Algebraic Structure (Group Theory)

⇒ binary operator

* is called binary operator iff
$\forall a, b \in A$, $A * A \rightarrow A$

Properties of Binary Operator

① Closure Property

$\forall a, b \in S \quad a * b \in S$
then S is closed under *

ex. ⇒ $(N, +)$ ✓ ⇒ $a, b \in N$ then $a+b \in N$
Addition follows closure property for natural nos.
$(N, -)$ ✗ $(I, +)$ ✓ $(I, -)$ ✓

② Associativity (order not important) ⇒ depends on operator

$\forall a, b, c \in S$, $a * b * c$ ∈ S

ex ⇒ $(N, +)$ ✓
$(N, -)$ ✗

③ Identity property (operator)

$\forall a \in S, \exists e \in S \Rightarrow a * e = e * a = a$

0 ⇒ additive identity 1 ⇒ multiplicative identity.

$(N, +)$ ✗ $(W, +)$ ✓ $(R, +)$ ✓

$(N, *)$ ✓

④ Inverse

$\forall a \in S, \exists b \Rightarrow a * b = b * a = e$

ex ⇒ $(R, +) \Rightarrow 2 + (-2) = 0 \quad \therefore b = -2.$

$(R, *) \Rightarrow 2 * (1/2) = 1 \quad \therefore b = 1/2$

⑤ Commutative property (operator)

$\forall a, b \in S \quad a * b = b * a$

ex ⇒ $(N, +)$ ✓

① ⇒ Algebraic structure.

① and ② ⇒ Semi-group.

①, ②, ③ ⇒ Monoid

①, ②, ③, ④ ⇒ Group

①, ②, ③, ④, ⑤ ⇒ Abelian group.

①, ②, ⑤ ⇒ Commutative semi-group.

Prove that $(Q - \{1\})$ is group, where

$a * b = a + b - ab$, $\forall a, b \in (Q - \{1\})$

Sol^n. ⇒ Closure:

$\forall a, b \in S$, $a * b \in S$

$a * b = a + b - a \times b$

$= Q + Q - (Q \times Q)$

$= Q - Q$

$= Q$

Associativity:

$\forall a, b, c$ $\quad (a * b) * c = a * (b * c)$

$LHS = (a * b) * c = (a + b - ab) * c$

$= a + b - ab + c - [(a + b - ab) \times c]$

$= a + b + c - ab - ac - bc + abc$

$RHS = a * (b * c) = a * (b + c - b \times c)$

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

$= a + b + c - bc - ab - ac + abc$

∴ semi-group

Identity:

$\forall a \in S$, $\exists e \in S$ $\quad a * e = e * a = a$

$a * e = a$

$a + e - ae = a$

$e(1 - a) = 0$ $\quad$ but $a \neq 1$ $\quad \therefore \boxed{e = 0}$

$a = e * a = e + a - ea = e(1 - a) = 0$ $\quad \therefore \boxed{e = 0}$ $\quad \therefore$ monoid

Inverse:

if $a^{-1} = b$ $\therefore a \times b = e$

$a * b = 0$

$a + b - ab = 0$

$a + b = ab \Rightarrow b = \frac{a}{a-1}$ $\therefore a^{-1} = \frac{a}{a-1}$

$\therefore$ ~~$a = ab - a$~~

$\therefore$ Group

Commutative:

$a * b = a + b - ab$ $\therefore$ Abelian group.

$b * a = b + a - ba$

classmate
Date
Page

Que 1] Let G be a set of all matrices of type $\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ where $m \in Z$. Prove that G is a group under multiplication. Is it Abelian group?

Sol^n ⇒ Closure: $\forall a, b, \in G \Rightarrow a * b \in G$

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}, \quad a+b \in Z \quad \therefore a * b \in G$$

$\therefore$ Closure

Associativity:
Multiplication is always associativity.

Identity:
$\because \forall m \in G \Rightarrow m * I = m * I = m$

$\therefore I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is identity.

Inverse:
for inverse, $|A| \neq 0$

$A = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \Rightarrow |A| = 1 \quad \therefore \forall m$ have inverse.

$A^{-1} = \begin{bmatrix} 1 & -m \\ 0 & 1 \end{bmatrix} \in G \quad \therefore$ Identity Inverse

Commutative:

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$$

$\therefore$ Commutative.

$$\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$$

⇒ This is Abelian group.

ex. 1] Prove that $G = \{1, -1, i, -i\}$ is group under multiplication. Is it Abelian?

