NEHRU COLLEGE OF ENGINEERING AND RESEARCH CENTRE

(Accredited by NAAC, Approved by AICTE New Delhi, Affiliated to APJKTU)

Pampady, Thiruvilwamala(PO), Thrissur(DT), Kerala 680 588

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE MATERIALS

CS201 DISCRETE COMPUTATIONAL STRUCTURES

VISION OF THE INSTITUTION

To mould our youngsters into Millennium Leaders not only in Technological and Scientific Fields but also to nurture and strengthen the innate goodness and human nature in them, to equip them to face the future challenges in technological break troughs and information explosions and deliver the bounties of frontier knowledge for the benefit of humankind in general and the down-trodden and underprivileged in particular as envisaged by our great Prime Minister Pandit Jawaharlal Nehru

MISSION OF THE INSTITUTION

To build a strong Centre of Excellence in Learning and Research in Engineering and Frontier Technology, to facilitate students to learn and imbibe discipline, culture and spirituality, besides encouraging them to assimilate the latest technological knowhow and to render a helping hand to the under privileged, thereby acquiring happiness and imparting the same to others without any reservation whatsoever and to facilitate the College to emerge into a magnificent and mighty launching pad to turn out technological giants, dedicated research scientists and intellectual leaders of the society who could prepare the country for a quantum jump in all fields of Science and Technology

ABOUT DEPARTMENT

- Established in: 2002
- Course offered: B.Tech COMPUTER SCIENCE AND ENGINEERING
  : M.TECH COMPUTER SCIENCE AND ENGINEERING
  :M.TECH CYBER SECURITY
- Approved by AICTE New Delhi and Accredited by NAAC
- Affiliated to the University of A P J Abdul Kalam Technological University.

DEPARTMENT VISION

Producing Highly Competent, Innovative and Ethical Computer Science and Engineering Professionals to facilitate continuous technological advancement

DEPARTMENT MISSION

M1: To Impart Quality Education by creative Teaching Learning Process

M2: To Promote cutting-edge Research and Development Process to solve real world problems with emerging technologies.

M3: To Inculcate Entrepreneurship Skills among Students

M4: To cultivate Moral and Ethical Values in their Profession

PROGRAMME EDUCATIONAL OBJECTIVES

PEO1: Graduates will be able to Work and Contribute in the domains of Computer Science and Engineering through lifelong learning.

PEO2: Graduates will be able to Analyse, design and development of novel Software Packages, Web Services, System Tools and Components as per needs and specifications.

PEO3: Graduates will be able to demonstrate their ability to adapt to a rapidly changing environment by learning and applying new technologies.

PEO4: Graduates will be able to adopt ethical attitudes, exhibit effective communication skills, Teamwork and leadership qualities.

SUBJECT CODE: C202	
COURSE OUTCOMES	
C202.1	Identify and apply operations on discrete structures such as sets, relations and functions in different areas of computing
C202.2	Solve problem using counting techniques and combinotrics and apply recurrence relation to solve the problems in different domain
C202.3	Solve problems using algebraic structures.
C202.4	Solve problems using Boolean algebra and Lattices
C202.5	Verify the validity of an argument using propositional and predicate logic.
C202.6	Construct proofs using direct proof, proof by contraposition, proof by contradiction and proof by cases, and by mathematical induction

PROGRAM OUTCOMES (PO'S)

After the successful completion of the Couse, B.Tech. Computer Science and Engineering, **Graduates can able to**

PO1: Engineering Knowledge: Apply the knowledge of Mathematics, Science, to solve complex engineering problems related to Design, Development, Testing and Maintenance of Software and System Tools

PO2: Problem Analysis: Identify, Analyse and Formulate complex problems to achieve significant conclusions by applying Mathematics, Natural Sciences and Computer Science and Engineering Principles and Technologies.

PO3: Design/Development of solutions: Design and construct software system, programme, component or process to meet the desired needs within the realistic constraints.

PO4: Conduct investigations of complex problems: Use research based knowledge and research methods to perform Literature Survey, design experiments for complex problems in designing, developing and maintaining computing systems, collect data from experimental outcome, analyse and interpret the interesting patterns and to provide effective conclusions.

PO5: Modern tool usage: Create, select and apply appropriate state-of-the-art Tools and Techniques in designing, developing, testing and validating Computing Systems, Tools and Components.

PO6: The engineer and society: Assess the societal, health, security, legal and cultural issues that might arise during Professional Practice in Computer Science and Engineering.

PO7: Environment and sustainability: Demonstrate the knowledge of sustainable development of Software, Components, Tools, Computing Systems and Solutions with an understanding of the impact of these engineering solutions on society and environment.

PO8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice of Computer Science and Engineering.

PO9: Individual and Team Work: Function effectively as an individual, and as a member or leader in multi-disciplinary teams, and strive to achieve common goals.

PO10:Communication: Communicate effectively with engineering community and society and be able to comprehend and write effective reports and documents, make effective presentations and give and receive clear instructions.

PO11:Project Management and Finance: Apply knowledge of the Engineering and Management principles to one's own work, as a member and leader in a team, to manage projects in Multidisciplinary Teams.

PO12:Life-long learning: Recognize the need for lifelong learning to cope up with the rapidly emerging Cutting Edge Technologies in Computer Science and Engineering and its allied Engineering application domains.

CO'S	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
C202.1	3	3	3	3								2
C202.2	3	3	3	3		2						
C202.3	3	3	3	3		2						
C202.4	3	3	3	3		2						
C202.5	3	3	3	3								
C202.6	3	3	3	3								
C202	3	3	3	3		2						2

HIGH	**3**
MODERATE	**2**
LOW	**1**
NIL	**-**

PROGRAM SPECIFIC OUTCOMES (PSO'S)

1). PSO1: Analysis Skills: Ability to Formulate and Simulate Innovative Ideas to provide software solutions for Real-time Problems.

2). PSO2: Design Skills: Ability to Analyse and design various methodologies for facilitating development of high quality System Software Tools and Efficient Web Design Models with a focus on performance optimization.

3). PSO3: Product Development: Ability to Apply Knowledge for developing Codes and integrating hardware/software products in the domains of Big Data Analytics, Web Applications and Mobile Apps

CO'S	PSO1	PSO2	PSO3
C202.1	3	3	
C202.2	2	2	
C202.3	2	2	
C202.4	2		
C202.5	2	3	
C202.6	2	2	
C202	2.16	2.4	0.00

MATHEMATICS -3 rd Semester BTech

For Computer Science and Engineering and Information Technology

DISCRETE MATHEMATICS

CS 201	**COURSE NAME: DISCRETE COMPUTATIONAL STRUCTURES**	**CATEGORY**	**L**	**T**	**P**	**CREDIT**
		BASIC SCIENCE COURSE	**3**	**1**	**0**	**4**

Preamble:

This course introduces the concept of mathematical structures that are fundamentally discrete. The course enable the students to understand and apply the fundamentals of enumeration and counting techniques and different way of arrangements. The course introduce the concept of relations and functions. Propositional logic and predicate calculus are introduced so that the students can test the validity of statements. Methodsof applying recurrence relations to solve problems in different domains are introduced. An introduction to algebraic structures such as monoid and group.

Prerequisite: A soundbackground in higher secondary school Mathematics

Course Outcomes: After the completion of the course the student will be able to

CO 1	Learn the ideas of Sets,relations, functions equivalence relation and posets and it's applications
CO 2	Learn the ideas of Permutations and combinations, Principle of inclusion exclusion, Pigeon Hole Principle, **Recurrence Relations and** some algebraic systems
CO 3	Understand Fundamentals of Algebraic structures its properties such as groups rings and fields
CO 4	Understand the properties of Lattices and Boolean algebra
CO 5	Learn the fundamentals of propositional logic and predicate calculus and apply to test the validity of statements
CO 6	Learn the fundamentals of predicate logic and theory of inference and certain proof techniques to check the validity of statements

Mapping of course outcomes with program outcomes

PO's	Broad area
PO 1	Engineering Knowledge
PO 2	Problem Analysis
PO 3	Design/Development of solutions
PO 4	Conduct investigations of complex problems
PO 5	Modern tool usage
PO 6	The Engineer and Society
PO 7	Environment and Sustainability
PO 8	Ethics
PO 9	Individual and team work
PO 10	Communication
PO 11	Project Management and Finance
PO 12	Lifelong learning

CO'S	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO 1	3	3	3	3								2
CO 2	3	3	3	3		2						
CO 3	3	3	3	3		2						
CO 4	3	3	3	3		2						
CO 5	3	3	3	3								
CO 6	3	3	3	3								
C202	3	3	3	3		2						2

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests(%)**		**End Semester Examination(%)**
	1	**2**	
Remember	10	10	10
Understand	30	30	30
Apply	30	30	30
Analyse	20	20	20
Evaluate	10	10	10
Create			

Course code	Course Name	L-T-P Credits	Year of Introduction
CS201	**DISCRETE COMPUTATIONAL STRUCTURES**	**3-1-0-4**	**2016**

Pre-requisite: NIL

Course Objectives

1. To introduce mathematical notations and concepts in discrete mathematics that is essential for computing.
2. To train on mathematical reasoning and proof strategies.
3. To cultivate analytical thinking and creative problem solving skills.

Syllabus

Review of Set theory, Countable and uncountable Sets, Review of Permutations and combinations, Pigeon Hole Principle, Recurrence Relations and Solutions, Algebraic systems (semigroups, monoids, groups, rings, fields), Posets and Lattices, Prepositional and Predicate Calculus, Proof Techniques.

Expected Outcome:

Students will be able to

1. identify and apply operations on discrete structures such as sets, relations and functions in different areas of computing.
2. verify the validity of an argument using propositional and predicate logic.
3. construct proofs using direct proof, proof by contraposition, proof by contradiction and proof by cases, and by mathematical induction.
4. solve problems using algebraic structures.
5. solve problems using counting techniques and combinatorics.
6. apply recurrence relations to solve problems in different domains.

Text Books

1. Trembly J.P and Manohar R, “Discrete Mathematical Structures with Applications to Computer Science”, Tata McGraw–Hill Pub.Co.Ltd, New Delhi, 2003.
2. Ralph. P. Grimaldi, “Discrete and Combinatorial Mathematics: An Applied Introduction”, 4/e, Pearson Education Asia, Delhi, 2002.

References:

1. Liu C. L., “Elements of Discrete Mathematics”, 2/e, McGraw–Hill Int. editions, 1988.
2. Bernard Kolman, Robert C. Busby, Sharan Cutler Ross, “Discrete Mathematical Structures”, Pearson Education Pvt Ltd., New Delhi, 2003
3. Kenneth H.Rosen, “Discrete Mathematics and its Applications”, 5/e, Tata McGraw – Hill Pub. Co. Ltd., New Delhi, 2003.
4. Richard Johnsonbaugh, “Discrete Mathematics”, 5/e, Pearson Education Asia, New Delhi, 2002.
5. Joe L Mott, Abraham Kandel, Theodore P Baker, “Discrete Mathematics for Computer Scientists and Mathematicians”, 2/e, Prentice-Hall India, 2009.

Course Plan			
Module	**Contents**	**Hours (54)**	**End Sem Exam Marks**
I	**Review of elementary set theory** : Algebra of sets – Ordered pairs and Cartesian products – Countable and Uncountable sets **Relations** :- Relations on sets –Types of relations and their properties – Relational matrix and the graph of a relation – Partitions – Equivalence relations - Partial ordering- Posets – Hasse diagrams - Meet and Join – Infimum and Supremum ***Functions*** *:-* *Injective, Surjective and Bijective functions - Inverse of a function- Composition*	3 6 1	15 %
II	Review of Permutations and combinations, Principle of inclusion exclusion, Pigeon Hole Principle, **Recurrence Relations**: Introduction- Linear recurrence relations with constant coefficients– Homogeneous solutions – Particular solutions – Total solutions **Algebraic systems**:- Semigroups and monoids - Homomorphism, Subsemigroups and submonoids	3 4 2	15 %
FIRST INTERNAL EXAM			
III	**Algebraic systems (contd…)**:- Groups, definition and elementary properties, subgroups, Homomorphism and Isomorphism, Generators - Cyclic Groups, Cosets and Lagrange's Theorem Algebraic systems with two binary operations- rings, fields-sub rings, ring homomorphism	6 2	15 %
IV	**Lattices and Boolean algebra** :- Lattices –Sublattices – Complete lattices – Bounded Lattices - Complemented Lattices – Distributive Lattices – Lattice Homomorphisms. Boolean algebra – sub algebra, direct product and homomorphisms	7 3	15 %
SECOND INTERNAL EXAM			
V	**Propositional Logic**:- Propositions – Logical connectives – Truth tables Tautologies and contradictions – Contra positive – Logical	2 3	20 %

	equivalences and implications Rules of inference: Validity of arguments.	3	
VI	**Predicate Logic**:- Predicates – Variables – Free and bound variables – Universal and Existential Quantifiers – Universe of discourse. Logical equivalences and implications for quantified statements – Theory of inference : Validity of arguments. **Proof techniques:** Mathematical induction and its variants – Proof by Contradiction – Proof by Counter Example – Proof by Contra positive.	3 3 3	20 %
END SEMESTER EXAM			

Question Paper Pattern:

1. There will be *five* parts in the question paper – A, B, C, D, E
2. Part A
    a. Total marks : 12
    b. *Four* questions each having *3* marks, uniformly covering module I and II; All *four* questions have to be answered.
3. Part B
    a. Total marks : 18
    b. *Three* questions each having *9* marks, uniformly covering module I and II; T*wo* questions have to be answered. Each question can have a maximum of three subparts
4. Part C
    a. Total marks : 12
    b. *Four* questions each having *3* marks, uniformly covering module III and IV; All *four* questions have to be answered.
5. Part D
    a. Total marks : 18
    b. *Three* questions each having *9* marks, uniformly covering module III and IV; T*wo* questions have to be answered. Each question can have a maximum of three subparts
6. Part E
    a. Total Marks: 40
    b. *Six* questions each carrying 10 marks, uniformly covering modules V and VI; *four* questions have to be answered.
    c. A question can have a maximum of three sub-parts.

7. There should be at least 60% analytical/numerical questions.

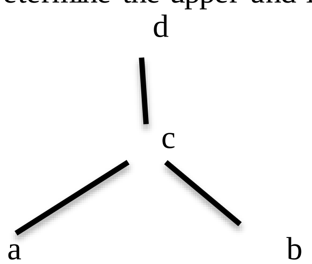
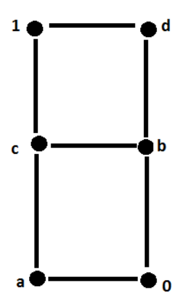
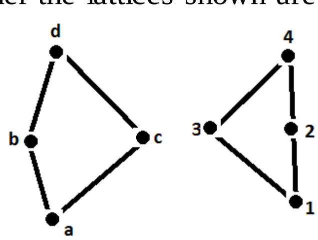
Question Bank

MODULE 1				
S. No	Questions	CO	KL	PAGE NO:
1	Consider f, g, h are functions on integers such that $f(n) = n^2$, $g(n) = n+1$, $h(n) = n-1$.Determine **(i)** $f \circ g \circ h$ **(ii)** $g \circ f \circ h$ **(iii)** $h \circ f \circ g$	CO1	K3	46
2	Draw the Hasse diagram for the divisibility relation on the set A={2,3,6,12,24,36}.	CO1	K6	59
3	Determine whether the functions f:z→z defined by $f(x) = 2x + 1$ is one to one and determine its range	CO1	K2	50
4	Let f(x) = x+2, g(x) = x-2 and h(x) =3x for x is in R, where R is the set of real numbers. Find gof, fog, (foh)og , hog .	CO1	K3	52
5	Define equivalence relation .Let R be a relation in the set of integers Z defined by $R = \{(x, y): x \in Z, y \in Z, (x - y) is\ divisible\ by\ 6\}$. Prove that R is an equivalence relation	CO1	K4	34
6	Let A={1,2,3,4,……..11,12} and let R be the equivalence relation on AXA defined by (a,b) R (c,d) iff a+d=b+c.Prove that R is an equivalence relation and find the equivalence class of (2,5)	CO1	K4	36
7	Show that $(A \cup B)^I) = A^I \cap B^I$	CO1	K6	35
8	Define equivalence relation .Let R be a relation in the set of integers Z defined by $R = \{(x, y): x \in Z, y \in Z, (x - y) is\ divisible\ by\ 7\}$. Prove that R is an equivalence relation	CO1	K6	36
9	Let R and S be two relations on a set A.If R and S are symmetric prove that $R \cap S$ is also symmetric	CO1	K3	32
10	Define a complimented lattice.Show that D42 with '/' as order is a complimented lattice	CO1	K2	69

MODULE 1I				
S. No	Questions	CO	KL	PAGE NO:
1	Solve the recurrence relation $a_r + 5a_{r-1} + 6a_{r-2} = 3r^2 - 2r + 1$	CO2	K3	95
2	Provide one example of linear homogeneous recurrence relation.Mention the degree also	CO2	K6	84
3	Solve the recurrence relation $a_n = 4a_{n-1} - 4a_{n-2} + (n+1)2^n$	CO2	K2	97
4	What is a Monoid? SemiGroup? Explain with examples	CO2	K3	105
5	Solve the recurrence relation $\mathrm{a_r} - 7\mathrm{a_{r-1}} + 10\mathrm{a_{r-2}} = 0$ for $r \geq 2$ given a_0=0,a_1=1 using generating function	CO2	K4	89
6	State Pigeonhole principle. A school has 550 students. Show that at least two of them were born on the same day of the year.	CO2	K4	82
7	Solve the recurrence relation $a_n = 2a_{n-1} + 2^n$ $with\, a_0 = 2$	CO2	K6	96
8	Find the no. of ways in which 5 people A,B,C,D,E can be seated at a round table such that (a)A and B must always sit together (b)C and D must not sit together	CO2	K6	75
9	Solve the recurrence relation $a_{n+2} - 6a_{n+1} + 9a_n = 3\ (2^n) + 7\ (3^n)$	CO2	K3	98
10	If $\{R^+, X)\}$ and {R,+} are two semigroups in the usual notation,prove that the mapping g(a):$R^+ \to R$ defined by g(a)=$log_e a$ is a semigroup isomorphism	CO2	K2	107

MODULE 1II				
S. No	Questions	CO	KL	PAGE NO:
1	Let (A,*) be a group.Show that $(ab)^{-1} = b^{-1}a^{-1}$	CO3	K3	112
2	Prove that the set Q of rational numbers other than 1 forms an abelian group with repect to the operation * defined by a * b =a+b-ab	CO3	K6	107
3	Show that subgroup of a cyclic group is cyclic.	CO3	K2	129
4	Let (A,*) be a Group.Show that (A,*) is an abelian group if and only if $a^2 * b^2 = (a * b)^2$	CO3	K3	110
5	Check whether the algebraic structure ($z_{5,}$+5,x5) defined over the set of positive integers is a ring or not.	CO3	K4	157
6	Define Cosets and Lagranges theorem	CO3	K4	134
7	Show that the set {1,2,3,4,5} is not a group under addition modulo 6	CO3	K6	115
8	Show that the set Q+ of rational numbers forms an abelian group under he operation * defined by a*b=$\frac{1}{2}$ab, a,b $\in Q+$	CO3	K6	107
9	Define ring ,field	CO3	K3	156
10	Prove that every finite integral domain is a field	CO3	K2	160

MODULE 1V

S. No	Questions	CO	KL	PAGE NO:
1	DefineGLB and LUB for a Partially ordered set.Give an example.Define a Lattice, and complimented lattice	CO4	K3	161
2	Consider the poset {a,b,c,d} as shown in figure and let B={c} Determine the upper and lowerbounds of B 	CO4	K6	162
3	Let P(S) be the powerset of S={1,2,3} Construct the hassediagram of the partial order induced on P(S) by the Lattice(P(s),$\wedge$,$\vee$)	CO4	K2	165
4	Determine all the sublatticec of D_{30}	CO4	K3	168
5	Define a Distributive Lattice.Explain with an example	CO4	K4	170
6	What is a Modular lattice	CO4	K4	172
7	What is a complimented Lattice.Determine the compliments Of a and c in fig 	CO4	K6	168
8	Find out all Boolean sub-algebra of D_{30}	CO4	K6	173
9	Determine Whether the lattices shown are isomorphic 	CO4	K3	172
10	Define a bounded Lattice with appropriate example	CO4	K2	167

MODULE V				
S. No	Questions	CO	KL	PAGE NO:
1	Prove that $(P \wedge Q) \rightarrow (P \leftrightarrow Q)$ is a tautology.	CO5	K3	184
2	Use the truth table to determine whether $p \rightarrow (q \wedge \rceil q)$ and $\rceil p$ are logically equivalent	CO5	K6	185
3	Construct a truth table for $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$ and determine whether it is a tautology or not	CO5	K2	184
4	Negate and simplify $\exists x[(p(x) \vee q(x)) \rightarrow r(x)]$	CO5	K3	190
5	Construct an argument to show that the following premises imply the conclusion "it rained" "if it does not rain or if there is no traffic dislocation,then the sports day will be held and the cultural programme will go on." "if the sports day is held,the trophy will be awarded" "the trophy was not awarded"	CO5	K4	192
6	Prove that $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$	CO5	K4	187
7	Verify that $p \vee \neg(p \wedge q)$ is a tautology	CO5	K6	185
8	Prove that the argument $p \rightarrow q, p \wedge r$ imply the conclusion q	CO5	K6	194
9	Prove Validity of the statement "If the market is free then there is no inflation .If there is no inflation then there are price controls.Since there are price controls,therefore the market is free"	CO5	K3	192
10	Construct the truth table for the following statements $(\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q)$	CO5	K2	182

MODULE VI				
S. No	Questions	CO	KL	PAGE NO:
1	Show that (x) (P(x) -> Q(x)) ^ (x) (Q(x) -> R(x)) => (x) (P(x) -> R (x))	CO6	K3	217
2	Symbolize the statements: i) All the world loves a lover ii) All men are giants	CO6	K6	215
3	Show that (∃x) M(x) follows logically from the premises (x) (H(x) -> M(x)) and (∃x) H(x)	CO6	K2	217
4	Negate and simplify $\exists x[(p(x) \vee q(x)) \rightarrow r(x)]$	CO6	K3	210
5	Prove by contradiction that if n^2 is an even integer then n is even	CO6	K4	223
6	Prove that $23^n - 1$ is divisible by 11 for all positive integers n	CO6	K4	223
7	Prove by contradiction method "$\sqrt{2}$ is irrational"	CO6	K6	221
8	Prove that the argument $p \rightarrow q, p \wedge r$ imply the conclusion q	CO6	K6	220
9	Prove by mathematical induction n(n+1)(2n+1) is divisible by 6	CO6	K3	223
10	Determine the negation of the following statement $\exists y \forall x \forall z \; p(x,y,z)$	CO6	K2	210

DISCRETE COMPUTATIONAL STRUCTURES

Module 1

Review of Elementary Set Theory
- Algebra of Sets
- Ordered pairs & cartiesian products
- Countable & Uncountable sets

Relations
- Relation on sets.
- Types of relation & their properties
- Relational Matrix & the graph of relation.
- Partitions
- Equavelence relations
- Partial odering
- Co-sets
- Hasse Diagram
- Meet & Join
- Infimum & Supremum

Functions
- Injective functions
- Surjective functions
- Bijective function
- Inverse of a function
- Composition of function.

Module II

Review of Computation & Permutation

- Principle of inclusion & exclution
- Pegion hole Principle

Recurence Relations

- Introduction
- Linear recurrence relation with constant coefficients
- Homogeneous solution
- Particular Solutions
- Total Solutions

Algebric Systems

- Semi groups & monoids
- Homomorphism
- Subsemiloops

Module III

Algebric Systems

- Groups
- Definition & elementary properties
- Subgroups
- Homomorphisms & Isomorphisms
- Generators
- Cyclic groups
- Coset & Lagrange's theorum

- Fields
- Subrings
- Ring homomorphism

Module IV

Lattices & Boolean Algebra

- Lattices
- Sublattices
- Complete lattices
- Bounded lattices
- Complemented lattices
- Distributive lattices
- Lattice homomorphism.

Boolean Algebra

- Sub Algebra
- Direct Product & homomorphism

Module V

Proportional Logics

- Propositions
- Logical connectives
- Truth tables
- Tautologies & condridictions
- Contrapositive
- Logical equivalence & implications
- Rules of inference
- Validity of Arguments.

Module VI

Predicate Logic

- Predicates
- Variables
- Free & Bound variables
- Universal & existential quantifiers
- Universe of discocurse
- Logic equilence & implecations for quatified
- Statements
- Theory of inference
- Validity of arguments

Proof Techniques

- Mathomatical Induction & its varience
- ~~Phrath~~ by Condridiction
- Proof by counter example
- Proof by contrapositive

Thursday

REVIEW OF ELEMENTARY SET THEORY

SET

A set is a well defined collection of objects. The objects are called elements or members of the set.

Note :-

- We use capital letters with/without subscripts to denote a set.
- Lowercase letters are used to denote the elements of the set.

There are two types of representation of set.

i) Roster method / Tabular form.

In this method we can list the elements in any order and enclosing them within curly braces

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

ii) Set builder form

In this method we will be giving a description about ~~whether~~ the element ~~belongs to the set~~. So that we can identify the elements of the set.

eg: $A = \{x / x$ is an odd integer b/w 1 & 10.$\}$

Here in the above example "is an odd integer b/w 1 & 10" is the discription of the elements of the set. x is the representativ above example is :

$$A = \{3, 5, 7, 9\}$$

Examples for a set

$N = \{1, 2, 3 \ldots\}$ set of natural numbers

$B = \{$ table, chair, pen, apple $\}$

$X = \{x : x$ is an vowel of English alphabet$\}$

Example for not a set

- Beautiful girls in the society
- Five eminet scientist in India.

> If an element p belongs to a set A. then we write $p \in A$.
> The symbol $\in$ denotes " element of "

> If q is not an element of A then will denote as, $q \notin A$

> We can write element of as included in or belongs to.

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

$1 \in A$

$2 \in A$

$6 \notin A$

Finite & Infinite Sets

The set which contains finite no:of elements is called as finite set. And a set with infinite no: of elements is called as infinite set.

eg: $A = \{1, 2, 3, 4, 5\}$ finite

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

Cardinality

The no:of distinct elements of a set is called its cardinality. It is usually denoted by n, #, $||$

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

$n(A) = 4$

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

$n(B) = 4$

Since from the repeatation we will consider only 1

Equal Sets & Equivalent Sets.

Let A and B be two sets the sets A & B are called equal sets if set A and B have same elements.

The set A and B are said to be equivalent sets if the cardinality of A and B are equal.

eg: $A = \{1, 2, 3\}$ $B = \{1, 2, 3\} \Rightarrow A = B$

$A = \{1, 2, 3\}$ $B = \{4, 5, 3\} \Rightarrow$ A & B are equivalent sets

since $n(A) = n(B)$

Subset and Superset

Let A and B be two sets we call A is a subset of B or A is included in B if every element of A is an element of B.
symbolically $A \subseteq B$. Then B is called the superset of A.

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

$B \subseteq A$

Remark: Every set is a subset of itself.

Empty Set or Null Set

A set which contains no elements is called an empty set or null set. It is usually denoted by 'ϕ' or $\{\}$.

Remark:

The cardinality of the null set is zero.
Null set is the subset of every set.

Universal Set

A set is called a universal set if it includes every set under discussion. It is denoted by E or U.

eg: $A \{1,2,3\}$ and $B = \{a,b,c,d\}$

$U = \{1,2,3,a,b,c,d\}$

Power Set

For a set A the family of all subsets of A is called the powerset of A. It is denoted by $\wp(A)$ or P(A). The cardinality of powerset of A is $2^{n(A)}$

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

$$P(A) = \{\phi, \{1,2,3,4\}, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}\}$$

$n(P(A)) = 2^4 = 16$

Proper Subset or Proper inclusion

A set A is called a proper subset of B if A is subset of B. But A is not equal to B. It is denoted by $\subset$.

eg: Consider a set $A = \{1,2,3\}$ & $B = \{1,2,3,4,5\}$.

Then A is a propersubset of B, symbolically, $A \subset B$

Operations on Set

1) Union

Let A & B to any two sets then the union of A & B denoted by '$A \cup B$' is defined as the set of all elements of A and the set of all elements of B and the common elements being taken once.

eg: Let $A = \{a, b, c, d\}$ $B = \{*, +, -, /\}$

then $A \cup B = \{a, b, c, d, *, +, -, /\}$

Let A & B be two sets then the intersection of A & B is denoted by '$A \cap B$' is a set of all elements common to both A & B.

eg: $A = \{1, 2\}$ $B = \{2, 4\}$.

