence closed interval  $[a, b]$  has the power of continuum. Similarly,  $[a, b)$ ,  $(a, b]$  and  $(a, b)$  also have the power of continuum.



# Power of the Continuum



# Real Numbers and the Power of Continuum Part 2



# Theorem 1

Prove that the set  $R$  of real numbers has the power of continuum.

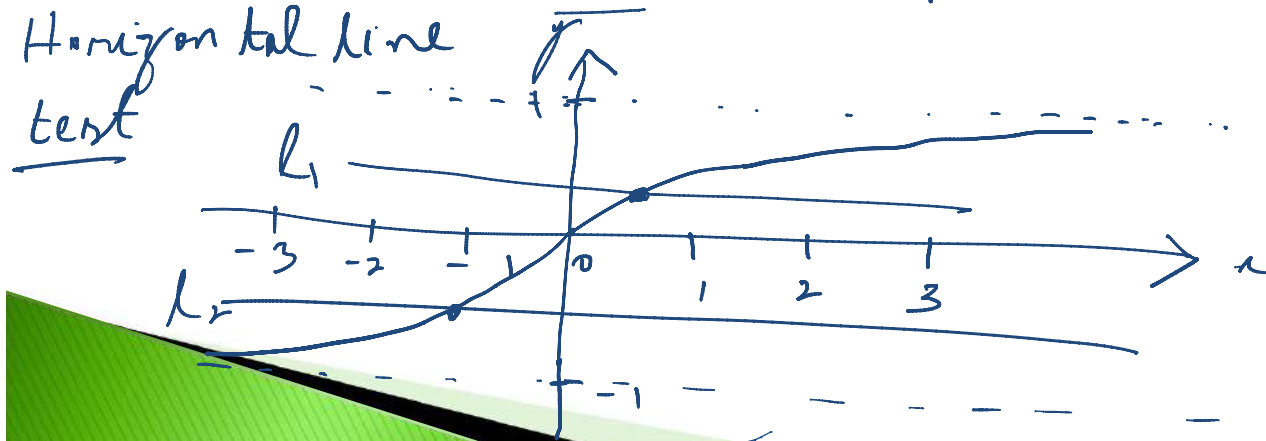
Proof. Consider the function

$f : R \rightarrow (-1, 1)$  defined by

$\forall f(x) = \frac{x}{1+|x|}$ . clearly  $\forall$  values of  $x$  belong to

$(-1, 1)$  since  $|x| < 1 + |x|$ .

Horizontal line test



①  $R \approx (-1, 1)$

②  $\forall (-1, 1) \approx [0, 1]$

Then

$R \approx [0, 1]$ .

$f(1) = \frac{1}{1+1} = \frac{1}{2} \in (-1, 1)$

$f(-2) = \frac{-2}{1+2} = \frac{-2}{3} \in (-1, 1)$

By horizontal line test,  $f(x)$  is bijective.  
Hence,  $R$  has the power of continuum.

# Theorem 1



# Cardinal Numbers



# Definition

Each set  $A$  is assigned a symbol in such a way that two sets  $A$  and  $B$  are assigned the same symbol if and only if they are equipotent. This symbol is called the cardinality or cardinal number of  $A$ , and it is denoted by

✓  
 $|A|$ ,  $n(A)$  or  $\text{card}(A)$

Thus,

$$|A| = |B| \text{ if and only if } A \approx B.$$





# Finite Cardinal Numbers

✓  
0 is assigned to the empty set  $\emptyset$ , and  $n$  is assigned to the set  $\{1, 2, \dots, n\}$ . Thus,

$$|A| = n$$

$$|A| = 3$$

$$A \approx \{1, 2, \dots, n\}$$

$$A \approx \{1, 2, 3\}$$

$$, \text{ e.g. } :- A = \{2, 3, 4\}$$

Alternatively, the symbols 0, 1, 2, 3, ... are assigned, respectively, to the sets

$$\emptyset, \{\emptyset\}, [\emptyset, \{\emptyset\}], [\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}], \dots$$



# Transfinite Cardinal Numbers

Cardinal numbers of infinite sets are called infinite or transfinite cardinal numbers.

The cardinal number of the infinite set  $P$  of positive integers is  $\underline{N}_0$  (aleph-nought)

Thus,

$$|A| = \underline{N}_0 \quad \text{iff} \quad A \approx P.$$

In particular,

$$|Z| = \underline{N}_0 \quad \text{since} \quad Z \approx P.$$

and  $|Q| = \underline{N}_0 \quad \text{since} \quad Q \approx P$



# Transfinite Cardinal Numbers

The cardinal number of the unit interval  $\overline{I} = [0, 1]$  is denoted by  $\underline{\mathbf{c}}$  and it is called the power of continuum.

Thus:

$$|A| = \underline{\mathbf{c}} \quad \text{iff} \quad A \approx \overline{I}.$$

In particular, we have  $|\underline{R}| = \underline{\mathbf{c}}$ , and the cardinal number of any interval is  $\underline{\mathbf{c}}$ .

$$\text{For example, } |(2, 3)| = \underline{\mathbf{c}} \quad \text{since } (2, 3) \approx [0, 1]$$

$$|[-1, 5]| = \underline{\mathbf{c}} \quad \text{'' } [-1, 5] \approx [0, 5]$$



# Some Important Statements

- (a)  $A$  is denumerable or countably infinite means  $|A| = \aleph_0$ .
- (b)  $A$  is countable means  $|A|$  is finite or  $|A| = \aleph_0$ .
- (c)  $A$  has the power of continuum if  $|A| = \underline{\underline{\mathbf{c}}}$ .

$$|\mathbb{R}| = c$$



# Tuatologies and Contradictions



A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called tautology. A compound proposition that is always false is called a contradiction.