Soln ⇒ 1] Composition Table

×	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

From table, $\forall a, b \in G$, $a * b \in G$

∴ Closure ✓ Algebraic structure

2] multiplication for nos. is associative ∴ Semi group

3] Identity

∵ First row = header of column
First column = index of row.
∴ Intersection of I row & I column = identity demand.
∴ $\boxed{I = 1}$ ∴ monoid

4] Inverse

$1^{-1} = 1$ $\quad -1^{-1} = -1$
$i^{-1} = -i$ $\quad -i = i$ ∵ Each element has inverse.
∴ Group. $\quad (G, \times)$ is group

5] ∵ Monoid is symmetric.
$\forall a, b \in G$ $\quad a * b = b * a$ Commutative
∴ Abelian group

Cyclic group

If in group $(G, *)$, there exists an element 'a' which power (integer) can generate all elements of a group then the group is called cyclic group. and 'a' is called generator.

OR

group $(G, *)$ is called cycle if all elements of G represented as a^k, $k \in I$.

Note ⇒ identity element is never generator (except trivial group)

⇒ if $a^{-1} = b$ and a is generator then b is also generator

⇒ if $a^{-1} = a$, it is generator only if $\{a, e\}$

⇒ every cyclic group is Abelian group.

ex. 2] Prove that $(G, +_6)$ is cyclic group where $+_6$ is addition module 6.

Sol" ⇒ $G = \{0, 1, 2, 3, 4, 5\}$ $\quad a +_6 b = (a+b) \cdot 1 \cdot 6$

$+_6$	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

i) Closure ⟶ $a_1 a_2 \in G$

ii) Associative ⟶

iii) Identity ⟶ $e=0$

iv) $0^{-1} = 0$

$\bar{1} = 5$

$2^{-1} = 4$

$3^{-1} = 3$

$4^{-1} = 2$

$5^{-1} = 1$ ~~Idd~~ Inverse. ⟶

v) Cyclic gup ⇒ $(1)^1 = 1$

$(1)^2 = 1 +_6 = 2$

$(1)^3 = 1^2 +_6 1 = 2+1 = 3$

$(1)^4 = 1^3 +_6 1 = 3+1 = 4$

$(1)^5 = 1^4 +_6 1 = 4+1 = 5$ ⟶

$(1)^6 = 1^5 +_6 1 = 5+1 = 6$

~~(1)~~^{7} = .

★ Coding theory

B^m $\quad m < n \quad$ B^n

$e : B^m \to B^n$

Ex. ⇒ 000 (original) $\quad 2^3 = 8$

000001 (encrypted msg) $\quad 2^6 = 64$

Group code

The encoding function $e : B^m \to B^n$ $(m < n)$ is said to be a group code if range of $e \in B^n$ is a subgroup.

i.e., prove $(e(B^n), \oplus)$ is subgroup.

(i) closure
(ii) identity
(iii) inverse

Ex. 1] Show that $e : B^2 \to B^5$ is group code.

$e_0(00) = 00000$
$e_1(01) = 01110$
$e_2(10) = 10101$
$e_3(11) = 11011$

Sol.⇒ $N = \{e_0, e_1, e_2, e_3\}$ $(N, \oplus)$

If $e_1 \oplus e_2 = e_3$
$e_1 \oplus e_3 = e_2$
$e_2 \oplus e_3 = e_1$

$\oplus$	e_0	e_1	e_2	e_3
e_0	e_0	e_1	e_2	e_3
e_1	e_1	e_0	e_3	e_2
e_2	e_2	e_3	e_0	e_1
e_3	e_3	e_2	e_1	e_0

$e_0 \oplus e_0 \Rightarrow$ 00000 + 00000 = 00000

EXOR anything with 0 ⇒ answer is other operand.

ex ⇒ $0 \oplus 1 = 1$
$0 \oplus 0 = 0$

EXOR anything with itself = 0

$e_1 \oplus e_2$: 01110 + 10101 = 11011

i] closure ⇒ all $\in N$
ii] identity ⇒ e_0
iii] inverse ⇒ every element has inverse

∴ Group code

Ex. 2] Show that (3, 7) encoding function given below is a group code.

