ANNA UNIVERSITY OF TECHNOLOGY, COIMBATORE
B.E./B.TECH. DEGREE EXAMINATIONS: NOV/DEC 2006
FIFTH SEMESTER : CSE
DISCRETE MATHEMATICS

Part-A $(\mathbf{2 \times 10 = 20})$

1. If $\boldsymbol{P}, \boldsymbol{Q}$ and $\boldsymbol{R}$ are statement variables, prove that

$$\boldsymbol{P \wedge \big((\sim P \wedge Q) \vee (\sim P \wedge \sim Q)\big) \Rightarrow R}$$

Solution:

$$P \wedge \big((\sim P \wedge Q) \vee (\sim P \wedge \sim Q)\big) \Leftrightarrow P \vee \big(\sim P \wedge (Q \vee \sim Q)\big)$$
$$\Leftrightarrow P \wedge (\sim P \wedge T)$$
$$\Leftrightarrow P \wedge \sim P \Leftrightarrow F \Rightarrow R\ [\because\ F\ is\ any\ statement\ formula]$$

2. Prove that whenever $\boldsymbol{A \wedge B \Rightarrow C}$, we also have $\boldsymbol{A \Rightarrow (B \rightarrow C)}$ and vice versa.

Solution:

Assume that $A \wedge B \Rightarrow C$. To prove $A \Rightarrow (B \rightarrow C)$. Suppose that A is True and $B \rightarrow C$ is False. Hence B is True and C is False. $\therefore$ $A \wedge B$ is True but C is False, which is contradiction to our assumption.

Assume that $A \Rightarrow (B \rightarrow C)$. To prove $A \wedge B \Rightarrow C$. Suppose that $A \wedge B$ is True and C is False. Hence A and B are True. $\therefore$ A is True but $B \rightarrow C$ is False, which is contradiction to our assumption.

$\therefore$ Whenever $A \wedge B \Rightarrow C$, we also have $A \Rightarrow (B \rightarrow C)$ and vice versa.

3. Give an example to show that $(\exists \boldsymbol{x})\big(\boldsymbol{A(x) \wedge B(x)}\big)$ need not be a conclusion from $(\exists \boldsymbol{x})\big(\boldsymbol{A(x)}\big)$ and $(\exists \boldsymbol{x})\big(\boldsymbol{B(x)}\big)$

Solution:

Let $A = \{1\}$ and $B = \{2\}$

Let $A(x) = x \in A$ and $B(x) = x \in B$

Since A and B are non empty, $(\exists x)A(x)$ and $(\exists x)B(x)$ are both true. Since $A \cap B = \emptyset$

$(\exists x)\big(A(x) \wedge B(x)\big)$ is false.

$(\exists x)\big(A(x) \wedge B(x)\big)$ need not be a conclusion from $(\exists x)\big(A(x)\big)$ and $(\exists x)\big(B(x)\big)$.

4. Find the truth value of $(\boldsymbol{x})\big(\boldsymbol{P \rightarrow Q(x)}\big) \vee (\exists \boldsymbol{x})\boldsymbol{R(x)}$ where $\boldsymbol{P}: \mathbf{2} > 1, Q(\boldsymbol{x}): \boldsymbol{x} > 3, R(\boldsymbol{x}): \boldsymbol{x} > 4$ with the universe of discourse being $\boldsymbol{E} = \{\mathbf{2}, \mathbf{3}, \mathbf{4}\}$.

Solution:

P is True and $Q(4)$ is false $P \rightarrow Q(4)$ is false.

$(x)\big(P \rightarrow Q(x)\big)$ is false

Since $R(2), R(3), R(4)$ are all false. $(\exists x)R(x)$ is false. Hence $(x)\big(P \rightarrow Q(x)\big) \vee (\exists x)R(x)$ is false.

5. For any sets $\boldsymbol{A}, \boldsymbol{B}$ and $\boldsymbol{C}$, prove that $\boldsymbol{A \times (B \cap C) = (A \times B) \cap (A \times B)}$.

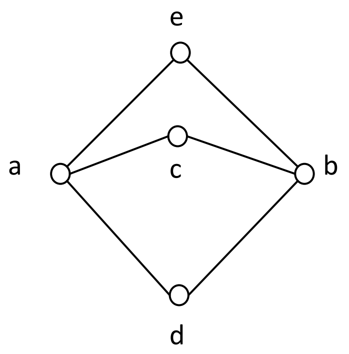
Solution:

Let $(x, y) \in A \times\ (B \cap C)$

$$\Leftrightarrow\ x \in\ A\ and\ y \in\ (B \cap C)$$
$$\Leftrightarrow (\ x \in\ A\ and\ y \in\ B)\ and\ (\ x \in\ A\ and\ y \in C)$$
$$\Leftrightarrow (x, y) \in A \times B\ and\ (x, y) \in A \times C$$
$$\Leftrightarrow (x, y) \in (A \times B) \cap (A \times C)$$

$$A \times (B \cap C) = (A \times B) \cap (A \times B)$$

6. The following is the Hasse diagram of a partially ordered set. Verify whether it is a Lattice.



Solution:

c and e are upper bounds of a and b. As c and e cannot be compared, the LUB of a, b does not exist. Therefore the Hasse diagram is not a Lattice.

