SHEET # 15

PUNE INSTITUTE OF COMPUTER TECHNOLOGY

27, DHANKAWADI, PUNE 411 043.

DEPT. CLASS DIV ROLL NO. DATE

SUBJECT

Questions	1	2	3	4	5	6	7	8	Total
Marks obtained									

Examiner

VISHAL JAISWAL - PICT PUNE. (IT Dept)

Group and Rings.

1) Let $A = \{₹5, ₹10\}$ & $B = \{Gum, Candy, Coke\}$

The operation of the vending m/c can be described formally as a func^n from A X A to B, as shown below.

Coins deposited	Merchandise delivered
(₹5, ₹5)	Gum
(₹5, ₹10)	Candy
(₹10, ₹5)	Candy
(₹10, ₹10)	Coke

Fig :- ①

1st coin deposited \ 2nd coin	₹5	₹10
₹5	Gum	Candy
₹10	Candy	Coke.

Fig:- ②

2) Suppose the hair color of a child is determined by that of her parents, as shown in fig ③. Clearly the relationship bet^n the hair color of a child & that of her parents can be described by a function from A X A to A where

$A = \{ light, dark \}$

Father \ Mother	light	dark
light	light	dark
dark	dark	dark.

Fig :- ③

Let A and B be two sets. A function from AXA to B is called a binary oper^n on set A.

A function from A X A to A is said to be a binary oper^n that is clos...

Let the function from $A \times A$ to A be named f.

$\therefore f(a_1, a_2)$ or $a_1 f a_2$ will denote the image of the ordered pair (a_1, a_2) in $A \times A$.

Operator symbols :- $\star, \ast, +, \cdot, \square, \oplus, \ldots$ as bin. op^n on a set. Thus we write

$\star(a_1, a_2)$ or $a_1 \star a_2$

A set together with a no. of op^n on the set, is called an algebraic system, or simply an algebra.

Let $(A, \ast)$ and $(B, \circ)$ be two algebraic systems of the same type. The algebra $(A \times B, \square)$ is called the direct product of the algebras $(A, \ast)$ & $(B, \circ)$, if the op^n $\square$ is defined for any $a_1, a_2 \in A$ & $b_1, b_2 \in B$ as

$$(a_1, b_1) \,\square\, (a_2, b_2) = (a_1 \ast a_2,\ b_1 \circ b_2)$$

The algebras $(A, \ast)$ & $(B, \circ)$ are called the factor algebra's of $(A \times B, \square)$.

Groups :-

Let $\star$ be a binary op^n on a set A. The op^n $\star$ is said to be associative if

$$(a \star b) \star c = a \star (b \star c)$$

for all a, b, c in A.

Let $(A, \star)$ be an algebra where $\star$ is binary op^n on A. $(A, \star)$ is called a **semi group** if the following cond^n are satisfied:

1. $\star$ is a closed op^n.
2. $\star$ is an associative op^n.

Ex 1:- $A = \{2, 4, 6, \dots\}$ all even +ve int. &
+ be the ordinary add^n op^n.

Ex 2:- $A = \{\alpha, \beta, \gamma, \alpha\alpha, \alpha\beta, \alpha\gamma, \dots, \alpha\alpha\alpha, \dots\}$ set of all nonempty str. from $S = \{\alpha, \beta, \gamma\}$
Let ~~A.B~~ a.b be the bin. op^n which concat^n of string a & b.

Let $(A, *)$ be an algebra where $*$ is a bin op^n on A. An element e, in A, is said to be a left identity if for all x in A, $e * x = x$

An element e in A is said to be right identity if for all x in A, $x * e = x$

L

$*$	α	β	γ	δ
α	δ	α	β	γ
β	α	β	γ	δ
γ	α	β	γ	γ
δ	α	β	γ	δ

R

$*$	α	β	γ	δ
α	α	β	δ	γ
β	β	α	γ	δ
γ	γ	δ	α	β
δ	δ	δ	β	γ

Suppose e_1 & e_2 are ~~right~~ left & right identity of an algebra $(A, *)$. Since e_1 is left identity, $e_1 * e_2 = e_2$, also e_2 is right identity, ~~then~~ $e_1 * e_2 = e_1$. Thus we have $e_1 = e_2$. It follows that w.r.t. the bin. op^n, there is at most one identity.

