DISCRETE MATHEMATICS

ANNA UNIVERSITY

SOLVED QUESTION PAPERS

B.E. B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2006.

Answer ALL questions

PART - A - (10 x 2 = 20 marks)

1. ***If* P, Q *and* R *are statement variables, prove that***

$$P \wedge ((7P \wedge Q) \vee (7P \wedge 7Q)) \Rightarrow R$$

Solution

$P \wedge (7P \wedge (Q \vee 7Q)) \Leftrightarrow P \wedge (7P \wedge T)$ where T is a Tautology

$\Leftrightarrow (P \wedge 7P) \wedge T$

$\Leftrightarrow F \wedge T$ where F is a contradication

$\Leftrightarrow$ F

$\Rightarrow$ R since F $\Rightarrow$ any statement formula.

2. ***Prove that whenever $A \wedge B \Rightarrow C$, we also have $A \Rightarrow (B \to C)$ and vice versa.***

Solution

Assume that to prove $A \wedge B \Rightarrow C$. To prove $A \Rightarrow (B \to C)$ Suppose that A is True and $B \to C$ is false. Hence B is True and C is false. Thus $A \wedge B$ is true where as C is false. This contradicts our assymption

Conversely assume that $A \Rightarrow (B \to C)$ Suppose that $A \wedge B \Rightarrow C$ is false. Hence $A \wedge B$ is true and C is false. Hence A is true and $B \to C$ is false. This is a contradication to our assumption.

The result follows

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

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 $A \cap B = \phi$, $(\exists x)(A(x) \wedge B(x))$ is false. $(\exists x)(A(x) \wedge B(x))$ need not be a conclusion from $(\exists x)\ A(x)$ and $(\exists x)\ B(x)$

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

Solution

P is true and Q(4) is false, $P \to Q(4)$ is false

$\therefore\ (x)(P \to Q(x))$ is false

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

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

Solution

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

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

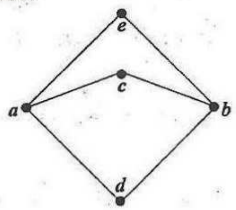
$\Leftrightarrow\ (x \in A$ and $y \in B)$ and $(x \in A$ and $y \in C)$

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

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

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

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



Solution

c and e are the upper bounds of a and b. As c and e cannot be compared, the $L \cup B$ of u,b doesnot exist. Since $a \oplus b = L \cup B\{a,b\}$ doesnot exist, the Harse diagram is not a Poset.

7. ***If $f: A \to B$ and $g: B \to C$ are mappings and $g \circ f: A \to C$ is one-to-one (Injection), prove that f is one-to-one.***

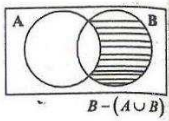
Solution

$(g \cdot f)(x) = (g \cdot f)(y) \Rightarrow x = y$ since g.f is one - to - one.

consider $f(x) = f(y) \Rightarrow g[f(x)] = g[f(y)]$

$\Rightarrow (g \cdot f)(x) = (g \cdot f)(y)$

8. *If $\psi_A(x)$ denotes characteristic function of the set A, prove that $\psi_{A\cup B}(x)=\psi_A(x)+\psi_B(x)-\psi_{A\cap B}(x)$, for all $x\in E$, the universal set.*



Solution

$x\in A\cup B$ if and only if $x\in A$ or $x\in B-(A\cap B)$

Then we have

(i) $x\in A$ only $\Rightarrow$ $x\in A\cup B$. In this case, $\psi_{A\cup B}(x)=1$,
$\psi_A(x)=1$, $\psi_B(x)=\psi_{A\cap B}(x)=0$

(ii) $x\in B-(A\cap B)$ only $\Rightarrow$ $x\in B$ and $x\notin A\cap B$. In this case
$\psi_{A\cup B}(x)=1$, $\psi_A(x)=0$, $\psi_B(x)=1$ and $\psi_{A\cap B}(x)=0$

(iii) $\psi_{A\cup B}(x)=0$, $\psi_A(x)=\psi_B(x)=\psi_{A\cap B}(x)=0$ (Not possible)

$\therefore$ In all cases, we find $\psi_{A\cup B}(x)=\psi_A(x)+\psi_B(x)-\psi_{A\cap B}(x)$

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

Solution

then $e\in Ha$, where e is the identity element in G. Ha is an equivalence class containing 'a' w.r.to an equivalence relation.