7. If $\boldsymbol{f: A \to B}$ and $\boldsymbol{g: B \to C}$ are mappings and $\boldsymbol{g \circ f: A \to C}$ one-to-one, prove that $\boldsymbol{f}$ is one-to-one.

Solution:

Let us assume that $f(x) = f(y) \Rightarrow g\big(f(x)\big) = g\big(f(y)\big)$

$$\Rightarrow g \circ f(x) = g \circ f(y)$$
$$\Rightarrow x = y \; (\because \; g \circ f \; is \; one-to-one)$$
$$\therefore f(x) = f(y) \Rightarrow x = y$$

$\therefore f$ is one-to-one.

8. If $\boldsymbol{\chi_A(x)}$ denotes the characteristic function of the set $\boldsymbol{A}$, prove that

$$\boldsymbol{\chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_{A \cap B}(x)}$$

Solution:

$$\chi_{A \cup B}(x) = 1 \ldots (1)$$
$$\Rightarrow x \in A \cup B$$
$$\Rightarrow x \in A \; or \; x \in B$$
$$\Rightarrow \chi_A(x) = 1 \; or \; \chi_B(x) = 1$$
$$\Rightarrow \chi_A(x) + \chi_B(x) - \chi_A(x).\chi_B(x) = 1$$
$$\Rightarrow \chi_A(x) + \chi_B(x) - \chi_{A \cap B}(x) = 1 \ldots (2)$$
$$\chi_{A \cup B}(x) = 1 \ldots (3)$$
$$\Rightarrow x \notin A \cup B$$
$$\Rightarrow x \notin A \; and \; x \notin B$$
$$\Rightarrow \chi_A(x) = 1 \; and \; \chi_B(x) = 1$$
$$\Rightarrow \chi_A(x) + \chi_B(x) - \chi_A(x).\chi_B(x) = 0$$
$$\Rightarrow \chi_A(x) + \chi_B(x) - \chi_{A \cap B}(x) = 0 \ldots (4)$$

From (1), (2), (3) and (4), we get

$$\chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_{A \cap B}(x)$$

9. If $\boldsymbol{S}$ denotes the set of positive integers $\boldsymbol{\leq 100}$, for $\boldsymbol{x, y \in S}$, define $\boldsymbol{x * y = \min\{x, y\}}$. Verify whether $\boldsymbol{(S, *)}$ is a Monoid assuming that $\boldsymbol{*}$ is associative.

Solution:

The identity element is $e = 100$ exists. Since for $x \in S, \min(x, 100) = x \Rightarrow x * 100 = x, \forall\, x \in S$

$\therefore$ $(S,*)$ is a Monoid.

10. If H is a subgroup of the group G, among the right cosets of H in G, prove that there is only one subgroup H.

Solution:

Let Ha be a right coset of H in G where $a \in G$. If Ha is a subgroup of G,

Then $e \in Ha$, where e is the identity element in G. Ha is an equivalence class containing a with respect to an equivalence relation.

$\therefore$ $e \in H \Rightarrow\ He = Ha$. But $He = H$

$\therefore$ $Ha = H$. This shows H is only subgroup.

Part-B $(\mathbf{5 \times 16 = 80})$

11. (a)(i) Prove that $(P \to Q) \wedge (Q \to R) \Rightarrow (P \to R)$

Solution:

To prove S: $\big((P \to Q) \wedge (Q \to R)\big) \to (P \to R)$ is a Tautology.

P	Q	R	$P \to Q$	$Q \to R$	$P \to R$	$(P \to Q) \wedge (Q \to R)$	S
F	F	F	T	T	T	T	T
F	T	F	T	F	T	F	T
T	F	F	F	T	F	F	T
T	T	F	T	F	F	F	T
F	F	T	T	T	T	T	T
F	T	T	T	T	T	T	T
T	F	T	F	T	T	F	T
T	T	T	T	T	T	T	T

$\therefore$ $\big((P \to Q) \wedge (Q \to R)\big) \to (P \to R)$ is a Tautology

$\therefore (P \to Q) \wedge (Q \to R) \Rightarrow (P \to R)$

(ii) Find the principal conjunctive and principal disjunctive normal forms of the formula

$$S \Leftrightarrow \big(P \to (Q \wedge R)\big) \wedge \big(\sim P \to (\sim Q \wedge \sim R)\big)$$