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

3) <u>Disjoint Sets</u>

Let A & B be two sets which are said to be disjoint if $A \cap B = \phi$

4) <u>Disjoint Collection</u>

A collection of sets is called a disjoint collection if every pair of the set two at a time in the collection are disjoint.

The elements of a disjoint collection are said to be mutually disjoint sets.

eg: $A = \{1\}$ $B = \{a\}$ $C = \{*\}$

Then $A \cap B = \phi$, $B \cap C = \phi$ & $A \cap C = \phi$

then the family A, B, C is a disjoint collection and A, B, & C are called mutually disjoint sets.

5) <u>Difference of Sets</u>

Let A & B be two sets the difference of A with respect to. B is the set of all elements that are in A but not in B. It is also called as relative compliment of B in A. It is denoted by A-B.

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

Note:

$A-B \neq B-A$

If A & B are equal sets then A-B and B-A are null se

6) Compliment set /Absolute Compliment

Let A be a set then compliment of A denoted by $\sim A$ or $\bar{A}$ is defined by $U-A$, where U is the universal set.

7) Symmetric difference / Boolean Sum

Let A & B be two sets then symmetric difference of A and B ~~be two sets then~~ denoted by either $A+B$, $A \oplus B$, $A \Delta B$ is defined as $A+B = (A-B) \cup (B-A)$

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

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

find the symmetric difference of A & B.

$A - B = \{3, 4\}$

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

$(A-B) \cup (B-A) = \{3, 4, a, b, c\}$

Venn Diagram

A venn diagram is the diagramatic representation of set operations.

Ordered Pairs

An ordered pair consists of two objects in a given fixed order. It is denoted by (,) or <,>

Note :-

The objects or elements to be ordered need not be distinct / different.

The equality of two ordered pairs. Let it be (x, y) & (u, v) is defined by $x = u$ & $y = v$

Cartesian Product

Let A and B be two sets, the cartesian product of A and B denoted by $A \times B$ is defined as $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$

ie, the set all ordered pairs in which the from B

? Let $A = \{\alpha, \beta, \alpha\}$ $\quad B = \{a, b, c, d, e\}$ find $A \times B$ & $B \times A$.

A. $A \times B = \{(\alpha, a), (\alpha, b), (\alpha, c), (\alpha, d), (\alpha, e),$
$(\beta, a), (\beta, b), (\beta, c), (\beta, d), (\beta, e),$
$(\gamma, a), (\gamma, b), (\gamma, c), (\gamma, d), (\gamma, e)\}$

$B \times A = \{(a, \alpha), (a, \beta), (a, \gamma), (b, \alpha), (b, \beta), (b, \gamma),$
$(c, \alpha), (c, \beta), (c, \gamma), (d, \alpha), (d, \beta), (d, \gamma),$
$(e, \alpha), (e, \beta), (e, \gamma)\}$

Note:-

→ $A \times B \neq B \times A$, but $n(A \times B) = n(B \times A)$

→ If A & B are two sets, then $n(A \times B) = n(A) \cdot n(B)$

RELATIONS

Relation can be refered to anything that connects to objects

Binary Relations

A binary relation denoted by R is the collection of all ordered pairs that satisfy some relational condition.

In other words, a binary operation R from A to B is the subset of cartesian product satisfying the relation.

[illegible]

forms :

$x \in A$, $y \in B$, $R: A \to B$. such that

i) $(x,y) \in R$. where R is the relation

ii) xRy which is read as x is related to y.

iii) The relation set will be given in the tabular form.

? Let R is the relation from A to B where A is the set of natural numbers and the ~~reta~~ B is set of ~~t~~ even numbers and the relation is. $\leq$

A. $A = \{1, 2, 3, 4 \ldots\}$ $B = \{2, 4, 6, \ldots\}$

Here the relation is given to $\leq$

ie, $(x,y) \in R$ if $x \leq y$ where $x \in A$ & $y \in B$.

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

? Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{6, 7, 8, 9, 10\}$.
R is a relation from $B \to A$ defined by $>$
ie, $(x,y) \in R \Rightarrow x > y$ $x \in A$ & $y \in B$

A. $R = \{\phi\}$

? In above question $x \in B$ & $y \in A$.
$R = \{(6,1), (6,2), (6,3), (6,4), (6,5),$

(8,1) , (8,2), (8,3), (8,4) , (8,5),
(9,1) , (9,2), (9,3), (9,4) , (9,5),
(10,1) , (10,2), (10,3), (10,4) , (10,5) }

7/8/2017 Remark

For every $A \in U$, $A \times \phi = \phi$

Proof.

Suppose that $A \times \phi \neq \phi$, that means there exist some ordered pair (atleast one) in $A \times \phi$. Let it be (a,b). By definition of cartesian product

if $(a,b) \in A \times \phi$

$\implies a \in A$ & $b \in \phi$

But $b \in \phi$ is impossible since ϕ is a null set. So assumption is wrong ie $A \times \phi \neq \phi$ is impossible

$\therefore$ If $A \in U$ then $A \times \phi = \phi$

Domain & Range of a Relation

Let R be a relation then the set D(R) called the domain the relation, is the collection of on x such that for some y: $(x,y) \in R$. Similary set range(R) is the set of all elements y such that for some x, $(x,y) \in R$ is called the range (R).

eg: In the above example ">" the domain(R) is $D(R) = \{6, 7, 8, 9, 10\}$

Range(R) = {1, 2, 3, 4, 5}

Inverse Relation

Let R be a relation from set A to B then the inverse of R is the relation from B to A and is given by $R^{-1} = \{(y,x) : (x,y) \in R\}$

? Let $A = \{1,2,3\}$ $B = \{6,7,8\}$. Let R be a relation from $A \to B$ defined by $x < y$ where $x \in A$ & $y \in B$

A. $R = \{(1,6), (1,7), (1,8), (2,6), (2,7), (2,8), (3,6), (3,7), (3,8)\}$

$R^{-1} = \{(6,1), (7,1), (8,1), (6,2), (7,2), (8,2), (6,3), (7,3), (8,3)\}$

$D(R) = \{1,2,3\}$ Range$(R) = \{6,7,8\}$

$D(R^{-1}) = \{6,7,8\}$ Range$(R^{-1}) = \{1,2,3\}$

Types of Relation & Their Properties

Void Relations (Empty Relation)

The relation R in a set A is called a void relation or empty relation if no element of set A is related to any element of set A.

ie $R = \phi$

eg: $A = \{1,2,5,8\}$

$R : A \to A$ defined by $x+y=1$

$R = \{\}$ $\Rightarrow$ R is an empty relation

For a given set A, $I = \{(a,a) : \forall a \in A\}$ is called the identity relation in A.

eg: $A = \{2, 3, 4\}$

$R : A \to A$ defined by $x = y$ $(x,y) \in A$

$R = \{(2,2), (3,3), (4,4)\}$ is an identity relation.

Symmetric Relation

A relation R is a set A is called symmetric relation if $\forall (x,y) \in A$ whenever $x R y$ then $y R x$

eg: $A = \{1, 2, 3\}$

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

This is a symmetric relation since the symmetric pairs (1,2) and (1,3) is present in R

Reflexive Relation

The relation R in a set A is reflexive if for every element of $x \in A$ x related to x itself.

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

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

This is reflexive relation but not a symmetric relation.

Transitive Relation

The relation R in a set A is transitive if $\forall (x,y,z) \in A$ whenever xRy & yRz then xRz

eg: $A = \{1,2\}$

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

This relation is reflexive, symmetric & transitive

Antisymmetric Relation.

A relation R, on a set A is antisymmetric if $\forall (x,y) \in A$ whenever xRy and yRx then $x = y$

eg: $A = \{1,2,3\}$

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

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

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

A relation R on a set A is irreflexive if $\forall x \in A$ $(x,x) \notin R$

eg: $A = \{1,2,3\}$

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

It is irreflexive, not symmetric, not transitive, not antisymmetric

Equivalence Relation

A relation on a set A is called an equivalence relation if and only if it is reflexive, symmetric, transitive.

? Let $A = \{1,2,3,4\}$ and R be a relation on A defined by $R = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4)\}$ Check whether it is an equivalence relation. R is defined on A.

A. For equivalence relation we have to check reflexivity, symmetry, and transitive

i) Reflexive

Here in this relation every element of A is related to itself and hence reflexivity is attained

ii) Symmetry

Here in this R for every pair the symmetric pairs are also present. So symmetry is attained.

iii) Transitive

Here $\forall$ pair if a & b are related and b & c are related $\rightarrow$ a & c are related. Hence transitive

? Let $X = \{1,2,3,4,5,6,7\}$. R is a relation on x defined by $R = \{(x,y) / x-y \text{ is divisible by } 3\}$

$R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (7,7)$
$(1,4), (4,1), (2,5), (5,2), (3,6), (6,3), (4,7), (7,4),$
$(1,7), (7,1)\}$

for equivalence R reflexivity, symmetry & transitivity must be attained.

Reflexive

Here in this relation every element of A is related to itself and hence reflexivity is attained.

Symmetry

Here in this R for every pair symmetric pairs are also present. So symmetry is attained.

Reflexive

For any $a \in X$, $a-a=0$ which is divisible by 3 so by definition of relation every element of A is connected itself which means it is reflexive

Symmetry

for any $(a,b) \in X$ if $(a-b)$ divisible by 3 then clearly $(b-a)$ divisible by 3 (In this case number will be same only sign changes

Hence it is symmetric

Transitive

For any $(a,b,c) \in X$

bRc then aRc

Here $aRb \Rightarrow a-b$ is divisible by 3

$\Rightarrow a-b$ is a multiple of 3

$bRc \Rightarrow b-c$ is divisible by 3

$\Rightarrow b-c$ is a multiple of 3

Our aim is to check $a-c$ is divisible by 3 or $a-c$ is multiple of 3

$$a-c = (a-b)+(b-c)$$
$$= a-b+b-c$$

$\Rightarrow a-c$ is a multiple of 3 since $(a-b)$ & $(b-c)$ is a multiple of 3.

Thus it is an equivalence relation.

10/8/17.

Relational Matrix & Graph of a Relation.

We can represent the relation from a set X to Y in three ways.

i) Matrix form

ii) Arrow diagram

iii) Graphical method

i) By Relational Matrix. | Matrix of Relation.

Step 1: Let $X = \{x_1, x_2, \cdots, x_m\}$

$Y = \{y_1, y_2, \cdots, y_n\}$ be any two sets

Step 2 : Construct a table from row entries at X and column entries at Y. If $x_i R y_i$ where $x_i \in X$ and $y_i \in Y$ then enter 1 in the i^{th} row and j^{th} column. If $x_k \not R y_l$ then we enter zero to k^{th} row & l^{th} column

Step 3 : Form the matrix from the above table containing only 1 and 0.

? Let $X = \{1,2,3\}$ and $Y = \{x, y, z\}$ a relation is from $X \to Y$ defined by $R = \{(1,y),(1,z),(3,y)\}$. Represent this in matrix form.

A. $X = \{1,2,3\}$ $\quad$ $Y = \{x,y,z\}$

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

X \ Y	x	y	z
1	0	1	1
2	0	0	0
3	0	1	0

The matrix form is.

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

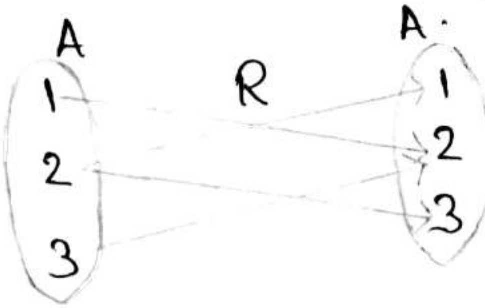
ii) By Arrow Diagrams

In this we write down the element of set A and the elements of set B in two disjoint disk, and then draw an arrow from $a \in A$ to $b \in B$ if and only if $(a,b) \in R$ and the relation is from $A \to B$.

? Consider $A = \{1,2,3\}$ R is a relation on A with relation, $R = \{(1,2),(2,1),(3,2),(2,3)\}$. Draw arrow diagram

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

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



iii) By Graphical Method/ Directed Graph method.

A relation can be represented pictorically or diagramatically by a graph. In this method the relation is taken from a finite set to itself ~~infinite sets~~.

Let R be a relation in a set $X = \{x_1, x_2, \dots x_m\}$. Then the elements of X are represented by points or ~~circlets~~ circles called nodes/vertices. The vertices corresponding to x_i & x_j must be labelled according to the given relation.

ie, if $x_i R x_j$ we connect x_i & x_j by a directed arc or a directed line.

the relation is reflexive we get a loop.

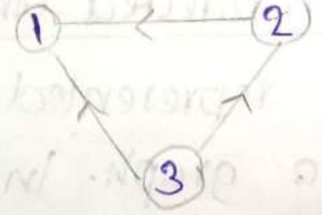
i.e, $x_i R x_i \Rightarrow$ there is an arc from x_i to x_i which is called loop.

If the relation is symmetric then we will be having two arcs in the opposite direction. For the sake of simplicity we can draw one line with 2 arrow signs in opposite direction.

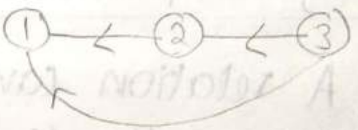
? $X = \{1,2,3\}$ R is a relation on X defined by $R = \{(x,y) \mid x>y\}$. Draw the directed graph of this relation.

A. $X = \{1,2,3\}$

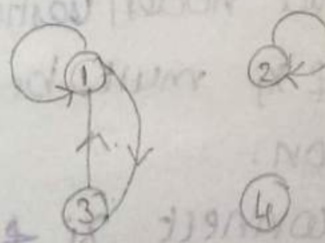
$R = \{(2,1),(3,1),(3,2)\}$



'or'



? $X = \{1,2,3,4\}$ R is a relation on X defined by $R = \{(1,1), (2,2), (3,1), (1,3)\}$. Draw this in directed graph.



11/8/'20

Let S be a given set and $A = \{A_1, A_2, \dots, A_m\}$ where each $A_1, A_2 \dots A_m$ are sets. A is said to be a covering of S if it satisfies two conditions

i) Each A_i where $i = 1, 2, \dots m$ is a non empty subset of S.

$A_i \subseteq S$ & $A_i \neq \phi$.

ii) $A_1 \cup A_2 \cup \dots \cup A_m = S$

In this case each A_i $i = 1$ to n is the power. of S. Let S. be a given set then $A = \{A_1, A_2, A_3 \dots A_m\}$ be a family of set.

then if it satisfies the following properties.

1) Each A_i, $i = 1$ to n is a non empty subset of S.

2) $A_1 \cup A_2 \cup \dots \cup A_m = S$.

3) Each A_i is mutually disjoint ie for $i \neq j$ $A_i \cap A_j = \phi$

If this is the case then A is called the partition of S. Here each A_i, $i = 1$ to m are called the blocks of the partitions.

? Let $S = \{a, b, c\}$ Consider the following collection

$A = \{\{a,b\}, \{b,c\}\}$ $B = \{\{a\}, \{a,c\}\}$

$C = \{\{a\}, \{b,c\}\}$ $D = \{\{a,b,c\}\}$

$E = \{\{a\}, \{b\}, \{c\}\}$ $F = \{\{a\}, \{a,b\}, \{a,c\}\}$

Find out which of the following are covering and partion of S.

A a) Consider $S = \{a, b, c\}$

$A = \{\{a,b\}, \{b,c\}\}$.

Let $A_1 = \{a,b\}$ and $A_2 = \{b,c\}$

For covering, we have to check 2 conditions.

1) Given A_1 & $A_2 \subseteq S \neq \phi$

2) $A_1 \cup A_2 = \{a,b,c\} = S$.

$\therefore$ A is covering of S.

To check the partition,

$A_1 \cap A_2 = \{b\} \neq \phi$ violates the condition, hence A is not a partition of S.

$\therefore$ Given family A is only a covering of S not a partition.

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

$B_1 = \{a\}$ $B_2 = \{a,c\}$

1) B_1 & $B_2 \subseteq S \neq \phi$.

2) $B_1 \cup B_2 = \{a,c\}$.

$\therefore \Rightarrow$ B not covering & not partions.

c) $C = \{\{a\}, \{b,c\}\}$

$C_1 = \{a\}$ $C_2 = \{b,c\}$

2) $C_1 \cup C_2 = \{a, b, c\} = S$.

3) $C_1 \cap C_2 = \phi$.

$\Rightarrow$ C is covering & partition.

d) $D = \{\{a, b, c\}\}$

$D_1 = \{a, b, c\}$ $D_2 =$

1) $D_1 \subseteq S \neq \phi$

2) $D_1 = S$.

3) Intersection always $= \phi$

$\Rightarrow$ D is covering & partition.

e) $E = \{\{a\}, \{b\}, \{c\}\}$

$E_1 = \{a\}$ $E_2 = \{b\}$ $E_3 = \{c\}$

1) E_1 & E_2 & $E_3 \subseteq S \neq \phi$

2) $E_1 \cup E_2 \cup E_3 = \{a, b, c\} = S$.

3) $E_1 \cap E_2 \cap E_3 = \phi$

$\Rightarrow$ E is covering & partition

f) $F = \{\{a\}, \{a, b\}, \{a, b\}\}$

$F_1 = \{a\}$ $F_2 = \{a, b\}$ $F_3 = \{a, c\}$

1) F_1 & F_2 & $F_3 \subseteq S \neq \phi$.

2) $F_1 \cup F_2 \cup F_3 = \{a, b, c\} = S$.

3) $F_1 \cap F_2 \cap F_3 = \{a\} \neq \phi$.

F is covering & not partition

from the above example ... we observe

i) For any finite set the smallest partition consists of singleton elements of the set.

ii) The largest partition consist of the block containing only one element ie the main set.

iii) Every partition is a covering by every covering is not a partition.

12/8/2017 Equivalence Class.

Suppose R is an equivalence relation on a set S for each 'a' $\in$ S, let the equivalence class of 'a' denoted by $[a]_R$. It is the set of all elements of S to which 'a' is related under R ie,

$$[a]_R = \{y / (a,y) \in R\}$$

The members of the equivalence class are called the representative of the equivalence class.

The collection of all equivalence classes of elements of S under an equivalence relation R is called the quotient of S by R and is denoted by S/R.

? Let $X = \{a,b,c,d,e\}$ and $R = \{(a,a), (b,b), (a,b), (b,a), (c,c), (d,d), (e,e), (d,e), (e,d)\}$ is a relation on S. Find the equivalence classes and hence the quotient set if it exist.

It is reflexive, because $\forall$ element of X is related to itself.
It is symmetric, since the pairs (a,b) & (d,e) have their symmetric pairs (b,a) & (e,d) in R.
It is transitive, since if you take xRy & yRz then we can find xRz in R where $x,y,z \in X$
$\therefore$ Given R is an equivalence relation.

Step 2: Finding equivalence class for every element of X

$[a]_R = \{a,b\}$
$[b]_R = \{b,a\}$
$[c]_R = \{c\}$
$[d]_R = \{d,e\}$
$[e]_R = \{e,d\}$

Step 3: The quotient set.

$$X|R = \{[a]_R, [b]_R, [c]_R, [d]_R, [e]_R\}$$
$$= \{a,b,c,d,e\}$$

Remark:-

We can generate an equivalence relation from a partition. For that.
Step 1: First we name with capital letters the blocks of the given partition. ie, if X is the given set and C is a partition

... ing the number of blocks of C as.
$C_1, C_2, C_3 \ldots C_n$

Step 2 : For any $a \in X$ we have to find a set or block, Let it be $C_1 \in C$ such that $a \in C_1$ but it doesnot belongs to any other blocks $C_2, C_3 \ldots C_n$.

Step 3 : Take the cartesion product of the corresponding block to itself $C_1 \times C_2$.

Step 4 : The equivalence relation R is the union of all cartesian products.

? Let $X = \{a, b, c, d, e\}$ and let $C = \{\{a,b\}, \{c\}, \{d,e\}\}$ be the partition. Find the equivalence relations to this partition.

A. Step 1 : $X = \{a, b, c, d, e\}$ and $C = \{\{a,b\}, \{c\}, \{d,e\}\}$

Let $C_1 = \{a,b\}$, $C_2 = \{c\}$, $C_3 = \{d,e\}$

Step 2 : Let $a \in X$, then $a \in C_1$ but $a \notin C_2 \,\&\, C_3$

Hence $C_1 \times C_2 = \{(a,a), (b,b), (a,b), (b,a)\}$

$b \in X \,\&\, b \in C_1$ but $b \notin C_2 \,\&\, C_3$

hence $C_1 \times C_2 = \{(a,a), (b,b), (a,b), (b,a)\}$

$c \in X \,\&\, c \in C_2$ but $c \notin C_1 \,\&\, C_3$

hence $C_2 \times C_2 = \{c, c\}$

$d \in X \,\&\, d \in C_3$ but $d \notin C_1 \,\&\, C_2$

hence $C_3 \times C_3 = \{(d,d), (e,e), (d,e), (e,d)\}$

hence $C_3 \times C_3 = \{(d,d), (e,e), (d,e), (e,d)\}$

Step 3 : Setting the relation S.

$S = (C_1 \times C_1) \cup (C_2 \times C_2) \cup (C_3 \times C_3)$

$= \{(a,a), (b,b), (a,b), (b,a), (c,c), (d,d), (e,e), (e,d), (d,e)\}$

17/8/17

FUNCTIONS

A function from $X \to Y$ is defined as a relation from $X \to Y$ such that every element of X is related to exactly one element in Y.

We usually denote the functions by lowercase letters.

eg: h, g, x etc.

Let $f : X \to Y$ be a function, the domain of the function is defined to be the set X

The co-domain of the function is defined to be the set Y

Consider an element $a \in X$ & $b \in Y$. If the element a is related to element b, then we call 'b' as an image of 'a' under f

In that case 'a' is called the pre image of 'b' under 'f'

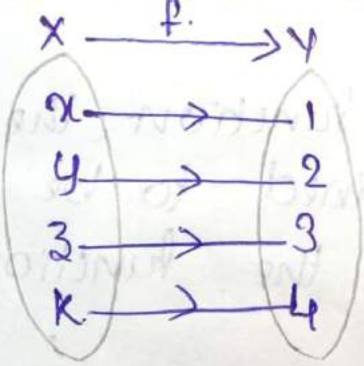
The range of a function 'f' is the collection of all images under 'f'

We normally represents the functions by arrow diagram where the given sets are represented by circles/disks & if the elements of the sets are related then we will be drawing an arrow b/w them.

? Let $X = \{x, y, z, k\}$ and $Y = \{1, 2, 3, 4\}$. Let 'f': $X \to Y$ determine which of the following are functions. Justify your answer draw the arrow diagram. Find domain, range & co-domain of the function

i) $f = \{(x,1), (y,2), (z,3), (k,4)\}$

It is a function since every element of X is related to Y and it have only one image.



Domain $= \{x, y, z, k\}$

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

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

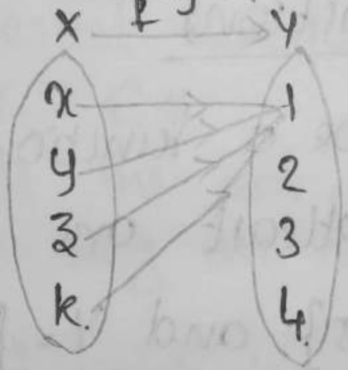
'g' is not a function, since every element of X is not related to Y.

iii) $h = \{(x,1), (x,2), (x,3), (x,4)\}$

'h' is not a function, since every element of X is not related to Y and the element 'x' has more than one image.

iv) $l = \{(x,1), (y,1), (k,1), (z,1)\}$

It is a function since every element of X has exactly one image.



Domain = $\{x, y, z, k\}$

Range = $\{1\}$

Co-domain = $\{1, 2, 3, 4\}$

Remark:

Codomain of a function need not be equal to range.

Type of Functions

1. Injective (One-to-one)

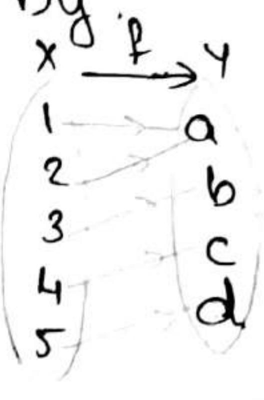
A mapping $f: X \to Y$ is called injective if the distinct elements of X are mapped to distinct elements of Y ie every element in X must have unique image in Y

eg: Let $X = \{x, y, 3, k\}$ $Y = \{1, 2, 3, 4\}$ $f: X \to Y$ is a function defined by $f = \{(x,1), (y,2), (3,3), (k,4)\}$

2. Surjective / Onto functions

Let $f: X \to Y$ be a function then if each $\in Y$ must have atleast one preimage in X.

eg: Let $X = \{1, 2, 3, 4, 5\}$ and $Y = \{a, b, c, d\}$ $f: X \to Y$ defined by



This is not one-one but onto.

Remark: If the function is onto the range of f is equal to co-domain.

functions as into functions.

3. Bijective Function

Let $f: X \to Y$ be a function then if 'f' is one-one & onto.

eg: Let $X = \{x, y, z, k\}$ & $Y = \{1, 2, 3, 4\}$ $f: X \to Y$.
defined by $f = \{(x,1), (y,2), (z,3), (k,4)\}$

18/8/17 Equal functions

Consider two functions f & g from set $X \to Y$. is called equal functions if and only if $f(a) = g(a)$ $\forall$ 'a' $\in X$
If this is not the case for atleast one element in X then they are called unequal functions.

? Let $X = \{1, 2, 3\}$ and $Y = \{a, b, c\}$. Let $f: X \to Y$ $g: X \to Y$ and $h: X \to Y$ be defined as
$f = \{(1,a), (2,a), (3,c)\}$ $g = \{(1,b), (2,a), (3,c)\}$
$h = \{(1,a), (2,a), (3,c)\}$
Which of the above are equal functions.

A. $f = \{(1,a), (2,a), (3,c)\} \Rightarrow f(1) = a;\ f(2) = a;\ f(3) = c.$
$g = \{(1,b), (2,a), (3,c)\} \Rightarrow g(1) = b;\ g(2) = a;\ g(3) = c$
$h = \{(1,a), (2,a), (3,c)\} \Rightarrow h(1) = a;\ h(2) = a;\ h(3) = c.$

$g \neq h$ since $g(1) = b \neq h(1) = a$.

$f = h$ since $f(1) = h(1)$; $f(2) = h(2)$; $f(3) = h(3)$

Identity Function

Consider any A. Let the function $f : A \to A$ is said to be identity function if each element of set A has image on itself.
ie, $f(a) = a \;\forall\, a \in A$

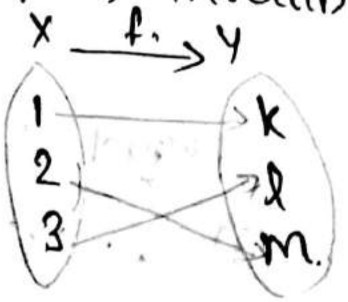
~~Note :-~~

Inverse of a Function / Invertible function.

A function $f : X \to Y$ is called invertible or it posses inverse if and only if 'f' is a bijective function.

? Let $X = \{1, 2, 3\}$ and $Y = \{k, l, m\}$ $f : X \to Y$ defined by $f = \{(1,k), (2,m), (3,l)\}$. Check whether f is invertible or not.

A.



Here f is one-one & onto and hence it is invertible.

$f^{-1} = \{(k,1), (m,2), (l,3)\}$

Composition of function

Consider functions $f: A \to B$ & $g: B \to C$ the composition of 'f' with 'g' is the function from $A \to C$ defined by $gof(x) = g(f(x)) \; \forall x \in A$

? $X = \{1,2,3\}$ $Y = \{a,b\}$ $Z = \{5,6,7\}$

$f: X \to Y$ $g: Y \to Z$ defined by

$f = \{(1,a), (2,a), (3,b)\}$ $g = \{(a,5), (b,7)\}$

Find the composition gof.

A. $f(1) = a$; $f(2) = a$; $f(3) = b$

$g(a) = 5$; $g(b) = 7$,

$gof: X \to Z$ defined by

$gof(1) = g(f(1)) = g(a) = 5$

$gof(2) = g(f(2)) = g(a) = 5$

$gof(3) = g(f(3)) = g(b) = 7$.

? $X = \{1,2,3\}$ f, g, h, s be functions from $X \to X$ defined by $f = \{(1,2), (2,3), (3,1)\}$

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

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

i) $f \circ g$

ii) $g \circ f$.

iii) $s \circ g$

iv) $g \circ s$.

v) $s \circ s$

vi) $f \circ s$

A.

