* UNIT-5 ALGEBRAIC STRUCTURES AND RING THEORY: 03/01/2022

→ Algebraic system - General properties.
→ Semi Groups - monoids - Groups - Example.
→ Theorems on sub groups & groups
→ Homomorphism - Co-sets
→ Lagrange's Theorem
→ Defn of Ring - Examples
→ Properties of ring - Sub-structures.
→ Ring homomorphism.
→ Isomorphism of Rings - Examples.

05/01/2022

BINARY OPERATOR (OR) BINARY COMPOSITION:

$+, \cdot, *, \oplus, \circ, -, \div$ → These 2 operators are do not satisfy

* Let S be a non-empty set. If $F: S \times S \to S$ is a mapping, then F is called a binary operation or binary composition in S. (Power set)
* The symbols $+, *, \cdot, \oplus$, etc. are used to denote binary operations on a set.

For $a, b \in S \Rightarrow a+b \in S \Rightarrow$ '+' is a binary operation in S.

For $a, b \in S \Rightarrow a \cdot b \in S \Rightarrow$ '$\cdot$' is a binary operation in S.

For $a, b \in S \Rightarrow a \circ b \in S \Rightarrow$ '$\circ$' " "

For $a, b \in S \Rightarrow a * b \in S \Rightarrow$ '$*$' is a "

This is said to be the closure property of the binary operation and the sets is said to be closed wrt to binary operation.

* Properties:

→ Commutative Law:

'$*$' is a binary operation in a set S if for $a, b \in S$; $a * b = b * a$ then $*$ is said to be commutative in S.
This is called commutative law.

→ Associative Law:

'$*$' is a binary operation in a set S. If for $a, b, c \in S$
(i) $a \circ (b * c) = (a \circ b) * (a \circ c)$
(ii) $(b * c) \circ a = (b \circ a) * (c \circ a)$ then '$\circ$' is said to be distributive wrt the operation $*$.

Ex: N is the set of natural numbers.

(i) $+, \cdot$ are binary operations in N, since $a, b \in N$, $a+b \in N$ and $a \cdot b \in N$.

In other words N is said to be closed wrt the operations $+$ and $\cdot$.

(ii) $+, \cdot$ are commutative in N, since for $a, b \in N$, $a+b = b+a$ and $a \cdot b = b \cdot a$.

(iii) $+, \cdot$ are associative in N, since for $a, b, c \in N$.

$a+(b+c) = (a+b)+c$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iv) '$\cdot$' is distributive wrt the operation $+$ in N, since for $a, b, c \in N$, $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.

(v) The operations subtraction ($-$) and division ($\div$) are not binary operations in N since for $3, 5 \in N$ does not imply $3-5 \in N$ and $\frac{3}{5} \in N$.

Ex: A is the set of even integers.

(i) $+, \cdot$ are binary operations in A, since for $a, b \in A$, $a+b \in A$ and $a \cdot b \in A$.

(ii) $+, \cdot$ are commutative in A; since for $a, b \in A$, $a+b = b+a$ and $a \cdot b = b \cdot a$.

(iii) $+, \cdot$ are associative in A, since for $a, b, c \in A$ $a+(b+c) = (a+b)+c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iv) '$\cdot$' is distributive wrt to the operation $+$ in A since for $a, b, c \in A$, $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.

Ex: Let S be a non empty set and $\circ$ be an operation on S defined by $a \circ b = a$ for $a, b \in S$. Determine whether '$\circ$' is commutative and associative in S.

* Since $a \circ b = a$ for $a, b \in S$ and $b \circ a = b$ for $a, b \in S$.

$a \circ b \neq b \circ a$.

$\therefore$ '$\circ$' is associative in S

Since $(a \circ b) \circ c = a \circ c = a$

$a \circ (b \circ c) = a \circ b = a$ for $a, b, c \in S$.

$\therefore$ '$\circ$' is associative in S.

Ex: '$\circ$' is operation defined on $\mathbb{Z}$ such that $a \circ b = a+b-ab$ for $a, b \in \mathbb{Z}$. Is the operation '$\circ$' a binary operation in $\mathbb{Z}$? If so, is it associative & commutative in $\mathbb{Z}$?

If $a, b \in \mathbb{Z}$, we have $a+b \in \mathbb{Z}$, $ab \in \mathbb{Z}$ and $a+b-ab \in \mathbb{Z}$

$a \circ b = a+b-ab \in \mathbb{Z}$

$a \circ b = b \circ a$.

$\therefore$ '$\circ$' is commutative in $\mathbb{Z}$.

$(a \circ b) \circ c = (a \circ b) + c - (a \circ b)c$

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

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

$a \circ (b \circ c) = a + (b \circ c) - a(b \circ c)$

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

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

$\therefore (a \circ b) \circ c = a \circ (b \circ c)$

$\rightarrow \circ$ is associative in $\mathbb{Z}$.

Ex: Fill in blanks in the following composition table so that '$\circ$' is associative in $S = (a, b, c, d)$.

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d				

$d \circ a = (c \circ b) \circ a \quad (\because c \circ b = d)$

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

$= c \circ b = \underline{d}$

$d \circ b = (c \circ b) \circ b = c \circ (b \circ b) = c \circ a = c.$

$d \circ c = (c \circ b) \circ c = c \circ (b \circ c) = c \circ c = c.$

$d \circ d = (c \circ b) \circ (c \circ b) = c \circ (b \circ c) \circ b$

$= c \circ c \circ b$

$= c \circ (c \circ b) = c \circ d = \underline{d}$

$\circ$	a	b	c	d
a	a	b	c	d
b	b	d	c	d
c	c	d	c	d
d	d	c	c	d

Ex: Let $P(S)$ be the power set of a non empty set S. Let $\cap$ be an operation in $P(S)$. Prove that associative law and commutative law are true for the operation in $P(S)$.

$P(S)$ = Set of all possible subsets of S

Let $A, B \in P(S)$

$\because A \subseteq S, B \subseteq S \Rightarrow A \cap B \subseteq S \Rightarrow A \cap B \in P(S)$

$\therefore \cap$ is a binary operation in $P(S)$

also $A \cap B = B \cap A$.

$\therefore \cap$ is commutative in $P(S)$.

Again $A \cap B$, $B \cap C$, $(A \cap B) \cap C$ and $A \cap (B \cap C)$ are subsets of S.

$\therefore (A \cap B) \cap C, A \cap (B \cap C) \in P(S)$

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

$\therefore \cap$ is associative in $P(S)$.

