ST- 2 Solution

Sub Code : RCS- 301

Sub Name : Discrete structure & theory of logic

Branch : CSE/IT

Section : CS-1, 2, 3 & IT-1, 2

Year : 2nd Year

Sem : IIIrd

Faculty : Mr. Narendra, Mr. Panchanan.
Ms. Nishu & Ms. Lipika Gupta.

Reviewer by :- Yogita Chhabra

Section-A (5X2=10)

A. Attempt all the parts

Q.1. Prove that a ring R is commutative if and only if
$$(a+b)^2 = a^2 + 2ab + b^2 \ \forall \ a, b \in R$$

Ans. Case 1 let R is commutative ring

i.e. $ab = ba$ —— (1)

$(a+b)^2 = \cancel{a^2+2ab}\ (a+b)(a+b) = aa + ab + b.a + b.b$

$= a^2 + ab + ab + b^2$ (from 1)

$= a^2 + 2ab + b^2$

Converse Case 2 let $(a+b)^2 = a^2+2ab+b^2 \ \forall \ a, b \in R$

& Prove $ab = ba$

$(a+b)^2 = a^2 + 2ab + b^2$

$\Rightarrow (a+b)(a+b) = a^2 + 2ab + b^2$

$\Rightarrow \cancel{a^2} + ab + ba + \cancel{b^2} = \cancel{a^2} + 2ab + \cancel{b^2}$ (by left & right cancellation law)

$\Rightarrow \cancel{ab} + ba = \cancel{ab} + ab$

$\Rightarrow ba = ab$

Hence proved R is commutative ring.

Q.2. Distinguish between bounded lattice and complemented lattice.

Ans. Bounded lattice $\Rightarrow$ A lattice is said to be bounded if there exist greatest & least element in the lattice.
Greatest element $= 1$ and least element $= 0$.

Complemented lattice ⇒ A lattice is said to be complemented if there exist unique complement of all element that belong to the lattice with these following conclusion.

$a, b \in L$

1) $a \wedge b = 0$

2) $a \vee b = 1$

if this will satisfy then we can say a and b are complement to each other.

Q.3. Let $G = \{1, -1, i, -i\}$, find order and subgroup of each elements.

Ans :- $G = \{1, -1, i, -i\}$

	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

$o(1) = 1 \quad (1^2 = 1)$

$o(-1) = 2 \quad (-1^2 = 1)$

$o(i) = 4 \quad (i^4 = 1)$

$o(-i) = 4 \quad ((-i)^4 = 1)$

Subgroup of $G(1) = \{1\}$

Subgroup of $G(-1) = \{-1, 1\}$

Subgroup of $G(i) = \{1, i, -i\}$

Subgroup of $G(-i) = \{1, i, -i\}$

Q.4. Let G be the set of all non-zero real numbers and let $a*b = ab/2$.
Show that $(G, *)$ be an abelian group.

Ans. R^+ is a set of non-zero real numbers

a) Closure property : let $a, b \in R^+$

$$a*b = \frac{ab}{2} \in R^+$$

So it satisfies closure property.

b) Associative law : let $a, b, c \in R^+$

$$a*(b*c) = a*\frac{bc}{2} = \frac{abc}{4}$$

$$(a*b)*c = \frac{ab}{2}*c = \frac{abc}{4}$$

So $a*(b*c) = (a*b)*c$

c) Existence of identity element

$$a*e = a$$

$$\Rightarrow \frac{ae}{2} = a$$

$$\Rightarrow e = 2 \in R^+$$

d) Existence of Inverse element

$$a*a^{-1} = e$$

$$\frac{aa^{-1}}{2} = e$$

$$\Rightarrow aa^{-1} = 4$$

$$a^{-1} = \frac{4}{a} \in R^+$$

e) Commutative law

$$a*b = b*a$$

$$\frac{ab}{2} = \frac{ba}{2} \Rightarrow \frac{ab}{2} = \frac{ab}{2}$$

(as multiplication of 2 real numbers is commutative)

Q.5. Define ring and give an example of a ring with zero-divisors.