Solution:

$S \Leftrightarrow \big(P \to (Q \wedge R)\big) \wedge \big(\sim P \to (\sim Q \wedge \sim R)\big)$

$\Leftrightarrow \big(\sim P \vee (Q \wedge R)\big) \wedge \big(P \vee (\sim Q \wedge \sim R)\big)$

$\Leftrightarrow (\sim P \vee Q) \wedge (\sim P \vee R) \wedge (P \vee \sim Q) \wedge (P \vee \sim R) \quad \textit{which is CNF}$

$\Leftrightarrow (\sim P \vee Q \vee F) \wedge (\sim P \vee F \vee R) \wedge (P \vee \sim Q \vee F) \wedge (P \vee F \vee \sim R)$

$\Leftrightarrow \big(\sim P \vee Q \vee (R \wedge \sim R)\big) \wedge (\sim P \vee (Q \wedge \sim Q) \vee R) \wedge \big(P \vee \sim Q \vee (R \wedge \sim R)\big)$
$\quad \wedge (P \vee (Q \wedge \sim Q) \vee \sim R)$

$\Leftrightarrow (\sim P \vee Q \vee R) \wedge (\sim P \vee Q \vee \sim R) \wedge (\sim P \vee Q \vee R) \wedge (\sim P \vee \sim Q \vee R) \wedge (P \vee \sim Q \vee R)$
$\quad \wedge (P \vee \sim Q \vee \sim R) \wedge (P \vee Q \vee \sim R) \wedge (P \vee \sim Q \vee \sim R)$

$\Leftrightarrow (\sim P \vee Q \vee R) \wedge (\sim P \vee Q \vee \sim R) \wedge (\sim P \vee \sim Q \vee R) \wedge (P \vee \sim Q \vee R)$
$\quad \wedge (P \vee \sim Q \vee \sim R) \wedge (P \vee Q \vee \sim R) \quad \textit{which is PCNF.}$

$\sim S \equiv \textit{Remaining max terms}$

$\sim S \equiv (P \vee Q \vee R) \wedge (\sim P \vee\sim Q \vee\sim R)$
$\sim\sim S \equiv\sim \big((P \vee Q \vee R) \wedge (\sim P \vee\sim Q \vee\sim R)\big)$
$S \equiv (P \wedge Q \wedge R) \vee (\sim P \wedge\sim Q \wedge\sim R)$ *which is PDNF*.

(b) (i) Using conditional proof, prove that

$$\sim \boldsymbol{P} \vee \boldsymbol{Q}, \sim \boldsymbol{Q} \vee \boldsymbol{R}, \boldsymbol{R} \to \boldsymbol{S} \Rightarrow \boldsymbol{P} \to \boldsymbol{S}$$

Solution:

i) $\sim P \vee Q$ *Rule P*
ii) $\sim Q \vee R$ *Rule P*
iii) $R \to S$ *Rule P*
iv) P *Rule Additional premises*
v) Q *Rule T, i, iv and Disjunctive Syllogism*
vi) R *Rule T, ii, v and Disjunctive Syllogism*
vii) S *Rule T, iii, vi and Modus phones*
viii) $P \to S$ *Rule CP*

(ii) By using truth tables, verify whether the following specifications are consistent; "Whenever the system software is being upgraded users cannot access the file system. If users can access the file system, then they can save new files. If users cannot save new files then the system software is not being upgraded.

Solution:

Let P represents the system software is being upgraded.
Let Q represents users can access the file system.
Let R represents users can save the file.

$$P \to\sim Q, Q \to R, \sim R \to\sim P$$

Let $S = (P \to\sim Q) \wedge (Q \to R) \wedge (\sim R \to\sim P)$

$\boldsymbol{P}$	$\boldsymbol{Q}$	$\boldsymbol{R}$	$\sim \boldsymbol{P}$	$\sim \boldsymbol{Q}$	$\sim \boldsymbol{R}$	$\boldsymbol{P} \to\sim \boldsymbol{Q}$	$\boldsymbol{Q} \to \boldsymbol{R}$	$\sim \boldsymbol{R} \to\sim \boldsymbol{P}$	$\boldsymbol{S}$
F	F	F	T	T	T	T	T	T	T
F	T	F	T	F	T	T	F	T	F
T	F	F	F	T	T	T	T	F	F
T	T	F	F	F	T	F	F	F	F
F	F	T	T	T	F	T	T	T	T
F	T	T	T	F	F	T	T	T	T
T	F	T	F	T	F	T	T	T	T
T	T	T	F	F	F	F	T	T	F

From the truth table, S has the truth value T whenever all premises are assigned the truth value T.
∴ The premises are consistent.

