

REPUBLIC OF THE PHILIPPINES
POLYTECHNIC UNIVERSITY OF THE PHILIPPINES
STA. MESA, MANILA

COLLEGE OF ENGINEERING

COMPUTER ENGINEERING DEPARTMENT



CMPE 30043

DISCRETE MATHEMATICS

INSTRUCTIONAL MATERIAL

ENGR. JOSHUA BENJAMIN B. RODRIGUEZ

Table of Contents

Chapter 1: Set Theory	3
Chapter 2: Logic	22
Chapter 3: Relations	40
Chapter 4: Functions	60
Chapter 5: Combinatorics	82
Chapter 6: Introduction to Number Theory	100
Chapter 7: Graphs	115
Exercises	123

CHAPTER 1: SET THEORY

A set is a well – defined collection of objects of any kind; the nature of the objects is immaterial. The objects are called the elements or members of the set. Sets are denoted by capital letters A, B, C ..., X, Y, Z. The elements of a set are represented by lower case letters a, b, c, ... , x, y, z.

List Form

We list all the elements of a set, separated by commas and enclosed within braces or curly brackets{ }.

Examples: We write the sets in List Form

$A = \{1, 2, 3, 4, 5\}$ is the set of first five **Natural Numbers**.

$B = \{2, 4, 6, 8, \dots, 50\}$ is the set of **Even numbers** up to 50.

$C = \{1, 3, 5, 7, 9, \dots\}$ is the set of **positive odd numbers**.

Note: The symbol “...” is called an ellipsis. It is a short for “and so forth.”

Descriptive Form

We state the elements of a set in words.

Examples: Now we will write the above examples in the Descriptive Form.

$A =$ set of first five Natural Numbers. (Descriptive Form)

$B =$ set of positive even integers less or equal to fifty. (Descriptive Form)

$C =$ set of positive odd integers. (Descriptive Form)

Set Builder Form

We write the common characteristics in symbolic form, shared by all the elements of the set.

Examples: Now we will write the same examples which we write in Tabular as well as Descriptive Form, in Set Builder Form .

$A = \{x \in \mathbb{N} \mid x \leq 5\}$ (Set Builder Form)

$B = \{x \in \mathbb{E} \mid 0 < x \leq 50\}$ (Set Builder Form)

$C = \{x \in \mathbb{O} \mid 0 < x\}$ (Set Builder Form)

Sets of Numbers:

1. Set of Natural Numbers

$\mathbb{N} = \{1, 2, 3, \dots\}$

2. Set of Whole Numbers

$\mathbb{W} = \{0, 1, 2, 3, \dots\}$

3. Set of Integers

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, +1, +2, +3, \dots\}$
 $= \{0, \pm 1, \pm 2, \pm 3, \dots\}$

{“Z” stands for the first letter of the German word for integer: Zahlen}

4. Set of Even Integers

$$E = \{0, \pm 2, \pm 4, \pm 6, \dots\}$$

5. Set of Odd Integers

$$O = \{\pm 1, \pm 3, \pm 5, \dots\}$$

6. Set of Prime Numbers

$$P = \{2, 3, 5, 7, 11, 13, 17, 19, \dots\}$$

7. Set of Rational Numbers (or Quotient of Integers)

$$Q = \{x \mid x = p/q, p, q \in \mathbb{Z}, q \neq 0\}$$

8. Set of Irrational Numbers

$$Q' = \{x \mid x \text{ is not rational}\}$$

For example, $\sqrt{2}$, $\sqrt{3}$, π , e , etc.

9. Set of Real Numbers

$$R = Q \cup Q'$$

10. Set of Complex Numbers

$$C = \{z \mid z = x + iy; x, y \in R\} \text{ where, } i = \sqrt{-1}$$

Subset

If A & B are two sets, then A is called a subset of B. It is written as $A \subseteq B$. The set A is subset of B if and only if any element of A is also an element of B.

Symbolically: $A \subseteq B \Leftrightarrow \text{if } x \in A, \text{ then } x \in B$

Example:

Let

$$A = \{1, 3, 5\}$$

$$B = \{1, 2, 3, 4, 5\}$$

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

$$D = \{3, 1, 5\}$$

Then

$$A \subseteq B \text{ (Because every element of A is in B)}$$

$$C \subseteq B \text{ (Because every element of C is also an element of B)}$$

$A \subseteq D$ (Because every element of A is also an element of D and also note that every element of D is in A so $D \subseteq A$)

and A is not subset of C (Because there is an element 5 of A which is not in C)

Proper Subset

Let A and B be sets. A is a proper subset of B, if and only if, every element of A is in B but there is at least one element of B that is not in A, and is denoted as $A \subset B$.

Example:

$$\text{Let } A = \{1, 3, 5\} \quad B = \{1, 2, 3, 5\}$$

then $A \subset B$ (Because there is an element 2 of B which is not in A).

Equal Sets

Two sets A and B are equal if and only if every element of A is in B and every element of B is in A and is denoted $A = B$. Symbolically: $A = B$ iff $A \subseteq B$ and $B \subseteq A$

Example:

Let $A = \{1, 2, 3, 6\}$ $B =$ the set of positive divisors of 6
 $C = \{3, 1, 6, 2\}$ $D = \{1, 2, 2, 3, 6, 6, 6\}$

Then A, B, C, and D are all equal sets.

Null Set

A set which contains no element is called a null set, or an empty set or a void set. It is denoted by the Greek letter \emptyset (phi) or $\{\}$.

Example:

$A = \{x \mid x \text{ is a person taller than 10 feet}\} = \emptyset$
 (Because there does not exist any human being which is taller than 10 feet)
 $B = \{x \mid x^2 = 4, x \text{ is odd}\} = \emptyset$
 (Because we know that there does not exist any odd number whose square is 4)

Remarks: \emptyset is regarded as a subset of every set.

Example:

Determine whether each of the following statements is true or false.

- a. $x \in \{x\}$ **TRUE**
 (Because x is the member of the singleton set $\{x\}$)
- b. $\{x\} \subseteq \{x\}$ **TRUE**
 (Because Every set is the subset of itself)

Note that every Set has necessarily two subsets \emptyset and the Set itself. These two subset are known as Improper subsets and any other subset is called Proper Subset)

- c. $\{x\} \in \{x\}$ **FALSE**
 (Because $\{x\}$ is not the member of $\{x\}$) Similarly other
- d. $\{x\} \in \{\{x\}\}$ **TRUE**
- e. $\emptyset \subseteq \{x\}$ **TRUE**
- f. $\emptyset \in \{x\}$ **FALSE**

Universal Set

The set of all elements under consideration is called the Universal Set. The Universal Set is usually denoted by U.

Example:

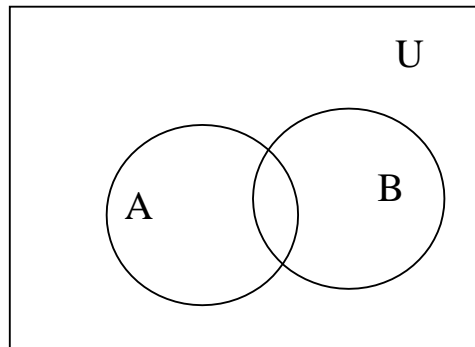
$A = \{2, 4, 6\}$ $B = \{1, 3, 5\}$
 Universal set: $U = \{1, 2, 3, 4, 5, 6\}$

Venn Diagram

A Venn diagram is a graphical representation of sets by regions in the plane. The Universal Set is represented by the interior of a rectangle, and the other sets are represented by disks lying within the rectangle.

Finite and Infinite Sets

A set S is said to be finite if it contains exactly m distinct elements where m denotes some non negative integer. In such case we write $|S| = m$ or $n(S) = m$. A set is said to be infinite if it is not finite.



Example:

1. The set S of letters of English alphabets is finite and $|S| = 26$
2. The null set \emptyset has no elements, is finite and $|\emptyset| = 0$
3. The set of positive integers $\{1, 2, 3, \dots\}$ is infinite.

Example:

Determine which of the following sets are finite/infinite.

- | | |
|---|-----------------|
| 1. $A = \{\text{month in the year}\}$ | FINITE |
| 2. $B = \{\text{even integers}\}$ | INFINITE |
| 3. $C = \{\text{positive integers less than 1}\}$ | FINITE |
| 4. $D = \{\text{animals living on the earth}\}$ | FINITE |
| 5. $E = \{\text{lines parallel to x-axis}\}$ | INFINITE |
| 6. $F = \{x \in \mathbb{R} \mid x^{100} + 29x^{50} - 1 = 0\}$ | FINITE |
| 7. $G = \{\text{circles through origin}\}$ | INFINITE |

Truth Table

A table displaying the membership of elements in sets. To indicate that an element is in a set, a 1 is used; to indicate that an element is not in a set, a 0 is used. Truth tables can be used to prove set identities.

A	A^c
1	0
0	1

The above table is the Truth table for Complement of A. Now in the above table note that if an element is the member of A, then it cannot be the Member of A^c thus where in the table we have 1 for A in that row we have 0 in A^c . Similarly, if an element is not a member of A, it will be the member of A^c . So we have 0 for A and 1 for A^c .

Union

Let A and B be subsets of a universal set U. The union of sets A and B is the set of all elements in U that belong to A or to B or to both, and is denoted $A \cup B$.

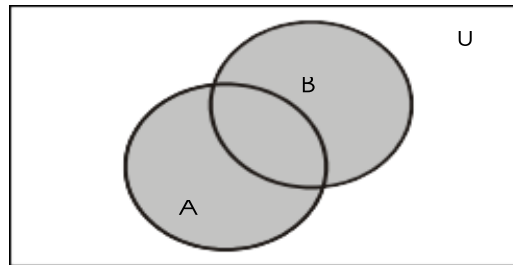
Symbolically: $A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$

Example:

Let $U = \{a, b, c, d, e, f, g\}$

$A = \{a, c, e, g\}$, $B = \{d, e, f, g\}$

Then $A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\} = \{a, c, d, e, f, g\}$

Venn Diagram for Union

$A \cup B$ is shaded

Remarks:

1. $A \cup B = B \cup A$

that is union is commutative you can prove this very easily only by using definition.

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

The above remark of subset is easily seen by the definition of union.

Truth Table for Union

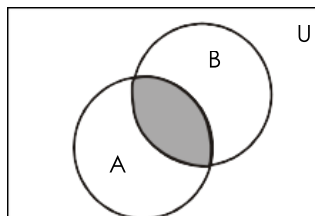
A	B	$A \cup B$
1	1	1
1	0	1
0	1	1
0	0	0

Intersection

Let A and B subsets of a universal set U. The intersection of sets A and B is the set of all elements in U that belong to both A and B and is denoted $A \cap B$.

Symbolically:

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

Venn Diagram for Intersection

$A \cap B$ is shaded

Example:

Let $U = \{a, b, c, d, e, f, g\}$

$A = \{a, c, e, g\}$, $B = \{d, e, f, g\}$

Then $A \cap B = \{e, g\}$

Remarks

1. $A \cap B = B \cap A$
2. $A \cap B \subseteq A$ and $A \cap B \subseteq B$
3. If $A \cap B = \phi$, then A & B are called disjoint sets.

Truth Table for Intersection

A	B	$A \cap B$
1	1	1
1	0	0
0	1	0
0	0	0

Difference

Let A and B be subsets of a universal set U. The difference of "A and B" (or relative complement of B in A) is the set of all elements in U that belong to A but not to B, and is denoted $A - B$ or $A \setminus B$.

Symbolically:

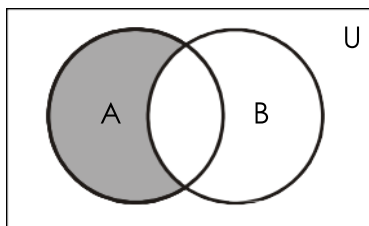
$$A - B = \{x \in U \mid x \in A \text{ and } x \notin B\}$$

Example

Let $U = \{a, b, c, d, e, f, g\}$

$A = \{a, c, e, g\}$, $B = \{d, e, f, g\}$

Then $A - B = \{a, c\}$

Venn Diagram for Set Difference

A-B is shaded

Remarks

1. $A - B \neq B - A$ that is Set difference is not commutative.
2. $A - B \subseteq A$
3. $A - B$, $A \cap B$ and $B - A$ are mutually disjoint sets.

Truth Table for Set Difference

A	B	$A - B$
1	1	0
1	0	1
0	1	0
0	0	0

Complement

Let A be a subset of universal set U . The complement of A is the set of allelement in U that do not belong to A , and is denoted A' or A^C .

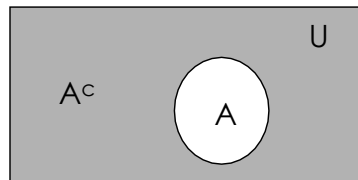
Symbolically: $A^C = \{x \in U \mid x \notin A\}$

Example

$U = \{a, b, c, d, e, f, g\}$ $A = \{a, c, e, g\}$

Then $A^C = \{b, d, f\}$

Venn Diagram for Complement



A^C is shaded

REMARK :

1. $A^C = U - A$
2. $A \cap A^C = \phi$
3. $A \cup A^C = U$

Truth Table for Complement

A	A^C
1	0
0	1

Example

Let $U = \{1, 2, 3, \dots, 10\}$

$X = \{1, 2, 3, 4, 5\}$

$Y = \{y \mid y = 2x, x \in X\}$

$Z = \{z \mid z^2 - 9z + 14 = 0\}$

Enumerate:

(1) $X \cap Y$

(4) Y^C

(2) $Y \cup Z$

(5) $X^C - Z^C$

(3) $X - Z$

(6) $(X - Z)^C$

Firstly, we enumerate the given sets.

$$U = \{1, 2, 3, \dots, 10\},$$

$$X = \{1, 2, 3, 4, 5\}$$

$$Y = \{y \mid y = 2x, x \in X\} = \{2, 4, 6, 8, 10\}$$

$$Z = \{z \mid z^2 - 9z + 14 = 0\} = \{2, 7\}$$

$$(1) X \cap Y = \{1, 2, 3, 4, 5\} \cap \{2, 4, 6, 8, 10\} = \{2, 4\}$$

$$(2) Y \cup Z = \{2, 4, 6, 8, 10\} \cup \{2, 7\} = \{2, 4, 6, 7, 8, 10\}$$

$$(3) X - Z = \{1, 2, 3, 4, 5\} - \{2, 7\} = \{1, 3, 4, 5\}$$

$$(4) Y^c = U - Y = \{1, 2, 3, \dots, 10\} - \{2, 4, 6, 8, 10\} = \{1, 3, 5, 7, 9\}$$

$$(5) X^c = \{6, 7, 8, 9, 10\}, Z^c = \{1, 3, 4, 5, 6, 8, 9, 10\}$$

$$X^c - Z^c = \{6, 7, 8, 9, 10\} - \{1, 3, 4, 5, 6, 8, 9, 10\} = \{7\}$$

$$(6) (X - Z)^c = U - (X - Z) = \{1, 2, 3, \dots, 10\} - \{1, 3, 4, 5\} = \{2, 6, 7, 8, 9, 10\}$$

Note: $(X - Z)^c \neq X^c - Z^c$

Example

Given the following universal set U and its two subsets P and Q , where

$$U = \{x \mid x \in \mathbb{Z}, 0 \leq x \leq 10\}$$

$$P = \{x \mid x \text{ is a prime number}\}$$

$$Q = \{x \mid x^2 < 70\}$$

- (i) Draw a Venn diagram for the above
- (ii) List the elements in $P^c \cap Q$

Solution:

First we write the sets in List form.

$$U = \{x \mid x \in \mathbb{Z}, 0 \leq x \leq 10\}$$

Since it is the set of integers that are greater than or equal 0 and less or equal to 10. So we have $U = \{0, 1, 2, 3, \dots, 10\}$

$$P = \{x \mid x \text{ is a prime number}\}$$

It is the set of prime numbers between 0 and 10. Remember Prime numbers are those numbers which have only two distinct divisors. $P = \{2, 3, 5, 7\}$

$$Q = \{x \mid x^2 < 70\}$$

The set Q contains the elements between 0 and 10 which have their square less or equal to 70. $Q = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

Venn Diagram

$$P^c \cap Q = ?$$

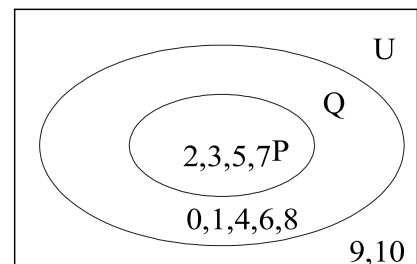
$$P^c = U - P = \{0, 1, 2, 3, \dots, 10\} - \{2, 3, 5, 7\}$$

$$= \{0, 1, 4, 6, 8, 9, 10\}$$

and

$$P^c \cap Q = \{0, 1, 4, 6, 8, 9, 10\} \cap \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

$$= \{0, 1, 4, 6, 8\}$$



Example

Let $U = \{1, 2, 3, 4, 5\}$, $C = \{1, 3\}$

and A and B are non empty sets. Find A in each of the following:

- (i) $A \cup B = U$, $A \cap B = \phi$ and $B = \{1\}$
- (ii) $A \subset B$ and $A \cup B = \{4, 5\}$
- (iii) $A \cap B = \{3\}$, $A \cup B = \{2, 3, 4\}$ and $B \cup C = \{1, 2, 3\}$
- (iv) A and B are disjoint, B and C are disjoint, and the union of A and B is the set $\{1, 2\}$.

(i) $A \cup B = U$, $A \cap B = \phi$ and $B = \{1\}$

Solution

Since $A \cup B = U = \{1, 2, 3, 4, 5\}$ and $A \cap B = \phi$,

Therefore $A = B^c = \{1\}^c = \{2, 3, 4, 5\}$

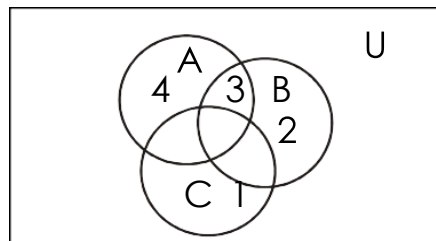
(ii) $A \subset B$ and $A \cup B = \{4, 5\}$ also $C = \{1, 3\}$

Solution

When $A \subset B$, then $A \cup B = B = \{4, 5\}$

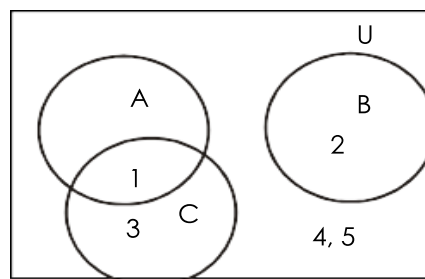
Also A being a proper subset of B implies $A = \{4\}$ or $A = \{5\}$

(iii) $A \cap B = \{3\}$, $A \cup B = \{2, 3, 4\}$ and $B \cup C = \{1, 2, 3\}$ also $C = \{1, 3\}$

Solution

Since we have 3 in the intersection of A and B as well as in C so we place 3 in common part shared by the three sets in the Venn diagram. Now since 1 is in the union of B and C it means that 1 may be in C or may be in B , but 1 cannot be in B because if 1 is in the B then it must be in $A \cup B$ but 1 is not there, thus we place 1 in the part of C which is not shared by any other set. Same is the reason for 4 and we place it in the set which is not shared by any other set. Now 2 will be in B , 2 cannot be in A because $A \cap B = \{3\}$, and is not in C . So $B = \{2, 3\}$ and $A = \{3, 4\}$.

(iv) $A \cap B = \phi$, $B \cap C = \phi$, $A \cup B = \{1, 2\}$. Also $C = \{1, 3\}$

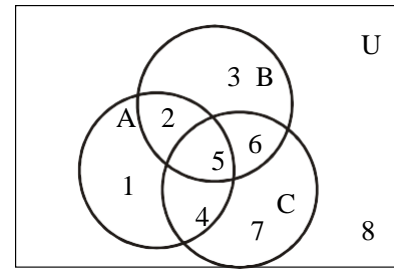
Solution

Therefore, $A = \{1\}$

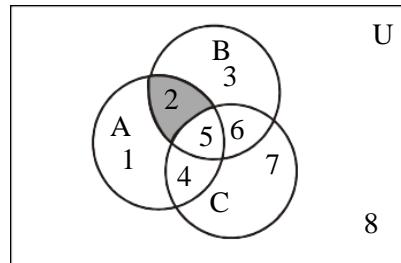
Example

Use a Venn diagram to represent the following:

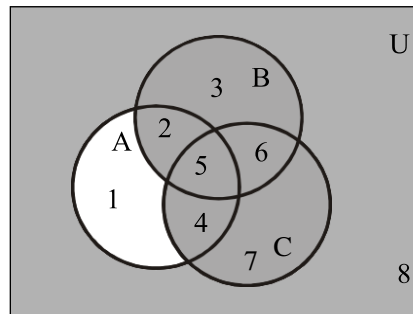
- (i) $(A \cap B) \cap C^c$
- (ii) $A^c \cup (B \cup C)$
- (iii) $(A - B) \cap C$
- (iv) $(A \cap B^c) \cup C^c$

**Solution**

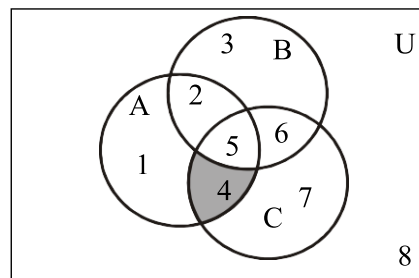
(i) $(A \cap B) \cap C^c$ is shaded



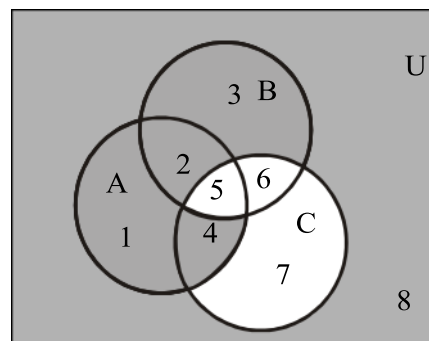
(ii) $A^c \cup (B \cup C)$ is shaded



(iii) $(A - B) \cap C$ is shaded



(iv) $(A \cap B^c) \cup C^c$ is shaded



Example: Proving Set Identities by Truth Table

Prove the following using Truth Table:

(i) $A - (A - B) = A \cap B$

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

(iii) $A - B = A \cap B^c$

Solution:

i.) $A - (A - B) = A \cap B$

A	B	A - B	A - (A - B)	A ∩ B
1	1	0	1	1
1	0	1	0	0
0	1	0	0	0
0	0	0	0	0

Since the last two columns of the above table are same hence the corresponding set expressions are same. That is **$A - (A - B) = A \cap B$** .

ii.) $(A \cap B)^c = A^c \cup B^c$

A	B	A ∩ B	(A ∩ B) ^c	A ^c	B ^c	A ^c ∪ B ^c
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

Since the fourth and last columns of the above table are same hence the corresponding set expressions are same. That is **$(A \cap B)^c = A^c \cup B^c$** .

iii.) $A - B = A \cap B^c$

A	B	A - B	B ^c	A ∩ B ^c
1	1	0	0	0
1	0	1	1	1
0	1	0	0	0
0	0	0	1	0

Since the third and last columns of the above table are same hence the corresponding set expressions are same. That is **$A - B = A \cap B^c$** .

SET IDENTITIES

Let A, B, C be subsets of a universal set U .

1. Idempotent Laws
 - a. $A \cup A = A$
 - b. $A \cap A = A$
2. Commutative Laws
 - a. $A \cup B = B \cup A$
 - b. $A \cap B = B \cap A$
3. Associative Laws
 - a. $A \cup (B \cap C) = (A \cup B) \cap C$
 - b. $A \cap (B \cup C) = (A \cap B) \cup C$
4. Distributive Laws
 - a. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
 - b. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
5. Identity Laws
 - a. $A \cup \emptyset = A$
 - b. $A \cap \emptyset = \emptyset$
 - c. $A \cup U = U$
 - d. $A \cap U = A$
6. Complement Laws
 - a. $A \cup A^c = U$
 - b. $A \cap A^c = \emptyset$
 - c. $U^c = \emptyset$
 - d. $\emptyset^c = U$
7. Double Complement Law

$(A^c)^c = A$
8. DeMorgan's Laws
 - a. $(A \cup B)^c = A^c \cap B^c$
 - b. $(A \cap B)^c = A^c \cup B^c$
9. Alternative Representation for Set Difference

$A - B = A \cap B^c$
10. Subset Laws
 - a. $A \cup B \subseteq C$ iff $A \subseteq C$ and $B \subseteq C$
 - b. $C \subseteq A \cap B$ iff $C \subseteq A$ and $C \subseteq B$
11. Absorption Laws
 - a. $A \cup (A \cap B) = A$
 - b. $A \cap (A \cup B) = A$

Example

1. $A \subseteq A \cup B$
2. $A - B \subseteq A$
3. If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$
4. $A \subseteq B$ if, and only if, $B^c \subseteq A^c$

1. Prove that $A \subseteq A \cup B$

Solution

Here in order to prove the identity you should remember the definition of Subset of a set. We will take the arbitrary element of a set then show that, that element is the member of the other, then the first set is the subset of the other. So

Let x be an arbitrary element of A , that is $x \in A$.

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

But x is an arbitrary element of A .

$$\therefore \mathbf{A \subseteq A \cup B} \quad (\text{proved})$$

2. Prove that $A - B \subseteq A$

Solution

Let $x \in A - B$
 $\Rightarrow x \in A$ and $x \notin B$ (by definition of $A - B$)
 $\Rightarrow x \in A$ (in particular)

But x is an arbitrary element of $A - B$
 $\therefore A - B \subseteq A$ (proved)

3. Prove that if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$

Solution

Suppose that $A \subseteq B$ and $B \subseteq C$.
 Consider $x \in A$
 $\Rightarrow x \in B$ (as $A \subseteq B$)
 $\Rightarrow x \in C$ (as $B \subseteq C$)

But x is an arbitrary element of A
 $\therefore A \subseteq C$ (proved)

4. Prove that $A \subseteq B$ iff $B^c \subseteq A^c$

Solution

Suppose $A \subseteq B$ {To prove $B^c \subseteq A^c$ }
 Let $x \in B^c$
 $\Rightarrow x \notin B$ (by definition of B^c)
 $\Rightarrow x \notin A$
 $\Rightarrow x \in A^c$ (by definition of A^c)

Now we know that implication and its contrapositivity are logically equivalent and the contrapositive statement of if $x \in A$ then $x \in B$ is: if $x \notin B$ then $x \notin A$ which is the definition of the $A \subseteq B$. Thus if we show for any two sets A and B , if $x \notin B$ then $x \notin A$ it means that $A \subseteq B$. Hence

But x is an arbitrary element of B^c
 $\therefore B^c \subseteq A^c$

Conversely,
 Suppose $B^c \subseteq A^c$ {To prove $A \subseteq B$ }

Let $x \in A$
 $\Rightarrow x \notin A^c$ (by definition of A^c)
 $\Rightarrow x \notin B^c$ ($\because B^c \subseteq A^c$)
 $\Rightarrow x \in B$ (by definition of B^c)
 But x is an arbitrary element of A .
 $\therefore A \subseteq B$ (proved)

Example

Let A and B be subsets of a universal set U . Prove that $A - B = A \cap B^c$.

Solution

Let $x \in A - B$

$\Rightarrow x \in A$ and $x \notin B$ (definition of set difference)

$\Rightarrow x \in A$ and $x \in B^c$ (definition of complement)

$\Rightarrow x \in A \cap B^c$ (definition of intersection)

But x is an arbitrary element of $A - B$ so we can write

$$\therefore A - B \subseteq A \cap B^c$$

Conversely, let $y \in A \cap B^c$

$\Rightarrow y \in A$ and $y \in B^c$ (definition of intersection)

$\Rightarrow y \in A$ and $y \notin B$ (definition of complement)

$\Rightarrow y \in A - B$ (definition of set difference)

But y is an arbitrary element of $A \cap B^c$

$$\therefore A \cap B^c \subseteq A - B$$

It follows that $A - B = A \cap B^c$

Example

Prove the DeMorgan's Law: $(A \cup B)^c = A^c \cap B^c$

Proof

Let $x \in (A \cup B)^c$

$\Rightarrow x \notin A \cup B$ (definition of complement)

$\Rightarrow x \notin A$ and $x \notin B$ (DeMorgan's Law of Logic)

$\Rightarrow x \in A^c$ and $x \in B^c$ (definition of complement)

$\Rightarrow x \in A^c \cap B^c$ (definition of intersection)

But x is an arbitrary element of $(A \cup B)^c$ so we have proved that

$$\therefore (A \cup B)^c \subseteq A^c \cap B^c$$

Conversely, let $y \in A^c \cap B^c$

$\Rightarrow y \in A^c$ and $y \in B^c$ (definition of intersection)

$\Rightarrow y \notin A$ and $y \notin B$ (definition of complement)

$\Rightarrow y \notin A \cup B$ (DeMorgan's Law of Logic)

$\Rightarrow y \in (A \cup B)^c$ (definition of complement)

But y is an arbitrary element of $A^c \cap B^c$

$$\therefore A^c \cap B^c \subseteq (A \cup B)^c$$

It follows that $(A \cup B)^c = A^c \cap B^c$

Example

Prove the associative law: $A \cap (B \cap C) = (A \cap B) \cap C$

Proof

Consider $x \in A \cap (B \cap C)$
 $\Rightarrow x \in A$ and $x \in B \cap C$ (definition of intersection)
 $\Rightarrow x \in A$ and $x \in B$ and $x \in C$ (definition of intersection)
 $\Rightarrow x \in A \cap B$ and $x \in C$ (definition of intersection)
 $\Rightarrow x \in (A \cap B) \cap C$ (definition of intersection)

But x is an arbitrary element of $A \cap (B \cap C)$

$$\therefore A \cap (B \cap C) \subseteq (A \cap B) \cap C$$

Conversely

let $y \in (A \cap B) \cap C$
 $\Rightarrow y \in A \cap B$ and $y \in C$ (definition of intersection)
 $\Rightarrow y \in A$ and $y \in B$ and $y \in C$ (definition of intersection)
 $\Rightarrow y \in A$ and $y \in B \cap C$ (definition of intersection)
 $\Rightarrow y \in A \cap (B \cap C)$ (definition of intersection)

But y is an arbitrary element of $(A \cap B) \cap C$

$$\therefore (A \cap B) \cap C \subseteq A \cap (B \cap C)$$

It follows that $A \cap (B \cap C) = (A \cap B) \cap C$

Example

For all subsets A and B of a universal set U , prove that $(A - B) \cup (A \cap B) = A$ using set identities.

Proof

$= (A - B) \cup (A \cap B)$	
$= (A \cap B^c) \cup (A \cap B)$	Alternative representation for set difference
$= A \cap (B^c \cup B)$	Distributive Law
$= A \cap U$	Complement Law
$= A$	Identity Law

Example

For any two sets A and B prove that $A - (A - B) = A \cap B$

Solution

$= A - (A - B)$	
$= A - (A \cap B^c)$	Alternative representation for set difference
$= A \cap (A \cap B^c)^c$	Alternative representation for set difference
$= A \cap (A^c \cup (B^c)^c)$	DeMorgan's Law
$= A \cap (A^c \cup B)$	Double Complement Law
$= (A \cap A^c) \cup (A \cap B)$	Distributive Law
$= \emptyset \cup (A \cap B)$	Complement Law
$= A \cap B$	Identity Law

Example

For all set A, B, and C prove that $(A - B) - C = (A - C) - B$

Solution

$= (A - B) - C$	
$= (A \cap B^c) - C$	Alternative representation of set difference
$= (A \cap B^c) \cap C^c$	Alternative representation of set difference
$= A \cap (B^c \cap C^c)$	Associative Law
$= A \cap (C^c \cap B^c)$	Commutative Law
$= (A \cap C^c) \cap B^c$	Associative Law
$= (A - C) \cap B^c$	Alternative representation of set difference
$= (A - C) - B$	Alternative representation of set difference

Example

Simplify $(B^c \cup (B^c - A))^c$

Solution

$= (B^c \cup (B^c \cap A^c))^c$	Alternative representation for set difference
$= (B^c)^c \cap (B^c \cap A^c)^c$	DeMorgan's Law
$= B \cap ((B^c)^c \cup (A^c)^c)$	DeMorgan's Law
$= B \cap (B \cup A)$	Double Complement Law
$= B$	Absorption Law

Example

For any sets A and B if $A \subseteq B$ then prove $A \cap B = A$

Solution

Let $x \in A \cap B$
 $\Rightarrow x \in A$ and $x \in B$
 $\Rightarrow x \in A$ (in particular)
 Hence $A \cap B \subseteq A$

Conversely,

let $x \in A$.

Then $x \in B$ (since $A \subseteq B$)

Now $x \in A$ and $x \in B$, therefore $x \in A \cap B$

Hence, $A \subseteq A \cap B$

It follows that $A = A \cap B$

APPLICATIONS OF VENN DIAGRAMS

Example

A number of computer users are surveyed to find out if they have a printer, modem or scanner. Draw separate Venn diagrams and shade the areas, which represent the following configurations.

1. modem and printer but no scanner
2. scanner but no printer and no modem
3. scanner or printer but no modem.
4. no modem and no printer

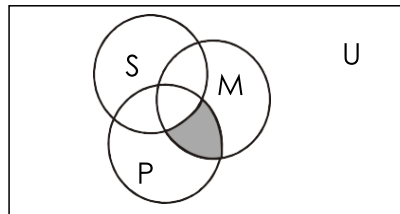
Solution

Let: **P** represent the set of computer users having printer.

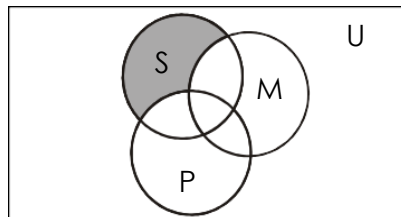
M represent the set of computer users having modem.

S represent the set of computer users having scanner.

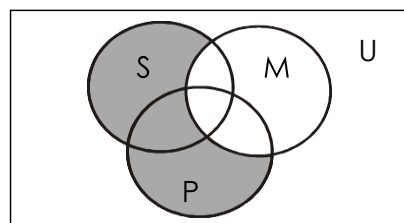
For (1) Modem and printer but no Scanner is shaded.



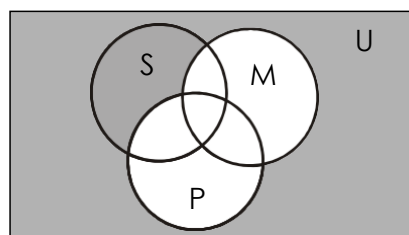
For (2) Scanner but no printer and no modem is shaded.



For (3) Scanner or printer but no modem is shaded.



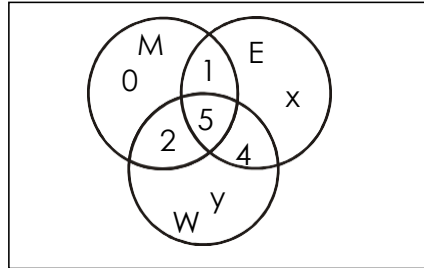
For (4) No modem and no printer is shaded.



Example

Of 21 typists in an office, 5 use all manual typewriters (M), electronic typewriters (E) and word processors (W); 9 use E and W; 7 use M and W; 6 use M and E; but no one uses M only.

- (i) Represent this information in a Venn Diagram.
- (ii) If the same number of typists use electronic as use word processors, then
 - (a) How many use word processors only,
 - (b) How many use electronic typewriters?

Solution (i)**Solution (ii-a)**

Let the number of typists using electronic typewriters (E) only be x , and the number of typists using word processors (W) only be y .