$f(1) = 2$ $\qquad f(2) = 3$ $\qquad f(3) = 1$

$g(1) = 2$ $\qquad g(2) = 1$ $\qquad g(3) = 3$

$h(1) = 1$ $\qquad h(2) = 2$ $\qquad h(3) = 1$

$s(1) = 1$ $\qquad s(2) = 2$ $\qquad s(3) = 3$

i)

$f \circ g(1) = f(g(1)) = f(2) = 3$

$f \circ g(2) = f(g(2)) = f(1) = 2$

$f \circ g(3) = f(g(3)) = f(3) = 1$

ii)

$g \circ f(1) = g(f(1)) = g(2) = 1$

$g \circ f(2) = g(f(2)) = g(3) = 3$

$g \circ f(3) = g(f(3)) = g(1) = 2$

iii)

$s \circ g(1) = s(g(1)) = s(2) = 2$

$s \circ g(2) = s(g(2)) = s(1) = 1$

$s \circ g(3) = s(g(3)) = s(3) = 3$

iv)

$g \circ s(1) = g(s(1)) = g(1) = 2$

$g \circ s(2) = g(s(2)) = g(2) = 1$

$g \circ s(3) = g(s(3)) = g(3) = 3$

$SoS(1) = S(S(1)) = S(1) = 1$

$SoS(2) = S(S(2)) = S(2) = 2$

$SoS(3) = S(S(3)) = S(3) = 3$

we have to [illegible] set

vi) $foS(1) = f(S(1)) = f(1) = 2$

$foS(2) = f(S(2)) = f(2) = 3$

$foS(3) = f(S(3)) = f(3) = 1$

21/8/17

? fohog from $X \to X$ is defined by.

$fohog(x) = foh(g(x))$

$fohog(1) = foh(g(1)) = foh(2) = f(h(2)) = f(2) = \underline{3}$

$fohog(2) = foh(g(2)) = foh(1) = f(h(1)) = f(1) = \underline{\underline{2}}$

$fohog(3) = foh(g(3)) = foh(3) = f(h(3)) = f(1) = \underline{\underline{2}}$

Countable & Uncountable Sets.

Two sets A & B are said to equipotent or to have the same number of elements or same cardinality if there exist a one-to-one & an onto mapping on a function $f: A \to B$

Any set which is equipotent to the set of natural number is called denumerable.

ie, there exist a bijection from the set A to the set of natural numbers then A is called denumerable set.

Otherwise the set is uncountable.
eg: set of natural numbers.
eg: set of even numbers with $f(x) = 2x$; $x \in$ set of even numbers;

Set of real numbers is uncountable.

Partial Oder Relation

Consider a relation R on a set P satisfying the properties
i) R is reflexive,
ii) R is antisymmetric
iii) R is transitive

Then R is called a partial order relation.
The set P together with a partial order relation is called a partial ordered set or poset.
The partial order relation is denoted by '$\leq$' and a poset is denoted by $(P, \leq)$

? Verify whether the set of natural numbers form a poset under the relation $\leq$.

A. For proving poset we have to check the conditions.
Reflexive : Since every element of N related to itself under the relation '$\leq$' (mainly =)
Antisymmetric: It is antisymmetric since we can only find either aRb or bRa

Transitive: The set N is transitive, since whenever xRy & yRz clearly xRz where $x, y, z \in N$.

$\therefore$ N is a poset.

? Consider a set $A = \{4, 9, 16, 36\}$ is the relation 'divides' is a partial order.

A. $R = \{\cancel{(4,16)}, \cancel{(4,36)}, \cancel{(9,36)}, (16,4), (36,4), (36,9), (4,4), (9,9), (16,16), (36,36)\}$

Reflexive: since every element of A is related to itself, R is reflexive.

Antisymmetric: for every xRy & yRx; $x \neq y$ where $x, y \in A$. Hence R is ~~not~~ antisymmetric for eg: $(4,16)$ & $(16,4) \in R$ but, $16 \neq 4$.

Transitive: for every xRy & yRz, xRz where $x, y, z \in A$. Hence R is transitive.

Since R is not antisymmetric it is ~~not~~ a partial order. since it is reflexive, antisymmetric & transitive

? Consider $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$. Can you form the ordered pairs that satisfies the condition divisibility.

A. $R = \{(1,1), (2,1), (2,2), (3,1), (3,3), (5,1), (5,5), (6,1), (6,2), (6,3), (6,6),$ ~~(30,30)~~ $(10,1), (10,2), (10,5), (10,10), (15,1), (15,3), (15,5),$ ~~(15,10)~~ $(15,15),$ ~~(30,1)~~

Reflexive : Since every element is divisible by itself. $(x,x) \in R \; \forall x \in A$. So R is reflexive.

Transitive : When xRy & yRz ; xRz where $x,y,z \in A$. Hence R is transitive.

Antisymmetric : It is antisymmetric since we can only find either xRy or yRx where $x,y \in A$.

22/8/17

Comparable elements.

Consider an ordered set A, two elements a & b of set A are called comparable. if a & b are related. If they are not related they are called non-comparable elements.

? Consider $A = \{1,2,3,5,6,10,15,30\}$ is ordered by divisibility. Determine all the comparable & non-comparable pairs of elements of A.

A. The comparable pair of elements are.

$\{ \{1,2\}, \{1,3\} \{1,5\} \{1,6\} \{1,10\} \{1,15\} \{1,30\}, \{2,6\}$
$\{2,10\} \{2,30\} \{3,6\} \{3,15\} \{3,30\} \{5,10\} \{5,15\} \{5,30\}$
$\{6,30\} \{10,30\} \{15,30\} \}$

Non comparable ...

$\{ \{2,3\}, \{2,5\}, \{2,15\}, \{3,5\}, \{3,10\}, \{5,6\}, \{6,10\}, \{6,15\}, \{10,15\} \}$

Total Order Relation | Linearly Ordered Relation

Consider an ordered set A. the set A is called totally ordered set if every pair of elements in A are comparable.

? Consider the set $I = \{1,2,3,\ldots\}$ is ordered by divisibility. Determine whether each of the following subsets of I are linearly ordered. or not.

i) $\{2,4,8\}$
The possible pairs are $\{2,4\}, \{4,8\}$ & $\{2,8\}$. We know that all these pairs satisfy divisibility & hence it is a totally ordered set.

ii) $\{3,6,9,11\}$
The possible pairs are $\{3,6\}$ $\{3,9\}$ $\{3,11\}$ $\{6,9\}$ $\{6,11\}$ $\{9,11\}$
Here $\{3,11\}$ is not divisible ie, it is not comparable. hence it is not a totally ordered set.

iii) $\{1\}$
Here only one element so no need to check for divisibility, it is always comparable. Hence it is totally ordered set.

iv) $\{2,4,6,8,10\ldots\}$
The set is not totally ordered since every pair is not comparable.

natural numbers is neither an equivalence relation nor an partial order relation but is a total order relation

A. The given set of natural numbers under the relation '<' is neither an equivalence relation nor a partial order relation since $(N, <)$ doesn't satisfy the reflexivity property.
This is a totally ordered set since every pair of this set are comparable under '<'

Hasse Diagram

In a partially ordered set $(A, \leq)$ under some relation. An element $y \in A$ is said to cover an element $x \in A$ if $x \leq y$ & if there doesn't exist any element $z \in A$ such that $x \leq z$ & $z \leq y$
The pictorial representation of partial order relation is called Hasse diagram.

Procedure for drawing Hasse Diagram
1) Each element is represented by small circle/dot.
2) The circle of $x \in A$ is drawn below the circle of $y \in A$ if y is a cover of x or y is directly related to x.
3) If there is any element in b/w x & y satisfying the relation, the line cannot be drawn b/w x & y.

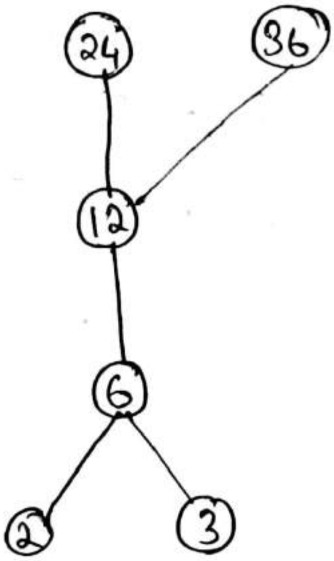
24/8/17

? Let $X = \{2, 3, 6, 12, 24, 36\}$ and the relation is divisibility. Draw the Hasse diagram with this relation.

A. $R = \{(2,6), (2,12), (2,24), (2,36), (3,6), (3,12), (3,24), (3,36), (6,12), (6,24), (6,36), (12,24), (12,36), (2,2), (3,3), (6,6), (12,12), (24,24), (36,36)\}$

This is a partial order relation.

Hasse Diagram.



? Consider the set $A = \{4, 5, 6, 7\}$ Let the relation be $\leq$. Draw the Hasse diagram.

A. $R = \{(4,5), (4,6), (4,7), (5,6), (4,4), (5,7), (5,5), (6,6), (6,7), (7,7)\}$

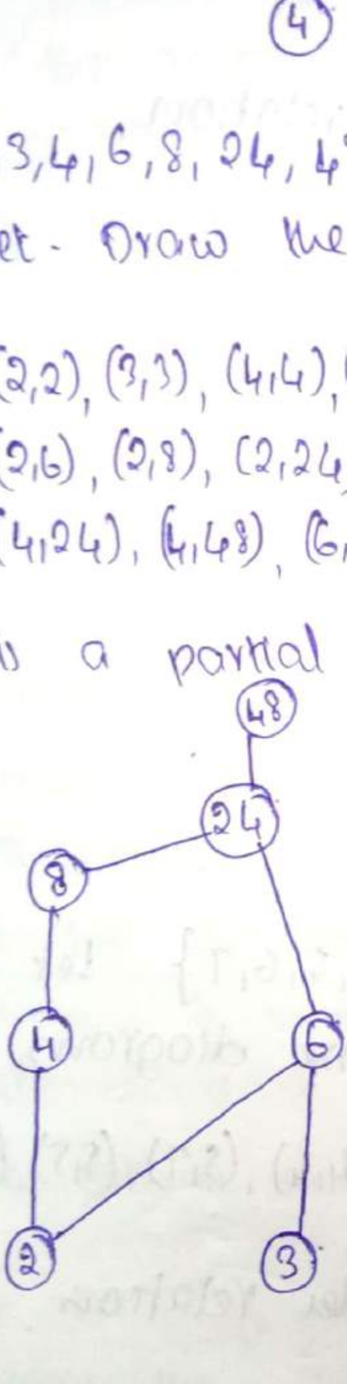
This is a partial order relation.

Hasse Diagram

? $A = \{2, 3, 4, 6, 8, 24, 48\}$ ordered by divisibility is a poset. Draw the Hasse diagram.

$R = \{(2,2), (3,3), (4,4), (6,6), (8,8), (24,24), (48,48), (2,4), (2,6), (2,8), (2,24), (2,48), (3,6), (3,24), (3,48), (4,8), (4,24), (4,48), (6,24), (8,24), (8,48), (24,48)\}$

This is a partial order relation.



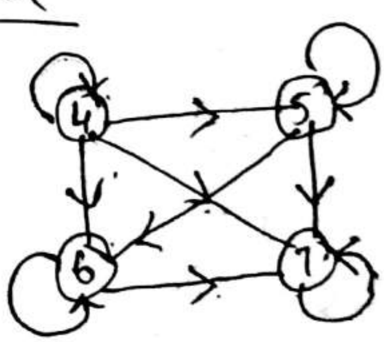
Procedure

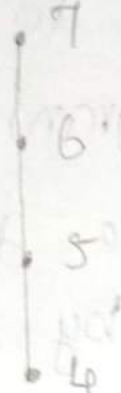
of a Relation to its equivalent Hasse Diagram.

1) The vertices in the Hasse diagrams are denoted by points rather than by circles.
2) Since a partial order relation is reflexive, each vertex must be related to itself. But in Hasse diagram these edges must be deleted.
3) A partial order is transitive. So in Hasse diagram, eliminate all the edges that are implied by the transitive property.
4) If a vertex 'a' is connected to vertex 'b' by an edge, then the vertex 'b' appears above the vertex 'a'. And therefore the arrows may be omitted in the Hasse diagram.

? Consider the set $A = \{4,5,6,7\}$ and let
$R = \{(4,5),(4,6),(4,7),(4,4),(5,5),(5,6),(5,7),(6,6),(6,7),(7,7)\}$
on A. Draw the directed graph & hence draw the Hasse diagram.

A. Directed Graph

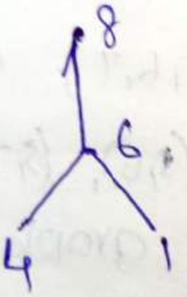




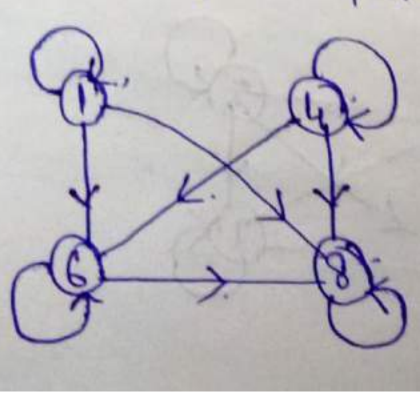
- Here we have deleted the loops in the directed graph, removed the arrows, the vertices are represented by dots and we have deleted the edges (4,7), (5,7) & (4,6) that resembles transitive property

? Draw the directed graph of the relation. Determined by the Hasse diagram defined on set A. A = {1,4,6,8} as shown below.

A.



R = {(4,4), (1,1), (6,6), (8,8), (4,6), (1,6), (6,8), (4,8), (1,8)}



Maximal Element

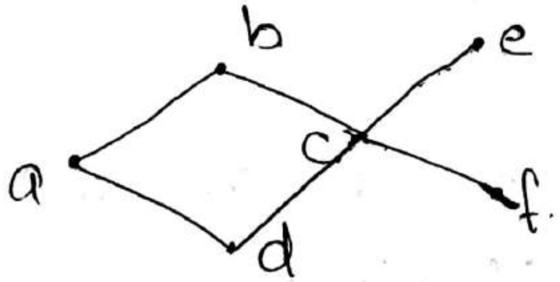
An element $x \in A$ is called a <u>maximal</u> element of A. If there is no element 'c' in A such that $x \leq c$ ($x \leq c \Rightarrow x$ is partially related to c)

Minimal Element

An element $y \in A$ is called a minimal element of A. If there is no element 'c' in A such that $c \leq y$

Remark:
There can be more that one maximal/minimal elements. It is not unique.

? Determine all the maximal & minimal elements of the poset shown by the Hasse diagram.



A. Here the maximal elements are b & e. and the minimal elements are d & f.

? Let $A = \{2, 3, 4, 6, 8, 24, 48\}$ with ordering divisibility. Determine all the maximal & minimal elements of A.

$\{2,4\}\ \{2,6\}\ \{2,8\}$ [illegible]

$\{4,8\}\ \{4,24\}\ \{4,48\}\ \{6,24\}\ \{6,48\}\ \{8,24\}\ \{8,48\}\ \{24,48\}$

Maximal: 48

Min: 2, 3

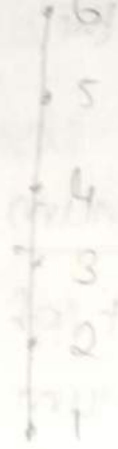
Greatest Element

An element $x \in A$ is called the greatest element of A if for all $y \in A$, $y \leq x$.

Least Element

An element $y \in A$ is called the least element of A if $\forall\ b \in A$, $y \leq b$.

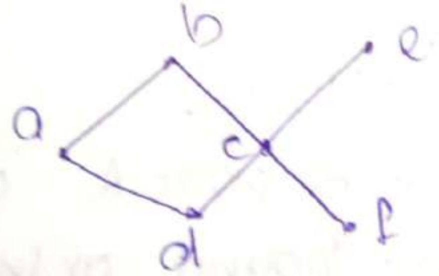
as below. find the greatest element & least element of A.



Greatest element = 6, least element = 1.

Remark :-

The greatest element & least element if they exist are unique.

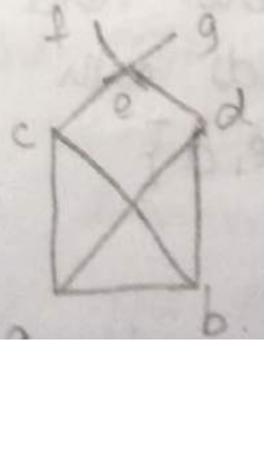


No greatest & least element since b & e are not related & d & f are not related.

Upper Bound

14/9/2021 Consider B be a subset of poset A. An element $x \in A$ is called an upper bound of B if $y \leq x, \forall y \in B$.

For ex:



Lower bound.

Consider B be a subset of the poset A an element $z \in A$ is called the lower bound of B, if $z \leq x \ \forall x \in B$

Least Upper Bound / Suprimum

Consider B be a subset of poset A. An element $x \in A$ is called a suprimum of B denoted by LUB(B) or Sup(B), if x is the upper bound of B and x' is any other upper bound of B then $x \leq x'$ [Supremum implies the least of all upper bounds]

Greatest Lower Bound / Infimum

Consider B be a subset of poset A. 'y' is said to be the greatest lower bound or infimum of B if y is the lower bound of B and if y' is any other lower bound of B then $y' \leq y$

[Infimum implies the greatest of all lower bounds]

Examples

Consider set $A = \{a, b, c, d, e, f, g\}$ The hasse diagram is given below. Find the upper bounds & lower bounds with their supremum & infimum for $B = \{c, e, d\}$

A. The upper bounds of B are e,f & g

$\therefore$ Sup(B) = e

Lower bounds of B = a,b

No infimum

? Determine the least. upper bound, infimum for the set B = {a,b,c} whose Hasse diagram is given below.

A. Least Upper bound of B ~~& Infimum~~

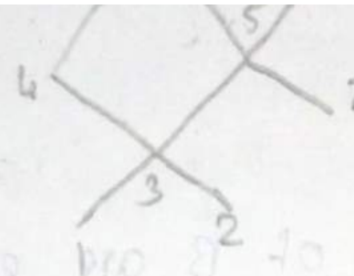
Upper bound of B = c,d,e

Sup(B) = C

Lower bound of B = k.

Infimum = k.

? Consider the poset A = {1,2,3,4,5,6,7,8} be ordered as below. B = {3,4,5}. Find the supremum & infimum



Upper bound is. 5, 6.

Sup (B) = 5

Lower bound = 3

LATTICES

A lattice is a poset in which every pair has a supremum & infimum

Join

Consider a poset L under the order ≤ Let a, b ∈ L. Then supremum of a & b is called join of a & b and is denoted by a⊕b or a∨b

Meet

Consider the poset L under the order ≤. Let a, b ∈ L. The infimum of a, b is called the meet of a & b is denoted by a∗b or a∧b.

Remark:

The lattice is denoted by (L, ∗, ⊕)

Permutations & Combinations

? How many variable names of 8 letters can be formed from the letters a, b, c, d, e, f, g, h, i without repeatation

A. This is a problem of permutation out of nine letters we have to select 8 letters without repeatation so the no: of permutations is given by ^nP_r where $n=9$ & $r=8$.

$$^9P_8 = \frac{9!}{(9-8)!} = \frac{9!}{1!} = \underline{\underline{9!}}$$

? There are 10 persons called on an interview each one is capable to be selected for the job. How many permutations are there to select 4 from 10.

A. Out of 10 people we have to select 4.

$\therefore$ No: of permutations $= {^{10}P_4} = \frac{10!}{6!} = \underline{\underline{5040}}$

? How many 6 digit numbers can be formed by using the digits 0, 1, 2, 3, 4, 5, 6, 7, 8. If every number is to start with 30. with no digit repeated.

A. Out of 9 numbers 30 is fixed ...

$\therefore n = 7$

For the selection of 6 digit number. Two numbers are already fixed and hence 4 numbers can only be selected $\therefore r = 4$.

$\therefore$ No:of permutations $= {}^7P_4 = \frac{7!}{3!} = \underline{\underline{840}}$

? How many permutations can be made out of the letter of the word 'COMPUTER'. How many of these

i) begin with C

ii) begin with C & end with R

iii) C & R occupy the end places

iv) end with R.

A. There are 8 letters in the word COMPUTER and all are distinct . $\therefore n = 8$

$\therefore$ Total no:of permutations $= 8!$

i) begin with C

In this case the first position is filled by the letter C & we can only arrange the remaining 7 letters & hence the number of permutations $= 1 \times 7!$

Here the first place is filled with C & last place is filled with R. So we can make the arrangements only for the remaining 6 letters. ∴ No:of permutations $= 1 \times 6! \times 1$

iii) C & R occupy the end places.

Here C & R occupy end places. Here the end places can be arranged either by C or R and the other places have to be arranged by the remaining 6 letters.

∴ No:of permutations $= 6!\ 2!$

? Determine the no:of permutations that can be made out of the letters of the word PROGRAMMING.

A. There are 11 letters in the word PROGRAMMING out of which G, M & R are two each

∴ No:of permutations $= \dfrac{11!}{2!\,2!\,2!} =$

? There are four blue 3 red & 2 black pens in the box which are drawn one

A. No: of Permutations $= \dfrac{9!}{4!\,3!\,2!}$

6/11/17

? How many 4 digit numbers can be formed by using the digits. 2, 4, 6, 8 when repeatation is allowed.

A. We have to make the 4 digit numbers were repeatation is allowed. So the no: of ways filling the unit's place. $= 4$

No: of filling the 10's place $= 4$

No: of filling the 100th place $= 4$

" " " 1000's place $= 4$

$\therefore$ Total no: of permutations $= 4 \times 4 \times 4 \times 4 = 256$.

? How many 2 digit even number can be formed. by using the digits. 1, 3, 4, 6, 8 when repeatation of digits are allowed.

A. In our given numbers three numbers are even & two numbers are odd. We are asked to form a 2 digit even number. $\therefore$ The no: of filling the unit's place $= 3$. & that of ten's place is 5

? In how many ways can the letters a, b, c, d, e, f be arranged in a circle

A. This is a problem of circular permutation

Here $n = 6$

$\therefore$ Total no: of permutations $= (6-1)! = 5!$

<u>Combination</u>

? How many 16 bit string are there containing exactly five zeros

A. This is a problem of combination because it is only told to have 5 zeros in the 16 bit string and were to put the zero is not given. $\therefore$ There no order for the arrangement.

$\therefore$ No: of combinations $= {}^{16}C_5 = \dfrac{16!}{5! \cdot (16-5)!}$

$= \dfrac{16!}{5!\ 11!} = \underline{\underline{4368}}.$

? From 10 programmers in how many ways can 5 be selected when

i) a particular programmer is included every time.

ii) a particular programmer is not included to select 5 is given by $^{10}C_5$

i) A particular programmer is always selected means we can select only 4 programmers from the remaining 9 programmers

$\therefore$ No:of combination $= {}^9C_4 = \dfrac{9!}{(9-4)!\,4!} = \underline{\underline{126.}}$

ii) A particular programmer is not included means we have to select 5 programmers out of 9 programmers.

$\therefore$ No:of combinations $= {}^9C_5 = \dfrac{9!}{5!\,(9-5)!} = \underline{\underline{126}}$

? Show that if any 4 members from 1 to 6 are choosen then 2 of them will add to 7

A We have given the numbers 1, 2, 3, 4, 5, 6. we have to choose any 4 numbers such that when we add 2 numbers of it we get a sum 7.

The 2 numbers whose sum is 7 are

$A = \{2,5\}$ $B = \{3,4\}$ $C = \{1,6\}$

$\therefore$ whenever we select the 4 numbers anyone of the set A, B or C will be

Hence the proof.

? Show that atleast 2 people must have their birthday in the same month if 13 people are assembled in a room. $n = 13$ $m = 12$ PHP

? Show that if 9 colours are used to paint 100 houses atleast 12 houses will be of the same colour. $n = 100$ $m = 9$ extended pigeonhole principle

Q. Out of 1200 students at a college. 582 took Economics 627 took English 563 to Mathematics. 217 took both Economics & English. 307 took both Economics & maths. 250 took both English & maths. 222 took all the courses. How many of them took none of these

A. Denote economics by A English by B & Mathematics by C.

Cardinality of,

$$|A| = 582.$$

$$|B| = 627$$

$$|C| = 543$$

$$|A \cap B| = 217$$

$$|A \cap C| = 307.$$

$$|B \cap C| = 250.$$

$$|A \cap B \cap C| = 222$$

We want to find the no:of students who have not take any of the courses. It can be found out by subtracting the no:of students who have taken any of the courses from the total no:of students.

have taken any of the courses.

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

$= 582 + 627 + 543 - 217 - 307 - 250 + 22.$

$= \underline{\underline{1200}}.$

$\therefore$ The no:of students who have not taken the courses $= 1200 - 1200 = 0$//

? Among 100 students, 32 study Maths, 20 study Physics, 45 Biology, 15 study Maths & Biology, 7 study Maths & Physics, 10 study Physics & Biology, 30 donot study any of the three subjects. Find the no:of students studying all the three subjects

A. Denote Maths by A, Physics. B, Biology C.

$|A| = 32.$ $\quad |A \cap C| = 15.$

$|B| = 20.$ $\quad |A \cap B| = 7$

$|C| = 45.$ $\quad |A \cap C| = 10.$

$|A \cup B \cup C| = 100 - 30$

$= \underline{70}$

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

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

$$= 70\cancel{100} - 32 - 20 - 65 + 15 + 7 + 10$$

$$= \underline{\underline{5}}$$

Review of Permutation & Combination

Definition

An ordered selection of r elements of a set containing n distinct elements is called an r-permutation of n elements and is denoted by $P(n,r)$ or ^nP_r, where $r \le n$.

An unordered selection of r elements of a set containing n distinct elements is called an r-combination of n elements and is denoted by $C(n,r)$ or ^nC_r or $\binom{n}{r}$.

Values of $P(n,r)$ & $C(n,r)$

1) The number of different permutations of n distinct objects taken r at a time, $r \le n$ is given by $\boxed{P(n,r) \text{ or } {}^nP_r = \frac{n!}{(n-r)!} = n(n-1)(n-2)\dots(n-r+1)}$

2) The number of permutations of n things taken all at a time is $n!$.

(ie) $\boxed{P(n,n) = n!}$

which n_1 identical objects, n_2 identical objects, ..., n_k identical objects, when all are taken at a time is given by

$$\boxed{\frac{n!}{n_1!\, n_2! \dots n_k!}}$$

4) The circular permutation are the permutations in which the objects are placed in a circle. The number of circular permutations of n different objects is $\boxed{(n-1)!}$.

5) The number of combinations of n different things taken r at a time is given by,

$$\boxed{nC_r = \frac{n!}{r!\,(n-r)!}, \quad 1 \le r \le n}$$

6) The number of combinations of n things taken all at a time is 1. (ie) $\boxed{nC_n = 1}$

7) The number of combinations of n things taken none at a time is 1 (ie) $\boxed{nC_0 = 1}$

Statement

If n pigeon's are accomodated in m pigeon holes and $n>m$, then atleast one pigion hole will contain two or more pigeons.

Proof:

Let the n pigeons be labelled $P_1, P_2, \dots, P_n$ and m pigeon holes be labelled $H_1, H_2, \dots, H_m$.

If $P_1, P_2, \dots, P_m$ are accomodated in to $H_1, H_2, \dots, H_m$ respectively, then we are left with $(n-m)$ pigeons $P_{m+1}, P_{m+2}, \dots, P_n$.

If these left over pigeons are accomodated to the m pigeon holes $H_1, H_2, \dots, H_m$ again in any random manner, then atleast one pigeon hole will contain two or more pigeons.

Hence proved.

Note:) Extended Pigeon Hole Principle

If n pigeons are accomodated in m pigeonholes and $m<n$, then one of the pigeon hole must contain atleast $\left[\frac{n-1}{m}\right]+1$ pigeons, where $[x]$ denotes the greatest integer less ~~that~~ than or equal to x, where x is a real number.

Principle of Inclusion - Exclusion

(1) If A and B are two finite sets on a Universe U, then $\boxed{|A \cup B| = |A| + |B| - |A \cap B|}$, where $|A|$ denotes the cardinality of A.

(2) If A and B are finite disjoint sets, then

$$\boxed{|A \cup B| = |A| + |B|}$$

(3) If A, B, C are the three finite sets, then

$$\boxed{|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|}$$

∴ In general,

Let $P_1, P_2, \ldots, P_n$ are finite sets, then

$$|P_1 \cup P_2 \cup \ldots \cup P_n| = \sum_{i=1}^{n} |P_i| - \sum_{1 \le i < j \le n} |P_i \cap P_j| + \sum_{1 \le i < j < k \le n} |P_i \cap P_j \cap P_k| + \ldots + (-1)^{n-1} |P_1 \cap P_2 \cap \ldots \cap P_n|$$

A recurrence relation is a functional relation between the independent variable x, dependent variable $f(x)$ and the difference of various order of $f(x)$.