Ex:- Let $(N, +)$ be an algebra, where N is set of natural nos. & + is the ord. add^n op^n of integers, clearly 0 is the identity.

Let $(A, *)$ be an algebra, where $*$ is a binary op^n on A. $(A, *)$ is called a **monoid** if the following cond^n are satisfied:-

1) $*$ is a closed op^n
2) $*$ is an asso. op^n
3) There is an identity.

Ex: A be a set of people of diff. heights. Δ be a binary operⁿ such that $a \Delta b$ equal to the taller one of a and b. We note that (A, Δ) is a monoid where the identity is the shortest person in A.

Let $(A, \ast)$ be an algebra with an identity. Let a be an element in A. An element b is said to be left inverse of a if $b \ast a = e$. An element b is said to be right inverse of a if $a \ast b = e$.

$\ast$	α	β	γ	δ
α	α	β	γ	δ
β	β	δ	α	γ
γ	γ	β	β	α
δ	δ	α	γ	δ

Fig:
α is identity.

β is left inv of γ & δ is right inv of γ

Let $(A, \ast)$ be an algebra where $\ast$ is bin opⁿ. $(A, \ast)$ is called a <u>group</u> if the foll. condⁿ are satisfied:

1) $\ast$ is a closed opⁿ
2) $\ast$ is an associative opⁿ
3) There is an identity.
4) Every element in A has left inv.

P.T left inv is also right inv.

Let b be a left inv of a & c be left inv of b. Let e be identity. Since

$$(b \ast a) \ast b = e \ast b = b \rightarrow (1)$$

we have

$$c \ast ((b \ast a) \ast b) = c \ast b = e \rightarrow (2)$$

From

$$c \ast ((b \ast a) \ast b) = ((c \ast b) \ast a) \ast b$$
$$= e \ast a \ast b = a \ast b \rightarrow (3)$$

we have $a \ast b = e$ $\rightarrow$ From 2 & 3

P.T. there is an unique inv for every elem

→ Suppose both b & c are inv's of a

i.e $b \star a = e$ & $c \star a = e$

It follows that.

$$(b \star a) \star b = (c \star a) \star b$$

$$b \star (a \star b) = c \star (a \star b)$$

$$\Rightarrow \quad b = c$$

Ex 1. $(I, +)$ be an algebra, where I is the set of all integers & + is the ord. add^n op^n of integers. It is clear that $(I, +)$ is a group with 0 being the identity & the inv of n being $-n$.

Ex 2. Let $G = \{EVEN, ODD\}$ & a bin op^n be defined as in fig below:-

$\oplus$	EVEN	ODD
EVEN	EVEN	ODD
ODD	ODD	EVEN

Identity → EVEN

Inv: Both EVEN & ODD are their own inv's.

Ex 3. Let $Z_n = \{0, 1, 2, \ldots, n-1\}$. Let $\oplus$ be a bin op^n on Z_n s.t. for a & b in Z_n

$$a \oplus b = \begin{cases} a+b & \text{if } a+b < n \\ a+b-n & \text{if } a+b \geq n \end{cases}$$

Identity → 0

Inv of a → b if $(a+b) \bmod n = 0$

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

Ex 4. Matrix Mult of $n \times n$ real matrices with non-zero determinant.

Let $\star$ be a binary op^n on A. The op^n $\star$ is said to be commutative if $a \star b = b \star a$ for all a, b in A.

A group $(A,*)$ is called a commutative group or an abelian group, if $*$ is commutative op^n.