Total number of typists using E = Total Number of typists using W

$$1 + 5 + 4 + x = 2 + 5 + 4 + y$$

$$\text{or, } x - y = 1 \quad (1)$$

Also, total number of typists = 21

$$\Rightarrow 0 + x + y + 1 + 2 + 4 + 5 = 21$$

$$\text{or, } x + y = 9 \quad (2)$$

Solving (1) & (2), we get

$$x = 5, y = 4$$

\therefore Number of typists using word processor only is $y = 4$

Solution (ii-a) How many typists use electronic typewriters?

Typists using electronic typewriters = No. of elements in E

$$= 1 + 5 + 4 + x$$

$$= 1 + 5 + 4 + 5$$

$$= 15$$

Example

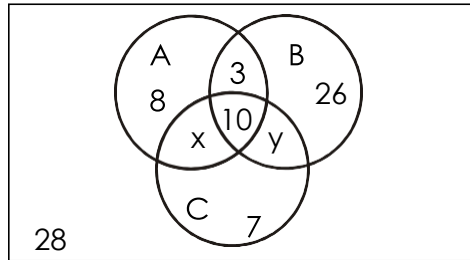
In a school, 100 students have access to three software packages, A, B and C. 28 did not use any software, 8 used only package A, 26 used only package B, 7 used only package C, 10 used all three packages, 13 used both A and B.

- (i) Draw a Venn diagram with all sets enumerated as far as possible. Label the two subsets which cannot be enumerated as x and y , in any order.

- (ii) If twice as many students used package B as package A, write down a pair of simultaneous equations in x and y .
- (iii) Solve these equations to find x and y .
- (iv) How many students used package C?

Solution (i)

Venn Diagram with all sets enumerated



Solution (ii)

We are given that

Number of students using package B = 2 (Number of students using package A)

Now the number of students which used package B and A are clear from the diagrams given below. So we have the following equation

$$\begin{aligned} \Rightarrow 3 + 10 + 26 + y &= 2(8 + 3 + 10 + x) \\ \Rightarrow 39 + y &= 42 + 2x \\ \text{or } y &= 2x + 3 \end{aligned} \quad (1)$$

$$\begin{aligned} \text{Also, total number of students} &= 100. \\ \text{Hence, } 8 + 3 + 26 + 10 + 7 + 28 + x + y &= 100 \\ \text{or } 82 + x + y &= 100 \\ \text{or } x + y &= 18 \end{aligned} \quad (2)$$

Solution (iii)

$$\begin{aligned} y &= 2x + 3 & (1) \\ x + y &= 18 & (2) \end{aligned}$$

Using (1) in (2), we get,

$$x + (2x + 3) = 18$$

$$\text{or } 3x = 15$$

$$x = 5 \text{ and using (1) or (2) we solve } y = 13$$

Solution (iv)

No. of students using package C

$$= x + y + 10 + 7$$

$$= 5 + 13 + 10 + 7$$

$$= 35$$

CHAPTER 2: LOGIC

Logic is an art or science of correct or valid reasoning.

Propositions and Truth Values

A **proposition** is any simple (also called **atomic**) declarative statement that is either true or false, yes or no, 1 or 0 but not both. We shall assign to each statement exactly one of two values – **true** (symbolized by “**T**”), or **false** (symbolized by “**F**”).

Example

Propositions

- 1) Grass is green.
- 2) $4 + 2 = 7$
- 3) There are four fingers in a hand

Not Propositions

- 1) Close the door
- 2) x is greater than 2
- 3) He is very rich

Logical Connectives and Truth Tables

There are five basic or fundamental connectives in symbolic logic. It combines two or more propositions into a single proposition. The following table summarizes their names and symbols.

Simple	Compound	Symbol	Name
P	not P	$\sim P$	Negation
P, Q	P or Q	$P \vee Q$	Disjunction
P, Q	P and Q	$P \wedge Q$	Conjunction
P, Q	If P, then Q	$P \rightarrow Q$	Conditional
P, Q	P if and only if Q	$P \leftrightarrow Q$	Biconditional

Truth Table

A **truth table** is a case table in which **T** represents “**true**” and **F** represents “**false**” that provides definition of any propositional logic. Following are truth tables for the five fundamental compound statements.

P	Q	$P \vee Q$	$P \wedge Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
F	F	F	F	T	T
F	T	T	F	T	F
T	F	T	F	F	F
T	T	T	T	T	T

P	$\sim P$
F	T
T	F

Example

p = “Manila is the capital of Philippines”

q = “17 is divisible by 3”

$p \wedge q$ = “Manila is the capital of Philippines and 17 is divisible by 3”

$p \vee q$ = “Manila is the capital of Philippines or 17 is divisible by 3”

$\sim p$ = “It is not the case that Manila is the capital of Philippines” or simply “Manila is the not the capital of Philippines”

Translating from English to Symbols

Example

Let p = "It is hot", and q = "It is sunny"

Sentence

1. It is not hot.
2. It is hot and sunny.
3. It is hot or sunny.
4. It is not hot but sunny.
5. It is neither hot nor sunny.

Symbolic Form

- $\sim p$
- $p \wedge q$
- $p \vee q$
- $\sim p \wedge q$
- $\sim p \wedge \sim q$

Example

Let h = "Zia is healthy" w = "Zia is wealthy" s = "Zia is wise"

Translate the compound statements to symbolic form:

- 1) Zia is healthy and wealthy but not wise. $(h \wedge w) \wedge (\sim s)$
- 2) Zia is not wealthy but he is healthy and wise. $\sim w \wedge (h \wedge s)$
- 3) Zia is neither healthy, wealthy nor wise. $\sim h \wedge \sim w \wedge \sim s$

Translating from English to Symbols

Example

Let m = "Master is good in Mathematics"
 c = "Master is a Computer Science student"

Translate the following statement forms into plain English:

- 1) $\sim c$ Master is not a Computer Science student
- 2) $c \vee m$ Master is a Computer Science student or good in Maths.
- 3) $m \wedge \sim c$ Master is good in Maths but not a Computer Science student

Exclusive OR

When OR is used in its exclusive sense, The statement " p or q " means " p or q but not both" or " p or q and not p and q " which translates into symbols as $(p \vee q) \wedge \sim (p \wedge q)$. It is abbreviated as $p \oplus q$ or p XOR q

Truth Table for Exclusive Or

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Note: Basically

$$\begin{aligned}
 p \oplus q &\equiv (p \wedge \sim q) \vee (\sim p \wedge q) \\
 &\equiv [p \wedge \sim q] \vee \sim p \wedge [(p \wedge \sim q) \vee q] \\
 &\equiv (p \vee q) \wedge \sim (p \wedge q) \\
 &\equiv (p \vee q) \wedge (\sim p \vee \sim q)
 \end{aligned}$$

Truth Table for $(p \vee q) \wedge \sim (p \wedge q)$

p	q	$p \vee q$	$p \wedge q$	$\sim (p \wedge q)$	$(p \vee q) \wedge \sim (p \wedge q)$
T	T	T	T	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	F	T	F

Tautologies, Contradictions and Contingencies

A compound proposition (or compound statement) that is true for all possible truth values of its constituent propositional variables is called a **tautology**. A compound proposition that is false for all possible truth values of its constituent propositional variables is called a **contradiction**. A compound proposition that is neither a tautology nor a contradiction – whose truth tables exhibit some T and some F entries – is called a **contingency**. We shall denote a tautology by t and a contradiction by f.

Example

Use truth table to show that $(p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$ is a tautology

Solution

Since we have to show that the given statement form is Tautology, so the column of the above proposition in the truth table will have all entries as T. As clear from the table below

p	q	$p \wedge q$	$\sim p$	$\sim q$	$p \wedge \sim q$	$\sim p \vee (p \wedge \sim q)$	$(p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$
T	T	T	F	F	F	F	T
T	F	F	F	T	T	T	T
F	T	F	T	F	F	T	T
F	F	F	T	T	F	T	T

Hence $(p \wedge q) \vee (\sim p \vee (p \wedge \sim q)) \equiv t$

Example

Use truth table to show that $(p \wedge \sim q) \wedge (\sim p \vee q)$ is a contradiction

Solution

Since we have to show that the given statement form is Contradiction, so its column in the truth table will have all entries as F. As clear from the table below.

p	q	$\sim q$	$p \wedge \sim q$	$\sim p$	$\sim p \vee q$	$(p \wedge \sim q) \wedge (\sim p \vee q)$
T	T	F	F	F	T	F
T	F	T	T	F	F	F
F	T	F	F	T	T	F
F	F	T	F	T	T	F

Logical Equivalence and Logical Implications

Suppose that the compound propositions P and Q are made up of the atomic propositions $p_1, p_2, p_3, \dots, p_n$ and $q_1, q_2, q_3, \dots, q_n$ respectively. We say that P and Q are **logically equivalent** and write $P \equiv Q$ if $P \leftrightarrow Q$ is a **tautology**. Similarly, if $P \rightarrow Q$ is a tautology then P is said to **tautologically imply** Q.

Example

Prove the logical implication $(P \wedge Q) \rightarrow Q$

Solution

p	q	$p \wedge q$	$(p \wedge q) \rightarrow q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

Example

Show that $P \leftrightarrow Q$ and $(P \rightarrow Q) \wedge (Q \rightarrow P)$ are logically equivalent

Solution

p	q	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$	$p \leftrightarrow q$	$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$
T	T	T	T	T	T	T
T	F	F	T	F	F	T
F	T	T	F	F	F	T
F	F	T	T	T	T	T

THE ALGEBRA OF PROPOSITIONS

The rules of replacement tell us that any logically equivalent expressions can replace each other wherever they occur. Let P, Q and R represent propositions. The rules of replacement are as follows

RULES OF REPLACEMENT						
1.	Idempotence					
	A.	$P \vee P \equiv P$	B.	$P \wedge P \equiv P$		
2.	Commutativity					
	A.	$P \vee Q \equiv Q \vee P$	B.	$P \wedge Q \equiv Q \wedge P$		
3.	Associativity					
	A.	$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$	B.	$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$		
4.	Distributivity					
	A.	$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$				
	B.	$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$				
5.	Double Negation					
	A.	$\sim(\sim P) \equiv P$				
6.	De Morgan's Law					
	A.	$\sim(P \vee Q) \equiv \sim P \wedge \sim Q$	B.	$\sim(P \wedge Q) \equiv \sim P \vee \sim Q$		
7.	Implication					
	A.	$P \rightarrow Q \equiv \sim P \vee Q$				
8.	Equivalence					
	A.	$P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$				
9.	Exportation					
	A.	$[(P \wedge Q) \rightarrow R] \equiv [P \rightarrow (Q \rightarrow R)]$				
10.	Absurdity					
	A.	$[P \rightarrow (Q \wedge \sim Q)] \equiv \sim P$				
11.	Contrapositive					
	A.	$P \rightarrow Q \equiv \sim Q \rightarrow \sim P$				
12.	Absorption					
	A.	$P \wedge (P \vee Q) \equiv P$	B.	$P \vee (P \wedge Q) \equiv P$		
13.	Identity					
	A.	$P \vee T \equiv T$	B.	$P \wedge T \equiv P$	C.	
		$P \vee F \equiv P$		$P \wedge F \equiv F$		$\sim T \equiv F$
		$P \vee \sim P \equiv T$		$P \wedge \sim P \equiv F$		$\sim F \equiv T$

Example

Simplify the statement form $p \vee [\sim(\sim p \wedge q)]$

Solution

$$\begin{aligned}
 p \vee [\sim(\sim p \wedge q)] &\equiv p \vee [\sim(\sim p) \vee (\sim q)] \\
 &\equiv p \vee [p \vee (\sim q)] \\
 &\equiv [p \vee p] \vee (\sim q) \\
 &\equiv p \vee (\sim q)
 \end{aligned}$$

DeMorgan's Law

Double Negative Law: $\sim(\sim p) \equiv p$

Associative Law for \vee

Idempotent Law: $p \vee p \equiv p$

Example

Using Laws of Logic, verify the logical equivalence $\sim (\sim p \wedge q) \wedge (p \vee q) \equiv p$

Solution

$$\begin{aligned}
 \sim (\sim p \wedge q) \wedge (p \vee q) &\equiv (\sim (\sim p) \vee \sim q) \wedge (p \vee q) && \text{DeMorgan's Law} \\
 &\equiv (p \vee \sim q) \wedge (p \vee q) && \text{Double Negative Law} \\
 &\equiv p \vee (\sim q \wedge q) && \text{Distributive Law} \\
 &\equiv p \vee f && \text{Negation Law} \\
 &\equiv p && \text{Identity Law}
 \end{aligned}$$

Simplifying a Statement

Example

"You will get an A if you are hardworking and the sun shines, or you are hardworking and it rains." Rephrase the condition more simply.

Solution

Let p = "You are hardworking" q = "The sun shines" r = "It rains" .

The condition is $(p \wedge q) \vee (p \wedge r)$

Using distributive law in reverse,

$$(p \wedge q) \vee (p \wedge r) \equiv p \wedge (q \vee r)$$

Putting $p \wedge (q \vee r)$ back into English, we can rephrase the given sentence as

"You will get an A if you are hardworking and the sun shines or it rains"

Example

Use Logical Equivalence to rewrite each of the following sentences more simply.

1. It is not true that I am tired and you are smart.

{I am not tired or you are not smart.}

2. It is not true that I am tired or you are smart.

{I am not tired and you are not smart.}

3. I forgot my pen or my bag and I forgot my pen or my glasses.

{I forgot my pen or I forgot my bag and glasses.}

4. It is raining and I have forgotten my umbrella, or it is raining and I have forgotten my hat.

{It is raining and I have forgotten my umbrella or my hat.}

Conditional Statements

Consider the statement:

"If you earn an A in Math, then I'll buy you a computer."

This statement is made up of two simpler statements:

p : "You earn an A in Math"

q : "I will buy you a computer."

The original statement is then saying :

If p is true, then q is true, or, more simply, **if p , then q .**

We can also phrase this as p **implies** q . It is denoted by $p \rightarrow q$.

Example

Determine the truth value of each of the following conditional statements:

- | | |
|--|--------------|
| 1. "If $1 = 1$, then $3 = 3$." | TRUE |
| 2. "If $1 = 1$, then $2 = 3$." | FALSE |
| 3. "If $1 = 0$, then $3 = 3$." | TRUE |
| 4. "If $1 = 2$, then $2 = 3$." | TRUE |
| 5. "If $1 = 1$, then $1 = 2$ and $2 = 3$." | FALSE |
| 6. "If $1 = 3$ or $1 = 2$ then $3 = 3$." | TRUE |

Alternative ways of expressing implications

The implication $p \rightarrow q$ could be expressed in many alternative ways as:

- | | |
|---------------------------|--------------------------|
| • "if p, q" | • "not p unless q" |
| • "p implies q" | • "q follows from p" |
| • "p only if q" | • "q if p" |
| • "p is sufficient for q" | • "q whenever p" |
| • "q provided that p" | • "q is necessary for p" |

Example

Write the following statements in the form "if p, then q" in English.

- a) Your guarantee is good only if you bought your CD less than 90 days ago.

If your guarantee is good, then you must have bought your CD player less than 90 days ago.

- b) To get tenure as a professor, it is sufficient to be world-famous.

If you are world-famous, then you will get tenure as a professor.

- c) That you get the job implies that you have the best credentials.

If you get the job, then you have the best credentials.

- d) It is necessary to walk 8 miles to get to the top of the Peak.

If you get to the top of the peak, then you must have walked 8 miles.

Translating English sentences to symbols**Example**

Let p and q be propositions:

p = "you get an A on the final exam"

q = "you do every exercise in this book"

r = "you get an A in this class"

Write the following propositions using p, q, and r and logical connectives.

1. To get an A in this class it is necessary for you to get an A on the final.

Solution $p \rightarrow r$

2. You do every exercise in this book; You get an A on the final, implies, you get an A in the class.

Solution $p \wedge q \rightarrow r$

3. Getting an A on the final and doing every exercise in this book is sufficient For getting an A in this class.

Solution $p \wedge q \rightarrow r$

Translating symbolic propositions to English

Example

Let p , q , and r be the propositions:

p = "you have the flu"

q = "you miss the final exam"

r = "you pass the course"

Express the following propositions as an English sentence.

1. $p \rightarrow q$

If you have flu, then you will miss the final exam.

2. $\sim q \rightarrow r$

If you don't miss the final exam, you will pass the course.

3. $\sim p \wedge \sim q \rightarrow r$

If you neither have flu nor miss the final exam, then you will pass the course.

Example

Construct a truth table for the statement form $(p \vee \sim q) \rightarrow \sim p$

Solution

p	q	$\sim q$	$\sim p$	$p \vee \sim q$	$p \vee \sim q \rightarrow \sim p$
T	T	F	F	T	F
T	F	T	F	T	F
F	T	F	T	F	T
F	F	T	T	T	T

Example

Construct a truth table for the statement form $(p \rightarrow q) \wedge (\sim p \rightarrow r)$

Solution

p	q	r	$p \rightarrow q$	$\sim p$	$\sim p \rightarrow r$	$(p \rightarrow q) \wedge (\sim p \rightarrow r)$
T	T	T	T	F	T	T
T	T	F	T	F	T	T
T	F	T	F	F	T	F
T	F	F	F	F	T	F
F	T	T	T	T	T	T
F	T	F	T	T	F	F
F	F	T	T	T	T	T
F	F	F	T	T	F	F

Other Related Conditionals

The conditional statement is of particular importance in mathematics because many theorems take the form IF (antecedent, hypothesis, condition), THEN (consequent, conclusion). Suppose we take the conditional form

Conditional: $P \rightarrow Q$

then we can construct other related conditionals

Converse of $P \rightarrow Q$: $Q \rightarrow P$
Inverse of $P \rightarrow Q$: $\sim P \rightarrow \sim Q$
Contrapositive of $P \rightarrow Q$: $\sim Q \rightarrow \sim P$

P	Q	$\sim P$	$\sim Q$	$P \rightarrow Q$	$Q \rightarrow P$	$\sim P \rightarrow \sim Q$	$\sim Q \rightarrow \sim P$
F	F	T	T	T	T	T	T
F	T	T	F	T	F	F	T
T	F	F	T	F	T	T	F
T	T	F	F	T	T	T	T

logically equivalent

logically equivalent

Biconditional

If p and q are statement variables, the biconditional of p and q is "p if and only if q". It is denoted $p \leftrightarrow q$. "if and only if" is abbreviated as iff. The double headed arrow " \leftrightarrow " is the biconditional operator.

Example

Identify which of the following are True or false?

1. " $1+1 = 3$ if and only if earth is flat"
2. "Sky is blue iff $1 = 0$ "
3. "Milk is white iff birds lay eggs"
4. "33 is divisible by 4 if and only if horse has four legs"
5. " $x > 5$ iff $x^2 > 25$ "

TRUE
FALSE
TRUE
FALSE
FALSE

Rephrasing Biconditional

$p \leftrightarrow q$ is also expressed as:

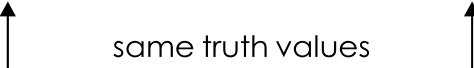
- "p is necessary and sufficient for q"
- "If p then q, and conversely"
- "p is equivalent to q"
- "p precisely then q"

Example

Show that $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Solution

p	q	$p \leftrightarrow q$	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T



Example

Rephrase the following propositions in the form “p if and only if q” in English.

1. For you to win the contest it is necessary and sufficient that you have the only winning ticket.

Solution **You win the contest if and only if you hold the only winning ticket.**

2. If you read the news paper every day, you will be informed and conversely.

Solution **You will be informed if and only if you read the news paper every day.**

3. It rains if it is a weekend day, and it is a weekend day if it rains.

Solution **It rains if and only if it is a weekend day.**

4. This number is divisible by 6 precisely when it is divisible by both 2 and 3.

Solution **This number is divisible by 6 if and only if it is divisible by both 2 and 3.**

Example

Construct the truth table of $(p \rightarrow q) \leftrightarrow (\sim q \rightarrow \sim p)$

Solution

p	q	$p \rightarrow q$	$\sim q$	$\sim p$	$\sim q \rightarrow \sim p$	$(p \rightarrow q) \leftrightarrow (\sim q \rightarrow \sim p)$
T	T	T	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

ARGUMENTS

It is an assertion that the conjunction of certain statements called the premises or hypotheses implies another statement, called the conclusion. If the implication holds, then the argument is **VALID**; otherwise, the argument is called **INVALID**.

$$\begin{array}{c} P_1 \\ P_2 \\ P_3 \\ \vdots \\ P_n \\ \hline \therefore Q \end{array}$$

is valid if and only if

$$(P_1 \wedge P_2 \wedge P_3 \wedge \cdots \wedge P_n) \rightarrow Q \text{ is a tautology.}$$

An argument is **invalid** if the conclusion is false when all the premises are true. Alternatively, an argument is invalid if conjunction of its premises does not imply conclusion.

Critical Rows: The critical rows are those rows where the premises have truth value T.

Example

Show that the following argument form is valid:

$$\begin{array}{l} p \rightarrow q \\ p \\ \therefore q \end{array}$$

Solution

premises		conclusion		
p	q	$p \rightarrow q$	p	q
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	F	F

← critical row

Since the conclusion q is true when the premises $p \rightarrow q$ and p are True. Therefore, it is a valid argument.

Example

Use truth table to determine the argument form is valid or invalid.

$$\begin{array}{l} p \vee q \\ p \rightarrow \sim q \\ p \rightarrow r \\ \therefore r \end{array}$$

Solution

			premises		conclusion	
p	q	r	$p \vee q$	$p \rightarrow \sim q$	$p \rightarrow r$	r
T	T	T	T	F	T	T
T	T	F	T	F	F	F
T	F	T	T	T	T	T
T	F	F	T	T	F	F
F	T	T	T	T	T	T
F	T	F	T	T	T	F
F	F	T	F	T	T	T
F	F	F	F	T	T	F

critical rows

In the third critical row, the conclusion is false when all the premises are true. Therefore, the argument is invalid.

Example**Word Problem**

If I got a monthly bonus, I'll buy a stereo.

If I sell my motorcycle, I'll buy a stereo.

\therefore If I get a monthly bonus or I sell my motorcycle, then I'll buy a stereo.

Solution

Let

b = I got a monthly bonus

s = I'll buy a stereo

m = I sell my motorcycle

The argument is

$b \rightarrow s$

$m \rightarrow s$

$\therefore b \vee m \rightarrow s$

b	s	m	$b \rightarrow s$	$m \rightarrow s$	$b \vee m$	$(b \vee m) \rightarrow s$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	F	F	T	F
T	F	F	F	T	T	F
F	T	T	T	T	T	T
F	T	F	T	T	F	T
F	F	T	T	F	T	F
F	F	F	T	T	F	T

The argument is valid because in the five critical rows, the conclusion is true

Example

If at least one of these two numbers is divisible by 6, then the product of these two numbers is divisible by 6. Neither of these two numbers is divisible by 6. Therefore, The product of these two numbers is not divisible by 6.

Solution

Let d = at least one of these two numbers is divisible by 6.

p = product of these two numbers is divisible by 6.

Then the argument become in these symbols

$d \rightarrow p$

$\sim d$

$\therefore \sim p$

d	p	$d \rightarrow p$	$\sim d$	$\sim p$
T	T	T	F	F
T	F	F	F	T
F	T	T	T	F
F	F	T	T	T

In the first critical row, the conclusion is false when the premises are true. Therefore, the argument is invalid.

RULES OF INFERENCE

The rules of inference specify the conclusion that can be drawn from assertions known or assumed to be true. Let P , Q , R and S represent propositions. The rules of inference are as follows:

Symbols	Names	Rule
1. $\frac{P}{\therefore P \vee Q}$	Addition	Given a statement, it is permissible to infer any disjunction having that statement as one disjunct.
2. $\frac{P \wedge Q \quad P \wedge Q}{Q \quad \text{or} \quad P}$ $\therefore P \quad \therefore Q$	Simplification	Simplification either of its conjuncts separately.
3. $\frac{P \quad Q}{\therefore P \wedge Q}$	Conjunction	Given two statements, it is permissible to infer the conjunction having them as conjuncts.
4. $\frac{P \rightarrow Q \quad P}{\therefore Q}$	Modus Ponens	Given a conditional, and given the antecedent of that same conditional, it is permissible to infer the consequent of the same conditional.
5. $\frac{P \rightarrow Q \quad \sim Q}{\therefore \sim P}$	Modus Tollens	Given a conditional, and given the NEGATION of its CONSEQUENT, it is permissible to infer the NEGATION of its antecedent.
6. $\frac{P \rightarrow Q \quad Q \rightarrow R}{\therefore P \rightarrow R}$	Hypothetical Syllogism (Transitivity)	Given two conditionals such that the consequent of one matches the antecedent of the other, it is permissible to infer a conditional having the UNMATCHED antecedent and the UNMATCHED consequent.

7.	$\frac{P \vee Q \quad \sim P}{\therefore Q} \text{ or } \frac{P \vee Q \quad \sim Q}{\therefore P}$	Disjunctive Syllogism (Cancellation)	Given a disjunction, and given the denial of one of its disjuncts, it is permissible to infer the other disjuncts.
8.	$\frac{P \rightarrow Q \quad R \rightarrow S \quad P \vee R}{\therefore Q \vee S}$	Constructive Dilemma	Given two conditionals (or a conjunction of two conditionals) and given the disjunction of their antecedents, it is permissible to infer the disjunction of their consequents.
9.	$\frac{P \rightarrow Q \quad R \rightarrow S \quad \sim Q \vee \sim S}{\therefore \sim P \vee \sim R}$	Destructive Dilemma	
10.	$\frac{P \leftrightarrow Q \quad P}{\therefore Q} \text{ or } \frac{P \leftrightarrow Q \quad Q}{\therefore P}$	Equivalence	Given a biconditional, and given one side of that same, biconditional, it is permissible to infer the other side of that biconditional.
11.	$\frac{P}{\therefore P}$	Repetition	Given a statement, it is permissible to infer that the same statement.
12.	$\frac{P \rightarrow Q}{\therefore P \rightarrow (P \wedge Q)}$	Absorption	

Example

Establish the validity of the following arguments using the rules of inference

$$\begin{array}{l} P \\ Q \rightarrow \sim P \\ \sim Q \rightarrow (R \vee \sim S) \\ \sim R \\ \hline \therefore \sim S \end{array}$$

Proof**Statement**

1. P
2. $Q \rightarrow \sim P$
3. $\sim Q \rightarrow (R \vee \sim S)$
4. $\sim R$
5. $\sim Q$
6. $R \vee \sim S$
7. $S \rightarrow R$
8. $\sim S$

Reason

- Hypothesis
Hypothesis
Hypothesis
Hypothesis
(1) & (2) Modus Tollens
(3) & (5) Modus Ponens
(6) Implication
(4) & (7) Modus Tollens

Example

Establish the validity of the following arguments using the rules of inference

$$\begin{array}{l} P \rightarrow Q \\ \sim Q \rightarrow \sim R \\ S \rightarrow (P \vee R) \\ S \\ \hline \therefore Q \end{array}$$

Proof**Statement**

1. $P \rightarrow Q$
2. $\sim Q \rightarrow \sim R$
3. $S \rightarrow (P \vee R)$
4. S
5. $P \vee R$
6. $\sim R \rightarrow P$
7. $\sim Q \rightarrow P$
8. $\sim Q \rightarrow Q$
9. $Q \vee Q$
10. Q

Reason

- Hypothesis
Hypothesis
Hypothesis
Hypothesis
(3) & (4) Modus Ponens
(5) Implication
(2) & (6) Hypothetical Syllogism
(1) & (7) Hypothetical Syllogism
(8) Implication
(9) Idempotent

Conditional Proof

Many Theorems in mathematics are stated in the form of conditionals ($P \rightarrow Q$); that is, if a certain condition or conditions (P) are met, then we try to deduce a conclusion or conclusions (Q).

The associated proof strategy (conditional proof) can be outlined in several steps:

1. We have a set of premises $P_1, P_2, P_3, \dots, P_n$, (the premises P_i , represent known information – definitions, axioms, theorems, results of problems, etc.)
2. We wish to deduce a statement in conditional form, $R \rightarrow C$ (i.e., we wish to derive as a conclusion the conditional $R \rightarrow C$ from the premises P_i).
3. We introduce the premise R as an added premise, and treat it as though it were known (or given) information.
4. Using the known information (premises $P_1, P_2, P_3, \dots, P_n$) together with the added information (premise R), we try to deduce the conclusion C .
5. If we are successful, we invoke the rule of conditional proof, and assert that we have derived the desired conditional $R \rightarrow C$ from the original set of premises alone.

Very Important Note:

Conditional proof is based on the **exportation tautology** $[(P \wedge Q) \rightarrow R] \equiv [P \rightarrow (Q \rightarrow R)]$ and it is an extension of this tautology to include any number of premises:

$$\{[(P_1 \wedge P_2 \wedge P_3 \wedge \dots \wedge P_n) \wedge R] \rightarrow C\} \equiv \{(P_1 \wedge P_2 \wedge P_3 \wedge \dots \wedge P_n) \rightarrow (R \rightarrow C)\}$$

$$\begin{array}{ccc}
 \begin{array}{l} P_1 \\ P_2 \\ P_3 \\ \vdots \\ P_n \\ \hline \therefore R \rightarrow C \end{array} & \Leftrightarrow & \begin{array}{l} P_1 \\ P_2 \\ P_3 \\ \vdots \\ P_n \\ R \\ \hline \therefore C \end{array}
 \end{array}$$

Example

Prove

$$\begin{array}{l} P \rightarrow Q \\ R \rightarrow \sim Q \\ \hline \therefore R \rightarrow \sim P \end{array}$$

Note that we wish to prove a statement in the form of a conditional. That might suggest that we try conditional proof with R as the added premise.

Proof**Statement**

1. $P \rightarrow Q$
2. $R \rightarrow \sim Q$
3. $R / \therefore \sim P$
4. $\sim Q$
5. $\sim P$

Reason

- Hypothesis
Hypothesis
Conditional Proof
(2) & (3) Modus Ponens
(1) & (4) Modus Tollens

Example

Prove

$$\begin{array}{l} P \rightarrow (Q \rightarrow R) \\ \sim S \vee P \\ Q \\ \hline \therefore S \rightarrow R \end{array}$$

Proof**Statement**

1. $P \rightarrow (Q \rightarrow R)$
2. $\sim S \vee P$
3. Q
4. $S / \therefore R$
5. P
6. $Q \rightarrow R$
7. R

Reason

- Hypothesis
Hypothesis
Hypothesis
Conditional Proof
(2) & (4) Disjunctive Syllogism
(1) & (5) Modus Ponens
(3) & (6) Modus Ponens

Indirect Proof

Indirect proof is a powerful proof strategy that is also known as **proof by contradiction** or **reductio ad absurdum**.

The associated proof strategy (Indirect proof) can be outlined in several steps:

1. We have a set of premises $P_1, P_2, P_3, \dots, P_n$, (the premises P_i represent known information – definitions, axioms, theorems, results of problems, etc.)
2. We wish to obtain a certain piece of information C (i.e., we wish to derive C as conclusion from the premises P_i).

3. We start by introducing the negation of C ($\sim C$) as an added premise.
4. From $\sim C$ and the original premises (information), $P_1, P_2, P_3, \dots, P_n$, we derive a contradiction (some statement having logical form $Q \wedge \sim Q$).
5. Invoking the rule of Indirect proof, we have essentially deduced the conclusion C from the original set of premises alone.

Very Important Note:

The logical basis of indirect proof is conditional proof and the ***reductio ad absurdum*** tautology, which is:

$$[\sim P \rightarrow (Q \wedge \sim Q)] \rightarrow P$$

That is, if the negation of P leads to a contradiction, we can deduce P.

$$\begin{array}{ccc}
 \begin{array}{l} P_1 \\ P_2 \\ P_3 \\ \vdots \\ P_n \\ \hline \therefore Q \end{array} & \Leftrightarrow & \begin{array}{l} P_1 \\ P_2 \\ P_3 \\ \vdots \\ P_n \\ \sim Q \\ \hline \therefore f \end{array}
 \end{array}$$

Example

Construct, using indirect proof strategy, proofs of the following symbolic arguments.

$$\begin{array}{l}
 \sim(P \wedge Q) \\
 \sim R \rightarrow Q \\
 \sim P \rightarrow R \\
 \hline
 \therefore R
 \end{array}$$

Proof

Statement

1. $\sim(P \wedge Q)$
2. $\sim R \rightarrow Q$
3. $\sim P \rightarrow R$
4. $\sim R / \therefore f$
5. Q
6. $\sim P \vee \sim R$
7. $\sim P$
8. R
9. $R \wedge \sim R$
10. f

Reason

- Hypothesis
- Hypothesis
- Hypothesis
- Indirect Proof
- (2) & (4) Modus Ponens
- (1) De Morgan's Law
- (5) & (6) Disjunctive Syllogism
- (3) & (7) Modus Ponens
- (4) & (8) Conjunction
- (9) Identity

Example

Construct, using indirect proof strategy, proofs of the following symbolic arguments.

$$\begin{array}{l} P \\ R \\ (Q \wedge P) \rightarrow \sim R \\ \hline \therefore \sim Q \end{array}$$

Proof**Statement**

1. P
2. R
3. $(Q \wedge P) \rightarrow \sim R$
4. $\sim(\sim Q) / \therefore f$
5. Q
6. $Q \rightarrow (P \rightarrow \sim R)$
7. $P \rightarrow \sim R$
8. $\sim R$
9. $R \wedge \sim R$
10. f

Reason

- Hypothesis
Hypothesis
Hypothesis
Indirect Proof
(4) Double Negation
(3) Exportation
(5) & (6) Modus Ponens
(1) & (7) Modus Ponens
(2) & (8) Conjunction
(9) Identity

Example

Show that the hypothesis "it is not sunny this afternoon and it is colder than yesterday", "we will go swimming only if it is sunny", "if we do not go swimming, then we will take a canoe trip", and "if we take a canoe trip then we will be home by sunset".

Lead to the conclusion: "we will be home by sunset."

Solution

Let	P = "it is sunny"	$\sim P \wedge Q$
	Q = "it is colder than yesterday"	$R \rightarrow P$
	R = "we will go swimming"	$\sim R \rightarrow S$
	S = "we will take a canoe trip"	$S \rightarrow W$
	W = "we will be home by sunset"	$\therefore W$

Proof**Statement**

1. $\sim P \wedge Q$
2. $R \rightarrow P$
3. $\sim R \rightarrow S$
4. $S \rightarrow W$
5. $\sim P$
6. $\sim R$
7. S
8. W

Reason

- Hypothesis
Hypothesis
Hypothesis
Hypothesis
(1) Simplification
(2) & (5) Modus Tollens
(3) & (6) Modus Ponens
(4) & (7) Modus Ponens

CHAPTER 3: RELATIONS

A **relation** for a sequence $A_1, A_2, A_3, \dots, A_n$ of sets is subset of the Cartesian product $A_1 \times A_2 \times A_3 \times \dots \times A_n$. A **relation from A to B** (or **between A and B**) is a subset of the Cartesian product $A \times B$.

Ordered Pair

An ordered pair (a, b) consists of two elements "a" and "b" in which "a" is the first element and "b" is the second element. The ordered pairs (a, b) and (c, d) are equal if, and only if, $a = c$ and $b = d$. Note that (a, b) and (b, a) are not equal unless $a = b$.

Example

Find x and y given $(2x, x + y) = (6, 2)$

Solution

Two ordered pairs are equal if and only if the corresponding components are equal. Hence, we obtain the equations:

$$\begin{array}{ll} 2x = 6 & (1) \\ x + y = 2 & (2) \end{array}$$

Solving equation (1) we get $x = 3$ and when substituted in (2) we get $y = -1$.

Ordered n-Tuple

The ordered n -tuple (a_1, a_2, \dots, a_n) consists of elements a_1, a_2, \dots, a_n together with the ordering: first a_1 , second a_2 , and so forth up to a_n . In particular, an ordered 2-tuple is called an ordered pair, and an ordered 3-tuple is called an ordered triple. Two ordered n -tuples (a_1, a_2, \dots, a_n) and (b_1, b_2, \dots, b_n) are equal if and only if each corresponding pair of their elements is equal, i.e., $a_i = b_i$, for all $i, j = 1, 2, \dots, n$.