# Example 1

The proposition  $p \vee \sim p$  is a tautology and the proposition  $p \wedge \sim p$  is a contradiction.

| $p$ | $\sim p$ | $p \vee \sim p$ | $p \wedge \sim p$ |
|-----|----------|-----------------|-------------------|
| T   | F        | T               | F                 |
| F   | T        | T               | F                 |



# Logical Equivalences





Compound propositions that have the same truth values in all possible cases are called logically equivalent. We can also define this notion as follows.

“The compound propositions p and q are called logically equivalent if  $p \leftrightarrow q$  is a tautology. The notation  $p \equiv q$  denotes that  $p$  and  $q$  are logically equivalent.”



# Example 1

One way to determine whether two compound propositions are equivalent is to use a truth table.

Consider the two propositions  $\sim(p \vee q)$  and  $\sim p \wedge \sim q$ . Truth tables for  $\sim(p \vee q)$  and  $\sim p \wedge \sim q$  are given below:

| $p$ | $q$ | $p \vee q$ | $\sim(p \vee q)$ | $\sim p$ | $\sim q$ | $\sim p \wedge \sim q$ |
|-----|-----|------------|------------------|----------|----------|------------------------|
| T   | T   | T          | F                | F        | F        | F                      |
| T   | F   | T          | F                | F        | T        | F                      |
| F   | T   | T          | F                | T        | F        | F                      |
| F   | F   | F          | T                | T        | T        | T                      |

$$\text{so } \sim(p \vee q) \equiv \sim p \wedge \sim q$$



## Example 2

Show that  $p \rightarrow q$  and  $\sim p \vee q$  are logically equivalent.

$$p \rightarrow q \equiv \sim p \vee q$$

| $p$ | $q$ | $p \rightarrow q$ | $\sim p$ | $\sim p \vee q$ |
|-----|-----|-------------------|----------|-----------------|
| T   | T   | T                 | F        | T               |
| T   | F   | F                 | F        | F               |
| F   | T   | T                 | T        | T               |
| F   | F   | T                 | T        | T               |

Proved:

# Example 3

Show that  $\underline{(p \rightarrow q) \wedge (p \rightarrow r)} \equiv \underline{p \rightarrow (q \wedge r)}$  and  ~~$\sim p \vee q$~~  are logically equivalent.

| $\checkmark$<br>$p$ | $q$ | $r$ | $\checkmark$<br>$p \rightarrow q$ | $\checkmark$<br>$p \rightarrow r$ | $\downarrow$<br>$(p \rightarrow q) \wedge (p \rightarrow r)$ | $\checkmark$<br>$q \wedge r$ | $\downarrow$<br>$p \rightarrow (q \wedge r)$ |
|---------------------|-----|-----|-----------------------------------|-----------------------------------|--------------------------------------------------------------|------------------------------|----------------------------------------------|
| T                   | T   | T   | T                                 | T                                 | T                                                            | T                            | T                                            |
| T                   | T   | F   | T                                 | F                                 | F                                                            | F                            | F                                            |
| T                   | F   | T   | F                                 | T                                 | F                                                            | F                            | F                                            |
| T                   | F   | F   | F                                 | F                                 | F                                                            | F                            | F                                            |
| F                   | T   | T   | T                                 | T                                 | T                                                            | T                            | T                                            |
| F                   | T   | F   | T                                 | T                                 | T                                                            | F                            | T                                            |
| F                   | F   | T   | T                                 | T                                 | T                                                            | F                            | T                                            |
| F                   | F   | F   | T                                 | T                                 | T                                                            | F                            | T                                            |

Proved

# Logical Equivalences involving Conditional Statements

$$1) P \rightarrow Q \equiv \sim P \vee Q$$

$$2) P \rightarrow Q \equiv \sim Q \rightarrow \sim P$$

$$3) P \vee Q \equiv \sim P \rightarrow Q$$

$$4) P \wedge Q \equiv \sim (P \rightarrow \sim Q)$$

$$5) \sim (P \rightarrow Q) \equiv P \wedge \sim Q$$

$$6) (P \rightarrow Q) \wedge (P \rightarrow R) \equiv P \rightarrow (Q \wedge R)$$

$$7) (P \rightarrow R) \wedge (Q \rightarrow R) \equiv (P \vee Q) \rightarrow R$$

$$8) (P \rightarrow Q) \vee (P \rightarrow R) \equiv P \rightarrow (Q \vee R)$$

$$9) (P \rightarrow R) \vee (Q \rightarrow R) \equiv (P \wedge Q) \rightarrow R$$



# Logical Equivalences involving Biconditional Statements

$$1) \quad p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

$$2) \quad p \leftrightarrow q \equiv \sim p \leftrightarrow \sim q$$

$$3) \quad p \leftrightarrow q \equiv (p \wedge q) \vee (\sim p \wedge \sim q)$$

$$4) \quad \sim (p \leftrightarrow q) \equiv p \leftrightarrow \sim q$$



# Algebra of Propositions



### 1) Idempotent Laws

$$(1a) P \vee P \equiv P \quad (1b) P \wedge P \equiv P$$

### 2) Associative Laws

$$(2a) (P \vee Q) \vee R \equiv P \vee (Q \vee R) \quad (2b) (P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$$