$e_0(000) = 000\ 0000$
$e_1(001) = 001\ 0110$
$e_2(010) = 010\ 1000$
$e_3(011) = 011\ 1110$
$e_4(100) = 100\ 0101$
$e_5(101) = 101\ 0011$
$e_6(110) = 110\ 1101$
$e_7(111) = 111\ 1011$

$\oplus$	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_0	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	e_0	e_3	e_2	e_5	e_4	e_7	e_6
e_2	e_2	e_3	e_0	e_1	e_6	e_7	e_4	e_5
e_3	e_3	e_2	e_1	e_0	e_7	e_6	e_5	e_4
e_4	e_4	e_5	e_6	e_7	e_0	e_1	e_2	e_3
e_5	e_5	e_4	e_7	e_6	e_1	e_0	e_3	e_2
e_6	e_6	e_7	e_4	e_5	e_2	e_3	e_0	e_1
e_7	e_7	e_6	e_5	e_4	e_3	e_2	e_1	e_0

Sol.⇒ $e_1 \oplus e_2 = 001\ 0110 + 010\ 1000 = 011\ 1110$

$e_1 \oplus e_3 = e_2$
$e_3 \oplus e_2 = e_1$

$e_2 \oplus e_5 \Rightarrow 010\ 1000 + 101\ 0011 = 111\ 1011 = e_7$

$e_1 \oplus e_4 = 001\ 0110 + 100\ 0101 = 101\ 0011 = e_5$

$e_4 \oplus e_4$: 010 1000 + 100 0101 = 110 1101 $= e_6$

$e_3 \oplus e_5 \Rightarrow 011\ 1110 + 101\ 0011 = 110\ 1101$

$e_3 \oplus e_4 = 011\ 1110 + 100\ 0101 = 111\ 1011 = e_7$

$e_5 \oplus e_6 \Rightarrow 101\ 0011 + 110\ 1101 = 011\ 1110$

$e_1 \oplus e_6$: 001 0110 + 110 1101 = 111 1011 $= e_7$

Weight

If a word $x \in B^n$, then the number of 1's in x is called weight of x.

ex. ⇒ $x = 01101$ $\quad |x| = 3$

$x = 00000$ $\quad |x| = 0$

$x = 11110$ $\quad |x| = 4$

Hamming distance

Hamming distance between x, y is weight of $x \oplus y$ or the no. of position in which x and y differ.
It is denoted as $\delta(x,y) = |x \oplus y|$

ex-1 $x = 1111$ $\quad \delta(x,y) = |x \oplus y|$

$y = 0116$ $\quad = |10011| = 2$

Theorem

If $e : B^m \to B^n$ is incoding function with minimum distance 'd' then,
it can detect 'd-1' or fewer errors.
it can correct $\frac{d-1}{2}$ or fewer errors.

Parity check matrix

Let $m < n$ and $k = n - m$.

A boolean matrix of order $n \times k$.

$$H = \left[\begin{array}{cccc} h_{11} & h_{12} & \cdots & h_{1k} \\ h_{21} & h_{22} & \cdots & h_{2k} \\ \vdots & & & \\ h_{m1} & h_{m2} & \cdots & h_{mk} \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \\ 0 & \cdots & & 1 \end{array}\right]$$

$h_{11} \ldots h_{mk}$: Parity matrix.

$1 \ldots 1$: $k \times k$ identity matrix.

Parity check matrix.

This is called Parity check matrix.

Group code

Let $e_h : B^m \to B^n$ and $b = b_1 b_2 b_3 \ldots b_m$ is element of B^m then encoding $e(b) = b_1 b_2 b_3 \ldots b_m x_1 x_2 \ldots x_k$ is called group code of b. where x_1, x_2, x_3 are parity bit given by

$$[x_1 \; x_2 \ldots x_k] = [b_1 \; b_2 \ldots b_m] \otimes \begin{bmatrix} h_{11} & h_{12} & h_{1k} \\ h_{21} & h_{22} & h_{2k} \\ h_{m1} & h_{m2} & h_{mk} \end{bmatrix}$$

Note : $[b_1 \; b_2] \otimes \begin{bmatrix} h_{11} \\ h_{21} \end{bmatrix} = (b_1 \otimes h_{11}) \oplus (b_2 \otimes h_{21})$

ex.1] Let $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ Determine the group code $B^2 \to B^5$.

Soln ⇒ Given ⇒ $B^2 \to B^5$

$B^2 = \{00, 01, 10, 11\} \Rightarrow B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$

Now, $H_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

$\therefore X = B \otimes H_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

$= \begin{bmatrix} (0\otimes 1)\oplus(0\otimes 0) & (0\otimes 1)\oplus(0\otimes 1) & (0\otimes 0)\oplus(0\otimes 1) \end{bmatrix}$

I ⇒ 00 ⇒ all zero
II ⇒ 01 ⇒ second row
III ⇒ 10 ⇒ first row
IV ⇒ 11 ⇒ bitwise add^n of first and second row.