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

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

PART - B (5x16 = 80 marks)

11 (a)(i) *Prove that $(P\to Q)\wedge(Q\to R)\Rightarrow(P\to R)$* (6)

Solution

Let S : $(P\to Q)\wedge(Q\to P)\to(P\to R)$

P	Q	R	$P\to Q$	$Q\to P$	$(P\to Q)\cap(Q\to P)$	$P\to R$	S :
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Since $((P\to Q)\wedge(Q\to R))\to(P\to R)$ is a Tautology,

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

(ii) Find the principal conjuctive and principal disjunctive normal forms of the formula $S \Leftrightarrow (P \to (Q \wedge R)) \wedge (7P \to (7Q \wedge 7R))$ ***(10)***

Solution

$$S \Leftrightarrow (7P \vee (Q \wedge R)) \wedge P \vee (7Q \wedge 7R)$$

$$\Leftrightarrow ((7P \vee Q) \vee (R \wedge 7R)) \wedge ((7P \vee R) \vee (Q \wedge 7Q)) \wedge ((P \vee 7Q) \vee (R \wedge 7R)) \wedge ((P \vee 7R) \vee (Q \wedge 7Q))$$

$$\Leftrightarrow (7P \vee Q \vee R) \wedge (7P \vee Q \vee 7R) \wedge (7P \vee 7Q \vee R) \wedge (P \vee 7Q \vee R) \wedge (P \vee 7Q \vee 7R) \wedge (P \vee Q \vee 7R)$$

The RHS is the PCNF of S.

PDNF of $S \equiv (P \wedge Q \wedge R) \vee (7P \wedge 7Q \wedge R)$

Or

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

$7P \vee Q, 7Q \vee R, R \to S \Rightarrow P \to S$ ***(8)***

Solution

Proof requence

Steps	**premises**	**Reason**
(1)	$7P \vee Q$	Given premise
(2)	$P \to Q$	(1), $P \to Q \Leftrightarrow 7P \vee Q$
(3)	P	Additional premise
(4)	Q	(2), (3) Modus ponens

(5)	$7Q \vee R$	Given premise
(6)	$Q \to R$	(5) $Q \to R \Leftrightarrow 7Q \vee R$
(7)	R	(4), (6) Modus ponens
(8)	$R \to S$	Given premise
(9)	S	(7), (8) Modus ponens
(10)	$P \to S$	CP rule

$\therefore 7P \vee Q,\ 7Q \vee R,\ R \to S \Rightarrow P \to S$

(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". (8)

Solution

The premises $H_1, H_2 \ldots\ldots H_n$ are consistent if $H_1 \wedge H_2 \wedge \ldots\ldots \wedge H_n$ has truth value T provided $H_1, H_2 \ldots\ldots H_n$ are assigned the truth value T

Truth table : Technique

Let P : The system software is being upgraded

Q : Users can access the file system

R : Users can save new files

$\therefore$ The premises are $P \to 7Q$, $Q \to R$ and $7R \to 7P$

Let $S = (P \to 7Q) \wedge (Q \to R) \wedge (7R \to 7P)$

P	Q	T	$P \to 7Q$	$Q \to R$	$7R \to 7P$	S
T	T	T	F	T	T	F
T	T	F	F	F	F	F
T	F	T	T	T	T	T
T	F	F	T	T	F	F
F	T	T	T	T	T	T
F	T	F	T	F	T	F
F	F	T	T	T	T	T
F	F	F	T	T	T	T

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

$\therefore$ The premises are consistent.