12.(a)(i) Use indirect method of proof to show that

$$(\boldsymbol{x})\big(\boldsymbol{P}(\boldsymbol{x}) \vee \boldsymbol{Q}(\boldsymbol{x})\big) \Rightarrow (\boldsymbol{x})\big(\boldsymbol{P}(\boldsymbol{x})\big) \vee (\exists \boldsymbol{x})\big(\boldsymbol{Q}(\boldsymbol{x})\big)$$

Solution:

Let us assume that $\neg\big((x)P(x) \vee\ (\exists x)Q(x)\big)$ as additional premise
$1. \neg\big((x)P(x) \vee\ (\exists x)Q(x)\big)$ *Additional premise*

2. $\neg(x)\ P(x) \wedge \neg\ (\exists x)Q(x)$	$1, De\ Morgan's\ law$
3. $\neg(x)\ P(x)$	$Rule\ T, 2$
4. $(\exists x)\neg\ P(x)$	$3, De\ Morgan's\ law$
5. $\neg\ P(a)$	$Rule\ ES, 4$
6. $\neg\ (\exists x)Q(x)$	$Rule\ T, 2$
7. $(x)\neg\ Q(x)$	$6, De\ Morgan's\ law$
8. $\neg Q(a)$	$Rule\ US, 7$
9. $\neg\ P(a) \wedge \neg Q(a)$	$5,8, conjunction$
10. $\neg\ \big(P(a) \vee Q(a)\big)$	$9, De\ Morgan's\ law$
11. $(x)\ (P(x) \vee (Q(x))$	$Rule\ P$
12. $P(a) \vee Q(a)$	$Rule\ US, 11$
13. $\neg\ \big(\ P(a) \vee Q(a)\big) \wedge \big(\ P(a) \vee Q(a)\big)$	$11,12, conjunction$
14. F	$Rule\ T, 13$

∴ By the method of contradiction

$$(x)\big(P(x) \vee Q(x)\big) \Rightarrow (x)\big(P(x)\big) \vee (\exists x)\big(Q(x)\big)$$

(ii) Prove that $(\exists \boldsymbol{x})\boldsymbol{P}(\boldsymbol{x}) \to (\boldsymbol{x})\boldsymbol{Q}(\boldsymbol{x}) \Rightarrow (\boldsymbol{x})(\boldsymbol{P}(\boldsymbol{x}) \to \boldsymbol{Q}(\boldsymbol{x}))$

Solution:

1. $(\exists x)P(x) \to (x)Q(x)$	$Rule\ P$
2. $\neg(\exists x)P(x) \vee (x)Q(x)$	$Rule\ T, conjuction\ as\ disjunction$
3. $(x)\neg P(x) \vee (x)Q(x)$	$Rule\ T, 2$
4. $(\neg P(a) \vee Q(a))$	$Rule\ US$
5. $(P(a) \to Q(a))$	$Rule\ T, 2, conjuction\ as\ disjunction$
6. $(x)(P(x) \to Q(x))$	$Rule\ UG$

(b) (i) Use conditional proof to prove that

$$(\boldsymbol{x})(\boldsymbol{P}(\boldsymbol{x}) \to \boldsymbol{Q}(\boldsymbol{x})) \Rightarrow\ (\boldsymbol{x})\boldsymbol{P}(\boldsymbol{x}) \to (\boldsymbol{x})\boldsymbol{Q}(\boldsymbol{x})$$

Solution:

1. $(x)P(x)$	$Additional\ Premise$
2. $(x)(P(x) \to Q(x))$	$Rule\ P$
3. $P(a) \to Q(a)$	$Rule\ US, 2$
4. $P(a)$	$Rule\ US, 1$
5. $Q(a)$	$Rule\ T, 3,4, Modus\ phones$
6. $(x)Q(x)$	$Rule\ UG\ ,5$
7. $(x)P(x) \to (x)Q(x)$	$Rule\ CP$

(ii) Prove that $(\exists x)(\boldsymbol{A}(\boldsymbol{x}) \vee \boldsymbol{B}(\boldsymbol{x})) \Leftrightarrow (\exists \boldsymbol{x})\boldsymbol{A}(\boldsymbol{x}) \vee (\exists \boldsymbol{x})\boldsymbol{B}(\boldsymbol{x})$

Solution:

Let us assume that $\neg\big((\exists x)A(x) \vee (\exists x)B(x)\big)$ as additional premise

1. $\neg\big((\exists x)A(x) \vee (\exists x)B(x)\big)$	$Additional\ premise$
2. $\neg(\exists x)A(x) \wedge \neg(\exists x)B(x)$	$1, De\ Morgan's\ law$
3. $(x)\neg A(x) \wedge (x)\neg B(x)$	$2, De\ Morgan's\ law$
4. $\neg A(a) \wedge \neg B(a)$	$Rule\ US, 3$
5. $\neg(A(a) \vee B(a))$	$4, De\ Morgan's\ law$
6. $(\exists x)(A(x) \vee B(x))$	$Rule\ P$
7. $A(a) \vee\ B(a)$	$Rule\ ES, 6$