*ALGEBRAIC STRUCTURES:

A non empty set G equipped with one or more binary operations is called an algebraic structure or algebraic system.

If $\circ$ is a binary operation on G; then the algebraic structure is written as $(G, \circ)$.

Ex: $(N,+), (Q,-), (R,+)$ are algebraic structures

→ Semi Group:

An algebraic structure $(S, \circ)$ is called a semi group if the binary operation $\circ$ is associative in S.

That is $(S, \circ)$ is said to be a semi group if

(i) ~~$a,b \in S$~~ $\Rightarrow a \circ b \in S$ for all $a, b \in S$

(ii) $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in S$

Ex:

1) $(N,+)$ is a semi group; for $a, b \in N$
$\Rightarrow a+b \in N$ and $a, b, c \in N \Rightarrow (a+b)+c = a+(b+c)$

2) $(Q,-)$ is not a semi group;
for $5, 3/2, 1 \in Q$ does not imply $(5-3/2)-1 = 5-(\frac{3}{2}-1)$

3) $(R,+)$ is a semi group for $a, b \in R \Rightarrow a+b \in R$ and $a, b, c \in R$
$(a+b)+c = a+(b+c)$.

06/01/2023

Ex: Given $a \circ b = a-b+ab$ for $a, b \in Q$.
Then $(Q, \circ)$ is not a semigroup.

$a \circ b = a-b+ab$

By defn of semigroup:

S.T. $(a \circ b) \circ c = a \circ (b \circ c)$

LHS: $(a \circ b) \circ c = (a \circ b) - c + (a \circ b) \cdot c$

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

$\boxed{LHS = a-b-c+ab+ac-bc+abc}$

RHS: $a \circ (b \circ c) = a-(b \circ c) + a(b \circ c)$

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

$\boxed{= a+c-b-bc+ab-ac+abc}$

LHS $\neq$ RHS.
$\therefore (Q, \circ)$ is not a SG.

* $(A, *)$ be a semigroup if $a*c = c*a$ — ①
$b*c = c*b$ — ②

Show that $(a*b)*c = c*(a*b)$

LHS: $(a*b)*c$

$\Rightarrow a*(b*c) \Rightarrow$ (By associative)

$= a*(c*b)$ (by ②)

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

$= (c*a)*b$ (by ①)

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

→ Identity element of algebraic structure is unique.

$(Z^+, +)$ is not a monoid ($\because 0 \notin Z^+$)

$\therefore$ do not satisfy identity property.

commutative ⟷ abelian.

invertible → $a \in M$; $a^{-1} \in M$

invertible is unique

power set

84, 85, 86, 87

* Examples of Sub Semi Group:

→ For the semi group $(N, +)$ where N is set of non-negative Natural numbers, the algebraic structure $(Z^+, +)$ is a sub semi group.

$\because Z^+$ is subset of N; Z^+ is closed under '+' $\therefore (Z^+, +)$ is a sub semi group

→ Consider $(S, +)$ where S is the set of odd integers $[\{1, 3, 5 \ldots\}]$ is not a sub semigroup of $(N, +)$

$\because$ Sum of 2 odd nos = even $\notin S$

$\because S$ is not closed wrt to '+'

$\therefore (S, +)$ is not a sub semi group of $(N, +)$.

Ex: The operation $\circ$ is defined by $a \circ b = a$ for all $a, b \in S$. Show that $(S, \circ)$ is a semi group

→ let $a, b \in S \Rightarrow a \circ b = a \in S$

$\therefore \circ$ is a binary operation in S.

let $a, b, c \in S$, $a \circ (b \circ c) = a \circ b = a$

$(a \circ b) \circ c = a \circ c = a$.

$(a \circ b) \circ c = a \circ c = a \Rightarrow \circ$ is associative in S.

$\therefore (S, \circ)$ is a semi group.

Ex: The operation $\circ$ is defined by $a \circ b = a + b - ab$ for all $a, b \in Z$. Show that $(Z, \circ)$ is a semi group.

→ let $a, b \in Z \Rightarrow a \circ b = a + b - ab \in Z$

$\therefore \circ$ binary operation in Z.

let $a, b, c \in Z$

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

$$a \circ (b \circ c) = a \circ (b + c - bc)$$
$$= a + b + c - bc - ab - ac + abc$$

$\therefore (a \circ b) \circ c = a \circ (b \circ c)$

$\therefore \circ$ is associative in Z $\therefore (Z, \circ)$ is semi group.

* $(P(S), \cap)$ is a semi group where $P(S)$ is the power set of a non-empty set S.

↠ $P(S)$ = set of all possible subsets of S.

Let $A, B \in P(S)$

$\because A \subseteq S, B \subseteq S \Rightarrow A \cap B \subseteq S \Rightarrow A \cap B \in P(S)$

$\therefore \cap$ is a binary operation in $P(S)$.

Let $A, B, C \in P(S)$

$\therefore (A \cap B) \cap C, A \cap (B \cap C) \in P(S)$

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

$\therefore \cap$ is associative in $P(S)$.

Hence; $(P(S), \cap)$ is a semi group.

Ex: $(P(S), \cup)$ is a semi group, where $P(S)$ is the power set of a non-empty set S.

$P(S)$ = set of all possible subsets of S.

Let $A, B \in P(S)$

$\because A \subseteq S, B \subseteq S \Rightarrow A \cup B \subseteq S \Rightarrow A \cup B \in P(S)$

$\because \cup$ is a binary operation in $P(S)$.

Let $A, B, C \in P(S)$.

$\therefore (A \cup B) \cup C, A \cup (B \cup C) \in P(S)$

$\because (A \cup B) \cup C = A \cup (B \cup C)$

$\therefore \cup$ is associative in $P(S)$

Hence $(P(S), \cup)$ is a semi group.

Ex:

Q is the set of rational numbers, $\circ$ is a binary operation defined on Q such that $a \circ b = a - b + ab$, for $a, b \in Q$. Then $(Q, \circ)$ is not a semi-group.