Set S
↓
Algebra with one op^n $*$
→ Closure property i.e $\forall\, a,b \in S \Rightarrow a*b \in S$
↓
SemiGroup
→ Closure property
→ Associative prop. i.e $\forall a,b,c \in S \Rightarrow a*(b*c) = (a*b)*c$
↓
Monoid
→ Closure property
→ Associative prop.
→ Existence of identity element
i.e $\forall a \in S\ \exists\, e \in S$ such that $a*e = a*e = a$
↓
Group
→ Closure property.
→ Associative
→ Identity.
→ Existence of inverse element
i.e $\forall a \in S\ \exists b \in S$ such that $a*b = e = b*a$
$b = a^{-1}$
↓
Abelian or Commutative Group
→ Closure
→ Associative
→ Identity
→ Inverse
→ Commutative property
i.e $\forall a,b \in S$ $a*b = b*a$.

Ex 1:- Let $R+$ be the set of all +ve rational numbers & $*$ a binary op^n on $R+$ defined

$a*b = ab/3$ is an abelian grp

1. Closure prop:- $\forall\, a,b$ in $R+$
$\Rightarrow a*b = ab/3 \in R+$
hence $R+$ is closed with $*$ op^n

2. Asso. prop:- $\forall\, a,b,c \in R+$

$(a*b)*c = \frac{ab}{3}*c = \frac{\frac{ab}{3}.c}{3} = \frac{abc}{9}$

$= \frac{a.\frac{bc}{3}}{3} = a*\frac{bc}{3} = a*(b*c)$

$\therefore$ $*$ is asso. on R^+.

3. Existence of Identity:-

$\frac{a.e}{3} = a$ $\therefore$ $e = 3$.

i.e $a*3 = 3*a = a$.

$\therefore$ 3 is identity element for $*$.

4. Existence of Inverse:-

$a*b = 3 \Rightarrow ab/3 = 3 \therefore b = 9/a$

$\therefore$ Every Element in R^+ has Inverse.

5. Commutative prop:- $\forall$ a, b in R^+

$a*b = \frac{ab}{3} = \frac{ba}{3} = b*a$

$\therefore$ $(R^+, *)$ is an abelian grp.

Ex 2:- The set Q_1 of all Rational nos. other than 1 with op^n $*$ defined by $a*b = a+b-ab$ is an abelian grp.

1) Closure prop:- $a, b \in Q_1$ & $a \neq 1$, $b \neq 1$

$\Rightarrow$ $a*b = a+b-ab \in Q_1$

Hence $*$ is closed on Q_1

2) Associative prop:- $\forall$ a, b, c in Q_1

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

$= a+b+c-ab-ac-bc+abc. \rightarrow (1)$

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

$= a+b+c-ab-bc-ac+abc. \rightarrow (1)$

Hence $(a*b)*c = a*(b*c)$ $\therefore$ $*$ is asso. on Q_1

3. Existence of Identity: $\forall a$ in Q, $\exists\, e$ in Q such that $a * e = a$

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

$\Rightarrow e = 0$ as $a \neq 1$

4. Existence of Inv: $\forall a$ in Q, $\exists\, b \in Q$, such that $a * b = 0 \Rightarrow a + b - ab = 0$

$a + b(1-a) = 0 \Rightarrow b = -a/(1-a) \in Q$

Hence Inv. is present for all elements.

5. Commutative prop: $\forall a, b$ in Q,

$a * b = a + b - ab = b + a - ba = b * a$.

Hence $(Q, *)$ is an abelian grp.

Ex 3 Let $R = \{0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}$ & $*$ b.o. opⁿ, so that for a & b in R, $a * b$ is over all angular rotation corresponding to successive rotations by a & then by b. Show that $(R, *)$ is a grp.

Ex 4 Show that $\langle Z_6, + \rangle$ is an abelian grp.

(16) **PUNE INSTITUTE OF COMPUTER T**
27, DHANKAWADI, PUNE 411 0

DEPT. CLASS DIV ROLL N

SUBJECT

Questions	1	2	3	4	5	6	7	8
Marks obtained								

and Fields.

) is called a ring satisfied:

VISHAL JAISWAL - PICT PUNE (IT DEPT)

ISOMORPHISMS & AUTOMORPHISMS

The algebraic system $(B, *)$ is isomorphic to the algebraic system $(A, \star)$ if we can obtain $(B, *)$ from $(A, \star)$ by renaming the elements and/or operations in $(A, \star)$. In more formal way, we say that $(B, *)$ is isomorphic to $(A, \star)$ if there exist a one-to-one onto function f from A to B such that for all a_1 and a_2 in A

$$f(a_1 \star a_2) = f(a_1) * f(a_2)$$

The function f is called an isomorphism from $(A, \star)$ to $(B, *)$ & $(B, *)$ is called an isomorphic image of A.