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

$\therefore$ Encoding Msg is group code

$e(b) = b_1 b_2 \cdots b_m x_1 x_2 \cdots x_3$

e(00) = 00 000
e(01) = 01 011
e(10) = 10 110
e(11) = 11 101

} group code

Ex. 2] Let $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ Determine the group code, $B^3 \to B^6$.

Sol.ⁿ ⇒ $B^3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$ $H_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

$\therefore X = B \otimes H_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

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

$e(000) = 000\,000$ $\quad e(100) = 100\,100$

$e(001) = 001\,111$ $\quad e(101) = 101\,011$

$e(010) = 010\,011$ $\quad e(110) = 110\,111$

$e(011) = 011\,100$ $\quad e(111) = 111\,000$

Decoding of encrypted message

Maximum likelihood test

Let group code $N = \{e_0, e_1, e_2, e_3\}$

Decode of word 'w' is group code which have minimum hamming distance from w.

i.e., $d(w) = \{e_i \mid e_i \in N \text{ & } \delta(w, e_i) \text{ is minimum}\}$

ex. 1] Consider (3, 5) group code $e_4 : B^3 \to B^5$

$e_0(000) = 000\ 00$
$e_1(001) = 001\ 10$
$e_2(010) = 010\ 01$
$e_3(011) = 011\ 11$
$e_4(100) = 100\ 01$
$e_5(101) = 101\ 01$
$e_6(110) = 110\ 10$
$e_7(111) = 111\ 00$

Decode the following word.

i) 11001
ii) 01010
iii) 00111

If d is 1 ⇒ that e_i is answer, no need to check further.

Soln. ⇒ Let w = 11001

Hamming dist.

$\delta(w, e_0)$	= 3	2	3
$\delta(w, e_1)$	= 5	2	1
$\delta(w, e_2)$	= 1	2	
$\delta(w, e_3)$	= 3	2	
$\delta(w, e_4)$	= 2	3	
$\delta(w, e_5)$	= 2	5	
$\delta(w, e_6)$	= 2	1	
$\delta(w, e_7)$	= 2	5	
	$\therefore d(w) = e_2 = 010$	$\therefore d(w) = e_6 = 110$	$\therefore d(w) = e_1 = 001$

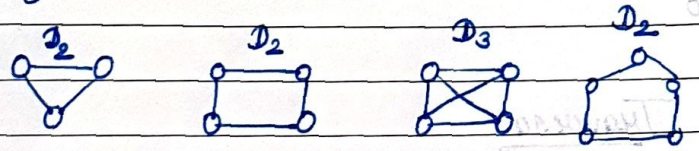
Graph Theory

A graph is a collection of object with relationship.
Object is called vertex or node and relationship is called edge.
A graph is represented by a ordered pair $G = (V, E)$
where $V \Rightarrow$ Non-empty set of vertices.
$E \Rightarrow$ set of edges.

Special graph

$G_1 \Rightarrow$ O $\Rightarrow$ trivial graph

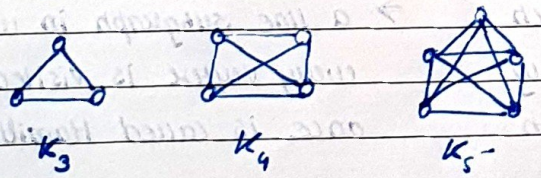
$G_2 \Rightarrow$ O O O $\Rightarrow$ NULL graph

$G_3 \Rightarrow$ 

$D_n \Rightarrow$ degree of each vertex is same $\Rightarrow$ Regular graph.

Complete graph (K_n)

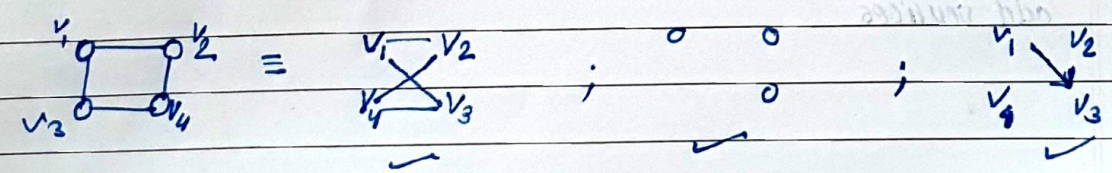
Every vertex is connected to all other vertices.