For $a, b, c \in Q$

$(a \circ b) \circ c = (a \circ b) - c + (a \circ b)c$

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

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

$a \circ (b \circ c) = a - (b \circ c) + a(b \circ c)$

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

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

$(a \circ b) \circ c \neq a \circ (b \circ c)$

Ex: Let $(A, *)$ be a semi group. Show that for a, b, c in A if $a * c = c * a$ and $b * c = c * b$ then $(a * b) * c = c * (a * b)$

* Given $(A, *)$ be a semi group

$a * c = c * a$ and $b * c = c * b$

↠ $(a * b) * c = a * (b * c)$ [$\because A$ is a semi group]

$= a * (c * b)$ [$\because b * c = c * b$]

$= (a * c) * b$ [$\because A$ is semi group]

$= (c * a) * b$ [$\because a * c = c * a$]

$= c * (a * b)$ [$\because A$ is semi group]

*HOMOMORPHISM OF SEMI GROUPS:

*↔ Let $(S,*)$ and $(T,\circ)$ be any 2 semi-groups. A mapping $f: S \to T$ such that for any 2 elements $a, b \in S$, $f(a*b) = f(a) \circ f(b)$ is called a semi-group homomorphism.

* A homomorphism of a semi-group into itself is called a semi-group endomorphism.

Ex:

Let $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ be semi-groups and $f: S_1 \to S_2$ and $g: S_2 \to S_3$ be homomorphisms. P.T. the mapping of $g \circ f: S_1 \to S_3$ is a semigroup homomorphism.

Given that $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ are three semigroups and $f: S_1 \to S_2$ and $g: S_2 \to S_3$ be homomorphisms

Let a, b be 2 elements of S_1

$$(g \circ f)(a *_1 b) = g[f(a *_1 b)]$$
$$= g[f(a) *_2 f(b)] \quad (\because f \text{ is homomorphism})$$
$$= g(f(a)) *_3 g(f(b)) \quad (\because g \text{ is homomorphism})$$

$\therefore g \circ f$ is a homomorphism.

→ Identity Element:

Let S be a non-empty set and $\circ$ be a binary operation on S. If there exists an element $e \in S$ such that $a \circ e = e \circ a = a$ for $a \in S$; then e is called an identity element of S.

Ex:

(i) In the algebraic system $(\mathbb{Z}, +)$, the number 0 is an identity element.

(ii) In the algebraic system $(R, \cdot)$ the number 1 is an identity element.

*↔ The identity element of an algebraic system is unique.

* MONOID:

A semi group $(S, \circ)$ with an identity element wrt to the binary operation $\circ$ is known as a monoid i.e. $(S, \circ)$ is a monoid if S is a non-empty set and $\circ$ is a binary operation in S such that $\circ$ is associative and there exists an identity element wrt.

Ex: (i) $(\mathbb{Z}, +)$ is a monoid and the identity is 0.

(ii) $(\mathbb{Z}, \cdot)$ is a monoid and the identity is 1

* MONOID HOMOMORPHISM:

Let $(M, \circ)$ and $(T, \circ)$ be any 2 monoids, e_m and e_t denote identity elements of $(M, \circ)$ and $(T, \circ)$ respectively.

A mapping $f: M \to T$ such that for any 2 elements $a, b \in M$

$f(a * b) = f(a) \circ f(b)$ and

$f(e_m) = e_t$ is called a monoid homomorphism.

→ Monoid homomorphism presents the associativity and identity. It also preserves commutative. If $a \in M$ is invertible and $a^{-1} \in M$ is the inverse of a in M, then $f(a^{-1})$ is the inverse of $f(a)$ i.e.

$f(a^{-1}) = [f(a)]^{-1}$.

*SubSemi Group:

Let $(S, *)$ be a semi group and T be a subset of S. Then $(T, \circ)$ is called a sub semi group of $(S, \circ)$ whenever T is closed under $\circ$ i.e. $a * b \in T$ for all $a, b \in T$.

SUB MONOID:

Let $(S, *)$ be a monoid with e is the identity element and T be a non-empty subset of S. Then $(T, *)$ is the sub monoid of $(S, *)$, if $e \in T$ and $a * b \in T$ whenever $a, b \in T$.

Ex:

1) Under the usual addition, the semi group formed by +ve integers is a sub semi group of all integers.

2) Under the usual addition, the set of all rational numbers forms a monoid.

We denote it as $(Q, +)$.

The monoid $(Z, +)$ is a sub monoid of $(Q, +)$

3) Under the usual multiplication, the set E of all even integers forms a semi group.

This semi group is sub semi group of $(Z, \cdot)$

But it is not a sub monoid of $(Z, \cdot)$, because $1 \notin E$.

Ex: S.T. the intersection of two sub monoids of a monoid is a monoid.

* Let S be a monoid with e as the identity and S_1 and S_2 be 2 submonoids of S.

Since S_1 and S_2 are submonoids; these are monoids.

$\therefore e \in S_1$ and $e \in S_2$.

$\because S_1 \cap S_2$ is a subset of S, the associative law holds in $S_1 \cap S_2$, because it holds in S. $\therefore S_1 \cap S_2$ forms a monoid with 'e' as the identity.

* INVERTIBLE ELEMENT:

Let $(S, \circ)$ be an algebraic structure with the identity element e in S wrt $\circ$. An element $a \in S$ is said to be invertible if there exists an element $x \in S$ such that $a \circ x = x \circ a = e$.

*Note:

The inverse of an invertible element is unique.

1) Closure property: If all entries in the table are elements of S; then S closed under $\circ$.

2) Commutative law: If every row of the table coincides with the corresponding column. then $\circ$ is commutative on S.

3) Identity Element: If the row headed by an element a of S coincides with top row; then a is called the identity element.

4) Invertible element: If the identity element e is placed in the table at the intersection of the row headed by 'a' and the column headed by b then $\boxed{b^{-1} = a \text{ and } a^{-1} = b}$

Ex: $A = (1, \omega, \omega^2)$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	$\omega^3 = 1$	$\omega^4 = \omega$

* GROUPS:

If G is non empty set and $\circ$ is a binary operation defined on G such that the following 3 laws are satisfied then $(G, \circ)$ is a group.

→ ASSOCIATIVE LAW:

For $a, b, c \in G$ $(a \circ b) \circ c = a \circ (b \circ c)$

→ IDENTITY LAW:

There exists $e \in G$ such that $a \circ e = a = e \circ a$ for every $a \in G$; e is called an identity element in G.

→ INVERSE LAW:

For each $a \in G$, there exists an element $b \in G$ such that $a \circ b = b \circ a = e$; b is called as inverse of a.

Ex: The set Z of integers is a group wrt usual addition

(i) for $a, b, c \in Z$, $(a+b)+c = a+(b+c)$.

(ii) for $a, b \in Z \Rightarrow a+b \in Z$.

