2.07.2019
Tuesday

Unit - I

Propositional Logic

The rules of logic specify the meaning of mathematical statements. For instance, these rules help to understand and ~~Bisten~~ reason with statements such as. 'there exists an integer that is not the sum of two squares' and 'for every positive integer n. the sum of the positive integers not exceeding n is $\frac{n(n+1)}{2}$'.

4.07.2019
Thursday

Logic is the basis of all mathematical reasoning, and of all automated reasoning. It has practical applications to the design of computing machines, to the specification of systems, to artificial intelligence, to computer programming and so on.

The rules of logic give precise meaning to mathematical statements. These rules are used to distinguish between valid and invalid mathematical arguments. Software systems have been developed for constructing proofs automatically. The rules are used in the design of computer circuits, the construction of computer programs, the verification of the correctness of programs, and in many other ways.

Propositions

A proposition is a declarative sentence, that is a sentence that declares a fact. This is either true or false, but not both.

eg:- all the following declarative sentences are propositions.

1. Toronto is the capital of Canada. (F) Ottawa
2. New Delhi is the capital of India. True (T)
3. ~~Dia~~ $1 + 1 = 2$ True (T)
4. $5 + 7 = 2$ False (F)

The following declarative sentences are not propositions.

1. What time is it ?
2. Read this carefully
3. $x + 1 = 2$
4. $x + y = z$

1 and 2 are not propositions because they are not declarative sentences. 3 and 4 are not propositions because they are neither true nor false.

We use letters to denote propositional variables or statement variables, that is, variables that represent propositions, just as letters are used to denote numerical values. The conventional letters used for propositional variables are p, q, r, s ... Truth value of a proposition is true, denoted by T,

if it is a true proposition and false, denoted by F. if it is a false proposition.

Area of logic that deals with propositions is called the propositional calculus. or propositional logic. It was first developed systematically by the Greek philosopher Aristotle more than 2800 years ago.

Negation of a proposition

This can be considered the result of the operation of the negation operator on a proposition. It shows the opposite meaning in effect.

The negation operator constructs a new proposition from a single existing proposition. The following table displays that truth table for the negation of a proposition p

p	¬p
T	F
F	T

This table has a row for each of the two possible truth values of a proposition p. Each row shows the truth value of ¬p (not p) corresponding to the truth value of p for this row.

definition:-

→ Let p be a proposition. The negation of p, denoted by ¬p (also denoted by $\bar{p}$), is the statement, "It is not the case that p".

eg:-

'Today is saturday' the negation of this proposition is, 'it is not the case that today is saturday'. This negation can be more simply expressed by 'today is not saturday' or 'it is not saturday today'.

eg:- Find the negation of the proposition, "at least 10 inches of rain fell today in Miami". Its negation is 'it is not the case that atleast 10 inches of rain fell today in Miama'. It can also simply expressed as 'less than 10 inches of rain fell today in Miami'.

Conjuction of 2 propositions :- (AND)

Definition

Let p and q be propositions. The conjunctions of p and q, denoted by $p \wedge q$, is the proposition "p and q". The conjuction p and q is true when both p and q are true and is false otherwise.

The truth table for the conjunction of two propositions

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

The word 'but' sometimes is used instead of 'AND' in a conjunction.
for eg:- the statement 'The sun is shining but it is rainining' is another way of saying 'The sun is shining and it is raining.'

Q:- Find the conjunction of the propositions p and q where p is the proposition 'Today is Sunday' and q is the proposition 'Today is holiday'

The conjunction of this proposition (p and q) $p \wedge q$, is the proposition, 'Today is sunday and today is holiday'.

Disjunction of two propositions ($\vee$)

Definition:
Let p and q be propositions. The disjunction of p and q denoted by ~~p or q~~ $p \vee q$, is the proposition p or q.

The disjunction $p \vee q$ is false when both p and q are false and is true otherwise.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

A disjunction is true when atleast one of the two propositions is true. For instance, the inclusive OR is being used in the statement, 'Students who have taken calculus or computer science can take this class.' This means that students who have taken both calculus and computer science can take the class as well as the students who have taken only one of the two subjects

Exclusive OR ($\oplus$)

Let p and q be propositions. the exclusive OR of p and q denoted by $p \oplus q$, is the proposition that is true when exactly one of p and q is true and is false otherwise.

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

when the exclusive OR is used to connect the propositions p and q, the proposition p or q (but not both is obtained).

eg:- Students who have taken calculus or computer science, but not both, can enroll in this class

Here, it means that students who have taken both calculus and computer science course cannot take the class. Only those who have taken exactly one of the two courses can take the class

eg:- when a menu at a restaurant states 'Soup or salad comes with an entree' the restaurant almost always means that customers can have either soup or salad, but not both. This is an exclusive OR rather than an inclusive, OR

1. Which of these sentences are propositions? What are the truth ~~tables~~ values of those that are propositions?

(a) Boston is the capital of Massachusetts
It is a proposition. True

(b) $2 + 3 = 5$
It is a proposition. True

(c) $5 + 7 = 10$
It is a proposition. False

(d) $x + 2 = 11$
It is not a proposition.

(e) Answer the question.
It is not a proposition

(f) What time is it?
It is not a proposition

(g) The moon is made of green cheese
It is a proposition. False

(h) Do not pass Go.
It is not a proposition.

(i) $2^n \geq 100$
It is not a proposition.

2. What is the negation of each of these propositions
(a) Flowers are beautiful
(b) There is no pollution in New Jersey.
(c) $2+1=3$
(d) The summer in Maine is hot and sunny.

(a) It is not the case that flowers are beautiful
(b) It is not the case that there is no pollution in New Jersey
(c) $2+1 \neq 3$
(d) It is not the case that the summer in Maine is hot and sunny.

3. Let p and q be the propositions
p: I bought a lottery ticket this week.
q: I won the million dollar jackpot on Friday
Express each of this propositions as an english sentence
(a) $\neg p$
(b) $p \wedge q$
(c) $p \vee q$

(a) I bought a lottery ticket this week and did not win the million dollar jackpot on Friday

(b) I bought a lottery ticket this week and won the million dollar jackpot on Friday.

(a) I did not buy a lottery ticket this week.

(c) I bought a lottery ticket this week or I won the million dollar jackpot on Friday

17/07/2019
Wednesday

Conditional Statement

Let p and q be propositions. The conditional statement $p \to q$ (p implies q) is the proposition "if p, then q". The conditional statement $p \to q$ is false when p is true and q is false, and true otherwise.
In the conditional statement $p \to q$, p is called the hypothesis (antecedent or premise) and q is called the conclusion (consequence).

A conditional statement is also called implication. The truth table for the conditional statement $p \to q$ is shown below

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

This conditional statement specifies in different forms

① "if p then q" , ② "p implies q"

③ "if p, q" , ④ "p only if q"

⑤ "p is sufficient for q" , ⑥ "a sufficient condition for q is p"

⑦ "q if p" , ⑧ "q whenever p"

⑨ "q when p" , ⑩ "q is necessary for p"

⑪ "a necessary condition for p is q" , ⑫ "q follows from p"

⑬ "q unless ~~not~~ ¬p",

eg:- p, "I am elected"

q, "I will lower taxes"

$p \to q$ "If I am elected, then I will lower taxes."

If the politician is elected, voters would expect this politician to lower taxes. Furthermore, if the politician is not elected, then the voters will not have any expectation that this person will lower taxes, although the person may have sufficient influence to cause those in power to lower taxes.

It is only when the politician is elected but does not lower taxes that voters can say that the politician has broken the campaign pledge. This last scenario corresponds to the case when p is true but q is false here

eg:- Let p be the statement "Maria learns discrete mathematics" and q be the statement "Maria will find a good job". p implies q is "Maria learns discrete mathematics ~~and~~ then she will find a good job."

There are many other ways to express this conditional statement in english. They are
"Maria will find a good job when she learns discrete mathematics."
"For Maria to get a good job, it is sufficient for her to learn discrete mathematics."
"Maria will find a good job unless she does not learn discrete mathematics."

eg:- p, "Today is Friday."
q, "2 + 3 = 5"

$p \to q$ "If today is Friday then 2 + 3 = 5."

is true for all days.

eg: p : "Today is Friday."
q : "$2+7=5$"

$p \to q$ " If today is Friday then $2+7=5$."

q is false for all days.

18/07/2019

Converse, Contrapositive and Inverse

The ~~pos~~ proposition $q \to p$ is called the converse of $p \to q$

The contrapositive of $p \to q$ is the proposition $\neg q \to \neg p$

The proposition $\neg p \to \neg q$ is called the inverse of $p \to q$

$p \to q$

Converse - $q \to p$

Contrapositive - $\neg q \to \neg p$

Inverse - $\neg p \to \neg q$

same value

same value

All these 3 conditional statements formed from $p \to q$, only the contrapositive always has the same truth value as $p \to q$.

The contrapositive is false only when $\neg p$ is false and $\neg q$ is true i.e. only when p is true and q is false.

It shows that neither the converse, $q \to p$, nor the inverse $\neg p \to \neg q$ has the same truth value as $p \to q$ for all possible truth values of p and q.

Note that when p is true and q is false, the original conditional statement is false but the converse and the inverse are both true.

When two compound propositions always have the same truth value, we call them equivalent so that a conditional statement and its contrapositive are equivalent.

The converse and inverse of a conditional statement are also equivalent, as the reader can verify, but neither is equivalent to the original conditional statement.

eg:- What are the contrapositive, converse and Inverse of the conditional statement "The hometeam wins whenever it is

raining."

sol. Because "q whenever p" is one of the ways to express the conditional statement $p \to q$, the original statement can be written as, "If it is raining, then the hometeam wins."

The contrapositive of this conditional statement is "If the hometeam does not win, then it is not raining."
The converse is "If the hometeam wins, then it is raining.".
The inverse is "If it is not raining, then the hometeam does not win.".

Biconditionals

This is the way to combine propositions that expresses that two propositions have the same truth value.

Definition: Let p and q be propositions. The biconditional statement $p \leftrightarrow q$ is the proposition "p if and only if q". The biconditional statement $p \leftrightarrow q$ is true when p and q have the same truth values, and is false otherwise. Biconditional statements are also called bi-implications

Truth table

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Note that the statement $p \leftrightarrow q$ is true when both the conditional statements ~~$p \to q$ and~~ $p \to q$ and $q \to p$ are true and is false otherwise

ie why we use the words "if and only if" to express this logical connective and why it is symbollically written by combining the symbols $\to$ and $\leftarrow$. There are some other common ways to express $p \to q$:
"p is necessary and sufficient for q"
"If p then q, and conversely"

"If p iff q"

Note that $p \leftrightarrow q$ has exactly the same truth values as $(p \to q)$ and $(q \to p)$

$(p \to q) \wedge (q \to p) = p \leftrightarrow q$

eg:- Let p be the statement "You can take the flight." and q be the statement "You buy a ticket." then $p \leftrightarrow q$ is the statement, "You can take the flight

if and only if you buy a ticket."

Truth Table of compound Propositions

There are four important logical connectives - conjunctions, disjunctions, conditional statements and biconditional statements - as well as negations.

We can use these connectives to build up complicated compound propositions involving any number of propositional variables. ~~For~~ For this purpose we can use the appropriate truth tables.

The truth values of the compound proposition for each combination of truth values of the propositional variables in it is found in the final column of the table.

eg:- Construct the truth table of the compound proposition $(p \vee q) \rightarrow (p \wedge \neg q)$

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

eg.-

① $p \oplus (p \vee q)$

② $(q \rightarrow \neg p) \leftrightarrow (p \leftrightarrow q)$

③ $(p \leftrightarrow q) \oplus (\neg p \leftrightarrow \neg r)$

HW

① $p \oplus (p \vee q)$

p	q	$p \vee q$	$p \oplus (p \vee q)$
T	T	T	F
T	F	T	F
F	T	T	T
F	F	F	F

② $(q \rightarrow \neg p) \leftrightarrow (p \leftrightarrow q)$

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

feet = 30 cm
inch = 2.5 cm
feet = 12 inch

③ $(p \leftrightarrow q) \oplus (\neg p \leftrightarrow \neg r)$

p	q	r	$\neg p$	$\neg r$	$p \leftrightarrow q$	$\neg p \leftrightarrow \neg r$	$(p \leftrightarrow q) \oplus (\neg p \leftrightarrow \neg r)$
T	T	T	F	F	T	T	F
F	F	F	T	T	T	T	F
T	T	F	F	T	T	F	T
T	F	T	F	F	F	T	T
F	T	T	T	F	F	F	F
F	F	T	T	F	T	F	F
F	T	F	T	T	F	T	F
T	F	F	F	T	F	F	T

	precedence order
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Translating English Sentences

There are many reasons to translate english sentences into expressions involving propositional variables are logical connectives. In particular, english is often ambigious (confusing). Translating sentences into compound statement removes the ambiguity. Once we have translated sentence from English into logical expressions we can analyse these logical expressions to determine their truth value

23/07/2019 Tuesday

eg:- Convert the following English sentence to a logical expression:
" You can access the internet from campus only if you are a computer science major or you are not a freshmen."

Let a, "you can access the internet from campus"
c, "you are a computer science major."
f, "you are a freshmen."

$$a \rightarrow (c \vee \neg f)$$

eg:- "You cannot ~~write~~ ride the roller coaster if you are under 4 feet tall unless you are older than 16."

Let q, "You can ride the roller coaster."
r, " You are under 4 feet tall."
s, " You are older than 16."

$$(r \wedge \neg s) \rightarrow \neg q$$

Boolean searches

Logical connectives are used extensively in searches of large collections of information, such as indexes of webpages. Because these searches are employed techniques from propositional logic, they are called Boolean searches.

In Boolean searches, the connective AND is used to match records that contain both of two search terms the connective OR is used to match one or both of two search terms, and

the connective NOT (AND NOT) is used to exclude a particular search term.

Boolean searches are used to locate information of potential interest.

Web Page Searching

This technique usually give the help to find web page about particular subjects. The result of the search will include those pages that contain the data or information supplied by the user by a web browser. For example:- Computer AND Calculator searches only the same term existing in a particular websites. Instead of AND when we used OR both the terms including in all webpages independently can view by the user. AND NOT is an exception for "computer" or "calculator".

Logic and Bit Operations

Computers represent information using bits

A bit is a symbol with two possible values, namely 0 and 1. This meaning of the word bit comes from binary digit, because zeroes and ones are the digits used in binary representation of numbers. (John Tukey)

T - 1
F - 0

A bit can be used to represent a truth value because there are two truth values namely true and false. ~~One~~ bit to represent true and 0 bit to represent false.

A variable is called a boolean variable if its value is either true or false.

Definition:-
A bit string is a sequence of 0 or more bits. The length of this string is the number of bits in the string.

Table for the bit operators OR, AND, and x vy

x	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
1	0	1	0	1
0	1	1	0	1
1	1	1	1	0

eg:-

```
  1100111
  1001011
  ------
  1000011 ∧
  1101111 ∨
  0101100 ⊕
```

Evaluate the following expressions

(a) $11000 \wedge (01011 \vee 11011)$

(b) $(01111 \wedge (10101) \vee 01000$

(c) $(11011 \vee 01010) \wedge (10001 \wedge 11011)$

(a)
$$\begin{array}{r} 01011 \\ \vee\ 11011 \\ \hline 11011 \\ \wedge\ 11000 \\ \hline 11000 \end{array}$$

(b)
$$\begin{array}{r} 01111 \\ \wedge\ 10101 \\ \hline 00101 \\ \vee\ 01000 \\ \hline 01101 \end{array}$$

(c)
$$\begin{array}{r} 11011 \\ \vee\ 01010 \\ \hline 11011 \end{array} \qquad \begin{array}{r} 10001 \\ \wedge\ 11011 \\ \hline 10001 \end{array}$$

$$\begin{array}{r} 11011 \\ \wedge\ 10001 \\ \hline 10001 \end{array}$$

27/07/2019
Wednesday

Unit - II

Sets

Sets are used to group objects together. Often the objects in a set have similar properties

for instance; all the students who are currently enrolled in a school make up a set.

Definition 1:
A set is an unordered collection of objects.

Definition 2:
The objects in a set are called the elements, or members, of the set. A set is said to contain its elements.

Definition 3:
There are several ways to describe a set. One way is ~~to the~~ list all the members of a set when this is possible. All members of the set are listed between braces ($\{\}$)

$a \in A$ to denote that 'a' is an element of the set 'A'. The notation $a \notin A$ or $a \notin A$ denotes that 'a' is not an element of ~~the~~ set 'A'.

Lower case letters are usually used to denote elements of sets.
e.g:- the set V of all vowels in the

English alphabet can be written as

$V = \{a, e, i, o, u\}$

eg:- the set O of odd positive integers less than 10 can be represented by

$O = \{1, 3, 5, 7, 9\}$

Although sets are usually used to group together elements with common properties, there is nothing that prevents a set from having seemingly unrelated elements

for instance; {10, Kumar, 5} is the set containing 3 elements.

Sometimes the brace notation is used to describe a set without listing all its numbers. In this case ellipses (.....) are used when the general pattern of the elements is ~~obvious~~ obvious

eg:- the set of positive integers less than 100 can be denoted by $\{1, 2, 3, 4, \ldots 99\}$

5/09/2019
Thursday

Set Builder Notation

Another way to describe a set is to use set builder notation. It characterises all those elements in the set by stating the property or properties they must have to be members

For instance, the set O of all odd positive integers less than 10 can be written as

$O = \{x \mid x$ is an odd positive integer less than $10\}$

or specifying the universe as the set of positive integers, as

$O = \{x \in Z^+ \mid x$ is odd and $x < 10\}$

The set Q^+ of all positive ~~integers~~ rational numbers can be written as

$Q^+ = \{x \in R \mid x = p/q$, for some positive integers s, p and q$\}$

$Q = \{p/q \mid p \in Z, q \in Z$, and $q \neq 0\}$ the set of rational numbers

Sets can have other sets as members for eg:- the set $\{N, Z, Q, R\}$ is a set containing four elements, each of which is a set

∴ Using set, in computer, data types can generate.