A recurrence relation is also called a <u>difference equation</u>.

<u>eg:</u>) The equation $f(x+3h)+3f(x+2h)+6f(x+h)+9f(x)=0$.

It can also be written as

$$a_{n+3}+3a_{n+2}+6a_{n+1}+9a_n=0. \text{ or}$$

$$y_{n+3}+3y_{n+2}+6y_{n+1}+9y_n=0.$$

For <u>eg:</u>) The Fibonacci sequence is defined by the recurrence relation $a_n = a_{n-2}+a_{n-1}, n \geq 2$ with initial conditions $a_0 = 1, a_1 = 1$.

<u>Order of the Recurrence Relation</u>

The order of the recurrence relation is defined to be the difference between the highest and lowest subscripts of $f(x)$ or a_n or y_n.

<u>eg:</u>) The eq^n. $13a_n + 20a_{n-1} = 0$.

Here, the highest order subscript is n and lowest order subscript is $n-1$

difference is $n-(n-1) = n-n+1 = 1$.

$\therefore$ eq^n is a first order recurrence relation.

can be written as $8a_n + 4a_{n+1} + 8a_{n+2} = K(x)$

$\therefore$ Highest subscript value $= n+2$

Lowest subscript value $= n$.

difference $= n+2-n = 2$//

$\therefore$ The given eq^n. is second order recurrence relation.

Degree of the Recurrence Relation

The degree of the recurrence relation is defined to be the highest power of $f(x)$ or a_n or y_n.

1) The eq^n. $y_{n+3}^{3} + 2y_{n+2}^{2} + 2y_{n+1} = 0$. has degree 3,

Since highest power of y_{n+3} is 3.

The eq^n. $a_n^4 + 3a_{n-1}^3 + 6a_{n-2}^2 + 4a_{n-3} = 0$

has degree 4, since highest power of a_n is 4

The eq^n. $y_{n+3} + 2y_{n+2} + 4y_{n+1} + 2y_n = K(x)$

has degree 1 and have order $n+3-n = 3$//

D) Linear Recurrence relation with Constant coefficients.- -

A recurrence relation is called linear, if its degree is one.

general form of linear recurrence relation with constant coefficients is

$$c_0 y_{n+r} + c_1 y_{n+r-1} + c_2 y_{n+r-2} + \cdots + c_n y_n = R(n)$$

where $c_0, c_1, c_2, \ldots, c_n$ are constants and $R(n)$ is a function of independent variable n.

Particular solution

(a) Homogeneous Linear Difference Equations

We can find the particular solution of the difference equation, when the equation is of homogeneous linear type by putting the values of the initial conditions in the homogeneous solution.

(1)

Solution of linear homogeneous recurrence relation with constant coefficients :-

Consider,

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} = 0 \quad \text{—} (1), \; c_k \neq 0$$

which is the general form of l.h. recu relation with const. coefficients of order k.

put $a_n = r^n$ $(r \neq 0)$ in equ. (1). Then,

$$c_0 r^n + c_1 r^{n-1} + c_2 r^{n-2} + \dots + c_k r^{n-k} = 0$$

$$\Rightarrow r^{n-k}\left[c_0 r^k + c_1 r^{k-1} + c_2 r^{k-2} + \dots + c_k\right] = 0$$

$$\Rightarrow c_0 r^k + c_1 r^{k-1} + c_2 r^{k-2} + \dots + c_k = 0, \text{ since } r \neq 0 \quad (2)$$

This equ. (2) is called characteristic equ. and the roots of the char equ. are called char. roots.

To find $a_n^{(P)}$

To find $a_n^{(P)}$ (i.e. particular solution) we make use of the 'method of undetermined coefficients'. The following table gives certain forms of $f(n)$ and corresponding choice for $a_n^{(P)}$.

(ii)

Notes

① If $f(n)$ is a linear combination of terms in the 1st column, then $a_n^{(P)}$ is assumed as linear combination of the corresponding terms in the 2nd column.

2 If $f(n) = r^n$ or $(A+Bn)r^n$, where 'r' is a non repeated characteristic root, then $a_n^{(P)}$ is assumed as Anr^n or $n(A+Bn)r^n$.

3) If $f(n) = r^n$, where 'r' is a twice repeated char. root then $a_n^{(P)}$ is taken as An^2r^n and so on

Solution for homogeneous Recurrence Relation with Constant Coefficients

Consider,

$C_0 a_n + C_1 a_{n-1} + C_2 a_{n-2} + \dots + C_k a_{n-k} = 0 \longrightarrow ①$, $C_k \neq 0$.

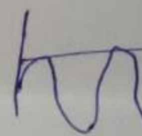
steps for finding solutions:-

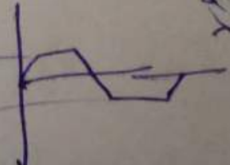
1] Put the unknown variable $a_n = r^n (r \neq 0)$ in equation ①.

2] Find the characteristic equation

3] Find the characteristic roots.

4] write the solution in the general form according to the cases.





Q) Solve $a_n - 6a_{n-1} + 8a_{n-2} = 0$.

A) Given, $a_n - 6a_{n-1} + 8a_{n-2} = 0 \longrightarrow ①$

Put $a_n = r^n$ in ①, $(r \neq 0)$

$\therefore$ ① becomes,

$r^n - 6r^{n-1} + 8r^{n-2} = 0$ [subscript will become the power of r in each term]

Taking the lowest power of r outside, we have

$r^{n-2}[r^2 - 6r + 8] = 0$.

$\longrightarrow r^2 - 6r + 8 = 0$, [Since $r \neq 0 \Rightarrow r^{n-2} \neq 0 \Rightarrow \frac{0}{r^{n-2}} = 0$]

$$r = \frac{6 \pm \sqrt{36-32}}{2}$$

$$= \frac{6 \pm \sqrt{4}}{2} = \frac{6+2}{2}, \frac{6-2}{2}$$

$$= \frac{8}{2}, \frac{4}{2}.$$

$$= 4, 2.$$

$\therefore$ The characteristic roots, $r_1 = 4$ and $r_2 = 2$.

$\therefore$ The general solution is,

$a_n^{(h)} = C_1 4^n + C_2 2^n$ [since r_1 & r_2 are distinct roots].

Q) solve $9y_{K+2} - 6y_{K+1} + y_K = 0$

A) Given $9y_{K+2} - 6y_{K+1} + y_K = 0 \longrightarrow ①$

Put $y_K = r^K$, where $r \neq 0$, in ① ~~[According~~ $\rightarrow ②$ ~~in the given equation~~,

[~~According~~ to the variable ~~Put~~ eq^n. ②]

$\therefore$ ① becomes,

$$9r^{K+2} - 6r^{K+1} + r^K = 0.$$

$$r^K[9r^2 - 6r + 1] = 0$$

$\therefore 9r^2 - 6r + 1 = 0$ is the characteristic equation.

$$= \frac{6 \pm \sqrt{0}}{18} = \frac{6}{18} = \frac{1}{3}, \frac{1}{3}$$ [Since eq^n. is quadratic, it must have 2 roots].

$\therefore r_1 = 1/3$ & $r_2 = 1/3$

Since the roots are equal, the general solution is

$$y_K^{(h)} = [C_1 + C_2 K](1/3)^K.$$

Q) Solve the recurrence relation,

$$a_n = 2(a_{n-1} - a_{n-2}).$$

A) 1st write in the general equation form,

(ie) $a_n = 2a_{n-1} - 2a_{n-2}$

$\Rightarrow a_n - 2a_{n-1} + 2a_{n-2} = 0. \longrightarrow (1)$

Put $a_n = r^n, (r \neq 0)$ in (1).

(1) becomes,

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

$$r^{n-2}[r^2 - 2r + 2] = 0.$$

$\therefore r^2 - 2r + 2 = 0$ is the characteristic equation.

$$r = \frac{2 \pm \sqrt{4 \ldots}}{2}$$

$$= \frac{2 \pm \sqrt{-4}}{2} = \frac{2 \pm 2i}{2}$$

$$= 1 \pm i.$$

J Jose.
Qun Con

$\therefore r_1 = 1+i$ and $r_2 = 1-i$ are complex roots.

$\therefore$ The general solution is,

$$a_n^{(h)} = c_1 (1+i)^n + c_2 (1-i)^n.$$

Particular solution in homogeneous recurrence relation

Step 1) Find the general solution of homogeneous recurrence relation as above.

Step 2) Apply the conditions given the problem to find out the constant values in the general solution.

Step 3) Substitute the constants in the general solution and then the solution is called particular solution.

Q) Solve $a_{n+2} + 4a_{n+1} + 4a_n = 0, n \geq 0, a_0 = 1, a_1 = 2$.

A) $a_{n+2} + 4a_{n+1} + 4a_n = 0 \rightarrow (1)$

Put $a_n = r^n$ in (1), $(r \neq 0)$

$$r^{n+2} + 4r^{n+1} + 4r^{n} = 0.$$

$$r^{n}\left[r^{2} + 4r + 4\right] = 0$$

$\therefore$ $r^2 + 4r + 4 = 0$ is the characteristic equation.

$\therefore$ $r = \dfrac{-4 \pm \sqrt{16-16}}{2} = \dfrac{-4}{2} = -2, -2$ are equal roots.

$\therefore$ General solⁿ. is given by,

$$a_n^{(h)} = (C_1 + C_2 n)(-2)^n \longrightarrow (2)$$

Given $a_0 = 1 \Longrightarrow$ when $n=0$, $a_n = 1$.
$a_1 = 2 \Longrightarrow$ when $n=1$, $a_n = 2$. $\Big\} \longrightarrow (3)$

$\therefore$ Applying (3) in (2), we have

$\underline{n=0}$ $a_0 = (C_1 + C_2 \times 0)(-2)^0$

$\Longrightarrow 1 = C_1 \times 1 \longrightarrow \boxed{C_1 = 1}$

$\underline{n=1}$

$a_1 = (C_1 + C_2 \times 1)(-2)^1$

$\Longrightarrow 2 = (C_1 + C_2) - 2$

$\Longrightarrow 2 = -2C_1 - 2C_2.$

$\Longrightarrow C_1 + C_2 = -1$ [Dividing throughout by -2]

$\Longrightarrow 1 + C_2 = -1$ [Since $C_1 = 1$]

$\Longrightarrow C_2 = -1 - 1 = -2$

$\Longrightarrow \boxed{C_2 = -2}$

Sub. the value of c_1 & c_2 in (2),

$a_n^{(h)} = (1-2n)(-2)^n$ is the particular solution.

Q) Solve $a_r - 7a_{r-1} + 10a_{r-2} = 0$ with $a_0 = 0, a_1 = 6$.

A) $a_r - 7a_{r-1} + 10a_{r-2} = 0 \longrightarrow (1)$

Put $a_r = k^r$, $k \neq 0$, in (1)

$k^r - 7k^{r-1} + 10k^{r-2} = 0$

$k^{r-2}\left[k^2 - 7k + 10\right] = 0$

$\therefore k^2 - 7k + 10 = 0$ is the characteristic equation.

$\therefore k = \dfrac{7 \pm \sqrt{49-40}}{2} = \dfrac{7 \pm \sqrt{9}}{2}$

$= \dfrac{7 \pm 3}{2} = \dfrac{7+3}{2}, \dfrac{7-3}{2}$

$= \dfrac{4}{2}, \dfrac{10}{2} = 2, 5$ are distinct roots.

$\therefore$ The general solution is given by,

$a_r^{(h)} = c_1 2^r + c_2 5^r \longrightarrow (2)$.

given, $a_0 = 0$ & $a_1 = 6 \longrightarrow (3)$

sub. (3) in (2), we have

$\underline{r=0}$ $\quad a_0 = c_1 2^0 + c_2 5^0$ $\qquad$ $\underline{r=1}$ $\quad a_1 = c_1 2^1 + c_2 5^1$

$\Rightarrow 0 = c_1 + c_2$ $\qquad$ $\Rightarrow 6 = 2c_1 + 5c_2$.

$\Rightarrow c_1 = -c_2$.

$$-2C_2 + 5C_2 = 6$$

$$3C_2 = 6$$

$$\boxed{C_2 = 2}$$

Sub. $C_2 = 2$ in $C_1 = -C_2$

$$\Longrightarrow \boxed{C_1 = -2}$$

$\therefore$ Sub. C_1 & C_2 in ②, we have

$a_r^{(h)} = -2 \cdot 2^r + 2 \cdot 5^r$ is the particular solution.

Solution of non-homogeneous recurrence relation with constant coefficients.

eq^n is of the form,

$C_0 a_n + C_1 a_{n-1} + C_2 a_{n-2} + \dots + C_n a_{n-k} = f(n) \rightarrow ①$ where

$f(n) \neq 0$, $C_k \neq 0$

General sol^n. of eq^n. ① is

$$a_n = a_n^{(h)} + a_n^{(P)},$$

where $a_n^{(h)}$ is the general solution of homogeneous recurrence relation and $a_n^{(P)}$ is the particular solution of non-homogeneous recurrence relation.

Method of finding a_n

To find $a_n^{(P)}$ (Particular solution of non-homogeneo

Step 1) write the general form ~~of~~ from the choice of $a_n^{(P)}$ from the below table corresponding to given $f(n)$ in ①.

$f(n)$	Choice of $a_n^{(P)}$
Z, Z is constant	A
Z^r, Z is constant	$A \cdot Z^r$
$P(r)$, a polynomial of degree n	$A_0 r^n + A_1 r^{n-1} + \dots + A_n$
$Z^r \cdot P(r)$, $P(r)$ polynomial of degree n & z constant	$(A_0 r^n + A_1 r^{n-1} + \dots + A_n) Z^r$

2) $F(n) = r^n$, non repeated.

$F(n) = 2^r$.

3) $F(n) = r^n$, r repeated

$A\, n^2 r^n$

General soln

$a_n = a_n^{(h)} + a_n^{(p)}$

→ To Find a_n

$a_n - 2a_{n-1} = 0$.

Remark:

① If $f(n)$ is a linear combination of terms in the 1st column, ~~then~~ (e)[eg. $2^n + 3$], then $a_n^{(P)}$ is assumed as linear combination of the corresponding terms in the 2nd column.

for eg:- Suppose $f(n) = 2^n + 3$, then the corresponding choice of ~~(an)~~ $a_n^{(P)}$ is $A \cdot 2^n + A$.

characteristic roots, then $a_n^{(p)}$ is assumed as Anr^n or $n(A+Bn)r^n$.

③ If $f(n) = r^n$, where 'r' is a twice repeated characteristic roots, then $a_n^{(p)}$ is taken as An^2r^n.

If $f(n) = r^n$, where 'r' is repeated thrice, then $a_n^{(p)}$ is taken as An^3r^n and so on.

Q) Solve $a_n - 2a_{n-1} = 3^n$, $a_1 = 5$.

A) $a_n - 2a_{n-1} = 3^n \longrightarrow ①$

The general solution for the non-homogeneous recurrence relation is

$$a_n = a_n^{(h)} + a_n^{(p)} \longrightarrow ②$$

~~Consider the~~

To find $a_n^{(h)}$

Consider the homogeneous equation from ①,

(ie) $a_n - 2a_{n-1} = 0 \longrightarrow ③$

Put $a_n = r^n$ in ③ [Proceed as in homogeneous form]

~~Sub this~~

$\therefore$ ③ becomes, $r^n - 2r^{n-1} = 0$

$r - 2 = 0$ is the characteristic equation

$\therefore r = 2$ is the characteristic root.

$\therefore a_n^{(h)} = c_1 2^n \longrightarrow (4)$

To find $a_n^{(P)}$

~~from~~ Since R.H.S of (1) is $f(n) = 3^n$ and since 3 is not a characteristic root, we can get the corresponding particular solution from the table.

$\therefore$ The choice of $a_n^{(P)} = A \cdot 3^n \rightarrow (5)$

sub. the choice in (1), we have

$A \cdot 3^n - 2A\, 3^{n-1} = 3^n$ [Power of 3 depends on subscripts]

$\cancel{A\, 3^{n-1}[3-2] = 3^n}$

$\Rightarrow 2A\, 3^{n-1} = 3^n$

$\Rightarrow 2A = \dfrac{3^n}{3^{n-1}} \Rightarrow 2A = 3^n \cdot 3^{-(n-1)}$

$\Rightarrow 2A = 3^{n-n+1}$

$\Rightarrow 2A = 3$

$\Rightarrow A = 3/2$

Taking 3^n outside,

$3^n \left[A - 2A \cdot \tfrac{1}{3}\right] = 3^n$

$\therefore$ ~~$A - 6A = 0 + $~~

$\Rightarrow$ " $\overline{\quad 3}$

$\Rightarrow 3A - 2A = 3$

$\Rightarrow \boxed{A = 3.}$

Sub. $A=3$ in eqⁿ. 5,

$a_n^{(P)} = 3 \cdot 3^n = 3^{n+1}. \longrightarrow 6$

Sub. 4 & 6 in 2, we have

$a_n = C_1 2^n + 3^{n+1} \longrightarrow 7.$

Given $a_1 = 5$.

(ie) $n=1$

$a_1 = C_1 2^1 + 3^{1+1}$

$\Rightarrow 5 = 2C_1 + 9$

$\Rightarrow 2C_1 = -9 + 5 = -4$

$\Rightarrow 2C_1 = -4$

$\Rightarrow C_1 = -2.$

Sub. $C_1 = -2$ in 7, we have

$a_n = -2 \cdot 2^n + 3^{n+1}$

(ie) $a_n = 3^{n+1} - 2^{n+1}$.

A) The general form is

$$a_n - 2a_{n-1} = 2^n \longrightarrow (1).$$

General solution is,

$$a_n = a_n^{(h)} + a_n^{(P)} \longrightarrow (2).$$

<u>To find $a_n^{(h)}$</u>

The homogeneous equation of (1) is

$$a_n - 2a_{n-1} = 0. \longrightarrow (3)$$

Put $a_n = r^n, (r \neq 0)$ in (3),

(3) becomes

$$r^n - 2r^{n-1} = 0$$

$$r^{n-1}[r-2] = 0$$

$\Longrightarrow r-2=0$ is the characteristic equation.

$\therefore r=2$ is the characteristic root.

$$\therefore a_n^{(h)} = c_1 2^n. \longrightarrow (4)$$

<u>To find $a_n^{(P)}$</u>

Since R.H.S of (1) is 2^n, but 2 is the characteristic root of (1) and hence the corresponding choice of $a_n^{(P)}$ will be $An2^n$. [refer Remark 2]

$$\therefore a_n^{(P)} = An2^n \longrightarrow (5)$$

~~Sub (5) in~~

$$An2^n - 2A(n-1)2^{n-1} = 2^n \Rightarrow An2^n - A(n-1)2 = 2$$

Taking 2^n outside,

$$\cancel{2^n\left[An - 2An \cdot \tfrac{1}{2}\right] = 2^n}$$

$$\cancel{\Rightarrow nA - nA = 1}$$

$$2^n\left[An - A(n-1)\right] = 2^n$$

$$An - An + A = 1$$

$$A = 1$$

$\therefore$ 5 becomes $a_n^{(p)} = n2^n \rightarrow$ 6

$\therefore$ sub. 4 & 6 in 2,

$$a_n = c_1 2^n + n2^n \rightarrow 7$$

Given $a_0 = 2$,

$n = 0$

$$a_0 = c_1 2^0 + 0 \times 2^0$$

$$2 = c_1$$

Sub. $c_1 = 2$ in 7, we have

$$a_n = 2 \cdot 2^n + n2^n$$

$$a_n = 2^{n+1} + n2^n = 2^n(2+n)$$

4) Solve $a_{n+2} - 6a_{n+1} + 9a_n = 3\cdot 2^n + 7\cdot 3^n$, $n \geq 0$

A) Given, $a_{n+2} - 6a_{n+1} + 9a_n = 3\cdot 2^n + 7\cdot 3^n \longrightarrow (1)$

The general solution of (1) is

$$a_n = a_n^{(h)} + a_n^{(p)} \longrightarrow (2)$$

To find $a_n^{(h)}$

The homogeneous equation of (1) is,

$$a_{n+2} - 6a_{n+1} + 9a_n = 0 \longrightarrow (3)$$

Put $a_n = r^n \ (r \neq 0)$ in (3)

(3) becomes,

$$r^{n+2} - 6r^{n+1} + 9r^n = 0$$

$$r^n\left[r^2 - 6r + 9\right] = 0$$

$r^2 - 6r + 9 = 0$ is the characteristic equation.

$$r = \frac{6 \pm \sqrt{36-36}}{2} = \frac{6}{2} = 3, 3.$$

$$\therefore a_n^{(h)} = (C_1 + C_2 n)3^n \longrightarrow (4)$$

To find $a_n^{(p)}$

R.H.S of (1) is $3\cdot 2^n + 7\cdot 3^n$.

Corresponding to $3\cdot 2^n$, we can assume $a_n^{(p)}$ as $A_0 \cdot 2^n$. (table)

Corresponding to $7\cdot 3^n$, we can assume $a_n^{(p)}$ as $A_1 n^2 3^n$ [refer Remark 3] sub ⑤ in ①,

~~$a_{n+2} - 6a_{n+1} + 9a_n = A_0 2^n + A_1 n^2 3^n$~~

$$A_0 2^{n+2} + A_1 (n+2)^2 3^{n+2} - 6\left[A_0 2^{n+1} + A_1 (n+1)^2 3^{n+1}\right] + 9\left[A_0 2^n + A_1 n^2 3^n\right] = 3\cdot 2^n + 7\cdot 3^n$$

(i) $$A_0 2^{n+2} + A_1 (n+2)^2 3^{n+2} - 6A_0 2^{n+1} - 6A_1 (n+1)^2 3^{n+1} + 9A_0 2^n + 9A_1 n^2 3^n = 3\cdot 2^n + 7\cdot 3^n$$

(ii) $$2^n\left[A_0 2^2 - 6A_0\cdot 2 + 9A_0\right] + 3^n\left[A_1 (n+2)^2\cdot 3^2 - 6A_1 (n+1)^2 3 + 9A_1 n^2\right] = 3\cdot 2^n + 7\cdot 3^n$$

equating the coefficients of 2^n,

$$4A_0 - 12A_0 + 9A_0 = 3 \longrightarrow ⑥$$

equating the coefficients of 3^n,

$$9A_1 (n+2)^2 - 18A_1 (n+1)^2 + 9A_1 n^2 = 7 \longrightarrow ⑦$$

$\underline{A_0 = 3}$ &

$$9A_1 (n^2 + 4n + 4) - 18A_1 (n^2 + 2n + 1) + 9A_1 n^2 = 7$$

$$9A_1 n^2 + 36A_1 n + 36A_1 - 18A_1 n^2 - 36A_1 n - 18A_1 + 9A_1 n^2 = 7$$

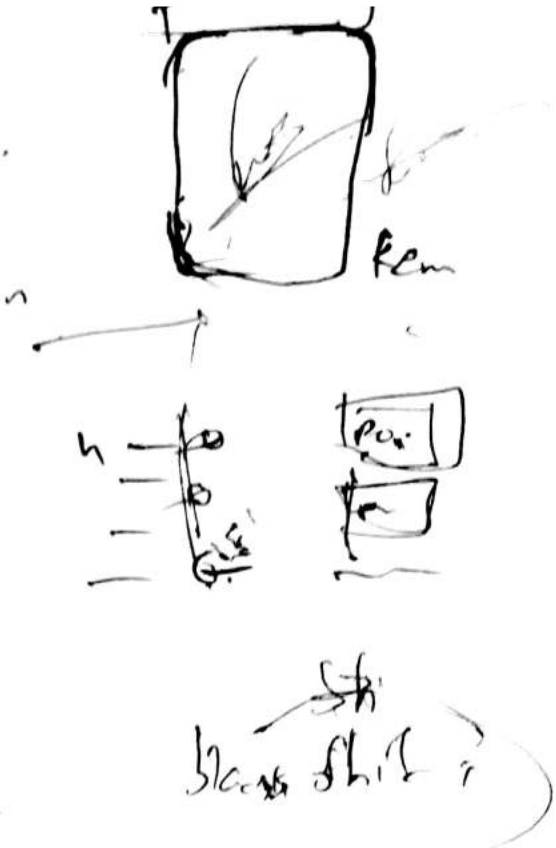
$$18A_1 = 7$$

$$\underline{A_1 = 7/18}$$

∴ Sub. in ⑤, we have $\underline{a_n^{(P)} = 3\cdot 2^n + \frac{7}{18} n^2 3^n} \longrightarrow ⑧$.

Sub. (1) & (2) in (1),

$a_n = (C_1 + C_2 n) 2^n + 3 \cdot 2^n + \frac{7}{18} 3^n \cdot n.$



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

LHS $= (A-B) - C$

$x \in [(A-B) - C]$

$x \in A \quad x \notin B \quad x \notin C$

$\Rightarrow x \in A \quad x \notin B$ or C

$x \in A \quad x \notin B \cup C$

$(A-B) - C \subset A - (B \cup C)$

RHS: $x \in [A-(B \cup C)]$

$x \in A \quad x \notin (B \cup C)$

Definition:-

If G is a nonempty set and $\circ$ is a binary operation on G, then $(G,\circ)$ is called a group, if the following conditions are satisfied:-

1) for all $a,b \in G$, $a \circ b \in G$ (Closure property)
2) for all $a,b,c \in G$, $a\circ(b \circ c) = (a \circ b)\circ c$ (Associative property)
3) There exist $e \in G$ with $a \circ e = e \circ a = a$, for all $a \in G$. (Existence of identity)
4) For each $a \in G$, there is an element $b \in G$ such that $a \circ b = b \circ a = e$. (Existence of Inverse).

Note:- If together with the above 4 conditions, ~~if for a,b∈~~ if $(G,\circ)$ satisfies the property, for all $a,b \in G$, $a \circ b = b \circ a$ (Commutative property), then G is called Commutative or abelian group.

Q) P.T the set Q of all rational numbers ~~other than~~ with operation defined by $a \circ b = a + b - ab$ constitutes an abelian group?

A) To S.T $(Q,\circ)$ is ~~by~~ an abelian group, it should satisfy the conditions.

Let $a, b \in Q$, then

$a \circ b = a+b-ab$ is also rational number

(ie) $a \circ b \in Q$.

$\therefore$ closure property is satisfied.

② Associativity

Let $a, b, c \in Q$, then we have to P.T

$a \circ (b \circ c) = (a \circ b) \circ c$.

$$
\begin{aligned}
L.H.S &= a \circ (b \circ c) \\
&= a \circ [b+c-bc] \\
&= a + [b+c-bc] - a[b+c-bc] \\
&= a+b+c-bc-ab-ac+abc \rightarrow ①
\end{aligned}
$$

$$
\begin{aligned}
R.H.S &= (a \circ b) \circ c \\
&= (a+b-ab) \circ c \\
&= (a+b-ab)+c-(a+b-ab)c \\
&= a+b-ab+c-ac-bc+abc \\
&= a+b+c-bc-ab-ac+abc \rightarrow ②
\end{aligned}
$$

from ① & ②,

$a \circ (b \circ c) = (a \circ b) \circ c$.

Hence Associativity holds.

Let $e \in Q$ be the identity and ~~let q~~
we have to S.T $a \circ e = a$. [e should be determined]
(by definition)

~~$a \circ e = a + e - ae$~~

~~$= a + e(1-a)$~~

(ie) $a \circ e = a$

$\Rightarrow a + e - ae = a$, by definition of $a \circ b$.

$\Rightarrow e(1-a) = a - a = 0$

$\Rightarrow e = \frac{0}{1-a} = 0 \in Q$.

Hence the identity exists.

④ Existence of Inverse

Let $a \in Q$, we have to find an element $b \in Q$ such that $a \circ b = e$

(ie) $a \circ b = 0$ [since $e = 0$]

$\Rightarrow a + b - ab = 0$

$\Rightarrow$ ~~$a(1-b) = -b$~~ $a + b(1-a) = 0$

$\Rightarrow b = \frac{-a}{1-a} = \frac{a}{a-1} \in Q$.

$\therefore$ the inverse of a (arbitrary) exist in Q.

$\therefore (Q, \circ)$ is group.

Also $(Q, \circ)$ to be an abelian group, it should

(ii) for $a, b \in Q$. we have to S.T $a \circ b = b \circ a$.