Cartesian Product of two sets

Let A and B be sets. The Cartesian product of A and B , denoted by $A \times B$ (read as "A cross B") is the set of all ordered pairs (a, b) , where a is in A and b is in B .

Symbolically: $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$

Note: If set A has m elements and set B has n elements then $A \times B$ has $m \times n$ elements.

Example

Let $A = \{1, 2\}$, $B = \{a, b, c\}$ then

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

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

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

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

Remark:

1. $A \times B \neq B \times A$ for non-empty and unequal sets A and B .
2. $A \times \phi = \phi \times A = \phi$
3. $|A \times B| = |A| \times |B|$

Binary Relation

Let A and B be sets. The binary relation R from A to B is a subset of $A \times B$. When $(a, b) \in R$, we say 'a' is related to 'b' by R , written aRb .

Domain of a Relation

The domain of a binary relation R is the set of all first components in the ordered pairs of the relation.

Symbolically: $\text{Dom}(R) = \{a \in A \mid (a, b) \in R\}$

Range of a Relation

The range of a binary relation R is the set of all second components in the ordered pairs of the relation.

Symbolically: $\text{Ran}(R) = \{b \in B \mid (a, b) \in R\}$

Example

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

Define a binary relation R from A to B as follows: $R = \{(a, b) \in A \times B \mid a < b\}$

- Find the ordered pairs in R .
- Find the Domain and Range of R .

Solution

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

- $R = \{(1,2), (1,3), (2,3)\}$
- $\text{Dom}(R) = \{1,2\}$ and $\text{Ran}(R) = \{2, 3\}$

Example

Let $A = \{\text{eggs, milk, corn}\}$ and $B = \{\text{cows, goats, hens}\}$

Define a relation R from A to B by $(a, b) \in R$ iff a is produced by b .

Then $R = \{(\text{eggs, hens}), (\text{milk, cows}), (\text{milk, goats})\}$

Thus, with respect to this relation eggs R hens , milk R cows, etc.

Relation on a Set

A relation on the set A is a relation from A to A . In other words, a relation on a set A is a subset of $A \times A$.

Example

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

Define a relation R on A as $(a,b) \in R$ iff a divides b {symbolically written as $a \mid b$ }

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

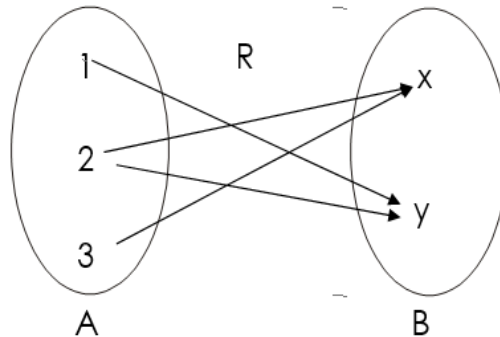
Remark:

For any set A

- $A \times A$ is known as the universal relation.
- \emptyset is known as the empty relation.

Arrow Diagram of a Relation

Let $A = \{1, 2, 3\}$, $B = \{x, y\}$ and $R = \{(1,y), (2,x), (2,y), (3,x)\}$ be a relation from A to B . The arrow diagram of R is:

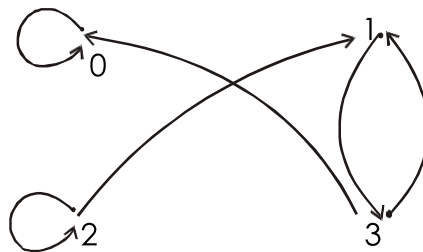


Directed Graph of a Relation

A directed graph for a binary relation R on A is a figure whose vertices are points representing the elements of A and with an arc or line from vertex a to vertex b (having an arrowhead pointing toward b) if and only if aRb . A loop at vertex a is an arc from a to itself.

Example

Let $A = \{0, 1, 2, 3\}$ and $R = \{(0,0), (1,3), (2,1), (2,2), (3,0), (3,1)\}$ be a binary relation on A .



DIRECTED GRAPH

Matrix Representation of a Relation

Let $A = \{a_1, a_2, \dots, a_n\}$ and $B = \{b_1, b_2, \dots, b_m\}$. Let R be a relation from A to B . Define the $n \times m$ order matrix M by

$$m(i, j) = \begin{cases} 1, & (a_i, b_j) \in R \\ 0, & (a_i, b_j) \notin R \end{cases}$$

For $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, m$

Example

Let $A = \{1, 2, 3\}$ and $B = \{x, y\}$

Let R be a relation from A to B defined as

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

$$M = \begin{matrix} & \begin{matrix} x & y \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix} \end{matrix}_{3 \times 2}$$

Example

Given binary matrix

$$M = \begin{matrix} & \begin{matrix} 1 & 2 & 3 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \end{matrix}$$

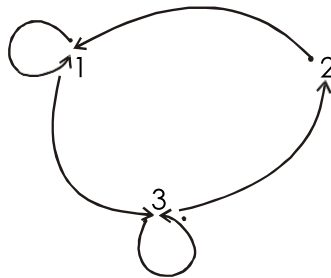
- List the set of ordered pairs represented by M.
- Draw the directed graph of the relation.

Solution

The relation corresponding to the given Matrix is

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

and its Directed graph is given below

**Example**

Let $A = \{2, 4\}$ and $B = \{6, 8, 10\}$ and define relations R and S from A to B as follows:

for all $(x,y) \in A \times B$, $x R y \Leftrightarrow x \mid y$

for all $(x,y) \in A \times B$, $x S y \Leftrightarrow y - 4 = x$

State explicitly which ordered pairs are in $A \times B$, R, S, $R \cup S$ and $R \cap S$.

Solution

$$A \times B = \{(2,6), (2,8), (2,10), (4,6), (4,8), (4,10)\}$$

$$R = \{(2,6), (2,8), (2,10), (4,8)\}$$

$$S = \{(2,6), (4,8)\}$$

$$R \cup S = \{(2,6), (2,8), (2,10), (4,8)\} = R$$

$$R \cap S = \{(2,6), (4,8)\} = S$$

TYPES OF RELATIONS

Reflexive Relation

Let R be a relation on a set A . R is reflexive if and only if, for all $a \in A$, $(a, a) \in R$ or equivalently aRa . That is, each element of A is related to itself.

Remark

R is not reflexive iff there is an element " a " in A such that $(a, a) \notin R$. That is, some element " a " of A is not related to itself.

Example

Let $A = \{1, 2, 3, 4\}$ and define relations R_1, R_2, R_3, R_4 on A as follows:

$$R_1 = \{(1, 1), (3, 3), (2, 2), (4, 4)\}$$

$$R_2 = \{(1, 1), (1, 4), (2, 2), (3, 3), (4, 3)\}$$

$$R_3 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$$

$$R_4 = \{(1, 3), (2, 2), (2, 4), (3, 1), (4, 4)\}$$

Then,

R_1 is **reflexive**, since $(a, a) \in R_1$ for all $a \in A$.

R_2 is **not reflexive**, because $(4, 4) \notin R_2$.

R_3 is **reflexive**, since $(a, a) \in R_3$ for all $a \in A$.

R_4 is **not reflexive**, because $(1, 1) \notin R_4, (3, 3) \notin R_4$

Directed Graph of a Reflexive Relation

The directed graph of every reflexive relation includes an arrow from every point to the point itself (i.e., a loop).

Example

Let $A = \{1, 2, 3, 4\}$ and define relations R_1, R_2, R_3 , and R_4 on A by

$$R_1 = \{(1, 1), (3, 3), (2, 2), (4, 4)\}$$

$$R_2 = \{(1, 1), (1, 4), (2, 2), (3, 3), (4, 3)\}$$

$$R_3 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$$

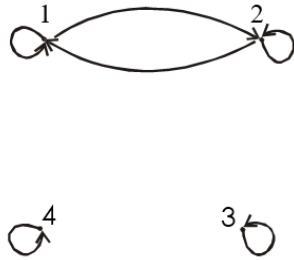
$$R_4 = \{(1, 3), (2, 2), (2, 4), (3, 1), (4, 4)\}$$

Then their directed graphs are the following:

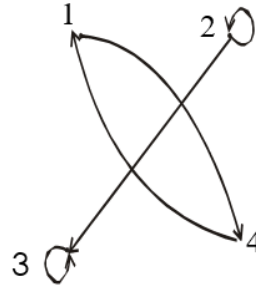


R_1 is reflexive because at every point of the set A we have a loop in the graph.

R_2 is not reflexive, as there is no loop at 4.



R_3 is reflexive



R_4 is not reflexive, as there are no loops at 1 and 3.

Matrix Representation of a Reflexive Relation

Let $A = \{a_1, a_2, \dots, a_n\}$. A Relation R on A is reflexive if and only if $(a_i, a_i) \in R \forall i = 1, 2, \dots, n$. Accordingly, R is reflexive if all the elements on the main diagonal of the matrix M representing R are equal to 1.

Example

The relation $R = \{(1, 1), (1, 3), (2, 2), (3, 2), (3, 3)\}$ on $A = \{1, 2, 3\}$ represented by the following matrix M , is reflexive.

$$M = \begin{matrix} & \begin{matrix} 1 & 2 & 3 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \end{matrix}$$

Symmetric Relation

Let R be a relation on a set A . R is symmetric if, and only if, for all $a, b \in A$, if $(a, b) \in R$, then $(b, a) \in R$. That is, if aRb then bRa .

Remark: R is not symmetric iff there are elements a and b in A such that $(a, b) \in R$, but $(b, a) \notin R$.

Example

Let $A = \{1, 2, 3, 4\}$ and define relations R_1, R_2, R_3 , and R_4 on A as follows.

$$R_1 = \{(1, 1), (1, 3), (2, 4), (3, 1), (4, 2)\}$$

$$R_2 = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$$

$$R_3 = \{(2, 2), (2, 3), (3, 4)\}$$

$$R_4 = \{(1, 1), (2, 2), (3, 3), (4, 3), (4, 4)\}$$

R_1 is symmetric because for every ordered pair (a, b) in R_1 also have (b, a) in R_1 . For example, we have $(1, 3)$ in R_1 then we have $(3, 1)$ in R_1 . Similarly all other ordered pairs can be checked.

R_2 is also symmetric. We say it is vacuously true.

R_3 is not symmetric, because $(2,3) \in R_3$ but $(3,2) \notin R_3$.

R_4 is not symmetric because $(4,3) \in R_4$ but $(3,4) \notin R_4$.

Directed Graph of a Symmetric Relation

For a symmetric directed graph whenever there is an arrow going from one point of the graph to a second, there is an arrow going from the second point back to the first.

Example

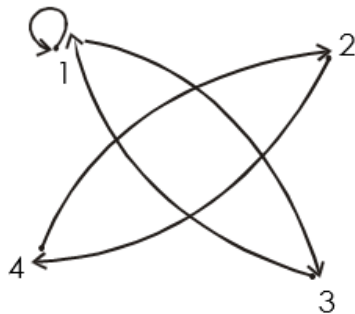
Let $A = \{1, 2, 3, 4\}$ and define relations R_1, R_2, R_3 and R_4 on A by the directed graphs:

$R_1 = \{(1, 1), (1, 3), (2, 4), (3, 1), (4, 2)\}$

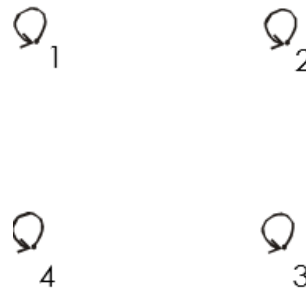
$R_2 = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$

$R_3 = \{(2, 2), (2, 3), (3, 4)\}$

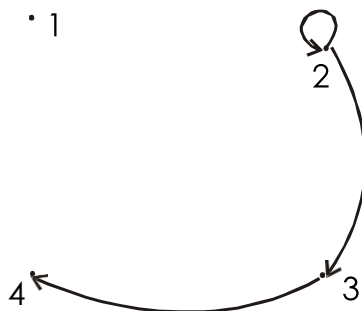
$R_4 = \{(1, 1), (2, 2), (3, 3), (4, 3), (4, 4)\}$



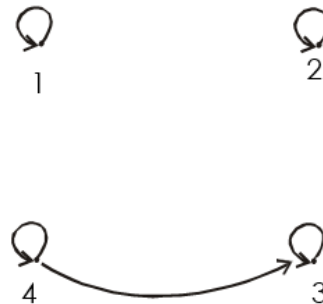
R_1 is symmetric.



R_2 is symmetric.



R_3 is not symmetric since there are arrows from 2 to 3 and from 3 to 4 but not conversely.



R_4 is not symmetric since there is an arrow from 4 to 3 but no arrow from 3 to 4.

Matrix Representation of a Symmetric Relation

Let $A = \{a_1, a_2, \dots, a_n\}$. The relation R on A is symmetric if and only if for all $a_i, a_j \in A$, if $(a_i, a_j) \in R$ then $(a_j, a_i) \in R$.

Accordingly, R is symmetric if the elements in the i th row are the same as the elements in the j th column of the matrix M representing R . More precisely, M is a symmetric matrix i.e. $M = M^T$

Example

The relation $R = \{(1,3), (2,2), (3,1), (3,3)\}$ on $A = \{1,2,3\}$ represented by the following matrix M is symmetric

$$M = \begin{matrix} & \begin{matrix} 1 & 2 & 3 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \end{matrix}$$

Transitive Relation

Let R be a relation on a set A . R is transitive if and only if for all $a, b, c \in A$, if $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$. That is, if aRb and bRc then aRc .

In words, if any one element is related to a second and that second element is related to a third, then the first is related to the third.

Note: The “first”, “second” and “third” elements need not to be distinct

Remark: R is not transitive iff there are elements a, b, c in A such that if $(a, b) \in R$ and $(b, c) \in R$ but $(a, c) \notin R$

Example

Let $A = \{1, 2, 3, 4\}$ and define relations R_1, R_2 and R_3 on A as follows:

$$R_1 = \{(1, 1), (1, 2), (1, 3), (2, 3)\}$$

$$R_2 = \{(1, 2), (1, 4), (2, 3), (3, 4)\}$$

$$R_3 = \{(2, 1), (2, 4), (2, 3), (3, 4)\}$$

R_1 is **transitive** because $(1, 1), (1, 2)$ are in R , then to be transitive relation $(1, 2)$ must be there and it belongs to R .

R_2 is **not transitive** since $(1, 2)$ and $(2, 3) \in R_2$ but $(1, 3) \notin R_2$.

R_3 is **transitive**.

Directed Graph of a Transitive Relation

For a transitive directed graph, whenever there is an arrow going from one point to the second, and from the second to the third, there is an arrow going directly from the first to the third.

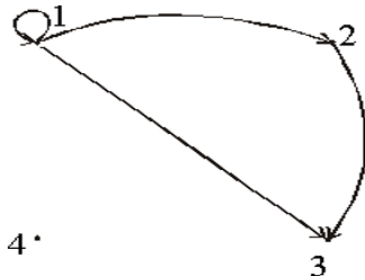
Example

Let $A = \{1, 2, 3, 4\}$ and define relations R_1 , R_2 and R_3 on A by the directed graphs:

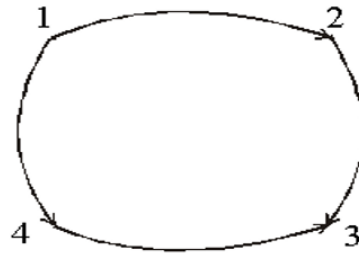
$$R_1 = \{(1, 1), (1, 2), (1, 3), (2, 3)\}$$

$$R_2 = \{(1, 2), (1, 4), (2, 3), (3, 4)\}$$

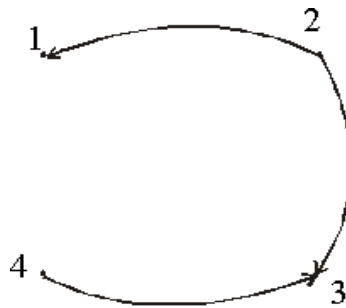
$$R_3 = \{(2, 1), (2, 4), (2, 3), (3, 4)\}$$



R_1 is transitive.



R_2 is not transitive since there is an arrow from 1 to 2 and from 2 to 3 but no arrow from 1 to 3 directly.



R_3 is transitive

Example

Let $A = \{0, 1, 2\}$ and $R = \{(0, 2), (1, 1), (2, 0)\}$ be a relation on A .

1. Is R reflexive? Symmetric? Transitive?
2. Which ordered pairs are needed in R to make it a reflexive and transitive relation.

Solution

1. R is **not reflexive**, since $0 \in A$ but $(0, 0) \notin R$ and also $2 \in A$ but $(2, 2) \notin R$.
 R is clearly **symmetric**.
 R is **not transitive**, since $(0, 2) \in R$ & $(2, 0) \in R$ but $(0, 0) \notin R$.
2. For R to be reflexive, it must contain ordered pairs $(0, 0)$ and $(2, 2)$.
 For R to be transitive, we note $(0, 2)$ and $(2, 0) \in R$ but $(0, 0) \notin R$.
 Also $(2, 0)$ and $(0, 2) \in R$ but $(2, 2) \notin R$.

Hence $(0, 0)$ and $(2, 2)$. Are needed in R to make it a transitive relation.

Example

Define a relation L on the set of real numbers \mathbf{R} be defined as follows:

for all $x, y \in \mathbf{R}$, $x L y \Leftrightarrow x < y$.

- Is L reflexive?
- Is L symmetric?
- Is L transitive?

SOLUTION

- L is **not reflexive**, because $x \not\prec x$ for any real number x .
(e.g. $1 \not\prec 1$)
- L is **not symmetric**, because for all $x, y \in \mathbf{R}$, if $x < y$ then $y \not\prec x$
(e.g. $0 < 1$ but $1 \not\prec 0$)
- L is **transitive**, because for all, $x, y, z \in \mathbf{R}$, if $x < y$ and $y < z$, then $x < z$.
(by transitive law of order of real numbers).

Example

Let “ D ” be the “divides” relation on \mathbf{Z} defined as: for all $m, n \in \mathbf{Z}$, $m D n \Leftrightarrow m \mid n$. Determine whether D is reflexive, symmetric or transitive. Justify your answer

Solution**Reflexive**

Let $m \in \mathbf{Z}$, since every integer divides itself.

So $m \mid m \forall m \in \mathbf{Z}$ therefore $m D m \forall m \in \mathbf{Z}$

Accordingly D is **reflexive**

Symmetric

Let $m, n \in \mathbf{Z}$ and suppose $m D n$.

By definition of D , this means $m \mid n$ (i.e. = an integer).

Clearly, then it is not necessary that $n \mid m$.

Accordingly, if $m D n$ then $n D m$, $\forall m, n \in \mathbf{Z}$

Hence D is **not symmetric**.

Transitive

Let $m, n, p \in \mathbf{Z}$ and suppose $m D n$ and $n D p$.

Now $m D n \Rightarrow m \mid n \Rightarrow$ = an integer.

Also $n D p \Rightarrow n \mid p \Rightarrow$ = an integer

Then $m D p \Rightarrow m \mid p \forall m, n, p \in \mathbf{Z}$

Hence D is **transitive**.

Equivalence Relation

Let A be a non-empty set and R a binary relation on A . R is an equivalence relation if, and only if, R is reflexive, symmetric, and transitive.

Example

Let $A = \{1, 2, 3, 4\}$ and $R = \{(1,1), (2,2), (2,4), (3,3), (4,2), (4,4)\}$ be a binary relation on A .

Note that R is reflexive, symmetric and transitive, hence an **equivalence relation**.

Irreflexive Relation

Let R be a binary relation on a set A . R is irreflexive iff for all $a \in A, (a,a) \notin R$. That is, R is irreflexive if no element in A is related to itself by R .

Remark: R is not irreflexive iff there is an element $a \in A$ such that $(a,a) \in R$.

Example

Let $A = \{1,2,3,4\}$ and define the following relations on A :

$$R_1 = \{(1,3), (1,4), (2,3), (2,4), (3,1), (3,4)\}$$

$$R_2 = \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}$$

$$R_3 = \{(1,2), (2,3), (3,3), (3,4)\}$$

R_1 is **irreflexive** since no element of A is related to itself in R_1 . i.e. $(1,1) \notin R_1, (2,2) \notin R_1, (3,3) \notin R_1, (4,4) \notin R_1$

R_2 is **not irreflexive**, since all elements of A are related to themselves in R_2

R_3 is **not irreflexive** since $(3,3) \in R_3$. Note that R_3 is not reflexive

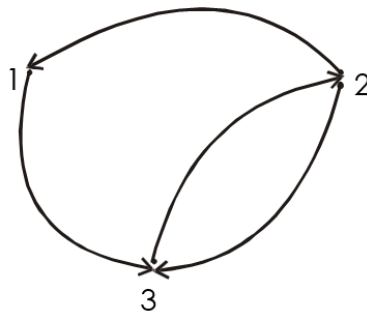
Note: A relation may be neither **reflexive** nor **irreflexive**

Directed Graph of an Irreflexive Relation

Let R be an irreflexive relation on a set A . Then by definition, no element of A is related to itself by R . Accordingly, there is no loop at each point of A in the directed graph of R .

Example

Let $A = \{1,2,3\}$ and $R = \{(1,3), (2,1), (2,3), (3,2)\}$ be represented by the directed graph



Matrix Representation of an Irreflexive Relation

Let R be an irreflexive relation on a set A . Then by definition, no element of A is related to itself by R .

Since the self related elements are represented by 1's on the main diagonal of the matrix representation of the relation, so for irreflexive relation R , the matrix will contain all 0's in its main diagonal. It means that a relation is irreflexive if in its matrix representation the diagonal elements are all zero, if one of them is not zero then we will say that the relation is not irreflexive

Example

Let $A = \{1,2,3\}$ and $R = \{(1,3), (2,1), (2,3), (3,2)\}$ be represented by the matrix

$$M = \begin{matrix} & \begin{matrix} 1 & 2 & 3 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \end{matrix}$$

Then R is **irreflexive**, since all elements in the main diagonal are 0's

Example

Let R be the relation on the set of integers Z defined as: for all $a, b \in \mathbb{Z}$, $(a, b) \in R \Leftrightarrow a > b$.
Is R irreflexive?

Solution

R is irreflexive if for all $a \in \mathbb{Z}$, $(a, a) \notin R$. Now by the definition of given relation R, for all $a \in \mathbb{Z}$, $(a, a) \notin R$ since $a \not> a$.
Hence R is **irreflexive**.

Antisymmetric Relation

Let R be a binary relation on a set A. R is anti-symmetric iff $\forall a, b \in A$ if $(a, b) \in R$ and $(b, a) \in R$ then $a = b$.

Remarks

- 1) R is not anti-symmetric iff there are elements a and b in A such that $(a, b) \in R$ and $(b, a) \in R$ but $a \neq b$.
- 2) The properties of being symmetric and being anti-symmetric are not negative of each other.

Example

Let $A = \{1, 2, 3, 4\}$ and define the following relations on A.

$$\begin{aligned} R_1 &= \{(1, 1), (2, 2), (3, 3)\} & R_2 &= \{(1, 2), (2, 2), (2, 3), (3, 4), (4, 1)\} \\ R_3 &= \{(1, 3), (2, 2), (2, 4), (3, 1), (4, 2)\} & R_4 &= \{(1, 3), (2, 4), (3, 1), (4, 3)\} \end{aligned}$$

R_1 is anti-symmetric and symmetric .

R_2 is anti-symmetric but not symmetric because $(1, 2) \in R_2$ but $(2, 1) \notin R_2$.

R_3 is not anti-symmetric since $(1, 3) \in R_3$ & $(3, 1) \in R_3$ but $1 \neq 3$. Note that R_3 is symmetric.

R_4 is neither anti-symmetric because $(1, 3) \in R_4$ & $(3, 1) \in R_4$ but $1 \neq 3$ nor symmetric because $(2, 4) \in R_4$ but $(4, 2) \notin R_4$.

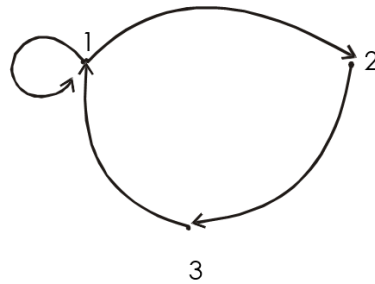
Directed Graph of an Antisymmetric Relation

Let R be an anti-symmetric relation on a set A. Then by definition, no two distinct elements of A are related to each other. Accordingly, there is no pair of arrows between two distinct elements of A in the directed graph of R.

Example

Let $A = \{1, 2, 3\}$ and R be the relation defined on A is $R = \{(1, 1), (1, 2), (2, 3), (3, 1)\}$.

Thus R is represented by the directed graph as



R is anti-symmetric, since there is no pair of arrows between two distinct points in A.

Matrix Representation of an Antisymmetric Relation

Let R be an anti-symmetric relation on a set $A = \{a_1, a_2, \dots, a_n\}$. Then if $(a_i, a_j) \in R$ for $i \neq j$ then $(a_j, a_i) \notin R$. Thus in the matrix representation of R there is a 1 in the i th row and j th column iff the j th row and i th column contains 0 vice versa.

Example

Let $A = \{1, 2, 3\}$ and a relation $R = \{(1, 1), (1, 2), (2, 3), (3, 1)\}$ on A be represented by the matrix.

$$M = \begin{matrix} & \begin{matrix} 1 & 2 & 3 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \end{matrix}$$

Then R is anti-symmetric as clear by the form of matrix M.

Inverse of a Relation

Let R be a relation from A to B. The inverse relation R^{-1} from B to A is defined as:

$$R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}$$

More simply, the inverse relation R^{-1} of R is obtained by interchanging the elements of all the ordered pairs in R.

Example

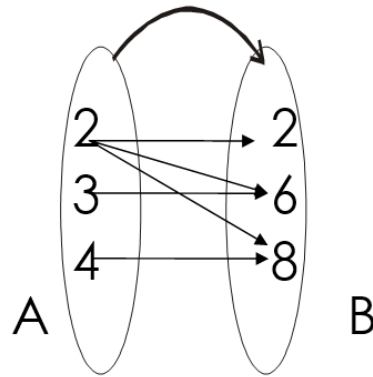
Let $A = \{2, 3, 4\}$ and $B = \{2, 6, 8\}$ and let R be the "divides" relation from A to B i.e. for all $(a, b) \in A \times B$, $a R b \Leftrightarrow a \mid b$ (a divides b)

Then $R = \{(2, 2), (2, 6), (2, 8), (3, 6), (4, 8)\}$ and $R^{-1} = \{(2, 2), (6, 2), (8, 2), (6, 3), (8, 4)\}$

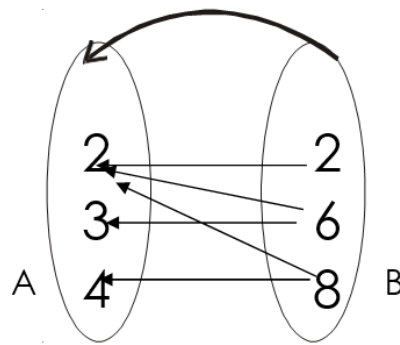
In words, R^{-1} may be defined as: for all $(b, a) \in B \times A$, $b R a \Leftrightarrow b$ is a multiple of a .

Arrow Diagram of an Inverse Relation

The relation $R = \{(2, 2), (2, 6), (2, 8), (3, 6), (4, 8)\}$ is represented by the arrow diagram.



Then inverse of the above relation can be obtained simply changing the directions of the arrows and hence the diagram is R^{-1}



Matrix Representation of Inverse Relation

The relation $R = \{(2, 2), (2, 6), (2, 8), (3, 6), (4, 8)\}$ from $A = \{2, 3, 4\}$ to $B = \{2, 6, 8\}$ is defined by the matrix M below:

$$M = \begin{matrix} & \begin{matrix} 2 & 6 & 8 \end{matrix} \\ \begin{matrix} 2 \\ 3 \\ 4 \end{matrix} & \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{matrix}$$

$$M' = \begin{matrix} & \begin{matrix} 2 & 3 & 4 \end{matrix} \\ \begin{matrix} 2 \\ 6 \\ 8 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \end{matrix}$$

The matrix representation of inverse relation R^{-1} is obtained by simply taking its transpose. (i.e., changing rows by columns and columns by rows). Hence R^{-1} is represented by M^T as shown.

Complementary Relation

Let R be a relation from a set A to a set B . The complementary relation \bar{R} of R is the set of all those ordered pairs in $A \times B$ that do not belong to R .

Symbolically: $\bar{R} = A \times B - R = \{(a, b) \in A \times B \mid (a, b) \notin R\}$

Example

Let $A = \{1, 2, 3\}$ and $R = \{(1, 1), (1, 3), (2, 2), (2, 3), (3, 1)\}$ be a relation on A . Then $\bar{R} = \{(1, 2), (2, 1), (3, 2), (3, 3)\}$

Composite Relation

Let R be a relation from a set A to a set B and S a relation from B to a set C . The composite of R and S denoted SoR is the relation from A to C , consisting of ordered pairs (a,c) where $a \in A$, $c \in C$, and for which there exists an element $b \in B$ such that $(a,b) \in R$ and $(b,c) \in S$.

Symbolically: $SoR = \{(a,c) \mid a \in A, c \in C, \exists b \in B, (a,b) \in R \text{ and } (b,c) \in S\}$

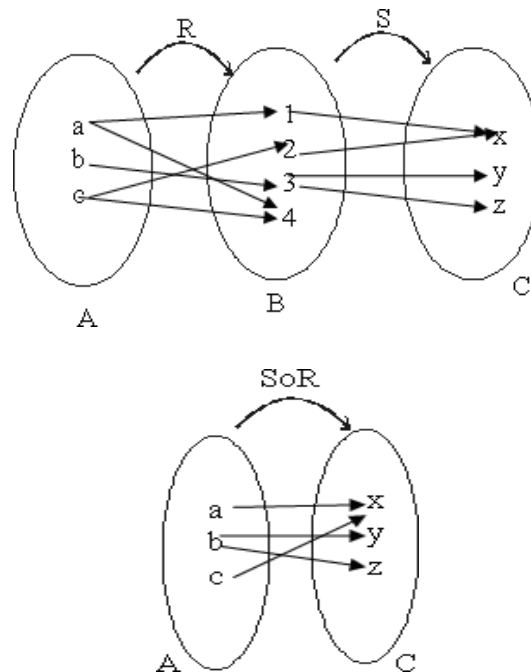
Example

Define $R = \{(a,1), (a,4), (b,3), (c,1), (c,4)\}$ as a relation from A to B and $S = \{(1,x), (2,x), (3,y), (3,z)\}$ be a relation from B to C .

Hence, $SoR = \{(a,x), (b,y), (b,z), (c,x)\}$

Composite Relation from Arrow Diagram

Let $A = \{a,b,c\}$, $B = \{1,2,3,4\}$ and $C = \{x,y,z\}$. Define relation R from A to B and S from B to C by the following arrow diagram



Matrix Representation of Composite Relation

The matrix representation of the composite relation can be found using the Boolean product of the matrices for the relations. Thus if M_R and M_S are the matrices for relations R (from A to B) and S (from B to C), then

$$M_{SoR} = M_R \times M_S$$

is the matrix for the composite relation SoR from A to C .

Boolean Addition

- a. $1 + 1 = 1$
- b. $1 + 0 = 1$
- c. $0 + 0 = 0$

Boolean Multiplication

- a. $1 \cdot 1 = 1$
- b. $1 \cdot 0 = 0$
- c. $0 \cdot 0 = 0$

Example

Find the matrix representing the relations SoR and RoS where the matrices representing R and S are

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad M_S = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Solution

The matrix representation for SoR is

$$\begin{aligned} M_{SOR} &= M_R O M_S = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \end{aligned}$$

The matrix representation for RoS is

$$\begin{aligned} M_{ROS} &= M_S O M_R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \end{aligned}$$

PARTIAL ORDER RELATION

Let A be a set and R be a binary relation on A. R is a partial order on A if and only if:

- (1) R is reflexive: $\forall a \in A, aRa$
- (2) R is anti-symmetric: $\forall a, b \in A$ (if aRb and bRa , then $a = b$)
- (3) R is transitive: $\forall a, b, c \in A$ (if aRb and bRc then aRc)

A non-empty set A together with a partial order relation on A is called **partially ordered set** or **POSET** in short.

There are three classic examples of partial orders on sets – the relation \leq on the set of real numbers, the subset relation (\subseteq) on the power set $P(A)$ of a given set A, and the divisibility relation ($a \mid b$) on the set of positive integers.

Hasse Diagrams

A **poset diagram** (or **Hasse Diagram**) for a poset (A, R) is a figure in which:

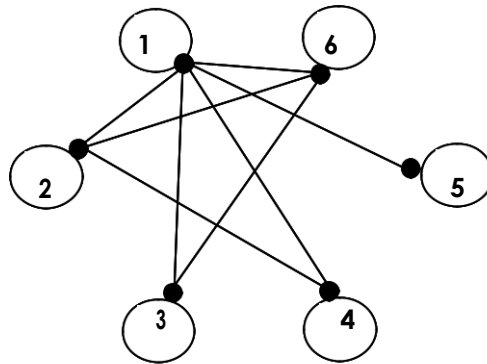
1. The vertices are points representing the elements of A .
2. There is an upward sloping line or broken line from a to b whenever $a \neq b$ and aRb .
3. The figure has the least number of segments that accomplish the property in (2).

Steps in Making Hasse Diagram:

1. Remove all loops.
2. Delete all the edges implied by transitivity property.
3. Arrange all edges to point upward and delete all arrowheads.

Example

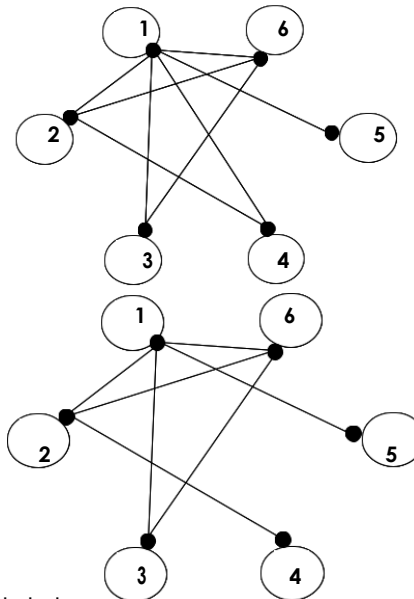
A partial order relation R on $A = \{1, 2, 3, 4, 5, 6\}$ has the directed graph given below. Draw its Hasse diagram.



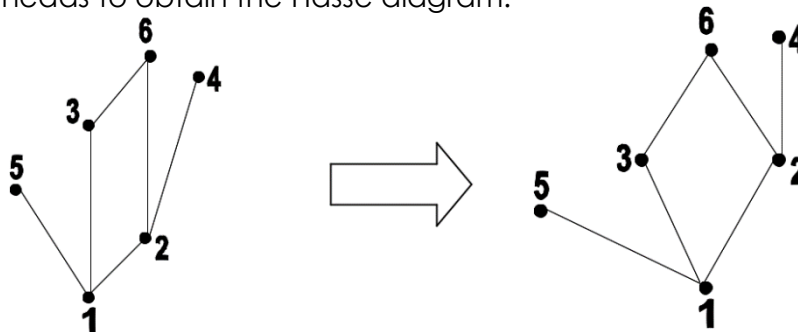
Solution

- (1) Loops are not drawn but are assumed to be present at each vertex because the R for a poset is reflexive.

- (2) Delete all the edges implied by the transitivity property. These are $(1, 6)$ and $(1, 4)$.

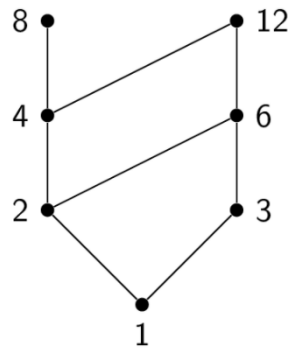


- (3) Arrange all edges to point upward and delete all arrowheads to obtain the Hasse diagram.