Type is the name of a set together with a set of operations that can be performed on subsets from that set.

for eg:- Boolean is the name of the set $\{0, 1\}$ together with operators on one or more elements of this set, such as AND, OR and NOT

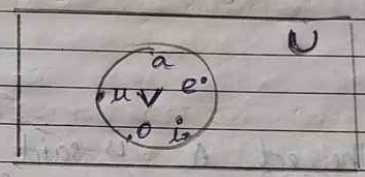
01/09/2019 (set)
Thursday Definition 3: Two sets are equal if and only if they have the same elements. That is if A and B are sets. then A and B are equal if and only if $\forall x\,(x \in A \leftrightarrow x \in B)$. We write $A = B$ if A and B are equal sets.

eg:- The sets $\{1, 3, 5\}$ and $\{3, 5, 1\}$ are equal, because they have the same elements. The order of elements of a set are listed does not matter. It does not matter if an element of a set is listed more than once, so $\{1, 3, 3, 3, 5, 5\}$ is the same as $\{1, 3, 5\}$.

Venn Diagram

Sets can be represented graphically using Venn diagrams, in this diagram the universal set U, which contains all the objects under consideration, is represented by a rectangle. Inside this rectangle, circles or other geometrical figures are used to represent sets. Sometimes points are used to represent a particular elements of the set.

Venn Diagrams are often used to indicate the relationships between sets. The ~~flowing~~ following venn Diagram shows 26 letters of the english alphabet as universal set and the vowels from this as a set



Null set

There is a special set that has no elements. This set is called the empty set or null set and is denoted by '$\emptyset$'.

The empty set can also be denoted by $\{\}$. (ie, we represent the empty set with a pair of braces that encloses all the elements in this set

for eg:- the set of all positive integers that

are greater than their squares is the null set.

A set with 1 element is called a single ton set. The empty set ϕ with the set $\{\phi\}$, which is a single ton set

Another equaluation is that an empty folder and the set consisting of just the empty set can be thought of as a folder with exactly one folder inside, namely the empty folder

02/08/2019
Friday

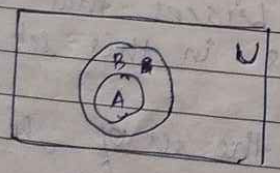
Subset

Definition: The set A is said to be a subset of B if and only if every element of A is also an element of B. We use the notation $A \subseteq B$ to indicate that A is a subset of the set B.

Subset

$A \subseteq B \leftrightarrow$ the quantification $\forall x (x \in A \rightarrow x \in B)$ is true.

The following venn diagram showing that A is a subset of B.



eg:- The set of all odd positive integers less than 10 is a subset of the set of all positive integers less than 10.

eg:- The set of rational numbers is a subset of the real numbers, and the set of all computer science majors in a college is a subset of the set of all students in that college.

Theorem: It shows that every non empty set S is guaranteed to have at least two subsets, the empty set and the set S itself.

ie. $\phi \subseteq S$ and $S \subseteq S$

Let S be a set. To show that ϕ (null) is the subset of S it shows that $\forall x (x \in \phi \rightarrow x \in S)$ is true. Because the empty set contains no elements, it follows that x is the element of null is always false.

It follows that the conditional statement $x \in \phi \rightarrow x \in S$ is always true, because it's hypothesis is always false and a conditional statement with a false hypothesis is true

Proper subset

A set A is the subset of the set B but that $A \neq B$. we write $A \subset B$ and we say that 'A is a proper subset of B'.

For $A \subset B$ to be true, it must be the case that $A \subseteq B$ and ~~there~~ there must exist an element x of B that is not an element of A.

06/08/2019 Tuesday

Cardinality of set

Sets are used extensively in counting problems and for such applications need to identify the size of sets.

Definition: Let 'S' be a set. If there are exactly 'n' distinct elements in 'S' where n is a non negative integer, we say that S is a finite set and n is the cardinality of S.

The cardinality of S is denoted by $|S|$

eg: ① Let A be the set of odd positive integer less than 10.
then $|A| = 5$

② Let S be the set of letters in the english alphabet, then $|S| = 26$

③ Because the null set has no elements, it follows that $|\phi| = 0$

Power set

Many problems involve testing all combinations of elements of a set to see if they satisfy some property. To consider all such combinations of elements of a set S, it build a new set that has ~~all~~ as it's number all the subsets of S.

Definition: Given a set S, the powerset of S is the set of all subsets of the set S. The power set of S is denoted by P(S)

eg:- what is the power set of the set $\{0, 1, 2\}$?
$P(S) = \{\{\}, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$

Note that the empty set and the set itself are members of this set of subsets.

$P(\{\phi\}) = \{\phi, \{\phi\}\}$

If a set has n elements then it's power set has 2^n elements.

Cartesian Products

The order of elements in a collection is often important because sets are unordered, a different structure is needed to represent ordered collections. This is provided by ordered n-tuples.

Definition :-

1. The order n-tuple $(a_1, a_2 \ldots a_n)$ is the ordered collection that has a_1 as its first element, a_2 as the second element ... and a_n as its ends element.

~~Two~~ ~~definition~~ ~~The ordered n-tuple~~ $(a_1$

* Two ordered n-tuples are equal if and only if each corresponding pair of their elements is equal.

In other words $(a_1, a_2, \ldots a_n) = (b_1, b_2 \ldots b_n)$ if and only if $a_i = b_i$ for $i = 1, 2, 3 \ldots n$. In particular, two types are called ordered pairs. 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 $a = b$

2. Let A and B be sets. The cartesian product of A and B, denoted by $A \times B$ is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$, hence $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$

eg: 1

Let A represent the set of all students in a university, and let B represent the set of all courses offered ~~by~~ at the university. What is $A \times B$? The $A \times B$ consists of all the ordered pairs of the form (a, b), where a is a student at the university. A set $A \times B$ can be used to represent all possible enrollments of students in courses at the university

eg: 2

what is the cartesian product of $A = \{1, 2\}$ and $B = \{a, b, c\}$?

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

The cartesian products $A \times B$ and $B \times A$ are not equal, unless $A = \phi$ or $B = \phi$

A subset R of the cartesian product $A \times B$ is called a relation from the set A to the set B. The elements of R are ordered pairs, where the first element belongs to A and the second to B. For example $R = \{(1, b)\ (2, a)\ (2, b)\}$

eg 3:

The cartesian product of the sets $A_1, A_2 \cdots A_n$ denoted by $A_1 \times A_2 \times \cdots \times A_n$, is the set of ordered $n^{\underline{-}}$ tuples $(a_1, a_2 \cdots a_n)$, where a_i belongs to A_i for $i = 1, 2, 3 \cdots n$. In other words $A_1 \times A_2 \times \cdots A_n = \{(a_1, a_2 \cdots a_n) \mid a_i \in A_i \text{ for } i = 1, 2 \ldots n\}$

eg:- What is the cartesian product $A \times B \times C$, where $A = \{0, 1\}$, $B = \{1, 2\}$ $C = \{0, 1, 2\}$

$A \times B \times C = \{(0, 1, 0), (0, 2, 1), (0, 2), (0, 2), (1, 1, 0) (1, 2, 1)$

20/08/2018
Tuesday Exercise

Ques 1 List the members of these sets

(a) $\{x \mid x$ is a real number such that $x^2 = 1\}$

$\{1, -1\}$

(b) $\{x \mid x$ is the square of an integer and $x < 100\}$

$\{0, 1, 4, 9, 16, 25, 36, 49, 64, 81\}$

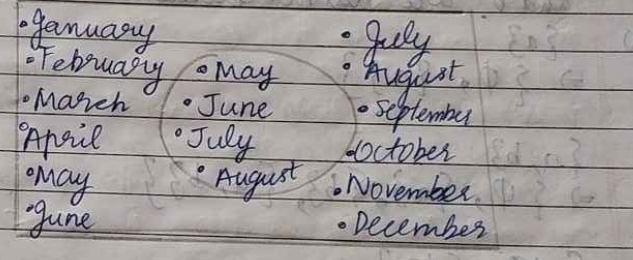
(c) $\{x \mid x$ is an integer such that $x^2 = 2\}$

$\{\phi\}$ or $\{\}$

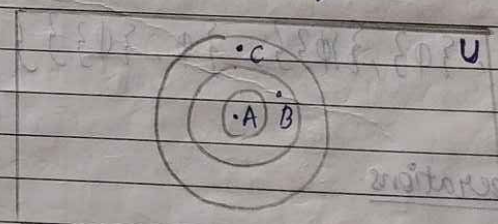
Ques 2 Suppose that $A = \{2, 4, 6\}$, $B = \{2, 6\}$ $C = \{4, 6\}$ and $D = \{4, 6, 8\}$. Determine which of these sets are subsets of which other of these sets.

- $B \subseteq A$
- $C \subseteq A$
- $C \subseteq D$

Ques 3(a) Using Venn Diagram ~~to~~ illustrate the set of all months of the year whose names donot contain the letter 'R' in the set of all months of the year.



(b) Using Venn Diagram illustrate the relationship (A is the proper subset of B) $A \subset B$ and $B \subset C$



Ques4 What is the cardinality of the following sets?

(a) $\{a\}$
$\Rightarrow 1$

(b) $\{\{a\}\}$
$\Rightarrow 1$

(c) $\{a, \{a\}\}$
$\Rightarrow 2$

(d) $\{a, \{a\}, \{a, \{a\}\}\}$

$\Rightarrow 3$

Ques 5 Find the power set of each of the sets, where a and b are distinct elements.

(a) $\{a\}$
$\Rightarrow \{\phi, \{a\}\}$

(b) $\{a, b\}$
$\Rightarrow \{\phi, \{a\}, \{b\}, \{a, b\}\}$

(c) $\{\phi\}, \{\phi\}\}$

$\Rightarrow$ ~~$\{\phi, \{\phi\}\}, \{\phi, \{\phi\}\}\}$~~

$\Rightarrow \{\phi, \{\phi\}, \{\{\phi\}\}, \{\phi, \{\phi\}\}\}$

Set Operations

Two sets can be combined in many different ways. For instance, starting with the set of mathematics majors in a product and the set of computer science majors, it can form the set of students who are maths majors or computer science majors, the set of students who are joint majors in maths and computer science, the set of all students not majoring in maths, and so on.

Union

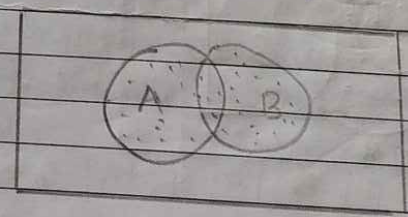
Definition :- Let A and B be sets. The union of the sets ~~A and~~ ~~con~~ A and B denoted by $A \cup B$ (A union B), is the set that contains those elements that are either in A or in B, or in both.

An element x belongs to the union of the sets A and B if and only if x belongs to A or x belongs to B. This tells that

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

27/08/2015 Thursday

The Venn Diagram shows the union of two sets A and B. The area that represents $A \cup B$ is the dotted area within either the circle representing A or the circle representing B



eg: The union of the sets $\{1, 3, 5\}$ and $\{1, 2, 3\}$ is the set $\{1, 2, 3, 5\}$

eg The union of the set of all computer science majors in a college and the set of all maths majors is the set of students who are major in either in mathematics or in computer science. (or in both)

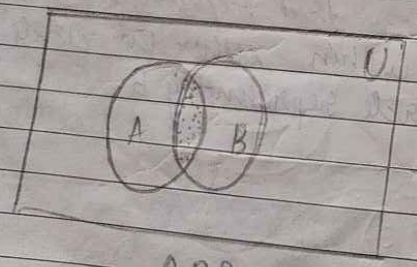
Intersection

Definition :- Let A and B be sets. The intersection of A and the intersection of set B denoted by $A \cap B$, is the set containing those elements in both A and B.

An element $x \in$ to the interection of the sets A and B if and only if $x \in A$ and $x \in B$
This tells that

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

The venn diagram is shown below



$A \cap B$

eg $A = \{1, 2, 3, 4, 5\}$; $B = \{2, 4, 7\}$

$A \cap B = \{2, 4\}$

Disjoint

Two sets are called disjoint if their intersection is the empty set

$A = \{1, 3, 7\}$ $B = \{2, 8, 9\}$

$A \cap B = \phi$

Here A and B are disjoint

Cardinality of union

To find the cardinality of a union of two finite sets A and B, note that ~~cardin~~ ~~the~~ $|A| + |B|$ counts each element that is in A but not in B or in B but not in A exactly once and each element that is in both A and B exactly twice.
Thus, if the number of elements that are in both A and B is subtracted from ~~cardin~~ $|A| + |B|$, elements in $A \cap B$ will be counted only once. Hence, ~~cardinality of~~ A

$$|A \cup B| = |A| + |B| - |A \cap B|$$

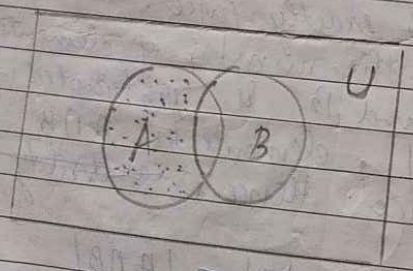
The generalization of this result to unions of an ~~arbitrary~~ arbitrary number of sets is called the principle of inclusion-exclusion. This is an important technique used in enumeration

Difference

Definition:- Let A and B be sets. The difference of A and B is denoted by $A - B$ ~~and~~ is the set ~~con~~ containing those elements that are in A but not in B. The difference of A and B is also called the complement of ~~the~~ B with respect to A.

An element ~~x~~ belongs to the difference of A and B if and only if x is ~~t~~ $x \in A$ and $x \notin B$. This tells that

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



eg:- $A = \{1, 3, 5, 7\}$ $B = \{1, 2\}$ from table 1

$U(A \cap C)$

$A - B = \{3, 7\}$

eg $A = \{1, 3, 5, 7\}$ $B = \{8, 9, 10\}$

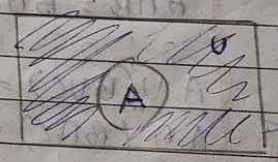
$A - B = \{1, 3, 5, 7\}$

Complement of a Set

Once the universal set U has been specified the compliment of a set can be defined

definition: Let U be the universal set. The compliment of set A, denoted by $\bar{A}$ or A', is the compliment of A with respect to universal set U. In other words, the compliment of set A is universal set ~~A~~ ie $U - A$

An element belongs to A' iff $x \notin A$, this tells that $A = \{x \mid x \in A\}$. The following fig. shows $\bar{A}$



$\bar{A}$

eg. Let $A = \{a, e, i, o, u\}$ where the universal set is the set of letters of the english alphabet, then:

$\bar{A} = \{b, c, d, f, g, h, j, k, l, m, n, p, q$

$\{8, t, v, w, x, y, z\}$

eg: Let A be the set of positive integers greater than 10. Then
$\bar{A} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Set Identities

Identity	Name
$A \cup \phi = A$ $A \cap U = A$	Identity Laws
$A \cup U = U$ $A \cap \phi = \phi$	Domination Laws
$A \cup A = A$ $A \cap A = A$	Idempotential law
$(\bar{A})^{-} = A$	Complementation Law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative Law
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative Laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive Laws
$\overline{A \cup B} = \bar{A} \cap \bar{B}$ $\overline{A \cap B} = \bar{A} \cup \bar{B}$	De - Morgan's Law

Complimentary Laws: $A \cup \bar{A} = U$, $A \cap \bar{A} = \phi$

Absorption Laws: $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$

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

27/08/2019
Tuesday

Prove the first distributive law from table 1, which states that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

It will prove this identity by showing that each side is a subset of the other side.
⇒ Suppose that ~~x is th~~ $x \in A \cap (B \cup C)$. Then ~~x is the or~~ $x \in A$ and $x \in (B \cup C)$.

By the definition of union, it follows that $x \in A$ and $x \in B$ or $x \in C$ (or both)

Consequently, it knows that $x \in A$ and $x \in B$ or that $x \in A$ and $x \in C$
By the definition of intersection, it follows that $x \in A \cap B$ or $x \in A \cap C$. Using the definition of union, it concludes that $x \in (A \cap B) \cup (A \cap C)$. It also concludes that $A \cap (B \cup C)$ ~~is th~~ $\subseteq (A \cap B) \cup (A \cap C)$

Now suppose that $x \in (A \cap B) \cup (A \cap C)$. Then by the definition of union $x \in (A \cap B)$ or $x \in (A \cap C)$. By the definition of intersection, it follows that $x \in A$ and $x \in B$ or that $x \in A$ and $x \in C$. From this we see that $x \in A$ and $x \in B$ or $x \in C$

Consequently, by the definition of union we see that $x \in A$ and $x \in (B \cup C)$. Furthermore, by the definition of intersection it follows that $x \in A \cap (B \cup C)$
We conclude that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$
This completes the proof of the identity.

Using Membership Tables

Set identities can also be proved using membership tables. It considers each combination of sets that an element can belong to and verify that elements in the same combination of sets belongs to both the sets in the identity.

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

Ques Use a membership table to show that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

A	B	C	$B \cup C$	$A \cap B$	$A \cap C$	$A \cap (B \cup C)$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	1	0	1	1
1	0	0	0	0	0	0	0
1	0	1	1	0	1	1	1
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Ques Let A, B and C be sets. Show that $\overline{A \cup (B \cap C)} = (\bar{C} \cup \bar{B}) \cap \bar{A}$

$\overline{A \cup B} = \bar{A} \cap \bar{B}$

$\overline{A \cap B} = \bar{A} \cup \bar{B}$

$\overline{A \cup (B \cap C)} = (\bar{C} \cup \bar{B}) \cap \bar{A}$

LHS $= \overline{A \cup (B \cap C)}$

$= \bar{A} \cap \overline{B \cap C}$ — first demorgan's law

$= \bar{A} \cap (\bar{B} \cup \bar{C})$ — second demorgan's law

$= (\bar{B} \cup \bar{C}) \cap \bar{A}$ — second commutative law

$= (\bar{C} \cup \bar{B}) \cap \bar{A}$ — first commutative law

LHS = RHS

30/08/2019 Friday

Computer Representation of Sets

There are various ways to represent sets using a computer.