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

$$(x)(P(x) \vee Q(x)) \Rightarrow (x)P(x) \vee (\exists x)Q(x) \qquad (8)$$

Solution

The negated conclusion is $7(x)\,P(x) \wedge 7(\exists x)\,Q(x)$ ie $(\exists x)7P(x) \wedge (\forall x)\,7Q(x)$ and it is used as an additional premise.

$\therefore$ We can use $(\exists x)7P(x)$ and $(x)7Q(x)$ as additional premises.

Proof sequence

Steps	Premises	Reason
(1)	$(\exists x)\ 7P(x)$	Assumed additional premise
(2)	$7P(y)$	(1) Es rule
(3)	$(x)7Q(x)$	Additional premised (assumed)
(4)	$7Q(y)$	(3) Us rule
(5)	$7P(y) \wedge 7Q(y)$	(2), (4) $P,Q \Rightarrow P \wedge Q$ (Rule T)
(6)	$(x)\ (P(x) \vee Q(x))$	Given premise
(7)	$P(y) \vee Q(y)$	(6) US rule
(8)	$7\,(P(y) \vee Q(y))$	(5) $7\ (P \vee Q) \Leftrightarrow 7P \wedge 7Q$
(9)	F	(7), (8) Rule T $P,Q \Rightarrow P \wedge Q$

$\therefore (x)\,P(x) \vee Q(x) \Rightarrow (x)P(x) \vee (\exists x)Q(x)$

(ii) *Prove that* $(\exists x)P(x) \to (x)Q(x) \Rightarrow (x)(P(x) \to Q(x))$ (8)

Solution

We assume that $(\exists x)P(x) \to (x)\,Q(x)$ is true and $(x)(P(x) \to Q(x))$ is false and obtain a contradition $(x)(P(x) \to Q(x))$ is false implies that $P(y) \to Q(y)$ is false for some y in the universe of discourse.

Hence P(y) must be true and Q(y) must be false Hence $(\exists x)P(x)$ is true and $(x)\,Q(x)$ is false.

This gives $(\exists x)P(x) \to (x)\,Q(x)$ is false. This contradiction our assumption.

$\therefore\ (\exists x)P(x) \to (x)\,Q(x) \Rightarrow (x)(P(x) \to Q(x))$

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

$$(x)(P(x) \to Q(x)) \Rightarrow (x)P(x) \to (x)Q(x) \qquad (8)$$

Solution

We assume (x)P(x) as an additional premise and derive (x) Q(x)

Proof sequence

Steps	Premises	Reason
(1)	(x)P(x)	Assumed additional premise
(2)	P(y)	(1) US rule
(3)	$(x)(P(x) \to Q(x))$	Rule P, Given premise
(4)	$P(y) \to Q(y)$	(3), US rule
(5)	Q(y)	(2), (4) Modus Ponens
(6)	(x) Q(x)	(5), US rule

(ii) Prove that $(\exists)(A(x) \vee B(x)) \Leftrightarrow (\exists x)A(x) \vee (\exists x)B(x)$ ***(8)***

Solution

Assume $(\exists x)(A(x) \vee B(x))$ is true

$\Rightarrow\ A(y) \vee B(y)$ for some y is true.

$\Rightarrow$ A(y) is true or B(y) is true

$\Rightarrow\ (\exists x)\,A(x)$ is true or $(\exists x)\,B(x)$ is true

$\Rightarrow\ (\exists x)\,A(x) \vee (\exists x)\,B(x)$ is true

$\therefore\ (\exists x)\,(A(x) \vee B(x)) \Rightarrow (\exists x)\,A(x) \vee (\exists x)\,B(x)$

Conversedy assume that $(\exists x)\,A(x) \vee (\exists x)\,B(x)$ is true

$\Rightarrow\ (\exists x)\,A(x)$ is true or $(\exists x)\,B(x)$ is true

If $(\exists x)\,A(x)$ is true, $A(y)$ is true for some y

$\Rightarrow\ A(y) \vee B(y)$ is true $\Rightarrow (\exists x)\,(A(x) \vee B(x))$ is true

If $(\exists x)\,B(x)$ is true, B(y) is true for some y

$\Rightarrow\ A(y) \vee B(y)$ is true

$\Rightarrow\ (\exists x)\,(A(x) \vee B(x))$ is true

$\therefore\ (\exists x)\,A(x) \vee (\exists x)\,B(x) \Rightarrow (\exists x)\,(A(x) \vee B(x))$

Hence we conclude that

13.(a)(i) Prove that distinct equivalence classes are disjoint. *(4)*

Solution

Let [x] denote an equivalence class with respect to an equivalence relation R.