(iii) $0 \in Z$ such that $0+a = a+0 = a$ for each $a \in G$

$\therefore 0$ is the identity element in Z.

(iv) For $a \in Z$ there exists $-a \in Z$ such that $a+(-a) = (-a)+a = 0$.

$\therefore -a$ is the inverse of a. $(Z, +)$ is a group.

Ex: Give an example of a monoid which is not a group.

* The set N of natural numbers wrt usual multiplication is not a group.

(i) For $a, b \in N \Rightarrow a \cdot b$.

(ii) For $a, b, c \in N$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(iii) $1 \in N$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in N$.

$\therefore (N, \cdot)$ is a monoid.

(iv) There is no $n \in N$ such that $a \cdot n = n \cdot a = 1$ for $a \in N$. $\therefore$ Inverse law is not true.

→ The algebraic structure $(N, \cdot)$ is not a group.

* $(R, +)$ is a Group

* Abelian group / Commutative Group:

Let $(G, *)$ be a group. If $*$ is commutative

that is $a*b = b*a$ for all $a, b \in G$ then $(G, *)$ is called an Abelian Group.

Ex: $(\mathbb{Z}, +)$ is an Abelian group.

Ex:

Prove that $G = \{1, \omega, \omega^2\}$ is a group wrt multiplication where $1, \omega, \omega^2$ are cube roots of unity.

→ Construct composition table as follows.

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	$\omega^3 = 1$	$\omega^4 = \omega$

The algebraic system is $(G, \cdot)$ where $\omega^3 = 1$ and multiplication is the binary operation on G.

It is clear that $(G, \cdot)$ is closed wrt the operations multiplication and operation is associative.

1 is the identity element in G such that $1 \cdot a = a \cdot 1 = a \quad \forall a \in G$

Each element of G is invertible

$1 \cdot 1 = 1 \cdot 1 = 1 \Rightarrow$ 1 is its own inverse

$2 \cdot \omega \cdot \omega^2 = \omega^3 = 1 \Rightarrow$

$\Rightarrow \omega^2$ is the inverse of ω and ω is the inverse of ω^2 in G.

$\therefore (G, \cdot)$ is a group and $a \cdot b = b \cdot a \ \forall a, b \in G$ that is commutative law holds in G wrt to multiplication.

$\therefore (G, \cdot)$ is an abelian group.

*

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +) \longrightarrow$ Abelian groups.

$(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot) \longrightarrow$ not Abelian groups ∵ multiplicative inverse does not exist.

Theorem:

For every group 'G' prove that:

(i) the identity of G is unique

(ii) If $a, b, c \in G$ and $ab = ac$ then $b = c$. (Left cancellation law)

(iii) If $a, b, c \in G$ and $ba = ca$ then $b = c$ (Right Cancellation law).

(iv) The inverse of element of 'G' is unique.

$w \cdot w^2 = w^3 = 1 \Rightarrow$

$\Rightarrow w^2$ is the inverse of w and w is the inverse of w^2 in G.

$\therefore (G, \cdot)$ is a group and $a \cdot b = b \cdot a \; \forall \; a, b \in G$

that is commutative law holds in G w.r.t to multiplication.

$\therefore (G, \cdot)$ is an abelian group.

*

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +) \longrightarrow$ Abelian groups.

$(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot) \longrightarrow$ not Abelian groups

$\because$ multiplicative inverse does not exist.

Theorem:

For every group 'G' prove that:

(i) the identity of G is unique

(ii) If $a, b, c \in G$ and $ab = ac$ then $b = c$.

(left cancellation law)

(iii) If $a, b, c \in G$ and $ba = ca$ then $b = c$

(Right Cancellation law).

(iv) The inverse of element of 'G' is unique

a) To prove identity of G is unique:

Assume that there exists 2 identity elements in G i.e. $e_1, e_2 \in G$

By defn of identity

Let us consider 'e' is the identity, 'e_2' be the element of G.

$\exists\ e_1 \cdot e_2 = e_2$ — ① $\quad \exists\ e_1 \in G,\ e_2 \in G$

If e_2 is the identity; e_1 be the element of G $\quad \exists\ e_2 \cdot e_1 = e_1$ — ② $\quad \exists\ e_2 \in G, e_1 \in G$.

→ WKT commutative law holds with identity so LHS of ① & ② are equal

Equating RHS of ① & ② we get

$$e_1 = e_2$$

So this is the contradiction.

∴ Identity is unique.

(b) To prove left cancellation law:

Let $a, b, c \in G$

Consider $ab = ac$ — ①

pre multiply by a^{-1} both sides of ①

$a^{-1}ab = a^{-1}ac \Rightarrow (a^{-1}a)\,b = (a^{-1}a)\,c$

$e\,b = e\,c$ (Inverse) $\Rightarrow$ (Associative)

$b = c$ (Identity).

c) To prove right cancellation law:

Let $a, b, c \in G$ Consider $ba = ca$ — ①

post multiply by a^{-1} both sides of ①

$(ba)(a^{-1}) = ca\,(a^{-1})$ (Associative).

$b(aa^{-1}) = c(a a^{-1}) \rightarrow b\,e = c\,e$ (Inverse)

$b = c$ (Identity)

(d) To prove inverse of 'G' is unique:

Assume that x_1 & x_2 are 2 inverses of G

By def^n of inverse $\forall\ a \in G\ \exists\ x_1 \in G$ is the inverse $\quad a \cdot x_1 = e = x_1 \cdot a$ — ①

$e \rightarrow$ identity.

$\forall\ a \in G\ \exists\ x_2 \in G$ is the inverse

$a \cdot x_2 = e = x_2 \cdot a$ — ②

Consider $x_1 = x_1 \cdot e$ ($\because e \rightarrow$ identity)

$= x_1 (a x_2)$ (By ②)

$= (x_1 a)\, x_2$ (Associative)

$\therefore x_1 = x_2$ $\quad = e\, x_2$ (By ①)

∴ Inverse of G if it exists ⇒ unique $= x_2$ (Identity).

* Show that $(A, \dot{e})$ is an abelian group where $A = \{a \in \mathbb{Q} / a \neq -1\}$ and for any $a, b \in A$; $a \cdot b = a + b + ab$. $\quad \frac{p}{q} \cdot \frac{r}{s}$

Soln:

Given $A = \{a \in \mathbb{Q} / a \neq -1\}$ & $\forall\ a, b \in A$;

$a \cdot b = a + b + ab$ — ①

* To show $(A, \cdot)$ is abelian group:

→ Closure: $\forall\ a, b \in A$; $a \cdot b = a + b + ab \in A$ is true.