8. $\neg\,(A(a) \vee\ B(a)) \wedge\ (A(a) \vee\ B(a))$ $\quad$ $5,7, conjunction$

9. F $\quad$ $Rule\ T, 8\ and\ negation\ law$

∴ By the method of contradiction

$$(\exists x)(A(x) \vee B(x)) \Leftrightarrow (\exists x)A(x) \vee (\exists x)B(x)$$

13.(a)(i) Prove that distinct equivalence classes are disjoint.

Solution:

Let R be an equivalence relation defined on set X.

Let $[x]_R, [y]_R$ are two distinct equivalence classes on X

i.e., xRy $\quad$ /

Let us assume that there is at least one element $z \in [x]_R\ and\ also\ z \in [y]_R$

i.e., $xRz\ and\ yRz \Rightarrow zRy(By\ symmetric)$

$$\therefore\ xRz\ and\ zRy \Rightarrow xRy(By\ transitivity)$$

Which is a contradiction.

$$[x]_R \cap [y]_R = \emptyset$$

∴Distinct equivalence classes are disjoint.

(ii) In a Lattice show that $a \leq b$ and $c \leq d$ implies $a * c \leq b * d$.

Solution:

For any $a, b, c \in L$

If $a \leq\ b \Rightarrow c * a \leq c * b$

$$\Rightarrow a * c \leq b * c \ldots (1)(By\ Commutative\ law)$$

For any $\ b, c, d \in L$

If $c \leq\ d \Rightarrow b * c \leq b * d \ldots (2)$

From (1) and (2) we get

$$a * c \leq\ b * d$$

(iii) In a distributive Lattice prove that $a * b = a * c$ and $a \oplus b = a \oplus c$ implies that $b = c$.

Solution:

$$(a * b) \oplus c = (a * c) \oplus c = c \ldots (1)\ [a * b = a * c\quad and\ absorbtion\ law]$$

$$(a * b) \oplus c = (a \oplus c) * (b \oplus c)\ [Distributive\ law]$$

$= (a \oplus b) * (b \oplus c) = (a \oplus b) * (c \oplus b)\ [a \oplus b = \ a \oplus c\ and\ commutative\ law]$

$$= (a * c) \oplus b = (a * b) \oplus b = b \ldots (2)[Distributive\ and\ absorbtion\ law]$$

From (1) and (2) we get,

$$b = c$$

(b) (i) Let $P = \{\{1, 2\}, \{3, 4\}, \{5\}\}$ be a partition of the set $S = \{1, 2, 3, 4, 5\}$. Construct an equivalence classes with respect to R are precisely the members of P.

Solution:

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

Since $(1, 1), (2, 2), (3, 3), (4, 4), (5, 5) \in R$

$$\therefore R\ is\ reflexive$$

$$For\ (1, 2), (3,4) \in R\ there\ is\ (2, 1), (4, 3) \in R$$

$$\therefore R\ is\ Symmetric$$

$$For\ (1,2)\ and\ (2,1) \in R\ there\ is\ (1,1) \in R$$
$$For\ (2,1)\ and\ (1,2) \in R\ there\ is\ (2,2) \in R$$
$$For\ (3,4)\ and\ (4,3) \in R\ there\ is\ (3,3) \in R$$
$$For\ (4,3)\ and\ (3,4) \in R\ there\ is\ (4,4) \in R$$
$$\therefore R\ is\ transitive$$
$$\therefore R\ is\ an\ equivalence\ relation$$
$$[1]_R = \{1,2\}, [3]_R = \{3,4\}, [5]_R = \{5\}$$

Equivalence classes with respect to $R = \{[1]_R, [3]_R, [5]_R\}$

The equivalence classes with respect to R are precisely the members of P

(ii) Show that a chain with three of more elements is not complemented.

Solution:

Let L be a chain with 0 and 1. Let $o < a < 1$.

We show that $'a'$ has no element in L.

Let $b \in L$ and b be a complement to a.

$\therefore\ a * b = 0$ and $a \oplus b = 1$

Since L is a chain, either $a \leq b$ or $b \leq a$

If $a \leq b$, then $0 = a * b = a$. But $a > 0$

Also if $b \leq a$, then $1 = a \oplus b = a$. But $a < 1$

$\therefore\ a$ has no complement.

(iii) Establish DeMorgan's laws in a Boolean Algebra.