One method is to store the elements of the set in an unordered fashion. We will represent a method for storing elements using an arbitrary ordering of the elements of the universal set.

Assume that the Universal set, U is finite (and of reasonable size so that the number of elements of U is not larger than the memory size of the computer being used). First, specify an arbitrary ordering of the elements of ~~this~~ U, for instance

$a_1, a_2 \ldots a_n$ represent a subset A of U with the bitstring of length n, where the ith bit in this string is 1. If a_i belongs to A and is 0, if a_i does not belong to A
(if $a_i \in A$ and is zero if $a_i \notin A$)

eg:- Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and the ordering of elements of U has the elements in increasing order; if $a_i = i$. What bitstrings represent the subset of all odd integers in U, the subset of all even integers in U and the subset of integers not exceeding 5 in U.

Soln: The bit string that represents the set of odd integers in U, namely $\{1, 3, 5, 7, 9\}$, has a 1 bit in the first, 3rd, 5th, 7th, 9th positions, and a 0 ~~in the~~ elsewhere.

It is 1010101010, similarly it represents the subsets of all even integers ie $\{2, 4, 6, 8, 10\}$ by the string 0101010101

The set of all integers in U that donot exceed 5 $\{1, 2, 3, 4, 5\}$ by the string 1111100000.

Using bitstrings to represent sets, to find complements of sets and union, intersections and differences of sets.

To find the complement of a string simply change each 1 to 0 and each 0 to 1, because $x \in A$ iff $x \notin A$.
Here 1 represents true, and 0 represents false.

04/09/2019 Wednesday

eg:- We have seen that the bit string for the set $\{1, 3, 5, 7, 9\}$ from the universal set $\{1, 2, 3, \ldots 10\}$ is 1010101010

What is the bit string for the complement of the set? 0101010101 is the bit string complement, which represents to the set $\{2, 4, 6, 8, 10\}$

eg:- The bit strings for the set $\{1, 2, 3, 4, 5\}$ and $\{1, 3, 5, 7, 9\}$ are 1111100000 and 1010101010 respectively

Use bit strings to find the union and the intersection of these sets. For this purpose the bitwise OR is used for union and bitwise AND is used for intersection

The bit string for the union of these sets is

$$\begin{array}{r} 1111100000 \\ 1010101010 \\ \hline 1111101010 \end{array} \quad \text{(union)}$$

Union = $\{1, 2, 3, 4, 5, 7, 9\}$

the intersection of these sets

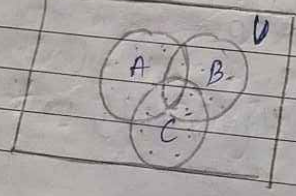
$$\begin{array}{r} 1111100000 \\ 1010101010 \\ \hline 1010100000 \end{array} \wedge \quad \text{(intersection)}$$

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

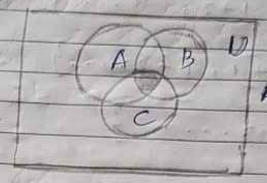
Generalised Unions and Intersections

Because unions and intersection of sets satisfy associative laws, the sets $A \cup B \cup C$ ~~set~~ and $A \cap B \cap C$ are well defined; ~~that~~ ie. the meaning of this notation is unambiguous (not confusing) when A, B and C are sets. ie. We donot have to use parantheses ({}) to indicate which operation comes first because $A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$.

Note that $A \cup B \cup C$ contains those elements that are in atleast one of the sets A, B and C and that $A \cap B \cap C$ contains those elements that are in all of A, B and C. These combinations of 3 sets, A, B and C are shown below.



$A \cup B \cup C$



$A \cap B \cap C$

Example : set $A = \{0, 2, 4, 6, 8\}$
$B = \{0, 1, 2, 3, 4\}$ and $C = \{0, 3, 6, 9\}$
what are $A \cup B \cup C$ and $A \cap B \cap C$

$A \cup B \cup C = \{0, 1, 2, 3, 4, 6, 8, 9\}$

$A \cap B \cap C = \{0\}$

It can also consider unions and intersections of an arbitrary number of sets. Its definition is <u>Union</u>: The union of a collection of sets is the set that contains those elements that are members atleast one set in the collection. It uses the notation $A_1 \cup A_2 \cup A_3 \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$, to denote the union of the sets $A_1, A_2, A_3 \cdots A_n$

<u>Intersection</u>: The intersection of a collection of sets is the set that contains those elements that are members of all the sets in the collection. It uses the notation $A_1 \cap A_2 \cap A_3 \cdots A_n = \bigcap^{n} A_i$ to denote the intersection of the sets $A_1, A_2 \cdots A_n$

eg:- Let $A_i = \{i, i+1, i+2, \ldots\}$ Then

$$\bigcup_{i=1}^{n} A_i = \bigcup_{1}^{n} \{i, i+1, i+2 \ldots\}$$
$$= \{1, 2, 3 \ldots\}$$

$$\bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n} \{i, i+1, i+2 \ldots\}$$
$$= \{n, n+1, n+2 \ldots\}$$

Using other families of sets

It can extend the notation we have introduced for unions and intersection to other families of sets.
In particular, you can use the notation $A_1 \cup A_2 \cup \ldots \cup A_n \ldots \infty = \bigcup_{i=1}^{\infty} A_i$ to denote the union of the sets $A_1, A_2, A_3 \ldots A_n, \ldots$ Simularly the intersection of these sets can be denoted by $A_1 \cap A_2 \cap A_3 \cap \ldots A_n \cap \ldots \cap \infty = \bigcap_{i=1}^{\infty} A_i$

More generally the notation $\bigcap_{i \in I} A_i$ and $\bigcup_{i \in I} A_i$ are used to denote the intersection and union of the sets A_i for $i \in I$ respectively. Note that we have $\bigcap_{i \in I} A_i = \{x \mid \forall i \in I\ (x \in A_i)\}$ and $\bigcup_{i \in I} A_i = \{x \mid \exists i \in I\ (x \in A_i)\}$

$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I\ (x \in A_i)\}$$

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I\ (x \in A_i)\}$$

eg:- Suppose that $A_i = \{1, 2, 3, \ldots i\}$ for $i = 1, 2, 3$, dots then $\bigcup_{i=1}^{\infty} A_i = \bigcup_{i=1}^{\infty} \{1, 2, 3 \ldots i\}$

$$= \{1, 2, 3, \ldots\} = \mathbb{Z}^+$$

$A_1 = \{1\}$
$A_2 = \{1, 2\}$
$A_3 = \{1, 2, 3\}$

and $\bigcap_{i=1}^{\infty} A_i = \{1, 2, 3 \ldots i\} = \{1\}$

To see that the union of these sets is the set of positive integers, note that every positive integer is in atleast one of the sets, because the integer n belongs to $A_n = \{1, 2 \ldots n\}$ and every elements of the sets in the union is a positive integer. In the case of intersection, the only element that belongs to all the sets $A_1, A_2 \ldots$ is 1

Ques Find $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$ for every positive integer i

(a) $A_i = \{-i, -i+1, \ldots -1, 0, 1, \ldots i-1, i\}$

(b) $A_i = \{-i, i\}$

(c) $A_i = [-i, i]$ ie the set of real numbers x with $-1 \le x \le i$

(d) $A_i = [i, \infty]$ ie, the set of real no.s x with $x \geq 1$

∞)

(a) $\bigcap_{i=1}^{\infty} A_i = -1, 0, 1$

$\bigcup_{i=1}^{\infty} A_i = \{-n \ldots -3, -2, -1, 0, 1, 2, 3 \ldots n\}$

(B)

(a) $A_i \{-i, -i+1 \ldots -1, 0, 1 \ldots i, -1, i\}$

$\bigcup_{i=1}^{\infty} A_i = \{-\infty, \ldots -1, 0, +1, \ldots \infty\} = Z$

$\bigcap_{i=1}^{\infty} A_i = \{-1, 0, 1\}$

(b) $A_i = \{-i, -i\}$

$\bigcup_{i=1}^{\infty} A_i = \{-n \ldots -3, -2, -1, 1, 2, 3 \ldots n\}$

$= Z - \{0\}$

$\bigcap_{i=1}^{\infty} A_i = \phi$

(c) $A_i = [-i, i]$

given that, $-i \leq x \leq i$ (where x is real no.)

$\bigcup_{i=1}^{\infty} A_i = \{-\infty, \infty\} = R$ (all real no s)

$\bigcap_{i=1}^{\infty} A_i = [-1, 1]$

(d) $A_i = \cancel{\{-i, -i+1}\ [i, \infty)$

given that $x \geq 1$ (where x is a real no)

$\bigcup_{i=1}^{\infty} A_i = [1, \infty)$

$\bigcap_{i=1}^{\infty} A_i = \phi$

17/09/2019
Tuesday

functions

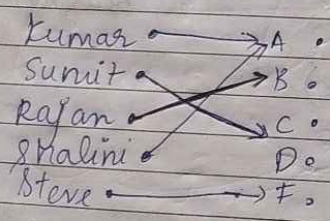
In many instances we assign to each element of a set, a particular element of a second set. (which may be the same as the first).

example

for eg:- Suppose that each student in a class is assigned a letter grade from the set $\{A, B, C, D, F\}$

Suppose that the grades are
A for Kumar
C for Sunit
B for Rajan
A for Shalini
F for Steve

This assignment of grade is shown below



This assignment is an example of a function. This concept is extremely important in mathematics and computer science. for example, in discrete mathematics functions are used in the definition of such discrete structures as sequences and strings functions are also used to represent how long it takes a computer to solve problems of a given size

definition:- Let A and B be non-empty sets. A function f from A to B $(A \to B)$ is an assignment of exactly one element of B to each element of A. we write $f(A) = b$ if b is the unique element of B assigned by the function f to the element a of A.

If f is a function from $A \to B$, we write $f : A \to B$

functions are sometimes are also called mapping or transformations

A function $f : A \to B$ can also be defined in terms of a relation from $A \to B$

A relation from $A \to B$ is just a subset of $A \times B$. A relation from $A \to B$ that contains 1 and only 1 ordered pair (a, b) for every element $a \in A$, defines a function f from $A \to B$. This function is defined by the assignment $f(a) = b$, where

(a, b) is the unique ordered pair in the relation that has 'a' as its first element.

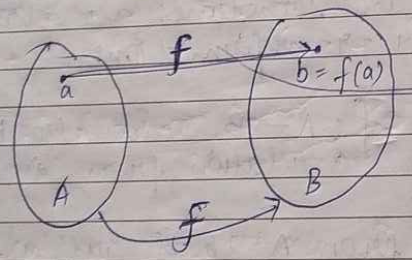
Definition 2 :-

If f is a function from $A \to B$, we say that A is the domain of f and B is the co-domain of f.

If $f(a) = b$, we say that b is the image of a and a is the pre image of b.

The range of f is the set of all images of elements of A. Also, if f is a function from $A \to B$, we say that f maps $A \to B$.

The following figure represents a function from $A \to B$



eg:- What are the domain, co-domain and range of the function that assigns grades to students described ~~below~~ above.

Let G be the function that assigns a grade to a student in the class. Note that

$G(\text{Kumar}) = A$
$G(\text{Sunit}) = C$
$G(\text{Rajan}) = B$
$G(\text{Shalini}) = A$
$G(\text{Steve}) = F$

The domain of G is the set {Kumar, Sunit, Rajan, Shalini, Steve} and co-domain is the set {A, B, C, D, F}

The range of G is the set {A, B, C, F}. because each grade except D is assigned to some student

eg: 2 Let R be the relation consisting of ordered pairs (Abdul, 22), (Vrindha, 24) (Karlos, 21) (Reny, 22) (Edwin, 24) (Febin, 22) where each pair consist of a graduate student and age of the student. what is the function that this relation determines.

$f(\text{Abdul}) = 22$
$f(\text{Vrindha}) = 24$
$f(\text{Karlos}) = 21$
$f(\text{Reny}) = 22$
$f(\text{Edwin}) = 24$
$f(\text{Febin}) = 22$

considering last 2 bits
$f(110\underline{10}) = \underline{10}$

00 - 0
01 - 1
10 - 2
11 - 3

The range is the set {21, 22, 24}

19/09/2019
Thursday

The domain or co-domain of functions are often specified in programming language.

for instance; the Java statement

int floor (float real) { . . . }

(int: codomain; real: domain)

State that the domain of the floor function is the set of real numbers and its codomain is the set of integers.

Two real-valued functions with the same domain can be added and multiplied

definition:

Let f_1 and f_2 be function from $A \to R$. Then $f_1 + f_2$ and $f_1 \times f_2$ or $(f_1 f_2)$ are also functions from $A \to R$ defined by

$$\begin{cases} (f_1 + f_2)(x) = f_1(x) + f_2(x) \\ (f_1 f_2)(x) = f_1(x) \cdot f_2(x) \end{cases}$$

Note that the functions $f_1 + f_2$ and $f_1 f_2$ have been defined by specifying their values at x in terms of the values of f_1 and f_2 at x

eg:- Let f_1 and f_2 be functions from $R \to R$ such that $f_1(x) = x^2$ and $f_2(x) = x - x^2$

What are the functions $f_1 + f_2$ and $f_1 f_2$?

$$f_1 + f_2 = x^2 + x - x^2 = x$$

$$f_1 f_2 = x^2(x - x^2) = x^3 - x^4$$

⇒ One-to-~~and~~ one (Injective) and Onto functions (surjective)

Some functions never assign the same value to two different domain elements. This functions are said to be one-to-one

definition:-

A function f is said to be one-to-one, or injective, if and only if $f(a) = f(b)$ ⇒ $a = b$ ~~and~~ for all a and b in the domain of f.

The function is said to be an injection if it is one-to-one

Note that a function f is one-to one if and only if $f(a) \neq f(b)$ whenever $a \neq b$

This way of expressing that f is one to one is obtained by taking the contrapositive

$p \to q$

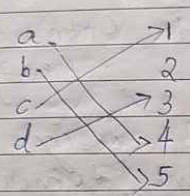
$\neg q \to \neg p$

$\neg q, \neg p$

of the implication in the definition.

23/09/2019
monday

eg:- Determine whether the function f from $\{a, b, c, d\}$ to $\{1, 2, 3, 4, 5\}$ with $f(a) = 4$ and $f(b) = 5$ ~~or~~ $f(c) = 1$ and $f(d) = 3$ is one-to-one.



It is a one-to-one function because f takes on different values at the four elements of its domain.

eg: Determine whether the function $f(x) = x^2$ from the set of integers to the set of integers is one to one.

This function is not one-to-one because for instance $f(1) = f(-1) = 1$, but $1 \neq -1$

note that this function with its domain restricted to Z^+ (only positive integers) is one to one

: Determine whether the function $f(x) = x+1$ from the set of real numbers to itself

is one-to one. to demonstrate this note that $(x+1) \neq (y+1)$ when $x \neq y$

The following definition gives some conditions that guarentees that a function is one-to-one.

definition:

A function f whose domain and co-domain are subsets of the set of real numbers is called increasing if $f(x) \leq f(y)$ and strictly increasing if $f(x) < f(y)$, whenever $x < y$ and x and y are in the domain of f.

similarly, f is called decreasing if $f(x) \geq f(y)$, and strictly decreasing if $f(x) > f(y)$

Onto functions

for some functions the range and the codomain are equal. ie, every member of the codomain is the image of some element of the domain. functions with property is called onto functions

definition

A function f from $A \to B$ is called onto or surjective if and only if for every element b is the element of B ($b \in B$) there is an element a is the element of A ($a \in A$) with $f(a) = b$

A function f is called a surjection if it is onto.

eg:- Let f be the function from $\{a, b, c, d\}$ to $\{1, 2, 3\}$ defined by $f(a) = 3$, $f(b) = 2$, $f(c) = 1$ and $f(d) = 3$. Is f an onto function?

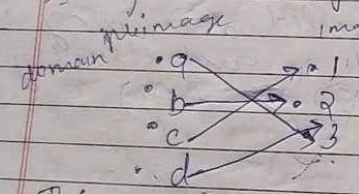
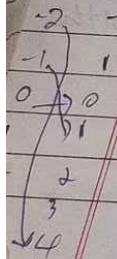


image always should have an element

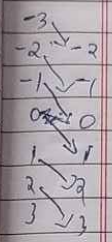
This is an onto function

eg Is the function $f(x) = x^2$ from the set of integers to the set of integers onto?



This is not onto because there is no integer x with $x^2 = -1$

eg: Is the function $f(x) = x + 1$ from the set of integers to the set of integers onto



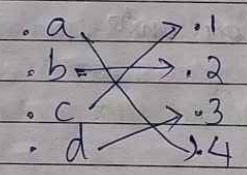
This is onto

Bijection

definition:

The function f is one-to-one correspondence, or a bijection if it is both one-to-one and onto.

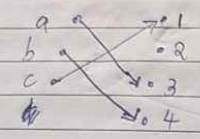
eg:- Let f be the function from $\{a, b, c, d\}$ to $\{1, 2, 3, 4\}$ with $f(a) = 4$, $f(b) = 2$, $f(c) = 1$ and $f(d) = 3$. Is f a bijection?



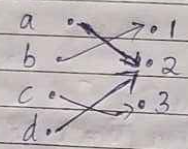
Yes it is a bijection.