→ Associative: $\forall\ a, b, c \in A$

Consider $(a \cdot b) \cdot c = (a \cdot b) + c + (a \cdot b)\,c$

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

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

$a \cdot (b \cdot c) = a + (b \cdot c) + a(b \cdot c)$

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

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

LHS = RHS.

$\therefore$ Hence $\cdot$ is associative.

Identity: $\forall a \in A \ \exists \ e \in A \ni$

$a \cdot e = e \cdot a = a$

Consider $a \cdot e = a + e + ae = a$

$a + e(1+a) = a$

$e(1+a) = 0$

$\boxed{e = 0 \text{ (or) } a = -1}$

As $a \neq -1$

$\therefore e = 0$ is the identity element of G.

III^{ly} $e \cdot a = a$ gives $e = 0$

$e \cdot a = e + a + ea = a$

$= e(1+a) + a = a$

$e = 0; a = -1$ ✗

$\therefore e = 0$ is the identity element.

Inverse: $\forall a \in A \quad \exists \ x \in A \quad a \cdot x = x \cdot a = e$

$a \cdot x = 0 \quad (\because e = 0)$

$a + x + ax = 0$

$a + x(1+a) = 0$

$x = \frac{-a}{1+a}$ which is inverse of G.

III^{ly} $x \cdot a = 0$

$x + a + ax = 0$

$a + x(1+a) = 0$

$x = \frac{-a}{1+a}$

*Commutative:

$\forall a, b \in A$

$a \cdot b = b \cdot a$

Consider $a \cdot b = a + b + ab$

$= b + a + ba$

$= b \cdot a$

$\therefore (A, \cdot)$ is an Abelian group.

* Prove that $(A, \cdot)$ is a non-abelian group where $A = R^* \times R$ and $(a, b) \cdot (c, d) = (ac, bc+d)$

→ Given $(A, \cdot)$ where $A = R^* \times R$.

and $(a,b) \cdot (c,d) = (ac, bc+d)$

Closure: $(a,b), (c,d) \in A \ni (a,b), (c,d)$

$= (ac, bc+d) \in A$.

closure exists.

Associative:

Let $(a,b), (c,d), (e,f) \in A$

Consider $(a,b)[(c,d).(e,f)]$

$= (a,b)\cdot[ce, de+f]$

$= [ace, bce+de+f]$

consider $= [(a,b)\cdot(c,d)]\cdot(e,f)$

$= (ac, bc+d)\cdot(e,f)$

$= (ace, (bc+d)e+f)$

$= (ace, bce+de+f)$

LHS = RHS $\Rightarrow$ Associative law holds.

Identity: $\forall (a,b) \in A \; \exists \; (e_1,e_2) \in A$

$\Rightarrow (a,b)\cdot(e_1,e_2) = (a,b)$ — (a.5)

$(ae, be_1+e_2) = (a,b)$

$ae_1 = a \Rightarrow e_1 = 1$

$be_1 + e_2 = b \Rightarrow e_2 = 0$

$\because (1,0)$ $\therefore$ Identity exists

Inverse: $\forall (a,b) \in A \; \exists (x_1,x_2) \in A$

$\Rightarrow (a,b)\cdot(x_1,x_2) = (e_1,e_2) = (1,0)$

$\because (e_1,e_2) = (1,0)$

$(ax_1, bx_1+x_2) = (1,0)$

$ax_1 = 1$ $\qquad bx_1 + x_2 = 0$

$x_1 = \frac{1}{a}$ $\qquad \frac{b}{a} + x_2 = 0$

$x_2 = -\frac{b}{a}$

$\therefore$ Inverse of (a,b) is $\left(\frac{1}{a}, -\frac{b}{a}\right)$

$\therefore$ Hence $(A,\cdot)$ is a group.

Commutative:

Consider $(a,b), (c,d) \in A$

We have to show that

$(a,b)\cdot(c,d) = (c,d)\cdot(a,b)$

$(ac, bc+d) \neq (ac, ad+b)$

$\therefore$ commutative fails

$\therefore (A,\cdot)$ is a non-abelian group.

* Show that 'G' is abelian iff $(ab)^2 = a^2b^2 \; \forall a,b \in G$.

Initially we have to consider 'G' is abelian $\forall a,b \in G$, $ab = ba$ — (1)

Now; we have to P.T $(ab)^2 = a^2b^2$

Consider: $(ab)^2 = (ab)(ab)$

$= a(ba)b$ (Associative)

$= a(ab)b$ (commutative)

$= (aa)(bb)$ (Associative)

$= a^2b^2$

$\therefore (ab)^2 = a^2b^2$

We now prove G is an abelian group

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

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

$a(ba)b = a(ab^2)$ (Associativ

$(ba)b = (ab)b$

(Left Cancellation)

$ba = ab$

(Right cancellation)

$\therefore$ G satisfies commutative

$\therefore$ G is abelian

12/01/2023

* SUB-GROUP:

* Theorem:

H is a non-empty set & H is a Sub-group of G iff (1) $\forall a, b \in H \Rightarrow ab \in H$

(2) $\forall a \in H \Rightarrow a^{-1} \in H$

$\therefore$ H is a sub-group of G

(i) $H \subset G$

(ii) G satisfies group properties → closure, associative, Identity, Inverse.

(iii) H satisfies same group properties → closure, associative, Identity, Closure.

Proof:

Given 'H' is a non-empty subset of 'G'

We have to prove 'H' is a sub-group of G

iff (i) $\forall a, b \in H$, $ab \in H$

(ii) $\forall a \in H$, $a^{-1} \in H$

→ Firstly, consider 'H' is a sub group of G and we have to P.T. a) & b) conditions

$\because$ H is a sub group of G it must satisfies the group properties.

Group properties:

By closure property of H

$\forall a, b \in H$, $ab \in H$

also $\forall a \in H$, $\exists\ a^{-1} \in H$ (By inverse property

Conversely,

Suppose that ⓐ & ⓑ conditions holds

good and we have to prove that H is a subgroup of G

∵ Given that $\forall a,b \in H, ab \in H$

i.e. closure is true.

∵ H is a non-empty subset of G and clearly H is the associative of G

i.e. $\forall a,b,c \in H \Rightarrow (ab)c = a(bc)$ in G and also $(ab)c = a(bc)$ in H.