Ans:- A ring $(R,+,\cdot)$ is a set R together with 2 binary operations + (addition) and $\cdot$ (multiplication) defined on R such that following axioms are satisfied :

(R1) $(a+b)+c = a+(b+c) \quad \forall\, a,b,c \in R$

(R2) $a+b = b+a \quad \forall\, a,b \in R$

(R3) There exist an element 0 in R such that
$$a+0 = a \quad \forall\, a \in R$$

(R4) For all $a \in R$, there exist an element $-a \in R$ such that $a+(-a)=0$

(R5) $(a\cdot b)\cdot c = a\cdot(b\cdot c) \quad \forall\, a,b,c \in R.$

(R6) $a\cdot(b+c) = (a\cdot b)+(a\cdot c) \quad \forall\, a,b,c \in R.$ (left distribution law)

(R7) $(b+c)\cdot a = (b\cdot a)+(c\cdot a) \quad \forall\, a,b,c \in R.$ (Right distribution law)

The algebraic system $(R,+,\cdot)$ is called a ring if

1. $(R,+)$ is an abelian group.
2. $(R,\cdot)$ is semigroup i.e $(a.b).c = a.(b.c) \;\forall\, a,b,c \in R.$
3. The operation $\cdot$ is distributive over the operation +.

Example of ring with zero divisors.

M is ring of all 2×2 matrices with their elements as integers, the addition & multiplication of matrices being the 2 ring composition. $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$ is zero element of this ring.

$$A\cdot B = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Section B

B. Attempt all the parts (5 × 5 = 25)

Q.6. Let G be a group and a, b be elements of G. Then show that:

(i) $(a^{-1})^{-1} = a$

Ans: let e be the identity element of G.

we have $a * a^{-1} = e$, where $a^{-1} \in G$

$(a^{-1})^{-1} * a^{-1} = e$.

$\therefore (a^{-1})^{-1} * a^{-1} = a * a^{-1}$

Thus, by right cancellation law, we have $(a^{-1})^{-1} = a$.

(ii) Let $a, b \in G$

$(ab)^{-1} = b^{-1}a^{-1}$

$a * b \in G$ (closure)

$\therefore (a*b)^{-1} * (a*b) = e$

let a^{-1} and b^{-1} be inverse of a and b respectively,

then $a^{-1}, b^{-1} \in G$

Therefore, $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$ (Associativity)

$= b^{-1} * e * b = b^{-1} * b = e$

From (1) & (2) we have $(a*b)^{-1} * (a*b) = (b^{-1} * a^{-1}) * (a*b)$

$(a*b)^{-1} = b^{-1} * a^{-1}$ by right cancellation law

6

Q.7. Consider the group $G = \{1,2,3,4,5,6\}$ under multiplication modulo 7

(i) Find the multiplication table of G

Ans.

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	5	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(ii) Find 2^{-1}, 3^{-1} and 6^{-1}.

Ans: identity element $e = 1$

$2^{-1} = 4$

$3^{-1} = 5$

$6^{-1} = 6$

(iii) $2^1 = 2$

$2^2 = 4$

$2^3 = 1$

so $O(2) = 3$

$gp(2) = \{1, 2, 4\}$

$3^1 = 3$ $\quad 3^5 = 5$

$3^2 = 2$ $\quad 3^6 = 1$

$3^3 = 6$ $\quad O(3) = 6$

$3^4 = 4$

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

(iv) Is G is cyclic?

Ans: 3 is the generator

G is cyclic since $G = gp(3)$.

Q.8. The order of each subgroup of a finite group is divisor of the order of the group.

Ans. Let H be any sub-group of order m of a finite group G of order n. We consider the left coset decomposition of G relatively to H.

& coset aH consists of m different elements

$$H = \{h_1, h_2, \ldots h_m\}$$

Then $ah_1, ah_2, \ldots ah_m$ are m members of aH, all distinct.

We have

$$ah_i = ah_j \Rightarrow h_i = h_j \text{, by Cancellation law in } G.$$

Since G is finite group, the number of distinct left cosets will also be finite, say K. Hence the total number of elements of all cosets is Km which is equal to the total number of elements of G.

Hence,
$$n = m.k$$

This shows that m, the order of H, is a divisor of n, the order of the Group G.

Q.10. Prove that the set $S = \{0,1,2,3\}$ forms a Ring under addition and multiplication modulo 4 but not a Field?

Ans: The composite table for the two operations is given by.

$+_4$	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	1

As we can see from the compositie table, the set S is a Ring since it is.

① Closure under addition:– for all $a, b \in S$, $a+b$ also $\in S$.

② Associative of addition :– $\forall a, b, c \in S$,
$$(a+b)+c = a+(b+c)$$

③ Existence of additive identity – There exists an element 0 in S, such that for all elements a in S, the equation $0+a = a+0 = a$ holds.
Here additive inverse is 0

④ Existence of additive inverse – $\forall$ each a in S, there exists an element b in S such that $a+b = b+a = 0$

⑤ Commutativity of addition – $\forall a, b$ in S, $a+b = b+a$

⑥ Closure under multiplication – $\forall a, b$ in S, $a \cdot b \in S$

⑦ Associativity of multiplication – $\forall a, b, c$ in S, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

⑧ Existence of multiplicative ~~inverse~~ identity – There exist an element

I in S, such that $\forall$ element a in S

$$I . a = a . I = a \text{ holds.}$$

Here the multiplicative identity is given by 1.