Solution:

$$(a * b)' = a' \oplus b', \forall a, b \in L$$
$$(a * b) \oplus (a' \oplus b') = \left(a \oplus (a' \oplus b')\right) * \left(b \oplus (a' \oplus b')\right)$$
$$= \left(a \oplus (a' \oplus b')\right) * \left((a' \oplus b') \oplus b\right)$$
$$= \left((a \oplus a') \oplus b'\right) * \left(a' \oplus (b' \oplus b)\right)$$
$$= (1 \oplus b') * (a' \oplus 1) = 1 * 1$$
$$(a * b) \oplus (a' \oplus b') = 1 \dots (1)$$
$$(a * b) * (a' \oplus b') = \left((a * b) * a'\right) \oplus \left((a * b) * b'\right)$$
$$= \left((b * a) * a'\right) \oplus \left((a * b) * b'\right)$$
$$= \left(b * (a * a')\right) \oplus \left(a * (b * b')\right)$$
$$= (b * 0) \oplus (a * 0) = 0 \oplus 0$$
$$(a * b) * (a' \oplus b') = 0 \dots (2)$$

$From\ (1)\ and\ (2)\ we\ get,$

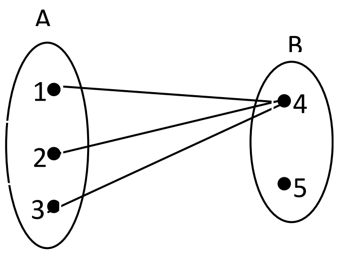
$$(a * b)' = a' \oplus b'$$

By duality, $(a \oplus b)' = a' * b'$

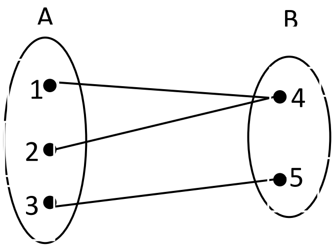
14.(a)(i) Find all mappings from $A = \{1, 2, 3\}$ to $B = \{4, 5\}$. Find which of them are one-to-one and which are onto.

Solution:

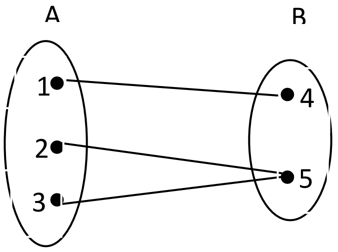
i)



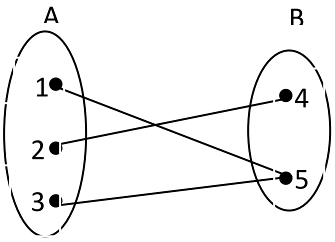
ii)



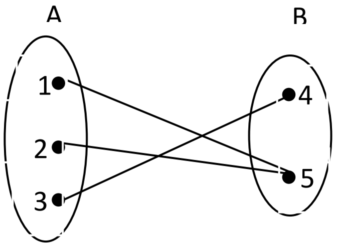
iii)



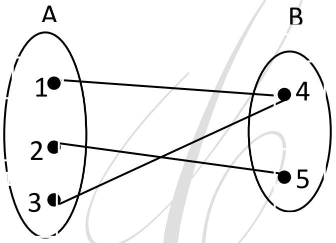
iv)



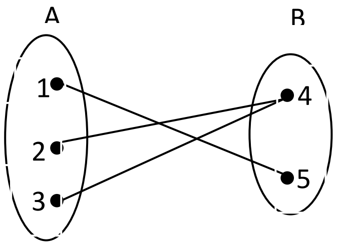
v)



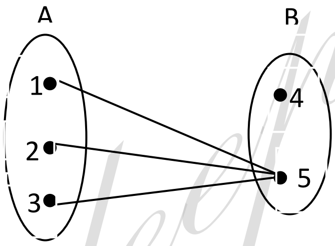
vi)



vii)



viii)



None of the above mappings are one-to-one. (i) and (viii) are not onto mapping but the remaining mappings are onto.

(ii) If $\boldsymbol{f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}}$ and $\boldsymbol{g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}}$, are permutations, prove that

$$\boldsymbol{(g \circ f)^{-1} = f^{-1} \circ g^{-1}}$$

Solution:

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \ldots (1)$$

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$f^{-1} \circ g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \ldots (2)$$

From (1) and (2), we get

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

(iii) If R denotes the set of real numbers and $\boldsymbol{f: R \to R}$ is given by $\boldsymbol{f(x) = x^3 - 2}$, find $\boldsymbol{f^{-1}}$.

Solution:

$$f(x) = f(y) \Rightarrow x^3 - 2 = y^3 - 2 \Rightarrow x^3 = y^3 \Rightarrow x = y$$

$\therefore f$ is one to one.

Let $y \in R$.

$$f(x) = y \Rightarrow x^3 - 2 = y \Rightarrow x^3 = y + 2 \Rightarrow x = (y+2)^{\frac{1}{3}}$$

Therefore for every image in R there is a pre-image in R.