Also from (b) $\forall a \in H, a^{-1} \in H$

using this in (a) $\forall a, a^{-1} \in H$

$aa^{-1} \in H$

$e \in H$

$\exists$ identity $e \in H$

So associative holds $\Rightarrow$ closure holds.

inverse holds $\Rightarrow$ identity exists.

∴ 'H' satisfies all the properties of a groups

∴ 'H' is a subgroup of G.

* SUB GROUPS:

If 'G' is a group and H is a non-empty subset of group 'G' then 'H' is said to be a sub group of 'G' if 'H' is a group under the binary operation of 'G'.

Note:

Every 'G' has 2 subgroups {e} and itself are called trivial subgroups (or) improper subgroups.

Other than {e} and itself are called non-trivial subgroups (or) proper subgroups.

Ex: The group $(\mathbb{Z},+)$ is a sub group of $(\mathbb{Q},+)$. Also $(\mathbb{Q},+)$ is a subgroup of $(\mathbb{R},+)$. $(\mathbb{Z},\cdot)$ is not a subgroup of $(\mathbb{Q},\cdot)$.

* Order of an element:

Let $(G,*)$ be a group and $a \in G$, then the least +ve integer 'n' if exists such that $a^n = e$ is called the order of $a \in G$.

The order of an element $a \in G$ is denoted by $O(a)$.

Ex: $G = \{1,-1,i,-i\}$ is a group wrt multiplication.

1 is the identity in G

$1^1 = 1^2 = 1^3 = \cdots = 1 \Rightarrow O(1) = 1$

$(-1)^2 = (-1)^4 = (-1)^6 = \cdots = (+1) \Rightarrow O(-1) = 2$

$i^4 = i^8 = \ldots = 1 \Rightarrow O(i) = 4$

$(-i)^4 = (-i)^8 = \ldots = 1 \Rightarrow O(-i) = 4$

Ex:

In a group G, a is an element of order 30. Find the order of a^5.

Given $O(a) = 30$

$a^{30} = e$, e is the identity element of G.

$O(a^5) = n$

$(a^5)^n = e$

$a^{5n} = e$, where n is the least +ve integer

Hence 30 is the divisor of $5n$:

$\therefore n = 6$

Hence $O(a^5) = 6$.

Ex:

Let $H = \{0, 2, 4\} \subseteq Z_6$ check that $(H, +_6)$ is a subgroup of $(Z_6, +_6)$.

Solve

Sol: $Z_6 = \{0, 1, 2, 3, 4, 5\}$

$\therefore (Z_6, +_6)$ is a group.

$H = \{0, 2, 4\}$

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

The following conditions are to be satisfied in order to prove that it is a subgroup.

(i) **closure:** Let $a, b \in H \Rightarrow a +_6 b \in H$

$0, 2 \in H \Rightarrow 0 +_6 2 = 2 \in H$

(ii) **Associative:** Let $a, b, c \in H \Rightarrow$

$(a +_6 b) +_6 c = a +_6 (b +_6 c)$

$0, 2, 4 \in H \Rightarrow (0 +_6 2) +_6 4$

$2 +_6 4 = 0$

$0 +_6 (2 +_6 4) = 0 +_6 (0) = 0$

(iii) **Identity element:** The row headed by 0 is exactly same as the initial row.

$\therefore 0$ is the identity element.

(iv) **Inverse element:** $0^{-1} = 0$; $2^{-1} = 4$ $\quad 4^{-1} = 2$

Inverse exist for each element of $(H, +_6)$

$\therefore (H, +_6)$ is a sub group of $(Z_6, +_6)$

* Homomorphism of Groups:

(i) Homomorphism into: Let $(G,*)$ and $(H,\circ)$ be 2 groups and f be a mapping from G into H. If $a, b \in G$

$$f(a*b) = f(a) * f(b) \quad \forall\ f(a), f(b) \in H$$

Then f is called homomorphism G into H.

(ii) Endomorphism:
A homomorphism of a group G into itself is called an endomorphism.

(iii) Homomorphism onto:
Let $(G,*)$ and $(H,\circ)$ be 2 groups and f be a mapping from G onto H.
If for $a, b \in G$ $f(a*b) = f(a) \circ f(b)$
$\forall\ f(a), f(b) \in H$
then f is called homomorphism G onto H.
Also there H is said to be a homomorphic image of G.
We write this as $f(a) \cong H$.

(iv) Epimorphism:
If the homomorphism is onto, then it is $\forall y \in G$ called epimorphism.

(v) Monomorphism:
A homomorphism is one-one, then it is called an monomorphism.

* Isomorphism of Groups:

Let $(G,*)$ and $(H,\circ)$ be 2 groups and f be a one-one mapping of G onto H If for $a, b \in G$, $f(a*b) = f(a) \circ f(b)$, then f is said to be an isomorphism forms G onto H.

* Automorphism:

An isomorphism of a group G into itself is called an automorphism.

Ex:
Let G be the additive group of integers and H be the multiplicative group. Then mapping $f: G \to H$ given by $f(x) = 2^x$ is a group homomorphism of G into H.

$\because x, y \in G \Rightarrow x+y \in G$ and $2^x, 2^y \in H$

$\therefore f(x+y) = 2^{x+y} = 2^x \cdot 2^y$.

$\therefore f(x+y) = f(x) \cdot f(y)$.

$\therefore f$ is a homomorphism of G into H.

Ex: Let G be a group of +ve real numbers under multiplication and H be a group of all real numbers under addition. The mapping $f: G \to H$ given by $f(x) = \log_{10} x$. Show that f is an isomorphism.

Sol: $f(x) = \log_{10} x$

Let $a, b \in G \Rightarrow ab \in G$,

also $f(a), f(b) \in H$

$\therefore f(ab) = \log_{10}(ab) = \log_{10} a + \log_{10} b$

$= f(a) + f(b)$

$\therefore$ f is a homomorphism from G into H.

$\ast\rightarrow$ f is one one:

Let $x_1, x_2 \in G$ & $f(x_1) = f(x_2)$ we have

to P.T. $x_1 = x_2$

$\log_{10} x_1 = \log_{10} x_2$

$10^{\log_{10} x_1} = 10^{\log_{10} x_2}$

$\boxed{x_1 = x_2}$

$\therefore$ f is one-one.

$\ast\rightarrow$ f is onto:

for every $y \in H$, $\exists\ 10^y \in G$ $\Rightarrow$

$\exists\ f(10^y) = y$

$f(10^y) = \log_{10} 10^y = y$

$\therefore$ f is onto ($\because$ Each element of H has a pre-image in G).