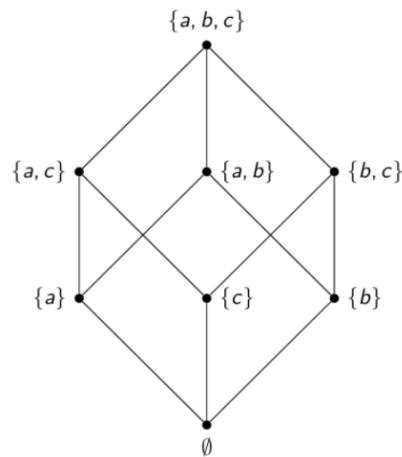


Example

Construct its hasse diagram of the given poset $(\{1,2,3,4,6,8,12\}, |)$.

**Example**

Construct its hasse diagram of the given poset $(P\{a,b,c\}, \subseteq)$.

**SEQUENTIAL PROCESSES AND MACHINES**

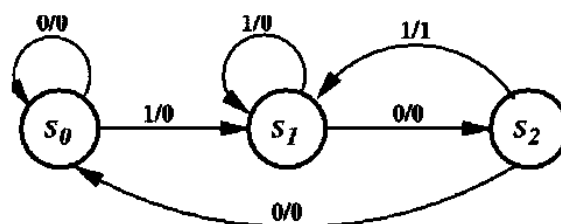
A sequential process starts in an initial state q_0 and in response to a sequence of states and generates a sequence of output. A sequential process can be described by a state table that lists the next state and output for each combination of the present state and output of the process.

State diagrams

A graphical representation of all information available in the state table with labeled edges (input/output). Each state a process is represented by a node (circle) that contains the state label. Each transition from q_i to q_j caused by input is represented by a directed branch from node q_i to node q_j which is labeled in the output.

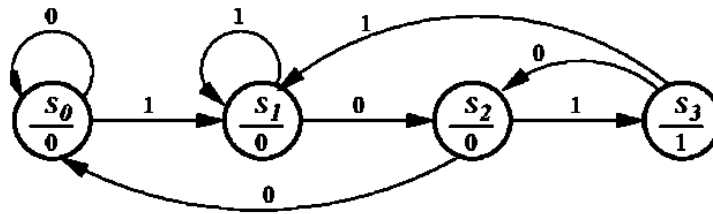
Mealy State Machines

A state diagram in which output are function of both states and input.



Moore State Machines

A state diagram in which the output is function of the state

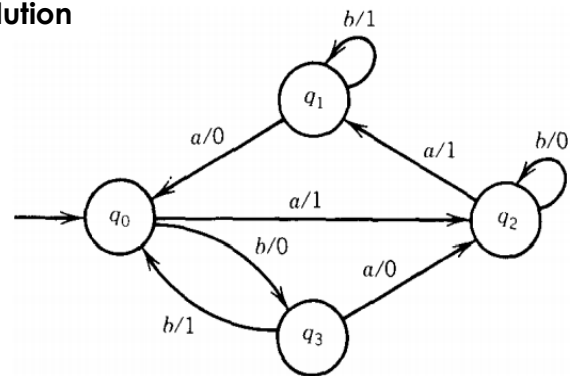


Example

Draw the state diagram for the Mealy state machine of the given state table.

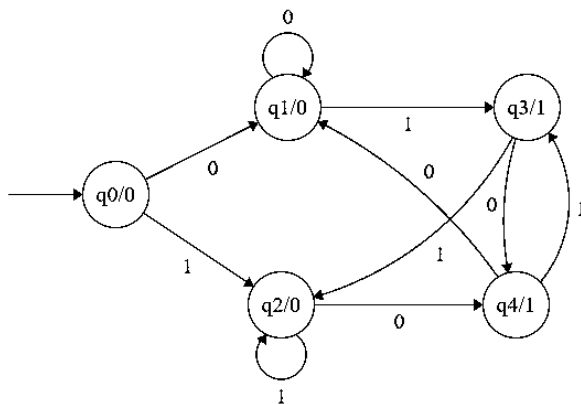
STATE	INPUT		OUTPUT	
	a	b	a	b
q_0	q_2	q_3	1	0
q_1	q_0	q_1	0	1
q_2	q_1	q_2	1	0
q_3	q_2	q_0	0	1

Solution



Example

Construct the state table for the Moore state machine with the given state diagram.



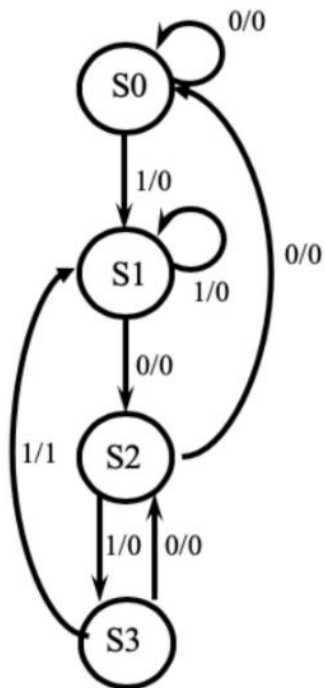
Solution

STATE	INPUT		OUTPUT	
	0	1	0	1
q_0	q_1	q_2	0	0
q_1	q_1	q_3	0	1
q_2	q_4	q_2	1	0
q_3	q_4	q_2	1	0
q_4	q_1	q_3	0	1

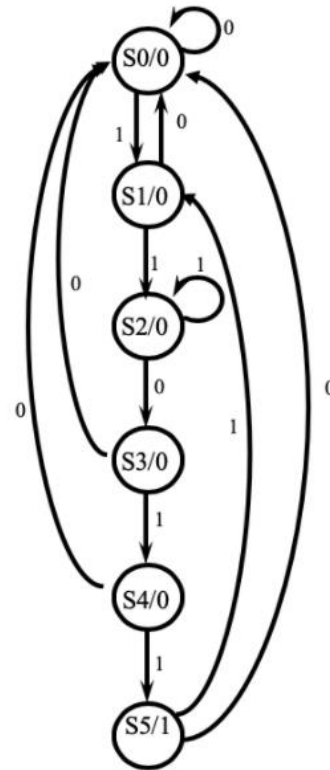
Example

Construct the state diagram of the following binary sequence:

a.) 1011 overlapping Mealy State Machine



b.) 11011 non-overlapping Moore State Machine



CHAPTER 4: FUNCTIONS

Relations and Functions

A function F from a set X to a set Y is a relation from X to Y that satisfies the following two properties:

1. For every element x in X , there is an element y in Y such that $(x,y) \in F$.
In other words every element of X is the first element of some ordered pair of F .
2. For all elements x in X and y and z in Y , if $(x,y) \in F$ and $(x,z) \in F$, then $y = z$
In other words no two distinct ordered pairs in F have the same first element

Example

Which of the relations define functions from $X = \{2,4,5\}$ to $Y = \{1,2,4,6\}$.

- a. $R_1 = \{(2,4), (4,1)\}$
- b. $R_2 = \{(2,4), (4,1), (4,2), (5,6)\}$
- c. $R_3 = \{(2,4), (4,1), (5,6)\}$

Solution

a. R_1 is not a function, because $5 \in X$ does not appear as the first element in any ordered pair in R_1 .

b. R_2 is not a function, because the ordered pairs $(4,1)$ and $(4,2)$ have the same first element but different second elements.

c. R_3 defines a function because it satisfy both the conditions of the function that is every element of X is the first element of some order pair and there is no pair which has the same first order pair but different second order pair.

Example

Let $A = \{4,5,6\}$ and $B = \{5,6\}$ and define binary relations R and S from A to B as follows:

- for all $(x,y) \in A \times B$, $(x,y) \in R \Leftrightarrow x \geq y$
- for all $(x,y) \in A \times B$, $xSy \Leftrightarrow 2 \mid (x-y)$

- a. Represent R and S as a set of ordered pairs.
- b. Indicate whether R or S is a function

Solution

a. Since we are given the relation R contains those order pairs of $A \times B$ which has their first element greater or equal to the second Hence R contains the order pairs.

$$R = \{(5,5), (6,5), (6,6)\}$$

Similarly S is such a relation which consists of those order pairs for which the difference of first and second elements difference divisible by 2.

$$\text{Hence } S = \{(4,6), (5,5), (6,6)\}$$

- b. R is not a function because $4 \in A$ is not related to any element of B .
 S clearly defines a function since each element of A is related to a unique element of B .

Function

A function f from a set X to a set Y is a relationship between elements of X and elements of Y such that each element of X is related to a unique element of Y , and is denoted $f : X \rightarrow Y$. The set X is called the domain of f and Y is called the co-domain of f .

Note: The unique element y of Y that is related to x by f is denoted $f(x)$ and is called f of x , or the value of f at x , or the image of x under f .

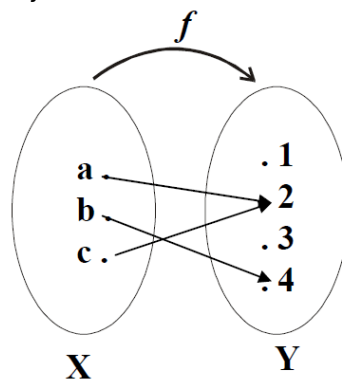
Arrow Diagram of a Function

The definition of a function implies that the arrow diagram for a function f has the following two properties:

1. Every element of X has an arrow coming out of it
2. No two elements of X has two arrows coming out of it that point to two different elements of Y .

Example

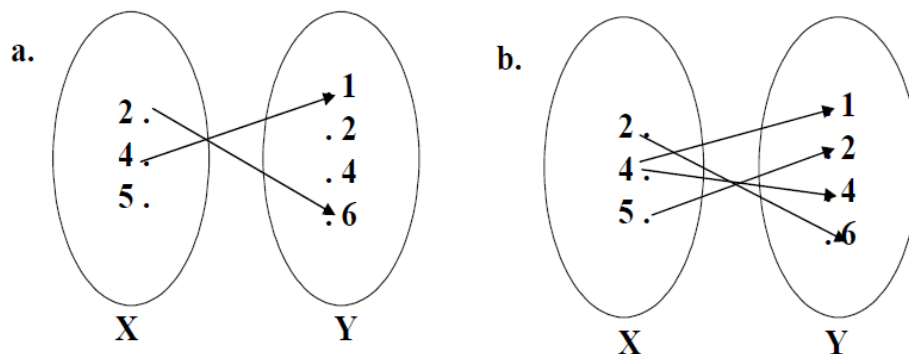
Let $X = \{a, b, c\}$ and $Y = \{1, 2, 3, 4\}$. Define a function f from X to Y by the arrow diagram.



You can easily note that the above diagram satisfy the two conditions of a function hence a graph of the function. Note that $f(a) = 2$, $f(b) = 4$, and $f(c) = 2$.

Functions and Nonfunctions

Which of the arrow diagrams define functions from $X = \{2, 4, 5\}$ to $Y = \{1, 2, 4, 6\}$.



The relation given in the diagram (a) is Not a function because there is no arrow coming out of $5 \in X$ to any element of Y .

The relation in the diagram (b) is Not a function, because there are two arrows coming out of $4 \in X$. i.e., $4 \in X$ is not related to a unique element of Y .

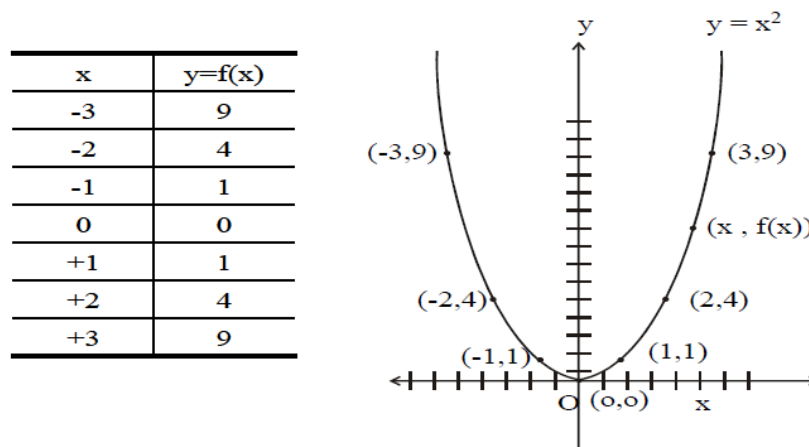
Graph of a Function

Let f be a real-valued function of a real variable. i.e. $f: \mathbb{R} \rightarrow \mathbb{R}$. The graph of f is the set of all points (x, y) in the Cartesian coordinate plane with the property that x is in the domain of f and $y = f(x)$.

Example

We have to draw the graph of the function f given by the relation $y = x^2$ in order to draw the graph of the function we will first take some elements from the domain will see the image of them and then plot them on the graph as follows

Graph of $y = x^2$.

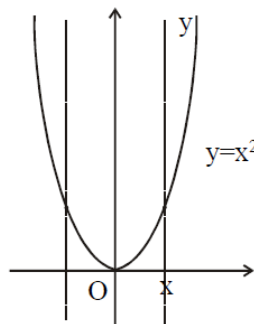


Vertical Line Test for the graph of a Function

For a graph to be the graph of a function, any given vertical line in its domain intersects the graph in at most one point.

Example

The graph of the relation $y = x^2$ on \mathbb{R} defines a function by vertical line test.

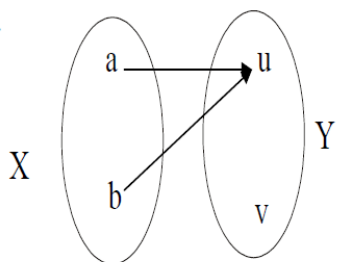


Example

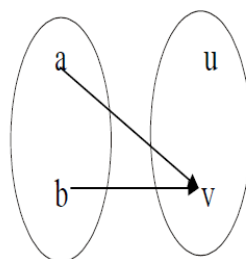
Find all functions from $X = \{a, b\}$ to $Y = \{u, v\}$

Solution

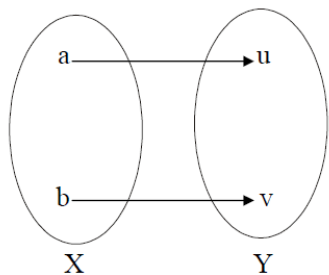
1.



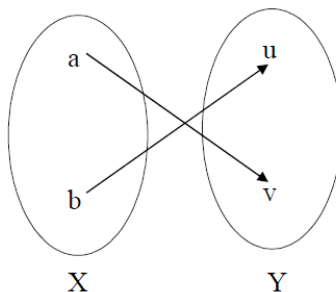
2.



3.



4.

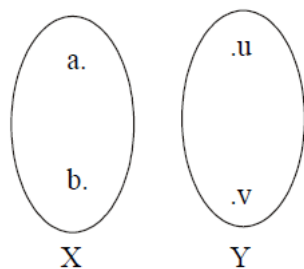
**Example**

Find four binary relations from $X = \{a,b\}$ to $Y = \{u,v\}$ that are not functions.

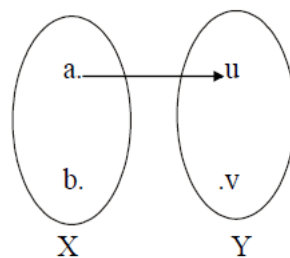
Solution

The four relations are

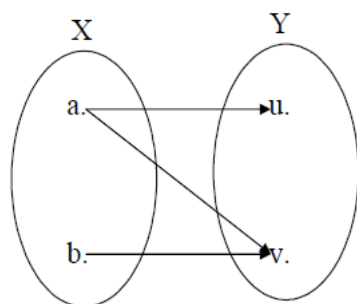
1.



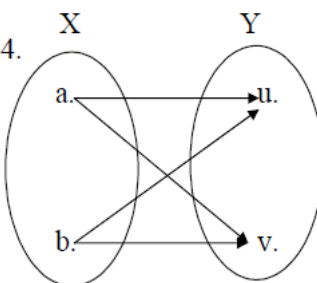
2.



3.



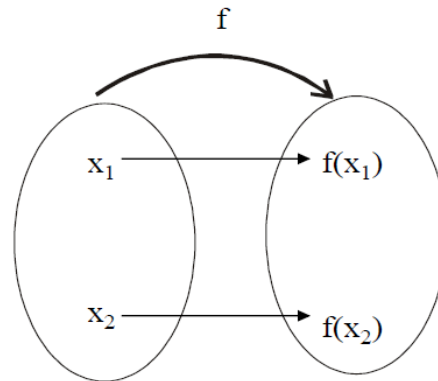
4.



TYPES OF FUNCTIONS

Injective or One-To-One Function

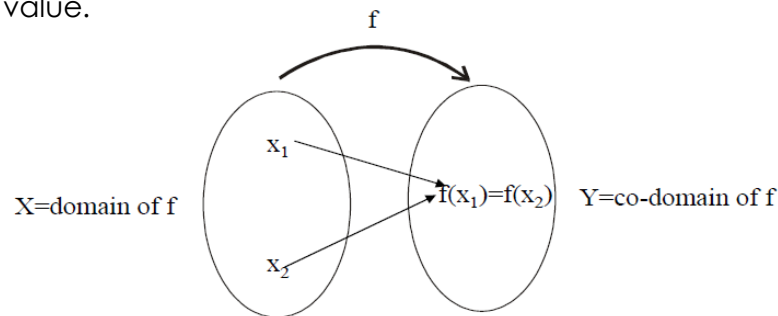
Let $f: X \rightarrow Y$ be a function. f is injective or one-to-one if, and only if, $\forall x_1, x_2 \in X$, if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$. That is, f is one-to-one if it maps distinct points of the domain into the distinct points of the co-domain.



A one-to-one function separates points.

Function Not One-To-One:

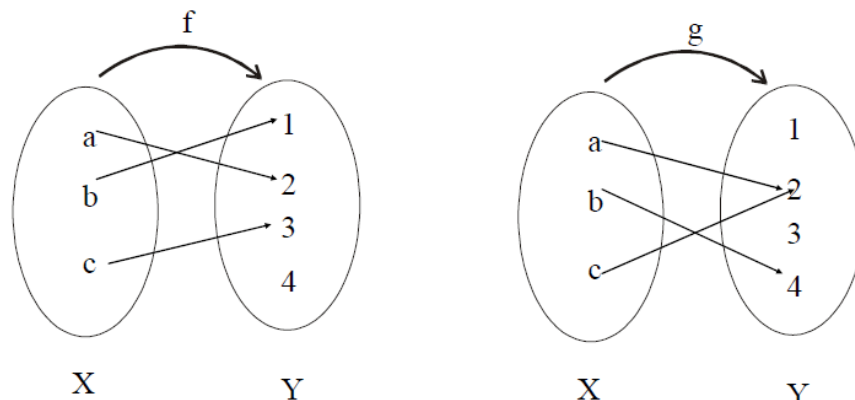
A function $f: X \rightarrow Y$ is not one-to-one iff there exist elements x_1 and x_2 in such that $x_1 \neq x_2$ but $f(x_1) = f(x_2)$. That is, if distinct elements x_1 and x_2 can be found in domain of f that have the same function value.



A function that is not one-to-one collapses points together

Example

Which of the arrow diagrams define one-to-one functions?



Solution

f is clearly one-to-one function, because no two different elements of X are mapped onto the same element of Y .

g is not one-to-one because the elements a and c are mapped onto the same element 2 of Y .

Alternative Definition For One-To-One Function:

A function $f: X \rightarrow Y$ is one-to-one (1-1) iff $\forall x_1, x_2 \in X$, if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$ (i.e distinct elements of 1st set have their distinct images in 2nd set). The equivalent contra-positive statement for this implication is $\forall x_1, x_2 \in X$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

Remark

$f: X \rightarrow Y$ is not one-to-one iff $\exists x_1, x_2 \in X$ with $f(x_1) = f(x_2)$ but $x_1 \neq x_2$

Example

Define $f: \mathbb{R} \rightarrow \mathbb{R}$ by the rule $f(x) = 4x - 1$ for all $x \in \mathbb{R}$. Is f one-to-one? Prove or give a counter example.

Solution

Let $x_1, x_2 \in \mathbb{R}$ such that $f(x_1) = f(x_2)$
 $\Rightarrow 4x_1 - 1 = 4x_2 - 1$ (by definition of f)
 $\Rightarrow 4x_1 = 4x_2$ (adding 1 to both sides)
 $\Rightarrow x_1 = x_2$ (dividing both sides by 4)

Thus we have shown that if $f(x_1) = f(x_2)$ then $x_1 = x_2$

Therefore, f is one-to-one

Example

Define $g: \mathbb{Z} \rightarrow \mathbb{Z}$ by the rule $g(n) = n^2$ for all $n \in \mathbb{Z}$. Is g one-to-one? Prove or give a counter example

Solution

Let $n_1, n_2 \in \mathbb{Z}$ and suppose $g(n_1) = g(n_2)$
 $\Rightarrow n_1^2 = n_2^2$ (by definition of g)
 \Rightarrow either $n_1 = +n_2$ or $n_1 = -n_2$

Thus $g(n_1) = g(n_2)$ does not imply $n_1 = n_2$ always.

As a counter example, let $n_1 = 2$ and $n_2 = -2$.

Then $g(n_1) = g(2) = 2^2 = 4$ and also $g(n_2) = g(-2) = (-2)^2 = 4$

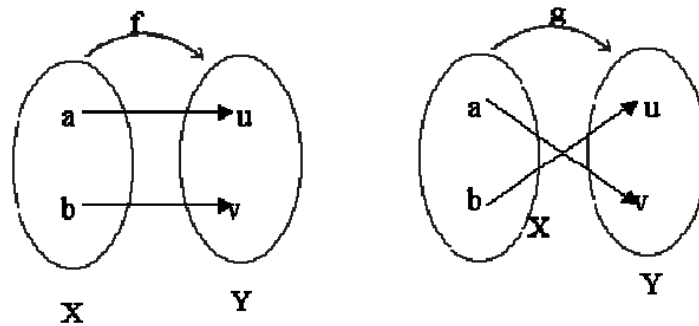
Hence $g(2) = g(-2)$ where as $2 \neq -2$ and so g is not one-to-one.

Example

Find all one-to-one functions from $X = \{a, b\}$ to $Y = \{u, v\}$

Solution

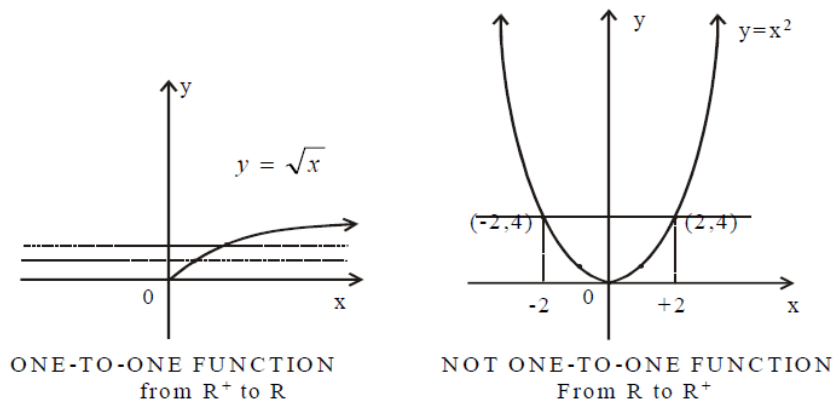
There are two one-to-one functions from X to Y defined by the arrow diagrams



Graph of One-To-One Function

A graph of a function f is one-to-one iff every horizontal line intersects the graph in at most one point.

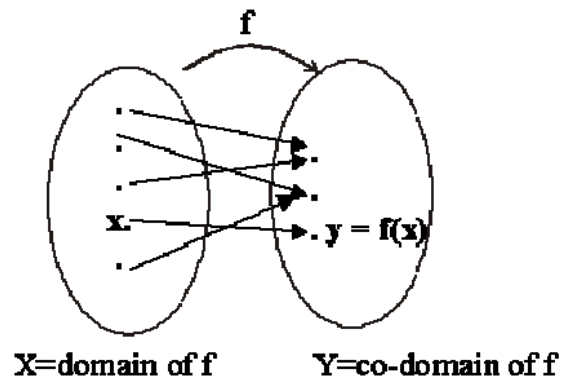
Example



Surjective Function or Onto Function

Let $f: X \rightarrow Y$ be a function. f is surjective or onto if, and only if, $\forall y \in Y, \exists x \in X$ such that $f(x) = y$.

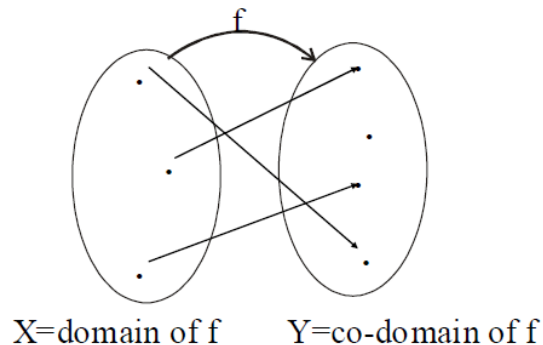
That is, f is onto if every element of its co-domain is the image of some element(s) of its domain i.e., co-domain of f = range of f



Each element y in Y equals $f(x)$ for at least one x in X

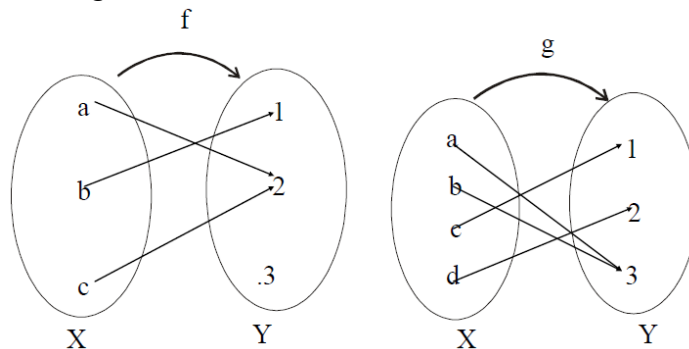
Function Not Onto

A function $f: X \rightarrow Y$ is not onto iff there exists $y \in Y$ such that $\forall x \in X, f(x) \neq y$. That is, there is some element in Y that is not the image of any element in X .



Example

Which of the arrow diagrams define onto functions?



Solution

f is not onto because $3 \neq f(x)$ for any x in X . g is clearly onto because each element of Y equals $g(x)$ for some x in X . as $1 = g(c)$; $2 = g(d)$; $3 = g(a) = g(b)$

Example

Define $f: \mathbb{R} \rightarrow \mathbb{R}$ by the rule $f(x) = 4x - 1$ for all $x \in \mathbb{R}$. Is f onto? Prove or give a counter example.

Solution

Let $y \in \mathbb{R}$. We search for an $x \in \mathbb{R}$ such that $f(x) = y$ or $4x - 1 = y$ (by definition of f)

Solving it for x , we find $x = \frac{y+1}{4} \in \mathbb{R}$.

Hence for every $y \in \mathbb{R}$, there exists $x = \frac{y+1}{4} \in \mathbb{R}$ such that $f(x) = f\left(\frac{y+1}{4}\right)$

$$f(x) = 4\left(\frac{y+1}{4}\right) - 1 = (y+1) - 1 = y$$

Hence f is onto.

Example

Define $h: \mathbb{Z} \rightarrow \mathbb{Z}$ by the rule

$h(n) = 4n - 1$ for all $n \in \mathbb{Z}$ Is h onto? Prove or give a counter example.

Solution

Let $m \in \mathbb{Z}$. We search for an $n \in \mathbb{Z}$ such that $h(n) = m$.
or $4n - 1 = m$ (by definition of h)

Solving it for n , we find $n = \frac{m+1}{4}$

But $n = \frac{m+1}{4}$ is not always an integer for all $m \in \mathbb{Z}$.

As a counter example, let $m = 0 \in \mathbb{Z}$, then $h(n) = 0$

$$\Rightarrow 4n - 1 = 0$$

$$\Rightarrow 4n = 1$$

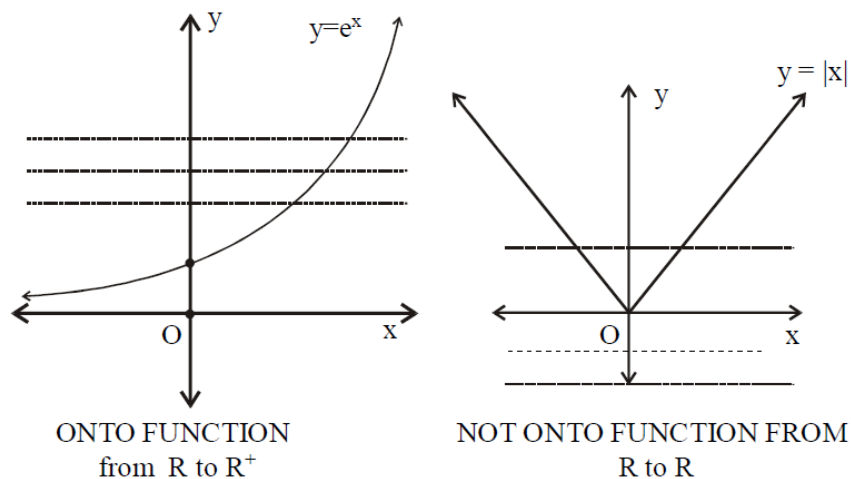
$$\Rightarrow n = \frac{1}{4} \notin \mathbb{Z}$$

Hence there is no integer n for which $h(n) = 0$.

Accordingly, h is not onto.

Graph of Onto Function

A graph of a function f is onto iff every horizontal line intersects the graph in at least one point.

Example**Example**

Let $X = \{1, 5, 9\}$ and $Y = \{3, 4, 7\}$. Define $g: X \rightarrow Y$ by specifying that $g(1) = 7$, $g(5) = 3$, $g(9) = 4$.
Is g one-to-one? Is g onto?

Solution

g is one-to-one because each of the three elements of X are mapped to a different elements of Y by g .

$$g(1) \neq g(5), g(1) \neq g(9), g(5) \neq g(9)$$

g is onto as well, because each of the three elements of co-domain Y of g is the image of some element of the domain of g .

$$3 = g(5), 4 = g(9), 7 = g(1)$$

Example

Define $f: P(\{a,b,c\}) \rightarrow \mathbb{Z}$ as follows: for all $A \in P(\{a,b,c\})$, $f(A)$ = the number of elements in A .

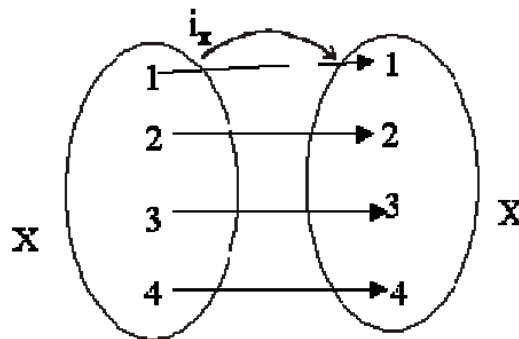
- Is f one-to-one? Justify.
- Is f onto? Justify.

Solution

- f is not one-to-one because $f(\{a\}) = 1$ and $f(\{b\}) = 1$ but $\{a\} \neq \{b\}$
- f is not onto because, there is no element of $P(\{a,b,c\})$ that is mapped to $4 \in \mathbb{Z}$.

Bijjective Function or One-To-One Correspondence

A function $f: X \rightarrow Y$ that is both one-to-one (injective) and onto (surjective) is called a bijective function or a one-to-one correspondence.

**Example**

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by the rule $f(x) = x^3$. Show that f is a bijective.

Solution

f is one-to-one

Let $f(x_1) = f(x_2)$ for $x_1, x_2 \in \mathbb{R}$

$$\Rightarrow x_1^3 = x_2^3$$

$$\Rightarrow x_1^3 - x_2^3 = 0$$

$$\Rightarrow (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) = 0$$

$$\Rightarrow x_1 - x_2 = 0 \text{ or } x_1^2 + x_1x_2 + x_2^2 = 0$$

$$\Rightarrow x_1 = x_2 \text{ (the second equation gives no real solution)}$$

Accordingly f is one-to-one.

f is onto

Let $y \in \mathbb{R}$. We search for a $x \in \mathbb{R}$ such that

$$f(x) = y$$

$$\Rightarrow x^3 = y \text{ (by definition of } f)$$

$$\text{or } x = (y)^{1/3}$$

Hence for $y \in \mathbb{R}$, there exists $x = (y)^{1/3} \in \mathbb{R}$ such that

$$f(x) = f((y)^{1/3})$$

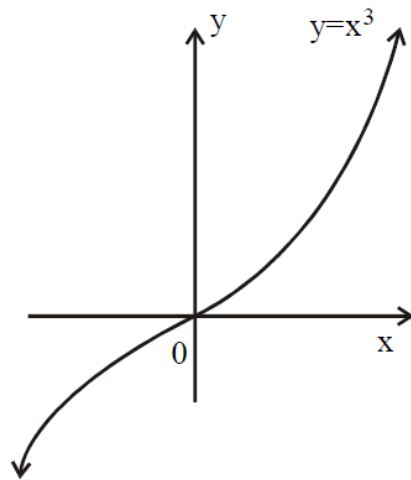
$$= ((y)^{1/3})^3 = y$$

Accordingly f is onto.

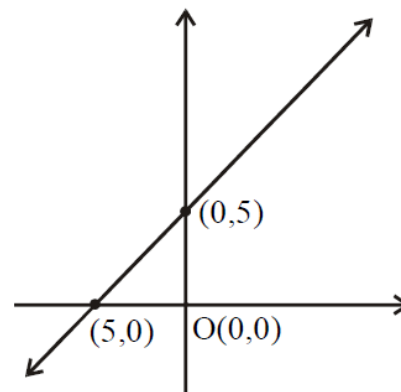
Thus, f is a bijective.

Graph of Bijective Function

A graph of a function f is bijective iff every horizontal line intersects the graph at exactly one point.



BIJECTIVE FUNCTION
from \mathbb{R} to \mathbb{R}



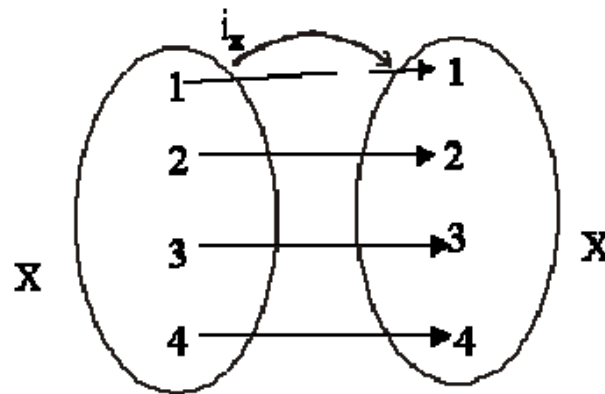
BIJECTIVE FUNCTION
from \mathbb{R} to \mathbb{R}

Identity Function on a Set

Given a set X , define a function i_X from X to X by $i_X(x) = x$ from all $x \in X$. The function i_X is called the identity function on X because it sends each element of X to itself.

Example

Let $X = \{1, 2, 3, 4\}$. The identity function i_X on X is represented by the arrow diagram



Example

Let X be a non-empty set. Prove that the identity function on X is bijective.

Solution

Let $i_X: X \rightarrow X$ be the identity function defined as $i_X(x) = x \forall x \in X$

1. i_X is injective (one-to-one)

Let $i_X(x_1) = i_X(x_2)$ for $x_1, x_2 \in X$

$\Rightarrow x_1 = x_2$ (by definition of i_X)

Hence i_X is one-to-one.