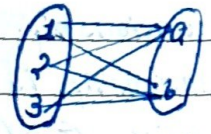
$K_n \Rightarrow n \Rightarrow$ no. of vertices.

Bipartite graph

If vertices are partitioned into two set such as all vertices of same partition are disconnected.



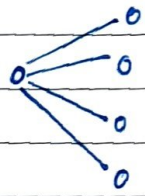
Complete bipartite graph ($K_{m,n}$)



$K_{3,2}$ (connected to all vertices of other partition)

$m=3 \quad n=2 \quad \Rightarrow$ edges $= m \times n = mn$

Star graph ($K_{1,m}$) ⇒ Hub one side; other vertices other side.



Graph Traversal

Graph Traversal

↓ Euler path

⇒ a line subgraph in which every edge is visited only once is called Euler path

Theorem ⇒ If graph has exactly two odd degree vertices then graph has Euler path ⇒ start and end at odd vertices

↓ Hamilton path

⇒ a line subgraph in which every vertex is visited only once is called Hamiltonian path.

Theorem ⇒ If in graph, sum of degree of each adjacent pairs of vertices is $< n-1$, then graph never have Hamiltonian path.

Euler graph

A closed Euler path is called Euler circuit and graph in which it exists is called Euler graph

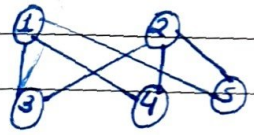
Theorem ⇒ If degree of each vertex is even, then graph is called Euler graph.

Hamiltonian graph

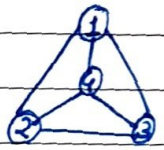
A closed Hamiltonian graph is called Hamiltonian circuit and graph in which it exists is called Hamiltonian graph.

Theorem ⇒ If degree of any vertex is $< n/2$, then graph never have Hamiltonian circuit.

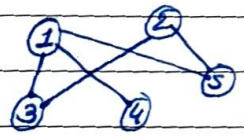
ex. ⇒



⇒ (1) and (2) has odd degree (3)
∴ Euler path
But not all have even degree
∴ not Euler graph.



⇒ All vertices covered ∴ Hamiltonian path



⇒ Hamiltonian path ✓
⇒ we can't return to starting pt.
∴ Not Hamiltonian circuit.

Logic

ex.

Logical operators

1] AND ($\wedge$)

⇒ binary operator

Truth table

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

2] OR ($\vee$)

⇒ binary operator

Truth table

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

3] Not ($\sim$)

$\sim p = p'$

p	$\sim p$
T	F
F	T

4] Implication

$p \to q$ = if p then q $\equiv \sim p \vee q$

Truth table

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

ex.1] Check truthness of $(p \to q) \vee q \to p$

p	q	$p \to q$	$(p \to q) \vee q$	$[(p \to q) \vee q] \to p$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F
F	T	T	T	F

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

p	q	$p \to q$	$(p \to q) \wedge p$	$[(p \to q) \wedge p] \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Mathematical induction (MI)

Induction base

Check the given statements/series is true or not for some value of n.
i.e. ⇒ n=0, n=1, etc.

Induction hypothesis

Assume that statement/series is true upto n=k
f(k) = True ⇒ Assume

Induction step

Check for n=k+1
f(k+1) = ?

Que 1] Prove by mathematical induction that $1^2+2^2+3^2+\ldots = n/6\ (n+1)(2n$

Sol^n ⇒ $f(n) = 1^2+2^2+3^2+\ldots = \frac{n(n+1)(2n+1)}{6}$

1] Induction base

n=1 ⇒ $f(1) = 1^2 \Rightarrow f(1) = 1^2 = 1$

~~for~~ n=1, true ∴

2] Induction hypothesis

Assume for n=k

∴ $f(k) = 1^2+2^2+3^2+\ldots \frac{k}{6}(k+1)(2k+1)$

classmate
Date
Page

3] Induction step

Check for $n=k+1$

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

$$= \frac{k+1}{6}[(k+1)+1][2k+1] + (k+1)^2$$

$$= \frac{(k+1)}{6}(k+1)\left\{\frac{k(2k+1)}{6} + k+1\right\}$$

$$= k+1\left\{\frac{2k^2+k+6k+6}{6}\right\}$$

$$= \frac{(k+1)}{6}[2k^2+7k+6)$$

$$= \frac{(k+1)}{6}(k+2)(k+3)$$

$$= \frac{(k+1)}{6}[(k+1)+1][2(k+1)+1]$$

$\therefore$ true for $n=k+1$.