$\therefore f$ is onto.

$\therefore f^{-1}$ exists.

$$f^{-1}(y) = (y+2)^{\frac{1}{3}}$$

14.(b) (i) If Z^+ denote the set of positive integers and Z denote the set of integers. Let f: $Z^+ \rightarrow Z$ be defined by

$f(n) = \begin{cases} \frac{n}{2}, if\ n\ is\ even \\ \frac{1-n}{2}, if\ n\ is\ odd \end{cases}$. Prove that f is a bijection and find f^{-1}.

Solution:

To prove f is one to one:

$$\forall x, y \in Z^+$$

Case: 1 when $x\ and\ y\ are\ even$

$$f(x) = f(y) \Rightarrow \frac{x}{2} = \frac{y}{2} \Rightarrow x = y$$

Case: 2 when $x\ and\ y\ are\ odd$

$$f(x) = f(y) \Rightarrow \frac{1-x}{2} = \frac{1-y}{2} \Rightarrow 1 - x = 1 - y \Rightarrow x = y$$

$\therefore$ From case: 1 and case: 2, f is one to one.

To prove f is onto:

$When\ x\ is\ even$

Let $y = \frac{x}{2} \Rightarrow x = 2y$

$$\forall x \in Z, x = f(2x)$$

$$\therefore\ \forall x \in Z, there\ is\ a\ pre\ image\ 2x \in Z^+$$

$When\ x\ is\ odd$

Let $y = \frac{1-x}{2} \Rightarrow 1 - x = 2y \Rightarrow x = 1 - 2y$

$$\forall x \in Z, x = f(1-2x)$$

$$\therefore\ \forall x \in Z, there\ is\ a\ pre\ image\ 1 - 2x \in Z^+$$

Every element has unique pre-image

$\therefore\ f$ is onto

$\therefore\ f$ is bijection $\Rightarrow\ f^{-1}$ exists.

$When\ x\ is\ even$

Let $y = \frac{x}{2} \Rightarrow x = f^{-1}(y) = 2y$

$When\ x\ is\ odd$

Let $y = \frac{1-x}{2} \Rightarrow 1 - x = 2y \Rightarrow x = f^{-1}(y) = 1 - 2y$

$$f^{-1}(n) = \begin{cases} 2n, if\ n\ is\ even \\ 1 - 2n, if\ n\ is\ odd \end{cases}$$

(ii) Let A, B and C be any three non empty sets. Let $f: A \to B$ and $g: B \to C$ be mappings. If f and g are onto, prove that $g \circ f: A \to C$ is onto. Also give an example to show that $g \circ f$ may be onto but both f and g need not be onto.

Solution:

Since $f: A \to B$ is onto

$f(x) = y, \forall x \in A \, and \, y \in B \dots (1)$

Since $g: B \to C$ is onto

$g(y) = z, \forall z \in C \, and \, y \in B \dots (2)$

$\forall x \in A, gof(x) = g(f(x)) = g(y) = z \, [from \, (1) \, and \, (2)]$

$\therefore \forall z \in C \, there \, exists \, a \, preimage \, x \in A \, such \, that \, gof(x) = z$

$\therefore gof: A \to C$ is onto

For example

Let $A = \{1, 2\}, B = \{a, b, c\} and \, C = \{d, e\}$

$$f = \{(1, a), (2, b)\}, g = \{(a, d), (b, e), (c, e)\}$$

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

$$gof(2) = g(f(2)) = g(b) = e$$

$$gof = \{(1, d), (2, e)\}$$

The function f is not onto because $c \in B$ does not have pre image.

The function g is not onto because every element of C have pre image but it is not unique. $e \in C \, have \, two \, pre \, images \, b, c \in B$

The function gof is onto because every element of C have pre image and it is unique.

$\therefore g \circ f$ may be onto but both f and g need not be onto.

15.(a)(i) State and prove Lagrange's theorem for finite groups.

Statement:

The order of a subgroup of a finite group is a divisor of the order of the group.

Proof:

Let aH and bH be two left cosets of the subgroup $\{H,*\}$ in the group $\{G,*\}$.

Let the two cosets aH and bH be not disjoint.

Then let c be an element common to aH and bH i.e., $c \in aH \cap bH$

$$\because c \in aH, c = a * h_1, for \, some \, h_1 \in H \dots (1)$$

$$\because c \in bH, c = b * h_2, for \, some \, h_2 \in H \dots (2)$$

From (1) and (2), we have

$$a * h_1 = b * h_2$$

$$a = b * h_2 * h_1^{-1} \dots (3)$$

Let x be an element in aH

$x = a * h_3, for \, some \, h_3 \in H$

$$= b * h_2 * h_1^{-1} * h_3, using \, (3)$$

Since H is a subgroup, $h_2 * h_1^{-1} * h_3 \in H$

Hence, (3) means $x \in bH$

Thus, any element in aH is also an element in bH. $\therefore aH \subseteq bH$

Similarly, we can prove that $bH \subseteq aH$

Hence $aH = bH$

Thus, if aH and bH are disjoint, they are identical.