(9) Distributive laws $\rightarrow \forall$ a, b, c in S, $a.(b+c) = (a.b) + (a.c)$ holds.

$\forall$ a, b, c in S, the equation $(a+b).c = (a.c) + (b.c)$ holds.

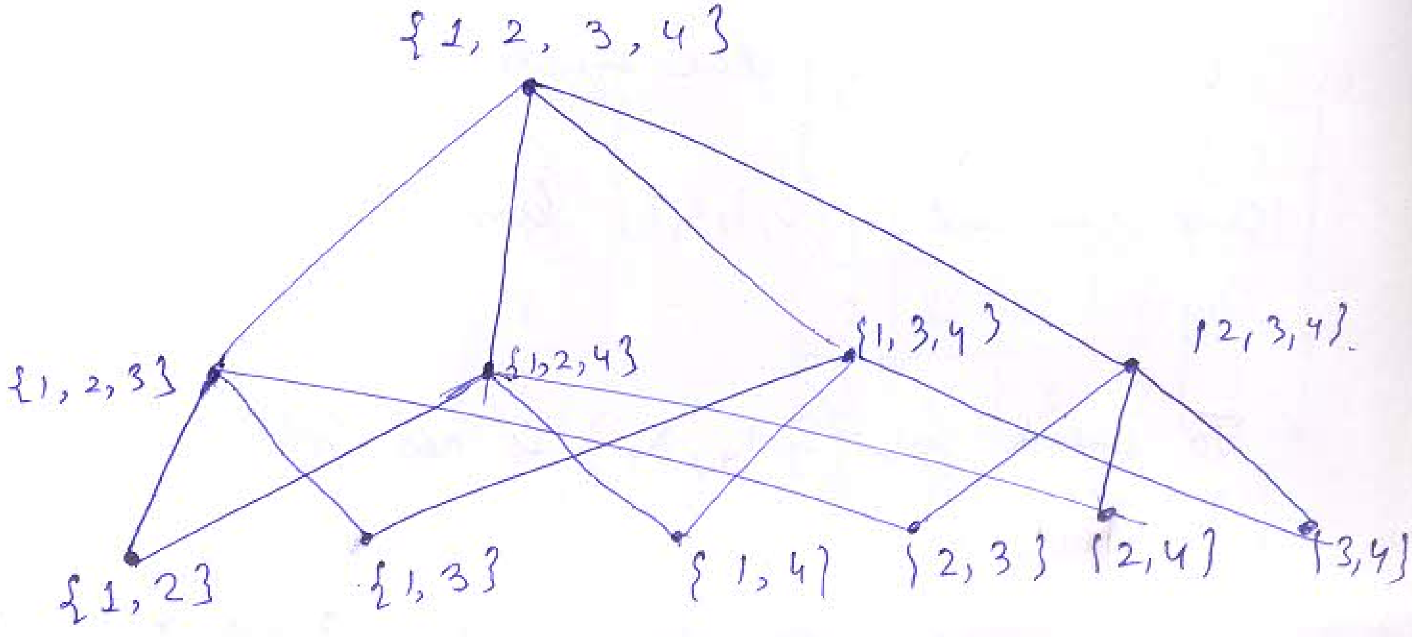
Hence the set $S = \{0, 1, 2, 3\}$ forms a ring under $+_4$ and X_4

To check for $(S, +_4, X_4)$ is not field :-

It is not a field because every element doesnot have multiplicative inverse.