$\therefore$ f is isomorphism from G to H.

$\ast\rightarrow$ **Ex:** (H.W)

If R is the group of real numbers under the addition and R^+ is the group of +ve real numbers under the multiplication. Let $f: R \to R^+$ be defined by $f(x) = e^x$, then show that f is one isomorphism.

* Theorem:

If H_1 and H_2 are 2 subgroups of a group G, then $H_1 \cap H_2$ is also a subgroup of G.

Proof:

Let H_1 and H_2 be two subgroups of a group G.

Let e be the identity element in G.

$\therefore e \in H_1$ and $e \in H_2$

$\therefore e \in H_1 \cap H_2$

$H_1 \cap H_2 \neq \emptyset$

Let $a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$

$\therefore a \in H_1, a \in H_2$ and $b \in H_1, b \in H_2$

$\Rightarrow ab^{-1} \in H_1$

Illly $ab^{-1} \in H_2$

$\therefore ab^{-1} \in H_1 \cap H_2$

Thus, we have $a \in H_1 \cap H_2, b \in H_1 \cap H_2$

$\Rightarrow ab^{-1} \in H_1 \cap H_2$

$\therefore H_1 \cap H_2$ is a subgroup of G.

Ex: Let G be the group and $Z = \{x \in G / xy = yx \text{ for all } y \in G\}$ P.T. Z is a subgroup of G.

$\because e \in G$ and $ey = ye$, for all $y \in G$

It follows that $e \in Z \therefore Z$ is non-empty.

Take any $a, b \in Z$ and $y \in a$ then

$(ab)y = a(by)$

$= a(yb)$; $\because b \in Z$, $by = yb$

$= (ay)b = (ya)b$

$= y(ab)$

$\Rightarrow$ This shows that $ab \in Z$

Let $a \in Z \Rightarrow ay = ya$ for $a \in H$

$a^{-1}(ay)a^{-1} = a^{-1}(ya)a^{-1}$

$(a^{-1}a)(ya^{-1}) = (a^{-1}y)(aa^{-1})$

$e(ya^{-1}) = (a^{-1}y)e$

$$\boxed{a^{-1}y = ya^{-1}}$$

This shows that $a^{-1} \in Z$.

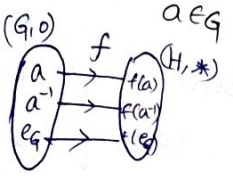
Thus, when $a, b \in Z$; we have $ab \in Z$ and $a^{-1} \in Z$ $\therefore Z$ is a subgroup of G

$\therefore$ This subgroup is called the centre of G.

*Theorem:

If (G,o) and $(H,*)$ are groups wrt identities e_G, e_H and if $f: G \to H$ is a homomorphism then prove

(a) $f(e_G) = e_H$ (b) $f(a^{-1}) = [f(a)]^{-1}$ $\forall$ $a \in G$



Proof:

Given (G,o) and $(H,*)$ are groups and $e_G \in G$, $e_H \in H$

also $f: G \to H$ is a homomorphism

$\forall a,b \in G$, $f(a \circ b) = f(a) * f(b)$ — (1)

to prove $f(e_G) = e_H$:

Consider $f(e_G) = f(e_a) * e_H$

(product of 2 identity elements is an identity)

i.e. $f(e_G) * e_H = f(e_G)$

$= f(e_G \circ e_G)$ $(\because e_G \circ e_G = e_G)$

$f(e_a) * e_H = f(e_a) * f(e_a)$ [By homomorphism]

$e_H = f(e_G)$ [By left cancellation law]

$\Rightarrow f(e_G) = e_H$

to prove $f(a^{-1}) = [f(a)]^{-1}$ $\forall$ $a \in G$

Let $a \in G$ then $e^H = f(e_G) = f(a \circ a^{-1})$

$e_H = f(a) * f(a^{-1})$

$f(a) * [f(a)]^{-1} = f(a) * f(a^{-1})$

$f(a^{-1}) = [f(a)]^{-1}$ (By Left Cancellation law)

$\Rightarrow$ Hence proved.

* To show $f(s)$ is a subgroup of H for each subgroup s of G:

$\because$ s is a subgroup of G we have $s \neq \emptyset$

$\Rightarrow f(s) \neq \emptyset$ — (1)

Let $x, y \in f(s)$

$\Rightarrow x = f(a)$ & $y = f(b)$ for some $a, b \in S$

(i) Now $x * y = f(a) * f(b)$

$= f(a \circ b) \in f(s)$ — (2)

(ii) Consider $x^{-1} = [f(a)]^{-1} = f(a^{-1})$ (by (b))

$x^{-1} = f(a^{-1}) \in f(s)$ — (3)

$\because a^{-1} \in S$ when $a \in S$.

By a theorem i.e. If H is a non empty subset of G and

(a) $\forall a \in H$, $a^{-1} \in H$ (b) $\forall a, b \in H$, $ab \in H$

from (1), (2), (3). it is clear that $f(s)$ is a subgroup of H.

Hence proved.

*Direct Product:

If $(G,\circ)$ and $(H,*)$ are 2 groups and there is defined a binary operation $\cdot$ on $G\times H$ by $(g_1,h_1)\cdot(g_2,h_2)=(g_1\circ g_2, h_1 * h_2)$ then $(G\times H,\cdot)$ is a group and is called the direct product of G & H.

→ COSETS:

If H is a subgroup of G then for each $a\in H$ the set $aH=\{ah/h\in H\}$ is called a left coset of H in G.

The set $Ha=\{ha/h\in H\}$ is called a right coset of H in G.

→ If the operation in 'G' is addition then we write

$a+H=\{a+h/h\in H\}$ → Left coset

$H+a=\{h+a/h\in H\}$ → Right coset

*Show that the set Q^+ of all +ve rational numbers forms an abelian group under the composition defined by '$\circ$' such that $a\circ b=ab/3$ for $a,b\in Q^+$.

Sol: Q^+ of the set of all +ve rational numbers and

Closure:

for $a,b\in Q^+$ we have the operation '$\circ$' such that $a\circ b=ab/3\in Q^+$

Associative:

for $a,b,c\in Q^+$

$\Rightarrow (a\circ b)\circ c=a\circ(b\circ c)$

$(ab/3)\circ c=a\circ(bc/3)$

$\frac{abc}{9}=\frac{abc}{9}$

LHS:

$(a\circ b)\circ c$

$=\frac{ab}{3}\circ c$

$=\frac{abc}{9}$

$a\circ(b\circ c)$

$=\frac{abc}{9}$

Identity:

Let $a\in Q^+$; Let $e\in Q^+ \ni e\circ a=a$.