$L.H.S = a \circ b$

$= a + b - ab \rightarrow (3)$

$R.H.S = b \circ a$

$= b + a - ba \rightarrow (4)$

$\therefore a \circ b = b \circ a$.

$\therefore$ Commutative property holds.

$\therefore (Q, \circ)$ is an abelian group.

Remark:-

1) $(Z, +) \rightarrow$ set of integers with binary operation addition.

$(R, +) \rightarrow$ Set of real numbers with binary operation addition.

$(Q, +) \rightarrow$ set of rational numbers with binary operation addition

These are all abelian groups.

2) $(Z, \cdot) \rightarrow$ set of integers with binary operation multiplication

This is not a ~~m~~ group, since no ~~multip~~ inverse exist in Z.

(*) $a * b$ can be also denoted by ab in a group $(G, *)$.

... each $a \in \mathbb{Z}$ is divided by n.

(ii) $\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$ ~~fro~~ eg: $\mathbb{Z}_3 = \{0, 1, 2\}$

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

4) Addition modulo n denoted by $+_n$ is the remainder obtained when $a+b$ is divided by n.

5) Multiplication modulo n denoted by $\times_n$ is the remainder obtained when $a \cdot b$ is divided by n.

~~Properties of gro~~

~~Proporto~~

eg: The set of $n \times n$ non singular matrices $\boxed{|A| \neq 0}$ is a group under matrix multiplication with identity matrix of order n as the identity. This group is not abelian because matrix multiplication is not commutative. eg: $A = \begin{bmatrix} 2 & 4 \\ 3 & 2 \end{bmatrix}$ $|A| = -8 \neq 0$ non singular.

Order of a Group

For every group G, the number of elements in G is called the order of G. This is denoted by $|(G, *)|$ or $O(G)$.

When the number of elements in a group is not finite, we say that G has infinite order.

eg: $|(\mathbb{Z}, +)|$ has infinite order.

$|(\mathbb{Z}_n, +_n)|$ has finite order.

Theorem 1) For every group $(G,*)$, P.T

ⓐ the identity of G is unique.

ⓑ the inverse of each element of G is unique.

ⓒ If $a,b,c \in G$ & $ab = ac$, then $b = c$
(left cancellation property)

ⓓ If $a,b,c \in G$ & $ba = ca$, then $b = c$.
(right cancellation property).

Proof:

ⓐ If possible, let e_1 and e_2 be two identity elements of $(G,*)$. (ie) $e_1, e_2 \in G$. We have to P.T $e_1 = e_2$.

By definition, since e_1 is an identity

$\Longrightarrow \forall a \in G, \; a * e_1 = a = e_1 * a$.

In particular, let $a = e_2 \in G$, then the above definition can be rewritten as,

$$e_2 * e_1 = e_2 = e_1 * e_2 \longrightarrow (1)$$

Since e_2 is an identity,

$\Longrightarrow \forall a \in G, \; a * e_2 = a = e_2 * a$.

In particular, let $a = e_1 \in G$, then the above definition can be rewritten as,

$$e_1 * e_2 = e_1 = e_2 * e_1 \longrightarrow (2)$$

From (1) and (2), we have $e_1 = e_2$.

$\therefore$ The identity of G is unique.

If possible, let a' and a'' be two inverses of $a \in G$. Then by definition, we have

$$a * a' = e = a' * a \rightarrow ①$$

so, $$a * a'' = e = a'' * a \rightarrow ②$$

Now we have to P.T $a' = a''$.

$\therefore a' = a' * e$ (since e is the identity for $a' \in G$.)

$= a' * (a * a'')$, from ②.

$= (a' * a) * a''$, by Associtivity property.

$= e * a''$, by ①.

$= a''$, ($\because e$ is the identity)

$\therefore a' = a''$.

$\therefore$ The inverse of each element of G is unique.

ⓒ Given $a, b, c \in G$ and $ab = ac$.

We have to P.T $b = c$.

$ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$, (multiplication by a^{-1} on both sides and a^{-1} is the inverse of a)

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$, by Associativity.

$\Rightarrow eb = ec$, (Since e is the identity & by definition of inverse)

$\Rightarrow b = c$, (by definition of identity).

(a) given ...

we have to P.T $b = c$.

~~$ba = ba$~~

$ba = ca \Rightarrow (ba)a^{-1} = (ca)a^{-1}$, [multiplication by a^{-1} on both sides and a^{-1} is the inverse of a]

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$, Associativity.

$\Rightarrow be = ce$, [by definition of inverse & e is the identity]

$\Rightarrow b = c$, by definition of identity.

Theorem 2| For every group $(G, *)$, P.T

~~(a) $(a^{-1})^{-1} = a$, $\forall a \in G$~~

(a) $(ab)^{-1} = b^{-1}a^{-1}$, $\forall a, b \in G$.

Proof.

(a) Let $a^{-1} = b$. ~~for $a, b \in G$~~

Then ~~by definition of inverse, we have~~

~~$a * b = e = b * a$.~~

(a) we have to P.T $(ab)^{-1} = b^{-1}a^{-1}$. $\forall a, b \in G$.

(ii) we have to P.T the inverse of ab is $b^{-1}a^{-1}$.

or it is enough if we P.T $(ab)(b^{-1}a^{-1}) = e$, the identity.

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$, Associativity

$= a e a^{-1}$, $(\because bb^{-1} = e)$

$= a a^{-1}$, $(\because ae = a)$

$\therefore (ab)(b^{-1}a^{-1}) = e$

$\Rightarrow$ the inverse of ab is $b^{-1}a^{-1}$.

$$\Rightarrow (ab)^{-1} = b^{-1}a^{-1}.$$

Theorem 3| The group $(G,*)$ cannot have an idempotent element except the identity element.

Proof.

[According to idempotent law, $\forall a \in G$, $a*a = a$]

We have to S.T $(G,*)$ cannot have any other idempotent element other than e.

If possible, let a be an idempotent element of $(G,*)$ other than e.

Then $a*a = a$, (by idempotent law) — ①

Now, $e = a*a^{-1}$

$= (a*a)*a^{-1}$, by ①

$= a*(a*a^{-1})$, by Associativity

$= a*e$

$= a$.

$\therefore e = a$.

Hence the only idempotent element of G is its identity element.

For an abelian group, $(ab)^n = a^n b^n$ any
$n(a+b) = na + nb$, $\forall a, b \in G$ and
n is any integer.

Q) Show that any group G is abelian iff $(ab)^2 = a^2b^2$, for all $a, b \in G$.

A) Given that G is abelian.
we have to P.T $(ab)^2 = a^2b^2$.

$$(ab)^2 = (ab)(ab)$$
$$= a(ba)b, \text{ (Associativity)}.$$
$$= a(ab)b, \text{ (abelian)}$$
$$= (aa)(bb), \text{ (Associativity)}.$$
$$= a^2b^2.$$

Conversely, Suppose $(ab)^2 = a^2b^2$.
we have P.T G is abelian.
(ie) we have to P.T $ab = ba, \forall a, b \in G$.

~~$(ab)^2 = (ab)(ab)$~~

$$(ab)^2 = a^2b^2 \Rightarrow (ab)(ab) = (aa)(bb)$$
$$\Rightarrow a(ba)b = a(ab)b, \text{ Associativity}$$
$$\Rightarrow (ba)b = (ab)b, \text{ by left Cancellation}.$$
$$\Rightarrow ba = ab, \text{ by right cancellation}$$
$$\Rightarrow G \text{ is abelian}.$$

P.T $(Z_6, +_6)$ is an abelian group!

i) We have $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

The Composition table is given by,

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

From, the table,

Closure property is attained.

Associative property holds.

Identity element is 0

The inverse of each element is given below,

inverse of 0 is 0
inverse of 1 is 5
inverse of 2 is 4
inverse of 3 is 3
inverse of 4 is 2
inverse of 5 is 1.

Hence $(Z_6, +_6)$ is a group.

Since rows & columns of the table are transpose to each other, $(Z_6, +_6)$ satisfies commutative property.

Subgroups

Let $(G, *)$ be a group and $H \subseteq G$ be a non-empty subset of G.

If H is a group under the binary operation of G, then we call H a subgroup of G.

Trivial subgroup

Every group G has $\{e\}$ and G as subgroups. These are called trivial subgroups of G.

All other subgroups are called nontrivial or proper subgroups.

Q) Let G be the set of integers and H be the set of even integers.
S.T $(H, +)$ is a subgroup of $(G, +)$
or H is a subgroup of G.

A) clearly H is a non empty subset of G.
Next to prove H is a subgroup of G, it is enough if we p.T H is a group under addition.

closure property

~~Every even~~ Addition of even integers always given an even integer.
Hence closure property is satisfied.

$\forall\ a, b, c \in H$, set of even integers,

$a+(b+c) = (a+b)+c$.

$\therefore$ Associativity holds.

<u>Existence of Identity</u>

let $a \in H$., then we have to find an identity element in H under addition and that must be the identity of G.

~~$a * e = a$~~ $\quad a + e = a$

$\Rightarrow e = a - a = 0$.

$e = 0$ is also the identity of G.

Hence identity exists in H.

<u>Existence of Inverse</u>

Let $a \in H$ and 0 is the identity of H.

Then $\quad a + a^{-1} = 0$

$\therefore a^{-1} = -a \in H$.

$\therefore$ Inverse exists H.

$\therefore (H, +)$ is a group

$\therefore$ H is a subgroup of G.

If H is a non-empty sub... then H is a subgroup of G if and only if
(a) for all $a, b \in H$, $ab \in H$ (closure property)
(b) for all $a \in H$, $a^{-1} \in H$. (Existence of Inverse).

Proof

Given that, H is a non-empty subset of group G.
Suppose that H is a subgroup of G.
∴ we have to P.T the above mentioned two conditions are holding.
Since H is a subgroup of G, by definition of subgroup, H is a group under the same binary operation.
Hence it satisfies all the group conditions, including the two mentioned here.

~~Conversely~~ Conversely,
let the two conditions are holding.
we have to P.T H is a subgroup of G.
According to definition, ~~~~ we have to P.T,
(1) H is a non-empty subset of G
(2) H is a group under the same binary operation in G

- H is a non-empty subset of G is already given as hypothesis.
- by (a), closure property is attained.

~~For Associativity~~

since G is a group, $a*(b*c) = (a*b)*c$ in G

and hence $a*(b*c) = (a*b)*c$ in H.

$\therefore$ Associativity holds in H.

- as $H \neq \phi$, let $a \in H$, by (b), $a^{-1} \in H$ and hence inverse exist in H.

Also by (a), we have $a a^{-1} \in H$

$\implies e \in H$

$\therefore$ H has the identity element.

$\therefore$ H is a group.

$\therefore$ H is a subgroup of G.

Theorem 5| Let $(G, \circ)$ and $(H, *)$ be groups. Define the binary operation $\cdot$ on $G \times H$ by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2).$$

Then P.T $(G \times H, \cdot)$ is a group.

Proof

Given that $(G, \circ)$ and $(H, *)$ are groups.

we have to S.T $(G \times H, \cdot)$ is a group

(ie) it is enough to S.T $(G \times H, \cdot)$ satisfies all the four properties.

let (g_1,h_1) and $(g_2,h_2) \in G \times H$.

we have to P.T $(g_1,h_1) \cdot (g_2,h_2) \in G \times H$.

$g_1, g_2 \in G \Rightarrow g_1 \circ g_2 \in G \rightarrow ①$, Since $(G, \circ)$ is a group.

$h_1, h_2 \in H \Rightarrow h_1 * h_2 \in H \rightarrow ②$, Since $(H, *)$ is a group.

From ① & ②, we have

$(g_1 \circ g_2, h_1 * h_2) \in G \times H$.

$\Longrightarrow (g_1,h_1) \cdot (g_2,h_2) \in G \times H$ [by definition of $\cdot$]

$\therefore$ closure property is attained.

② Associative Property

let (g_1,h_1), (g_2,h_2) & (g_3,h_3) belongs to $G \times H$.

We have to P.T

$$[(g_1,h_1) \cdot (g_2,h_2)] \cdot (g_3,h_3) = (g_1,h_1) \cdot [(g_2,h_2) \cdot (g_3,h_3)]$$

$$L.H.S = [(g_1,h_1) \cdot (g_2,h_2)] \cdot (g_3,h_3)$$

$$= (g_1 \circ g_2, h_1 * h_2) \cdot (g_3,h_3)$$

$$= (g_1 \circ g_2 \circ g_3, h_1 * h_2 * h_3) \rightarrow ①$$

~~Since $g_1 \circ g_2 \circ g_3 \in G$ & $h_1 * h_2 * h_3 \in H$~~

$$R.H.S = (g_1,h_1) \cdot [(g_2,h_2) \cdot (g_3,h_3)]$$

$$= (g_1,h_1) \cdot [(g_2 \circ g_3, h_2 * h_3)]$$

$$= (g_1 \circ g_2 \circ g_3, h_1 * h_2 * h_3) \rightarrow ②.$$

$$[(g_1, h_1) \cdot (g_2, h_2)] \cdot (g_3, h_3)$$
$$= (g_1, h_1) \cdot [(g_2, h_2) \cdot (g_3, h_3)].$$

$\therefore$ Associativity holds.

③ Existence of Identity

Let e_G be the identity of $(G, \circ)$ &
Let e_H be the identity of $(H, *)$.
let $(g, h) \in G \times H$, where $g \in G$ & $h \in H$.

$$(g, h) \cdot (e_G, e_H) = (g \circ e_G, h * e_H)$$
$$= (g, h).$$

Also,
$$(e_G, e_H) \cdot (g, h) = (e_G \circ g, e_H * h)$$
$$= (g, h)$$

$\therefore (e_G, e_H) \in G \times H$ is the identity element.

④ Existence of Inverse

Since $(G, \circ)$ is a group, for every $g \in G$, there exist a $g^{-1} \in G$ such that $g \circ g^{-1} = e_G = g^{-1} \circ g$.

Since $(H, *)$ is a group, for every $h \in H$, there exist a $h^{-1} \in H$ such that $h * h^{-1} = e_H = h^{-1} * h$.

Now,
$$(g, h) \cdot (g^{-1}, h^{-1}) = (g \circ g^{-1}, h * h^{-1})$$
$$= (e_G, e_H)$$

$(g^{-1}, h^{-1}) \cdot (g, h) = (\ldots$

$= (e_G, e_H)$

Thus, $(g^{-1}, h^{-1}) \in G \times H$ is the inverse of (g, h).

Hence $(G \times H, \cdot)$ is a group.

Remark: The group $(G \times H, \cdot)$ defined above is called a direct product of G & H.

Q) Consider the groups $(Z_2, +_2)$ and $(Z_3, +_3)$.
S.T ~~$(Z_2 \times Z_3, \cdot)$~~ $(Z_2 \times Z_3, \cdot)$ is group, where $\cdot$ is defined as $(a_1, b_1) \cdot (a_2, b_2) = (a_1 +_2 a_2, b_1 +_3 b_2)$, where $a_1, a_2 \in Z_2$ & $b_1, b_2 \in Z_3$.

A) $Z_2 = \{0, 1\}$, $Z_3 = \{0, 1, 2\}$

$Z_2 \times Z_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$.

The Composition Table is given by,

$\cdot$	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1).

closure property is satisfied.
Associative property is satisfied.
The identity element is (0,0).
The inverse of each element is as follows:-

inverse of (0,0) is (0,0)
inverse of (0,1) is (0,2)
inverse of (0,2) is (0,1)
inverse of (1,0) is (1,0)
inverse of (1,1) is (1,2).
inverse of (1,2) is (1,1).

$\therefore [(Z_2 \times Z_3), \cdot]$ is a group.

Q) If G is a group, let $H = \{a \in G \mid ag = ga, \forall g \in G\}$.
P.T H is a subgroup of G.

A) By theorem 4, to prove that H is a subgroup, we need only to prove the closure property and inverse existence in H.

To prove H is closed

let $a_1, a_2 \in H$, we have to P.T $a_1 * a_2 \in H$.

$a_1 \in H \Rightarrow a_1 g = g a_1$, by def^n. of H & $g \in G$.

$a_2 \in H \Rightarrow a_2 g = g a_2$, by def^n. of H & $g \in G$.

$$(a_1 a_2) g = g(a_1 a_2).$$

$$(a_1 a_2) g = a_1 (a_2 g)$$

$= a_1 (g a_2)$, $\because a_2 \in H$.

$= (a_1 g) a_2$, $\because$ Associativity

$= (g a_1) a_2$, $\because a_1 \in H$

$= g(a_1 \cdot a_2)$, Associativity

~~$= (a_1 a_2) g$, commutativity~~.

~~$= a_1 a_2$, by right cancellation~~

$\therefore (a_1 a_2) g = g(a_1 \cdot a_2)$

$\Rightarrow (a_1 a_2) \in H$.

$\therefore$ H is closed or satisfies closure property.

<u>To prove H posses inverse</u>

Let $a \in H$, then $ag = ga$, $\forall g \in G$, by definition of H. Since G is a group, for $g \in G$, $\exists\ g^{-1} \in G$ s.t. $gg^{-1} = e$, identity of G.

We have to P.T $a^{-1} \in H$.
(ie) by definition we have to P.T $a^{-1} g = g a^{-1}$.

$a \in H \Rightarrow a g^{-1} = g^{-1} a \Rightarrow (a g^{-1})^{-1} = (g^{-1} a)^{-1}$

$\Rightarrow (g^{-1})^{-1} a^{-1} = a^{-1} (g^{-1})^{-1}$

$\Rightarrow g a^{-1} = a^{-1} g \Rightarrow a^{-1} \in H.$

7) what is the order of the group $Z_6 \times Z_6 \times Z_6$?
Determine the inverse of $(2,3,4),(4,0,2)$ & $(5,1,2)$?

A) $O(Z_6) = 6 \quad \because Z_6 = \{0,1,2,3,4,5\}$.

$\therefore O(Z_6 \times Z_6 \times Z_6) = O(Z_6) \times O(Z_6) \times O(Z_6)$

$= 6 \times 6 \times 6$

$= \underline{216}$

$(2,3,4)^{-1} = (4,3,2) \left[\because \begin{array}{l} 2 +_6 4 = 0 \\ 3 +_6 3 = 0 \\ 4 +_6 2 = 0 \end{array}\right]$

$(4,0,2)^{-1} = (2,0,4)$

$(5,1,2)^{-1} = (1,5,4)$

8) a) if H, K are subgroups of group G, P.T $H \cap K$ is also a subgroup of G.

b) Give an example of a group G with subgroups H, K such that $H \cup K$ is not a subgroup of G.

1) a) given that H and K are subgroups of G.
Then H is closed and inverse exists
IIIly K is closed & inverse exists
since H is closed and K closed
$\Rightarrow H \cap K$ is closed.

Homomorphisms & Isomorphisms

Defⁿ: If $(G,\circ)$ & $(H,*)$ are groups, and $f: G \to H$ be a function.
Then f is called group homomorphism, if ~~for~~ all $a, b \in G$, $f(a \circ b) = f(a) * f(b)$.

Theorem 6)

Let $(G,\circ)$ & $(H,*)$ be groups with respective identities e_G & e_H. If $f: G \to H$ is a homomorphism, then

(a) $f(e_G) = e_H$

(b) $f(a^{-1}) = [f(a)]^{-1}$, $\forall a \in G$.

(c) $f(a^n) = [f(a)]^n$, $\forall a \in G$, and all $n \in \mathbb{Z}$.

(d) $f(S)$ is a subgroup of H, for each subgroup S of G.

Proof:

Given that $(G,\circ)$ and $(H,*)$ be groups.
and $e_G \in G$ be the identity of G &
$e_H \in H$ be the identity of ~~H~~.
If $e_G \in G$ then ~~f(G)~~ $f(e_G) \in H$, Since $f: G \to H$.

(a) $e_H * f(e_G) = f(e_G)$, since $e_H, f(e_G) \in H$ & ~~H is a group~~ $(H,*)$ is a group with identity e_H

$= f(e_G \circ e_G)$, since $e_G \in G$ and e_G is identity $(G,\circ)$

$= f(e_G) * f(e_G)$, Since f is a homomorphism

$= f(e_G)$, by right cancellation.

$f(a) * f(a^{-1}) = f(a \circ a^{-1})$, since f is homomorphism

$= f(e_G)$, since e_G is the identity of $(G, \circ)$

$= e_H$, by ⓐ.

$\therefore f(a) * f(a^{-1}) = e_H$

$\Rightarrow f(a)$ has the inverse $f(a^{-1})$.

$\Rightarrow [f(a)]^{-1} = f(a^{-1})$

ⓒ To prove this, we use the method of induction.

For $n=1$, $f(a^1) = [f(a)]^1$

$\Rightarrow f(a) = f(a)$, the result is true.

Assume the result is true for $n-1$.

(ie) $f(a^{n-1}) = [f(a)]^{n-1}$

Now, we will prove that the result is true for n.

(ie) we have to P.T $f(a^n) = [f(a)]^n$.

$\therefore f(a^n) = f(a^{n-1} \circ a)$

$= f(a^{n-1}) * f(a)$, since f is homomorphism

$= [f(a)]^{n-1} * [f(a)]^1$, by assumption

$= [f(a)]^n$.

and hence $f(S) \neq \phi$.

Now we have to P.T $f(S)$ is a subgroup of H.

by thm 4, we have to P.T $f(S)$ is closed and the inverse exists in H.

To P.T $f(S)$ is closed in H.

let $x, y \in f(S)$, then ~~$x*y \in f(S)$~~. we have to P.T $x * y \in f(S)$.

$x, y \in f(S)$, then $x = f(a)$ and $y = f(b)$, where $a, b \in S$.

Since S is a subgroup of G, $a, b \in S \Rightarrow a \circ b \in S$.

$x * y = f(a) * f(b) = f(a \circ b)$, $\because f$ is homomorphism

$\in f(S)$.

$\therefore f(S)$ is closed.

To P.T $f(S)$ posses inverse

let $x \in f(S)$, then we P.T $x^{-1} \in f(S)$.

$x^{-1} = [f(a)]^{-1} = f(a^{-1})$, by (c) and $a \in S$.

$\in f(S)$, Since $a \in S$ and S subgroup, hence $a^{-1} \in S$.

$\therefore$ Inverse exists in $f(S)$.

$\therefore f(S)$ is a subgroup of H.

If $f:(G,\circ)\rightarrow(H,*)$ is a homomorphism, we call f an isomorphism if it is one-to-one and onto. In this case, G & H are said to be isomorphic groups.

Cyclic groups

A group G is called cyclic if there is an element $x \in G$ such that for each $a \in G$, $a = x^n$, for some $n \in \mathbb{Z}$.
($a = nx$, if the operation is addition)
Then x is known as the generator of G and is denoted by $G = \langle x \rangle$

Q) S.T the group $(Z_4, +)$ is cyclic.
A) To show that the group $(Z_4, +)$ is cyclic, we have to find atleast one generator for Z_4 under $+_4$ (means $+_4$).
[Since $(Z_4, +)$ is given to be group, no need for checking group].
Since addition, the generator will be that element $x \in Z_4$ that generators the entire set $Z_4 = \{0, 1, 2, 3\}$ using $a = nx$, n is an integer.

The possible ...

consider 0:

$1 \cdot 0 = 0$

$2 \cdot 0 = 0 +_4 0 = 0$

$\vdots$

$\therefore$ 0 is not a generator.

Consider 2

$1 \cdot 2 = 2$

$2 \cdot 2 = 2 +_4 2 = 0$

$3 \cdot 2 = 2 +_4 2 +_4 2 = 2.$

$4 \cdot 2 = 2 +_4 2 +_4 2 +_4 2 = 0.$

$\vdots$

$\therefore$ 2 is not a generator.

Consider 1

$1 \cdot 1 = 1$

$2 \cdot 1 = 1 +_4 1 = 2$

$3 \cdot 1 = 1 +_4 1 +_4 1 = 3$

$4 \cdot 1 = 1 +_4 1 +_4 1 +_4 1 = 0$

$\therefore$ 1 is ~~the~~ a generator.

consider 3

$1 \cdot 3 = 3$

$2 \cdot 3 = 3 +_4 3 = 2$

$3 \cdot 3 = 3 +_4 3 +_4 3 = 1$

$4 \cdot 3 = 3 +_4 3 +_4 3 +_4 3 = 0$

$\therefore$ 3 is a generator

$\therefore$ The only generators of $(\mathbb{Z}_4, +_4)$ is 1 & 3.

$\therefore (\mathbb{Z}_4, +_4) = \langle 1 \rangle = \langle 3 \rangle.$

$\therefore (\mathbb{Z}_4, +_4)$ is a cyclic group.

Definition

If G is a group, & $a \in G$, the order of the element, a denoted by $O(a)$ ~~or $|\langle a \rangle|$~~ is the smallest positive integer n for which $a^n = e$.

($na = e$ in the case of additive operation).

group generated ...

Q) write ~~is~~ the order of elements of the ~~set~~ group $(w_4, \cdot)$

A) $w_4 = \{1, -1, i, -i\}$.

~~First~~ The order of the element is the smallest positive integer n s.t. $a^n = 1$ (identity of w_4), $a \in w_4$.

Consider 1

$1^1 = 1$

$\therefore O(1) = 1$

~~consider -1~~

consider -1

$(-1)^1 = -1$

$(-1)^2 = 1$

$\therefore O(-1) = 2$.

consider i

$i^1 = i$

$i^2 = -1$

$i^3 = -i$

$i^4 = 1$

$\therefore O(i) = 4$

consider $-i$

$(-i)^1 = -i$

$(-i)^2 = -1$

$(-i)^3 = i$

$(-i)^4 = 1$

$\therefore O(-i) = 4$.

$\therefore O(1) = 1$

$O(-1) = 2$

$O(i) = 4$

$O(-i) = 4$

the elements of Z_4.

A) $Z_4 = \{0, 1, 2, 3\}$.

The identity element is 0.

$\therefore$ The order is the ~~ka~~ least positive integer such that $na = 0$, $a \in Z_4$.

Consider 0

$1 \cdot 0 = 0$

~~$\therefore$ order 0~~

$\therefore O(0) = 1$

Consider 1

$1 \cdot 1 = 1$

$2 \cdot 1 = 1 +_4 1 = 2$

$3 \cdot 1 = 1 +_4 1 +_4 1 = 3$

$4 \cdot 1 = 1 +_4 1 +_4 1 +_4 1 = 0$

$\therefore O(1) = 4$

~~Consider 2~~

~~$2 \cdot 1 = 2$~~

~~$3 \cdot 1$~~

Consider 2

$1 \cdot 2 = 2$

$2 \cdot 2 = 2 +_4 2 = 0$

$\therefore O(2) = 2$

Consider 3

$1 \cdot 3 = 3$

$2 \cdot 3 = 3 +_4 3 = 2$

$3 \cdot 3 = 3 +_4 3 +_4 3 = 1$

$4 \cdot 3 = 3 +_4 3 +_4 3 +_4 3 = 0$

$\therefore O(3) = 4$.

$\therefore$ order of the elements of $(Z_4, +_4)$ are

$O(0) = 1$; $O(1) = 4$; $O(2) = 2$; $O(3) = 4$.

~~Of2~~

Note:

If $|\langle a \rangle|$ is infinite, we say that a has infinite order.

Every subgroup ~~of a~~ cyclic ~~group~~ is cyclic.

Theorem

A cyclic group is abelian.

Proof.

Let $(G,*)$ be a cyclic group with $a \in G$ as generator.
Let $b, c \in G$, we have to P.T $b*c = c*b$.

Since $b \in G \Rightarrow b = a^n$ &
$c \in G \Rightarrow c = a^m$. $\Big\} \rightarrow (1)$

$b*c = a^n * a^m$, by (1)

$= a^{n+m}$

$= a^{m+n} = a^m \cdot a^n = c*b$.

$\therefore b*c = c*b$.

$\therefore G$ is abelian

Remark:-

1) Every subgroup of a cyclic group is cyclic
2) If 'a' is a generator of a cyclic group, $\{G,*\}$, then ~~a~~ 'a^{-1}' is also a generator of $\{G,*\}$.
3) An abelian group need not be cyclic. ~~Since~~

Cosets & Lagrange's theorem

Definition:-

If H is a subgroup of G, then for each $a \in G$, the set $aH = \{ah \mid h \in H\}$ is called the left coset of H in G. The set $Ha = \{ha \mid h \in H\}$ is called the right coset of H in G.

If the operation is addition, we write $a+H = \{a+h \mid h \in H\}$ is the left coset of H in G and $H+a = \{h+a \mid h \in H\}$ is the right coset of H in G.

Remark:-

For an abelian group, $aH = Ha$.
(i.e) left coset = right coset).