If $z \in [x]$, then $[z] = [x]$

If $[x]$ and $[y]$ are district equivalence classes and assume $z \in [x] \cap [y]$, we obtain a contradiction.

$$z \in [x] \cap [y] \Rightarrow z \in [x] \text{ and } z \in [y]$$

$$\Rightarrow [z] = [x] \text{ and } [z] = [y]$$

$$\Rightarrow [x] = [y]$$

This is a contradiction to our assumption that $[x]$ and $[y]$ are distinct.

$\therefore [x] \cap [y] = \phi \Rightarrow [x]$ and $[y]$ are disjoint.

(ii) In a Lattice show that $a \le b$ and $c \le d$ implies $a * c \le b * d$. *(4)*

Aolution

b*d is the glb of b and b $\quad a * c \le a \le b$ and $a * c \le c \le d$

$\therefore$ a*c is a lower bound of b and d.

But b * d is the glb of b and d.

Hence $a * c \le b * d$ by definition.

(iii) In a distributive lattice prove that $a * b = a * c$ and $a \oplus b = a \oplus c$ implies that $b = c$. *(8)*

$$\begin{aligned} b &= b \oplus a*b && \text{(by absorption law)} \\ &= b \oplus (a*c) && \text{(by Hypothesis)} \\ &= (b \oplus a) * (b \oplus c) && \text{(by distributive law)} \\ &= (a \oplus c) * (b \oplus c) && \text{(by Hypothesis)} \\ &= (a*b) \oplus c && \text{(by distributive law)} \\ &= (a*c) \oplus c && \text{(by hypothesis)} \\ \therefore\ b &= c && \text{(by absorption law)} \end{aligned}$$

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

Solution

$c_1 = \{1,2\}, c_2 = \{3,4\}$ and $c_3 = \{5\}$ are the blocks of the partition.

The equivalence relation R is given by

$$R = (c_1 \times c_2) \cup (c_2 \times c_2) \cup (c_3 \times c_3)$$

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

(ii) ***Show that a chain with three or more elements is not complemented.*** ***(4)***

Solution

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

we show that 'a' has no complement in L

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

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

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

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

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

$\therefore$ 'a' has no complement

(iii) ***Establish DeMorgan's laws in a Boolean Algebra.*** ***(8)***

Solution

To show that $(a*b)^1 = a^1 \oplus b^1$, we need to show that $(a*b) * (a^1 \oplus b^1) = 0$ and $(a*b \oplus (a^1 \oplus b^1) = 1$.

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

$$= (b * a * a^1) \oplus (a * (b * b^1))$$

$$= b * 0 \oplus (a * 0) = 0 \oplus 0 = 0$$

$$= (b * a) \oplus a^1) \oplus (a * b) \oplus b^1)$$

$$= (b \oplus a^1) \oplus (a \oplus b^1)$$

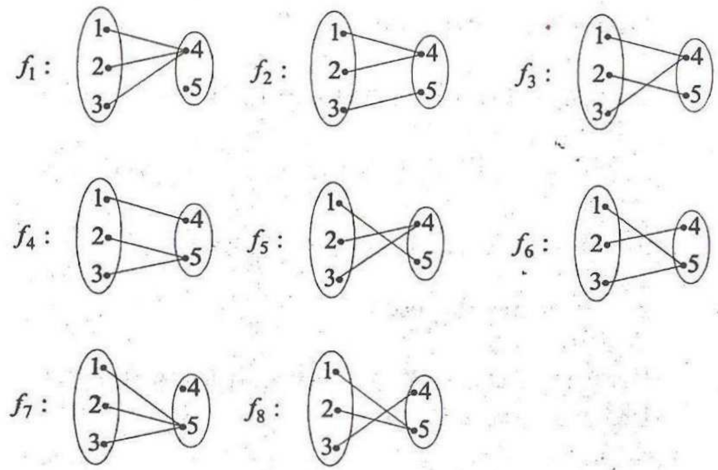
$$= (a \oplus a^1) \oplus (b \oplus b^1) = 1 \oplus 1 = 1$$