2. i_x is surjective (onto)

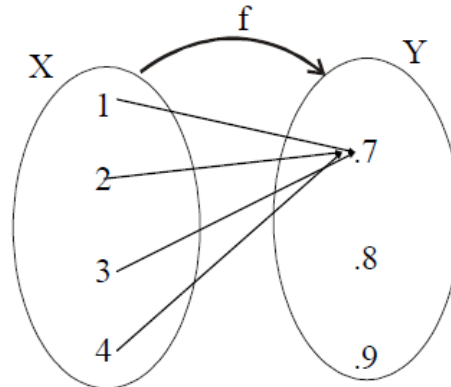
Let $y \in X$ (co-domain of i_x) Then there exists $y \in X$ (domain of i_x) such that $i_x(y) = y$ Hence i_x is onto. Thus, i_x being injective and surjective is bijective.

Constant Function

A function $f: X \rightarrow Y$ is a constant function if it maps (sends) all elements of X to one element of Y i.e. $\forall x \in X, f(x) = c$, for some $c \in Y$.

Example

The function f defined by the arrow diagram is constant.



Remark:

1. A constant function is one-to-one iff its domain is a singleton.
2. A constant function is onto iff its co-domain is a singleton.

Equality of Functions

Suppose f and g are functions from X to Y . Then f equals g , written $f = g$, if, and only if, $f(x) = g(x)$ for all $x \in X$.

Example

Define $f: \mathbb{R} \rightarrow \mathbb{R}$ and $g: \mathbb{R} \rightarrow \mathbb{R}$ by formulas:

$$f(x) = |x| \text{ for all } x \in \mathbb{R}$$

$$g(x) = \sqrt{x^2} \text{ for all } x \in \mathbb{R}$$

Since the absolute value of a real number equals to square root of its square

i.e. $|x| = \sqrt{x^2}$ for all $x \in \mathbb{R}$

Therefore $f(x) = g(x)$ for all $x \in \mathbb{R}$

Hence $f = g$

Example

Define functions f and g from \mathbb{R} to \mathbb{R} by formulas:

$$f(x) = 2x \text{ and } g(x) = \frac{2x^3 + 2x}{x^2 + 1} \text{ for all } x \in \mathbb{R}$$

Show that $f = g$

Solution

$$g(x) = \frac{2x^3 + 2x}{x^2 + 1}$$

$$g(x) = \frac{2x(x^2 + 1)}{x^2 + 1} = 2x$$

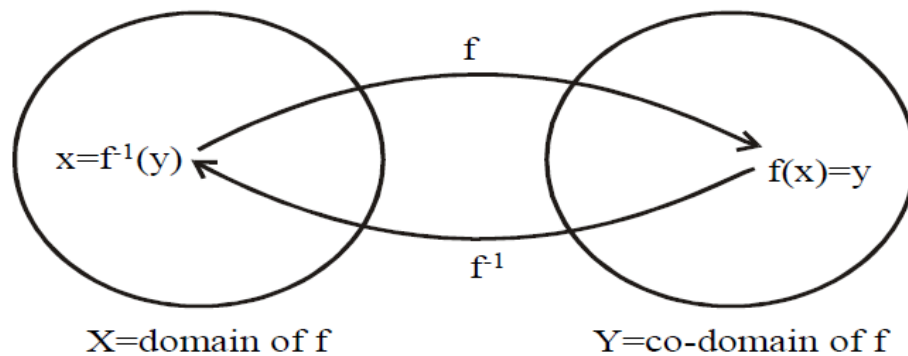
$$g(x) = f(x) \quad \text{for all } x \in \mathbb{R}$$

Inverse Function

Suppose $f: X \rightarrow Y$ is a bijective function. Then the inverse function $f^{-1}: Y \rightarrow X$ is defined as:

$$\forall y \in Y, f^{-1}(y) = x \Leftrightarrow y = f(x)$$

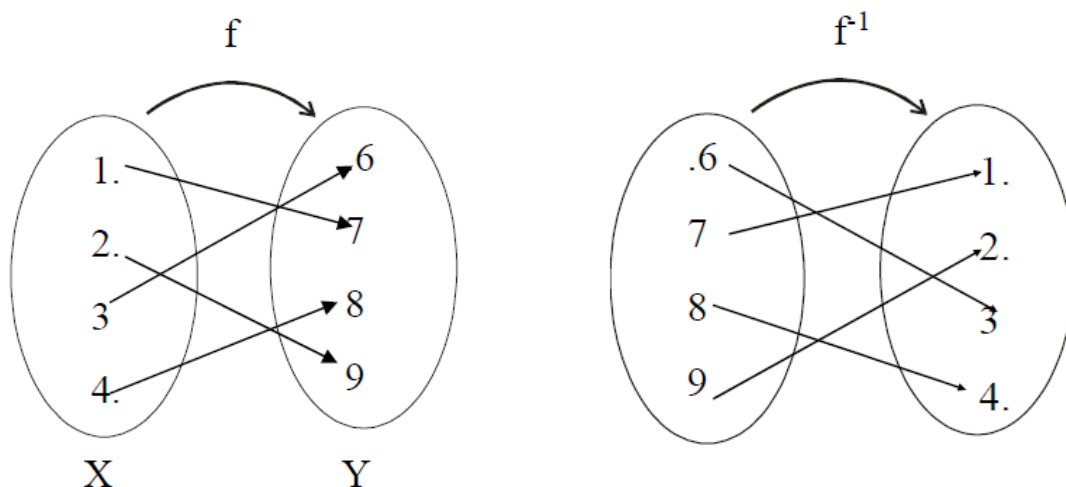
That is, f^{-1} sends each element of Y back to the element of X that it came from under f .

**Remark**

A function whose inverse function exists is called an invertible function.

Inverse Function from an Arrow Diagram

Let the bijection $f: X \rightarrow Y$ be defined by the arrow diagram. The inverse function $f^{-1}: Y \rightarrow X$ is represented below by the arrow diagram.

**Inverse Function from a Formula**

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by the formula $f(x) = 4x - 1 \quad \forall x \in \mathbb{R}$. Then f is bijective, therefore f^{-1} exists.

By definition of f^{-1} ,

$$f^{-1}(y) = x \Leftrightarrow f(x) = y$$

Now solving $f(x) = y$ for x

$$\Leftrightarrow 4x-1 = y \text{ (by definition of } f)$$

$$\Leftrightarrow 4x = y + 1$$

$$\Leftrightarrow x = \frac{y+1}{4}$$

Hence, $f^{-1}(y) = \frac{y+1}{4}$ is the inverse of $f(x)=4x-1$ which defines $f^{-1}: \mathbb{R} \rightarrow \mathbb{R}$.

Working Rule to find Inverse Function

Let $f: X \rightarrow Y$ be a one-to-one correspondence defined by the formula $f(x)=y$.

1. Solve the equation $f(x) = y$ for x in terms of y .
2. $f^{-1}(y)$ equals the right hand side of the equation found in step 1.

Example

Let a function f be defined on a set of real numbers as

$$f(x) = \frac{x+1}{x-1} \text{ for all real numbers } x \neq 1.$$

1. Show that f is a bijective function on $\mathbb{R} - \{1\}$.
2. Find the inverse function f^{-1} .

Solution

1. To show f is injective

Let $x_1, x_2 \in \mathbb{R} - \{1\}$ and suppose

$f(x_1) = f(x_2)$ we have to show that $x_1 = x_2$

$$\Rightarrow \frac{x_1+1}{x_1-1} = \frac{x_2+1}{x_2-1} \quad (\text{by definition of } f)$$

$$\Rightarrow (x_1 + 1)(x_2 - 1) = (x_2 + 1)(x_1 - 1)$$

$$\Rightarrow x_1x_2 - x_1 + x_2 - 1 = x_1x_2 - x_2 + x_1 - 1$$

$$\Rightarrow -x_1 + x_2 = -x_2 + x_1$$

$$\Rightarrow 2x_1 = 2x_2$$

$$\Rightarrow x_1 = x_2$$

Hence f is injective.

Next to show that f is surjective

Let $y \in \mathbb{R} - \{1\}$. We look for an $x \in \mathbb{R} - \{1\}$ such that $f(x) = y$.

$$\Rightarrow x + 1 = y(x-1)$$

$$\Rightarrow 1 + y = xy - x$$

$$\Rightarrow 1 + y = x(y-1)$$

$$\Rightarrow x = \frac{y+1}{y-1}$$

Thus for each $y \in \mathbb{R} - \{1\}$, there exists $x = \frac{y+1}{y-1} \in \mathbb{R} - \{1\}$ such that $f(x) = f\left(\frac{y+1}{y-1}\right) = y$

2. Inverse function of f

The given function f is defined by the rule

$$f(x) = \frac{x+1}{x-1} = y$$

$$\Rightarrow x+1 = y(x-1)$$

$$\Rightarrow 1+y = xy-x$$

$$\Rightarrow 1+y = x(y-1)$$

$$\Rightarrow x = \frac{y+1}{y-1}$$

Hence

$$f^{-1}(y) = \frac{y+1}{y-1}, y \neq 1$$

Example

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x^3 + 5$

Show that f is one-to-one and onto. Find a formula that defines the inverse function f^{-1} .

Solution

1. f is one-to-one

Let $f(x_1) = f(x_2)$ for $x_1, x_2 \in \mathbb{R}$

$$\Rightarrow x_1^3 + 5 = x_2^3 + 5$$

$$\Rightarrow x_1^3 = x_2^3$$

$$\Rightarrow x_1 = x_2$$

(by definition of f)

(subtracting 5 on both sides)

Hence f is one-to-one.

2. f is onto

Let $y \in \mathbb{R}$. We search for an $x \in \mathbb{R}$ such that $f(x) = y$.

$$\Rightarrow x^3 + 5 = y$$

(by definition of f)

$$\Rightarrow x^3 = y - 5$$

$$\Rightarrow x = \sqrt[3]{y-5}$$

Thus for each $y \in \mathbb{R}$, there exists $x = \sqrt[3]{y-5} \in \mathbb{R}$ such that

$$f(x) = f(\sqrt[3]{y-5})$$

$$f(x) = (\sqrt[3]{y-5})^3 + 5$$

(by definition of f)

$$f(x) = y - 5 + 5 = y$$

Hence f is onto.

3. formula for f^{-1}

f is defined by $y = f(x) = x^3 + 5$

$$\Rightarrow y-5 = x^3$$

$$\Rightarrow x = \sqrt[3]{y-5}$$

Hence $f^{-1}(x) = \sqrt[3]{x-5}$ which defines the inverse function.

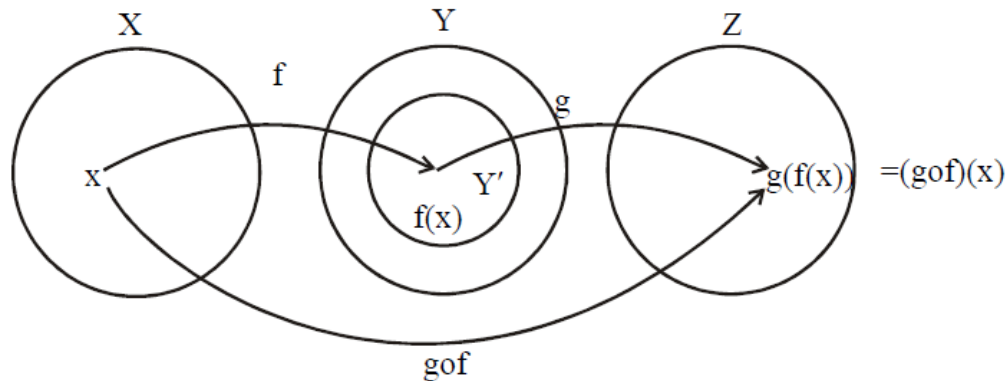
COMPOSITION OF FUNCTIONS

Let $f: X \rightarrow Y'$ and $g: Y \rightarrow Z$ be functions with the property that the range of f is a subset of the domain of g i.e. $f(X) \subseteq Y$.

Define a new function $g \circ f$ of: $X \rightarrow Z$ as follows

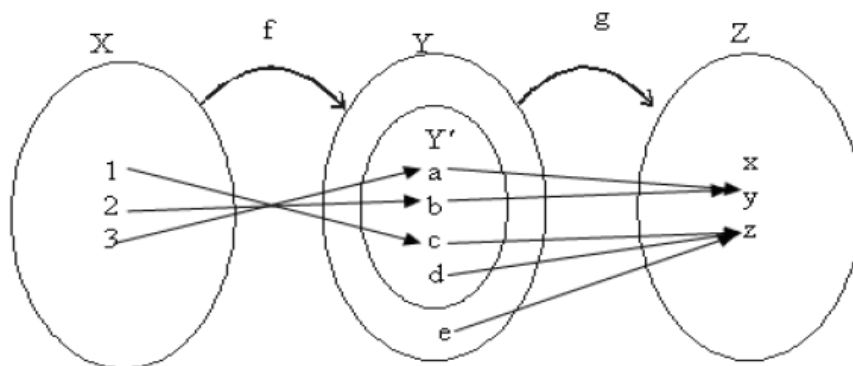
$$(g \circ f)(x) = g(f(x)) \text{ for all } x \in X$$

The function $g \circ f$ is called the composition of f and g .

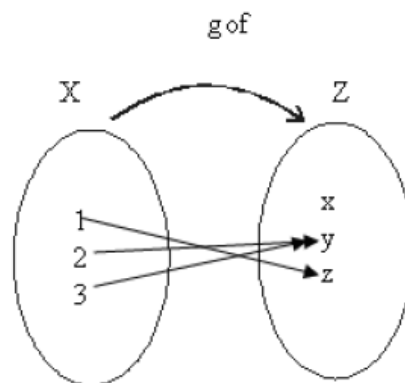


Composition of Functions defined by Arrow Diagrams

Let $X = \{1, 2, 3\}$, $Y' = \{a, b, c, d\}$, $Y = \{a, b, c, d, e\}$ and $Z = \{x, y, z\}$. Define functions $f: X \rightarrow Y'$ and $g: Y \rightarrow Z$ by the arrow diagrams:



Then $g \circ f: X \rightarrow Z$ is represented by the arrow diagram.



Example

Let $A = \{1, 2, 3, 4, 5\}$ and we define functions $f: A \rightarrow A$ and then $g: A \rightarrow A$:

$$\begin{array}{ccccc} f(1)=3, & f(2)=5, & f(3)=3, & f(4)=1, & f(5)=2 \\ g(1)=4, & g(2)=1, & g(3)=1, & g(4)=2, & g(5)=3 \end{array}$$

Find the composition functions $f \circ g$ and $g \circ f$.

Solution

We use the definition of the composition of functions and compute:

$$\begin{aligned} (f \circ g)(1) &= f(g(1)) = f(4) = 1 \\ (f \circ g)(2) &= f(g(2)) = f(1) = 3 \\ (f \circ g)(3) &= f(g(3)) = f(1) = 3 \\ (f \circ g)(4) &= f(g(4)) = f(2) = 5 \\ (f \circ g)(5) &= f(g(5)) = f(3) = 3 \end{aligned}$$

Also

$$\begin{aligned} (g \circ f)(1) &= g(f(1)) = g(3) = 1 \\ (g \circ f)(2) &= g(f(2)) = g(5) = 3 \\ (g \circ f)(3) &= g(f(3)) = g(3) = 1 \\ (g \circ f)(4) &= g(f(4)) = g(1) = 4 \\ (g \circ f)(5) &= g(f(5)) = g(2) = 1 \end{aligned}$$

Remark: The functions $f \circ g$ and $g \circ f$ are not equal.

Composition of Functions defined by Formulas

Let $f: \mathbb{Z} \rightarrow \mathbb{Z}$ and $g: \mathbb{Z} \rightarrow \mathbb{Z}$ be defined by:

$$\begin{aligned} f(n) &= n+1 & \text{for } n \in \mathbb{Z} \\ g(n) &= n^2 & \text{for } n \in \mathbb{Z} \end{aligned}$$

- Find the compositions $g \circ f$ and $f \circ g$.
- Is $g \circ f = f \circ g$?

Solution

- By definition of the composition of functions

$$\begin{aligned} (g \circ f)(n) &= g(f(n)) = g(n+1) = (n+1)^2 \text{ for all } n \in \mathbb{Z} \text{ and} \\ (f \circ g)(n) &= f(g(n)) = f(n^2) = n^2 + 1 \text{ for all } n \in \mathbb{Z} \end{aligned}$$

- Two functions from one set to another are equal if, and only if, they take the same values. In this case,

$$\begin{aligned} (g \circ f)(1) &= g(f(1)) = (1+1)^2 = 4 \text{ where as} \\ (f \circ g)(1) &= f(g(1)) = 1^2 + 1 = 2 \end{aligned}$$

Thus $f \circ g \neq g \circ f$

Remark: The composition of functions is not a commutative operation.

Composition with the Identity Function

Let $X = \{a, b, c, d\}$ and $Y = \{u, v, w\}$ and suppose $f: X \rightarrow Y$ be defined by:

$$f(a) = u, f(b) = v, f(c) = v, f(d) = u$$

Find $f \circ i_X$ and $i_Y \circ f$, where i_X and i_Y are identity functions on X and Y respectively.

Solution

The values of foi_x on X are obtained as:

$$(foi_x)(a) = f(i_x(a)) = f(a) = u$$

$$(foi_x)(b) = f(i_x(b)) = f(b) = v$$

$$(foi_x)(c) = f(i_x(c)) = f(c) = v$$

$$(foi_x)(d) = f(i_x(d)) = f(d) = u$$

For all elements x in X $(foi_x)(x) = f(x)$ so that $foi_x = f$

The values of i_yof on X are obtained as:

$$(i_yof)(a) = i_y(f(a)) = i_y(u) = u$$

$$(i_yof)(b) = i_y(f(b)) = i_y(v) = v$$

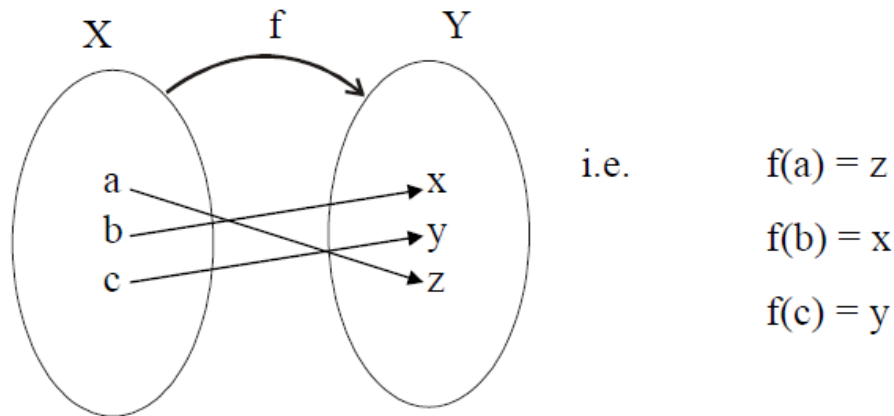
$$(i_yof)(c) = i_y(f(c)) = i_y(v) = v$$

$$(i_yof)(d) = i_y(f(d)) = i_y(u) = u$$

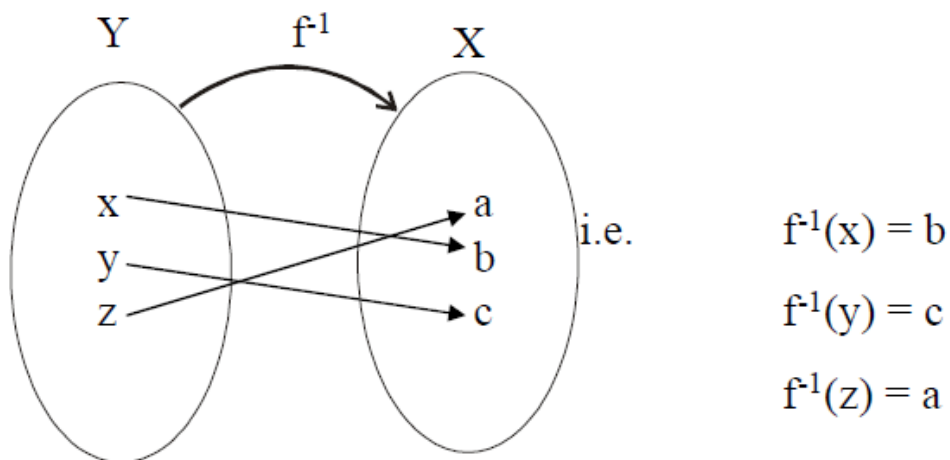
For all elements x in X $(i_yof)(x) = f(x)$ so that $i_yof = f$

Composing a Function with its Inverse

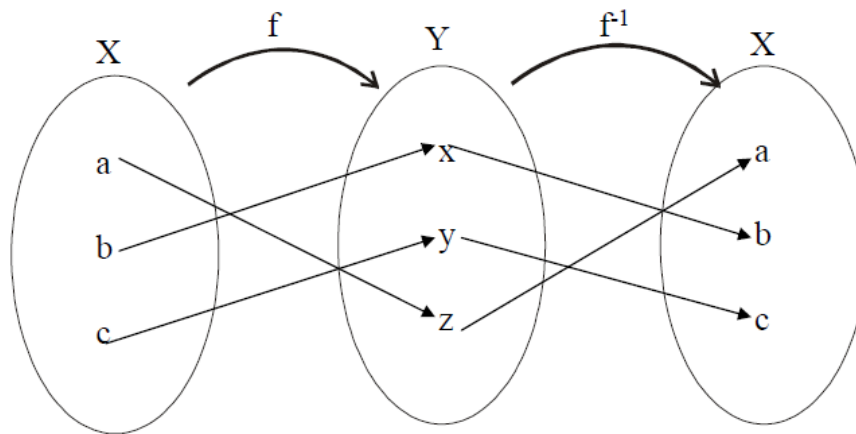
Let $X = \{a, b, c\}$ and $Y = \{x, y, z\}$. Define $f: X \rightarrow Y$ by the arrow diagram.



Then f is one-to-one and onto. So f^{-1} exists and is represented by the arrow diagram below



$f^{-1}of$ is found by following the arrows from X to Y by f and back to X by f^{-1} .



Thus, it is quite clear that

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(x) = a$$

$$(f^{-1} \circ f)(b) = f^{-1}(f(b)) = f^{-1}(y) = b \text{ and } (f^{-1} \circ f)(c) = f^{-1}(f(c)) = f^{-1}(z) = c$$

Remark 1

$f^{-1} \circ f : X \rightarrow X$ sends each element of X to itself. So by definition of identity function on X , $f^{-1} \circ f = i_X$. Similarly, the composition of f and f^{-1} sends each element of Y to itself. Accordingly $f \circ f^{-1} = i_Y$.

Remark 2

The function $f: X \rightarrow Y$ and $g: Y \rightarrow X$ are inverses of each other iff $g \circ f = i_X$ and $f \circ g = i_Y$.

Example

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ and $g: \mathbb{R} \rightarrow \mathbb{R}$ be defined by

$$f(x) = 3x + 2 \quad \text{for all } x \in \mathbb{R}$$

$$\text{and } g(x) = \frac{x-2}{3} \quad \text{for all } x \in \mathbb{R}$$

Show that f and g are inverse of each other.

Solution

f and g are inverse of each other iff their composition gives the identity function. Now for all $x \in \mathbb{R}$,

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) \\ &= g(3x + 2) && \text{(by definition of } f) \\ &= \frac{(3x+2)-2}{3} && \text{(by definition of } g) \\ &= \frac{3x}{3} \\ &= x \end{aligned}$$

$$\begin{aligned} (f \circ g)(x) &= f(g(x)) \\ &= f\left(\frac{x-2}{3}\right) && \text{(by definition of } f) \\ &= 3\left(\frac{x-2}{3}\right) + 2 && \text{(by definition of } g) \\ &= x - 2 + 2 = x \end{aligned}$$

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

Hence $g \circ f$ and $f \circ g$ are identity functions. Accordingly f and g are inverse of each other.

OPERATIONS ON FUNCTIONS

Sum of Functions

Let f and g be real valued functions with the same domain X . That is $f: X \rightarrow \mathbb{R}$ and $g: X \rightarrow \mathbb{R}$. The sum of f and g denoted by $f+g$ is a real valued function with the same domain X i.e. $f+g: X \rightarrow \mathbb{R}$ defined by

$$(f+g)(x) = f(x) + g(x) \quad \forall x \in X$$

Example

Let $f(x) = x^2 + 1$ and $g(x) = x + 2$ defines functions f and g from \mathbb{R} to \mathbb{R} .

$$\begin{aligned} \text{Then } (f+g)(x) &= f(x) + g(x) \\ &= (x^2 + 1) + (x + 2) \\ &= x^2 + x + 3 \quad \forall x \in \mathbb{R} \end{aligned}$$

which defines the sum functions $f+g: X \rightarrow \mathbb{R}$

Difference of Functions

Let $f: X \rightarrow \mathbb{R}$ and $g: X \rightarrow \mathbb{R}$ be real valued functions. The difference of f and g denoted by $f-g$ which is a function from X to \mathbb{R} defined by

$$(f - g)(x) = f(x) - g(x) \quad \forall x \in X$$

Example

Let $f(x) = x^2 + 1$ and $g(x) = x + 2$ define functions f and g from \mathbb{R} to \mathbb{R} .

$$\begin{aligned} \text{Then } (f-g)(x) &= f(x) - g(x) \\ &= (x^2 + 1) - (x + 2) \\ &= x^2 - x - 1 \quad \forall x \in \mathbb{R} \end{aligned}$$

which defines the difference function $f-g: X \rightarrow \mathbb{R}$

Product of Functions

Let $f: X \rightarrow \mathbb{R}$ and $g: X \rightarrow \mathbb{R}$ be real valued functions. The product of f and g denoted $f \cdot g$ or simply fg is a function from X to \mathbb{R} defined by

$$(f \cdot g)(x) = f(x) \cdot g(x) \quad \forall x \in X$$

Example

Let $f(x) = x^2 + 1$ and $g(x) = x + 2$ define functions f and g from \mathbb{R} to \mathbb{R} .

$$\begin{aligned} \text{Then } (f \cdot g)(x) &= f(x) \cdot g(x) \\ &= (x^2 + 1) \cdot (x + 2) \\ &= x^3 + 2x^2 + x + 2 \quad \forall x \in \mathbb{R} \end{aligned}$$

which defines the product function $f \cdot g: X \rightarrow \mathbb{R}$

Quotient Of Functions:

Let $f: X \rightarrow \mathbb{R}$ and $g: X \rightarrow \mathbb{R}$ be real valued functions. The quotient of f by g denoted by f/g is a function from X to \mathbb{R} defined by

$$\left(\frac{f}{g}\right)(x) = \frac{f(x)}{g(x)}, \text{ where } g(x) \neq 0$$

Example

Let $f(x) = x^2 + 1$ and $g(x) = x + 2$ defines functions f and g from R to R .

Then

$$\begin{aligned}\left(\frac{f}{g}\right)(x) &= \frac{f(x)}{g(x)}, \forall x \in X \text{ \& } g(x) \neq 0 \\ &= \frac{x^2 + 1}{x + 2}\end{aligned}$$

which defines the quotient function $\frac{f}{g}: X \rightarrow R$

Scalar Multiplication

Let $f: X \rightarrow R$ be a real valued function and c is a non-zero number. Then the scalar multiplication of f is a function $c \cdot f: R \rightarrow R$ defined by $(c \cdot f)(x) = c \cdot f(x) \forall x \in X$

Example

Let $f(x) = x^2 + 1$ and $g(x) = x + 2$ defines functions f and g from R to R .

Then

$$\begin{aligned}(3f - 2g)(x) &= (3f)(x) - (2g)(x) \\ &= 3 \cdot f(x) - 2 \cdot g(x) \\ &= 3(x^2 + 1) - 2(x + 2) \\ &= 3x^2 - 2x - 1 \quad \forall x \in X\end{aligned}$$

Example

Given a set S and a subset A , the characteristics function of A , denoted χ_A , is the function defined from S to the set $\{0, 1\}$ defined as

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

Show that for all subsets A and B of S

1. $\chi_{A \cap B} = \chi_A \cdot \chi_B$
2. $\chi_{A \cup B} = \chi_A + \chi_B - \chi_{A \cap B}$

Solution

1. Prove that $\chi_{A \cap B} = \chi_A \cdot \chi_B$.

Let $x \in A \cap B$; therefore $x \in A$ and $x \in B$. Then $\chi_{A \cap B}(x) = 1$; $\chi_A(x) = 1$; $\chi_B(x) = 1$

$$\text{Hence } \chi_{A \cap B}(x) = 1 = (1)(1) = \chi_A(x) \chi_B(x) = (\chi_A \cdot \chi_B)(x)$$

Next, let $y \in (A \cap B)'$

$$\begin{aligned}\Rightarrow y &\in A' \cup B' \\ \Rightarrow y &\in A' \text{ or } y \in B'\end{aligned}$$

Now $y \in (A \cap B)'$ i.e. $y \notin (A \cap B)$

$$\Rightarrow \chi_{A \cap B}(y) = 0$$

and $y \in A'$ or $y \in B'$

$$\Rightarrow \chi_A(y) = 0 \text{ (as } y \notin A) \text{ or } \chi_B(y) = 0 \text{ (as } y \notin B)$$

$$\text{Thus } \chi_{A \cap B}(y) = 0 = (0)(0) = \chi_A(y) \chi_B(y) = (\chi_A \cdot \chi_B)(y)$$

Hence, $\chi_{A \cap B}$ and $\chi_A \cdot \chi_B$ assign the same number to each element x in S , so by definition $\chi_{A \cap B} = \chi_A \cdot \chi_B$.

2. Prove that $\chi_{A \cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B$

Let $x \in A \cup B$ then $x \in A$ or $x \in B$

Now $\chi_{A \cup B}(x) = 1$ and $\chi_A(x) = 1$ or $\chi_B(x) = 1$

Three cases arise depending upon which of $\chi_A(x)$ or $\chi_B(x)$ is 1.

CASE 1: (if $\chi_A(x) = 1$ & $\chi_B(x) = 1$)

$$\begin{aligned} \text{Now } \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x) \\ = 1 + 1 - (1)(1) \\ = 1 = \chi_{A \cup B}(x) \end{aligned}$$

CASE 2: (if $\chi_A(x) = 1$; $\chi_B(x) = 0$)

$$\begin{aligned} \text{Now } \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x) \\ = 1 + 0 - (1)(0) \\ = 1 \\ = \chi_{A \cup B}(x) \end{aligned}$$

CASE 3: (if $\chi_A(x) = 0$; $\chi_B(x) = 1$)

$$\begin{aligned} \text{Now } \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x) \\ = 0 + 1 - (0)(1) \\ = 1 \\ = \chi_{A \cup B}(x) \end{aligned}$$

Thus in all cases

$$\chi_{A \cup B}(x) = 1 = \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x) \quad \forall x \in A \cup B$$

Next let $y \notin A \cup B$. Then $y \in (A \cup B)'$

$$\Rightarrow y \in A' \cap B' \text{ (DeMorgan's Law)}$$

$$\Rightarrow y \in A' \text{ and } y \in B'$$

$$\Rightarrow y \notin A \text{ and } y \notin B$$

$$\text{Thus } \chi_{A \cup B}(y) = 0; \chi_A(y) = 0; \chi_B(y) = 0$$

$$\text{Consider } \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x)$$

$$= 0 + 0 - 0$$

$$= 0$$

$$= \chi_{A \cup B}(y)$$

Hence for all elements of S

$$\chi_{A \cup B} = \chi_A + \chi_B - \chi_{A \cap B}$$

CHAPTER 5: COMBINATORICS

Definition: Combinatorics is the mathematics of counting and arranging objects. Counting of objects with certain properties (enumeration) is required to solve many different types of problem.

For example, counting is used to:

- 1) Determine number of ordered or unordered arrangement of objects.
- 2) Generate all the arrangements of a specified kind which is important in computer simulations.
- 3) Compute probabilities of events.
- 4) Analyze the chance of winning games, lotteries etc.
- 5) Determine the complexity of algorithms.

The Sum Rule

If one event can occur in n_1 ways, a second event can occur in n_2 (different) ways, then the total number of ways in which exactly one of the events (i.e., first or second) can occur is $n_1 + n_2$.

Example

Suppose there are 7 different optional courses in Computer Science and 3 different optional courses in Mathematics. Then there are $7 + 3 = 10$ choices for a student who wants to take one optional course.

Example

A student can choose a computer project from one of the three lists. The three lists contain 23, 15 and 19 possible projects, respectively. How many possible projects are there to choose from?

Solution

The student can choose a project from the first list in 23 ways, from the second list in 15 ways, and from the third list in 19 ways. Hence, there are $23 + 15 + 19 = 57$ projects to choose from.

The Product Rule

If one event can occur in n_1 ways and if for each of these n_1 ways, a second event can occur in n_2 ways, then the total number of ways in which both events occur is $n_1 \cdot n_2$.

Example

Suppose there are 7 different optional courses in Computer Science and 3 different optional courses in Mathematics. A student who wants to take one optional course of each subject, there are $7 \times 3 = 21$ choices.

Example

The chairs of an auditorium are to be labeled with two characters, a letter followed by a digit. What is the largest number of chairs that can be labeled differently?

Solution

The procedure of labeling a chair consists of two events, namely,

1. Assigning one of the 26 letters: A, B, C, ..., Z and
2. Assigning one of the 10 digits: 0, 1, 2, ..., 9

By product rule, there are $26 \times 10 = 260$ different ways that a chair can be labeled by both a letter and a digit.

Example

Find the number n of ways that an organization consisting of 15 members can elect a president, treasurer, and secretary. (assuming no person is elected to more than one position)

Solution

The president can be elected in 15 different ways; following this, the treasurer can be elected in 14 different ways; and following this, the secretary can be elected in 13 different ways.

Thus, by product rule, there are $n = 15 \times 14 \times 13 = 2730$ different ways in which the organization can elect the officers.

Example

There are four bus lines between A and B; and three bus lines between B and C. Find the number of ways a person can travel:

- (a) By bus from A to C by way of B;
- (b) Round trip by bus from A to C by way of B;
- (c) Round trip by bus from A to C by way of B, if the person does not want to use a bus line more than once.

Solution

(a) There are 4 ways to go from A to B and 3 ways to go from B to C; hence there are $4 \times 3 = 12$ ways to go from A to C by way of B.

(b) The person will travel from A to B to C to B to A for the round trip. i.e. $(A \rightarrow B \rightarrow C \rightarrow B \rightarrow A)$. The person can travel 4 ways from A to B and 3 way from B to C and back.

$$\text{i.e., } \overset{4}{A} \rightarrow \overset{3}{B} \rightarrow \overset{3}{C} \rightarrow \overset{4}{B} \rightarrow A$$

Thus there are $4 \times 3 \times 3 \times 4 = 144$ ways to travel the round trip.

(c) The person can travel 4 ways from A to B and 3 ways from B to C, but only 2 ways from C to B and 3 ways from B to A, since bus line cannot be used more than once.

Thus

$$\text{i.e., } \overset{4}{A} \rightarrow \overset{3}{B} \rightarrow \overset{2}{C} \rightarrow \overset{3}{B} \rightarrow A$$

Hence there are $4 \times 3 \times 2 \times 3 = 72$ ways to travel the round trip without using a bus line more than once.

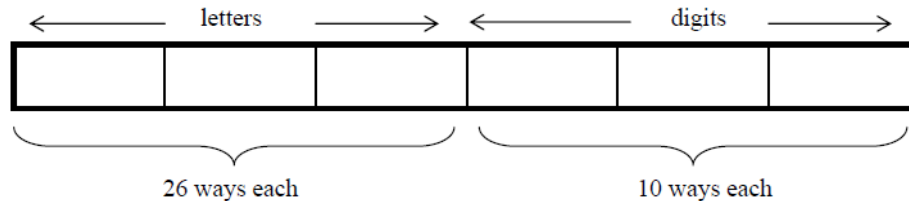
Example

Suppose that an automobile license plate has three letters followed by three digits.

(a) How many different license plates are possible?

Solution

Each of the three letters can be written in 26 different ways, and each of the three digits can be written in 10 different ways.