Q) Let $(\mathbb{Z},+)$ and its subgroup $(3\mathbb{Z},+)$.
Find the left & right cosets of $3\mathbb{Z}$ in $\mathbb{Z}$?

~~A) The left cosets~~

A) we have,

$$\mathbb{Z} = \{\ldots, -3,-2,-1,0,1,2,3,\ldots\}$$

$$3\mathbb{Z} = \{\ldots, -9,-6,-3,0,3,6,9,\ldots\}.$$

The left cosets of $(3\mathbb{Z},+)$ in $(\mathbb{Z},+)$ are

$$0+3\mathbb{Z} = \{\ldots, -9,-6,-3,0,3,6,9,\ldots\}$$

$$1+3\mathbb{Z} = \{\ldots, -8,-5,-2,1,4,7,10,\ldots\}$$

~~$2+3\mathbb{Z} = \{\ldots, -6,-3,0,3,6,9,12,\ldots\}$~~

$$2+3\mathbb{Z} = \{\ldots, -7,-4,-1,2,5,8,11,\ldots\}$$

Thus we can see that $0+3\mathbb{Z}$, $1+3\mathbb{Z}$ and $2+3\mathbb{Z}$ are the distinct left cosets of $3\mathbb{Z}$ in $\mathbb{Z}$.

The right cosets are,

$3\mathbb{Z}+0 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$3\mathbb{Z}+1 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$

$3\mathbb{Z}+2 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$

$3\mathbb{Z}+3 = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} = 3\mathbb{Z}+0.$

$\therefore$ The distinct right cosets are

$3\mathbb{Z}+0$, $3\mathbb{Z}+1$ and $3\mathbb{Z}+2$.

Remark:

From the above problem, we can see that the union of distinct (left) or right cosets gives the entire set $\mathbb{Z}$.

(ie) $\mathbb{Z} = (0+3\mathbb{Z}) \cup (1+3\mathbb{Z}) \cup (2+3\mathbb{Z})$

Illly, the intersection of distinct left or right cosets is empty.

(ie) $(0+3\mathbb{Z}) \cap (1+3\mathbb{Z}) \cap (2+3\mathbb{Z}) = \phi$.

Thus we can say that "the set of all left (right) cosets of a ~~subgroup~~ subgroup H in G forms a Partition of G.

If G is a finite group of order n with H a subgroup of order m, then m divides n.

or

The order of a subgroup H of a finite group G is a divisor of the order of the group G.

Proof.

Given $|G| = n$. & $|H| = m$.

If $H = G$, then the result follows.

Otherwise, if $H \subset G$, (ie) $m < n$ $[O(H) \leq O(G)]$

Then there exist an element $a \in G$ but not in H.

(ie) $a \in G - H$.

Since $a \notin H$, it follows that $aH \neq H$.

which implies $aH \cap H = \phi$.

If $G = aH \cup H$, then $|G| = |aH| + |H|. = m + m = 2m = 2|H|$

(ie) $|G| = 2|H| \Rightarrow |G|$ is a multiple of $|H|$.

$\Rightarrow |H|$ divides $|G|$

$\Rightarrow m$ divides n.

$\therefore$ The theorem follows.

If not, (ie) $G \neq aH \cup H$.

$\Rightarrow$ There exist an element $b \in G - (H \cup aH)$, with $bH \cap H = \phi = bH \cap aH$ and $|bH| = |H|$.

If $G = bH \cup aH \cup H$, then $|G| = |bH| + |aH| + |H| = 3m = 3|H|$ ~~$= 3m = 3|H|$.~~

(ie) $|G|$ is a multiple of $|H|$.

(ie) $|H|$ divides $|G|$.

otherwise, we are back to an element $c \in G$ with $c \notin bH \cup aH \cup H$. ~~the~~ and proceeds as above.

Since the group G is finite, this process terminat

and we find that $G = a_1H \cup a_2H \cup \cdots \cup a_KH$.

$\therefore |G| = K|H|$.

$\therefore$ $|G|$ is a multiple of $|H|$.

$\therefore$ $|H|$ divides $|G|$

(i.e) m divides n.

Corollary 1:) If G is a finite group & $a \in G$, then $O(a)$ divides $|G|$.

Corollary 2:) Every group of prime order is cyclic.

- A Binary operation on a set A is a ...
- In general, n-ary operation on A is a function f from $\underbrace{A \times A \times \cdots \times A}_{n \text{ times}} \to A$. (i.e.) $f: A^n \to A$.
- A set A is said to be **closed** with respect to an operation, if applying the operation on members of A always produce another member of A.
- An algebraic system or algebraic structure is a System consisting of a non-empty set A and one or more n-ary operations on the set A. It is denoted by $(A, f_1, f_2, \ldots, f_n)$, where $f_1, f_2, \ldots, f_n$ are the operations on A.
- Homomorphisms & Isomorphisms

Let $(X, \cdot)$ & $(Y, *)$ be two algebraic system where $\cdot$ & $*$ are both n-ary operations.
A function $f: X \to Y$ is called a homomorphism from $(X, \cdot)$ to $(Y, *)$, if for any $x_1, x_2 \in X$, we have

$$f(x_1 \cdot x_2) = f(x_1) * f(x_2).$$

A homomorphism is known as isomorphism if f is onto & one-to-one. ~~or~~
If between two algebraic systems $(X, \cdot)$ & $(Y, *)$ an isomorphism exists, then $(X, \cdot)$ & $(Y, *)$ are said to be isomorphic and then the two algebraic systems are structurally indistinguishable.

Q) Consider the set $A = \{1,2,3\}$ and a binary operation $*$ on the set A defined by $a*b = 2a+2b$. Represent the operation $*$ as a table on A.

A) Given $A = \{1,2,3\}$ & $a*b = 2a+2b$.

*	1	2	3
1	4	6	8
2	6	8	10
3	8	10	12

$1*1 = 2\times1+2\times1 = 4$
$1*2 = 2\times1+2\times2 = 6$
$1*3 = 2\times1+2\times3 = 8$
$2*1 = 4+2 = 6$
$2*2 = 4+4 = 8$
$2*3 = 4+6 = 10$
$3*1 = 6+2 = 8$
$3*2 = 6+4 = 10$
$3*3 = 6+6 = 12$

This table is also known as Composition Table.

Closure Property

) Consider the set $A = \{-1,0,1\}$. Determine whether A is closed under ① Addition ② multiplication.

A) ① Here $(-1)+(-1) = -2 \notin A$

Hence A is not closed under addition.

② $-1\times-1 = 1 \in A$. $\quad 0\times0 = 0 \in A \quad 1\times1 = 1 \in A$
$-1\times0 = 0 \in A \quad 0\times-1 = 0 \in A \quad 1\times-1 = -1 \in A$
$-1\times1 = -1 \in A \quad 0\times-1 = 0 \in A \quad 1\times0 = 0 \in A$.

$\therefore$ A is closed under multiplication.

W.

Q) Consider the set $A = \{1,3,5,7,9,\ldots\}$, the set of odd +ve integers. Determine whether A is closed under ① addition ② Multiplication.

Hence A is not closed under addition.

(2) The set A is closed under multiplication because multiplication of two odd numbers gives an odd number.

Associative Property

Consider a non-empty set A and a binary operation $*$ on A. Then $*$ on A is associative, if for every $a, b, c \in A$, $(a*b)*c = a*(b*c)$.

Q) Consider the binary operation $*$ on Q, the set of rational no.'s, defined by

$a*b = a+b-ab, \forall a,b \in Q$.

Determine whether $*$ is associative.

A) Let $a, b, c \in Q$; then we have to P.T

$(a*b)*c = a*(b*c)$

$L.H.S = (a*b)*c$

$= (a+b-ab)*c$, by def^n. of $*$

$= (a+b-ab) + c - (a+b-ab)c$

$= a+b-ab+c-ac-bc+abc$

$= a+b+c-ab-ac-bc+abc \rightarrow (1)$

$R.H.S = a*(b*c)$

$= a*(b+c-bc)$

$= a+b+c-bc-a(b+c-bc)$.

$= a+b+c-ab-ac-bc+abc \rightarrow ②$

From ① & ②,

$(a*b)*c = a*(b*c), \forall a,b,c \in Q.$

Q.
) Consider the binary operation * & Q, the set of rational no.'s defined by $a*b = \frac{ab}{2}, \forall a,b \in Q.$
Determine Associativity?.

) Let $a,b,c \in Q.$

$L.H.S = (a*b)*c = \left(\frac{ab}{2}\right)*c$

$= \frac{abc}{4} \rightarrow ①$

$R.H.S = a*(b*c) = a*\left(\frac{bc}{2}\right) = \frac{abc}{4} \rightarrow ②$

From ① & ②, $a*(b*c) = (a*b)*c.$

Commutative Property

Consider a non-empty set A and a binary operation * on A. Then * on A is commutative, if $\forall a,b \in A, a*b = b*a.$

) Consider the binary operation * on Q, set of rational numbers defined by $a*b = a^2+b^2, \forall a,b \in Q.$
Determine Commutivity?

Check $a*b = b*a$.

~~L.H.S~~ $a*b = a^2+b^2 = b^2+a^2 = b*a$.

$\therefore$ Commutativity holds.

Identity

Consider a non-empty set A and a binary operation $*$ on A. Then the operation $*$ has an identity property, if there exist an element e in A such that
$a*e$ (right identity) $= a =$ $e*a$ (left identity), $\forall a \in A$.

Q) Consider the binary operation $*$ on I_+, the set of positive integers defined by $a*b = \frac{ab}{2}$
Determine the identity for the binary operation $*$, if exists.

A) Let assume $a \in I_+$ and e be any +ve ~~no.~~ integer, then we have to find e s.t. $a*e = a$.

By def^n. $a*e = a \implies \frac{ae}{2} = a$

$$\implies ae = 2a$$

$$\implies e = \frac{2a}{a} = 2.$$

$\therefore$ The identity element $e = 2$.

Inverse

Consider a non-empty set A and a binary operation $*$ on A. Then $*$ has the inverse property if for each $a \in A$, there exists an element b in A such that
$a*b$ (right inverse) $= b*a$ (left inverse) $= e$, then b

4) Consider the binary operation $*$ on Q, defined by ~~$a*b = a+b-ab, \forall a,b \in Q$~~ $a*b = \frac{ab}{4}$,

Determine the inverse, if exists.

A) To find inverse, 1st we have to find the identity element e.

(ie) $a*e = a$.

$$\Rightarrow \frac{ae}{4} = a \Rightarrow ae = 4a \Rightarrow e = 4.$$

For inverse,

$$a*a^{-1} = e \Rightarrow a*a^{-1} = 4$$

$$\Rightarrow \frac{aa^{-1}}{4} = 4$$

$$\Rightarrow aa^{-1} = 16$$

$$\Rightarrow a^{-1} = \frac{16}{a}.$$

$\therefore$ Inverse of a in Q is $16/a$.

Semigroups and Monoids

The algebraic system $(S,*)$ is known as a semigroup, where S is a non-empty set & $*$ is a binary operation which is associative.

If $*$ is commutative, then the semigroup is said to be commutative (or abelian) semigroup.

If * is commutative, then monoid is called as commutative or abelian monoid.

or

An algebraic system (A,*), where * is a binary operation on A. Then, the system (A,*) is said to be a Semi-group, if it satisfies the following properties:-

1) The operation * is a closed operation on A.
2) The operation * is an associative operation.

Q) Consider an algebraic system $(\{0,1\},*)$, where * is a multiplication operation. Determine whether $(\{0,1\},*)$ is a semi group.

A) To check the * is a semigroup, the operation * is closure & Associativity.

Closure property:-

$0*0=0\in\{0,1\}$; $0*1=0\in\{0,1\}$; $1*0=0\in\{0,1\}$;

$1*1=1\in\{0,1\}$.

$\therefore$ The operation * is closed.

Associative property

The operation * is associative, since we have.

$(a*b)*c=a*(b*c)$, $\forall\, a,b,c\in\{0,1\}$.

$\therefore$ Since the algebraic system is closed & Associative

Hence * is a semi group

1 Let $N = \{0, 1, 2, 3, \ldots\}$ be the set of Natural Numbers.
Then S.T $(N, +)$ is a monoid.
For a set $(N, +)$ to be ~~mono~~ monoid, it should
satisfy, ① $(N, +)$ must be semigroup
② $(N, +)$ must have an identity element e.

1) $(N, +)$ ~~can~~ be a Semigroup

Closure property

when two natural numbers are added, then the result will be always a natural number.
∴ closure property is satisfied.

Associativity

The ~~operation~~ operation + defined on the set N is always associative, since ~~a+1~~
~~(a+b)+c = (a+c)+(b~~
$(a+b)+c = a+(b+c), \forall a, b, c \in N$.
∴ Associativity is attained.

② Checking for identity

Let $a \in N$, then by definition of identity,
$a * e = a \Rightarrow e = a - a = 0 \in N$.
∴ 0 is the identity element and it is a member of N.
∴ property of identity is attained.

Then S.T $(Z^+,+)$ is not a monoid?

A) ① $(Z^+,+)$ be a semigroup.

closure property

Any ~~post~~ two positive integer in Z^+ when added will again give a positive integer in Z^+.

$\therefore$ closure property is attained.

Associative property

Associativity always holds for the set of positive integers, Z^+, since $(a+b)+c = a+(b+c)$, $\forall\ a,b,c \in Z^+$

② checking for identity

Let $a \in N$, then by definition of identity,

$a+e = a \implies e = a-a = 0 \notin Z^+$.

$\therefore$ Identity doesnot belong to Z^+.

$\therefore$ $(Z^+,+)$ is not a monoid

Result::

Every semigroup need not be monoid.

Subsemigroups

Let $(S,*)$ be a semigroup & $T \subseteq S$. Then $(T,*)$ is said to be a subsemigroup of $(S,*)$, if T is closed under the operation $*$.

Let $(M, *, e)$ be a monoid & $T \subseteq M$. Then $(T, *, e)$ is known as a submonoid of $(M, *, e)$, if T is closed under the operation $*$ and the identity $e \in T$.

Q) Consider the semigroup $(N, +)$.
S.T $(Z^+, +)$ is a subsemigroup of $(N, +)$.

A) Since Z^+ is the set of positive integers
$\{1, 2, 3, \dots\}$ is a subset of N and
$(Z^+, +)$ is closed under addition,
$(Z^+, +) \subseteq (N, +)$ is a subsemigroup.

Q) Consider the semigroup $(N, +)$. S.T $(T, +)$, where T is the set of odd integers is a subsemigroup?

A) $T = \{1, 3, 5, \dots\} \subseteq N = \{1, 2, 3, \dots\}$.
Here $(T, +)$ is a not a subsemigroup, since T is not closed under the binary operation $+$.

Q) Consider the monoid $(R, \cdot, 1)$, where R is the set of Real no.'s. S.T $(N, \cdot, 1)$ is a submonoid.

A) $N = \{1, 2, 3, \dots\} \subseteq R$.
N is closed under the operation $\cdot$ (multiplication), since when any 2 natural no's are multiplied, the result will be a natural number.

of R is an identity element of N and also that element belongs to N.

By def^n of identity, e, we have

$\forall a \in N$, $a \cdot e = a$.

$\implies e = a/a = 1 \in N$.

$\therefore (N, \cdot)$ is a submonoid

Remark: The set of even positive integer under multiplication is not a submonoid of $(R, \cdot, 1)$.

Homomorphism of Semigroup & Monoids

Let $(S, *)$ and (T, Δ) be any two semigroup. A function $f: S \to T$ is called semigroup homomorphism if for any two elements $a, b \in S$, we have

$$f(a * b) = f(a) \,\Delta\, f(b).$$

If f is one-one and onto, then the above subsemigroup homomorphism can be called as semigroup isomorphism.

Let $(M, *, e_M)$ and (T, Δ, e_T) be any two monoids. A function $f: M \to T$ is known as monoid homomorphism if for any $a, b \in M$, we have $f(a * b) = f(a) \Delta f(b)$ & $f(e_M) = e_T$.

4) ~~Let L~~ be the set of posi... integers

5) Let $(N, +, 0)$ and $(N, \cdot, 1)$ be two semigroups.
Let $f: N \to N$ be defined as $f(m) = 3^m$, for any $m \in N$.

Then f is a semigroup homomorphism, because
$f(m+n) = f(m) \cdot f(n)$ should be satisfied.

~~L.H.S~~ $f(m+n) = 3^{m+n} = 3^m \cdot 3^n = f(m) \cdot f(n)$.

Also,
$(N, +)$ and $(N, \cdot)$ are two monoids.
and let $f: N \to N$ be defined by $f(m) = 3^m$, for any $m \in N$.

Then f is a monoid homomorphism, because
$f(m+n) = 3^{m+n} = 3^m \cdot 3^n = f(m) \cdot f(n)$
and ~~the co~~
the identity element for $(N, +)$ is 0 and that of $(N, \cdot)$ is 1.

$\therefore f(0) = 3^0 = 1$ [identity element of $(N, \cdot)$]

Rings

Definition

Let R be a non-empty set together with two closed binary operations '+' & '·'. Then $(R, +, \cdot)$ is a ring if for all $a, b, c \in R$, the following conditions are satisfied:-

(a) $a+b = b+a$ [Commutative law of +]

(b) $a+(b+c) = (a+b)+c$ [Associative law of +]

(c) There exist $z \in R$ such that $a+z = z+a = a$, for every $a \in R$.
(existence of identity for +)

(d) For each $a \in R$ there is an element $b \in R$ with $a+b = b+a = z$. (Existence of Inverse under +)

(e) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ [Associative law for ·]

(f) $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$
~~$a+(b+c) = a+b$~~
$(b+c) \cdot a = (b \cdot a) + (c \cdot a)$ } Distributive law of · over +.

Remark: The Properties from (a) to (d) shows that $(R, +)$ is an abelian group.

Q) For the set $I_4 = \{0, 1, 2, 3\}$, show that modulo 4 system is a ring.

A). we have to S.T $(I_4, +_4, \times_4)$ is a ring.
so we have to S.T (1) I_4 is closed under $+_4$ & $\times_4$
(2) I_4 is abelian group under $+_4$
(3) ... satisfies associativity & distributive

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	~~0~~ 1

∴ From the Composition table for $+_4$, we have closure property is attained.

Associativity holds.

The identity is 0

The Inverses are :-

Inverse for 0 is 0

Inverse for 1 is 3

Inverse for 2 is 2

Inverse for 3 is 1.

From the Composition table of $+_4$, the rows & columns are transpose to each other, hence commutative.

∴ $(I_4, +_4)$ is an abelian group.

From the composition table of $\times_4$, it is clear that $\times_4$ ~~is clos~~ satisfies closure property.

Since this I_4 is a number system and ~~to~~ under $\times_4$ it is always associative and satisfies distributive law of $\times_4$ over $+_4$.

$a \oplus b = a+b-1$ and $a \odot b = \ldots$

A) Here Z is the set of Integers and the operations $\oplus$ & $\odot$ are defined.

To show that $(Z, \oplus, \odot)$ is a ring, we have to S.T $(Z, \oplus)$ is an abelian group & $(Z, \odot)$ satisfies closure property, Associativity & distributive for $\odot$ over $\oplus$

<u>1st we S.T $(Z, \oplus)$ is an abelian group</u>

<u>closure property,</u>

Let $a, b \in Z$, then ~~a⊕b~~ $a \oplus b = a+b-1 \in Z$.

$\therefore$ closure property is attained.

<u>Associativity</u>

Let $a, b, c \in Z$, we have to P.T

$(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

$L.H.S = (a \oplus b) \oplus c = (a+b-1) \oplus c$

$= a+b-1+c-1 = a+b+c-2 \rightarrow (1)$

$R.H.S = a \oplus (b \oplus c)$

$= a \oplus (b+c-1) = a+b+c-1-1$

$= a+b+c-2 \rightarrow (2)$

From (1) & (2), $L.H.S = R.H.S$

$\therefore (a \oplus b) \oplus c = a \oplus (b \oplus c)$

Associativity holds.

For ~~ex~~ this, we have to find an element e ∈
Such that $a \ominus e = a$.

$\Rightarrow a + e - 1 = a$ [by definition of $\ominus$]

$\Rightarrow e = a - a + 1$

$\Rightarrow e = 1 \in \mathbb{Z}$.

$\therefore$ $e = 1$ is the identity

Existence of Inverse

For this, we have to p.T for $a \in \mathbb{Z}$, we have to find an $a^{-1} \in \mathbb{Z}$ such $a \ominus a^{-1} = e$.

(ie) $a \ominus a^{-1} = 1$ [$\because e = 1$]

$\Rightarrow a + a^{-1} - 1 = 1$ [by definition of $\ominus$]

$\Rightarrow a^{-1} = 1 + 1 - a$

$= 2 - a$.

$\therefore$ The inverse a is $(2-a) \in \mathbb{Z}$, since $a \in \mathbb{Z}$.

$\therefore$ Inverse exists.

Commutative property

Let $a, b \in \mathbb{Z}$, we have to S.T $a \ominus b = b \ominus a$

L.H.S $= a \ominus b = a + b - 1 \rightarrow$ (a)

R.H.S $= b \ominus a = b + a - 1 = a + b - 1 \rightarrow$ (b)

From (a) & (b), R.H.S = L.H.S. (ie) $a \ominus b = b \ominus a$.

Consider $(Z, \odot)$ Let $a, b, c \in Z$.

Associative law for $\odot$

we have to P.T $a \odot (b \odot c) = (a \odot b) \odot c$

$L.H.S = a \odot (b \odot c)$

$= a \odot [b + c - bc]$, by definition of $\odot$.

$= a + (b + c - bc) - a(b + c - bc)$

$= a + b + c - bc - ab - ac + abc \rightarrow (a)$

$R.H.S = [a \odot b] \odot c$

$= (a + b - ab) \odot c$

$= a + b - ab + c - (a + b - ab)c$

$= a + b + c - ab - ac - bc + abc \rightarrow (b)$

From (a) & (b), $R.H.S = L.H.S$.

$\therefore a \odot (b \odot c) = (a \odot b) \odot c$.

$\therefore$ Associativity holds for $\odot$.

Distributive law for $\odot$ over $\ominus$.

we have to P.T $a \odot (b \ominus c) = (a \odot b) \ominus (a \odot c)$ and

$(b \ominus c) \odot a = (b \odot a) \ominus (c \odot a)$

1st we prove $a \odot (b \ominus c) = (a \odot b) \ominus (a \odot c)$

$L.H.S = a \odot (b \ominus c) = a \odot (b + c - 1)$

$= a + (b + c - 1) - a(b + c - 1)$

$= a + b + c - 1 - ab - ac + a$ (a)

$= (a+b-ab) \ominus (a+c-ac)$

$= a+b-ab+a+c-ac-1 = 2a+b+c-ab-ac-1 \longrightarrow (b)$

~~$2a+b-ab-ac+$~~

Form (a) & (b), L.H.S = R.H.S.

(ii) $a \odot (b \ominus c) = (a \odot b) \ominus (a \odot c)$ is proved.

Next we prove ~~$(b \ominus c) \odot a = (b \odot a) \odot (c$~~

$(b \ominus c) \odot a = (b \odot a) \ominus (c \odot a)$

L.H.S $= (b \ominus c) \odot a$

$= (b+c-1) \odot a$

$= b+c-1+a-(b+c-1)a$

$= b+c-1+a-ab-ac+a$

$= 2a+b+c-ab-ac-1 \longrightarrow (a)$

R.H.S $= (b \odot a) \ominus (c \odot a)$

$= (b+a-ab) \ominus (c+a-ca)$

$= b+a-ab+c+a-ca-1$

$= 2a+b+c-ab-ac-1 \longrightarrow (b)$

Form (a) & (b), L.H.S = R.H.S.

$\therefore (b \ominus c) \odot a = (b \odot a) \ominus (c \odot a)$ is proved.

$\therefore$ Distributive law of $\odot$ over $\ominus$ is attained.

$\therefore (Z, \ominus, \odot)$ is a Ring.

Let $(R,+,\cdot)$ is a ring.

ⓐ If $ab=ba$, for all $a,b \in R$, then R is called a commutative ring.

ⓑ The ring R is said to have no proper divisors of zero, if for all $a,b \in R$, $ab = e \Rightarrow a = e$ or $b = e$, where e is the ~~ide~~ additive identity, (normally 0).
[(ie) $ab = 0 \Rightarrow$ either $a=0$ or $b=0$].

ⓒ If an element $u \in R$ is such that $u \neq e$ (identity) and $au = ua = a$, for all $a \in R$, we call u a unity, or multiplicative identity, of R.
Hence R is called a ring with unity.

eg: Consider the above problem, $(Z, \ominus, \odot)$, where $\ominus$ and $\odot$ is defined by, for all $a,b,c \in Z$.

$a \ominus b = a+b-1$ & $a \odot b = a+b-ab$.

we are going to verify that whether ~~this~~ $(Z, \ominus, \odot)$ which is a ring satisfy,

ⓐ Commutative ring.

ⓑ no proper divisors of zero

ⓒ ring with identity.

A) ⓐ In order, to verify commutative ring, we have to S.T

$a \odot b = b \odot a$, for $a,b \in Z$.

~~$a \odot$~~ $L.H.S = a \odot b = a+b-ab$

$R.H.S = b \odot a = b+a-ba = a+b-ab$

(b) In order to P.T no proper divisors of zero, we have to P.T $a \odot b = 1$ (Since 1 is the identity element of $\odot$) we have to S.T either $a = 1$ or $b = 1$.

$$a \odot b = 1 \implies a + b - ab = 1$$

if $a = 1$, then $1 + b - b = 1$
$1 + 0 = 1$
$1 = 1$, which is true.

if $b = 1$, then $a + 1 - a = 1$
$0 + 1 = 1$
$1 = 1$, which is true.

$\therefore$ if $a \odot b = 1$, then either $a = 1$ or $b = 1$.

$\therefore (Z, \oplus, \odot)$ has ~~proper~~ no proper divisors of zero.

(c) In order to P.T ring with ~~identity~~ unity, we have to find an element $u \in R$ such that $u \neq e$ & $a \odot u = u \odot a = a$, for $a \in R$.

Here $e = 1$.

~~$\therefore a \odot u = a + u - au$~~ $\therefore a \odot u = a$

$\implies a + u - au = a$

$\implies a + u(1 - a) = a$

$\implies u(1 - a) = 0$

$\implies u = 0 \neq 1 = e$.

$\therefore$ The integer $u = 0$ is the unity of Z.

$\therefore (Z, \oplus, \odot)$ is a ring with unity.

Let R be a ring with unity u. If a ... exist $b \in R$ such that $ab = ba = u$, then b is called a multiplicative inverse of a and a is called a unit of R.

Definition

Let R be a commutative ring with unity. Then

(a) R is called an integral domain of R if R has no proper divisors of zero.

(b) R is called a field if every non-zero element of R is a unit.

Note:-

1. Every field is a ring.
2. Every field is an integral domain but every integral domain is not a field.
3. Every finite integral domain is a field.

Subring

A subset A of a ring $(R, +, \cdot)$ is called a subring of R, if it satisfies following conditions:-

(i) $(A, +)$ is a subgroup of a group $(R, +)$.

(ii) A is closed under the multiplication operation.

(ie) if $a, b \in A$, then $a \cdot b \in A$.

Note :-)

1) If R is a ring, then $\{0\}$ & R are subrings of R.

2) Sum of two subrings may not be subring.

3) Intersection of subrings is a subring.

Ring Homomorphisms

Definition :-)

Let $(R,+,\cdot)$ and $(S,\oplus,\odot)$ be rings.
A function $f: R \to S$ is called a ring homomorphism,
if for all ~~a,b∈R,~~ $a,b \in R$,

ⓐ $f(a+b) = f(a) \oplus f(b)$ &
ⓑ $f(a \cdot b) = f(a) \odot f(b)$.

When the function f is onto we say that S is a homomorphic image of R

Definition :)

Let $f: (R,+,\cdot) \to (S,\oplus,\odot)$ be a ring homomorphism.
If f is one-to-one and onto, then f is a called a ring isomorphism and we say that R & S are isomorphic rings.

Q) A finite Integral Domain $(D, +, \cdot)$ is a field.

A) Since D is finite, we can list the element of D as $\{d_1, d_2, \ldots, d_n\}$.

For $d \in D$, where $d \neq e$ (identity element of +), ~~when~~ we have $dD = \{dd_1, dd_2, \ldots, dd_n\} \subseteq D$, because D is closed under multiplication.

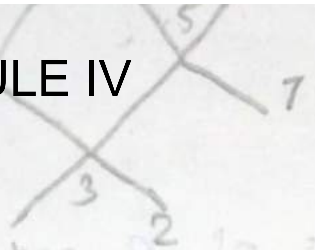
Now, $|D| = n$ and $dD \subseteq D$, so if we could show that dD contains n elements, we would have $dD = D$.