24/09/2019
Tuesday The following figure displays different types of functions:-

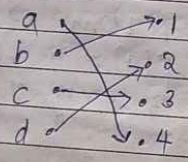
(a) One to one, not onto



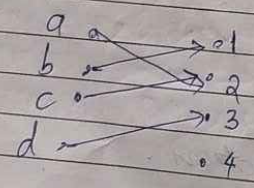
(b) onto, ~~but~~ not one-to-one



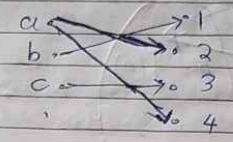
(c) ~~onto~~ one-to-one and onto



(d) Neither one to one nor onto



(e) Not a function



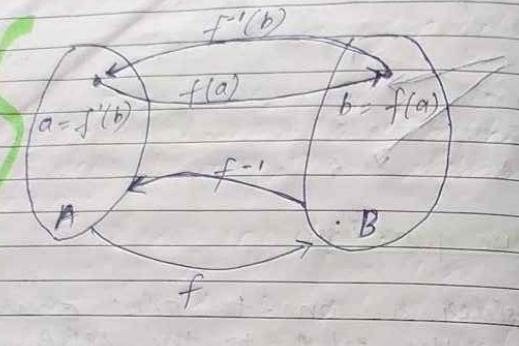
Inverse functions

Consider a one-to-one correspondence from the set A to the set B ($A \to B$). Because f is an onto function, every element of B is the image of some element in A.
Furthermore, because f is also a one-to-one function, every element of B is the image of a unique element of A.

definition:-

Let f be a one-to-one correspondence from the set A to the set B. The inverse function of f is the function that assigns to an element b belongs to B. The unique element a in A such that $f(a) = b$. The inverse function of f is denoted by f^{-1} ~~(b) = a~~. Hence inverse of $f^{-1}(b) = a$ when $f(a) = b$

The following figure illustrates the concept of an inverse function.



If a function f is not a one-to-one correspondence it cannot define an inverse function of f.

When f is not one-to-one correspondence, either it is not one-to-one or it is not onto.

If f is not one-to-one, some element b in the codomain is the image of more than one element in the domain. If f is not onto, for some element b in the codomain, no element A in the domain exists for which $f(a) = b$.

Consequently, if f is not a one-to-one correspondence, it cannot assign to each element b in the codomain a unique element a in the domain such that $f(a) = b$.

A one to one correspondence is called invertible because it can define an inverse of this function. A function is not invertible if it is not a one-to one correspondence because the inverse of such a function does not exist.

eg:- Let f be the function from $\{a, b, c\}$ to $\{1, 2, 3\}$ such that $f(a) = 2$, $f(b) = 3$, $f(c) = 1$. Is f invertible and if it is what is its inverse?

The function f is invertible because it is a one-to-one correspondence. The inverse function f^{-1} reverses the correspondence given by f so $f^{-1}(1) = c$, $f^{-1}(2) = a$ and $f^{-1}(3) = b$

eg: Let f ~~such that~~: $Z \to Z$ be such that ~~f(n)~~ $f(n) = n + 1$. Is f invertible? And if it is what is its inverse?

The function f has an inverse because it is a one-to-one correspondence. To reverse the correspondence, suppose that y is the image of x so that $y = x + 1$ then $x = y - 1$. This means that $y - 1$ is the unique element of Z that is sent to y by f.

Consequently $f^{-1}(y) = y - 1$

eg:- Let f be the function from $R \to R$ with $f(x) = x^2$. Is f invertible/invertible?

Because $f(-2) = f(2) = 4$, f is not one to one. If an inverse function were defined, it would have to assign two elements to 4.

Hence f^{-1} is not invertible.

25/09/2019
Wednesday

Composition of function

definition:

Let g be a function from the set A to the set B and let f be a function from the set B to the set C.

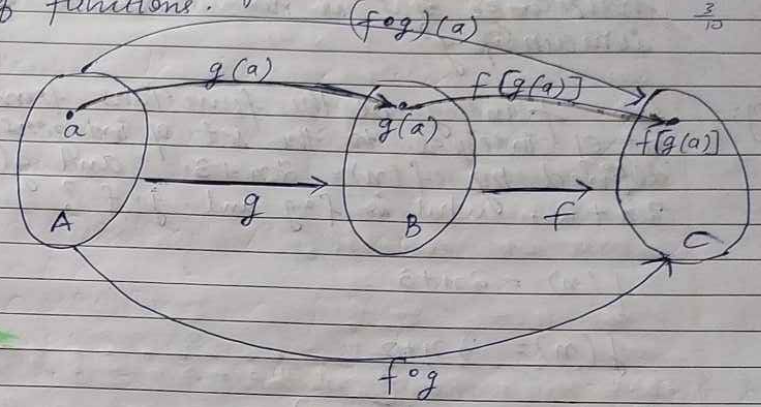
The composition of the functions f and g, denoted by $f \circ g$, is defined by

$$(f \circ g)(a) = f[g(a)]$$

Composition of f and g $(f \circ g)$ is the function that assigns to element a of A. The element assigned to $f \to g(a)$. That is to find $(f \circ g)(a)$ first applies the function ~~g to~~ $g \to a$ to obtain $g(a)$ and then it applies the function f to the result $g(a)$ to obtain ~~$f[g(a)]$~~ $(f \circ g)(a) = f[g(a)]$

Note that the composition $f \circ g$ cannot be defined unless g is a subset of the domain

The following figure shows the com of functions.



eg:- Let g be the function from the set $\{a, b, c\}$ to itself such that $g(a) = b$, $g(b) = c$ and $g(c) = a$.
Let f be the function from the set $\{a, b, c\}$ to the set $\{1, 2, 3\}$ such that $f(a) = 3$; $f(b) = 2$; $f(c) = 1$
~~Find~~ What is the composition of ~~f~~ f and g and what is the composition of g and f.

The composition $f \circ g$ is defined by

$(f \circ g)(a)$
$= f(g(a)) = f(b) = 2$

$(f \circ g)(b) = f(g(b)) = f(c) = 1$

$(f \circ g)(c) = f(g(c)) = f(a) = 3$

Note that $g \circ f$ is not defined, because the range of f is not a subset of the domain of g

eg:- Let f and g be the functions from the set of integers to the set of integers defined by $f(x) = 2x+3$ and $g(x) = 3x+2$. What is $f \circ g$ and $g \circ f$?

$f(x) = 2x+3$

$g(x) = 3x+2$

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

$= f(3x+2)$

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

$= 6x+7$

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

$= g(2x+3)$

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

$= 6x+9+2$

$= 6x+11$

27/09/2019
Friday

Graphs of Functions

We can associate a set of pairs in $A \times B$ to each function from $A \to B$. This set of pairs is called the graph of the function and is often displayed pictorally to aid in understanding the behaviour of the function.

Definition:

Let f be a function from the set A to the set B. The graph of the function f is the set of ordered pairs $\{(a, b) \mid a \in A \text{ and } f(a) = b\}$

From the definition the graph of a function f from $A \to B$ is the subset of $A \times B$ containing the ordered pairs with the second entry equal to the element of B assigned by f to the first entry.

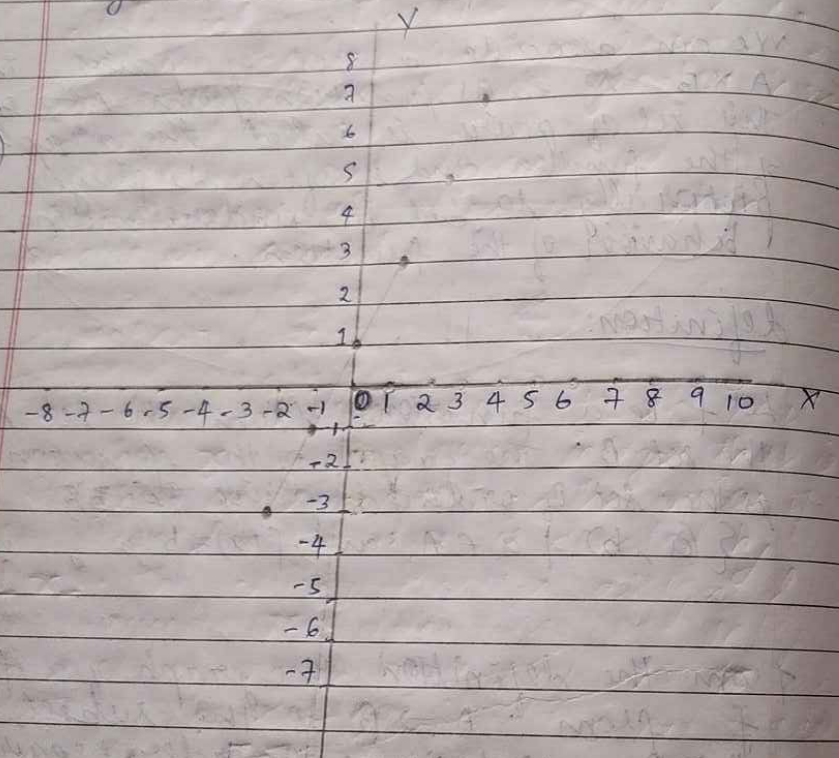
eg:1 Display the graph of the function $f(n) = 2n+1$ from the set of integers to the set of integers.

The graph of f is the set of ordered pairs of the form $(n, 2n+1)$ ~~from the~~ where n is an integer ⇒

x	-2	-1	0	1	2	3
y	-3	-1	1	3	5	7

$-2+1$

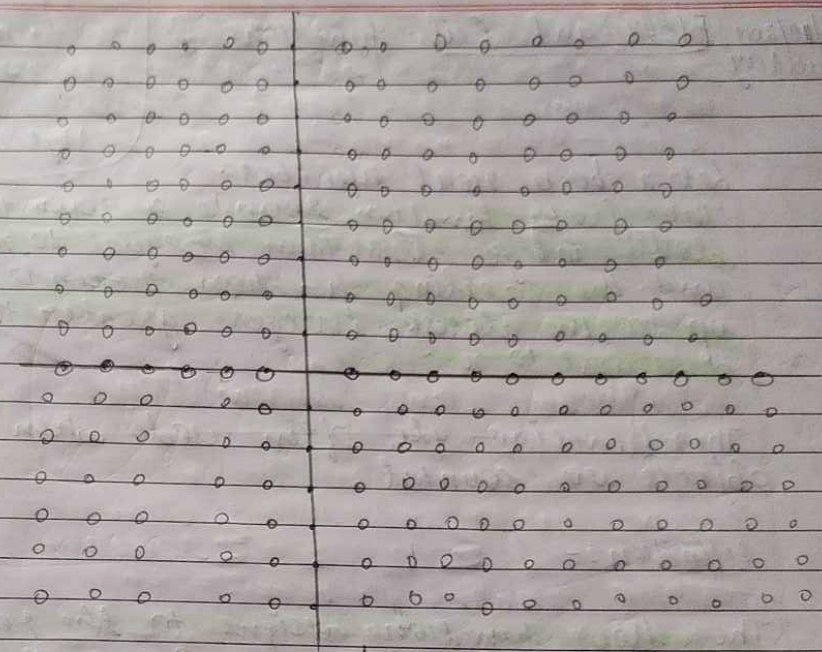
Ans①



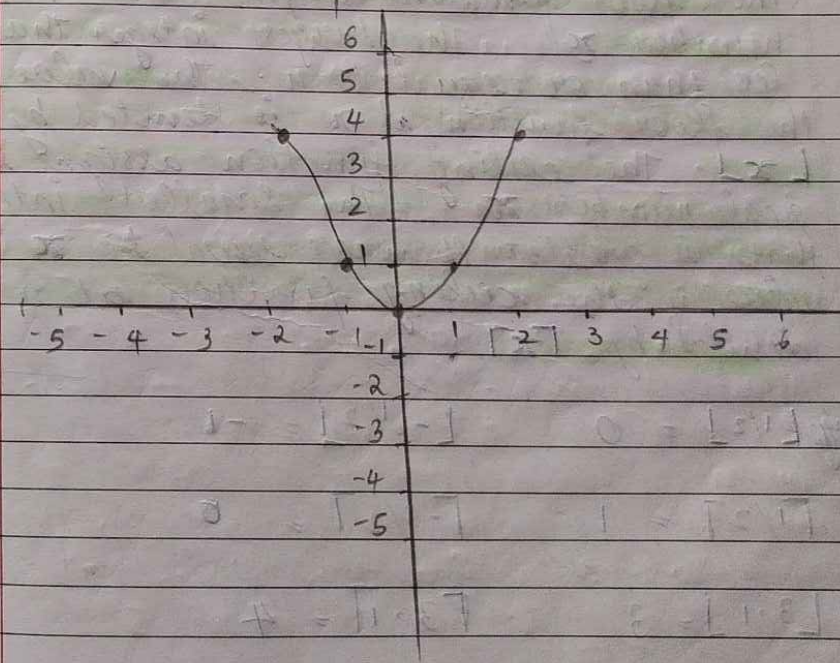
Ques 2 Draw the graph of the function $f(n) = n^2$ from the set of integers to the set of integers ⇒ (n, n^2)

x	-2	-1	0	1	2	3
y	4	1	0	1	4	9

Ans①



Ans②



01/00/2019 Tuesday

Floor and Ceil functions

1 Byte = 8 bit

Let x be a real number.
The floor function rounds x down to the closest integer less than or equal to x, and the ceiling function rounds x up to the closest integer greater than or equal to x.

These functions are often used when objects are counted

definition:-

The floor function assigns to the real number x the largest integer that is less than or equal to x. The value of the floor function at x is denoted by $\lfloor x \rfloor$. The ceiling function assigns to the real number x the smallest integer that is greater than or equal to x. The value of the ceiling function at x is denoted by $\lceil x \rceil$

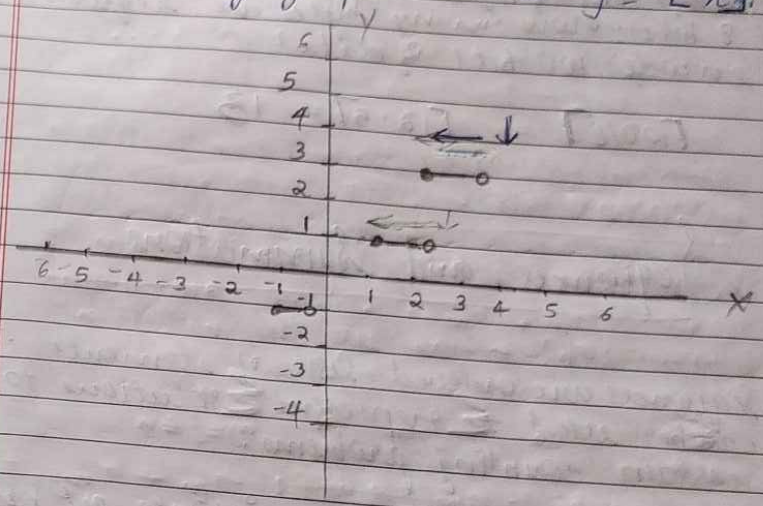
eg:- $\lfloor 1/2 \rfloor = 0$ $\quad \lfloor -1/2 \rfloor = -1$

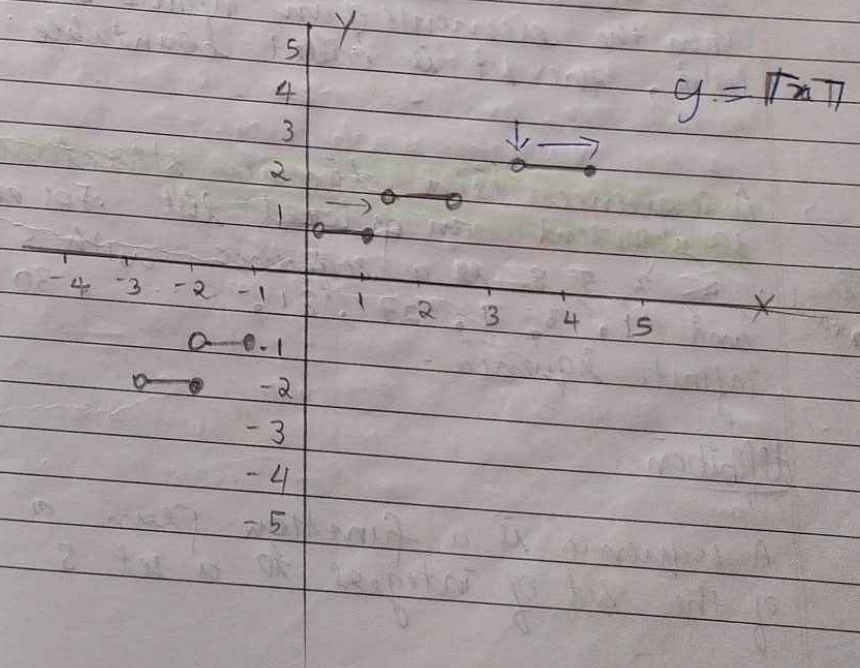
$\lceil 1/2 \rceil = 1$ $\quad \lceil -1/2 \rceil = 0$

$\lfloor 3.1 \rfloor = 3$ $\quad \lceil 3.1 \rceil = 4$

$\lceil 8 \rceil = 8$ $\quad \lfloor 8 \rfloor = 8$

The following graph shows $y = \lfloor x \rfloor$





Data stored on a computer disk or transmitted on a data network are usually represented as a string of bytes. Each byte is made up of 8 bits. How many bytes are required to encode 100 bits of data

$\lceil 100/8 \rceil = \lceil 12.5 \rceil = 13$

Sequences and Summations

Sequences are ordered lists of elements. They can be used to represent solutions to certain counting problems.

When the elements of an infinite set can be listed, the set is called countable.

→ A sequence is a discrete structure used to represent an ordered list. For example 1, 2, 3, 5, 8 is a sequence with 5 terms and 1, 3, 9, 27, 81, ..., 30 is an infinite sequence.