### 3) Commutative Laws

$$(3a) P \vee Q \equiv Q \vee P \quad (3b) P \wedge Q \equiv Q \wedge P$$

### 4) Distributive Laws

$$(4a) P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$

$$(4b) P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

### 5) Identity Laws

$$(5a) \underline{P \wedge T \equiv P} \quad (5b) \underline{P \vee F \equiv P}$$

| P | T | $P \wedge T$ |
|---|---|--------------|
| T | T | T            |
| F | T | F            |

| P | F | $P \vee F$ |
|---|---|------------|
| T | F | T          |
| F | F | F          |



6) Domination laws

$$(6a) P \vee \underline{T} \equiv \underline{T} \quad (6b) P \wedge \underline{F} \equiv \underline{F}$$

7) Double negation law

$$\sim(\sim P) \equiv P$$

8) De Morgan's laws

$$(8a) \sim(P \wedge Q) \equiv \sim P \vee \sim Q$$

$$(8b) \sim(P \vee Q) \equiv \sim P \wedge \sim Q$$

9) Absorption laws

$$(9a) \underline{P} \vee (\underline{P} \wedge Q) \equiv \underline{P} \quad (9b) \underline{P} \wedge (\underline{P} \vee Q) \equiv \underline{P}$$

10) Negation laws

$$(10a) P \vee \sim P \equiv T \quad (10b) \underline{P \wedge \sim P} \equiv F$$

prove  $p \vee \sim p \equiv T$ .

|               | $p$ | $\sim p$ | $p \vee \sim p \equiv T$ | $p \wedge \sim p \equiv F$ |
|---------------|-----|----------|--------------------------|----------------------------|
| $\rightarrow$ | T   | F        | T                        | F                          |
| $\rightarrow$ | F   | T        | T                        | F                          |

11) Distributive laws

(11a)  $p \vee (q$





# Constructing New Logical Equivalences



The logical equivalences that have been established so far can be used to construct additional logical equivalences. This technique is illustrated in the following examples.



# Example 1

Show that  $\overset{1}{\sim(p \rightarrow q)}$  and  $\overset{2}{p \wedge \sim q}$  are logically equivalent.

Sol We want to prove  $\sim(p \rightarrow q) \equiv \underline{\underline{p \wedge \sim q}}$ .

$$\sim(p \rightarrow q) \equiv \sim(\sim p \vee q)$$

$$\equiv \sim(\sim p) \wedge \sim q, \text{ by De Morgan Law}$$

$$\equiv p \wedge \sim q, \text{ by the double negation Law.}$$

$$\underline{\underline{p \rightarrow q \equiv \sim p \vee q}}$$



## Example 2

Show that  $\sim(p \vee (\sim p \wedge q))$  and  $\sim p \wedge \sim q$  are logically equivalent by developing a series of logical equivalences.

$$\begin{aligned}\sim(p \vee (\sim p \wedge q)) &\equiv \sim p \wedge \sim(\sim p \wedge q), && \text{by the 2nd De Morgan Law} \\ &\equiv \sim p \wedge [\sim(\sim p) \vee \sim q], && // \\ &\equiv \sim p \wedge [p \vee \sim q], && \text{by the double negation law.} \\ &\equiv (\sim p \wedge p) \vee (\sim p \wedge \sim q), && \text{by the distributive Law.} \\ &\equiv F \vee (\sim p \wedge \sim q) \\ &\equiv \sim p \wedge \sim q, && \text{by the identity Law.}\end{aligned}$$

## Example 3

$$P \vee P \equiv P$$
$$\underline{P \rightarrow Q \equiv \sim P \vee Q}$$

Show that  $(p \wedge q) \rightarrow (p \vee q)$  is a tautology.

$$(P \wedge Q) \rightarrow (P \vee Q) \equiv \sim(P \wedge Q) \vee (P \vee Q)$$

$$\equiv (\sim P \vee \sim Q) \vee (P \vee Q), \quad \text{by the DeMorgan law}$$

$$\equiv (\sim P \vee P) \vee (\sim Q \vee Q), \quad \text{by the asso. and the comm. law}$$

$$\equiv \underline{I} \vee \underline{I}$$

$$\equiv \underline{\underline{I}}$$

, by the domination law.





## Example 4

Show that  $\sim ((p \rightarrow q) \wedge p) \vee q$  is a tautology.

$$\begin{aligned} & \sim((p \rightarrow q) \wedge p) \vee q \\ \equiv & \sim(\underline{(\sim p \vee q)} \wedge \underline{p}) \vee q \\ \equiv & \sim(\underline{(\sim p \wedge p)} \vee (q \wedge p)) \vee q \\ \equiv & \sim(F \vee (q \wedge p)) \vee q \\ \equiv & [\sim F \wedge \sim(q \wedge p)] \vee q \\ \equiv & [\underline{T} \wedge \sim(\underline{q \wedge p})] \vee q \\ \equiv & \sim(q \wedge p) \vee q \\ \equiv & (\sim q \vee \sim p) \vee q \\ \equiv & (\underline{\sim q} \vee \underline{q}) \vee \sim p \\ \equiv & T \vee \sim p \\ \equiv & \underline{T} \end{aligned}$$

# Converse, Contrapositive, and Inverse



We can form some new conditional statements starting with a conditional statement  $p \rightarrow q$ . In particular, there are three related conditional statements that occur so often that they have special names.