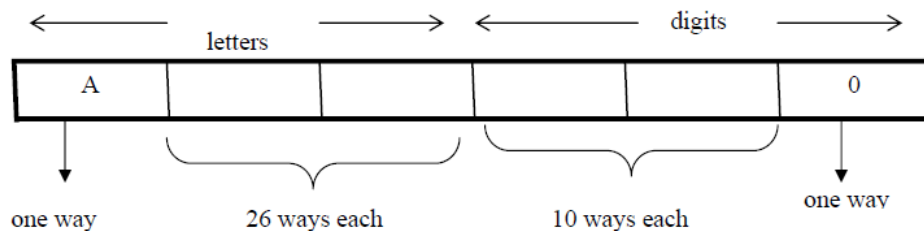


Hence, by the product rule, there is a total of
 $26 \times 26 \times 26 \times 10 \times 10 \times 10 = 17,576,000$
 different license plates possible.

(b) How many license plates could begin with A and end on 0?

Solution

The first and last place can be filled in one way only, while each of second and third place can be filled in 26 ways and each of fourth and fifth place can be filled in 10 ways.



Number of license plates that begin with A and end in 0 are
 $1 \times 26 \times 26 \times 10 \times 10 \times 1 = 67600$

(c) How many license plates are possible in which all the letters and digits are distinct?

Solution

The first letter place can be filled in 26 ways. Since, the second letter place should contain a different letter than the first, so it can be filled in 25 ways. Similarly, the third letter place can be filled in 24 ways and the digits can be respectively filled in 10, 9, and 8 ways.

Hence, number of license plates in which all the letters and digits are distinct are
 $26 \times 25 \times 24 \times 10 \times 9 \times 8 = 11,232,000$

Example

A variable name in a programming language must be either a letter or a letter followed by a digit. How many different variable names are possible?

Solution

First consider variable names one character in length. Since such names consist of a single letter, there are 26 variable names of length 1. Next, consider variable names two characters in length. Since the first character is a letter, there are 26 ways to choose it. The second character is a digit, there are 10 ways to choose it. Hence, to construct variable name of two characters in length, there are

$$26 \times 10 = 260 \text{ ways.}$$

Finally, by sum rule, there are $26 + 260 = 286$ possible variable names in the programming language.

Example

A computer access code word consists of from one to three letters of English alphabets with repetitions allowed. How many different code words are possible.

Solution

Number of code words of length 1 = 26^1

Number of code words of length 2 = 26^2

Number of code words of length 3 = 26^3

Hence, the total number of code words = $26^1 + 26^2 + 26^3 = 18,278$

Factorial of a Positive Integer

For each positive integer n , its factorial is defined to be the product of all the integers from 1 to n and is denoted $n!$. Thus $n! = n(n - 1)(n - 2) \dots 3 \cdot 2 \cdot 1$

In addition, we define $0! = 1$

Remark: $n!$ can be recursively defined as

Base: $0! = 1$

Recursion $n! = n(n - 1)!$ for each positive integer n .

Example

Compute each of the following

1. $\frac{7!}{5!}$
2. $(-2)!$
3. $\frac{(n+1)!}{n!}$
4. $\frac{(n-1)!}{(n+1)!}$

Solution

$$1. \frac{7!}{5!} = \frac{7 \cdot 6 \cdot 5!}{5!} = 7 \cdot 6 = 42$$

$$2. (-2)! \text{ is not defined}$$

$$3. \frac{(n+1)!}{n!} = \frac{(n+1)n!}{n!} = n + 1$$

$$4. \frac{(n-1)!}{(n+1)!} = \frac{(n-1)!}{(n+1)(n)(n-1)!} = \frac{1}{n^2 + n}$$

Counting Formulas

From a given set of n distinct elements, one can choose k elements in different ways. The number of selections of elements varies according as:

- (i) elements may or may not be repeated.
- (ii) the order of elements may or may not matter.

k-Sample

A k -sample of a set of n elements is a choice of k elements taken from the set of n elements such that the order of elements matters and elements can be repeated.

Remark:

With k -sample, repetition of elements is allowed, therefore, k need not be less than or equal to n . i.e. k is independent of n .

Formula for K-Sample

Suppose there are n distinct elements and we draw a k -sample from it. The first element of the k -sample can be drawn in n ways. Since, repetition of elements is allowed, so the second element can also be drawn in n ways. Similarly each of third, fourth, ..., k -th element can be drawn in n ways.

Hence, by product rule, the total number of ways in which a k -sample can be drawn from n distinct elements is

$$n \cdot n \cdot n \cdot \dots \cdot n = n^k \text{ (k-times)}$$

Example

How many possible outcomes are there when a fair coin is tossed three times.

Solution

Each time a coin is tossed its outcome is either a head (H) or a tail (T). Hence in successive tosses, H and T are repeated. Also the order in which they appear is important. Accordingly, the problem is of 3-samples from a set of two elements H and T. [$k = 3$, $n = 2$]

$$\begin{aligned} \text{Hence number of samples} &= n^k \\ &= 2^3 = 8 \end{aligned}$$

These 8-samples may be listed as:
HHH, HHT, HTH, THH, HTT, THT, TTH, TTT

Example

Suppose repetition of digits is permitted.

(a) How many three-digit numbers can be formed from the six digits 2, 3, 4, 5, 7 and 9

Solution

Given distinct elements = $n = 6$

Digits to be chosen = $k = 3$

While forming numbers, order of digits is important. Also digits may be repeated.

Hence, this is the case of 3-sample from 6 elements.

$$\text{Number of 3-digit numbers} = n^k = 6^3 = 216$$

(b) How many of these numbers are less than 400?

Solution

From the given six digits 2, 3, 4, 5, 7 and 9, a three-digit number would be less than 400 if and only if its first digit is either 2 or 3. The next two digits positions may be filled with any one of the six digits.

Hence, by product rule, there are $2 \cdot 6 \cdot 6 = 72$ three-digit numbers less than 400.

(c) How many are even?

Solution

A number is even if its right most digit is even. Thus, a 3-digit number formed by the digits 2, 3, 4, 5, 7 and 9 is even if its last digit is 2 or 4. Thus the last digit position may be filled in 2 ways only while each of the first two positions may be filled in 6 ways.

Hence, there are $6 \cdot 6 \cdot 2 = 72$ three-digit even numbers.

(d) How many are odd?

Solution

A number is odd if its right most digit is odd. Thus, a 3-digit number formed by the digits 2, 3, 4, 5, 7 and 9 is odd if its last digit is one of 3, 5, 7, 9. Thus, the last digit position may be filled in 4 ways, while each of the first two positions may be filled in 6 ways.

Hence, there are $6 \cdot 6 \cdot 4 = 144$ three-digit odd numbers.

Example

A multiple choice test contains 10 questions; there are 4 possible answers for each question.

(a) How many ways can a student answer the questions on the test if every question is answered?

(b) How many ways can a student answer the questions on the test if the student can leave answers blank?

Solution

(a) Each question can be answered in 4 ways. Suppose answers are labeled as A, B, C, D. Since label A may be used as the answer of more than one question. So repetition is allowed. Also the order in which A, B, C, D are chosen as answers for 10 questions is important.

Hence, this is the one of k-sample, in which

n = no. of distinct labels = 4

k = no. of labels selected for answering = 10

$$\begin{aligned} \therefore \text{No. of ways to answer 10 questions} &= n^k \\ &= 4^{10} \\ &= 1048576 \end{aligned}$$

(b) If the student can leave answers blank, then in addition to the four answers, a fifth option to leave answer blank is possible. Hence, in such case

$$\begin{aligned} n &= 5 \\ \text{and } k &= 10 \text{ (as before)} \\ \therefore \text{No. of possible answers} &= n^k \\ &= 5^{10} \\ &= 9765625 \end{aligned}$$

k-Permutation

A k-permutation of a set of n elements is a selection of k elements taken from the set of n elements such that the order of elements matters but repetition of the elements is not allowed. The number of k-permutations of a set of n elements is denoted $P(n, k)$ or ${}_nP_k$.

Remark:

1. With k-permutation, repetition of elements is not allowed, therefore $k \leq n$.
2. The wording "number of permutations of a set with n elements" means that all n elements are to be permuted, so that $k = n$.

Formula for k-Permutation

Suppose a set of n elements is given. Formation of a k-permutation means that we have an ordered selection of k elements out of n, where elements cannot be repeated.

1st element can be selected in n ways

2nd element can be selected in (n-1) ways

3rd element can be selected in (n-2) ways

.....

kth element can be selected in (n-(k-1)) ways

Hence, the number of ways to form a k-permutation is

$$P(n, k) = \frac{n!}{(n-k)!}$$

Example

How many 2-permutation are there of {W, X, Y, Z}? Write them all.

Solution

Number of 2-permutation of 4 elements is

$$P(4, 2) = \frac{4!}{(4-2)!} = 4(3) = 12$$

These 12 permutations are:

WX, WY, WZ,
XW, XY, XZ,
YW, YX, YZ,
ZW, ZX, ZY.

ExampleFind (a) $P(8, 3)$ (b) $P(8, 8)$ **Solution**

$$a) P(8, 3) = \frac{8!}{(8-3)!} = 8(7)(6) = 336$$

$$b) P(8, 8) = \frac{8!}{(8-8)!} = 8! = 40320 \quad (\text{as } 0! = 1)$$

ExampleFind n if(a) $P(n, 2) = 72$ (b) $P(n, 4) = 42 P(n, 2)$ **Solution**(a) Given $P(n, 2) = 72$

$$\Rightarrow n(n-1) = 72$$

$$\Rightarrow n^2 - n = 72$$

$$\Rightarrow n^2 - n - 72 = 0$$

$$\Rightarrow n = 9, -8$$

(by using the definition of permutation)

Since n must be positive, so the only acceptable value of n is 9.(b) Given $P(n, 4) = 42P(n, 2)$

$$\Rightarrow n(n-1)(n-2)(n-3) = 42n(n-1)$$

$$\Rightarrow (n-2)(n-3) = 42$$

$$\Rightarrow n^2 - 5n + 6 = 42$$

$$\Rightarrow n^2 - 5n - 36 = 0$$

$$\Rightarrow (n-9)(n+4) = 0$$

$$\Rightarrow n = 9, -4$$

(by using the definition of permutation)
if $n \neq 0, n \neq 1$ Since n must be positive, the only answer is $n = 9$ **Example**Prove that for all integers $n \geq 3$

$$P(n+1, 3) - P(n, 3) = 3P(n, 2)$$

SolutionSuppose n is an integer greater than or equal to 3

$$\begin{aligned} \text{Now L.H.S} &= P(n+1, 3) - P(n, 3) \\ &= (n+1)(n)(n-1) - n(n-1)(n-2) \\ &= n(n-1)[(n+1) - (n-2)] \\ &= n(n-1)[n+1-n+2] \\ &= 3n(n-1) \\ \text{R.H.S} &= 3P(n, 2) \\ &= 3n(n-1) \end{aligned}$$

Thus $L.H.S = R.H.S$.

Example

(a) How many ways can five of the letters of the word ALGORITHM be selected and written in a row?

(b) How many ways can five of the letters of the word ALGORITHM be selected and written in a row if the first two letters must be TH?

Solution

(a) The answer equals the number of 5-permutation of a set of 9 elements and

$$P(9,5) = \frac{9!}{(9-5)!} = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 = 15120$$

(b) Since the first two letters must be TH hence we need to choose the remaining three letters out of the left $9 - 2 = 7$ alphabets.

Hence, the answer is the number of 3-permutations of a set of seven elements which is

$$P(7,3) = \frac{7!}{(7-3)!} = 7 \cdot 6 \cdot 5 = 210$$

Example

Find the number of ways that a party of seven persons can arrange themselves in a row of seven chairs.

Solution

The seven persons can arrange themselves in a row in $P(7,7)$ ways.

Now

$$P(7,7) = \frac{7!}{(7-7)!} = 7!$$

Example

A debating team consists of three boys and two girls. Find the number n of ways they can sit in a row if the boys and girls are each to sit together.

Solution

There are two ways to distribute them according to sex: BBBGG or GG BBB.

In each case, the boys can sit in a row in

$$P(3,3) = 3! = 6 \text{ ways}$$

and the girls can sit in

$$P(2,2) = 2! = 2 \text{ ways}$$

and Every row consist of boy and girl which is $2! = 2$

Thus, The total number of ways: $n = 2 \cdot 3! \cdot 2!$

$$= 2 \cdot 6 \cdot 2 = 24$$

Example

Find the number n of ways that five large books, four medium sized book, and three small books can be placed on a shelf so that all books of the same size are together.

Solution

In each case, the large books can be arranged among themselves in $P(5,5) = 5!$ ways, the medium sized books in $P(4,4) = 4!$ ways, and the small books in $P(3,3) = 3!$ ways.

The three blocks of books can be arranged on the shelf in $P(3,3) = 3!$ ways.

Thus

$$n = 3! \cdot 5! \cdot 4! \cdot 3! = 103680$$

k-Combinations

With a k -combinations the order in which the elements are selected does not matter and the elements cannot repeat.

Definition: A k -combination of a set of n elements is a choice of k elements taken from the set of n elements such that the order of the elements does not matter and elements can't be repeated. The symbol $C(n, k)$ denotes the number of k -combinations that can be chosen from a set of n elements.

Note: k -combinations are also written ${}_nC_k$ or $\binom{n}{k}$.

Remark: With k -combinations of a set of n elements, repetition of elements is not allowed, therefore, k must be less than or equal to n , i.e., $k \leq n$.

Example

Let $X = \{a, b, c\}$. Then 2-combinations of the 3 elements of the set X are: $\{a, b\}$, $\{a, c\}$, and $\{b, c\}$. Hence $C(3,2) = 3$.

Example

Let $X = \{a, b, c, d, e\}$.

List all 3-combinations of the 5 elements of the set X , and hence find the value of $C(5,3)$.

Solution

Then 3-combinations of the 5 elements of the set X are:

$\{a, b, c\}$, $\{a, b, d\}$, $\{a, b, e\}$, $\{a, c, d\}$, $\{a, c, e\}$,
 $\{a, d, e\}$, $\{b, c, d\}$, $\{b, c, e\}$, $\{b, d, e\}$, $\{c, d, e\}$

Hence $C(5, 3) = 10$

Permutations and Combinations**Example**

Let $X = \{A, B, C, D\}$.

The 3-combinations of X are:

{A, B, C}, {A, B, D}, {A, C, D}, {B, C, D}

Hence $C(4, 3) = 4$

The 3-permutations of X can be obtained from 3-combinations of X as follows.

ABC, ACB, BAC, BCA, CAB, CBA

ABD, ADB, BAD, BDA, DAB, DBA

ACD, ADC, CAD, CDA, DAC, DCA

BCD, BDC, CBD, CDB, DBC, DCB

So that $P(4, 3) = 24 = 4 \cdot 6 = 4 \cdot 3!$

Clearly $P(4, 3) = C(4, 3) \cdot 3!$

In general we have, $P(n, k) = C(n, k) \cdot k!$

In general we have,

$$P(n, k) = C(n, k) \cdot k!$$

or

$$C(n, k) = \frac{P(n, k)}{k!}$$

But we know that

$$P(n, k) = \frac{n!}{(n - k)!}$$

Hence

$$C(n, k) = \frac{n!}{(n - k)! k!}$$

Example

Compute $C(9, 6)$.

Solution

$$\begin{aligned} C(9, 6) &= \frac{9!}{(9 - 6)! 6!} \\ &= \frac{9!}{3! 6!} \\ &= \frac{9(8)(7)6!}{(3)(2)6!} \\ &= 84 \end{aligned}$$

Some Important Results

$$(a) C(n, 0) = 1$$

$$(b) C(n, n) = 1$$

$$(c) C(n, 1) = n$$

$$(d) C(n, 2) = \frac{n(n - 1)}{2}$$

$$(e) C(n, k) = C(n, n - k)$$

$$(f) C(n, k) + C(n, k + 1) = C(n + 1, k + 1)$$

Example

A student is to answer eight out of ten questions on an exam.

- (a) Find the number m of ways that the student can choose the eight questions
- (b) Find the number m of ways that the student can choose the eight questions, if the first three questions are compulsory.

Solution

- (a) The eight questions can be answered in $m = C(10, 8) = 45$ ways.
- (b) The eight questions can be answered in $m = C(7, 5) = 21$ ways.

Example

An examination paper consists of 5 questions in section A and 5 questions in section B. A total of 8 questions must be answered. In how many ways can a student select the questions if he is to answer at least 4 questions from section A.

Solution

There are two possibilities:

- (a) The student answers 4 questions from section A and 4 questions from section B. The number of ways 8 questions can be answered taking 4 questions from section A and 4 questions from section B are

$$C(5, 4) \cdot C(5, 4) = 5 \cdot 5 = 25$$

- (b) The student answers 5 questions from section A and 3 questions from section B. The number of ways 8 questions can be answered taking 5 questions from section A and 3 questions from section B are

$$C(5, 5) \cdot C(5, 3) = 1 \cdot 10 = 10$$

Thus there will be a total of $25 + 10 = 35$ choices.

Example

A computer programming team has 14 members.

- (a) How many ways can a group of seven be chosen to work on a project?
- (b) Suppose eight team members are women and six are men
 - (i) How many groups of seven can be chosen that contain four women and three men
 - (ii) How many groups of seven can be chosen that contain at least one man?
 - (iii) How many groups of seven can be chosen that contain at most three women?
- (c) Suppose two team members refuse to work together on projects. How many groups of seven can be chosen to work on a project?
- (d) Suppose two team members insist on either working together or not at all on projects. How many groups of seven can be chosen to work on a project?
- (e) How many ways a group of 7 be chosen to work on a project?

(a) Number of committees of 7

Solution

$$C(14, 7) = \frac{14!}{(14-7)!7!} = 3432$$

(b) Suppose eight team members are women and six are men

(i) How many groups of seven can be chosen that contain four women and three men?

Solution

Number of groups of seven that contain four women and three men

$$C(8, 4) \cdot C(6, 3) = \frac{8!}{4!4!} \cdot \frac{6!}{3!3!} = 70 \cdot 20 = 1400$$

(ii) How many groups of seven can be chosen that contain at least one man?

Solution

Total number of groups of seven

$$C(14, 7) = \frac{14!}{(14-7)!7!} = 3432$$

Number of groups of seven that contain no men

$$C(8, 7) = \frac{8!}{1!7!} = 8$$

Hence, the number of groups of seven that contain at least one man

$$C(14, 7) - C(8, 7) = 3432 - 8 = 3424$$

(iii) How many groups of seven can be chosen that contain at most three women?

Solution

Number of groups of seven that contain no women = 0

Number of groups of seven that contain one woman = $C(8, 1) \cdot C(6, 6) = 8 \cdot 1 = 8$

Number of groups of seven that contain two women = $C(8, 2) \cdot C(6, 5) = 28 \cdot 6 = 168$

Number of groups of seven that contain three women = $C(8, 3) \cdot C(6, 4) = 56 \cdot 15 = 840$

Hence the number of groups of seven that contain at most three women

$$= 0 + 8 + 168 + 840 = 1016$$

(c) Suppose two team members refuse to work together on projects. How many groups of seven can be chosen to work on a project?

Solution

Call the members who refuse to work together A and B. Number of groups of seven that contain neither A nor B

$$C(12, 7) = \frac{12!}{5!7!} = 792$$

Number of groups of seven that contain A but not B

$$C(12, 6) = 194$$

Number of groups of seven that contain B but not A

$$C(12, 6) = 194$$

Hence the required number of groups are

$$C(12, 7) + C(12, 6) + C(12, 6) = 792 + 924 + 924 \\ = 2640$$

(d) Suppose two team members insist on either working together or not at all on projects. How many groups of seven can be chosen to work on a project?

Solution

Call the members who insist on working together C and D.

Number of groups of seven containing neither C nor D

$$C(12, 7) = 792$$

Number of groups of seven that contain both C and D

$$C(12, 5) = 792$$

Hence the required number: $C(12, 7) + C(12, 5) = 792 + 792 = 1584$

k-Selections

k-selections are similar to k-combinations in that the order in which the elements are selected does not matter, but in this case repetitions can occur.

Definition: A k-selection of a set of n elements is a choice of k elements taken from a set of n elements such that the order of elements does not matter and elements can be repeated.

Remark:

1. k-selections are also called k-combinations with repetition allowed or multisets of size k.
2. With k-selections of a set of n elements repetition of elements is allowed. Therefore k need not to be less than or equal to n.

Theorem

The number of k-selections that can be selected from a set of n elements is $C(n + k - 1, k)$.

Example

A camera shop stocks ten different types of batteries.

(a) How many ways can a total inventory of 30 batteries be distributed among the ten different types?

(b) Assuming that one of the types of batteries is A76, how many ways can a total inventory of 30 batteries be distributed among the 10 different types if the inventory must include at least four A76 batteries?

Solution

$$(a) \quad \begin{aligned} k &= 30 \\ n &= 10 \end{aligned}$$

The required number is

$$\begin{aligned} C(30 + 10 - 1, 30) &= C(39, 30) \\ C(39, 30) &= \frac{39!}{(39 - 30)! 30!} = 211915132 \end{aligned}$$

$$(b) \quad \begin{aligned} k &= 26 \\ n &= 10 \end{aligned}$$

The required number is

$$\begin{aligned} C(26 + 10 - 1, 26) &= C(35, 26) \\ C(35, 26) &= \frac{35!}{(35 - 26)! 26!} = 70607460 \end{aligned}$$

Ordered and Unordered Partitions

An unordered partition of a finite set S is a collection $[A_1, A_2, \dots, A_k]$ of disjoint (nonempty) subsets of S (called cells) whose union is S . The partition is ordered if the order of the cells in the list counts.

Example

Let $S = \{1, 2, 3, \dots, 7\}$

The collections

$$P_1 = [\{1, 2\}, \{3, 4, 5\}, \{6, 7\}]$$

$$\text{and } P_2 = [\{6, 7\}, \{3, 4, 5\}, \{1, 2\}]$$

determine the same partition of S but are distinct ordered partitions.

Example

Suppose a box B contains seven marbles numbered 1 through 7. Find the number m of ways of drawing from B firstly two marbles, then three marbles and lastly the remaining two marbles.

Solution

The number of ways of drawing 2 marbles from 7 = $C(7, 2)$

Following this, there are five marbles left in B .

The number of ways of drawing 3 marbles from 5 = $C(5, 3)$

Finally, there are two marbles left in B .

The number of way of drawing 2 marbles from 2 = $C(2, 2)$

Thus

$$\begin{aligned} m &= \binom{7}{2} \binom{5}{3} \binom{2}{2} \\ m &= \frac{7!}{2! 5!} \cdot \frac{5!}{2! 3!} \cdot \frac{2!}{0! 2!} = 210 \end{aligned}$$

Theorem

Let S contain n elements and let n_1, n_2, \dots, n_k be positive integers with $n_1 + n_2 + \dots + n_k = n$. Then there exist

$$\frac{n!}{n_1! n_2! n_3! \dots n_k!}$$

different ordered partitions of S of the form $[A_1, A_2, \dots, A_k]$, where

A_1 contains n_1 elements

A_2 contains n_2 elements

A_3 contains n_3 elements

.....

A_k contains n_k elements

Remark: To find the number of unordered partitions, we have to count the ordered partitions and then divide it by suitable number to erase the order in partitions.

Example

Find the number m of ways that nine toys can be divided among four children if the youngest child is to receive three toys and each of the others two toys.

Solution

We find the number m of ordered partitions of the nine toys into four cells containing 3, 2, 2 and 2 toys respectively.

Hence

$$m = \frac{9!}{3! 2! 2! 2!} = 2520$$

Example

How many ways can 12 students be divided into 3 groups with 4 students in each group so that

- (i) one group studies English, one History and one Mathematics.
- (ii) all the groups study Mathematics.

Solution

(i) Since each group studies a different subject, so we seek the number of ordered partitions of the 12 students into cells containing 4 students each.

Hence there are

$$\frac{12!}{4! 4! 4!} = 34650 \text{ such partitions}$$

(ii) When all the groups study the same subject, then order doesn't matter. Now each partition $\{G_1, G_2, G_3\}$ of the students can be arranged in $3!$ ways as an ordered partition.

Hence there are

$$\frac{12!}{4! 4! 4!} \cdot \frac{1}{3!} \text{ unordered partitions}$$

Example

How many ways can 8 students be divided into two teams containing

- (i) five and three students respectively.
- (ii) four students each.

Solution

(i) The two teams (cells) contain different number of students; so the number of unordered partitions equals the number of ordered partitions, which is

$$\frac{8!}{5!3!} = 56$$

(ii) Since the teams are not labeled, so we have to find the number of unordered partitions of 8 students in groups of 4. Firstly, note, there are $\frac{8!}{4!4!} = 70$ ordered partitions into two cells containing four students each.

Since each unordered partition determine $2! = 2$ ordered partitions, there are $\frac{70}{2} = 35$ unordered partitions

Example

If 20 people are divided into teams of size 3, 3, 4, 4, 2, 4, find the number of possible arrangements.

Solution

Here, we are asked to count unlabeled groups. Accordingly, this is the case of ordered partitions.

$$\begin{aligned} \text{Now number of ordered partitions} &= \frac{20!}{3!3!4!4!2!4!} \cdot \frac{1}{3!2!} \\ &= 203693490000 \end{aligned}$$

Generalized Permutation or Permutations with Repetitions

The number of permutations of n elements of which n_1 are alike, n_2 are alike, ..., n_k are alike is

$$\frac{n!}{n_1!n_2!n_3! \dots n_k!}$$

Remark: The number $\frac{n!}{n_1!n_2!n_3! \dots n_k!}$ is often called a multinomial coefficient, and is denoted by the symbol.

Example

Find the number of distinct permutations that can be formed using the letters of the word "BENZENE".

Solution

The word "BENZENE" contains seven letters of which three are alike (the 3 E's) and two are alike (the 2 N's)

Hence, the number of distinct permutations are: $\frac{7!}{3!2!} = 420$

Example

How many different signals each consisting of six flags hung in a vertical line, can be formed from four identical red flags and two identical blue flags?

Solution

We seek the number of permutations of 6 elements of which 4 are alike and 2 are alike. There are $\frac{6!}{4!2!} = 15$ different signals

Example

(i) Find the number of permutations that can be formed from all the letters of the word BASEBALL

(ii) Find, if the two B's are to be next to each other.

(iii) Find, if the words are to begin and end in a vowel.

Solution

(i) There are eight letter of which two are B, two are A, and two are L. Thus,

$$m = \frac{8!}{2!2!2!} = 5040$$

(ii) Consider the two B's as one letter. Then there are seven letters of which two are A and two are L. Hence

$$m = \frac{7!}{2!2!} = 1260$$

(iii) There are three possibilities, the words begin and end in A, the words begin in A and end in E, or the words begin in E and end in A. In each case there are six positions left to fill where two are B and two are L. Hence,

$$m = 3 \frac{6!}{2!2!} = 540$$

Example

(i) Find the number of "words" that can be formed of the letters of the word ELEVEN.

(ii) Find, if the words are to begin with E and end in N.

Solution

(i) There are six letters of which three are E; hence required number of "words" are

$$m = \frac{6!}{3!} = 120$$

(ii) If the words are to begin with E and end in N, then there are four positions left to fill where two are E.

$$m = \frac{4!}{2!} = 12$$

CHAPTER 6: INTRODUCTION TO NUMBER THEORY

Introduction

One of the oldest and liveliest branches of mathematics, Number Theory, is noted for its theoretical depth and applications to other fields, including representation theory, physics, and cryptography. The forefront of Number Theory is replete with sophisticated and famous open problems; at its foundation, however, are basic, elementary ideas that can stimulate and challenge beginning students. By thoroughly discussing interesting examples and applications and by introducing and illustrating every key idea, by relevant problems of various levels of difficulty, the book motivates, engages and challenges the reader. The exposition proceeds incrementally, intuitively and rigorously uncovers deeper properties. This will appeal to senior high school and undergraduate students, their instructors, as well as to all who would like to expand their mathematical horizons. It is a source of fascinating problems for readers at all levels and widely opens the gate to further explorations in mathematics.

Divisibility

For integers a and b , $a \neq 0$, we say that a **divides** b if $b = ac$ for some integer c . We denote this by $a \mid b$. We also say that b is divisible by a or that b is multiple of a .

We can derive the following properties:

1. If $a \mid b$, $b \neq 0$, then $|a| \leq |b|$.

Proof: If $a \mid b$, then there exists c such that $ac = b$. Then $|b| = |ac| = |a| |c|$

Hence either $|c| = 1$ or $|a| < |a| |c| = |b|$. If $|c| = 1$, then $c = \pm 1$; where $a = \pm b$

2. If $a \mid b$ and $a \mid c$, then $a \mid xb + cy$ for any integers x and y .

Proof: According to the divisibility definition we have:

$$\begin{aligned} a \mid b &\Rightarrow \exists p \in \mathbb{Z} \quad \text{such that} \\ b &= pa, \quad a \mid c \Rightarrow \exists q \in \mathbb{Z} \quad \text{such that} \\ c &= qa \text{ then } bx + cy = pax + qay = (px + qy)a \end{aligned}$$

Now, let $k' = (px + qy)$ such that $k' \in \mathbb{Z}$ then

It follows that $bx + cy = k'a$

which means $a \mid (bx + cy)$.

3. If $a \mid b$ and $a \mid c$ then; $a \mid b \pm c$.

Proof: Suppose a , b and c are any integers such that $a \mid b$ and $a \mid c$. We must show that $a \mid (b + c)$. By definition of divisibility, we have

$$\begin{aligned} a \mid b &= b = (a)(r) \text{ for some integer } r \\ \text{and } a \mid c &= c = (a)(s) \text{ for some integer } s. \end{aligned}$$

Then, by substitution, we have

$$b + c = (a)(r) + (a)(s) = a(r + s).$$

Let $k = r + s$.

Then k is an integer (being a sum of integers), and

thus $b + c = (a)(k)$ for some integer k .

Then, by definition of divisibility,
 $a \mid (b+c)$ and this completes the proof.

4. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ and $a \mid (b - c)$.

Proof: If $a \mid b$ and $a \mid c$, then there exist integers x and y such that $ax = b$ and $ay = c$. Adding the equalities, we obtain $ax + ay = b + c$ and so $a(x + y) = b + c$. Hence $a \mid (b + c)$. Subtracting the equalities $ay = b$ and $by = c$, we obtain $ax - ay = b - c$ and so $a(x - y) = b - c$. Thus $a \mid (b - c)$.

5. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: If $a \mid b$ and $b \mid c$, then there exist integers x and y such that $ax = b$ and $by = c$. Replacing b by ax , we obtain $axy = c$. Hence $a \mid c$.

6. If $a \mid b$ and $b \mid a$, then $|a| = |b|$.

Proof: Because $a \mid b \Rightarrow |a| \mid |b|$ and $b \mid a \Rightarrow |b| \mid |a|$. Since $|a|, |b| \geq 0$, we have : $|b| \geq |a|$ and $|a| \geq |b| \Rightarrow |a| = |b| \Rightarrow a = \pm b$.

7. If $a \mid b$ then, for any integer x , $a \mid bx$.

Proof: If $a \mid b$, then there exists an integer c such that $ac = b$. Multiplying the equation by x , we obtain $acx = bx$. Hence $a \mid bx$.

Note: Because $0 = a \cdot 0$, it follows that $a \mid 0$ for all integers a , $a \neq 0$.

Divisibility Rule

A divisibility rule is a shorthand way of discovering whether a given number is divisible by a fixed divisor without performing the division, usually by examining its digits. Although there are divisibility tests for numbers in any radix and they are all different. See examples below.

Note: In mathematical numeral systems, the base or radix for the simplest case is the number of unique digits, including zero, that a positional numeral system uses to represent numbers.

Divisibility Tests

1. A number is divisible by 2 if the last digit is 0, 2, 4, 6 or 8.
2. A number is divisible by 3 if the sum of the digits is divisible by 3.
3. A number is divisible by 4 if the number formed by the last two digits is divisible by 4.
4. A number is divisible by 5 if the last digit is either 0 or 5
5. A number is divisible by 6 if it is divisible by 2 and it is divisible by 3.
6. A number is divisible by 8 if the number formed by the last three digits is divisible by 8.
7. A number is divisible by 9 if the sum of the digits is divisible by 9.
8. A number is divisible by 10 if the last digit is 0.

Example

Determine whether 150 is divisible by 2, 3, 4, 5, 6, 9 and 10.

Solution

150 is divisible by 2 since the last digit is 0.

150 is divisible by 3 since the sum of the digits is 6 ($1+5+0 = 6$), and 6 is divisible by 3.

150 is not divisible by 4 since 50 is not divisible by 4.

150 is divisible by 5 since the last digit is 0.

150 is divisible by 6 since it is divisible by 2 and by 3.

150 is not divisible by 9 since the sum of the digits is 6, and 6 is not divisible by 9.

150 is divisible by 10 since the last digit is 0.

Therefore 150 is divisible by 2, 3, 5, 6, and 10.

Example

Determine whether 7,168 is divisible by 2, 3, 4, 5, 6, 8, 9 and 10.

Solution

7,168 is divisible by 2 since the last digit is 8.

7,168 is not divisible by 3 since the sum of the digits is 22, and 22 is not divisible by 3.

7,168 is divisible by 4 since 168 is divisible by 4.

7,168 is not divisible by 5 since the last digit is not 0 or 5.

7,168 is not divisible by 6 since it is not divisible by both 2 and 3.

7,168 is divisible by 8 since the last 3 digits are 168, and 168 is divisible by 8.

7,168 is not divisible by 9 since the sum of the digits is 22, and 22 is not divisible by 9.

7,168 is not divisible by 10 since the last digit is not 0 or 5.

Therefore 7,168 is divisible by 2, 4 and 8.

Example

Is the number 91 prime or composite? Use divisibility when possible to find your answer.

Solution

91 is not divisible by 2 since the last digit is not 0, 2, 4, 6 or 8.

91 is not divisible by 3 since the sum of the digits ($9+1=10$) is not divisible by 3.

91 is not evenly divisible by 4 (remainder is 3).

91 is not divisible by 5 since the last digit is not 0 or 5.

91 is not divisible by 6 since it is not divisible by both 2 and 3.

91 divided by 7 is 13.

The number 91 is divisible by 1, 7, 13 and 91. Therefore 91 is composite since it has more than two factors.

Division Algorithm

Theorem: For any positive integers a and b there exists a unique pair (q, r) of nonnegative integers such that $b = aq + r$, $r < a$.

Prime Factorization

The numbers that we are interested in factoring are the natural numbers $1, 2, 3, \dots$. The word factor is used as both a noun and a verb. The factors (noun) of a number are the numbers that divide evenly into the number. For example the factors of the number 12 are the numbers 1, 2, 3, 4, 6 and 12. (Notice that the smallest factor is always 1 and the biggest factor is always the number itself.) To factor (verb) a number means to express it as a product of smaller numbers. For example we can factor the number 12 like this: $12 = 3 \cdot 4$. The numbers 3 and 4 are called the factors. Another way to factor 12 is like this: $12 = 2 \cdot 2 \cdot 3$. Now the factors are 2, 2 and 3. Each way of factoring a number is called a factorization. A number that cannot be factored further is called a prime number. To factor a number completely means to write it as a product of prime numbers. This is also called the prime factorization. Now let us define Two integers a and b which is said to be relatively prime.

Remarks: Two integers a and b are said to be relatively prime or coprime if $\gcd(a, b) = 1$. Accordingly, if a and b are relatively prime, then there exist integers x and y such that $ax + by = 1$

Example

The **factors** of 24 are: 1, 2, 3, 4, 6, 8, 12 and 24 since each of these numbers divides exactly into 24.

The **factors** of 40 are: 1, 2, 4, 5, 8, 10, 20 and 40, since each of these numbers divides exactly into 40.

The **factors** of 50 are: 1, 2, 5, 10, 25 and 50. since each of these numbers divides exactly into 50.

Example

Find the unique factorization of each number:

(a) 135; (b) 1330; (c) 3105; (d) 211

Solution

(a) $135 = 5 \cdot 27 = 5 \cdot 3 \cdot 3 \cdot 3$ or $135 = 3^3 \cdot 5$.