Fibonacci

Definition

A sequence is a function from a subset of the set of integers to a set S

We use the notation a_n to denote the image of the integer n. We call a_n a term of the sequence

eg:- Consider the sequence $\{a_n\}$ where $a_n = 1/n$

The list of the terms of this sequence, beginning with a_1, namely $a_1, a_2, a_3, a_4 \ldots$ starts with $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4} \ldots$

Ques find formulae for the sequences with the following first 5 terms

(a) 1, 1/2, 1/4, 1/8, 1/16, 1/32 ...

(b) 1, 3, 5, 7, 9

(c) 1, -1, 1, -1, 1, -1 ...

(a) $a_n = \frac{1}{2^n}$

(b) $a_n = 2n+1$

(c) $a_n = (-1)^n$

Ques How can we produce the terms of a sequence if the first 10 terms are 5, 11, 17, 23, 29, 35, 41, 47

$6n - 1 \qquad n = 1, 2, 3 \ldots$

$5n - 1$

03/10/2019
Thursday

Summations

The notation used to express the sum of the terms $a_m, a_{m+1}, \ldots a_n$ from the sequence $\{a_n\}$ - We use the notation

$$\sum_{j=m}^{n} a_j \quad \text{or} \quad \sum_{j=m}^{n} a_j \quad \text{or} \quad \sum_{m \le j \le n} a_j$$

to represent ~~a_m, a_{m+1}~~ $a_m + a_{m+1} + \ldots a_n$

Here, the variable j is called the index of summation, and the choice of the letter j as the variable is arbitrary, & we can use any other letter such as i or k

eg:- $\sum_{j=m}^{n} a_j = \sum_{i=m}^{n} a_i = \sum_{k=m}^{n} a_k$

Here the index of summation runs through all integers starting with its lower limit m and ending with its upper limit n.

The usual laws for arithmetic applied to summations for eg. when a and b are real numbers, we have $\sum_{j=1}^{n} (a x_j + b y_j)$

$= a \sum_{j=1}^{n} x_j + b \sum_{j=1}^{n} y_j$

Ques Express the sum of first 100 terms of the sequence $\{a_n\}$, where $a_n = \frac{1}{n}$ for $n = 1, 2, 3, \ldots$

$$\sum_{j=1}^{n} a_j = \sum_{j=1}^{100} 1/j$$

Ques What is the value of $\sum_{j=1}^{5} j^2$

$$\sum_{j=1}^{5} j^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2$$
$$= 1 + 4 + 9 + 16 + 25$$
$$= \underline{\underline{55}}$$

What is the value of $\sum_{k=4}^{8} (-1)^k$

$$= (-1)^4 + (-1)^5 + (-1)^6 + (-1)^7 + (-1)^8$$
$$= 1 + -1 + 1 + -1 + 1$$
$$= \underline{\underline{1}}$$

09/10/2019
Wednesday ~~Nested~~

Ques $\sum_{K=1}^{5} K = \frac{n(n+1)}{2}$

$= \frac{5(5+1)}{2}$

$= \frac{5 \times 6}{2}$

$= 15$

$\Rightarrow 1+2+3+4+5 = 15$

Ques $\sum_{K=1}^{5} K^2 = 1^2+2^2+3^2+4^2+5^2$

$= 1+4+9+16+25$

$= 55$

$= \frac{n(n+1)(2n+1)}{6}$

$= \frac{5(5+1)(2 \times 5+1)}{6}$

$= \frac{5 \times 6 \times 11}{6}$

$= 55$

$(100-50)+1$

Ques $\sum_{K=50}^{100} K = \frac{n(n+1)}{2}$

$= \frac{51 \times 52}{2}$

$\sum_{K=1}^{100} K - \sum_{K=1}^{49} K = \frac{100 \times 101}{2} - \frac{49 \times 50}{2}$

$= 5050 - 1225$

The following sum statement $\sum_{j=1}^{3} j^2$ can be written in another form

Sum ie $\sum_{K=0}^{4} (j+1)^2$

Here the output is produced 55

10/10/2019
Thursday

Double Summations

This mathematical method can implement as nested loops in computer programs.

Ques Find the double summation of $\sum_{i=1}^{4} \sum_{j=1}^{3} ij$

$= \sum_{i=1}^{4} (i+2i+3i)$

$$= \sum_{i=1}^{4} 6i$$

$2\times1+2\times2+2\times3 = 12$

$3\times1+3\times2+3\times3 = 18$

$4\times1+4\times2+4\times3 = 24$

$= 6+12+18+24$

$= 60$

It can also use summation notation to add all values of a function, or terms of an ~~indd set~~ indexed set where the index of summation runs over all values in a set.

ie it can write $\sum_{s\in S} f(s)$ to represent the sum of the values $f(s)$ for all members s of S.

What is the value of $\sum_{s\in\{0,2,4\}} s$

It calculates the sum of the values of s for all the members of the set. It shows that

$$\sum_{s\in\{0,2,4\}} s = 0+2+4 = 6$$

Sum	Closed form
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$

Ques find $\sum_{k=50}^{100} k^2$

$$\sum_{k=1}^{100} k^2 - \sum_{k=1}^{49} k^2$$

$$= \frac{100(100+1)(2\times100+1)}{6} - \frac{49(49+1)(49\times2+1)}{6}$$

$$= \frac{100\times101\times201}{6} - \frac{49\times50\times99}{6}$$

$$= \frac{2030100}{6} - \frac{\cancel{237600}\ 242550}{6}$$

$$= \frac{1787550}{6} = 297925$$

MODULE - 4

10/10/2019
Thursday

Relations

14/10/2019
Monday

Relationships between elements of sets occur in many contexts.
Every day, we deal with relationships such as those between a business and its telephone number, an employee and his salary, a person and a relative and so on.

In mathematics, relationships such as those between a positive integer and one that it divides, a real number and one that is larger than it, a real number x and the value $f(x)$.

Relationships between elements of sets are represented using the structure called a relation, which is just a subset of the Cartesian product of the sets.

Relations can be used to solve problems such as determining which pairs of series are linked by airline flights in a week, finding a variable order for the different phases of a complicated project, or producing a useful way to store information in computer data bases.

Relations and their properties

The most direct way to express a relationship between elements of a sets is to use ordered pairs made up of two related elements. For this reason, sets of ordered pairs are called binary relations.

definition:

Let A and B be sets. A binary relation from $A \to B$ is a subset of $A \times B$

In other words a binary relation from $A \to B$ is a set R of ordered pairs where the first element of each ordered pair comes from A and the second element comes from B. The notation used as aRb to denote that $(a, b) \in R$, and $a \not R b$ to denote that $(a, b) \notin R$.

Binary relations represent relationships between the elements of two sets. The n-ary relations, which express the relationships among elements of more than two sets.

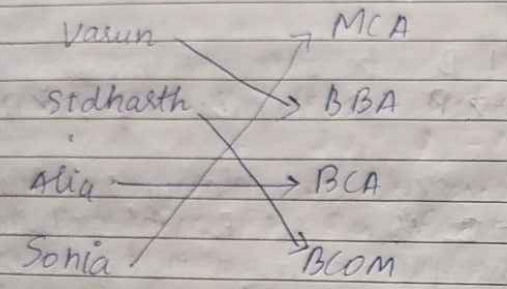
eg:- Let A be the set of students in a college and let B be the set of courses. Let R be the relation that consists of those pairs (a, b), where 'a'

is a student enrolled in course B

eg:- A {Varun, Sidharth, Alia, Sonia, } ~~Anadhan~~

B{ MCA, BBA, BCA, BCOM}

R = {(Varun, BBA), (Sidhasth, BCOM)
(Alia, BCA), (Soma, MCA)}



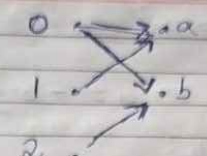
:- Let A = {0, 1, 2}
B = {a, b}

{(0, a) (0, b) (1, a) (2, b) }

is a relation from A → B

This means for instance, that 0Ra
but that 1 ~~R~~ B

The following figure shows the relationship as ordered pairs.



R	a	b
0	×	×
1	×	
2		×

Relation on a Set

definition:-
A relation on the set A is a relation from A → A

In other words a relation on a set A is a subset of A × A

eg:- Let A be the set {1, 2, 3, 4}, which ordered pairs are in the relation
R = { (a, b) | a divides b }

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

eg:- Consider the following relations on the set of integers.

$R_1 = \{(a,b) \mid a \leq b\}$

$R_2 = \{(a,b) \mid a > b\}$

$R_3 = \{(a,b) \mid a = b \text{ or } a = -b\}$

$R_4 = \{(a,b) \mid a = b\}$

$R_5 = \{(a,b) \mid a = b+1\}$

$R_6 = \{(a,b) \mid a + b \leq 3\}$

Which of these relations contain each of the pairs $(1,1)$ $(1,2)$ $(2,1)$ $(1,-1)$ and $(2,2)$

$(1,1) \Rightarrow R_1, R_3, R_4, R_6$

$(1,2) \Rightarrow R_1, R_5, R_6$

$(2,1) \Rightarrow R_2, R_6$

$(1,-1) \Rightarrow R_2, R_3, R_6$

$(2,2) \Rightarrow R_1, R_3, R_4$

2019

Properties of Relations

In some relations an element is always related to itself. For instance, Let R be the relation on the set of all people consisting of pairs (x, y) where x and y have the same mother and the same father. Then ~~x R x~~ xRx ~~or~~ for every person x.

~~define~~

Reflexive

Definition:-

A relation R on a set A is called reflexive if $(a,a) \in R$ for every element $a \in A$

eg Consider the following relations on $(2^n)^2$ $\{1,2,3,4\}$

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

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

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

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

$R_5 = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$

$R_6 = \{(3,4)\}$

Reflexive $\rightarrow R_3, R_5$

Symmetric $\rightarrow R_2, R_3,$

Anti symmetric $\rightarrow R_4, R_5, R_6$

Is the divides relation on the set of positive integers reflexive?

Yes, it is reflexive, because a/a whenever integer is positive a is a positive integer.

If it replace the set of positive integers with the set of all integers the relation is not reflexive because 0 doesnot divide 0.

Anti-Symmetric and Symmetric

In some relations an element is related to a second element if and only if the second element is also related to the first element.

Definition:-

A relation R on a set A is called symmetric if (b,a) is the element of R ie $(b,a) \in R$ whenever $(a,b) \in R$, for all $(a,b) \in A$.

A relation R on a set A such that for all $(a,b) \in A$, if $(a,b) \in R$ and $(b,a) \in R$ then $a=b$ be called antisymmetric.

ie A relation is symmetric if and only if a is related to b implies that b is related to a.

$aRb \rightarrow bRa$

A relation is antisymmetric if and only if if there are no pair of distinct elements a and b with aRb and bRa $(a \neq b)$ ie the only ways to have a related to b and b related to a (bRa) is for a and b to be the same element.

The term symmetric and anti-symmetric are not opposite

6/10/2019 Wednesday

Combining Relations

Because relations from $A \rightarrow B$ are subset of $A \times B$,

Two relations from $A \rightarrow B$ can be combined in any way two sets can be combined.

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

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

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

can be combined to obtain

$R_1 \cup R_2 = \{(1,1)\ (1,2)\ (1,3)\ (1,4)\ (2,2)\ (3,3)\}$

$R_1 \cap R_2 = \{(1,1)\ (1,3)\}$

$R_1 - R_2 = \{(2,2)\ (3,3)\}$

$R_2 - R_1 = \{(1,2)\ (1,4)\}$

$R_1 \oplus R_2 = \{(1,2)\ (1,4)\ (2,2)\ (3,3)\}$

Ques Let A and B be the set of all students and ~~let A and B be~~ the set of all courses in a college respectively. Suppose that R_1 consists of all ordered pairs (a, b), where a is a student ~~and~~ who has taken course b, and R_2 consists of all ordered pairs (a, b) where a is a student ~~who~~ who requires courses to be graduate.
What are the relations $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 \oplus R_2$, $R_1 - R_2$, $R_2 - R_1$

$A = \{S_1$

~~Repre~~

Representing relations

A relation between finite sets can be represented using a ~~(0-1)~~ 0-1 matrix. Suppose that R is a relation from $A = \{a_1, a_2 \ldots\ldots a_m\}$ to $B = \{b_1, b_2, \ldots\ldots b_n\}$.

The relation R can be represented by the matrix

$$M_R = [M_{ij}] \text{ where}$$

$$m_{ij} = \begin{cases} 1 & \text{if } (a_i, b_j) \in R \\ 0 & \text{if } (a_i, b_j) \notin R \end{cases}$$

eg:- Suppose that $A = \{1, 2, 3, 4\}$ and $B = \{1, 2, 3\}$. Let R be the relation from $A \to B$ containing (a, b) if $a \in A, b \in B$ and $a > b$. What is the matrix representing R if $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $b_1 = 1$, $b_2 = 2$.

3×2 matrix

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

The matrix R is

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$$

(1,1) (1,2)
(2,1) (2,2)
(3,1) (3,2)

~~(1,1) (1,2)~~
~~(2,1) (2,2)~~
~~(3,1) (3,2)~~

The zeroes show that no other pairs belong to R

eg Let $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3, b_4, b_5\}$. Which ordered pairs are in the relation R represented by the matrix

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \end{array} \begin{array}{c} \begin{array}{ccccc} b_1 & b_2 & b_3 & b_4 & b_5 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

(a_1, b_1) (a_1, b_2) (a_1, b_3)
(a_2, b_1) (a_2, b_2) (a_2, b_3)
(a_3, b_1) (a_3, b_2) (a_3, b_3)

$R = \{(a_1, b_2)\ (a_2, b_1)\ (a_2, b_1)\ (a_2, b_3)\ (a_2, b_4)\ (a_3, b_1)\ (a_3, b_3)\ (a_3, b_5)\}$

Reflexive matrix

The matrix of a relation of a set, which is a square matrix, can be used to determine whether the relation has certain properties. A relation R on A is reflexive if $(a, a) \in R$ whenever $a \in A$.

Thus R is reflexive if and only if $(a_i, a_i) \in R$ for $i = 1, 2, 3 \ldots n$.

Hence R is reflexive if and only if

$m_{ii} = 1$ for $i = 1, 2, 3 \ldots n$. In other words, R is reflexive if all the elements on the main diagonal of M_R are equal to one. It is shown below:-

$$\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

Symmetric Relation

The relation R is symmetric if pair $(a, b) \in R$ implies that $(b, a) \in R$.

Consequently, the relation R on the set A $A = \{a_1, a_2, a_3 \ldots a_n\}$ is symmetric if and only if $(a_j, a_i) \in R$ whenever $(a_i, a_j) \in R$

In terms of the entries of M_R, R is

symmetric if and only iff $m_{ji} = 1$ whenever $m_{ij} = 1$

This also means $m_{ji} = 0$ where $m_{ij} = 0$
Consequently, R is symmetric iff $m_{ij} = m_{ji}$

The transpose of a matrix is the same is also considered as symmetric matrix

$$M_R = (M_R)^t$$

Anti-Symmetric Relation

The relation R is anti-symmetric iff $(a, b) \in R$ and $(b, a) \in R$ implies that $a = b$

Consequently the matrix of an anti-symmetric relation has the property that $m_{ij} = 1$ with $i \neq j$ then $m_{ji} = 0$ or, in other words either $m_{ij} = 0$ or $m_{ji} = 0$ when $i \neq j$

It's form is shown below

$$\begin{bmatrix} & & 1 \\ 0 & & \\ & 0 & \\ 1 & & \end{bmatrix}$$

Ques The relation R on a set is represented by the matrix

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

Is R reflexive, symmetric / anti-symmetric

→ Reflexive, symmetric but not anti-symmetric

diagonal transpose

Join and Meet

join - union - $\vee$
meet - intersection - $\wedge$

The Boolean operations join and meet can be used to find the matrices representing the union and the intersection of 2 relations

Suppose that R_1 and R_2 are relations on a set A represented by the matrices M_{R_1} and M_{R_2} respectively.

The matrix representing the intersection of these relations has a 1 with the positions where M_{R_1} and M_{R_2} have a 1. The matrix representing the union of these relations has a 1 in the positions where either M_{R_1} or M_{R_2} has a 1

Thus the matrices representing the union and intersection of these relations are

$M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2}$ JOIN

$M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2}$ MEET

eg:- Suppose that the relations R_1 and R_2 on a set A are represented by the matrices

$$M_{R_1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

What are the matrices representing $R_1 \cup R_2$, $R_1 \cap R_2$?

$$M_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$M_{R_1 \cup R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$ join

$$M_{R_1 \cap R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$ meet

Transitive

A relation R on a set A is called transitive if whenever pair $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$, for all ($\forall$) $a, b, c \in A$

Using quantifiers we see that the relation R on a set A is transitive if it has

$$\forall a \forall b \forall c \left(((a,b) \in R \wedge (b,c) \in R) \rightarrow (a,c) \in R \right)$$

Ques Which of the following relations are transitive?

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

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

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

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

$R_5 = \{(1,1)\ (1,2)\ (1,3)\ (1,4)\ (2,2)\ (2,3)\ (2,4)\ (3,3)\ (3,4)\ (4,4)\}$

$R_6 = \{(3,4)\}$

Transitive = R_2, R_3, R_4, R_5, R_6

18/10/2019
Friday

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 is the relation consisting of ordered pairs (a, c), where $a \in A$, $c \in C$ and for it ~~there~~ exists an element $b \in B$. such (which) that $(a, b) \in R$ and $(b, c) \in S$.