# Converse of $p \rightarrow q$

The proposition  $q \rightarrow p$  is called the converse of  $p \rightarrow q$ .

Example 1: Write the converse of the conditional statement "The home team wins whenever it is raining".

*If whenever  $p =$  if  $p$  then  $q$   
"if it is raining, then the home <sup>team</sup> wins".*

*Now the converse is:*

*If the home team wins, then it is raining.*



# Contrapositive of $p \rightarrow q$

The contrapositive of  $\check{p} \rightarrow \check{q}$  is the proposition  $\sim q \rightarrow \sim p$ . We first show that the contrapositive,  $\sim q \rightarrow \sim p$  of a conditional statement  $p \rightarrow q$  always has the same truth value as  $p \rightarrow q$ .

| $p$ | $q$ | $\sim p$ | $\sim q$ | $p \rightarrow q$ | $\sim q \rightarrow \sim p$ |
|-----|-----|----------|----------|-------------------|-----------------------------|
| T   | T   | F        | F        | T                 | T                           |
| T   | F   | F        | T        | F                 | F                           |
| F   | T   | T        | F        | T                 | T                           |
| F   | F   | T        | T        | T                 | T                           |

$$\therefore \underline{p \rightarrow q} \equiv \underline{\sim q \rightarrow \sim p}$$

Example 2: Write the contrapositive of the conditional statement "The home team wins whenever it is raining".

"If it is raining, then the home team wins."

Contrapositive is:

"If the home team does not win, then it is not raining."

# Inverse of $p \rightarrow q$

The proposition  $\sim p \rightarrow \sim q$  is called the inverse of  $p \rightarrow q$ . We will show that the converse and the inverse of a conditional statement are also equivalent.

| $p$ | $q$ | $\sim p$ | $\sim q$ | $\sim p \rightarrow \sim q$ | $q \rightarrow p$ |
|-----|-----|----------|----------|-----------------------------|-------------------|
| T   | T   | F        | F        | T                           | T                 |
| T   | F   | F        | T        | T                           | T                 |
| F   | T   | T        | F        | F                           | F                 |
| F   | F   | T        | T        | T                           | T                 |

$$\therefore \sim p \rightarrow \sim q \equiv q \rightarrow p$$

Example 3: Write the inverse of the conditional statement "The home team wins whenever it is raining".

"If it is raining, then the home team wins."

Inverse is:

"If it is not raining, then the home team does not win."

# Example 4

State the converse, contrapositive, and inverse of ~~each of~~<sup>of</sup>  
"A positive integer is a prime only if it has no divisors other than 1 and itself."

"If a positive integer is a prime, then it has no divisors other than 1 and it self."

converse is:

"If a positive integer has no divisors other than 1 and itself, then a positive integer is a prime."

then  
if  $p$  and  $q$ ,  
or  
 $p$  only if  $q$ .

$p \rightarrow q$

converse:  $q \rightarrow p$

contrapositive:  
 $\sim q \rightarrow \sim p$

## Example 4

contrapositive is:

"If a positive integer has a divisor other than 1 and itself, then it is not prime".

Inverse is:

"If a positive integer is not prime, then it has a divisor other than 1 and itself".

$$p \rightarrow q$$

Inverse is:

$$\sim p \rightarrow \sim q$$





# Argument

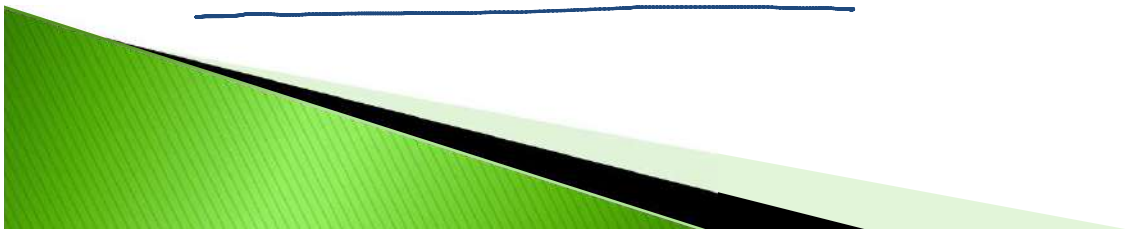


# Argument and Valid Argument

An argument in propositional logic is a sequence of propositions. All but the final proposition in the argument are called premises and the final proposition is called the conclusion.

An argument is valid if the truth of all its premises implies that the conclusion is true.

It means the argument form with premises  $\underline{p_1, p_2, \dots, p_n}$  and conclusion  $\underline{q}$  is valid, when  $\underline{(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow q}$  is a tautology.