The two cosets aH and bH are disjoint or identical. …(4)

Now every element $a \in G$ belongs to one and only one left coset of H in G,
For,
$a = ae \in aH, since\ e \in H \Rightarrow a \in aH$

$a \notin bH$, since aH and bH are disjoint i.e., a belongs to one and only left coset of H in G i.e., aH … (5)

From (4) and (5), we see that the set of left cosets of H in G form the partition of G. Now let the order of H be m.

Let $H = \{h_1, h_2, \dots, h_m\}, where\ h_i's$ are distinct

Then $aH = \{ah_1, ah_2, \dots, ah_m\}$

The elements of aH are also distinct, for, $ah_i = ah_j \Rightarrow h_i = h_j$, which is not true.

Thus H and aH have the same number of elements, namely m.

In fact every coset of H in G has exactly m elements.

Now let the order of the group $\{G,*\}$ be n, i.e., there are n elements in G

Let the number of distinct left cosets of H in G be p.

$\therefore$ The total number of elements of all the left cosets $= pm$ $=$ the total number of elements of G. i.e., $n = pm$

i.e., m, the order of H is adivisor of n, the order of G.

(ii) Find all the non-trivial subgroups of $(Z_6, +_6)$.

Solution: $(Z_6\ , +_6), S = \{[0]\}\ under\ binary\ operation +_6$ are trivial subgroups

$+_6$	**[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]

$S_1 = \{[0], [2], [4]\}$

$+_6$	**[0]**	**[2]**	**[4]**
[0]	[0]	[2]	[4]
[2]	[2]	[4]	[0]
[4]	[4]	[0]	[2]

From the above cayley's table,

All the elements are closed under the binary operation $+_6$

Associativity is also true under the binary operation $+_6$

[0] is the identity element.

Inverse element of [2] is [4] and vise versa

Hence $S_1 = \{[0], [2], [4]\}$ is a subgroup of $(Z_6\ , +_6)$

$S_2 = \{[0], [3]\}$

$+_6$	**[0]**	**[3]**
[0]	[0]	[3]
[3]	[3]	[0]

From the above cayley's table,

All the elements are closed under the binary operation $+_6$

Associativity is also true under the binary operation $+_6$

[0] is the identity element.

Inverse element of [3] is itself.

Hence $S_2 = \{[0], [3]\}$ is a subgroup of $(Z_6 \,, +_6)$

Therefore $S_1 = \{[0], [2], [4]\}$ and $S_2 = \{[0], [3]\}$ are non trivial subgroups of $(Z_6 \,, +_6)$

(b) If $H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$ is the parity check matrix, find the Hamming code generated by H (in which the first three bits represent information portion and the next four bits are parity check bits). If $y = (0, 1, 1, 1, 1, 1, 0)$ is the received word find the corresponding transmitted code word.

Solution:

Here $e: B^3 \to B^7$

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = [A^T | I_{n-m}] = [A^T | I_4]$$

The generator function is given by

$$G = [I_m | A] = [I_3 | A] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$B^3 \equiv \{000, 001, 010, 100, 011, 101, 110, 111\}$$

$$e(w) = w.G$$

$$e(000) = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$e(001) = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$e(010) = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$e(100) = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$e(011) = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$e(101) = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$e(110) = [1 \quad 1 \quad 0]\begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 1\\ 0 & 1 & 0 & 1 & 0 & 0 & 1\\ 0 & 0 & 1 & 1 & 1 & 1 & 0\end{bmatrix} = [1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0]$$

$$e(111) = [1 \quad 1 \quad 1]\begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 1\\ 0 & 1 & 0 & 1 & 0 & 0 & 1\\ 0 & 0 & 1 & 1 & 1 & 1 & 0\end{bmatrix} = [1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0]$$

$$H.[y]^T = \begin{bmatrix}0 & 1 & 1 & 1 & 0 & 0 & 0\\ 1 & 0 & 1 & 0 & 1 & 0 & 0\\ 1 & 0 & 1 & 0 & 0 & 1 & 0\\ 1 & 1 & 0 & 0 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix}0\\1\\1\\1\\1\\1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\1\end{bmatrix}$$

$Since, the\ syndrome \begin{bmatrix}1\\0\\0\\1\end{bmatrix}$ *is same as the second column of* H, *the element in the second position of* y *is changed.*

$\therefore$ *The decoded word is* 0011110 *and the original message is* 001.