Ex 1

$\star$	a	b	c	d
a	a	b	c	d
b	b	a	a	c
c	b	d	d	c
d	a	b	c	d

$*$	α	β	γ	δ
α	α	β	γ	δ
β	β	α	α	γ
γ	β	δ	δ	γ
δ	α	β	γ	δ

f

$f(a) = \alpha$
$f(b) = \beta$
$f(c) = \gamma$
$f(d) = \delta$

Ex 2

$(A, \star)$

$\star$	a	b
a	a	b
b	b	a

~~$(B, *)$~~ $(B, \oplus)$

$\oplus$	Even	odd
Even	Even	odd
Odd	Odd	Even

$*$	0°	180°
0°	0	180°
180°	180°	0°

$(C, *)$

+	20	25
20	20	25
25	25	20

$(D, +)$

An Isomorphism.
$(A, *)$ to $(A, *)$
Isom...
...phism from an algebraic sys...
$(A, *)$ is called an **Automor...**
$*)$

$f(a) = d$; $f(b) = c$
$f(c) = b$; $f(d) = a.$

Homomorphism :-

Let $(A, *)$ & $(B, *)$ be two algebraic systems. Let f be a function from A onto B such that for any a_1 & a_2 in A

$$f(a_1 * a_2) = f(a_1) * f(a_2)$$

f is called a homomorphism from $(A, *)$ to $(B, *)$ & $(B, *)$ is called a homomorphic image of $(A, *)$

Ex

$\alpha \to 1$
$\beta \to 1$
$\gamma \to 1$
$\delta \to 0$
$\varepsilon \to 0$
$\zeta \to -1$

$*$	α	β	γ	δ	ε	ζ
α	α	β	α	α	γ	δ
β	β	α	γ	β	γ	ε
γ	α	γ	α	β	γ	ε
δ	α	β	β	δ	ε	ζ
ε	γ	γ	γ	ε	ε	ζ
ζ	δ	ε	ε	ζ	ζ	ζ

$*$	1	0	-1
1	1	1	0
0	1	0	-1
-1	0	-1	-1

$f(\gamma * \varepsilon) = f(\gamma) * f(\varepsilon)$
$f(\gamma) = 1 * 0$
$1 = 1$

$f(\delta * \zeta)$

8, 13, 14, 35, 36
21, 22, 30, 46, 47, 8, 51
4, 61, 62, 96, 98
7, 95

Rings, Integral Domains, and Fields

Rings :-

An algebraic system $(A, +, \cdot)$ is called a ring if the following conditions are satisfied:

1. $(A, +)$ is an abelian group.
2. $(A, \cdot)$ is a semigroup.
3. The operation $\cdot$ is distributive over opⁿ $+$.

Integral Domains :-

An algebra $(A, +, \cdot)$ is called an Integral Domain if:

1. $(A, +)$ is an abelian group.
2. The opⁿ $\cdot$ is commutative. Furthermore, if $c \neq 0$ & $c \cdot a = c \cdot b$, then $a = b$, where 0 denotes the additive identity.
3. The opⁿ $\cdot$ is the distributive over opⁿ $+$.

Fields :

$(A, +, \cdot)$ is called a field if :

1. $(A, +)$ is an abelian group.
2. $(A - \{0\}, \cdot)$ is an abelian group.
3. The opⁿ $\cdot$ distributes over the opⁿ $+$.

i) $(I, +, \cdot)$ is a ring

$+ \rightarrow$ Addⁿ

$\cdot \rightarrow$ Mult

$I \rightarrow$ set of all integers

ex: $(Z, +, \odot)$

$(a \odot b) \odot c = a \odot (b \odot c)$

$(8 \odot 9) \odot 7 = (9 \odot 7)$ ... $\{0, 1\}$