Q.2) P.T $\frac{1}{1\cdot3} + \frac{1}{3\cdot5} + \frac{1}{5\cdot7} + \dots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$

S.1 Induction base

$f(n) = \dots$

$f(1) = \frac{1}{1\cdot3} = \frac{1}{3}$

$f(1) = \frac{1}{(2(1)-1)(2(1)+1)} = \frac{1}{1(3)} = \frac{1}{3}$ | f(1) is true.

$f(1) = \frac{1}{2(1)+1} = \frac{1}{3}$ //

2

#25 February 2003

Camlin Page (1)

6.

x	0	1	2	3
P(x=x)	1/6	1/3	1/3	1/6

S.2 Induction Hypothesis assumes induct^n is true for $n=k$

$f(k) = \frac{1}{1\cdot3} + \frac{1}{3\cdot5} + \frac{1}{5\cdot7} + \dots + \frac{1}{(2k-1)(2k+1)} = \frac{k}{(2k+1)}$

S.3 Ind^n step check for $n=k+1$

$f(k+1) = \frac{1}{2k} \quad \frac{1}{1\cdot3} + \frac{1}{3\cdot5} + \dots + \frac{1}{(2(k+1)+1)(2(k+1)-1)}$

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

$= \frac{1}{(2k+2)}\left\{1 + \frac{1}{2k+1}\right\}$

$= \frac{2(k+1)}{(2k+3)(2k+1)}$

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

$= \frac{k}{2k+1} + \frac{1}{(2k+1)(2k+3)}$

$= \frac{1}{(2k+1)}\left[k + \frac{1}{(2k+3)}\right]$

$=$

$$f(k+1) = \frac{k(2k+3)+1}{(2k+1)(2k+3)}$$

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

$$= \frac{(k+1)}{(2k+1)(2k+3)}$$

$$f(k+1) = \frac{(k+1)}{(2(k+1)-1)(2(k+1)+1)} \quad //$$

Q.3] $11^{n+2} + 12^{2n+1}$ is divisible by 133. $(n \geq 1)$

Sol:⇒ $f(n) = 11^{n+2} + 12^{2n+1}$

1] Base:

Check for $n=1$

$(11)^3 + (12)^3 = 3059 \div 133 = 23$

True for $n = 1$.

2] Hypothesis

Assume for $n=k$, true

$\therefore f(k) = 11^{k+2} + 12^{2k+1} = 133x, \; x \in I$

3] Step.

Check for $n=k+1$

$f(k+1) = 11^{(k+3)} + 12^{2k+3}$

$= (11)^{k+2} \cdot 11 + (12)^{2k+1} \cdot (12)^2$

$= (11)^{k+2} \cdot 11 + 11 \cdot (12)^{2k+1} + 133 \cdot (12)^{2k+1}$

$= 11\left[(11)^{k+2} + (12)^{2k+1}\right] + 133 \cdot (12)^{2k+1}$

$= 11[133x] + 133(12)^{2k+1}$

$= 133\left[11x + (12)^{2k+1}\right] = 133y, \; y \in I.$

4] P.T. $7^n - 1$ is divisible by 6. $(n \geq 1)$

Soln:⇒ $f(n) = 7^n - 1$

1] Base

Check for $n = 1$

$\Rightarrow 7^{(1)} - 1 = 7 - 1 = 6$

$\therefore$ True for $n = 1$

2] Hypothesis.

Assume true for $n = k$

$\therefore f(k) = 7^k - 1 = 6x \quad , x \in I$

3] Step

Check for $n = k+1$

$\therefore f(k+1) = 7^{k+1} - 1$

$= 7^k \cdot 7 - 1$

$= 7^k \cdot 7 - 7 \cdot 1 + 6 \cdot 1$

$= 7[7^k - 1] + 6 \cdot 1$

$= 7[6x] + 6$

$= 6[7x + 1] = 6y \quad , y \in I.$

$\therefore$ True for $n = k+1$.

5] 13 students are selected from a class. Prove that atleast 2 of them must have their birthday in the same month of the year.

6] Prove that if 8 people are assembled in a room, then 2 of them are on same day of week.

7] How many friends must have to guarantee that atleast 5 of them will have birthday in same month?

8] Prove that 7 colours are used to paint 50 bicycles, then 8 of them must have same colour.