It denotes the composite of R and S by $S \circ R$

Computing the composite of two relations requires that we find elements that are the second element of ordered pairs in the first relation and the first element of ordered pairs in the second relation

Ques. What is the composite of relations R and S, where R is the relation from $\{1, 2, 3\}$ to $\{1, 3, 4\}$ with $R = \{(1,1)\ (1,4)\ (2,3)\ (3,1)\ (3,4)\}$ and S is the relation from $\{1, 2, 3, 4\}$ to $\{0, 1, 2\}$ with $S = \{(1,0)\ (2,0)\ (3,1)\ (3,2)\ (4,1)\}$

$S \circ R = \{(1,0)\ (1,1)\ (2,1)\ (2,2)\ (3,0)\ (3,1)\}$

here $S \circ R$ is constructed using all ordered pairs in R and ordered pairs in S, where the second element of the ordered pairs in R agrees with the first element of the ordered pairs in S.

eg:- The ordered pairs $(2, 3)$ in R and $(3, 1)$ in S produce the ordered pair $(2, 1)$ in $S \circ R$.

Boolean Multiplication / Boolean Product

The boolean product of two relations can be represented as

$$M_{S \circ R} = M_R \odot M_S.$$

While considering ~~these as~~ these are two matrices its definition is shown below

Let $A = [a_{ij}]$ be an $m \times k$ 0-1 matrix and $B = [b_{ij}]$ an $k \times n$ 0-1 matrix. Then the boolean product of A and B denoted by $A \odot B$ is the $m \times n$ matrix with (i, j)th entry c_{ij} where ~~$c_{ij} = (a_{ij}$~~

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \cdots (a_{ik} \wedge b_{kj})$$

Note that the boolean product of A and B is obtained in an analogous way to the ordinary product of these matrices but with addition replaced with the operation ($\vee$) and with multiplication replaced with the operation $\wedge$.

Date : / /
Page :

Ques Find the boolean product of A and B

$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$ $B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ $(3\times 2)\ (2\times 3)$

$A \odot B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

$= \begin{bmatrix} (1\wedge 1)\vee(0\wedge 0) & (1\wedge 1)\vee(0\wedge 1) & (1\wedge 0)\vee(0\wedge 1) \\ (0\wedge 1)\vee(1\wedge 0) & (0\wedge 1)\vee(1\wedge 1) & (0\wedge 0)\vee(1\wedge 1) \\ (1\wedge 1)\vee(0\wedge 0) & (1\wedge 1)\vee(0\wedge 1) & (1\wedge 0)\vee(0\wedge 1) \end{bmatrix}$

Transform
$\wedge$ - And
$\vee$ - OR
Union

$= \begin{bmatrix} 1\vee 0 & 1\vee 0 & 0\vee 0 \\ 0\vee 0 & 0\vee 1 & 0\vee 1 \\ 1\vee 0 & 1\vee 0 & 0\vee 0 \end{bmatrix}$

$A \odot B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$

Date : / /
Page :

Ques Find the matrix representing the relation R^2 where the matrix represent R is $M_R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$

$R^2 = R \odot R$

$R \odot R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$

$R \odot R = \begin{bmatrix} 0\vee 0\vee 0 & 0\vee 1\vee 0 & 0\vee 1\vee 0 \\ 0\vee 0\vee 1 & 0\vee 1\vee 0 & 0\vee 1\vee 0 \\ 0\vee 0\vee 0 & 1\vee 0\vee 0 & 0\vee 0\vee 0 \end{bmatrix}$

$= \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

Representing relations using di-graphs

(Pictorial representation of relation)
Each element of the set is represented by a point, and each ordered pair is represented using an arc with its direction indicated by an arrow

This graph is also known as digraphs

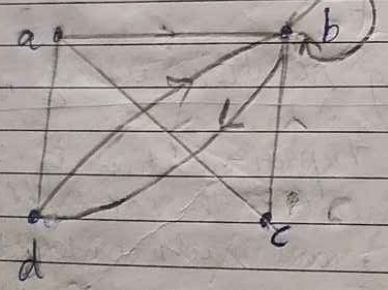
definition

a directed graph or digraph consists of a set V of vertices (or nodes) together with a set E of ordered pairs of elements of V called edges (arcs)

The vertex 'a' is called the initial vertex of the edge (a,b), and the vertex 'b' is called the ~~inter~~ terminal vertex of this edge

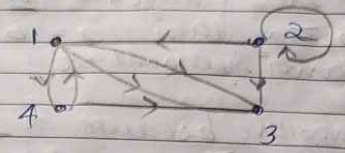
An edge of the form (a, a) is represented using an arc ~~with~~ from the vertex 'a' back to itself.
Such an edge is called a loop

Ques Draw a directed graph with vertices a, b, c and d and edges (a,b) (a,d) (b,b) (b,d) (c,a) (c,b) (d,b)

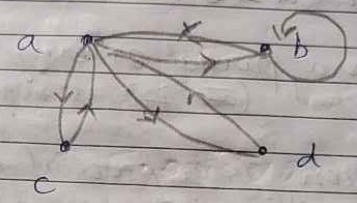


Determine whether the relations for the directed graphs shown below are reflexive, symmetric, anti-symmetric and/or transitive

(a)



(b)



21/10/2019 Monday

Partial Orderings

definition:

A relation R on a set S is called a partial ordering or partial order if it is reflexive, antisymmetric and transitive.
A set S together with a partial ordering R is called a partially ordered set or poset and is denoted by (S, R)

Members of S are called elements of the poset

eg Show that the 'greater than' or 'equal' relation is a partial

ordering on the set of integers

soln:- Because $a \geq a$ for every integer a, $\geq$ is reflexive
If $a \geq b$ and $b \geq a$ then $a = b$
hence, $\geq$ is anti symmetric.

Finally $\geq$ is transitive because $a \geq b$ and $b \geq c$ imply that $a \geq c$.

It follows that $\geq$ is a partial ordering on the set of integers and $(\mathbb{Z}, \geq)$ is a poset.

eg The divisiblity relation is a partial ordering on the set of positive integers, because it is reflexive, anti-symmetric, and transitive. $(\mathbb{Z}^+, |)$ is a poset

eg Ques Let R be the relation on the set of people such that xRy if x and y are people and x is older than y. Show that R is not a partial ordering.

soln. Note that R is antisymmetric because if a person x is older than a person y, then y is not older than x
ie; if xRy, then $x \not R y$ and $y \not R x$
The relation R is transitive because if person x is older than person y and y is older than person z; then x is older than z.
ie, if xRy and yRz, then xRz

However R is not reflexive, because no person is older than himself or himself
ie $x \not R x$. It follows that R is not a partial ordering

definition 2

The elements a and b of a poset $(S, \leq)$ are called comparable if either $a \leq b$ or $b \leq a$. When a and b are elements of S such that neither $a \leq b$ nor $b \leq a$, a and b are called incomparable

eg In the poset $(\mathbb{Z}^+, |)$ are the integers 3 and 9 comparable? Are 5 and 7 comparable?

The integers 3 and 9 are comparable because $(3 | 9)$.
The integers 5 and 7 are incomparable because $5 \nmid 7$ and $7 \nmid 5$

definition 3.

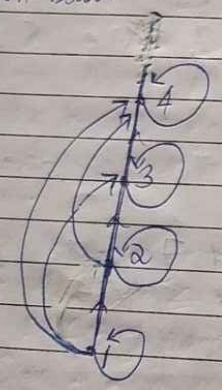
If $(S, \leq)$ is a poset and every elements of S are comparable, S is called a totally ordered or linearlly ordered set, and $\leq$ is called a total order or a linear order. A totally ordered set is called a chain.

eg:- The poset $(Z, \leq)$ is totally ordered because $a \leq b$ or $b \leq a$ whenever a and b are integers.

eg The poset $(Z^+, /)$ is not totally ordered because it contains elements that are incomparable such as 5 and 7.

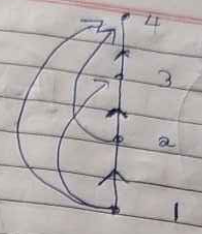
Hasse Diagram

Many edges in the directed graph for a finite poset donot have to be shown because they must be present. for instance, consider the directed graph for the partial ordering $\{(a, b) \mid (a \leq b)\}$ on the set $\{1, 2, 3, 4\}$ shown below



because this relation is a Partial ordering it is reflexive, and its directed graph has loops at all vertices

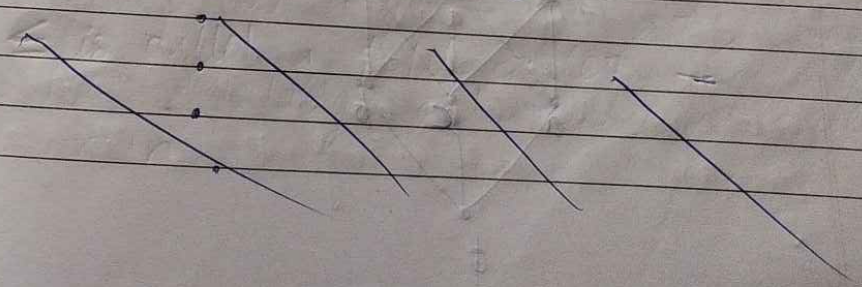
Consequently, we donot have to show these loops because they must be present.
The following figure loops are not shown

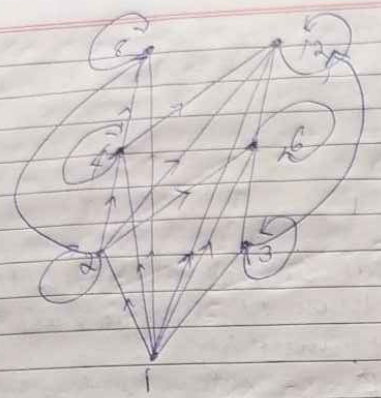


Because a partial ordering is transitive, we donot have to show those edges that must be present because of transitivity.
The following figure shows this and the edges (1, 3) (1, 4) (2, 4) are not shown because they must be present.

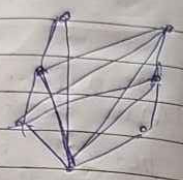
All edges are pointed "upward", we donot have to show the direction of the edges

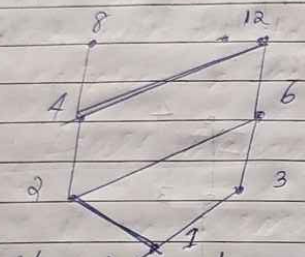
Ques Draw the Hasse diagram Representing the partial ordering $\{(a, b) \mid a \text{ divides } b\}$ on $\{1, 2, 3, 4, 6, 8, 12\}$





Digraphs



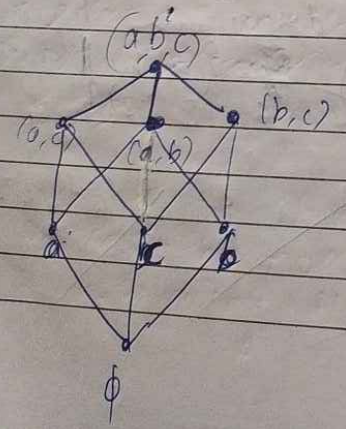


P'

P>

this is the resulting Hasse diagram

Que Draw the Hasse diagram for partial ordering $\{(A,B) \mid A \leq B\}$ on the power set $P(S)$ where $S = \{a, b, c\}$



The Hasse diagram for the partial ordering is obtained from the associated digraph by deleting all the loops and all the edges that occur from transitivity, namely $(\phi, \{a,b\})$, $(\phi, \{a,c\})$, $(\phi, \{b,c\})$, $(\phi, \{a,b,c\})$, $(\{a\}, \{a,b,c\})$, $(\{b\}, \{a,b,c\})$, $(\{c\}, \{a,b,c\})$

finally all edges point upward and arrows are deleted

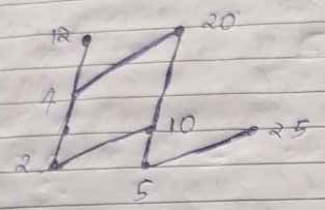
22/10/2019 **Maximal and minimal Elements**

elements of posets that have certain external properties are important for many applications. An element of a poset is called maximal if it is not less than any element of the poset.

ie, A is maximal in the poset $(S, \leq)$ if there is no $b \in S$ such that $a < b$. Similarly an element of a poset is called minimal if it is not greater than any element of the poset.

ie, A is minimal if there is no element $b \in S$. such that $b < a$. Maximal and minimal elements are easy to spot using a Hasse diagram. They are the 'top' and 'bottom' elements in the diagram

Ques Which elements of the poset $(\{2, 4, 5, 10, 12, 20, 25\}, |)$



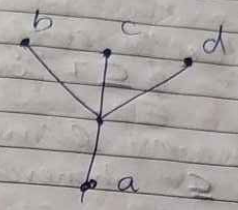
In the diagram the poset shows that the maximal elements are 12, 20, and 25, and the minimal elements are 2 and 5

Greatest and Least Elements

Sometimes there is an element in a poset that is greater than every other element. Such an element is called the greatest element.
ie A is the greatest element in the poset $(S, \leq)$ if $b \leq a$ for all $b \in S$.
Likewise, an element is called the least element if it is less than all the other elements in the poset. ie a is the least element of $(S, \leq)$ if $a \leq b$ for all $b \in S$

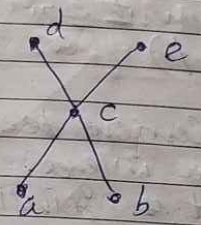
Determine whether the posets represented by each of the following Hasse diagrams have a greatest element and a least element

(a)



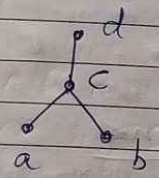
→ The least element of the poset is a
→ no greatest

(b)



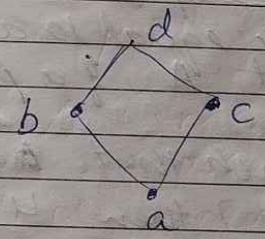
→ no least / greatest (neither least nor greatest)

(c)



→ no least
→ greatest is d.

(d)



→ least - a
→ greatest - d

Ques Let S be a set. Determine whether these

is a greatest element and a least element poset ~~(P(S))~~ $P((S), \subseteq)$

The least element is the empty set, because null is the $\emptyset \subseteq T$ for any subset $T(S)$.
The set S is the greatest element in this poset, because $T \subseteq S$ whenever T is a subset of S.

Ques Is there a greatest element and least element in poset $(Z^+, /)$

The integer 1 is the least element because $1/n$ whenever n is a positive integer. Because there is no integer that is divisible by all positive integers, there is no greatest element

Upper Bound and Lower Bound

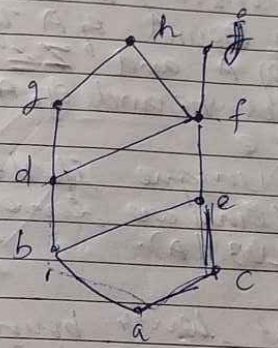
Sometimes it is possible to find an element that is greater than or equal to all the elements in a subset A of a poset $(S, \leq)$.
If u is a element of S such that $a \leq u$ for all elements $a \in A$, then u is called an upper bound of A.

Likewise, there may be an element less

$l \leq a \leq u$

than or equal to all the elements in A. If $l \in S$ such that $l \leq a$ for all elements $a \in A$, then l is called the lower bound of A.

eg:- Find the lower and upper bounds of the subsets $\{a, b, c\}$ $\{j, h\}$ and $\{a, c, d, f\}$ in the poset with the Hasse diagram shown below:-



The upper bounds of $\{a, b, c\}$ are e, f, j and h and its only lower bound is a.

There is no upper bounds of $\{j, h\}$ and its lower bounds are a, b, c, d, e, and f.
The upper bounds of $\{a, c, d, f\}$ are f, h, and j. The lower bound is a.

Least upper bound and greatest lower bound

The element x is called LUB of the subset A if x is an upper bound that is

less than every other upper bound of A. Because there is only one such element if it exists, it makes sense to call this element the least upper bound i.e. x is the least upper bound of A if $a \le x$ whenever $a \in A$, and $x \le z$ whenever x is an upper bound of A.

Similarly, the element y is called the greatest lower bound of A if y is a lower bound of A and $z \le y$ whenever z is the lower bound of A.

The GLB of A is unique if it exists. The ~~least~~ two terms are denoted by GLB (A) and LUB (A).

Ques Find the greatest lower bound and least upper bound of {b, d, g} if they exist in the poset shown in the figure

The upper bounds of {b, d, g} are g and h because $g < h$, g is the least upper bound.

The lower bounds of {b, d, g} are a and b because $a < b$, b is the greatest lower bound

In the GLB and LUB of the sets {3, 9, 12} and {1, 2, 4, 5, 10}. If they exist in the poset $(Z^+, /)$

An integer is a lower bound of {3, 9, 12} if {3, 9, and 12} are divisible by the integer. The only such integers are 1 and 3. because 1/3, 3 is the greatest lower bound of {3, 9, 12}. The only lower bound for the set {1, 2, 4, 5, 10} with respect to / is the element '1'. Hence 1 is the greatest lower bound for {1, 2, 4, 5, 10}.

An integer (2) is an upper bound for {3, 9, 12} if and only if it is divisible by 3, 9 and 12. The integers with this property are those divisible by the least common multiple of 3, 9, and 12, which is 36. Hence 36 is the least upper bound of {3, 9, 12}

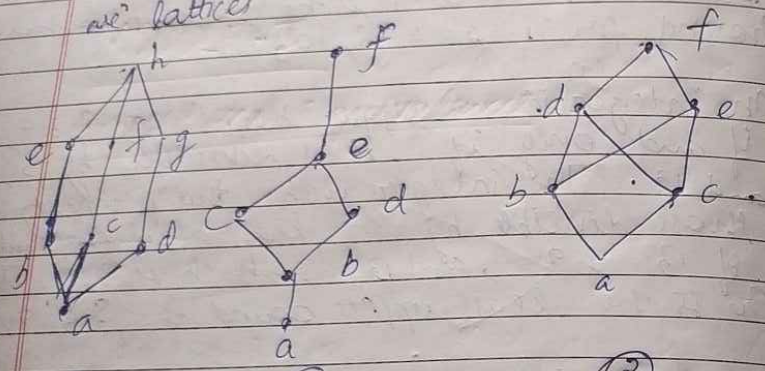
A positive integer is an upper bound for the set {1, 2, 4, 5, 10} iff it is divisible by 1, 2, 3, 4 and 10. The integers with this property are those integers divisible by the least common multiple of these integers, which is 20. Hence 20 is the least upper bound of {1, 2, 4, 5, 10}

Lattices

A partially ordered set in which every pair of elements has both a LUB and a GLB is called a lattice.