# Example to Understand valid Argument

Consider the following argument involving propositions:

✓1) "If you have a current password, then you can log onto the network."  
 $\frac{P}{q}$

✓2) "You have a current password." =  $P$

Therefore,

3) "You can log onto the network." (conclusion) =  $q$

$$\left\{ \begin{array}{l} P \rightarrow q \\ P \\ \hline \therefore q \end{array} \right.$$

✓  $(P \rightarrow q) \wedge P \rightarrow q$  is a tautology?

| $P$      | $q$      | $P \rightarrow q$ | $(P \rightarrow q) \wedge P$ | $(P \rightarrow q) \wedge P \rightarrow q$ |
|----------|----------|-------------------|------------------------------|--------------------------------------------|
| $\oplus$ | $\oplus$ | $\oplus$          | T                            | T                                          |
| T        | F        | F                 | F                            | T                                          |
| F        | T        | T                 | F                            | T                                          |
| F        | F        | F                 | F                            | T                                          |

# Example to Understand valid Argument

suppose

$p$  : You have access to the network.

$q$  : You can change your grade

Also  $p$  is true, but  $p \rightarrow q$  is false.

{ "If you have access to the network, then  
you can change your grade"  
"You have access to the network."  
Therefore,  
"You can change your grade".

{ 
$$\begin{array}{r} p \rightarrow q \checkmark \\ p \\ \hline \therefore q \end{array}$$

# Example to Understand valid Argument

The argument we obtained is a valid argument, but because one of the premises, namely the  $P \rightarrow Q$  is false, we cannot conclude that the conclusion is true.

In next topic, we will see more valid argument forms.



# Rules of Inference for Propositional Logic



The tautology  $(p \wedge (p \rightarrow q)) \rightarrow q$  is the basis of the rule of inference called **modus ponens**, or the **law of detachment**. This tautology leads to the following valid argument form:

$$\left\{ \begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array} \right.$$





# Example 1

Suppose that the conditional statement "If it snows today , then we will go skiing" and its hypothesis, "It is snowing today," are true.

Then, by law of detachment, it follows that the conclusion of the conditional statement, "We will go skiing," is true. In notation form, we see that

$\checkmark P$  : It is snowing today.

$q$  : we will go skiing.

$$\left\{ \begin{array}{l} P \rightarrow q \checkmark \\ P \checkmark \\ \hline \therefore q \end{array} \right.$$

we can conclude that  
by law of detachment that  
"we will go skiing" is true.



## Example 2

Determine whether the argument given here is valid and determine whether its conclusion must be true because of the validity of the argument.

"If  $\sqrt{2} > \frac{3}{2}$ , then  $(\sqrt{2})^2 > (\frac{3}{2})^2$ . We know that  $\sqrt{2} > \frac{3}{2}$ .  
Consequently,  $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$ .

Solution.

Let  $p : \sqrt{2} > \frac{3}{2}$  and  $q : (\sqrt{2})^2 > (\frac{3}{2})^2$  ( $\because 2 < \frac{9}{4}$ ).

Here  $p \rightarrow q$  } = Law of detachment.

$\frac{XP}{\therefore \textcircled{q}}$  } Now we want to determine is true or not? Here one of its premises is false, which is  $\sqrt{2} > \frac{3}{2}$ . We cannot conclude that the conclusion is true.

# Rules of Inference

$$1) \frac{P \quad P \rightarrow q}{\therefore q}$$

$(P \wedge (P \rightarrow q)) \rightarrow q$  is a tautology. (Modus ponens)

$$2) \frac{\sim q \quad P \rightarrow q}{\therefore \sim P}$$

$(\sim q \wedge (P \rightarrow q)) \rightarrow \sim P$  is a tautology. (Modus tollens)

$$3) \frac{P \rightarrow q \quad q \rightarrow r}{\therefore P \rightarrow r}$$

$((P \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (P \rightarrow r)$  is a tautology. (Hypothetical syllogism)

$$4) \frac{P \vee q \quad \sim P}{\therefore q}$$

$((P \vee q) \wedge \sim P) \rightarrow q$  is a tautology. (Disjunctive syllogism)

# Rules of Inference

$$5) \frac{P}{\therefore P \vee q}$$

$P \rightarrow (P \vee q)$  is a  
tautology.

(Addition)

$$6) \frac{P \wedge q}{\therefore P}$$

$P \wedge q \rightarrow P$  is a  
tautology

(simplification)

$$7) \frac{P}{q} \\ \hline \therefore P \wedge q$$

$(P \wedge q) \rightarrow P \wedge q$   
is a tautology

(conjunction)

$$8) \frac{P \vee q}{\sim P \vee r} \\ \hline \therefore q \vee r$$

$((P \vee q) \wedge (\sim P \vee r)) \rightarrow q \vee r$   
is a tautology.

(Resolution)



# Examples Using Rules of Inference



# Example 1

Find the argument form for the following argument and determine whether it is valid. Can we conclude that the conclusion is true if the premises are true?

If Socrates is human, then Socrates is mortal.

→ Socrates is human.

∴ Socrates is mortal. (conclusion)

Let  $p$ : Socrates is human.

$q$ : Socrates is mortal.

$$\left\{ \begin{array}{l} p \rightarrow q \quad \checkmark \\ p \quad \checkmark \\ \hline \therefore q \quad \checkmark \end{array} \right.$$

This is Modus ponens.

Here the conclusion is true if the premises are true because it is a valid argument.

# Example 2

What rule of inference is used in each of these arguments?

a) Salman is a mathematics major. Therefore, Salman is either a mathematics major or a computer science major.

Sol: Let  $p$ : Salman is a mathematics major.

$q$ : " " " " computer science major.