$\therefore$ $(a * b)^1 = a^1 \oplus b^1$. By duality, $(a \oplus b)^1 = a^1 * b^1$.

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.*** ***(8)***

Solution

The mappings from {1,2,3} to {4,5} are given as



Name of the above functions is one - to - one f_1 and f_7 are not onto. f_2, f_3, f_4, f_5, f_6, f_8 are onto

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

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

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

$$f^{-1} \bullet g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad \text{Hence } (g.f)^{-1} = f^{-1} \bullet g^{-1}$$

(iii) ***If R denotes the set of real numbers and $f : R \to R$ is given by $f(x) = x^3 - 2$, find f^{-1}.*** ***(4)***

Solution

Assume $f(x) = f(y) \Rightarrow x^3 = y^3$

$\Rightarrow$ Both x and y are ≥ 0 (or) both x and y are negative

$\therefore x^3 = y^3 \Rightarrow |x| = |y|$. If both x, y $\geq$ 0, then $x = y$.

If both x, y < 0, $-x = -y \Rightarrow x = y$

$\therefore$ f is one - to - one

f is onto : Let $y \in R$. To find x, such that f(x) = y,
$f(x) = y \Rightarrow x^3 - 2 = y \quad \therefore y + 2 = x^3$

If $y + 2 \geq 0$, then $x = (y+2)^{\frac{1}{3}}$ and if $y + 2 < 0$, $x = [-(y+2)]^{\frac{1}{3}}$

Hence f^{-1} exists. clearly

$f^{-1}(y) = \Big[\ (y+2^{\frac{1}{3}} \quad if \quad y+2 \geq 0$

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

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

Prove that f is a bijection and find f^{-1}. ***(8)***

Solution

Let f(m) = f(n)

If both m and n are even, $\frac{m}{2} = \frac{n}{2} \Rightarrow m = n$

Also if both m and n are odd, $\frac{1-m}{2} = \frac{1-n}{2} \Rightarrow m = n$

We show that f(m) = f(n) $\Rightarrow$ m even and n odd cannot occur.
Suppose m is even and n is odd.

Then $\frac{m}{2} = \frac{1-n}{2} \Rightarrow m + n = 1$. But m and n are the integers $\Rightarrow m + n \geq 2$

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

We next show that f is onto. If n is an integer we must find a positive interger, m such that f(m) = n

If $n > 0$, take $m = 2n$. If $n \leq 0$, take $m = 1 - 2n$.

Hence f is onto $\Rightarrow$ f is a bijection Further

$f^{-1}(n) = \Big[\ 2n \quad if \quad n > 0$

(ii) ***Let A, B and C be any three nonempty 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.*** *(8)*

Solution

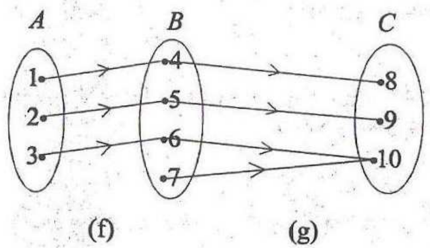
Let $z \in C$. Since $g : B \to C$ is onto, $\exists y \in B$ such that $g(y) = z$.