If $|dD| < n$, then $dd_i = dd_j$, for some $1 \leq i < j \leq n$.

But since D is an integral Domain and $d \neq e$, we have $d_i = d_j$, when they are supposed to be distinct.

So $dD = D$ and for some $1 \leq k \leq n$, $dd_k = u$, the unity of D.

Then $dd_k = u \Rightarrow d$ is a unit of D & since d is chosen arbitrarily, it follows that $(D, +, \cdot)$ is a field.



Upper bound is. 5, 6.

Sup (B) = 5

Lower bound = 3

LATTICES

A lattice is a poset in which every pair has a supremum & infimum

Join

Consider a poset L under the order ≤ Let a, b ∈ L. Then supremum of a & b is called join of a & b and is denoted by $a \oplus b$ or $a \vee b$

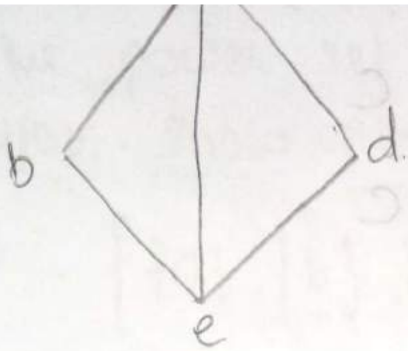
Meet

Consider the poset L under the order ≤. Let a, b ∈ L. The infimum of a, b is called the meet of a & b is denoted by $a * b$ or $a \wedge b$.

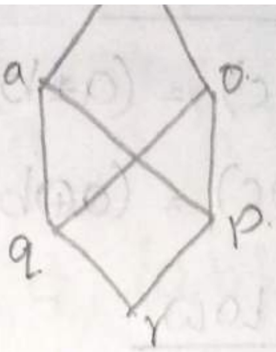
Remark:

The lattice is denoted by $(L, *, \oplus)$

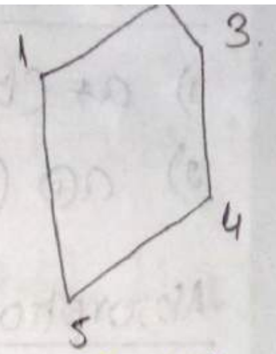
15)



fig(1)



fig(3)



fig(2)

→ from figure (1), every pair {a,b}, {b,e}, {a,e}, {a,c}, {c,e} {e,d}, {a,d}, {a,e}. All have supremum & infimum. and hence figure(1) is a lattice

→ In figure(2) every pair has infimum & supremum. so fig (2) is a lattice.

→ figure (3) is not a lattice if we are considering pairs {p,q} it has upper bounds. n, o & m but no supremum violates the condition.

<u>Some Properties of Lattice.</u>

<u>Idempotent law.</u>

1) $a * a = a$

2) $a \oplus a = a$

where $a \in L$.

<u>Commutative Law.</u>

1) $a \oplus b = b \oplus a$

2) $a * b = b * a$

where $a, b \in L$.

1) $a * (b \circledast c) = (a * b) \circledast c$

2) $a \oplus (b \oplus c) = (a \oplus b) \oplus c$

Absorption Law

1) $a * (a \oplus b) = a$

2) $a \oplus (a * b) = a.$

Distribution Law

1) $a * (b \oplus c) = (a * b) \oplus (a * c)$

2) $a \oplus (b * c) = (a \oplus b) * (a \oplus c)$

The Bounded Lattice

A littice L is called a bounded lattice if it has a greatest element and a least element from the above figures (1) & (2) are bounded. lattices.

It has no greatest element but have least element and hence not a bounded lines.

Remark:-

The greatest element is denoted by either '1' or 1.
The least element is denoted by '0'.

For the power set of $\{a,b,c\}$ with odering inclusion. Show that it is a bounded lattic.

A. $P = \{\{a\}, \{b\}, \{c\}, \phi, \{a,b\} \{a,c\} \{b,c\}$

Complete Lattice

A lattice is said to be complete if every nonempty subset has a supremum & infimum.

Remark:-

Every finite lattices must be complete.

Ex: figure (1) & (2) drawn above are complete lattice.

Distributive Lattice.

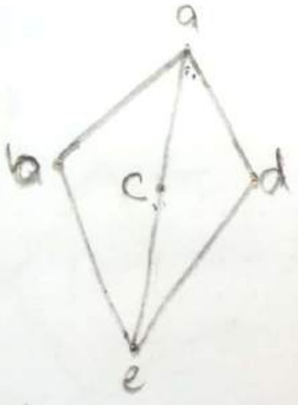
The lattice is called distributive lattice if it satisfies the distributive law.

ie. $a, b, c \in L$. then

1) $a * (b \oplus c) = (a * b) \oplus (a * c)$

2) $a \oplus (b * c) = (a \oplus b) * (a \oplus b)$

16/9/17.



GLB	a	b	c	d	e
a	a	b	e	d	e
b	b	b.	e	e	e
c	e	e	c	e	e
d	d	e	e	d	e
e	e	e	e	e	e

{a, b, c} {a, b, d} {b, c, e}
{a, c, d} {a, b, e} {b, d, e}
{a, d, e} {b, c, d} {c, d, e}

$b \oplus c$	$a * (b \oplus c)$	$a * b$	$a * c$	$(a*b) \oplus (a*c)$
$c \oplus d$ a				e

First to check the distributive lattice we have to first check whether it is a lattic and secondly whether every subset of three element satisfies distributive law.

<u>Checking for lattice</u>

*GLB	a	b	c	d	e
a	a	b	c	d	e
b	b	b	e	e	e
c	c	b	c	e	e
d	d	e	e	d	e
e	e	e	e	e	e

⊕LUB	a	b	c	d	e
a	a	a	a	a	a.
b	a	b	a.	a	b.
c	a	a	c	a	c
d	a	a	a	d	d
e.	a	b	c	d.	e

From the tables it is clear that every pair has a supremum & infimum & hence a lattice

Now, according to distributive

$\forall\, a,b,c \in L$.

$$a * (b \oplus c) = (a * b) \oplus (a * c)$$
$$a \oplus (b * c) = (a \oplus b) * (a \oplus c)$$

Consider the subsets.

$\{a,b,c\}$ $\{a,b,d\}$ $\{a,c,d\}$ $\{e,d,c\}$ $\{e,b,d\}$ $\{e,c,d\}$
$\{b,c,d\}$ $\{e,d,a\}$ $\{e,c,a\}$ $\{e,d,a\}$

Consider the $\{b,c,d\}$ start with disjoint sets first.

We have to show that:

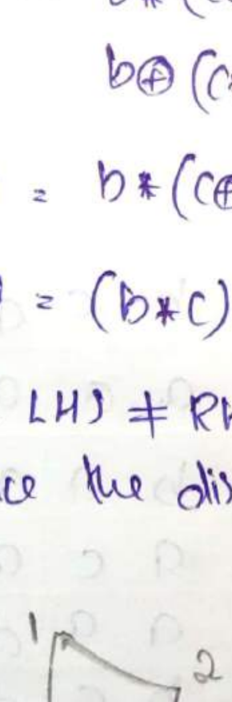
$$b * (c \oplus d) = (b * c) \oplus (b * d)$$
$$b \oplus (c * d) = (b \oplus c) * (b \oplus d)$$

$LHS = b * (c \oplus d) = b * a = b$

$RHS = (b * c) \oplus (b * d) = e \oplus e = e$

$\therefore LHS \neq RHS$

Hence the distributive law fails.



26/4/11.

Complemented Lattice

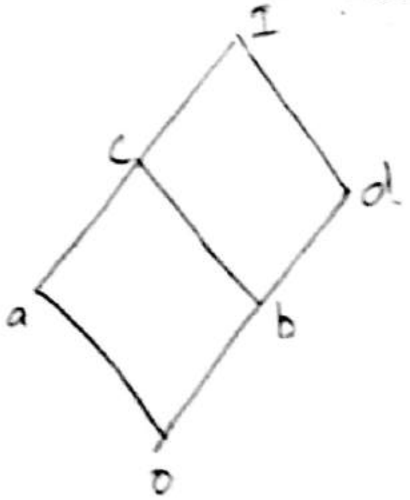
An element 'a' $\in L$ were L is a lattice, is said to have a complement b then $a * b = 0$ and $a \oplus b = I$ (one) ie, Infimum(a,b) = least element & sup(a,b) = greatest element.

A complemented lattice is a bounded lattice with every element has atleast one complement.

Remark:

1) The complement of least element (zero) is the greatest element (one)
Also the complement of greatest element (one) is the least element (zero)
2) The complement is always symmetric functions ie. if 'a' is a complement of 'b' then, 'b' is the complement of 'a' also.

? Determine whether the given Hasse diagram is a complemented lattice.



infimum & supremum

This is a bounded lattice since it has greatest & least element.

$a * b = 0$

$a \oplus b = c \neq 1$

b not complement of a

~~a*b~~

The complement of a is d

Since $a * d = 0$ & $a \oplus d = 1$

The complement of d is a (by symmetry)

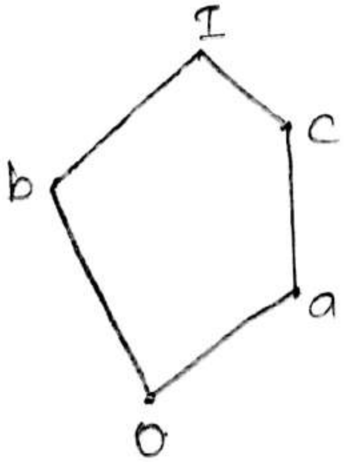
$c * d = 0$ $\qquad c * a = a \qquad c * d \neq 0$

$c \oplus b = c$

$\Rightarrow$ c has no complement.

Since c has no complement it is not a complemented lattice.

? Check whether the given hasse diagram is a complemented lattice.



i) Checking for a lattice

This is a lattice.

ii) Bounded lattice

This is a bounded lattice since it has greatest & lowest element.

iii) Checking for complement

$a * b = 0$ $\quad$ $b * c = a$

$a \oplus b \neq I = c$ $\quad$ $b \oplus c = I$.

It is not a complemented lattice.

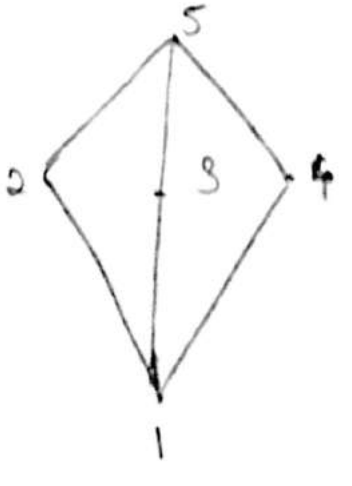
Sub Lattice

Let $(L, *, \oplus)$ be a lattice and $S \subseteq L$, then $(S, *, \oplus)$ is a sublattice if and only if S is closed under the operations of $*$ and $\oplus$ of L
ie, A non-empty set S of the lattice L is said to be a sublattice if S itself is a lattice w.r.t the operations of L

Remark

For finding sublattice we have to check.
i) for the poset & draw Hasse diagram
ii) Existance of supremum & infimum ∀ pair in the subset.
iii) The supremum & infimum element of each pair should belong to the subset under considerat:

Q. Consider the lattice $L = \{1, 2, 3, 4, 5\}$ given by the Hasse diagram. Determine all the possible sublattices with three or more elements.



A. The sub lattices are {1,4,5} $S=4$ $\quad$ $S=5$ / $I=1$ $\quad$ $I=1$

This is a sublattice since every pair (1,4), (1,5), (4,5) have a supremum & infimum & these values belongs to set 1,4,5.

The other sublattices are {1,2,5}, {1,3,5}, {1,2,3,5}, {1,3,4,5}, {1,2,4,5}, {1,2,3,4,5}

Remark.

{2,3,4} is not a sublattice since for the pair (2,3) supremum is 5 & infimum is 1 but they donot belong to {2,3,4}.

Lattice Homomorphism

Let $(L, *, \oplus)$ & ~~$(S, *, \oplus)$~~ $(S, \wedge, \vee)$ be two lattices then a mapping $g: L \to S$ is said to be a lattice homomorphism if it satisfies. for any $a, b \in L$

1) $g(a*b) = g(a) \wedge g(b)$
2) $g(a \oplus b) = g(a) \vee g(b)$

Boolean Algebra

A boolean algebra is a complemented distributed lattice and is denoted by $(B, *, \oplus, ', 0, 1)$

Since B is a lattice it satisfies all the properties of the lattice ie,

for any $a, b, c \in B$.

i) Idempotent law

$$a \oplus a = a$$
$$a * a = a.$$

ii) Commutative law

$$a * b = b * a$$
$$a \oplus b = b \oplus a$$

iii) Associative law

$$(a*b)*c = a*(b*c)$$
$$(a \oplus b) \oplus c = a \oplus (b \oplus c)$$

iv) Absorption law

$$a \oplus (a*b) = a.$$
$$a * (a \oplus b) = a$$

Since B is distributive, it satisfy the condition Distributive law.

$$a * (b \oplus c) = (a*b) \oplus (a*c)$$
$$a \oplus (b*c) = (a \oplus b) * (a \oplus c)$$

i) $0 \leq a \leq I$

ii) $a \oplus 0 = a$ & $a * 0 = 0$.

iii) $a \oplus I = I$ & $a * I = a$

Since B is complemented, it satisfies

i) $a \oplus a' = I$, $a * a' = 0$

ii) $I' = 0$, $0' = I$

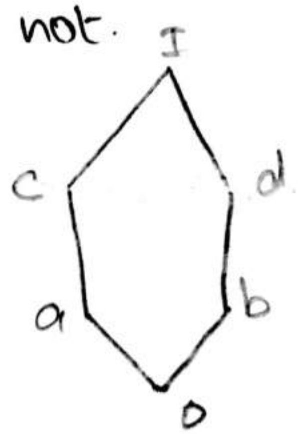
iii) $(a \oplus b)' = a' * b'$, $(a * b)' = a' \oplus b'$

Remark:

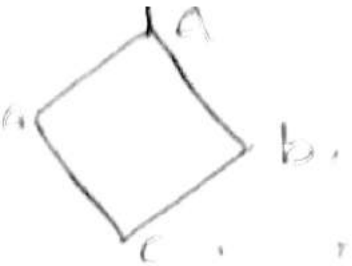
> If a finite lattice L doesnot contain 2^n elements for some positive integer n then L cannot be boolean algebra.

> For a distributed lattice, the complements are unique.

? Determine whether the following are boolean algebra or not.



A. This is not a boolean algebra since the number of elements = 6. cannot be written in the form 2^n where n is +ve integer.



This is not a boolean algebra since the no:of elements 5 cannot written in form of 2^n.

?

A. Since This a lattice, we can check whether it is complemented & distributed lattice.
This is a bounded lattice since it has least & greatest element.

$a * b = b \neq 0$.
$a * 0 = 0$
$a \oplus 0 = a \neq I$

Here $0' = I$, $I' = 0$, but we cannot find complements for a & b Hence it is not a complemented lattice.

Consider the boolean algebra $(B, *, \oplus, ', 0, I)$ and A is said to be a sub algebra of B, then it should satisfy the conditions.

i) $A \subseteq B$

ii) A itself should be a boolean algebra.

Remark

Sub algebra can be also called as sub boolean algebra.

Direct Product

Let $(B_1, *_1, \oplus_1, ', 0_1, I_1)$ & $(B_2, *_2, \oplus_2, '', 0_2, I_2)$ be two different boolean algebra. The direct product two boolean algebras is defined to be a boolean algebra denoted by $(B_1 \times B_2, *_3, \oplus_3, ''', 0_3, I_3)$ and is defined by. For any $(a_1, b_1), (a_2, b_2) \in B_1 \times B_2$ it satisfies the condition.

i) $(a_1, b_1) *_3 (a_2, b_2) = (a_1 *_1 a_2, b_1 *_2 b_2)$

ii) $(a_1, b_1) \oplus_3 (a_2, b_2) = (a_1 \oplus_1 a_2, b_1 \oplus_2 b_2)$

iii) $(a_1, b_1)''' = (a_1', b_1'')$

iv) $0_3 = (0_1, 0_2)$ & $I_3 = (I_1, I_2)$

Boolean Homomorphism

Let $(B, *, \oplus, ', 0, I)$ & $(P, \wedge, \vee, -, \alpha, \beta)$ be two boolean algebras. A mapping $f: B \to P$ is called a boolean homomorphism if all the operations of boolean algebra are reserved. ie, for any $a, b \in B$ $f(a*b) = f(a) \wedge f(b)$.

$f(a \oplus b) = f(a) \vee f(b)$

$f(a') = \overline{f(a)}$

$f(0) = \alpha$

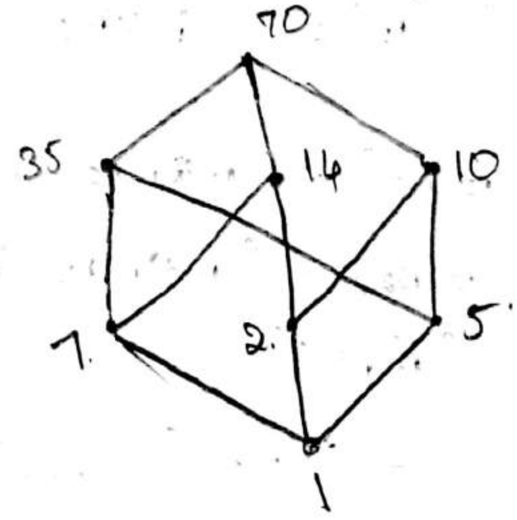
$f(I) = \beta$

$D_n \quad n>0$ → collection of all divisors

? Consider the boolean algebra D_{70} whose Hasse diagram is given. List out the sub algebra of D_{70}.

A. $D_{70} = \{1, 2, 5, 7, 10, 14, 35, 70\}$

The Hasse diagram is



The subalgebra is $A = \{1, 7, 10, 70\}$

Here set of 3 doesn't work (usually take subset of 3 ele)

Do definition of boolean algebra in this set

second algebra. $\{1, 2, 35, 70\}$

3\...

MODULE V

Proporsitional Logic

Proporsitions.

A proposition is a statement which is either true or false but not the both

ex: Jawaharlal Nehru is the 1st Prime Minister of India - It is a proposition

Why is your name - not proposition

If $x^2 = 13$. What is the value of x - not propositn

Remark :-

The two truth values are 'True' & 'False' and can be denoted by the symbols 'T' or '1' and 'F' or '0' respectively.

Remark:-

The propositions are usually denoted by the lowercase letters starting with 'p'

?. Classify the following statements as propositions or non-proposion

> The population of India goes upto 100 million in the year 2000. - propositn

> $x+y=30$. - not propstn.

Truth Table

A truth table displays the relationship b/w the truth values of compound propositions constructed from ~~fr~~ simpler propositions

Logical Connectives

1) Conjunction

The conjunction of the proposition 'p' & 'q' denoted by 'p∧q' and it is read 'p AND q'. Conjunction will have truth value 'T' or '1' when both 'p' & 'q' have the truth value 'T' or '1' In all other cases it will be false.

p	q	p∧q
T	T	T
T	F	F
F	T	F
F	F	F

2) Disjunction

The expression for disjunction is given to be 'p∨q' where 'p' & 'q' are propositions and it is read 'p OR q'. The disjunction will have the truth value 'T' or '1' when either one or both 'p' & 'q' are true & is false when both 'p' & 'q' are false.

T	T	T
T	F	T
F	T	T
F	F	F

3) Negation

Negation means the opposite of the original proporsition. Negation of p which is denoted by '~p' or '¬p' is a proposition which is true when 'p' is false & is false when 'p' is true.

p	¬p
T	F
F	T

5/10/17

4) Implication or Conditional connective.

We say that "p implies" q & is denoted by "p→q" where p is called the hypothesis & q is called the conclusion. This implication have the truth value false only when p is true & q is false and in all other cases the truth value will be true. We can denote the implication by

i) if p, then q

ii) p is sufficient for q

iv) q is necessary for p
v) q is a necessary condition for p.
vi) p only if q

Truthtable

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

Different Types of Implications.

i) Contrapositive

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

ii) Converse

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

iii) Inverse

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

5) Biconditional

The biconditional of two statement p & q is denoted by $p \leftrightarrow q$ which is read "p if and only if q" or "p is necessary and sufficient for q"

The proposition $p \leftrightarrow q$ have the truth value false, if p and q donot have the same truth values and is true when both p and q have same true values.

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

6/10/2017.

? Consider the propositions p : He is a rich man and q : He is not greedy. Write the contrapositive, converse & inverse of the implication $q \rightarrow p$.

A. Implication

Here $q \rightarrow p$ is the preposition if ~~p~~
If he is not greedy he is a rich man.

Contrapositive.

$\neg p \rightarrow \neg q$.

If he is not a rich man then he is greedy. which is the proposition as above.

Converse

$p \rightarrow q$.

If he is a rich man then he is not greed.

Inverse $\neg q \rightarrow \neg p$ which is the proposition
If he is a greedy then he is not a ...

$p \vee (q \wedge r)$ & $(p \vee q) \wedge r$.

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

p	q	r	$p \vee q$	$(p \vee q) \wedge r$
T	T	T	T	T
T	F	F	T	F
F	T	F	T	F
F	F	T	F	F
T	T	F	T	F
F	T	T	T	T
T	F	T	T	T
F	F	F	F	F.

? Draw the truth table of $(p \to q) \leftrightarrow (\neg q \to \neg p)$

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

? A preposition p is called to be tautology if it is true under all circumstances. That means it containing only the truth value 'T' in the final column of the truth table. The above question is an example for tautology.

If it is all false then it is called contradiction.

A compound statement ... neither a tautology nor a condridiction is called a contingency.

? Check whether the preposition $(p \wedge \neg p)$ belongs to tautology, contridiction, contigency.

p	q	$\neg p$	$p \wedge \neg p$
T		F	F
F		T	F.

It is a contridiction.

Logical Equalence

Two propositions are said to be logically equalent if they have exactly the same truth values under all circumstances. It is denoted by '$\cong$' or '$\equiv$' or $\Leftrightarrow$

? Check whether $(\neg p \vee \neg q) \cong \neg(p \wedge q)$.

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

$\therefore (\neg p \vee \neg q) \cong \neg(p \wedge q)$

? ~~Consider~~ ~~proposition~~ ~~P~~ ~~such that~~ ~~P.~~ ~~He is a~~
~~ft~~

Remark : We use the denotion T_0 tautology & F_0 for contradiction.

Remark : Simple proposition are also called as primitive statements.

Precedance of Logical Operators.

1) The bracketed expressions are always evaluated first & normally we do our evaluation from left to right.
2) The negation operator before all other operators.
3) The conjunction operator is to be applied before disjunction.
4) The implication operation is done before bicondition

Laws of Logic

For any primitive statements P, q & r and any tautology T_0 & for contradiction F_0 we have following laws.

1. Law of Double Negation

$$\neg(\neg p) \Leftrightarrow p.$$

2. De-Morgan's Law

$$\sim(p \land q) \Leftrightarrow \neg p \lor \neg q.$$

$$\neg(p \lor q) \Leftrightarrow \neg p \land \neg q$$

$$p \vee q \Leftrightarrow q \vee p.$$

$$p \wedge q \Leftrightarrow q \wedge p.$$

4. Associative Law

$$p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r.$$

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

5. Distributive Law

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

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

6. Idempotent Law.

$$p \vee p \Leftrightarrow p.$$

$$p \wedge p \Leftrightarrow p.$$

7. Identity Law.

$$p \vee F_0 \Leftrightarrow p.$$

$$p \wedge T_0 \Leftrightarrow p$$

8. Inverse Law.

$$p \vee \neg p \Leftrightarrow T_0$$

$$p \wedge \neg p \Leftrightarrow F_0$$

9. Domination Law.

$$p \vee T_0 \Leftrightarrow T_0.$$

$$p \wedge F_0 \Leftrightarrow F_0.$$

10. Absorption Law.

$$p \vee (p \wedge q) \cong p$$

$$p \wedge (p \vee q) \cong p$$

truth table.

A. LHS $= (p \vee q) \wedge \neg(\neg p \wedge q)$ given

$\Leftrightarrow (p \vee q) \wedge [\neg(\neg p) \vee \neg q]$ Demorgan's law

$\Leftrightarrow (p \vee q) \wedge (p \vee \neg q)$ Double negation.

$\Leftrightarrow p \vee (q \wedge \neg q)$ Distributive.

$\Leftrightarrow p \vee F_0$ Inverse

$\Leftrightarrow p =$ RHS. Identity.

Dual of the Proposition.

Let 's' be a statements. If s contains no logical connectives other than conjuction & disjunction. Then the dual of s is denoted by s^d and is obtained by replacing the symbol disjunction by conjunction, conjuction by disjunction T_0 by F_0 and. F_0 by T_0.

? Given the primitive statements p, q, r and the compound statements $s : (p \wedge \neg q) \wedge (r \wedge T_0)$ Write the dual of s.

A. The dual $s^d : (p \vee q) \vee (r \vee F_0)$

Principle of Duality

Let 's' & 't' be the statements that contains no logical connectives other than conjunction & disjunction.

If $s \Leftrightarrow t$, then the ~~dual~~ $s^d \Leftrightarrow t^d$

? Prove that $\neg[\neg[(p \vee q) \wedge r] \vee \neg q] \Leftrightarrow q \wedge r$ without truth table.

	Reason	
LHS $= \neg[\neg[(p \vee q) \wedge r] \vee \neg q]$	given	Do negation all first.
$\Leftrightarrow \neg \cdot \neg[(p \vee q) \wedge r] \wedge \neg\neg q$	Demorgan's law.	
$\Leftrightarrow [(p \vee q) \wedge r] \wedge q$	Double negation.	
$\cancel{(p \wedge r) \vee (q \wedge r)}$		
$\Leftrightarrow (p \vee q) \wedge (r \wedge q)$	Associative law.	
$\Leftrightarrow (p \vee q) \wedge (q \wedge r)$	Commutative law	
$\Leftrightarrow [(p \vee q) \wedge q] \wedge r$	Associative law.	
$\Leftrightarrow \cancel{q \vee p}\,[q \wedge (p \vee q)] \wedge r$	Commutative law.	
$\Leftrightarrow [q \wedge (q \vee p)] \wedge r$	Commutative law	
$\Leftrightarrow \underline{q \wedge r}$	Absorption law	

Let us consider the implication $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \to q$ where n is a positive integer. The statements $P_1, P_2 \cdots P_n$ are called premises of the argument and the statement q is the conclusion of the argument.

The preceding argument is called valid if whenever each of the premises $P_1, P_2 \cdots P_n$ is true then the conclusion is likewise true. Note that if anyone of the premises $P_1, P_2 \cdots P_n$ is false then the hypothesis $P_1 \wedge P_2 \wedge \cdots P_n$ is false and then the implication $P_1 \wedge P_2 \wedge \cdots \wedge P_n \longrightarrow q$ is automatically true.

Consequently one way to establish the validity of the given argument is to show that the statement or argument $P_1 \wedge P_2 \wedge \cdots \wedge P_n \leftrightarrow q$ is a tautology.

? Let p, q, r be the premitive statements such that p: Rojer studies well q: Rojer plays racket ball r: Rojer passes in all subjects. Now let P_1, P_2 & P_3 denote the premises, P_1: If Rojer studies well then he will pass in all subjects.

P_2: If Rojer doesn't play racket ball then he will study well. P_3: Rojer failed in all subjects. Show that $P_1 \wedge P_2 \wedge P_3 \longrightarrow q$ is a valid

A. $P_1 : p \to r$

$P_2 : \neg q \to p$

$P_3 : \neg r$

Here the premises can be rewritten as above

$$(P_1 \wedge P_2 \wedge P_3) \to q$$

We want to check $(P_1 \wedge P_2 \wedge P_3) \to q$ is a valid argument ie. $[(p \to r) \wedge (\neg q \to p) \wedge \neg r] \to q$

This substitution is a valid argument.

For the validity we will be checking $[(p \to r) \wedge (\neg q \to p) \wedge \neg r] \to q$ is a tautology with the help of truth table

p	q	r	$\neg q$	$\neg r$	$p \to r$	$\neg q \to p$	$(p \to r) \wedge (\neg q \to p)$	$(p \to r) \wedge (\neg q \to p) \wedge \neg r$	$\to q$
T	T	T	F	F	T	T	T	F	T
T	F	F	T	T	F	T	F	F	T
F	F	T	T	F	T	F	F	F	T
F	T	F	F	T	T	T	T	T	T
T	T	F	F	T	F	T	F	F	T
F	T	T	F	F	T	T	T	F	T
T	F	T	T	F	T	T	T	F	T
F	F	F	T	T	T	F	F	F	T

The given argument is a valid.