$\left\{ \frac{p}{\therefore p \vee q} \right.$  Here addition is used.

b) Ezaan is a mathematics major and a computer science major. Therefore, Ezaan is a mathematics major.

Sol: Let  $p$ : Ezaan is a mathematics major.

$q$ : Ezaan is a computer science major.

$\left\{ \frac{p \wedge q}{\therefore p} \right.$  Here simplification is used.

## Example 2

c) If it is rainy, then the pool will be closed. It is rainy. Therefore, the pool is closed.

Sol. Let  $p$  : it is rainy.  
 $q$  : the pool is closed.

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

Here Modus ponens is used.

d) If it snows today, the university will close. The university is not closed today. Therefore, it did not snow today.

Sol. Let  $p$  : it snows today.  
 $q$  : the university is closed.

Here the argument is :

$$\left\{ \begin{array}{l} p \rightarrow q \\ \sim q \\ \hline \sim p \end{array} \right.$$

Here Modus tollens is used.



# Example 3

Use rules of inference to show that the hypotheses "Khan works hard," "If Khan works hard, then he is a dull boy," and "If Khan is a dull boy, then he will not get a job" imply the conclusion "Khan will not get the job."

Sol. Let  $p$ : Khan works hard.  
 $q$ : Khan is a dull boy.  
 $r$ : he will get a job.

Therefore, we have reached the conclusion.

Hypotheses are:

$$\begin{cases} p \\ p \rightarrow q \\ q \rightarrow \sim r \end{cases}$$
$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

Now we will use the conclusion  $q$  as a hypothesis in the 2nd stage.

$$\begin{array}{l} q \checkmark \\ q \rightarrow \sim r \checkmark \\ \hline \therefore \sim r \end{array}$$

# Propositional Functions



# Propositional Functions

Let  $A$  be a given set. A propositional function(or an open sentence) defined on  $A$  is an expression

$$\underline{p(x)}$$

which has the property that  $p(a)$  is true or false for each  $a \in A$ . That is,  $p(x)$  becomes a statement (with a truth value) whenever any element  $a \in A$  is substituted for the variable  $x$ .



# Domain and Truth Set of $p(x)$

The set  $A$  is called the domain of  $p(x)$ , and the set  $T_p$  of all elements of  $A$  for which  $p(a)$  is true is called the truth set of  $p(x)$ . In other words,

$$T_p = \{x: x \in A, \text{  $p(x)$  is true}\}$$

Note: Frequently, when  $A$  is some set of numbers, the condition  $p(x)$  has the form of an equation or inequality involving the variable  $x$ .



# Example 1

Let  $p(x)$  denote the statement " $x > 3$ ." What are the truth values of  $p(4)$  and  $p(2)$ ?

Solution.

Here  $p(x) : \underline{x > 3}$

So  $p(4) : 4 > 3$  is a true statement.

Also  $p(2) : 2 > 3$  is a false statement.

Hence  $p(4)$  is true and  $p(2)$  is false.



## Example 2

Let  $p(x)$  denote the statement  
"the word  $x$  contains the letter  $a$ ." What are the  
truth values of  $P(\text{orange})$  and  $P(\text{lemon})$ ?  
Solution.

Here  $p(a)$ : the word  $x$  contains the letter  $a$ .

So  $p(\text{orange})$ : the word orange contains the letter  $a$ ,  
which is a true statement.

and  $p(\text{lemon})$ : the word lemon contains the letter  $a$ ,  
which is a false statement.



## Example 3

Let  $p(x)$  denote the statement " $\underline{x} + 2 > 7$ ." Find the truth set  $T_p$  of each propositional function  $p(x)$  defined on the set  $P = \{1, 2, 3, \dots\}$ .

Solution. Here  $p(x): x + 2 > 7$ .

$$\begin{aligned} \text{So } T_p &= \{x : x \in \underline{P}, \underline{x} + 2 > 7\} = \\ &= \{6, 7, 8, \dots\} \end{aligned}$$



## Example 4

Let  $p(x)$  denote the statement " $x + 5 < 3$ ." Find the truth set  $T_p$  of each propositional function  $p(x)$  defined on the set  $P = \{1, 2, 3, \dots\}$ .

Solution.

$$\text{Here } p(x) : \underline{x + 5 < 3}.$$

Now,  $T_p = \{ \} = \emptyset$  because  $p(x)$  is not true for any value from the domain set  $P$ .





## Example 5

Let  $p(x)$  denote the statement " $x + 5 > 1$ ." Find the truth set  $T_p$  of each propositional function  $p(x)$  defined on the set  $P = \{1, 2, 3, \dots\}$ .

Solution.

Here  $p(x) : \underline{x} + 5 > 1$ .

So,  $T_p = \{1, 2, 3, \dots\} = P$ .



# Propositional Function of Two Variables

We can also have expressions that involve more than one variable. For instance, consider the expression “ $x = y + 3$ .” We can denote this expression by  $Q(x, y)$ , where  $x$  and  $y$  are variables. When value are assigned to the variables  $x$  and  $y$ , the statement  $Q(x, y)$  has a truth value.



## Example 5

Let  $Q(x, y)$  denote the statement " $x = y + 3$ ."  
What are the truth values of the propositions  $Q(1, 2)$  and  $Q(3, 0)$ ?

Solution.