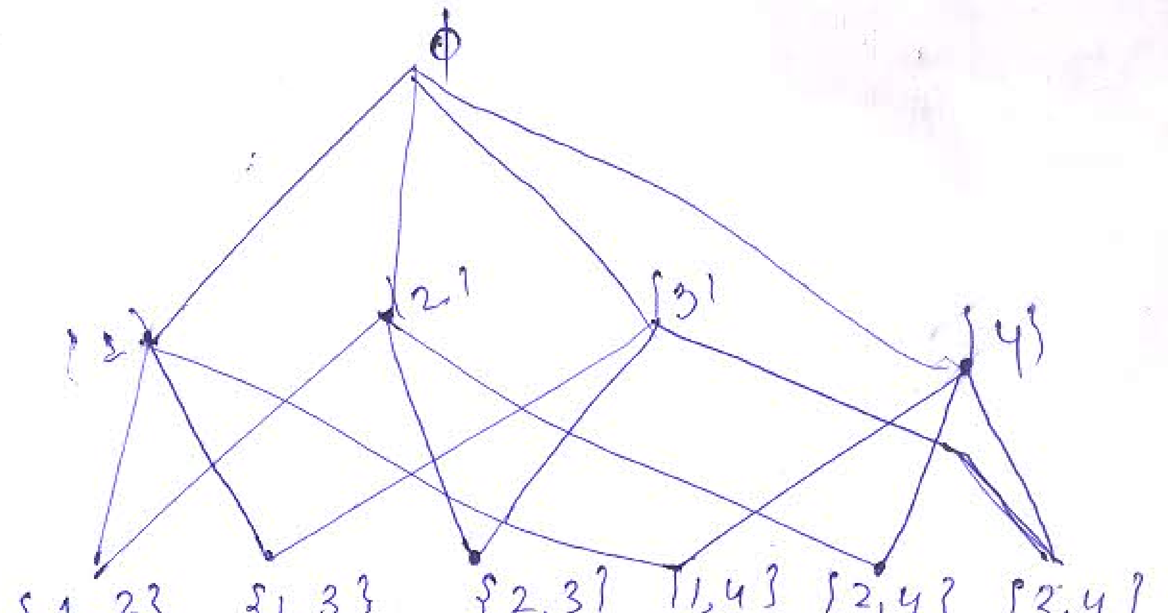
(10)
(9). Draw the Hasse-diagram to illustrate the following partial ordering.

(a). The set of all subset of {1, 2, 3, 4} having atleast two numbers partially ordered by ⊆



{1, 2, 3, 4} is maximal and greatest
All 2 element sets are minimal

b



ϕ is maximal and greatest
All 2 element sets are minimal.

Section = C

c. attempt all the parts.

(ii). Simplify the following Boolean expression using K-Map.

(i) $Y = ((AB)' + A' + AB)'$

$Y = \overline{\bar{A}\bar{B} + \bar{A} + AB}$

$Y = \overline{\bar{A}\bar{B}} \cdot \bar{\bar{A}} \cdot \overline{AB}$

$Y = AB \cdot A \cdot \overline{AB}$

$Y = A(B \cdot 1) \cdot \overline{AB}$

$Y = AB \cdot \overline{AB}$

$Y = 0$

$(\bar{A} + \bar{B} + \bar{A} + AB)'$

$= (\bar{A} + \bar{B} + AB)'$

	B'	B
$\bar{A}$	1	1
A	1	1

K-map for $(\bar{A} + \bar{B} + AB)$ $Y = 1$

$\therefore$ " " $(\bar{A} + \bar{B} + AB)'$ $Y = 0$.

(ii). $\bar{A}\bar{B}\bar{C}\bar{D} + \bar{A}\bar{B}\bar{C}D + \bar{A}\bar{B}CD + \bar{A}\bar{B}C\bar{D}$

AB \ CD	$\bar{C}\bar{D}$	$\bar{C}D$	CD	$C\bar{D}$
$\bar{A}\bar{B}$	1 0	1 1	1 3	1 2
$\bar{A}B$	4	5	7	6
AB	12	13	15	14
$A\bar{B}$	8	9	11	10

$Y = \bar{A}\bar{B}$

(12). Prove that every cyclic group is an abelian group.

sol :- Let G be a cyclic group and let a be a generator of a so that $G = \langle a \rangle = \{a^n : n \in Z\}$

If g_1 and g_2 are any two elements of G, there exist integers r and s such that $g_1 = a^r$ and $g_2 = a^s$

then $g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s . a^r = g_2 \cdot g_1$

So. G is abelian.

Hence Prove.

(1). obtain all distinct left cosets of $\{(0), (3)\}$ in the group $(Z_6, +_6)$ and find their union

$Z_6 = \{1, 2, 3, 6\}$

$0 +_6 1 = 1$ $\quad$ $3 +_6 1 = 4$

$0 +_6 2 = 2$ $\quad$ $3 +_6 2 = 5$

$0 +_6 3 = 3$ $\quad$ $3 +_6 3 = 0$

$0 +_6 6 = 0$ $\quad$ $3 +_6 6 = 3$

union = $\{0\ 1\ 2\ 3\ 4\ 5\}$

(ii).

(a). $a \vee b = b \wedge c$

L.H.S

$\because a \le b \le c$

$\therefore a \vee b = b.$

R.H.S $\quad b \wedge c = b.$

$\therefore$ L.H.S = R.H.S

(b). $(a \vee b) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = b$

L.H.S $\quad a \vee b = b.$

$b \wedge c = b.$

$(a \vee b) \vee (b \wedge c) = b.$

L.H.S = RHS

$a \vee b = b$

$a \vee c = c$

$(a \vee b) \wedge (a \vee c) = b \wedge c = b.$