12/10/11 If p and q are arbitrary statements such that $p \to q$ is a tautology then we say that p <u>logically implies</u> q or $p \to q$ is a <u>logical implication</u> and is denoted by ~~$p \Leftrightarrow q$~~ $p \Rightarrow q$.

If an expression is said to be tautologically imply another expression then the logical implication of the two expression will be a tautology

<u>Rule of Inference</u>

1. p
$p \to q$
$\therefore q$ (modus ponens)

Rule of Inference	Related Logical Implication	Name of the Rule
p $p \to q$ $\therefore q$	$[p \wedge (p \to q)] \to q$	modus ponens or Rule of detachment
$p \to q$ $q \to r$ $\therefore p \to r$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Law of syllogism
$p \to q$ $\sim q$ $\therefore \sim p$	$[(p \to q) \wedge \sim q] \to \sim p$	Modus tollens
p q $\therefore p \wedge q$	$(p \wedge q) \to (p \wedge q)$	Rule of conjunction

$\sim p$ $\therefore q$	$[(p \vee q) \wedge \sim p] \to q$	... disjunctive syllogism
$\sim p \to F_0$ $\therefore p$	$[\sim p \to F_0] \to p$	Rule of contradiction
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Rule of conjunctive simplification.
p $\therefore p \vee q$	$p \to (p \vee q)$	Rule of disjunctive simplification
$p \wedge q$ $p \to (q \to r)$ $\therefore r$	$[(p \wedge q) \wedge (p \to (q \to r))] \to r$	Rule of conditional proof.
$p \to r$ $q \to r$ $\therefore (p \vee q) \to r$	$[(p \to r) \wedge (q \to r)] \to [(p \vee q) \to r]$	Rule ofor proof by cases.
$p \to q$ $r \to s$ $p \vee r$ $\therefore q \vee s$	$[(p \to q) \wedge (r \to s) \wedge (p \vee r)] \to (q \vee s)$	Rule of the constructive Dilemma
$p \to q$ $r \to s$ $\sim q \vee \sim s$	$[(p \to q) \wedge (r \to s) \wedge (\sim q \vee \sim s)] \to \sim p \vee \sim r$	Rule of destructive Dilemma

"Reeta is baking a cake. If Reeta is baking a cake then she is not practicing her flute. If Reeta is not practicing her flute then her father will not buy her a car. Therefore Reeta's father will not buy her a car".

A. In this problem first we have to write the given argument with the help of premitive statements & logical connectives. i.e.

p: Reeta is baking a cake
q: Reeta is practicing her flute
r: Reeta's father will buy her a car.

Now the premises will be.

$$\begin{array}{l} p \\ p \to \neg q \\ \neg q \to \neg r \\ \hline \therefore \neg r \end{array}$$

we have to check the validity of this argument. This can be done either by the truth table method or by the rule of inference.

1) By truth table method

For doing this method we have to write the related logical expression & check whether it is a tautology.
The related logical expression is.

$[p \wedge (p \to \neg q) \wedge (\neg q \to \neg r)] \to \neg r$

p	q	r	$\neg q$	$\neg r$	$p \to \neg q$	$p \wedge (p \to \neg q)$	$\neg q \to \neg r$	$\ldots \wedge (\neg q \to \neg r)$	$\ldots \to \neg r$
T	T	T	F	F	F	F	T	F	T
T	T	F	F	T	F	F	T	F	T
T	F	T	T	F	T	T	F	F	T
F	T	T	F	F	T	F	T	F	T
T	F	F	T	T	T	T	T	T	T
F	T	F	F	T	T	F	T	F	T
F	F	T	T	F	T	F	F	F	T
F	F	F	T	T	T	T	T	T	T

only once

times.

→ By using rules of inference.

Steps	Reasons
1) p	premise
2) $p \to \neg q$	premise
3) $\neg q$	step 1 & 2 with modus ponens.
4) $\neg q \to \neg r$	premise
5) $\neg r$	step. 3 & 4 with modus ponens.

? Check the validity of the following

$$\begin{array}{l} p \to \neg q \\ p \\ \hline \therefore \neg q \end{array}$$

A.

Steps	Reasons
1) $p \to \neg q$	premises.
2) p	premises
3) $\neg q$	steps 1 & 2 with modus ponens

(p→q)
$\neg r$

$\therefore \neg p$

A. Steps. | Reason.

1) $(p \vee q) \to r$ — premise
2) $\neg r \to \neg(p \vee q)$ — contrapositive
3) $\neg r \to \neg p \vee \neg q$ — demorgan's law.
4) $\neg r$ — premise
5) $\neg p \wedge \neg q$ — Step 4 & 3 with modus ponens
6) $\neg q$ — step 5 with rule of conjunctive

'or'

Steps | Reason

1) $(p \vee q) \to r$ — premise
2) $\neg r$. — premise
3) $\neg(p \vee q)$ — 1 & 2 with modus tollens
4) $\neg p \wedge \neg q$. — demorgan
5) $\neg p$

? $p \to q$
$q \to r$
$r \to s$
p

$\therefore s$

Steps | Reasons

1) $p \to q$ — premise
2) $q \to r$ — premise

3) $p \to r$ ... r)

4) $r \to s$ premis

5) $p \to s$ 3 & 4 law of syllogism

6) p premise

7) s 5 & 6 law of modus ponens

'OR'

Steps	Reasons
1) $p \to q$	premise
2) p	premise
3) q	1 & 2 modus ponens
4) $q \to r$	premise
5) r	3 & 4 modus ponens
6) $r \to s$	premise
7) s	5 & 6 modus ponens

?

$p \to \neg q$
$r \to q$
r
___
$\neg p$

2) $p \to q$
$q \to r$
$r \to s$
$\neg s$
$p \vee t$
___
$\neg t$

3) $p \to q$
$p \wedge r$
___
q

4) $(p \to q) \wedge (r \to s)$
$(p \vee r) \wedge (q \wedge r)$
___

Steps	Reason $q \vee s$
$p \to \neg q$	premise.
$r \to q$	premise.
$\neg q \to \neg r$	contrapositive
$p \to \neg r$	step 1 & 3 law of syllogism.
$\neg\neg r \to \neg p$	
$r \to \neg p$	
r	
$\neg p$	

by truth table & also by rule of inference
"If I study then I will pass examination. If I donot go to picnic then I will study. But I failed examination. Therefore I went to picnic.

A. p : I study.

q : I will pass examination.

r : I go to picnic.

~~s : I failed examination~~

$$\begin{array}{l} p \to q \\ \neg r \to p \\ \neg q \\ \hline \therefore r \end{array}$$

Steps.	Reasons.
1) $p \to q$	premise
2) $\neg q$ ~~$\neg r \to p$~~	premise
~~$p \to \neg r$~~	~~converse~~
3) $\neg p$	step 1 & 2 modus tollens.
~~$p \to q$~~.	
4) $\neg r \to p$.	premise.
5) $\neg\neg r$	Step 3 & 4 modus tollens
6) r.	double negation

Truth Table

$$\left[(p \to q) \wedge (\neg r \to p) \wedge [\neg q\right] \to r$$

p	q	r	$p \to q$	$\neg r$	$\neg q$	$\neg r \to p$	$\overbrace{p \to q \wedge \neg r \to p}^{x}$	$\underbrace{x \wedge \neg q}_{y}$	$y \to$
F	F	F	T	T	T	F	F	F	T
F	F	T	T	F	T	T	T	T	T
F	T	F	T	T	F	F	F	F	T
F	T	T	T	F	F	T	T	F	T
T	F	F	F	T	T	T	F	F	T
T	F	T	F	F	T	T	F	F	T
T	T	F	T	T	F	T	T	F	T
T	T	T	T	F	F	T	T	F	T

PREDICATE LOGIC

Consider the following two statements

Every SCE student must study Physics
Jackson is a SCE student.
Therefore, Jackson must study Physics.

This cannot be expressed by proporitional logic because non of the logical connectives are applicable here.
This kinds of problems are evaluated by predicate logic

A predicate is a statement that contains variables (predicate variables) that may be true or false depending on the values of the variable. We will denote the predicate P[variable]
For ex: i) John is a batchelor
Smith is a batchelor
Therefore John & smith are batchelor.

Here the predicate is "is a batchelor"
ii) P[x] = "x^2 is greater than x
iii) P(y) = y+2 is non negative

The domain of a predicate variable is the collection of all possible values that the variable may take to become a proposition.

20/10/19

The domain can be also called as the Universe or universe of discours.

The domain can be finite or infinite set.

for ex:-

→ Let $P(x,y) = x>y$ is a predicate in two variables. Let the universe of dicourse P be the set of integers. Then by applying the elements of the universe we can make this predicate a proposition.

ie, set of integers. $\{\ldots -3,-2,-1,0,1,2,3,\ldots\}$

$P(x,y) = x>y$

Take any two values from set,

let $x=1$, $y=2$.

$P(1,2) = 1>2$ which is false. Hence it is a proposition.

$x=-1$ $y=-5$

$P(-1,-5) = -1>-5$ which is true. Hence proposition

If there are more than one predicate variable in the given predicate. Then the universe of discourse may be the same or different for each variable.

In this example, the universe of discourse may not be given to you directly because from the arrangement of predicate, it is clear that x is taken from the universe of individuals, y is taken from universe of cities and z is taken from the universe of years.

But in another example, $P(x,y) = x+y=7$.
$P(x) = x>3$. In these predicates the universe of discourse must be clearly mention.

Now if the predicate is of one variable ie, $P(x)$ where x is the variable then we call $P(x)$ as <u>unary</u> predicate.

If the predicate is of two variables ie $P(x,y)$ then we call it as <u>binary</u> predicate.

And hence the predicate with 'n' variables ie $P(x_1, x_2, \ldots x_n)$ is called <u>n-array</u> predicate or <u>n-place</u> predicate.

<u>Note :-</u>

The predicate variables must be finite.

If $P(x_1, x_2, \ldots, x_n)$ is true for all values $c_1, c_2, c_3 \ldots c_n$ from the universe U then we say that $P(x_1, x_2, \ldots x_n)$ is valid in U.

If it is not all true, i.e., for some values of $c_1, c_2, \dots c_n$ if the predicate $P(x_1, x_2, \dots x_n)$ is false then we say that P is <u>satisfiable</u> in U.

If for all values of $c_1, c_2 \dots c_n$ from the universe U, if the predicate $P(x_1, x_2, \dots x_n)$ is false then we call P as <u>unsatisfiable</u> in U

? Check whether the predicate is valid or not $P(x,y) = (x+y) > (x-y)$ where the universe is the set $\{1,2,3,4,5\}$ ~~6,7,8,9,10}~~.

A. In this we have to substitute the values of x & y from $U = \{1,2,3,4,5\}$

Let $x=1, y=2$

$P(1,2) = 3 > -1$; ~~P(1,2)~~ True

$P(1,3) = 4 > -2$; True

$P(1,4) = 5 > -3$; True

$P(1,5) = 6 > -4$; True

$P(2,3) = 5 > -1$; True

$P(2,4) = 6 > -2$; True

$P(2,5) = 7 > -3$; True

$P(3,4) = 7 > -1$; True

$P(3,5) = 8 > -2$; True

$P(4,5) = 9 > -1$; True.

$P(2,1) = 3 > 1$; True

$P(3,1) = 4 > 2$; True

$P(3,2) = 7 > 1$; True

$P(4,1) = 5 > 3$; True

$P(4,2) = 6 > 2$; True

$P(4,3) = 7 > 1$; True

$P(5,1) = 6 > 4$; True

$P(5,2) = 7 > 3$; True

$P(5,3) = 8 > 2$; True

$P(5,4) = 9 > 1$; True.

This predicate is a valid predicate

A quantifier is something that tells about the amount or quantity of the universe that satisfy the predicate.

There are two types of quantifications/quantifier.

i) Universal quantification / universal quantifier.

A universal quantifier is a quantifier which have the meaning "for all", "for every", "for each", "for any", "for arbitrary". We use the symbol '$\forall$' to denote this ie, if are given the condition that the predicate $P(x)$ is true for every x in the universe U we can denote it by $\forall x \in U, P(x)$ is true.

Eg:-

The square of every real number is non negative can be represented by $\forall x \in R,\ x^2 \geq 0$ where R is the universe of discourse which is the set of real numbers and the predicate $P(x)$ is $x^2 \geq 0$. In other words we write this as U be the set of real numbers $x \in U$. $P(x)$ is $x^2 \geq 0$ $\therefore \forall x\, P(x)$

2) Existential quantifier / Existential Quantification

This is a quantifier which means "there exist", "there is atleast one", "for some". We use the symbol $\exists$ denote this one value of x in the universe.

1) ? Write in the form of qualifier. universe of 2 wheeler

U

i) Every two wheeler is a scooter. predicate = scooter

ii) There exist a lion who drinks coffee.

2) ? Check whether the predicate is satisfiable

$U = \{1, 2, 3, 5\}$ $P(x)$: x^2 is an even number.

1) i) The universe of discourse is two wheelers.

~~Pi~~ 'x' is a scooter.

$\therefore$ The statement is represented by the universal quantifier. $\forall x \in U \; P(x)$

ii)

Let the universe U = is set of integers.
Consider the predicates $x < x+1$ $x=1$ $x=x+1$ where $x \in U$.

Here by applying universal quantifier we have the following truth values

$\forall x\ [x < x+1]$ True

$\forall x\ [x = 3]$ False

$\forall x\ [x = x+1]$ False

By applying the existential quantifier we have

$\exists x\ [x < x+1]$; True.

$\exists x\ [x = 3]$; True.

$\exists x\ [x = x+1]$; False

In general there are two ways to make a predicate into proposition.

1) By assigning particular values to the predicate variables.

ii) By using quantifiers.

Free & Bound Variables.

A variable 'x' in each of the predicate is called a free variable. As 'x' varies over the universe the truth value of the statement may vary.

to be bound variable ie, the variable will be connected by any of the quantifier.
A quantified statement has a fixed truth value

Eg: $\forall x [P(x,y,z)]$ here x is the bound variable whereas y & z are free variables.
Let $y=2$ in the above predicate then the predicate becomes $\forall x [P(x,2,z)]$ here 'x' is the bound variable and 'z' is the free variable

Convertion of a Simple Quantified Statement into compound Statement

$U = \{1,2,3\}$ then $\forall x [P(x)]$ means that $P(x)$ is true for every $x \in U$ and can be represented by $P(1) \wedge P(2) \wedge P(3)$

There exist $\exists x [P(x)]$ means $P(x)$ is true for some values of or for atleast one value of $x \in U$ ie $P(1) \vee P(2) \vee P(3)$

Note:- We cannot interchange the universal quantifier & existential quantifier. But you can interchange the universal quantifier by itself and also existential quantifier by itself every married people.

$\forall x \exists y$ [x is married to y] means that for any 'x' there exist a person y to whom 'x' is married. and hence ~~there~~ this is true.

$\exists x \forall y$ [x is married to y] means that there exist a person y to whom every person 'x' is married and which is false. and hence interchange of order ~~of~~ for different quantifiers are not allowed.

26/10/17.

Negation of a Quantified Statements.

$$\neg[\forall x P(x)] \equiv \exists x \neg P(x)$$

$$\neg[\exists x P(x)] = \forall x \neg P(x)$$

$$\neg[\exists x \neg P(x)] = \forall x \neg\neg P(x)$$

$$= \forall x P(x.$$

Note:-

The negation for quantified statements with n array predicates. we apply the rules of negations from left to right.

ie $\neg(\forall x \exists y P(x,y)] \equiv \exists x(\neg(\exists y P(x,y))$

$$\equiv \exists x \forall y \neg P(x,y)$$

Logical Equivalence of Predicates

$P(x)$ & $Q(x)$ be two predicates defined for a given universe..

$P(x)$ and $Q(x)$ are called logically equalent if by applying the values for the variable from the universe, we must get the same truth value for each predicate. ie
ie, $P(a) \leftrightarrow Q(a)$ is true for every value of 'a' in universe.

? Check the logical equivalence where
$U = \{1, 2, 3, 4\}$.
$P(x): x^2 < 10$ $\quad$ $q(x): 2x > x$

A. $P(1) = 1 < 10 - T$ $\quad$ $q(1) = 2 > 1 - T$
$P(2) = 4 < 10 - T$ $\quad$ $q(2) = 4 > 2 - T$
$P(3) = 9 < 10 - T$ $\quad$ $q(3) = 6 > 3 - T$
$P(4) = 16 < 10 - F$ $\quad$ $q(4) = 8 > 4 - T$

This is not logically equivalence

Logical Implication

Let $P(x)$ & $q(x)$ be two predicates defined on the universe if the implication $P(a) \rightarrow q(a)$ is true for every 'a' in the universe we say that ~~$P(x) \rightarrow Q(x)$~~

denoted by $p(x) \Rightarrow q(x)$.

? $U = \{1,2,3,4\}$ $p(x) = x^2 < 10$ $q(x) ; 2x > x$

check $p(x) \Rightarrow q(x)$

$p(1) = 1 < 10$ T $\quad q(1) = 2 > 1$ T $p(1) \rightarrow q(1)$ is true

$p(2) = 4 < 10$ T $\quad q(2) = 4 > 2$ T $p(2) \rightarrow q(2)$ "

$p(3) = 9 < 10$ T $\quad q(3) = 6 > 3$ T $p(3) \rightarrow q(3)$ "

$p(4) = 16 < 10$ F $\quad q(4) = 8 > 4$ T $p(4) \rightarrow q(4)$ true

$\therefore$ $p(x) \Rightarrow q(x)$.

27/10/17

Theory of Inference - Validity of Arguments.

? For every integer n, n is even if it is divisible by 2.

A. The logical expression will be

Universe of discourse is the set of integers.

$x \in U$

$p(x)$: x is even

$q(x)$: x is divisible by 2.

$\therefore$ $\forall x \left[q(x) \rightarrow p(x) \right]$

? All mathematics professors have studies calculus.

Universe of discourse is set collection of maths professors.

$x \in U$

$p(x)$: x have studies calculus.

expressions $\underline{\quad\quad}$.

'or'

Let universe of discase be collection of all people then the predicates p(x) : x is a mathematics professor, q(x) : x have studied calculus.

∴ The logical expression is

$$\forall x\,[p(x) \wedge q(x)]$$

? All mathematics professors have studied calculus. Leena is a mathematics professor. Therefore Leena have studied calculus. here U cannot be maths pro becoz we cannot rep and state so U → people

A. Let the universe of discourse be collection of people. The predicates are.

p(x) : x is a mathematics professor.

q(x) : x have studies calculus.

l : Leena

The logical expression is

$$\forall x\,[p(x) \rightarrow q(x)]$$

$$p(l)$$

$$\therefore \cancel{[p(l) \wedge q(x)]}$$

$$\therefore q(l)$$

Socrates is a men.
Therefore Socrates is mortal.

A. U is the collection of all people.
The predicates are.

p(x) : x is a men.
q(x) : x is ~~socrates~~ mortal.
s : Socrates

The logical expression is.

$$\forall x \left[p(x) \rightarrow q(x)\right]$$
$$\underline{p(s)}$$
$$\therefore q(s)$$

? One student in the class knowns how to make programs in JAVA and everyone who knows how to write programs in JAVA can get a high paying job. imply the condcusion someone in this class can get a high paying job.

p(x) : x is a student in the class
q(x) : x knows how to write progms in JAVA.
r(x) : x. ~~get~~ will get a high paying job.

$\exists x \; [p(x) \wedge \ldots]$
$\forall x \; [q(x) \rightarrow r(x)]$

$\therefore \exists x \; [p(x) \rightarrow r(x)]$

30/10/17

? Every computer science student needs a course in Maths. Salim is a CS student.
$\therefore$ Salim needs a course in Maths.

A. The logical expression are :-

$p(x)$: x is a cs student.
$q(x)$: x needs a course in Maths.
s : salim.

$\therefore$ The premise & the conclusion are.

$\forall x \, [p(x) \rightarrow q(x)]$
$p(s)$

$\therefore q(s)$

? A student in this class has not read the book. and everyone in this class passed the first examination imply the conclusion. Someone who passed in the first examination has not read the book.

and means next premise

$p(x)$: x is in this class.

$q(x)$: x has read the book.

$r(x)$: x has passed in the first examination.

The premise & conclusion are.

$$\exists x\, [p(x) \rightarrow \neg q(x)]$$
$$\forall x.\, [p(x) \rightarrow r(x)]$$
$$\therefore \exists x.\, [r(x) \rightarrow \neg q(x)]$$

Inference Theory for Predicate calculus.

1) Rule of universal specifications.

If a predicate becomes true for all replacements by the member of the given universe then that predicate is true for each specific individual. member in that universe ie,

if $\forall x\, p(x)$ is true. then we can conclude that $p(c)$ is true, for c is an arbitrary member of the universe

2) Rule of Universal Generalisation

If a predicate $p(x)$ is proved to be true when x is replaced by any arbitrarly choosen element c from our universe then the universal quantifier ~~A~~ $\forall x\, p(x)$ is true.

universe and if $p(c)$ is true then we conclude that $\forall x\ p(x)$ is true.

3) <u>Rule of Existential Specification</u>

This rule allows us to conclude that if $\exists x\ p(x)$ is true then $p(c)$ is true where c is not an arbitrary member of the universe, but one among them for which $p(c)$ is true

4) <u>Rule of Existential Generalisation.</u>

This rule is used to conclude that for a particular element c in the universe, if $p(c)$ is true then $\exists x\ p(x)$ is true

31/10/19 <u>Note :-</u>

→ Universal specification is used to eliminate the universal quantifier from the quantified statement. Universal generalisation is used to introduce the universal quantifier into the statement.

→ Existential Specification is used to eliminate existential quantifier. And Existential generalisation is used to introduce existential quantifier.

Consider the predicates

$m(x)$: x is a Physics professor.

$c(x)$: x have done Physics lab.

r : Rashmi

The logical expression is:

$$\begin{array}{l} \forall x\,[m(x) \rightarrow c(x)] \\ m(r) \\ \hline \therefore\ c(r) \end{array}$$

A.

Steps	Reason
1) $\forall x\,[m(x) \rightarrow c(x)]$	premise
2) $m(r) \rightarrow c(r)$	U. Specifications.
3) $m(r)$	premise
4) $c(r)$	2,3 by modus ponens

?

$$\begin{array}{l} \forall x\,[p(x) \rightarrow Q(x)] \\ \forall x\,[R(x) \rightarrow \neg Q(x)] \\ \hline \forall x\,[R(x) \rightarrow \neg p(x)] \end{array}$$

Steps	Reason
1) $\forall x\,[R(x) \rightarrow \neg Q(x)]$	premis.
2) $R(a) \rightarrow \neg Q(a)$	U.S.
3) $\forall x\,[p(x) \rightarrow Q(x)]$	Premise.
4) $p(a) \rightarrow Q(a)$	U.S.

6) $R(a) \longrightarrow \neg P(a)$ 2&5 Law of syllogism

7) $\forall x \, [R(x) \longrightarrow \neg P(x)]$ U. G.

Proof Technique

Direct Proof

Here we begin with the premise (hypothesis), continuing with a sequance of deduction we end with a conclusion

? For eg: If m is an even integer then prove that $m+7$ is odd integer. by direct proof method

A. Here the given hypothesis is m is an even integer we have to prove that $m+7$ is an odd integer.

Since m is even $\rightarrow m = 2k$, k is any integer.

Substituting $m = 2k$ in $m+7$ we have

$$m+7 = 2k+7$$
$$= (2k+6)+1$$
$$= 2(k+3)+1$$
$$= 2t+1 \quad ; \; t = k+3$$

Here $2t+1$ is an odd number since $2t$ is an even number. $\therefore$ $m+7$ is an odd numb

Note:-

In many cases direct proof may not reach at a conclusion. then we use another methods for proving the theorems of the form $p \to q$ These are called indirect proofs. They are:-

1) Proof By Contraposition | Contrapositive Proof | Indirect Proof
2) Proof By Contradiction.
3) Proof By Counter example.
4) By Mathematical Induction.

1) Proof By Contraposition.

We know that the contrapositive of $p \to q$ is $\neg q \to \neg p$. So proving in this method we apply direct proof method to the statements. $\neg q \to \neg p$.

? If m is an even integer then m+7 is an odd integer by using contrapositive method

A. The contrapositive argument is.
"If m+7 is not odd integer then m is not an even integer. $(\neg q \to \neg p)$.
To prove this let m+7 is not an odd integer implies m+7 is an even integer $\to$ m+7 = 2s

$= 2s - 8 + 1$
$= 2(s-4)+1$

$\rightarrow$ m is a odd integer $\rightarrow$ m is not even integer. Hence proved.

Q Prove that a perfect number is not prime by indirect proof method.

A. This statement can be rewritten as
"If x is a perfect number then x is not a prime number."
The contrapositive statement is.
"If x is a prime number then x is not a perfect number."

A perfect number is a number whose divisors except the given number when added gives the given number.
eg: 6 divisors: 1, 2, 3, 6. exclude 6 & $1+2+3 = \underline{6}$
$\therefore$ 6 is a perfect number
18 is not a perfect number 1, 2, 3, 6, 9, 18
$1+2+3+6+9 \neq 18$.

Let x is a prime number then the only divisors of x are 1 & x
Leaving out x we will have the only divisor as 1 and 1 cannot ... to x

is not a perfect number. Hence proved.

2) <u>Proof By condridiction</u>

In this method to prove $p \rightarrow q$ we will be assuming $\neg q$ (ie, the conclusion is false). And by deducing we will reach at a condition where some of our predefined statement is false. This will be happening since we have assumed a wrong argument.

? Prove that $\sqrt{2}$ is not a rational number by contradiction method.

A. Suppose that $\sqrt{2}$ is a rational number. Then by definition, of rational number, we have $\sqrt{2} = \frac{p}{q}$, where p & q are integers and p & q are relatively prime ie, there is no common divisors for p & q.

$\sqrt{2} = p/q$

on squaring, we have $2 = \frac{p^2}{q^2}$

$\Rightarrow 2q^2 = p^2$ ie $p^2 = 2q^2$.

$\Rightarrow p^2$ is an even number.

$\Rightarrow p$ is an even number.

$p = 2k$, k is an integer.

Substituting,

$p = 2k$ in $p^2 = 2q^2$, we have

$$(2k)^2 = 2q^2 \Rightarrow 4k^2 = 2q^2$$
$$\Rightarrow q^2 = 4k^2$$
$$\Rightarrow q^2 \text{ is even number.}$$
$$\Rightarrow q \text{ is even number}$$

ie, q can be written in the form $q = 2s$, where s is an integer.

$\therefore$ we have $p = 2k$ and $q = 2s$, where $k, s \in I$

ie, p and q have a common factor 2.

ie, p and q are not relatively prime.

This is contradiction.

$\therefore$ our assumption is false.

$\therefore$ $\sqrt{2}$ is not a rational number.

3/11/17

3) Proof By Counterexample

Suppose we want to prove that the statement $\forall x$. is false then. by this method we want to find an element x such that $p(x)$ is false. The number x

? Check whether the given statement is true or false with counter example method.
All prime numbers are odd

A. Consider the number 2 which is a prime number but not an odd number. Hence our statement is false. 2 is the counter example

4) Proof by Mathematical Induction

In this method we show that the result is true for $n=1$
Assume that the result is true for $n=k$
Then we will show that the result will be true for $n=k+1$ if so we conclude that the result is true for all natural numbers 'n'

? Using mathematical induction prove that if 's' is a finite set with n elements then s has 2^n subsets.

A. By mathematical induction first we have to prove that the given statement is true for $n=1$
For every set with one element it will definitely have only two subsets ie null sell $\{\phi\}$ & the set itself. Therefore the

[illegible]
have only one element then it have two subsets.

Assume that the result is true for $n=k$ ie, if a set ~~A~~ S has k elements then it have 2^k subsets.

Finally we will prove that the statement is true for $n=k+1$ ie, we have to prove that if S is a set, with $k+1$ elements then it has 2^{k+1} subsets.

Let $S=\{a_1, a_2, a_3, \ldots a_k, a_{k+1}\}$ with cardinality $k+1$

Let $S_1=\{a_1, a_2, a_3, \ldots a_k\}$ then $S=S_1\cup\{a_{k+1}\}$

By assumption S_1 has 2^k subsets and $\{a_{k+1}\}$ has two subsets. Therefore in total S has $2^k \cdot 2$ subsets ie, 2^{k+1} subsets.

$\therefore$ The statement is true for $n=k+1$.

Hence the proof.