Since $f : A \to B$ is onto, $y \in B \Rightarrow \exists x \in A$ such that $f(x) = y$

$\therefore$ $z = g(y) = g[f(x)] = (g.f)(x)$ Hence g.f is onto

Example

g.f is onto . But g is onto and f is not onto



15. (a)(i) ***State and prove Lagrange's theorem for finite groups.*** *(12)*

Solution

Statement :

If H is a subgroup of a finite group G, then O(H) disides O(G)

Proof :

Let $O(G) = n$ and $O(H) = m$.

Consider the left cosets aH and bH of H. These are either identical or disjoint

$\therefore$ $aH \cap bH = \phi$

Further the union distinct left cosets of H is the group G.

Since G is a finite group, let there be k distinct left cosets of H.

Suppose $a_1H, a_2H, \ldots\ldots\ldots a_kH$ are the distinct left cosets of H in G

Then they are pairwise disjoint and we have

$$G = (a_1H) \cup (a_2H) \cup \ldots\ldots\ldots \cup (a_kH) \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Further any left coset of H contains the same number of elements of H.

From (1), $O(G) = O(a_1H) + O(a_2H) + \ldots\ldots\ldots + O(a_kH)$

$= O(H) + O(H) + \ldots\ldots\ldots\ldots + O(H)$ (k times)

$\Rightarrow$ $n = km$

$\therefore$ $m =$ divides $n \Rightarrow O(H)$ divides $O(G)$

(ii) ***Find all the non-trivial subgroups of $(Z_6, +_6)$*** *(4)*

Solution

$H_1 = \{[0], [3]\}$ $H_2 = \{[0], [2], [4]\}$ are non - trivial subgroups of $(z_6, +_6)$ since H_1, H_2 are closed under $+_6$

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

$(H_1, +_6)$ is a non – trivial subgroup

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

$(H_2, +_6)$ is a non – trivial

(b) If $H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

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. (16)

Solution

The Hamming code C is given by

$$C = \{x = (x_1, x_2 \ldots\ldots x_7) / x . H^T = 0 \ (\text{mod}2)\}$$

$$x.H^T = 0 \ (\text{mod } 2) \Rightarrow \quad x_4 = x_2 +_2 x_3$$

$$x_5 = x_1 +_2 x_3 \ ; \quad x_6 = x_1 +_2 x_3$$

$$x_7 = x_1 +_2 x_2$$

$$C = \{x = (x_1, x_2, x_3 \ldots\ldots x_7) / (x_1, x_2, x_3) \in B^3\}$$

x_1	x_2	x_3	x_4	x_5	x_6	x_7
0	0	0	0	0	0	0
0	0	1	1	1	1	0
0	1	0	1	0	0	1
0	1	1	0	1	1	1
1	0	0	0	1	1	1
1	0	1	1	1	1	1
1	1	0	1	1	1	0
1	1	1	0	0	0	0

Thus the code words are (0,0,0,0,0,0,0), (0,0,1, 1,1,1,0), (0,1,0,1,0,0,1), (0,1,1,0,1,1,1), (1,0,0,0,1,1,1), (1,0,1,1,0,0,1), (1,1,0,1,1,1,0), (1,1,1,0,0,0,0)

Let y = (0,1,1,1,1,1,0) be the received word. To find the corres ponding transmitted word, adding this to each code above we get

$$C \oplus y = (0, 1, 1, 1, 1, 1, 0)$$

$$= (0, 0, 1, 0, 1, 1, 1)$$

$$= (1, 1, 1, 1, 0, 0, 1)$$

$$= (1, 0, 1, 0, 0, 0, 0)$$

$$= (0, 1, 0, 0, 0, 0, 0)$$

$$= (0, 0, 0, 1, 0, 0, 1)$$

$$= (1, 1, 0, 0, 1, 1, 1)$$

$$= (0, 0, 0, 1, 1, 1, 0)$$

The word of least weight in $C \oplus y = e = (0, 1, 0, 0, 0, 0)$

$\therefore$ Transmitted code word $= e \oplus y$

$$= (0, 1, 0, 0, 0, 0, 0) \oplus (0, 1, 1, 1, 1, 1, 0)$$

$$= (0, 0, 1, 1, 1, 1, 0)$$