(b) $1330 = 2 \cdot 665 = 2 \cdot 5 \cdot 133 = 2 \cdot 5 \cdot 7 \cdot 19$.

(c) $3105 = 5 \cdot 621 = 5 \cdot 3 \cdot 207 = 5 \cdot 3 \cdot 3 \cdot 69 = 5 \cdot 3 \cdot 3 \cdot 3 \cdot 23$, or $3105 = 3^3 \cdot 5 \cdot 23$.

(d) None of the primes 2, 3, 5, 7, 11, 13 divides 211; hence 211 cannot be factored, that is, 211 is a prime.

Greatest Common Divisor

A positive integer can be a factor of two positive integers, a and b . Such factors are common divisors, or common factors, of a and b . For example, 14 and 28 have four common divisors, namely, 1, 2, 7, and 14; whereas 13 and 27 have exactly one common factor, namely, 1. The greatest common divisor (\gcd) of two integers a and b , not both zero, is the

largest positive integer that divides both a and b ; it is denoted by (a, b) . Often we are not interested in all common divisors of a and b , but in the largest common divisor, so we make the following definition

- Def. A positive integer d is the gcd of two positive integers a and b if
- $d \mid a$ and $d \mid b$; and
 - if $d' \mid a$ and $d' \mid b$, then $d' \leq d$, where d' is also a positive integer.

Example

Find the gcd:

- a. $(12, 18, 28)$ b. $(12, 36, 60, 108)$ c. $(15, 28, 50)$

Solution

- a) The largest positive integer that divides 12, 18, and 28 is 2, so $(12, 18, 28) = 2$
 b) 12 is the largest factor of 12, and 12 is a factor of 12, 36, 60, and 108
 c) Since $(15, 28) = 1$, the largest common factor of 15, 28, and 50 is 1

Euclidean Algorithm

Let a and b be any two positive integers with $a \geq b$. If $a = b$, then $(a, b) = a$, so Assume $a > b$. (If this is not true, simply switch them.) Let $r_0 = b$. Then by successive application of the division algorithm, we get a sequence of equations:

$$\begin{aligned} a &= q_0 r_0 + r_1, 0 \leq r_1 < r_0 \\ r_0 &= q_1 r_1 + r_2, 0 \leq r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3, 0 \leq r_3 < r_2 \end{aligned}$$

...

Continuing like this, we get the following sequence of remainders:

$$b = r_0 > r_1 > r_2 > r_3 > \dots \geq 0$$

Since the remainders are nonnegative and are getting smaller and smaller, this sequence should eventually terminate with remainder $r_{n+1} = 0$. Thus, the last two equations in the above procedure are

$$\begin{aligned} r_{n-2} &= q_{n-1} r_{n-1} + r_n, 0 \leq r_n < r_{n-1} \text{ and} \\ r_{n-1} &= r_n q_n \end{aligned}$$

It follows by induction that $(a, b) = (a, r_0) = (r_0, r_1) = (r_1, r_2) = \dots = (r_{n-1}, r_n) = r_n$ the last nonzero remainder.

Example

Using Euclidean Algorithm find the greatest common divisor of 60 and 84 and express it as an integral linear combination of these numbers.

Solution

Since the greatest common divisor only depends on the numbers involved and not their order, we might as take the larger one first, so set $a = 84$ and $b = 60$. Then

$$\begin{aligned} 84 &= (1)(60) + 24 & 24 &= 84 + (-1)(60) \\ 60 &= (2)(24) + 12 & 12 &= 60 + (-2)(24) \\ 24 &= (2)(12) & 12 &= \gcd(60, 84) \end{aligned}$$

Working back we find

$$\begin{aligned} 12 &= 60 + (-2)(24) \\ 12 &= 60 + (-2)[84 + (-1)(60)] \\ 12 &= (-2)(84) + (3)(60) \end{aligned}$$

Thus $\gcd(60, 84) = 12 = (3)(60) + (-2)(84)$

Example

Using Euclidean Algorithm find the greatest common divisor of 190 and -72, and express it as an integral linear combination of these numbers.

Solution

Taking $a = 190$, $b = -72$ we have

$$\begin{aligned} 190 &= (-2)(-72) + 46 & 46 &= (190) + (2)(-72) \\ -72 &= (-2)(46) + 20 & 20 &= (-72) + (2)(46) \\ 46 &= (2)(20) + 6 & 6 &= (-2)(20) + 46 \\ 20 &= (3)(6) + 2 & 2 &= 20 + (-3)(6) \\ 6 &= (3)(2) & 2 &= \gcd(190, -72) \end{aligned}$$

Working back we find

$$\begin{aligned} 2 &= 20 + (-3)(6) \\ 2 &= 20 + (-3)[(-2)(20) + 46] \\ 2 &= (-3)(46) + (7)(20) \\ 2 &= (-3)(46) + (7)[(-72) + (2)(46)] \\ 2 &= (7)(-72) + (11)(46) \\ 2 &= (7)(-72) + 11[(190) + (2)(-72)] \\ 2 &= (11)(190) + (29)(-72) \end{aligned}$$

Thus $\gcd(190, -72) = 2 = (11)(190) + (29)(-72)$

Linear Combination

A **linear combination** of the integers a and b is a sum of multiples of a and b , that is, a sum of the form $ax + by$, where x and y are integers.

Example

Using the Euclidean algorithm, express $(4076, 1024)$ as a linear combination of 4076 and 1024.

Solution

All we need to do is use the equations in the previous example in the reverse order, each time substituting for the remainder from the previous equation.

$(4076, 1024) = 4 = \text{last nonzero remainder}$

$$4 = 1004 - (50)(20)$$

$$4 = 1004 - 50[1024 + (-1)(1004)] \quad (\text{substitute for } 20)$$

$$4 = (51)(1004) + (-50)(1024)$$

$$4 = 51[4076 + (-3)(1024)] + (-50)(1024) \quad (\text{substitute for } 1004)$$

$$4 = (51)(4076) + (-203)(1024)$$

Therefore $x=51$ and $y=-203$ (We can verify this by direct computation)

Linear Diophantine Equation

Consider the following problem:

Find all integer solutions $x; y$ of the equation $35x + 61y = 1$. Such problems in which we are only interested in integer solutions are called Diophantine problems and are named after the Greek Diophantus in whose book many examples appeared. Diophantine problems were also studied in several ancient civilizations including those of China, India and the Middle East. Since $\gcd(35; 61) = 1$, we can use the Euclidean Algorithm to find a specific solution of this problem.

$$61 = (1)(35) + 26$$

$$26 = 61 + (-1)(35)$$

$$35 = (1)(26) + 9$$

$$9 = 35 + (-1)(26)$$

$$26 = (2)(9) + 8$$

$$8 = 26 + (-2)(9)$$

$$9 = (1)(8) + 1$$

$$1 = 9 + (-1)(8)$$

$$8 = 1 \times 8:$$

Hence a solution is obtained from

$$1 = 9 + (-1)(8)$$

$$= 9 + (-1)[26 + (-2)(9)] = (-1)(26) + (3)(9)$$

$$= (-1)(26) + 3[35 + (-1)(26)] = (3)(35) + (-4)(26)$$

$$= (3)(35) + (-4)[61 + (-1)(35)] = (7)(35) + (-4)(61)$$

So $x = 7, y = -4$ is an integer solution. To find all integer solutions, notice that another solution $x; y$ must satisfy $35(x-7) + 61(y+4) = 0$, hence we have $35 \mid 61(y+4)$ and $35 \mid (y+4)$.

Thus $y = -4 + 35k$ and then $x = 7 - 61k$ for some integer k . The general integer solution is $x = 7 - 61k$ and $y = -4 + 35k$.

Theorem: If a, b and c are all integers and $d = \gcd(a, b)$ and

- If $d \nmid c$, then the equation $ax + by = c$ has no integer solutions. If $d \mid c$, then the equation $ax + by = c$ has integer solutions.
- If x_0 and y_0 is a particular integer solution, then the general integer solution is $x = x_0 + \left(\frac{b}{d}\right)k$ and $y = y_0 - \frac{a}{d}k$ where k is an integer.

Corollary: If $(a, b) = 1$, then the Linear Diophantine Equation $ax + by = c$ is solvable and the general solution is given by $x = x_0 + bt, y = y_0 - at$, where x_0, y_0 is a particular solution.

Example

Find the general solution if $63x - 23y = -7$

Solution

To find a particular solution $!!$, $!!$, first we express the gcd 1 as a linear combination of 63 and 23. To accomplish this, we apply the Euclidean algorithm:

$$63 = 2 \cdot 23 + 17$$

$$23 = 1 \cdot 17 + 6$$

$$17 = 2 \cdot 6 + 5$$

$$6 = 1 \cdot 5 + 1$$

$$5 = 5 \cdot 1 + 0$$

Now, use the first four equations in reverse order:

$$\begin{aligned} 1 &= 6 - (1 \cdot 5) \\ &= 6 - 1[17 - (2 \cdot 6)] \\ &= 3 \cdot 6 - 1 \cdot 17 \\ &= 3[23 - (1 \cdot 17)] - 1 \cdot 17 \\ &= 3 \cdot 23 - 4 \cdot 17 \\ &= 3 \cdot 23 - 4[63 - (2 \cdot 23)] \\ &= (-4) \cdot 63 + 11 \cdot 23 \end{aligned}$$

Multiply both sides of this equation by -7 :

$$\begin{aligned} -7 &= (-7)(-4)(63) + (-7)(11)(23) \\ &= (63)(28) - (23)(77) \end{aligned}$$

which shows $x_0 = 28, y_0 = 77$ is a particular solution of the Linear Diophantine Equation. Therefore the general solution is given by $x = x_0 + bk = 28 - 23k$ and $y = y_0 - ak = 77 - 63k$, where k is an arbitrary integer.

Congruences and its Application

One of the most remarkable relations in number theory is the congruence relation, introduced and developed by the German mathematician Karl Friedrich Gauss, who is ranked with Archimedes (287–212 B.C.) and Isaac Newton (1642–1727) as one of the greatest mathematicians of all time. Gauss, known as the “prince of mathematics,” presented the theory of congruences, a beautiful arm of divisibility theory, in his outstanding work **Disquisitiones Arithmeticae**, published in 1801 when he was only 24. Gauss is believed to have submitted a major portion of the book to the French Academy for publication, but they rejected it. “It is really astonishing,” writes the German mathematician Leopold Kronecker, “to think that a single man of such young years was able to bring to light such a wealth of results, and above all to present such a profound and well-organized treatment of an entirely new discipline.” The congruence relation, as we will see shortly, shares many interesting properties with the equality relation, so it is no accident that the congruence symbol \equiv , invented by Gauss around 1800, parallels the equality symbol $=$. The congruence symbol facilitates the study of divisibility theory and has many fascinating applications. Let us begin our discussion with a definition.

Definition: Given three integers a, b, n where $n > 0$. Then, a is said to be congruent to b modulo n (denoted as $a \equiv b \pmod{n}$) if and only if $n \mid (a-b)$

Proposition:

For $a, b, n \in \mathbb{Z}$ the followings are true :

- (i) $a \equiv a \pmod{m}$ Reflexive Property
- (ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ Symmetric Property
- (iii) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$ Transitive Property
- (iv) $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$

Proof:

- (i) The difference $a - a = 0$ is divisible by m ; hence $a \equiv a \pmod{m}$.
- (ii) If $a \equiv b \pmod{m}$, then $m \mid (a - b)$. Hence m divides $-(a - b) = b - a$. Therefore, $b \equiv a \pmod{m}$.
- (iii) We are given $m \mid (a - b)$ and $m \mid (b - c)$. Hence m divides the sum $(a - b) + (b - c) = a - c$. Therefore, $a \equiv c \pmod{m}$.

Proposition:

Given $a \equiv c \pmod{m}$, $b \equiv d \pmod{m}$

- (i) $a + b \equiv c + d \pmod{m}$
- (ii) $a \cdot b \equiv c \cdot d \pmod{m}$
- (iii) $ax \equiv ay \pmod{m}$ implies $x \equiv y \pmod{m}$ if $\gcd(a, m) = 1$
- (iv) $ab \equiv bc \pmod{m}$ if $\gcd(b, m) = d$ then $a \equiv c \pmod{\frac{m}{d}}$

Proof:

(i) Then m divides the sum $(a - c) + (b - d) = (a + b) - (c + d)$.

Hence $a + b \equiv c + d \pmod{m}$.

(ii) Then m divides $b(a - c) = ab - bc$ and m divides $c(b - d) = bc - cd$.

Thus m divides the sum $(ab - bc) + (bc - cd) = ab - cd$. Thus $ab \equiv cd \pmod{m}$.

(iii) By hypothesis, m divides $ab - bc = b(a - c)$. Hence, there is an integer x such that $b(a - c) = mx$. Dividing by d yields $(b/d)(a - c) = (m/d)x$. Thus m/d divides $(b/d)(a - c)$. Since m/d and b/d are relatively prime, m/d divides $a - c$. That is, $a \equiv c \pmod{m/d}$, as required.

Arithmetic Inverse

Definition: a^{-1} is called arithmetic inverse of a modulo n if $aa^{-1} \equiv 1 \pmod{n}$

Proposition:

(i) a^{-1} exists if and only if $\gcd(a, m) = 1$

(ii) a^{-1} is unique

Example

(i) $83 \equiv 23 \pmod{2}$ since 2 divides $83 - 23 = 60$.

(ii) $79 \equiv 1 \pmod{6}$ since 6 divides $79 - 1 = 78$.

(iii) $65 \equiv -5 \pmod{7}$ since 7 divides $65 - (-5) = 70$.

(iv) $27 \not\equiv 8 \pmod{9}$ since 9 does not divide $27 - 8 = 19$.

Example

Find the remainder when 16^{53} is divided by 7.

Solution

First, reduce the base to its least residue that is, $16 \equiv 2 \pmod{7}$. Then it follows that $16^{53} \equiv 2^{53} \pmod{7}$. Now express a suitable power of 2 congruent modulo 7 to a number less than 7 we have, $2^3 \equiv 1 \pmod{7}$. Therefore,

$$2^3 \equiv 1 \pmod{7}$$

$$(2^3)^{17} \equiv (1)^{17} \pmod{7}$$

$$(2^{51})(2^2) \equiv (1)(4) \pmod{7}$$

$$2^{53} \equiv 4 \pmod{7}$$

So $16^{53} \equiv 4 \pmod{7}$, by the transitive property. Thus, when 16^{53} is divided by 7, the remainder is 4.

Example

Find the remainder when 3^{247} is divided by 17

Solution

Now we let the congruence do the job for us. We have

$$\begin{aligned}
 27 &\equiv 10 \pmod{17} && \text{(Squaring both sides)} \\
 (3^3)^2 &\equiv 10^2 \pmod{17} \\
 3^6 &\equiv -2 \pmod{17} && \text{(Raise both sides to the fourth power)} \\
 3^{24} &\equiv (-2)^4 \pmod{17} \\
 3^{24} &\equiv 16 \pmod{17} \\
 3^{24} &\equiv -1 \pmod{17} && \text{(Raise both sides to the tenth power)} \\
 (3^{24})^{10} &\equiv (-1)^{10} \pmod{17} && \text{(Multiply both sides by 3!)} \\
 3^{247} &\equiv 2187 \pmod{17} \\
 3^{247} &\equiv 11 \pmod{17}
 \end{aligned}$$

Thus, the remainder is 11.

Linear Congruence

A equation of the form $ax \equiv b \pmod{m}$ where a, b, m are positive integers and x is a variable is called a linear congruence. If we assume that $\gcd(a, m) = 1$ then the equation has infinitely many solutions. We can find all solutions as follows.

1. Using Euclid's extended algorithm, we find an integer a^{-1} such that $aa^{-1} \equiv 1 \pmod{m}$. Such an a^{-1} is called an inverse of a modulo m .
2. Multiplying equation (1) by b , we obtain $a(a^{-1}b) \equiv b \pmod{m}$ so that $x = a^{-1}b$ is a solution of the linear congruence.
3. For any integer k , $x = a^{-1}b + mk$ is a solution of the linear congruence. The number $x = a^{-1}b \pmod{m}$ is the unique solution over $0 \leq x < m$.

Note:

- The linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if $d \mid b$, where $d = \gcd(a, m)$. If $d \mid b$, then it has d incongruent solutions.
- The linear congruence $ax \equiv b \pmod{m}$ has a unique solution if and only if $\gcd(a, m) = 1$.
- The linear congruence $ax \equiv b \pmod{m}$ has no solution if d does not divide b .

The linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if $d \mid b$, where $d = \gcd(a, m)$. If $d \mid b$, then it has d incongruent solution.

Proof:

The linear congruence $ax \equiv b \pmod{m}$ is equivalent to the Linear Diophantine Equation $ax - my = b$; so the congruence is solvable if and only if the Linear Diophantine Equation is solvable. But Linear Diophantine Equation is solvable if and only if $d \mid b$. Thus $ax \equiv b \pmod{m}$ is solvable if and only if $d \mid b$. When $d \mid b$, the Linear Diophantine Equation has infinitely many solutions, given by $x = x_0 + \left(\frac{m}{d}\right)t$ and $y = y_0 + \left(\frac{a}{d}\right)t$ so the congruence has infinitely many solutions $x = x_0 + \left(\frac{m}{d}\right)t$, where x_0 is a particular solution. To find the number of incongruent solutions when the congruence is solvable, suppose $x_1 = x_0 + \left(\frac{m}{d}\right)t_1$ and $x_2 = x_0 + \left(\frac{m}{d}\right)t_2$ are two congruence solutions: $x_0 + \left(\frac{m}{d}\right)t_1 \equiv x_0 + \left(\frac{m}{d}\right)t_2$. Then subtracting x_0 from both sides, $\left(\frac{m}{d}\right)t_1 \equiv \left(\frac{m}{d}\right)t_2$. Since $\frac{m}{d}$ divides m then it follows that $t_1 \equiv t_2 \pmod{d}$. Thus, the solutions x_1 and x_2 are congruent if and only if $t_1 \equiv t_2 \pmod{d}$; that is, if and only if t_1 and t_2 belong to the same congruence class modulo d . In other words, they are incongruent solutions if and only if they belong to distinct congruence classes. Then there are exactly d incongruent classes modulo d . Therefore, the linear congruence, when solvable, has exactly d incongruent solutions, given by $x = x_0 + \left(\frac{m}{d}\right)t$, where $0 \leq t < d$.

Example

Solve each linear congruence equation:

(a) $3x \equiv 2 \pmod{8}$;

(b) $6x \equiv 5 \pmod{9}$;

(c) $4x \equiv 6 \pmod{10}$

Solution

Since the moduli are relatively small, we find all the solutions by testing. Recall $ax \equiv b \pmod{m}$ has exactly $d = \gcd(a, m)$ solution providing d divides b .

(a) Here $\gcd(3, 8) = 1$, hence the equation has a unique solution. Testing $0, 1, 2, \dots, 7$, we find that $3(6) = 18 \equiv 2 \pmod{8}$. Thus 6 is the unique solution.

(b) Here $\gcd(6, 9) = 3$, but 3 does not divide 5. Hence the system has no solution.

(c) Here $\gcd(4, 10) = 2$ and 2 divides 6; hence the system has two solutions. Testing $0, 1, 2, 3, \dots, 9$, we see that $4(4) = 16 \equiv 6 \pmod{10}$ and $4(9) = 36 \equiv 6 \pmod{10}$. Hence 4 and 9 are our two solutions.

Example

Let's find all solutions of $9x \equiv 15 \pmod{23}$ and identify the unique solution over $0 \leq x < 23$.

Solution

Let's first use Euclid's algorithm to find $\gcd(23, 9)$.

$$23 = 9(2) + 5$$

$$9 = 5(1) + 4$$

$$5 = 4(1) + 1$$

$$4 = 1(4) + 0$$

Using back substitution we obtain

$$\begin{aligned} 1 &= 5 - 4 \\ &= 5 - (9 - 5) = 5(2) - 9 \\ &= (2)[23 - 9(2)] - 9 = 23(2) - 9(5) \end{aligned}$$

The last equation implies that $9(-5) = 1 + 23(-2) \equiv 9(-5) - 1 \pmod{23}$. We conclude that $a^{-1} = -5$ is an inverse of 9 modulo 23. Multiplying equation by 15 we obtain $9(-75) \equiv 15 \pmod{23}$. Then, for any integer k , $x = -75 + 23k$ are solutions of the linear congruence. The unique solution in $0 \leq x < 23$ is $x = -75 \pmod{23} = 17$.

$$9x \equiv 15 \pmod{23}$$

$$3x \equiv 5 \pmod{23}$$

$$3x \equiv 51 \pmod{23}$$

$$x \equiv 17 \pmod{23}$$

Therefore $x = 17$

Example

Solve each congruence equation:

(a) $4x \equiv 9 \pmod{15}$

(b) $8x \equiv 12 \pmod{28}$

(c) $23x \equiv 37 \pmod{20}$

Solution

(a) $4x \equiv 9 \pmod{15}$

$$4x \equiv 24 \pmod{15}$$

$$x \equiv 6 \pmod{15}$$

(b) $8x \equiv 12 \pmod{28}$

$$2x \equiv 3 \pmod{7}$$

$$2x \equiv -4 \pmod{7}$$

$$x \equiv 5 \pmod{7}$$

(c) $23x \equiv 37 \pmod{20}$

$$3x \equiv 17 \pmod{20}$$

$$3x \equiv -3 \pmod{20}$$

$$x \equiv -1 \pmod{20}$$

$$x \equiv 19 \pmod{20}$$

Therefore **$x=6$**

Therefore **$x=5, 12, 19$ and 26**

Therefore **$x=19$**

Example

Solve the congruence $12x \equiv 48 \pmod{18}$

Solution

Since $(12, 18) = 6$ and $6 \mid 48$, the congruence has six incongruent solutions modulo 6. They are given by $x = x_0 + \left(\frac{m}{d}\right)t = x_0 + \left(\frac{18}{6}\right)t = x_0 + 3t$, where x_0 is a particular solution and $0 \leq t < 6$. By trial and error, $x_0 = 1$ is a solution. Thus, the six incongruent solutions modulo 18 are $1 + 3t$, where $0 \leq t < 6$, that is, 1, 4, 7, 10, 13, and 16.

The same congruence can be solved in a slightly different way, we have

$$12x \equiv 48 \pmod{18}$$

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

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

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

Therefore **$x = 1, 4, 7, 10, 13$, and 16**

Chinese Remainder Theorem

An old Chinese riddle asks the following question. Is there a positive integer x such that when x is divided by 3 it yields a remainder 2, when x is divided by 5 it yields a remainder 4, and when x is divided by 7 it yields a remainder 6? In other words, we seek a common solution of the following three congruence equations:

$$x \equiv 2 \pmod{3}, x \equiv 4 \pmod{5}, x \equiv 6 \pmod{7}.$$

Consider the systems $x \equiv r_1 \pmod{m_1}, x \equiv r_2 \pmod{m_2}, \dots, x \equiv r_k \pmod{m_k}$ where the m_i are pairwise relatively prime. Then the system has a unique solution modulo $M = m_1 m_2 m_3 \dots m_k$ and $M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, M_3 = \frac{M}{m_3} = \dots = M_k = \frac{M}{m_k}$ (Then each pair M_i and m_i are co-prime). Let $s_1, s_2, s_3, \dots, s_k$ be the solutions respectively of the congruence equations $M_1 x \equiv 1 \pmod{m_1}, M_2 x \equiv 1 \pmod{m_2}, \dots, M_k x \equiv 1 \pmod{m_k}$.

$$x = M_1 s_1 r_1 + M_2 s_2 r_2 + \dots + M_k s_k r_k$$

where $M_i = \frac{M}{m_i}$ and s_i is the unique solution of $M_i x \equiv 1 \pmod{m_i}$.

Example

Using Chinese Remainder theorem Solve the Congruence's:

$$x \equiv 2 \pmod{3}, x \equiv 4 \pmod{5}, x \equiv 6 \pmod{7}$$

Solution

Using the above notation, we obtain $M = (3)(5)(7) = 105$

$$M_1 = 105/3 = 35, M_2 = 105/5 = 21, M_3 = 105/7 = 15.$$

We now seek solutions to the equations

$$\begin{aligned} 35x &\equiv 1 \pmod{3} & 21x &\equiv 1 \pmod{5} & 15x &\equiv 1 \pmod{7} \\ 2x &\equiv 1 \pmod{3} & x &\equiv 1 \pmod{5} & x &\equiv 1 \pmod{7} \\ 2x &\equiv -2 \pmod{3} \\ x &\equiv -1 \pmod{3} \\ x &\equiv 2 \pmod{3} \end{aligned}$$

The solutions of these three equations are, respectively, $s_1 = 2, s_2 = 1, s_3 = 1$

$$x = M_1 s_1 r_1 + M_2 s_2 r_2 + \dots + M_k s_k r_k \pmod{105}$$

$$x = [(35)(2)(2) + (21)(1)(4) + (15)(1)(6)] \pmod{105}$$

$$x = 314 \pmod{105}$$

Therefore $x = 104$

Example

Find the smallest positive solution of each system of congruence equations:

$$(a) x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}, x \equiv 4 \pmod{11}$$

$$(b) x \equiv 3 \pmod{5}, x \equiv 4 \pmod{7}, x \equiv 6 \pmod{9}$$

Solution

(a.) Using the above notation, we obtain $M = (3)(5)(11) = 165$
 $M_1 = 165/3 = 55$, $M_2 = 165/5 = 33$, $M_3 = 165/11 = 15$.

We now seek solutions to the equations

$$\begin{array}{lll} 55x \equiv 1 \pmod{3} & 33x \equiv 1 \pmod{5} & 15x \equiv 1 \pmod{11} \\ x \equiv 1 \pmod{3} & 3x \equiv 1 \pmod{5} & 4x \equiv 1 \pmod{11} \\ & 3x \equiv 6 \pmod{5} & 4x \equiv 12 \pmod{11} \\ & x \equiv 2 \pmod{5} & x \equiv 3 \pmod{11} \end{array}$$

The solutions of these three equations are, respectively, $s_1 = 1$, $s_2 = 2$, $s_3 = 3$

$$x = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k \pmod{165}$$

$$x = [(55)(1)(2) + (33)(2)(3) + (15)(3)(4)] \pmod{165}$$

$$x = 488 \pmod{165}$$

Therefore $x = 158$

(b.) Using the above notation, we obtain $M = (5)(7)(9) = 315$
 $M_1 = 315/5 = 63$, $M_2 = 315/7 = 45$, $M_3 = 315/9 = 35$.

We now seek solutions to the equations

$$\begin{array}{lll} 63x \equiv 1 \pmod{5} & 3x \equiv 1 \pmod{7} & 35x \equiv 1 \pmod{9} \\ 3x \equiv 1 \pmod{5} & 3x \equiv -6 \pmod{7} & 8x \equiv 1 \pmod{9} \\ 3x \equiv 6 \pmod{5} & x \equiv -2 \pmod{7} & 8x \equiv -8 \pmod{9} \\ x \equiv 2 \pmod{5} & x \equiv 5 \pmod{7} & x \equiv -1 \pmod{9} \\ & & x \equiv 8 \pmod{9} \end{array}$$

The solutions of these three equations are, respectively, $s_1 = 2$, $s_2 = 5$, $s_3 = 8$

$$x = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k \pmod{315}$$

$$x = [(63)(2)(3) + (45)(5)(4) + (35)(8)(6)] \pmod{315}$$

$$x = 2958 \pmod{315}$$

Therefore $x = 123$

CHAPTER 7: GRAPHS

A **graph** $G = (V, E)$ consists of V , a nonempty set of vertices (or nodes) and E , a set of edges. Each edge has either one or two vertices associated with it, called its endpoints. An edge is said to connect its endpoints.

Classification of Graphs

A. Undirected graph

1. Simple graph

A graph in which each edge connects two different vertices and where no two edges connect the same pair of vertices.

2. Multigraph

Graphs that may have multiples edges connecting the same vertices.

3. Pseudograph

Graph that may include loops(edges that connect a vertex to itself) and possibly multiple edges connecting the same pair of vertices.

B. Directed graph

1. Simple directed graph

A directed graph with no loops and no multiple edges.

2. Multiple directed graph

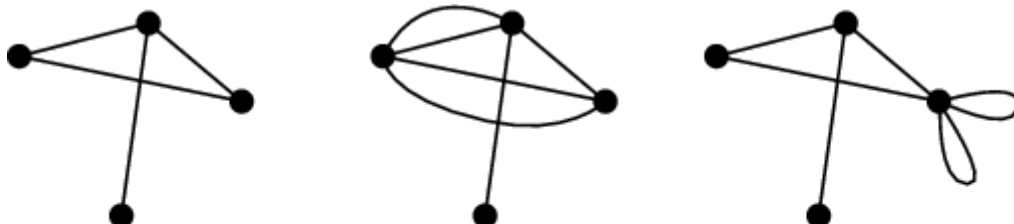
Directed graph that may have multiple directed edges from a vertex to a second vertex.

C. Mixed graph

A graph that is undirected and directed and in which multiple edges and multiple loops are allowed.

Type	Edges	Multiple Edges	Loops Allowed?
		Allowed?	
Simple graph	Undirected	No	No
Multigraph	Undirected	Yes	No
Pseudograph	Undirected	Yes	Yes
Simple directed graph	Directed	No	No
Directed multigraph	Directed	Yes	Yes
Mixed graph	Directed and	Yes	Yes
	Undirected		

Example: The following are illustrations of different types of graphs:

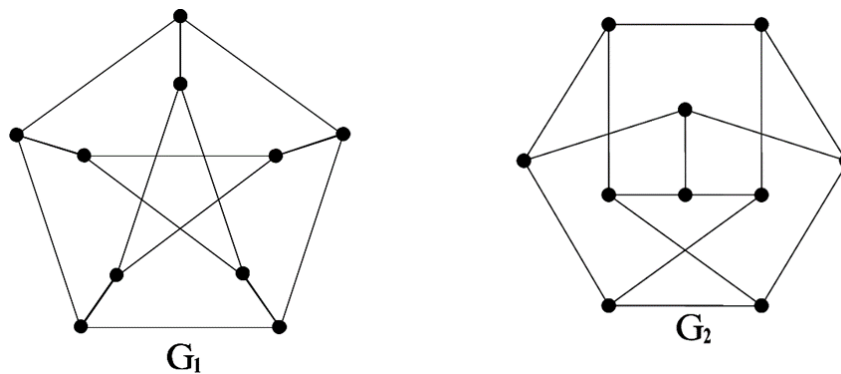


Basic Graph Terminology

1. A pair of vertices v and w is **adjacent** if there exist an edge e joining them. In this case we say both v and w are incident to e . We can also say that e is incident to v and to w .
2. The **valency** or **degree**, $\deg(v)$, of a vertex v is the number of edges which are incident to v . Note that a loop contributes twice to the degree of that vertex.
3. A graph in which every vertex has the same valency r is called **regular (with valency r)**.

Example

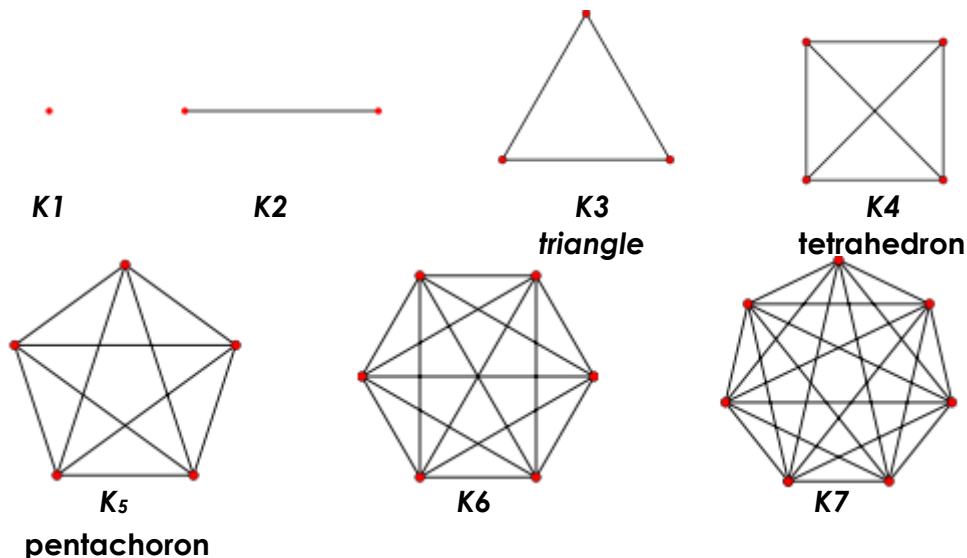
A well – known regular (with valency 3) simple graph is **Petersen's graph**. Two diagrams representing this graph are shown below.

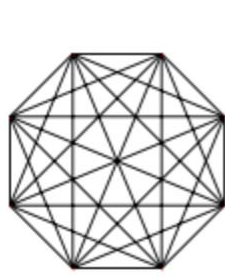
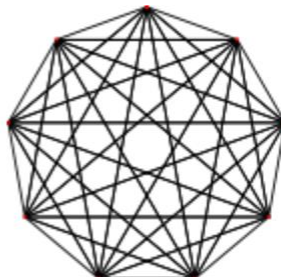
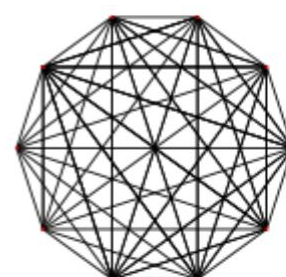


Some Special Simple Graphs

1. Complete Graphs

The **complete graph** on n vertices, denoted by K_n , is the simple graph that contains **exactly one edge** between each pair of **distinct vertices**.

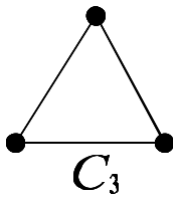
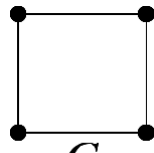
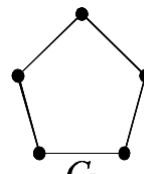
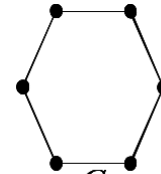


 K_8  K_9  K_{10}

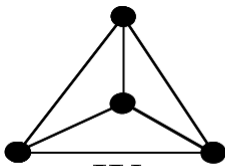
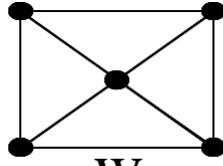
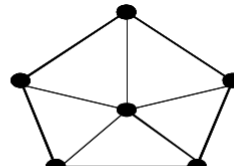
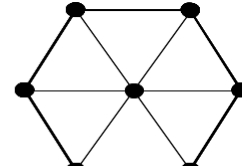
Note: A complete graph contains all $\frac{n(n-1)}{2}$ possible edges.

2. Cycles

The **cycle** C_n , $n \geq 3$, consists of n vertices v_1, v_2, \dots, v_n and edges $(v_1, v_2), (v_2, v_3), \dots, (v_{n-1}, v_n)$ and (v_n, v_1) . The cycles C_3, C_4, C_5 and C_6 are displayed

 C_3  C_4  C_5  C_6

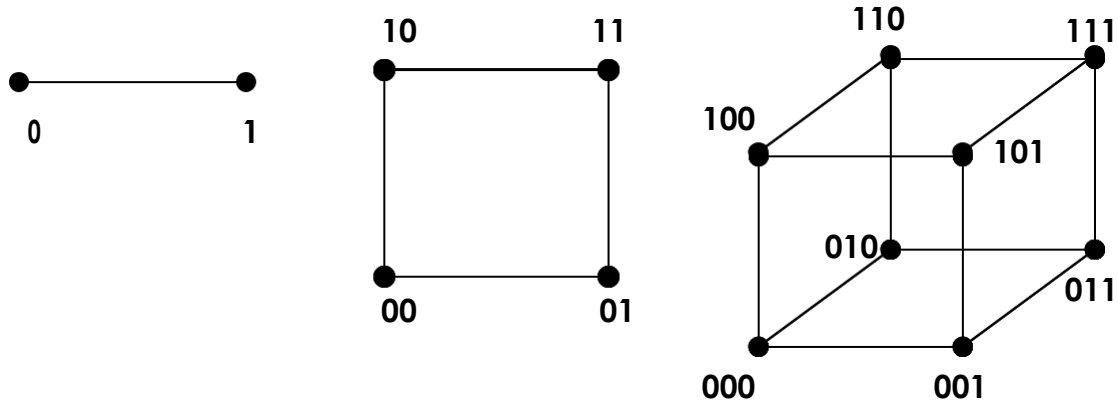
We obtain the wheel, W_n when we add an additional vertex to the cycle C_n , for $n \geq 3$, and connect this new vertex to each of the n vertices in C_n , by new edges. The wheels W_3, W_4, W_5 and W_6 are displayed.