Here  $Q(x, y) : x = y + 3$

so,  $Q(1, 2) : "1 = 2 + 3"$  is a false statement.

and  $Q(3, 0) : 3 = 0 + 3$  is a true statement.



# Propositional Function of $n$ Variables

In general, a statement involving  $n$  variables  $x_1, x_2, \dots, x_n$  can be denoted by  $p(x_1, x_2, \dots, x_n)$ .

A statement of the form  $p(x_1, x_2, \dots, x_n)$  is the value of the propositional function  $p$  at the  $n$ -tuple  $(x_1, x_2, \dots, x_n)$ .



# Quantifiers and Universal Quantifiers



# Introduction

When the variables in a propositional function are assigned values, the resulting statement becomes a Proposition with a certain truth value. However, there is another important way, called **quantification**, to create a proposition from a propositional function. Quantification expresses the extent to which a propositional function is true over a range of elements. In English, *all*, *some*, *many*, *none* and *few* are used in quantifications. We will focus on two types of quantifications here: universal quantification, which tells us that a propositional function is true for every element under consideration, and existential quantification, which tells us that there is one or more element under consideration for which the propositional function is true.



# Universal Quantifier

Let  $p(x)$  be a propositional function defined on a set  $A$ . Consider the expression

$$(\forall x \in A)p(x) \text{ or } \forall x p(x) \quad (1)$$

which reads “For every  $x$  in  $A$ ”,  $p(x)$  is a true statement” or, simply, “For all,  $x, p(x)$ ”. The symbol  $\forall$  which reads “for all” or “for every” is called the *universal quantifier*.

The statement (1) is equivalent to the statement

$$T_p = \{x: x \in A, p(x)\} = A$$

that is, that the truth set of  $p(x)$  is the entire set  $A$ .



# Example 1

Let  $p(x)$  be the statement " $x + 1 > x$ ." What is the truth value of the quantification  $\forall x p(x)$ , where the domain consists of all real numbers?  
Solution.

Here  $p(x): x + 1 > x$ .

Because  $p(x)$  is true for all real numbers  $x$ , that is,

$$T_p = \{x : x \in \mathbb{R}, x + 1 > x\} = \mathbb{R}$$

So,  $\forall x p(x)$  is a true statement.





## Example 2

- (a) The proposition  $(\forall n \in P)(\underline{n + 4 > 3})$  is true since

$$T_P : \{x : x \in P, n+4 > 3\} = \{1, 2, 3, \dots\} = P$$

so  $(\forall n \in P)(n+4 > 3)$  is true.

- (b) The proposition  $(\forall n \in P)(\underline{n} + 2 > 8)$  is false since

$$T_P = \{7, 8, \dots\} \neq P$$



## Example 2

- (a) The proposition  $(\forall n \in P)(n + 4 > 3)$  is true since
  
- (b) The proposition  $(\forall n \in P)(n + 2 > 8)$  is false since



## Example 3

Let  $p(x)$  be the statement " $x < 2$ ." What is the truth value of the quantification  $\forall x p(x)$ , where the domain consists of all real numbers?

Sol.: Here  $p(x): \underline{x < 2}$

put  $x = 3$ ,

$p(3): 3 < 2$  is a false statement.

so,  $\forall x p(x)$  is false.



## Example 4

What is the truth value of  $\forall x(\underline{x^2 \geq x})$  if the domain consists of all real numbers. What is the truth value of this statement if the domain consists of all integers.

Sol. For example, if we take  $x = \frac{1}{2}$ , then

$$\left(\frac{1}{2}\right)^2 < \frac{1}{2}.$$
$$\Rightarrow \frac{1}{4} < \frac{1}{2}$$

so  $\forall x(x^2 \geq x)$  is false.

If we put  $0 < x < 1$ ,  
 $x^2 \geq x$  is false.

Now, consider  $x$  from the set of integers.

$$\text{Here } T_p = \{x : x \in \mathbb{Z}, x^2 \geq x\} = \mathbb{Z}$$

so,  $\forall x(x^2 \geq x)$  is true.

# Existential Quantifier



# Existential Quantifiers

Let  $p(x)$  be a proposition function defined on a set  $A$ . Consider the expression

Which reads

Statement in (1) is equivalent to the statement



# Example 1

- a) The proposition  $(\exists n \in P)(n + 4 < 7)$  is true since
  
  
  
  
  
  
  
  
  
  
- b) The proposition  $(\exists n \in P)(n + 6 < 4)$  is false since

## Example 2

What is the truth value of  $\exists x p(x)$ , where  $p(x)$  is the statement “ $x^2 > 10$ ” and the domain consists of the positive integers not exceeding 4?



# Example 3

Determine the truth value of each of these statements if the domain of each variable consists of all real numbers.

a)  $\exists x(x^2 = 2)$

b)  $\exists x(x^2 = -1)$

c)  $\forall x(x^2 + 2 \geq 1)$

d)  $\forall x(x^2 \neq x)$

# Universal and Existential Quantifier as Conjunction and Disjunction



Consider the propositional function  $p(x)$  as “ $x$  is prime” with domain set  $A = \{2,3,5\}$ .

Consider the propositional function  $p(x)$  as " $x^2 > 10$ " with domain set  $A = \{1, 2, 3, 4\}$ .