Lattices have many special properties, they are used in many different applications such as models of information flow and play an important role in Boolean Algebra.

eg: Determine whether the posets represented by each of the following Hasse diagrams are lattices



(3) (1) (2)

The Hasse diagram both (1) and (3) are lattices because in each poset every pair of elements has both the least upper bound and a greatest lower bound. On the other hand the poset with the diagram 2 is not a lattice because the elements b and c has no least upper bound. To see this note that each of the elements d, e, and f is an upper bound but none of these 3 elements proceeds the other 2 with respect ~~to the~~ to the ordering of this poset.

Ques Is the poset (Z, /) a lattice?

Let A and B be two positive integer. The least upper bound and greatest upper bound of these two integer are the least common multiple and the greatest common divisor of these integers respectively.

Ques Determine whether posets ~~(Z~~ {1, 2, 3, 4, 5} ~~divides~~) and ({1, 2, 4, 8, 16}, /) are lattices?

Because 2 and 3 have no upper bounds in ({1, 2, 3, 4, 5}, /) they certainly do not have an LUB. Hence this poset is not a lattice

Every 2 elements of the second poset have both an LUB and GLB. The LUB of 2 elements in this poset is the larger of the elements and the GLB of 2 elements is the smaller of the elements. Hence this poset is a lattice

2nd poset

Date :
Page :

Ques Determine whether $(P(S), \subseteq)$ is a lattice where S is a set

Soln: Let A and B be two subsets of S. The least upperbound and the greatest lower bound of A and B are $A \cup B$ and $A \cap B$ respectively. Hence $(P(S), \subseteq)$ is a lattice

MODULE-I

Propositional Equivalences

1) Let p, q and r be the propositions :-

p: You get an A on the final exam.

q: You do every exercise in this book.

r: You can get an A in this class.

Write these propositions using p, q, and r and logical connectives

(a) You get an A in this class, but you donot do every exercise in this book.

(b) You get an A on the final exam, You do every exercise in this book, and you get an A in this class.

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

(d) You get an A on the final, but you donot do every exercise in this book: nevertheless you get an A in this class

(e) getting an A on the final and doing every exercise in this book is sufficient for getting an A in this class.

(f) You will get an A in this class if and only if you either do every exercise in this book or you get an A on the final.

Ans:-

(a) $r \wedge \neg q$

(b) $p \wedge q \wedge r$

(c) $r \rightarrow p$

(d) $p \wedge \neg q \wedge r$

(e) $(p \wedge q) \rightarrow r$

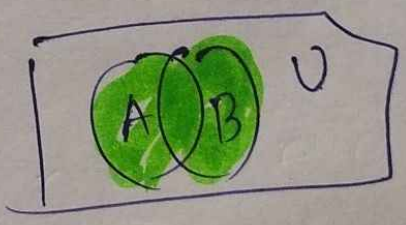
(f) $r \leftrightarrow (q \vee p)$

2) Explain different set operations with valid sets

Sets are used to group objects together. Often the objects in a set have similar properties. A set can be defined as an unordered collection of objects. The objects in a set are called elements or members of a set.

Following are the four different type of set operation of which is explained below:-

- Union
- Intersection
- Compliment
- Differentce



Union (U)

The union of two sets is a set containing all elements that are in A and B. For example, $\{1, 2\} \cup \{2, 3, 4, 5\} = \{1, 2, 3, 4, 5\}$

$A \quad \cup \quad B \qquad = A \cup B$

Similarly we can define the union of three or more sets. In particular if $A_1, A_2, A_3 \ldots A_n$ are sets their union $A_1 \cup A_2 \cup A_3 \ldots A_n$ is a set containing all elements that are in atleast one of the sets.

We can write this union more compactly by

$$\bigcup_{i=1}^{n} A_i$$

for example, if $A_1 = \{a, b, c\}$, $A_2 = \{b, a\}$, $A_3 = \{c, d\}$, $A_1 \cup A_2 \cup A_3 = \{a, b, c, a, d\}$

<u>Intersection</u> ($\cap$)

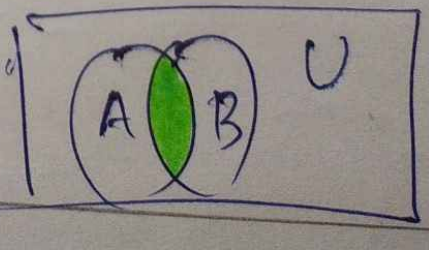
The intersection of two sets A and B denoted by $A \cap B$, consisting of all elements that are both in A and B. for example, $A = \{1, 3, 5, 7\}$ and $B = \{3, 5, 8\}$ then $A \cap B = \{3, 5\}$

for all sets $A_1, A_2, A_3 \ldots$ their intersection $\cap_i A_i$ is defined as the set containing of all elements that are in A_i's.

eg:- Let $A = \{x \mid x$ is a natural number ~~for~~ and factor of $21\}$

$B = \{x \mid x$ is a natural number and less than $10\}$

then $A \cap B \Rightarrow$

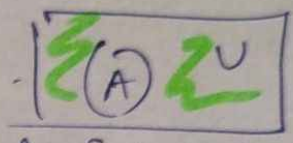


$A = \{1, 3, 21, 7\}$, $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$A \cap B = \{1, 3, 7\}$

Compliment ($\bar{A}$)

The compliment of a set A denoted $\bar{A}$ or A' is the set of elements that are in the universal set U but not A.



eg:- $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $A = \{1, 2, 3, 4\}$,

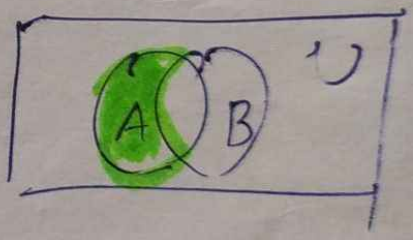
$B = \{2, 4, 6, 8\}$, $A' = U - A = \{5, 6, 7, 8, 9\}$

Difference (−)

The difference is defined as follows, the set A − B consist of elements that are in A but not in B.

eg:- $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$

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



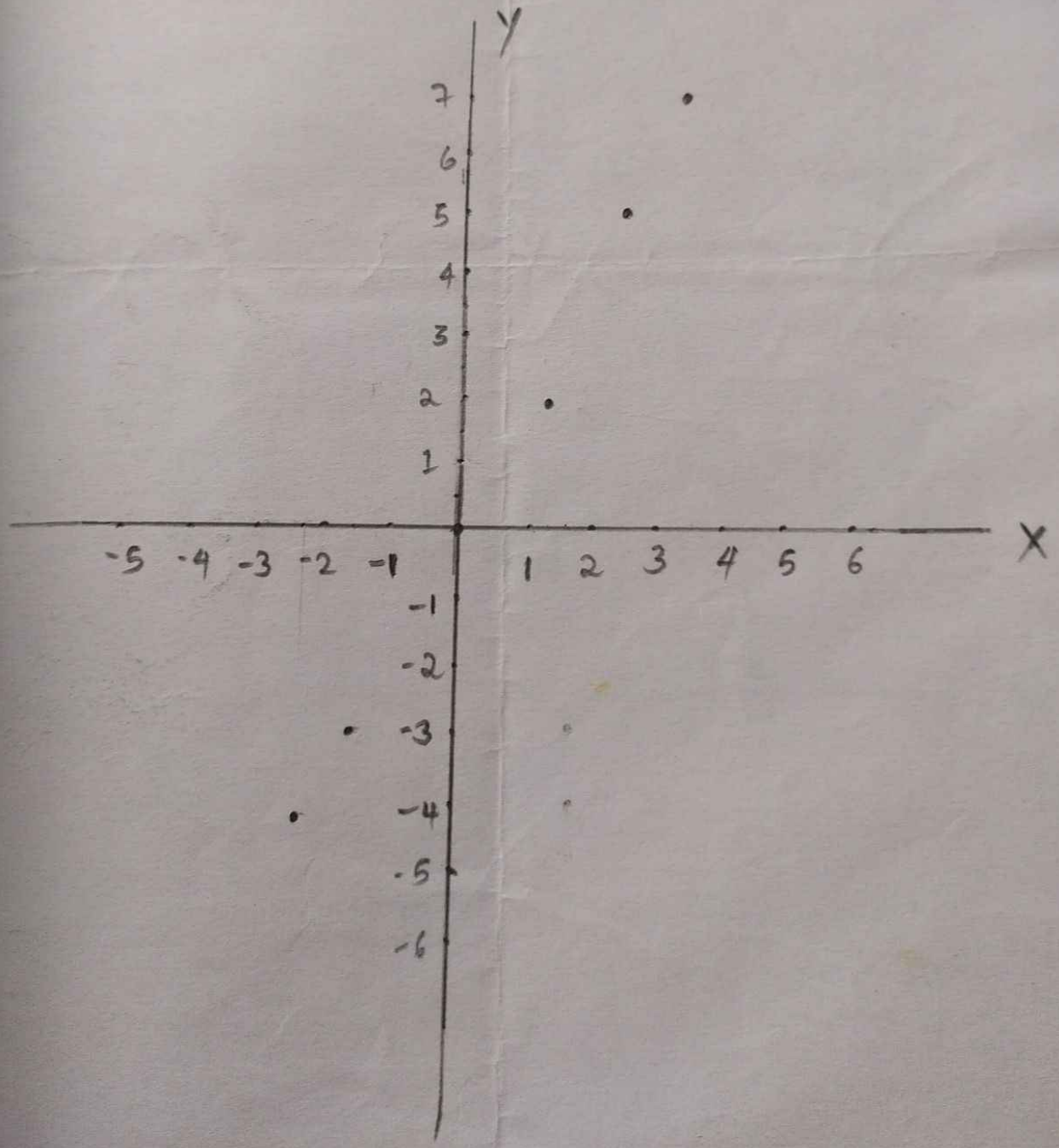
Disjoint

Two sets are called disjoint if their intersection is the empty set.

$A = \{1, 3, 7\}$. $B = \{2, 8, 9\}$ $\boxed{A \cap B = \phi.}$ here A and B are disjoint.

3) Draw the graph of the function $f(x) = \lfloor 2x \rfloor$ from R to R.

x	-2.3	-1.6	0	1.2	2.5	3.5
y	-4	-3	0	2	5	7



4) Represent each of these relations on $\{1, 2, 3, 4\}$ with a matrix (with the elements of this set listed in increasing order.

(a) $\{(1,2)\ (1,3)\ (1,4)\ (2,3)\ (2,4)\ (3,4)\}$

$$\Rightarrow \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

(b) $\{(1,2)\ (1,3)\ (1,4)\ (2,1)\ (2,3)\ (2,4)\ (3,1)\ (3,2)\ (3,4)\ (4,1)\ (4,2)\ (4,3)\}$

$$\Rightarrow \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

5) List the ordered pairs in the relations on $\{1, 2, 3, 4\}$ corresponding to these matrices

(a) $\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$

$\Rightarrow \{(1,1)\ (1,2)\ (1,4)\ (2,1)\ (2,3)\ (3,2)\ (3,3)\ (3,4)\ (4,1)\ (4,3)\ (4,4)\}$

(h) $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$

$\Rightarrow \{(1,1)\ (1,2)\ (1,3)\ (2,2)\ (3,3)\ (3,4)\ (4,1)\ (4,4)\}$

6) Let R_1 and R_2 be the relations on a set A represented by the matrices;

$M_{R_1} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ and $M_{R_2} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$

find the matrices that represent :-

(a) $R_1 \cup R_2$

$M_{R_1} \cup M_{R_2}$
$M_{R_1} \vee M_{R_2}$ $= \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

(b) $R_1 \cap R_2$

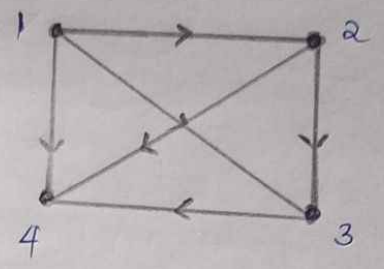
$M_{R_1} \cap M_{R_2}$
$M_{R_1} \wedge M_{R_2}$ $= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$

(c) $R_1 \oplus R_2$

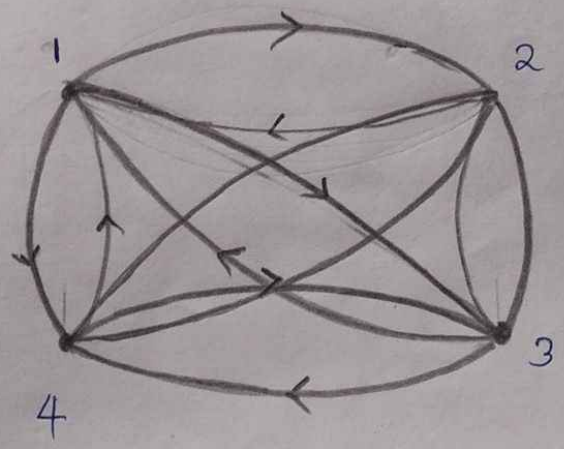
$M_{R_1} \oplus M_{R_2} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

7) Draw the directed graphs representing each of the relations

(a) $\{(1,2)\ (1,3)\ (1,4)\ (2,3)\ (2,4)\ (3,4)\}$



(b) $\{(1,2)\ (1,3)\ (1,4)\ (2,1)\ (2,3)\ (2,4)\ (3,1)\ (3,2)\ (3,4)\ (4,1)\ (4,2)\ (4,3)\}$



4.5/5

23/10/2017

MATHS

MODULE - I

Propositional Equivalences

A mathematical argument is the replacement of a statement with another statement with the same truth value.

The term compound proposition refers to an expression formed from propositional variables using logical operators, such as (p and q) $p \wedge q$.

definition:-

A compound proposition that is always true, no matter what the truth ~~table~~ values of the proposition that occur in it, is called tautology.

A compound proposition that is always false, is called a contradiction.

The compound proposition that is neither a ~~tato~~ tautology ~~nor~~ nor a contradiction is called contingency.

Tautologies and contradictions are often important in mathematical reasoning.

Logical equivalences

Compound propositions that have the same truth values in all possible cases are called logically equivalent.

definition:

The compound propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology. The notation $p \equiv q$ denotes that p and q are logically equivalent

Ques Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent

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

Logical equivalences - Table

Equivalence	Name
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity Laws
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination Laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent Laws
$\neg(\neg p) \equiv p$	Double negation Law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative Laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative Laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive Laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De-Morgan's Laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption Laws
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation Laws

29/8/2019
Thursday

Conditional Statements

Table ①

① $p \to q \equiv \neg p \vee q$

$p \to q \equiv \neg q \to \neg p$

$p \vee q \equiv \neg p \to q$

$p \wedge q \equiv \neg(q \to \neg p)$

$\neg(p \to q) \equiv p \wedge \neg q$

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

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

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

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

Biconditional Statements

Table ②

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Ques

Use De-Morgan's Laws to express the negations of "Miguel has a cellphone and he has a laptop computer". and "Heather will go to the concert or Steve will go to the concert".

Let p be "Miguel has a cellphone" and q be "Miguel has a laptop computer". then "Miguel has a cellphone and he has a laptop computer". can be represented by $p \wedge q$.

By the first De-Morgan's Law $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$

Consequently we can express the negation of the original statement as "Miguel does not have a cellphone or he doesnot have a laptop computer.

Let r be "Heather will go to the concert". and s be "Steve will go to the concert". Then "Heather will go to the concert or Steve will go to the concert". can be represented by $r \vee s$. By the second De-Morgan's Law $\neg(r \vee s) \equiv \neg r \wedge \neg s$

Consequently we can express the negation of the original statement as "Heather will ~~do~~ not go to the concert and Steve will not go to the concert".

Constructing New Logical Equivalences

A proposition in a compound proposition can be replaced by a compound proposition that is logically equivalent to it without changing the truth value of the original compound proposition.

eg:- Show that $\neg(p \to q)$ and $p \wedge \neg q$ are logically equivalent

$(\neg p \to q) \equiv \neg(\neg p \vee q)$ ① st

$\neg(p \vee q) = \neg p \wedge \neg q$ $\quad = \neg(\neg p) \wedge \neg q$ Demorgan's Law ②

$= p \wedge \neg q$ Double negation Law

eg:- Show that $\neg p \vee (\neg p \wedge q)$ and $\neg p \wedge \neg q$ are logically equivalent by developing a series of logical equivalences $\neg(p \vee q) \equiv \neg p \wedge \neg q$

$\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg(\neg p \wedge q)$ the second demorgan law

$\equiv \neg p \wedge (\neg(\neg p) \vee \neg q)$ first demorgan's law

$\equiv \neg p \wedge (p \vee \neg q)$ by double negation law

$\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q)$ distributive law

$\equiv F \vee (\neg p \wedge \neg q)$ $\quad \neg p \wedge p \equiv F$

$\equiv (\neg p \wedge \neg q) \vee F$ commutative law

$p \vee q \equiv q \vee p$

$\equiv (\neg p \wedge \neg q)$ $\quad p \vee F = p$

show that $(p \wedge q) \to (p \vee q)$ is a tautology

by $p \to q \equiv \neg p \vee q$

$(p \wedge q) \to (p \vee q) \equiv (\neg p \wedge q) \vee (p \vee q)$

by the Fir Demorgan Law $\equiv (\neg p \vee \neg q) \vee (p \vee q)$

by the associative and commutative laws for disjunction $\equiv (\neg p \vee p) \vee (\neg q \vee q)$

$\equiv T \vee T$

by the domination law $\equiv T$

The specified example is

Consider the truth ~~values~~ tables of $p \vee \neg p$ and $p \wedge \neg p$ are shown in the table below because $p \vee \neg p$ is always true it is tautology. Because $p \wedge \neg p$ is always false.