 W_3  W_4  W_5  W_6

Note: A wheel graph contains all $2(n-1)$ possible edges.

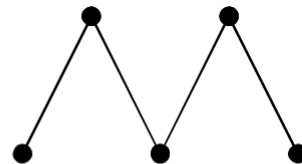
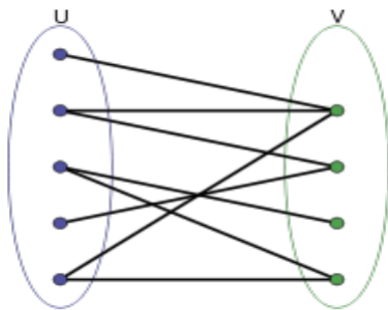
3. n – Cubes

The **n – cube**, denoted by Q_n , is the graph that has vertices representing the 2^n bit strings of length n . Two vertices are adjacent if and only if the bit strings that they represent differ in **exactly one bit**. The graphs Q_1, Q_2 and Q_3 are displayed below.

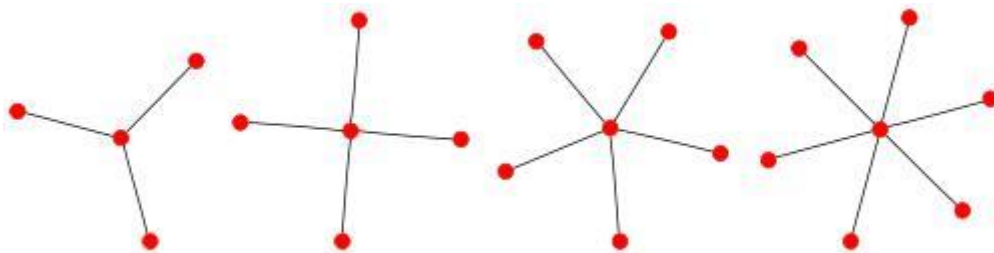


4. Bipartite Graphs

A simple graph G is called **bipartite** if its vertex set V can be partitioned into two disjoint nonempty sets U and V such that every edge in the graph connects a vertex in U and a vertex in V (so that no edge in G connects either two vertices in U or two vertices in V).

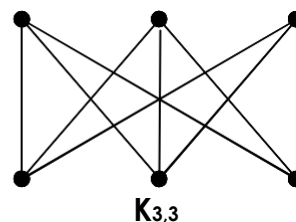
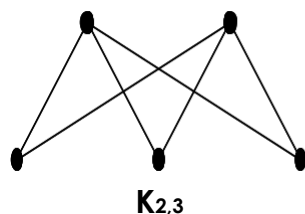


Star Graphs



5. Complete Bipartite Graphs

The **complete bipartite graph** $K_{m,n}$ is the graph that has its vertex set partitioned into two subsets of m and n vertices, respectively.



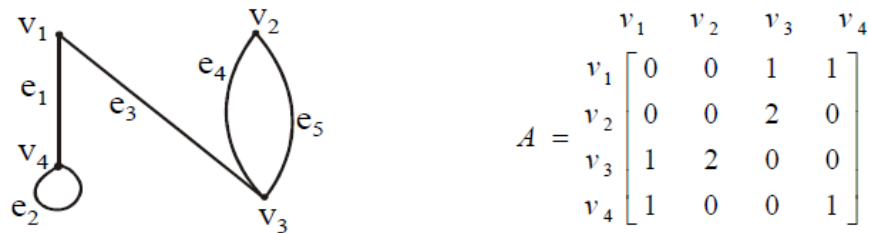
Representing Graphs

1. Adjacency Matrices

Let $G = \langle V, E \rangle$ be a graph with vertex set $\{v_1, v_2, \dots, v_n\}$. The adjacency matrix of G is the $n \times n$ matrix $A = A(G)$ such that a_{ij} is the number of distinct edges joining v_i and v_j .

Example

A graph with it's adjacency matrix is shown



Note that the nonzero entries along the main diagonal of A indicate the presence of loops and entries larger than 1 correspond to parallel edges. Also note A is a symmetric matrix.

Example

Find directed graph that has the adjacency matrix

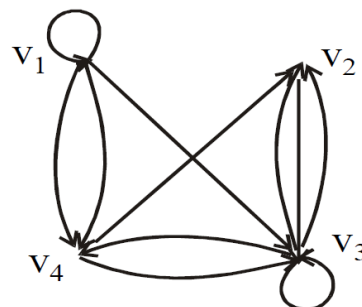
$$\begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Solution

The 4×4 adjacency matrix shows that the graph has 4 vertices say v_1, v_2, v_3 and v_4 labeled across the top and down the left side of the matrix.

$$A = \begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} & \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{matrix}$$

A corresponding directed graph is



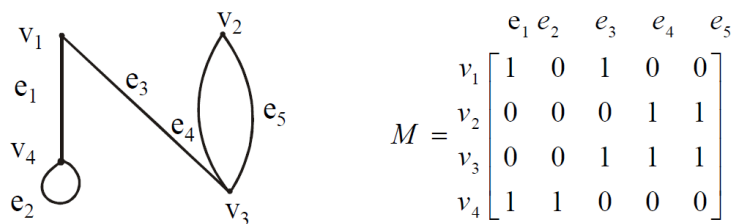
2. Incidence Matrix

Suppose that v_1, v_2, \dots, v_n are the vertices and e_1, e_2, \dots, e_m are the edges of G . Then the **incidence matrix** with respect to this ordering of V and E is the $n \times m$ matrix $M = [m_{ij}]$; where

$$m_{ij} = \begin{cases} 1, & e_j \text{ is incident to } v_i \\ 0, & \text{otherwise} \end{cases}$$

Example

A graph with its incidence matrix is shown



Paths and Circuits

1. An **edge sequence of length n** in a graph G is a sequence of (not necessarily distinct) edges e_1, e_2, \dots, e_n such that e_i and e_{i+1} are adjacent for $i = 1, 2, \dots, n-1$. The edge sequence determines a sequence of vertices (again, not necessarily distinct) $v_0, v_1, v_2, \dots, v_{n-1}, v_n$ where $f(e_i) = \{v_{i-1}, v_i\}$. We say v_0 is the **initial vertex** and v_n the **final vertex** of the edge sequence.
2. A $v_0 - v_n$ **walk** of graph G is a finite, alternating sequence

$$v_0 - v_n \rightarrow v_0, e_1, v_1, e_2, v_2, e_3, \dots, v_{n-1}, e_n, v_n$$

of vertices and edges, with an initial vertex v_0 and final vertex v_n , such that

$$e_i = v_{i-1} v_i \text{ for } i = 1, 2, \dots, n.$$

The number n (the number of occurrences of edges) is called the **length** of the walk.

A **trivial walk** contains no edges, that is, $n = 0$.

A $v_0 - v_n$ **walk** is closed or open depending on whether $v_0 = v_n$ or $v_0 \neq v_n$.

Note: There may be repetition of vertices and edges in a walk.

3. A $v_0 - v_n$ **trail** is a $v_0 - v_n$ walk in which no edge is repeated.
4. A $v_0 - v_n$ **path** is a $v_0 - v_n$ walk in which no vertex is repeated.

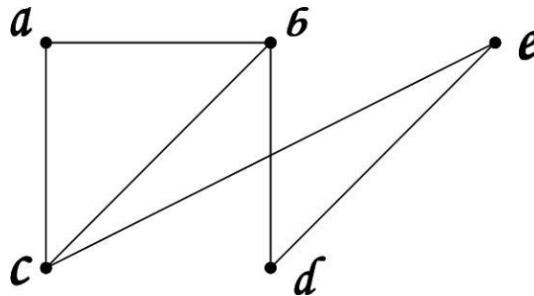
A **path** is an edge sequence in which all the edges are distinct. If in addition all the vertices are distinct (except possibly $v_0 = v_n$) the path is called **simple**.

Note: Every path is therefore a trail. Every path is a walk.

5. An edge sequence is closed if $v_0 = v_n$ (which starts and ends on the same vertex). A closed simple path containing at least one edge is called a **circuit**.

Example

Consider the graph as shown



Hence,

$W_1: c, b, a, c, b, d, e$ is a $c - e$ walk, which is not a trail.

$W_2: c, b, a, c, e$ is a $c - e$ trail, which is not a path.

$W_3: c, b, d, e$ is a $c - e$ path.

Eulerian Trail and Eulerian Circuits

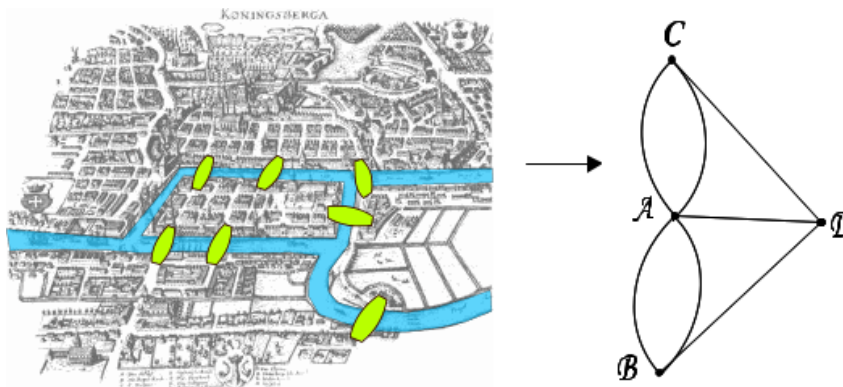
An **eulerian trail** of a connected graph (multigraph) G is an open trail of G containing all the edges of G , while an **eulerian circuit** of G is a circuit containing all the edges of G . A graph (multigraph) possessing an eulerian circuit is called an **eulerian graph** (multigraph).

Theorem (Euler):

A connected graph G is Eulerian if and only if each of its vertices has even degree.

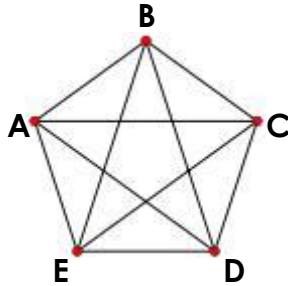
Example: Königsberg Bridge Problem

The Pregel River flows through the town of Königsberg (now Kaliningrad in Russia). There are two islands in the river, connected to the banks and each other by bridges as shown. The problem for the citizens of Königsberg was whether there was a walk, beginning on one of the banks or islands, which took in every bridge exactly once and finished back at its starting position.



Solution

Since the graph representing these bridges has four vertices of odd degree, it does not have an Eulerian trail. There is no way to start at a given point, cross each bridge exactly once, and return to the starting point.

Example: Complete Graph of 5 vertices, K_5 .**Solution:**

Since the graph is connected and every vertex has degree 4, so K_5 is Eulerian.

One eulerian trail beginning at the vertex A has the following vertex sequence:

A,B,D,A,C,E,B,C,D,E,A

EXERCISE 1: SET THEORY

1. Let $A = \{x \in U \mid x \text{ is a multiple of } 2\}$ $C = \{x \in U \mid x \text{ is a multiple of } 3\}$
 $B = \{x \in U \mid x \text{ is a perfect square}\}$ $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Find each set.

- a.) $A \cup B$ d.) $\bar{B} \cap (A \cup C)$
b.) $A \cup C$ e.) $(C - B) \cup (B - A)$
c.) $B - \bar{C}$ f.) $\overline{C - (B - A)}$

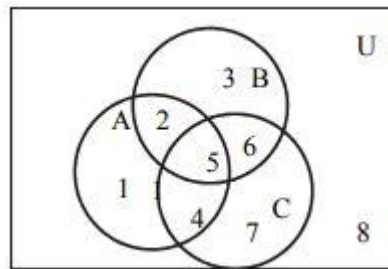
2. Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ $X = \{1, 3, 5, 6, 7\}$
 $Y = \{y \mid y = 2x, x \in Z\}$ $Z = \{z \mid z \text{ is a prime number}\}$

Enumerate:

- a.) $\overline{X - \bar{Z}}$ c.) $\bar{Z} - \overline{Y - \bar{X}}$
b.) $\bar{X} \cup (Y \cap \bar{Z})$ d.) $Y \cup (\bar{X} - Z)$

3. Let U be the universal set and let A , B and C be subsets of U . Sketch a Venn diagram for each set.

- a.) $A \cap (B \cap \bar{C})$
b.) $(A \cap \bar{B}) \cup \bar{C}$
c.) $\overline{[(A - B) \cap C] \cup B}$



4. Represent the Venn diagrams that indicate the following:

- a.) Examination, Question and Practice
b.) Dogs, pet animals and animals
c.) Lion, Dog and Snake
d.) Judge, Thieves and Criminals
e.) Teacher, Writer and Musician

5. In a school, 100 students have access to three software packages A, B and C

28 did not use any software

8 used only packages A

26 used only packages B

7 used only packages C

10 used all three packages 13 used both A and B

- a.) Draw a Venn diagram with all sets enumerated as far as possible. Label the two subsets which cannot be enumerated as x and y , in any order

- b.) If twice as many students used package B as package A, write down a pair of simultaneous equations in x and y .
- c.) Solve these equations to find x and y .
- d.) How many students used package C?

6. A group of 54 students were surveyed, and it was found that each of the students surveyed liked at least one of the following three fruit: apples, blueberries and cranberries.

28 liked apples

36 liked blueberries

31 liked cranberries

8 liked apples and blueberries, but not cranberries

9 liked blueberries and cranberries, but not apples

11 liked all three of the following fruit: apples, blueberries and cranberries.

- a.) How many students liked apples, but not blueberries or cranberries?
- b.) How many students liked cranberries, but not blueberries or apples?
- c.) How many students liked none of the following three fruit: apples, blueberries and cranberries?

7. A survey was carried out to find if students in the theater department liked the following three actors: Marlon Brando, Clint Eastwood and Paul Newman. Exactly 51 students participated in the survey.

26 students liked Marlon Brando.

34 students liked Clint Eastwood.

29 students liked Paul Newman.

2 students liked Paul Newman and Marlon Brando, but not Clint Eastwood.

9 students liked Paul Newman and Clint Eastwood, but not Marlon Brando.

19 students liked exactly two of the following three actors: Marlon Brando, Clint Eastwood and Paul Newman.

11 students liked all of the following three actors: Marlon Brando, Clint Eastwood and Paul Newman.

- a.) How many students liked exactly one of the following three actors: Marlon Brando, Clint Eastwood and Paul Newman?
- b.) How many students liked none the following three actors: Marlon Brando, Clint Eastwood and Paul Newman?
- c.) How many students liked at most two of the following three actors: Marlon Brando, Clint Eastwood and Paul Newman?

8. Simplify each of the following sets using Set Identities

$$a) Z = (P \cup Q) \cap (\bar{Q} \cap S)$$

$$b) Z = (A - B) \cup (A \cap B)$$

$$c) Z = \overline{(\bar{P} \cup Q) \cap (\bar{Q} \cap \bar{S})}$$

$$d) Z = S \cap (P \cup \bar{S}) \cap (Q \cup \bar{S}) \cap \overline{P \cap Q \cap S}$$

9. Construct the truth table of the following set equations

$$a) Z = (A - \bar{B}) - \bar{A} \cap (A - \bar{B})$$

$$b) Z = \overline{[(A - B) \cap C] \cup B}$$

$$c) Z = S \cap (P \cup \bar{S}) \cap (Q \cup \bar{S}) \cap \overline{P \cap Q \cap S}$$

EXERCISE 2: LOGIC

1. Let p = "It is raining"

q = "I am wearing my rubbers",

s = "I am carrying my umbrella".

Express each of the following statements in symbols:

a) "It is raining and I am not wearing my rubbers."

b) "Either it is not raining or I am wearing my rubbers."

c) "It is not true that it is raining and I am wearing my rubbers."

d) "Either it is raining, or it is not true that it is raining or I am wearing my rubbers."

e) "Either it is not raining, or I am wearing my rubbers and I am carrying my umbrella."

f) "It is raining, still I am neither wearing my rubbers nor carrying my umbrella."

g) "Either it is raining and I am wearing my rubbers, or it is not raining and I am not carrying my umbrella."

2. Let's consider a compound propositions where

A = "Angelo comes to the party",

B = "Bruno comes to the party",

C = "Carlo comes to the party",

D = "David comes to the party".

Represent the following statements into a Boolean expression:

a) "If David comes to the party then Bruno and Carlo come too"

b) "Carlo comes to the party only if Angelo and Bruno do not come"

c) "David comes to the party if and only if Carlo comes and Angelo doesn't come"

d) "If David comes to the party, then, if Carlo doesn't come then Angelo comes"

e) "Carlo comes to the party provided that David doesn't come, but, if David comes, then Bruno doesn't come"

f) "A necessary condition for Angelo coming to the party, is that, if Bruno and Carlo aren't coming, David comes"

g) "Angelo, Bruno and Carlo come to the party if and only if David doesn't come, but, if neither Angelo nor Bruno come, then David comes only if Carlo comes"

3. Construct the Truth Table and Determine whether each of the following compound proposition is a Tautology, Contradiction or Contingency.

a) $X \equiv (P \wedge \neg Q) \wedge (\neg P \vee Q)$

b) $Z \equiv (\neg P \rightarrow Q) \vee [(P \wedge \neg R) \leftrightarrow Q]$

c) $Z \equiv [\neg P \rightarrow (P \rightarrow Q)] \rightarrow [Q \rightarrow (P \rightarrow P)]$

d) $Z \equiv (P \wedge R) \leftrightarrow [\neg S \vee (Q \rightarrow P)]$

e) $Z \equiv \{[(A \rightarrow B) \wedge (C \rightarrow D)] \wedge (A \vee C)\} \wedge \neg B \rightarrow D$

4. Simplify the following using the algebra of propositions. Show your solutions

a) $A \equiv \neg\{[Q \vee (P \wedge Q)] \wedge [P \wedge (P \wedge Q)]\}$

b) $B \equiv \{[\neg(P \wedge S) \vee \neg Q] \wedge (P \vee \neg Q) \wedge \neg(P \wedge S)\}$

c) $C \equiv [\neg P \rightarrow (P \rightarrow Q)] \rightarrow [Q \rightarrow (P \rightarrow P)]$

d) $X \equiv [(P \vee \neg Q) \wedge (Q \vee \neg S) \wedge S \wedge \neg(P \wedge Q \wedge S)]$

e) $X \equiv \{S \vee \neg(\neg P \wedge \neg Q) \vee [(P \vee Q) \wedge S]\}$

5. Supply the reasons for each step needed to show that the following argument is valid.

a) The Chairman on the board of XYZ Automobile Company was strongly urging that the company purchase Ace Rubber Company. He based his recommendation on the following argument.

"If we buy Ace Rubber Co., then we can make our own tires. Our earnings will be higher if we sell our cars cheaper. People will invest in our company provided that our earnings are higher. Now, it is impossible to make our own tires and not sell our cars cheaper. Therefore, if we buy Ace Rubber Co. then the people will invest in our company."

b) At the end of a long and heated trial, the defense attorney sums up his case as follows:

"If my client were guilty (G), then he must have been at the scene of the crime (A). It is certainly not true that he was at the scene of the crime and at the same time was out of town (O). Now, if the witness who identified my client as being out of town was not mistaken ($\sim M$), then my client must have been out of town. But, the Prosecution Attorney was not able to prove that the witness was mistaken. Therefore, my client is not guilty."

On the basis of this summation, should the defendant be found guilty or not guilty?

c) Hypothesis:

$$P \rightarrow R$$

$$Q \rightarrow R$$

$$\therefore (P \vee Q) \rightarrow R$$

d) Hypothesis:

$$\neg(P \wedge Q)$$

$$\neg R \rightarrow Q$$

$$\neg P \rightarrow R$$

$$\therefore R$$

e) Hypothesis:

P

$P \rightarrow Q$

$S \vee R$

$R \rightarrow \neg Q$

$\therefore S \vee T$

PROOF	REASON
1. P	
2. $P \rightarrow Q$	
3. $S \vee R$	
4. $R \rightarrow \neg Q$	
5. Q	
6. $Q \rightarrow \neg R$	
7. $\neg R$	
8. S	
9. $S \vee T$	

f) Hypothesis: (Indirect Proof)

$\neg Q \vee R$

$P \rightarrow \neg R$

Q

$\therefore \neg P$

PROOF	REASON
1. $\neg Q \vee R$	
2. $P \rightarrow \neg R$	
3. Q	
4. $P \therefore f$	
5. $Q \rightarrow R$	
6. R	
7. $\neg P$	
8. $P \vee \neg P$	
9. f	

EXERCISE 3: RELATIONS

1. Let $A = \{2, 3, 4, 5, 6, 7, 8\}$ and R a relation over A . Draw the directed graph and the binary matrix of R , after realizing that xRy iff $x - y = 3n$ for some $n \in \mathbb{Z}$.

2. Given Binary Matrix Relations Q , R , and S :

$$Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \quad R = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Evaluate:

a.) M_{RoQ}

b.) M_{SoQ}

c.) $M_{SoR^{-1}}$

3. Given set $A = \{1, 2, 3, 4, 5\}$ and let R and S be a binary relation on set A .

$R = \{(a, b) \in A \times A \mid b|a\}$ and $S = \{(2, 1), (2, 3), (3, 4), (3, 5), (4, 5)\}$

a.) Evaluate the Domain and Range of SoR .

b.) Evaluate $(SoR)^{-1}$ and \overline{SoR} .

4. Construct the Hasse Diagram of the following posets:

a.) $(\{1, 2, 3, 6, 12, 24\}, |)$

b.) $(\{2, 3, 4, 5, 6, 30, 60\}, |)$

c.) $(\{2, 4, 6, 12, 24, 36\}, |)$

d.) $(\{a, b, c, d\}, \subseteq)$

e.) $R = \{(a, a), (a, c), (a, b), (a, e), (d, d), (d, b), (d, e), (c, c), (c, e), (b, b), (b, e), (e, e)\}$

(Show the step by step procedure of making Hasse Diagram)

5. Construct the state diagram of the following sequences.

a.) Overlapping 10110 sequence using Mealy State Machine.

b.) Non-overlapping 10011 sequence using Mealy State Machine.

c.) Overlapping 101101 sequence using Moore State Machine.

d.) Non-overlapping 110100 sequence using Moore State Machine.

6. For each of the following relations on sets $\{a, b, c, d\}$, decide whether it is reflexive, irreflexive, symmetric, antisymmetric and transitive.

- a) $\{(c, b), (c, c), (c, d), (d, b), (d, c), (d, d)\}$
- b) $\{(a, a), (a, c), (c, a), (b, b), (c, c), (d, d)\}$
- c) $\{(c, d), (d, c)\}$
- d) $\{(a, b), (b, c), (c, d)\}$
- e) $\{(a, a), (b, b), (c, c), (d, d)\}$

EXERCISE 4: FUNCTIONS

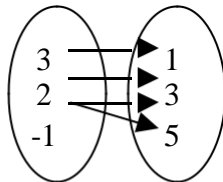
1. Determine if the given describes a function or not.

a. $\{(1,8), (7,5), (7,2), (7,-1)\}$

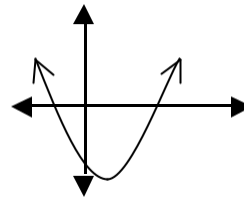
b.

x	5	10	20	15
y	-2	-2	-2	-2

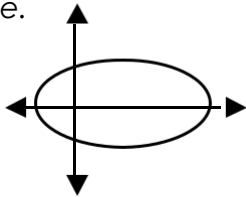
c.



d.



e.



2. Determine the domain and range of each function.

a. $y = \sqrt{x-3}$

b. $y = \frac{5}{4-x}$

c. $f(x) = x^2 + 1$

3. Let $f(x) = x^3 - 3$, $g(x) = 9 - 5x$ and $h(x) = \begin{cases} \frac{x^2-3x-4}{x-4}, & x \neq 4 \\ 5, & x = 4 \end{cases}$

Find:

a. $h(5)$

e. $(g \circ h)(-1)$

b. $g(-2)$

f. $\left(\frac{f-h}{g}\right)(4)$

c. $f(x+1)$

g. $(f \circ g)\left(\frac{2}{5}\right)$

d. $(g+h)(-3)$

h. $\left(\frac{f}{g}\right)\left(\frac{1}{x}\right)$

4. Let f be a function from X to Y . Determine whether f is one-to-one or onto.

- a. $f(x) = \{(1, b), (3, a), (2, c)\}; X = \{1, 2, 3\} Y = \{a, b, c, d\}$
- b. $f(x) = \{(1, a), (2, c), (3, b)\}; X = \{1, 2, 3\} Y = \{a, b, c\}$
- c. $f(x) = \{(1, b), (2, b), (3, a)\}; X = \{1, 2, 3\} Y = \{a, b, c\}$
- d. $f(x) = \{(1, a), (2, c), (3, c)\}; X = \{1, 2, 3\} Y = \{a, b, c, d\}$

5. Determine whether each of these functions from the set of integers to the set of integers is one-to-one or onto.

- a. $f(x) = x - 2$
- b. $f(x) = x^2 + 3$
- c. $f(x) = \frac{x^2+1}{x^2+2}$

6. Determine whether each of these functions from the set of real numbers to the set of real numbers is one-to-one or onto.

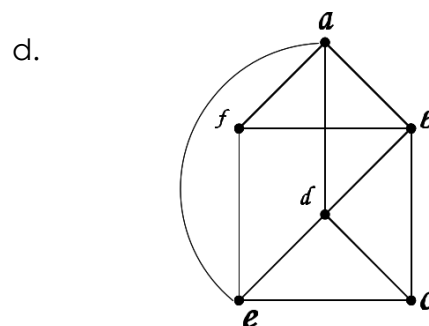
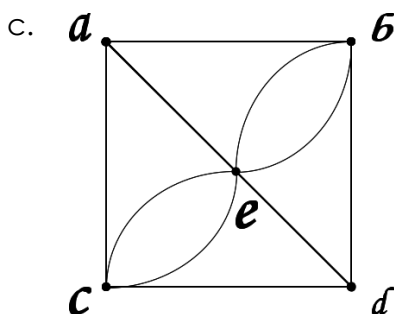
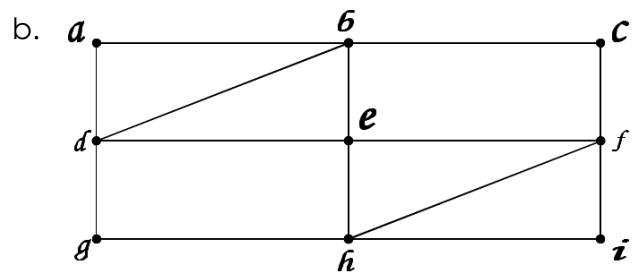
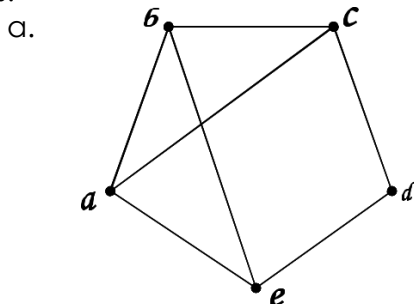
- a. $f(x) = 3x - 6$
- b. $f(x) = 2x^3 - 7$
- c. $f(x) = \frac{x}{x^2+1}$

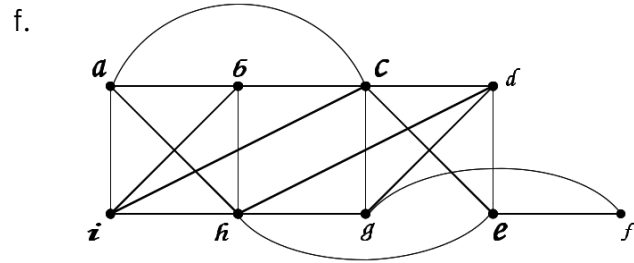
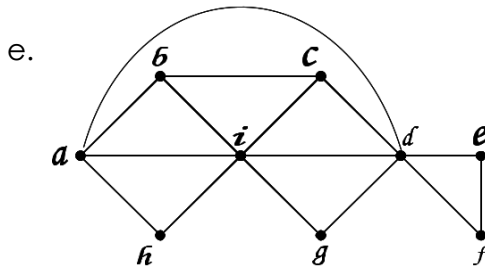
7. Find the inverse of each function

- a. $f(x) = 2x + 5$
- b. $f(x) = x^3 + 4$
- c. $f(x) = \frac{x-1}{x+5}$

EXERCISE 5: GRAPHS

1. Determine whether each graph has an Euler circuit. Construct such circuit when one exists.





EXERCISE 6: NUMBER THEORY

A. Solve the following:

1. For each pair of integers a and b , find $d = \gcd(a, b)$ and find x and y such that $d = ax + by$:

(a) $a = 356, b = 48$

(c) $a = 2310, b = 168$

(b) $a = 1287, b = 165$

(d) $a = 195, b = 968$

2. Using the Euclidean algorithm, find the \gcd of each pair of integers.

(a) 28, 12

(c) 1947, 63

(b) 784, 48

(d) 5076, 1076

3. Suppose $a = 5880$ and $b = 8316$.

(a) Express a and b as products of primes.

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

(c) Verify that $\text{lcm}(a, b) = |ab| / \gcd(a, b)$

4. Find them if:

(a) lcm of two consecutive positive integers is 812;

(b) lcm of twin primes is 899.

5. List all prime numbers between 1000 and 1500.

B. Find the general solution of each Linear Diophantine Equation.

1. $12x + 16y = 20$

3. $28x + 91y = 119$

2. $15x + 21y = 39$

4. $1776x + 1976y = 4152$

C. Determine whether each linear congruence is solvable.

1. $12x \equiv 18 \pmod{16}$

4. $276y \equiv 3476 \pmod{1276}$

2. $15y \equiv 18 \pmod{12}$

5. $x \equiv 3 \pmod{9}$

3. $22x \equiv 14 \pmod{14}$

6. $4x \equiv 6 \pmod{14}$

D. Determine the number of incongruent solutions of each linear congruence.

- | | |
|------------------------------|--------------------------------|
| 1. $22x \equiv 18 \pmod{75}$ | 6. $37x \equiv 1 \pmod{249}$ |
| 2. $2z \equiv 119 \pmod{98}$ | 7. $195x \equiv 23 \pmod{968}$ |
| 3. $9x \equiv 95 \pmod{36}$ | 8. $48x \equiv 284 \pmod{356}$ |

E. Using congruence's, solve each Linear Diophantine Equation

- | | |
|----------------------|---------------------------|
| 1. $3x + 4y = 5$ | 4. $1776x + 1976y = 4152$ |
| 2. $15x + 21y = 39$ | 5. $6x + 9y = 15$ |
| 3. $48x + 84y = 144$ | 6. $28x + 91y = 119$ |

E. Find the remainder when;

1. 3100 is divided by 91
2. $1! + 2! + \dots + 300!$ is divided by 13
3. 23243 is divided by 17
4. $2^{100} + 3^{123}$ is divided by 11
5. Find the ones digit in the sum $1! + 2! + \dots + 100$

F. Determine whether each linear system is solvable.

- | | | | |
|---------------------------|------------------------|------------------------|-------------------------|
| 1. $x \equiv 4 \pmod{6}$ | $x \equiv 2 \pmod{8}$ | $x \equiv 1 \pmod{9}$ | |
| 2. $x \equiv 3 \pmod{4}$ | $x \equiv 5 \pmod{9}$ | $x \equiv 8 \pmod{12}$ | |
| 3. $x \equiv 7 \pmod{12}$ | $x \equiv 7 \pmod{15}$ | $x \equiv 7 \pmod{18}$ | |
| 4. $x \equiv 2 \pmod{6}$ | $x \equiv 5 \pmod{9}$ | $x \equiv 8 \pmod{11}$ | $x \equiv 11 \pmod{15}$ |
| 5. $x \equiv 2 \pmod{6}$ | $x \equiv 5 \pmod{7}$ | $x \equiv 6 \pmod{8}$ | $x \equiv 8 \pmod{9}$ |

EXERCISE 7: COMBINATORICS

A. Solve the following problems. Show your solutions.

1. A combination lock consists of the 26 letters of the English alphabet. If a 3-letter combination is needed, how many possible combination locks are there?
2. Marie, Ten-ten, My-my, Shayne, and Gelli plan to form a musical band. In how many ways can they be seated in a round table if Ten-ten and My-my will not sit next to each other?
3. There are 9 dots randomly placed on a circle. How many triangles can be formed within the circle?
4. The dean of science wants to select a committee consisting of mathematicians and physicists to discuss a new curriculum. There are 15 mathematicians and 20 physicists at the faculty; how many possible committees of 8 members are there, if there must be more mathematicians than physicists (but at least one physicist) on the committee?
5. A delegation of 4 students is selected each year from a college to attend the National Student Association annual meeting. There are 12 eligible students to comprise the delegation.
 - a. In how many ways can the delegation be chosen from among all the eligible students?

- b. In how many ways can the delegation be chosen if two of the eligible students will not attend the meeting together?
- c. In how many ways can the delegation be chosen if two of the eligible students are married and will only attend the meeting together?
6. How many different signals, each consisting of 6 flags hung in a vertical line, can be formed from 4 identical red flags and 2 identical blue flags?
7. There are 12 students in a class. In how many ways can the 12 students take 3 different tests if 4 students are to take each test?
8. Find the number m of ways that a class X with ten students can be partitioned into four teams A_1 , A_2 , B_1 and B_2 where A_1 and A_2 contain two students each and B_1 and B_2 contain three students each.
9. Bridge is played with a standard deck of 52 cards, each player receives 13 cards. How many possible hands can a player get in a game of bridge? In the HCP (high card points) system, four points are assigned to an ace, three points to a king, two to a queen and one to a jack. How many possible hands result in a total of (a) exactly three points? (b) at least three points?
10. The South African National Assembly consists of 400 members. How many possible ways are there to divide the 400 seats among three parties (a) such that none of them has a majority? (b) such that none of them has a 2/3-majority?
11. In how many possible orders can the letters of the word MATHEMATICS be arranged?
12. At a dance, there are 20 girls and 20 boys. How many ways are there to form 20 pairs? How many, if boys may dance with boys and girls with girls?
13. A single piece is placed on the lower-left corner square of an 8×8 -chessboard. The piece may only move horizontally or vertically, one square at a time. How many possible ways are there to move the piece to the opposite corner in 14 moves (the smallest possible number of moves)?
14. The four women Anne, Betsie, Charlotte and Dolores and the six men Eric, Frank, George, Harry, Ian and James are friends. Each of the women wants to marry one of the six men. In how many ways can this be done?
15. A palindrome is a word that can be read the same way in either direction (such as RACECAR). How many 9-letter palindromes (not necessarily meaningful) can be formed using the letters A–Z?

B. Solve the following equations

1. Solve for n in the equation: $\frac{P(n,4)}{P(n-1,4)} = \frac{5}{3}, n > 4$
2. Solve for n , $C(n,4) = 210$
3. Find the value of n in the equation $3P(n,4) = P(n-1,5)$
4. Solve for n if $3C(n,2) = P(6,2)$
5. If $P(n,r) = 506$ and $C(n,r) = 253$. Find n and r .