# Negation of Quantified Statements



# Negation of Universal Quantifier

Consider the propositional function  $p(x)$  as “ $x$  has taken a course in calculus” and the domain consists of the students in your class. Then the statement:

“Every student in your class has taken a course in calculus.” This statement is a universal quantification, namely,

# Negation of Universal Quantifier



# Negation of Existential Quantifier

Consider the proposition,

“There is a student in this class who has taken a course in calculus.”

This is the existential quantification, namely,





# Negation of Existential Quantifier

Consider the proposition,

“There is a student in this class who has taken a course in calculus.”

This is the existential quantification, namely,



# Example 1

What are the negations of the statements  $\forall x(x^2 > x)$  and  $\exists x(x^2 = 2)$ .

# Example 2

Suppose that the domain of the propositional function  $p(x)$  consists of the integers 0, 1, 2, 3 and 4. Write out each of these propositions using disjunctions, conjunctions, and negations.

a)  $\exists x p(x)$

b)  $\forall x p(x)$

c)  $\exists x \sim p(x)$

d)  $\forall x \sim p(x)$

e)  $\sim \exists x p(x)$

f)  $\sim \forall x p(x)$

# Introduction to Proofs



# Some Terminology

Theorem:

Propositions:

Proof:

Axioms

Lemma:



# Some Terminology

Corollary:

Conjecture:



# Methods of Proving Theorems Part 1



Proving mathematical theorems can be difficult. To construct proofs we need all available ammunition, including a powerful of different proof methods. These methods provide the overall approach and strategy of proofs. Understanding these methods is a key component of learning how to read and construct mathematical proofs.

In this course, we will focus on proving the conditional statements. The followings proofs technique will be discussed here:

- 1) Direct proofs
- 2) Indirect proofs



# Direct Proofs

A direct proof of a conditional statement  $p \rightarrow q$  is constructed when the first step is the assumption that  $p$  is true; subsequent steps are constructed using axioms, definitions, and previously proved theorems, together with rules of inference, to show that  $q$  must also be true. Before we give the first example, we need to define some terminology.



# Even and Odd Integers

The integer  $n$  is even if there exists an integer  $k$  such that  $n = 2k$ , and  $n$  is odd if there exists an integer  $k$  such that  $n = 2k + 1$ .



# Example 1

Give a direct proof of the theorem “If  $n$  is an odd integer, then  $n^2$  is odd.”

Solution:



# Example 2

Give a direct proof that if  $m$  and  $n$  are both perfect squares, then  $nm$  is also a perfect square.

Solution:



# Example 3

Prove that if  $n$  is any even integer, then  $(-1)^n = 1$ .

Solution:



# Example 5

Use a direct proof to show that the product of two rational numbers is rational.

Solution.



# Exercise

- 1) Prove that the product of an even integer and an odd integer is even.
  - 2) Prove that the square of an even integer is even.
  - 3) Prove that if  $n$  is an odd integer, then  $n^3 + n$  is even.
  - 4) Prove that the sum of any three consecutive integers is divisible by 3.
- 

# Methods of Proving Theorems Part 2





# Indirect Proofs

Direct proofs lead from the premises of a theorem to the conclusion. They begin with the premises, continue with a sequence of deductions, and end with the conclusion. However, we will see that attempts at direct proofs often reach dead ends. Proofs of theorems that are not direct proofs, that is, that do not start with the premises and end with the conclusion, are called indirect proofs.



# Proof by Contraposition

Proofs by contraposition make use of the fact that the conditional statement  $p \rightarrow q$  is equivalent to its contrapositive,  $\sim q \rightarrow \sim p$ . In a proof by contraposition of  $p \rightarrow q$ , we take  $\sim q$  as premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that  $\sim p$  is true.

# Example 1

Prove that if  $n$  is an integer and  $3n + 2$  is odd, then  $n$  is odd.

Solution.



## Example 2

Prove that if  $n = ab$ , where  $a$  and  $b$  are positive integers, then  $a \leq \sqrt{n}$  or  $b \leq \sqrt{n}$ .

Solution.



# Example 3

Prove that if  $n$  is an integer and  $n^2$  is odd, then  $n$  is odd.

Solution.



# Proof by Contradiction

Suppose we want to prove that a statement  $p$  is true. Furthermore, suppose that we can find a contradiction  $q$  such that  $\sim p \rightarrow q$  is true. Because  $q$  is false, but  $\sim p \rightarrow q$  is true, we can conclude that  $\sim p$  is false, which means that  $p$  is true.

Because the statement  $r \wedge \sim r$  is a contradiction whenever  $r$  is proposition, we can prove that  $p$  is true if we can show that  $\sim p \rightarrow (r \wedge \sim r)$  is true. Proofs of this type are called proofs by contradiction.



# Example 4

Prove that  $\sqrt{2}$  is irrational.



# Example 4





Proof by contradiction can be used to prove conditional statements. In such proofs, we first assume the negation of the conclusion. We then use the premises of the theorem and the negation of the conclusion to arrive at a contradiction.



# Example 5

Give a proof by contradiction of the theorem “If  $3n + 2$  is odd, then  $n$  is odd.”



# Example 6

Show that if  $n$  is an integer and  $n^3 + 5$  is odd, then  $n$  is even using

- a) a proof by contraposition
- b) A proof by contradiction

# Example 6



# Example 7

Use a proof by contradiction to prove that the sum of an irrational number and a rational number is irrational.