It is a contradiction

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

25/9/24

Friday

Predicates and Quantifiers

Predicates

Statements involving variables such as $x > 3$, $x = y + z$, $x + y + 3$, $x + y = z$, "computer x is under attack by an intruder" and "computer x is functioning properly." are often found in mathematical assertions, in computer programs and in system specifications.

These statements are neither true nor false when the values of the variables are not specified

~~x > 5~~

The statement "x is greater than 5" has two parts. The first part, the variable "x" is the subject of the statement. The second part - predicate, "is greater than 5" refers to a property that the subject of the statement can have. We can denote the statement "x ~~> 5~~" by "is greater than 5" by P(x) where P denotes the predicate "is greater than 5" and x is the variable.

The statement P(x) is also said to be the value of the propositional function P at x. Once a value has been assigned to the variable x, the statement P(x) becomes a proposition and has a truth value.

$x > 3$

Ex 1. Let P(x) denote the statement "x greater than 3". What are the truth values of P(4) and P(2)?

P(4) → 4 > 3 T
P(2) → 2 > 3 F

Ex 2: Let A(x) denote the statement "computer x is under attack by an intruder". Suppose that of the computers on campus, only CS2 and MATH1 are currently under attack by intruders. What are truth values of A(CS1) ~~and~~, A(CS2) and A(MATH1)?

A(CS1) - F
A(CS2) - T
A(MATH1) - T

Ex 3: Consider the statement $x = y + 3$. Denote the statement Q(x, y) where x and y are variables and Q is the predicate. What are the truth values of the propositions Q(1, 2), Q(3, 0)?

Q(1, 2) - F
Q(3, 0) - T

N-place predicate (n-ary predicate)

In general, a statement involving the n-variables $x_1, x_2, x_3 \ldots x_n$ can be denoted by $P(x_1, x_2, x_3 \ldots x_n)$. A statement of the form $P(x_1, x_2, x_3 \ldots x_n)$ is the value of the propositional function P at the n-tuple $(x_1, x_2, x_3 \ldots x_n)$ and P is also called an n-place predicate or n-ary predicate.

eg:- Consider the statement if $x > 0$ then $x := x + 1$

The variable x at the point in the execution of the program is inserted into $P(x)$, which is $x > 0$. If $P(x)$ is true, the assignment statement $x : x+1$ is executed.

Preconditions and Post conditions

Predicates are also used in verification that computer programs always produce the desired output when given valid input. The statements that describe valid input are known as preconditions and the conditions that the output should satisfy when the program has run are known as post conditions.

Consider the following program designed to interchange the values of two variables x and y

```
temp := x
x := y
y := t
```

The predicate $P(x, y)$ is the statement $x = a$ and $y = b$ in precondition. For the post condition, it can use $Q(x, y)$ where $Q(x, y)$ is the statement and the input values are $x = b$ and $y = a$.

temp := x	x := y	y := temp
x = a	x = b	x = b
temp = a	temp = a	temp = a
y = b	y = b	y = a

Quantifiers

28/10/2019
Monday

There are two types of quantifications

① Universal which tells that a predicate is true for every element under consideration and
② Existential tells that a predicate is true if there is one or more element under consideration.

The area of logic that deals with predicates and quantifiers is called the predicate calculus.

The Universal Quantifier

Many mathematical statement assert that a property is true for all values of a variable in a particular domain, called the domain of discourse OR the universe of discourse. It often referred to as domain.

The universal quantification of $P(x)$ for a particular domain is the proposition that asserts that $P(x)$ is true for all values of x in this domain.

$P(x_1) \wedge P(x_2) \ldots$

Note that the domain specifies the possible values of the variable x

definition:

The universal quantification of $P(x)$ is the statement "$P(x)$ for all values of x in the domain"

The notation $\forall x P(x)$ denotes the universal quantification of $P(x)$. Here $\forall$ is called the universal quantifier. We read "$\forall$" as "for all ~~x P(x)~~" $\forall x P(x)$ as "for every x $P(x)$ or" for all x $P(x)$.

An element for which $P(x)$ is false is called a counter example of $\forall x P(x)$

The meaning of the universal quantifier is summarised below

Statement	when True?	when False?
$\forall x P(x)$	$P(x)$ is true for every x	There is an x for which $P(x)$ is false

eg: Let $P(x)$ be the statement $(x+1) > x$. What is the truth value of the quantification $\forall x P(x)$, where the domain consists of all real numbers.

$\forall x P(x)$ is true

1.2 be x then $1.2 + 1 = 2.2$

$((x+1) > x)$ ie $(2.2 > 1.1)$

~~Decide~~ Besides "for all" and "for every" universal quantification can be expressed in many other ways including "all of", "for each", "given any", "for arbitrary", ~~"for ea~~

Ques Let $q(x)$ be the statement $x < 2$. What is the truth value of the quantification $\forall x\, Q(x)$ where the domain consist of all real numbers

$Q(x)$ is not true for every real number x because for instance $Q(3)$ is false ie $x = 3$ is a counter example for the statement $\forall x . Q(x)$.

~~Ques~~ When all the elements in the domain can be listed say, $x_1, x_2 \ldots x_n$ - it follows that the universal quantification $\forall x\, P(x)$ is the same as the conjunction $P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \ldots \wedge P(x_n)$

Ques What is the truth value of ~~for all P(x)~~ $\forall x\, P(x)$ where $P(x)$ is a statement $x^2 < 10$ and the domain consists of the positive integers not exceeding 4

as $P(4) = 16$, $x^2 \not< 10$

$P(1) \wedge P(2) \wedge P(3) \wedge P(4)$

from this $P(4)$ is not satisfied because $\forall x\, P(x)$ is false.

Ques What does the statement ~~for all x~~ $\forall x\, N(x)$ means if $N(x)$ is "computer x is connected to the network" and the domain consist of all computers on campus"

The statement means that for every college x on campus, that computer x is connected to the network. This statement can be expressed in english as "Every computer on campus is connected to the network."

What is the truth value if $\forall x\, P(x^2 \geq x)$ if the domain consists of all real numbers? What is the truth value of this statement if the domain consists of all integers?

Existential quantifier

A proposition that is true ~~iff P(x) is true~~ ~~for~~ atleast one value of x in the domain

$P(x_1) \vee P(x_2)$

definition:

The existential quantification of $P(x)$ is the proposition "There exists an element x in the domain such that $P(x)$". We use the notation $\exists x P(x)$ for the existential quantification of $P(x)$. Here $\exists$ is called the

existential - quantifier.

Without specifying the domain, the statement $\exists x P(x)$ has no meaning

Besides the words "There exists" we can also express this quantification in many other ways such as by using the words "for some", "for atleast one", or "there is".

This notation can be read as "There is an x such that $P(x)$", "There is atleast One x such that $P(x)$" OR "For some x: $P(x)$"

Ques Let $P(x)$ denote the statement $(x > 3)$. What is the truth value of the quantification $\exists x P(x)$, where the domain consists of all real numbers.

Because $x < 3$ is sometimes true for instance $x = 4$. In this reason, this quantification is true.

when all elements in the domain can be listed say $x_1, x_2, \ldots x_n$ - the existential quantification is the same as the disjunction.

$P(x_1) \vee P(x_2) \vee P(x_3) \vee \ldots \vee P(x_n)$

Quantifiers with restricted domains

An abbreviated notation is ~~used~~ often used to restrict the domain of a quantifier. In this notation, a condition a variable must satisfy is included after the quantifier

eg:- What do the statements $\forall x < 0 (x^2 > 0)$, $\forall y \neq 0 (y^2 \neq 0)$, and $\exists z > 0 (z^2 = 2)$ mean, where the domain in each case consists of the real numbers

The statement ① $\forall x < 0 (x^2 > 0)$ states that for every real number x with $x < 0$, $x^2 > 0$. ie it states the square of a negative real number is positive. This statement is the same as $\forall x (x < 0 \rightarrow x^2 > 0)$

The statement ② $\forall y \neq 0 (y^2 \neq 0)$ states that for every real number y with $y \neq 0$ we have $y^2 \neq 0$. ie it states "the square of every non-zero real number is non-zero.

This statement is equivalent to $\forall y (y \neq 0 \leftrightarrow y^2 \neq 0)$

The statement ③ $\exists z > 0 (z^2 = 2)$ it states "there is a positive square root of 2" The statement is equivalent to $\exists z [z > 0 \wedge z^2 = 2)$

Negating Quantified Expressions

consider the negation of the statement every student in the class has taken a course in calculus

The following table shows De-morgan's laws for quantifiers.

Negation	Equivalent statement	When is negation True?	When is negation False?
$\neg \exists x P(x)$	$\forall x \neg P(x)$	For every x, $P(x)$ is false	There is an x for $P(x)$ is true
$\neg \forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false	$P(x)$ is true for every x

Examples of Lewis Carroll

① consider these statements. The first two are called premises and the third is called the conclusion. The entire set is called an argument

All lions are fierce.
Some lions do not drink coffee.
Some fierce creatures do not drink coffee.

Let $P(x)$, "x is a lion", $Q(x)$, "x is fierce" and $R(S)$, "x drinks coffee".

from this we can express these statements as $\forall x\ P(x) \rightarrow Q(x)$ ~~$\exists x\ P(x)$ and~~ $\neg R(x)$ ~~$\neg P$~~ $\neg \exists P(x) \wedge \neg R(x)$ and $\exists x\ Q(x) \wedge \neg R(x)$

② Consider these statements of which the first 3 are premises and the fourth is a valid conclusion

All Hummingbirds are richly coloured.
No large birds live on honey.
Birds that do not live on honey are dull in colour.
Humming birds are small.

Let $P(x)$, "x is a humming bird",
$Q(x)$, "x is large",
$R(x)$, "x lives on honey": and
$S(x)$, "x is richly coloured

$\forall x\ (P(x) \rightarrow S(x))$
$\neg \exists x\ (Q(x) \wedge R(x))$
$\forall x\ (\neg R(x) \rightarrow S(x))$
$\forall x\ (P(x) \rightarrow \neg Q(x))$

21/10/2021

MODULE - III

Number theory and Cryptosystem

The Integers and division

Division

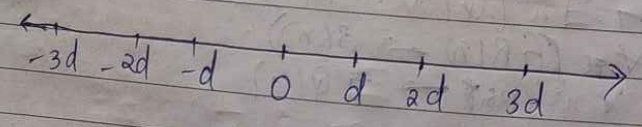
When one integer is divided by a second non ~~ne~~ zero integer, the quotient may or may not be an integer.
For eg $12/3 = 4$ is an integer, whereas $11/4 = 2.75$ is not.

Definition

If A and B are integers with $A \neq 0$, we say that A divides B. if there is an integer C such that $B = A \cdot C$. When A divides B, A is a factor of B and that B is a multiple of A.

The notation ~~A divides B~~ ~~denotes~~ "$A|B$" denotes that "A divides B" and "$A \nmid B$" denotes that "A does not divide B".

The following figure specifies a number line which indicates which integers are divisible by positive ~~indi~~ integer d.



$a|b = b/a$

Determine whether ~~3 divi~~ $3|7$ and whether $3|12$

Because $7/3$ is not an integer and $12/3$ is 4

Let n and d be positive integers. How many positive integer not exceeding n are divisible by d

The positive integers divisible by d are all the integers into the form dk where k is the positive integer.
Hence the number of positive integers divisible by d that do not exceed n equals the number of integers k with $0 < dk \leq n$ OR with $0 < k \leq n/d$.
Therefore there are $\lfloor n/d \rfloor$ positive integers are not exceeding n that are divisible by d.

Some of the basic properties of divisibility of integers are given in the following theorem

Theorem

Let a, b and c be integers then
1. If $a|b$ and $a|c$ then $a|(b+c)$
2. If $a|b$ then $a|bc$ for all integers c

③ If $a|b$ and $b|c$, then $a|c$

The Division Algorithm

When an integers is divided by a positive integer, there is a quotient and remainder, as the division algorithm shows.

Theorem Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r \leq d$ such that
$a = dq + r$

definition:

In the equality given in the division algorithm, 'd' is called the divisor, 'a' is called the dividend, 'q' is called the quotient and 'r' is called the remainder.

This notation is used ~~the~~ to express the quotient and remainder:

$q = a \text{ div } d$, $r = a \bmod d$

What are the quotient and remainder when 101 is divided by 11

$$\begin{array}{r|l} 11 & 101 \\ & 99 \\ \hline & 2 \end{array}$$

$q = 9$ $\quad r = 2$

$a = 101 / 11$
$r = 101 \% 11$

$a = dq + r$
$101 = 11 \cdot 9 + 2$

Hence the quotient when 101 is divided by 11 is 9 ~~and the rema~~ $= 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$

What are the quotient and remainder when -11 is divided by 3?

$-11 = 3(-4) + 1$

$a = dq + r$
$101 = 3 \cdot -4 + 1$

Hence, the quotient when -11 is divided by 3 is $-4 = -11 \text{ div } 3$ and the remainder is $1 = -11 \bmod +3$.

Modular arithmetic

If a and b are integers and m is a positive integer, then a is congruent to b modulo m. If m divides $(a-b)$

We use the notation $a \equiv b \pmod{m}$ to indicate that "a is congruent to b modulo m"

If a and b are not congruent modulo m, you write $a \not\equiv b \pmod{m}$

Theorem:

Let a and b are integers, and let m be a positive integer. Then $a \equiv b$ if and only if $a \pmod{m} = b \pmod{m}$

Ques Determine whether $17 \equiv 5 \pmod{6}$ and whether 24 and 14 are congruent (mod 6)

$17 - 5 = 12 \bmod 6$

$24 - 14 = 10 \bmod 6$

Because 6 divides $17 - 5 = 12$, we say that ~~12 congruent~~ $17 \equiv 5 \pmod{6}$

However $24 - 14 = 10$, is not divisible by 6, we say that $24 \not\equiv 14 \pmod{6}$

Primes and Greatest Common Divisor (GCD)

Primes

Every positive integer greater than one is divisible by atleast two integers, because a positive integer is divided by one and by itself.

positive integers that have exactly two different positive integer factors are called primes

Definition

A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite

The integer 7 is prime because its only positive factors are 1 and 7, where as integer 9 is composite because it is divisible by 3.

Write prime numbers less than 100.

2, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 5

The Fundamental Theorem of Arithmetic

Every positive integer greater than 1 can be written uniquely as a prime or the product of two or more primes where the prime factors are written in order of non-decreasing size.

The prime factorisation of 100, 641, 999 and 1024 are given below

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^5$
$641 = 641$
$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Ques Show that 101 is prime.

The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7, it follows that 101 is prime

Ques Find the prime factorisation of 7007

$7007 = 1001 \times 7$

$7007 / 2$
$7007 / 3$
$7007 / 5$ } nil

$7 \overline{)7007}$
$7 \overline{)1001}$
$11 \overline{)143}$
13

$7007 / 7 = 1001$
$1001 / 7 = 143$
$143 / 11 = 13$

$7007 = 7 \cdot 7 \cdot 11 \cdot 13$

Cryptology

One of the most important applications of congruences involves cryptology, which is the study of secret messages. One of the earliest known uses of cryptology was Julius Caesar.

He made messages secret by shifting each letter 3 letters forward in the alphabet. To this method of making a message in secret as encryption. To express Caesar's encryption process mathematically, first replace each letter by an integer from 0 to 25 based on its position in the alphabet.

Caesar's encryption method can be represented by the function f that assigns to the non-negative integer p, $p <= 25$, the integer f(p) in the set {0, 1, 2, ..., 25}. It executes with a function process

$f(p) = (p+3) \bmod 26$

encryption - original msg coded as one message
decryption - changing to original form

Ques What is the secret message produced from the message "Meet You In the PARK"
(using the Caesar cipher)
First replace the letters in the message with numbers. This produces 12 4 4 19
24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by
$f(p) = (p+3) \bmod 26$

~~15 7 7 22~~ 15 7 7 22 1 17 23 11 16
22 10 7 18 3 20 13

The encrypted message is PHHW BRX ~~LQ~~ LQ WKH SDUN

The decryption can be carried out using
$f^{-1}(p) = (p-K) \bmod 26$

Ques What letter ~~to~~ replaces the letter K when the function $f(p) = (7p+3) \bmod 26$ is used for encryption

$f(10) = 7$

$f(p) = (7 \times 10 + 3) \bmod 26$

$f(p) = 73 \bmod 26$

$f(p) = 21$

26 | 73
2
1
9
26
23
3

Because 21 represents V, K is replaced by V in the encrypted message

RSA cryptosystem

It is a public key crypto system based on modular ~~exponentiation~~ exponentiation modulo the product of 2 large primes. Each individual has an encryption key consisting of a modulus $n = pq$ where p and q are large primes and an exponent e, that is relatively prime to $(p-1)(q-1)$

RSA encryption

In this method messages are translated into sequence of integers from alphabet positions

These integers are grouped together to form large integers, each representing a block of letters

The encryption proceeds by transforming the integer m, representing the plane text to an integer c, representing the cipher text ie the encrypted message, using the function

$c = m^e \bmod n$

eg:- Encrypt message ~~stop~~ STOP using the RSA cryptosystem with $p = 43$, $q = 59$ so that $n = 43 \cdot 59 = 2537$ and $e = 13$

note that $\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$

Soln We translate the letters STOP into their numeric equivalence and then group the numbers into blocks of 4 -

$\overset{S}{18}$ $\overset{T}{19}$ $\overset{O}{14}$ $\overset{P}{15}$

We encrypt each block using the mapping $c = m^{13} \bmod 2537$

Computations using fast modular ~~application~~ multiplication show that $1819^{13} \bmod 2537 = 2081$

$1415^{13} \bmod 2537 = 2182$

The encrypted message is 2081 2182