$\Rightarrow a\circ e=a$ to get $e=3\in Q^+$ $\frac{ea}{3}=a$

Inverse:

Let $a\in Q^+$; Let $x\in Q^+$ such that $a\circ x=e$

$\frac{ax}{3}=3$

$x=\frac{9}{a}\in Q^+$

$\Rightarrow x\circ a=e$; we get $x=\frac{9}{a}\in Q^+$

Commutative: Let $a,b\in Q^+ \Rightarrow a\circ b=b\circ a$

$\frac{ab}{3}=\frac{ba}{3}$

$(Q^+,\circ)$ is an abelian group

* Prove that set G of rational numbers other than 1 with operation $\oplus$ such that $a \oplus b = a+b-ab$ for $a, b \in G$ is an abelian group. (HW)

* Let $(G, *)$ where G is the set of all non-zero real numbers and $*$ is a binary operation defined by $a * b = \frac{ab}{4}$ $\forall a, b \in G$ s.t. $(G, *)$ is an abelian group. (HW)

* **Addition modulo m:**

If 'a' and 'b' are any 2 integers, 'm' is fixed integer and 'r' is the least non-negative remainder obtained by dividing the ordinary sum of a and b by m; then the addition modulo m of a & b is 'r' symbolically

$$a +_m b = r \quad ; \quad 0 \leq r < m$$

Ex: $20 +_6 5 = 1$; $\because 20+5 = 25$
$= 24+1 = 4(6)+1$ i.e.
1 is the remainder when 20+5 is divisible by 6.

* **Multiplication modulo p:**

If a and b are any 2 integers and r is the least non-negative remainder obtained by dividing the ordinary product of a & b by p, then multiplication modulo p of a & b is r. Symbolically $a \times_p b = r \; ; \; a \leq r < p$

Ex: Show that the set $G = \{0, 1, 2, 3, 4\}$ is an abelian group wrt to addition modulo 5.

→ We construct the composition table as follows:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$4 +_5 1 = 5$
$4 +_5 2 = 6$
$4 +_5 3 = 7$
$4 +_5 4 = 8$

Closure:

∵ All the entries in the composition table are elements of G, the set G is closed wrt addition modulo 5.

Associative:

$\forall a, b, c \in G$ $(a +_5 b) +_5 c$ and $a +_5 (b +_5 c)$ leaves the same remainder when divided by 5

$(1 +_5 3) +_5 4 = 3 = 1 +_5 (3 +_5 4)$

Identity:

Clearly $0 \in G$, is the identity element;

∵ $0 +_5 a = 4 = a +_5 0$ $\forall a \in G$

Inverse: Each element in G is invertible wrt addition modulo 5.

0 is

Inverse of '1' is 4
Inverse of '2' is 3
Inverse of '3' is 2
Inverse of '4' is 1

Commutative:

from the table, we observed that I^{st} is equal to I^{st} column

III^{ly} all rows satisfies the same property so commutative property satisfies in a symmetric matrix.

Hence $(G, +_5)$ is an abelian group.

* Consider the group $G = \{1, 5, 7, 11, 13, 17\}$ under multiplication modulo 18. Construct the multiplication table of G and find the values of $5^{-1}, 7^{-1}, 17^{-1}$. (HW)

Ex: Show that $G = \{x \mid x = 2^a 3^b \text{ for } a, b \in z\}$ is a group under multiplication.

Closure: $\forall x, y \in G \Rightarrow x, y \in G$

Consider $x = 2^a 3^b$, $y = 2^c \cdot 3^d$

$x \cdot y = 2^{a+c} \cdot 3^{b+d} \in G \quad \forall a+c, b+d \in z$

Associative:

$\forall x, y, z \in G \Rightarrow (x \cdot y) \cdot z = x \cdot (y \cdot z)$

LHS: $(x \cdot y) \cdot z$ $\qquad x = 2^a \cdot 3^b$

$= (2^a \cdot 3^b \cdot 2^c \cdot 3^d)\, 2^e \cdot 3^f$ $\qquad y = 2^c 3^d$

$= 2^{a+e+c} \cdot 3^{b+d+f}$ $\qquad z = 2^e \cdot 3^f$

RHS: $(x \cdot (y \cdot z)) = 2^a 3^b \left((2^c 3^d)(2^e 3^f) \right)$

$= 2^a 3^b \cdot (2^{c+e} \cdot 3^{d+f})$

$= 2^{a+c+e} \cdot 3^{b+d+f}$.

LHS = RHS.

Existence of identity: Let $x \in G$; we have

$e = 2^0 3^0 \in G$; since $0 \in z$

$x \cdot e = x = e \cdot x$

$(2^a \cdot 3^b)(2^0 \cdot 3^0) = 2^{a+0} \cdot 3^{b+0} = 2^a \cdot 3^b = x$

$\Rightarrow e \cdot x = x$

$\therefore e = 2^0 3^0$ is the identity element in G.

Existence of Inverse

Let $y = 2^{-a} \cdot 3^{-b}$ exists

$\because -a, -b \in z$

$\exists\ x \cdot y = e = y \cdot x \quad \forall x = 2^a 3^b \in G$

$\because a, b \in z$

$(2^a \cdot 3^b)(2^{-a} \cdot 3^{-b}) = 2^0 3^0 \quad (\because e = 2^0 3^0)$

$\Rightarrow y \cdot x = 2^0 3^0 = e$

$\therefore (G, \cdot)$ is a group.

Ex: Show that $G = \{x \mid x = 2^a 3^b \text{ for } a, b \in \mathbb{Z}\}$ is a group under multiplication.

Closure: $\forall x, y \in G \Rightarrow x \cdot y \in G$

Consider $x = 2^a 3^b$, $y = 2^c \cdot 3^d$

$x \cdot y = 2^{a+c} \cdot 3^{b+d} \in G \quad \forall a+c, b+d \in \mathbb{Z}$

Associative:

$\forall x, y, z \in G \Rightarrow (x \cdot y) \cdot z = x \cdot (y \cdot z)$

LHS: $(x \cdot y) \cdot z$

$= (2^a \cdot 3^b \cdot 2^c \cdot 3^d)\, 2^e \cdot 3^f$

$= 2^{a+c+e} \cdot 3^{b+d+f}$

$x = 2^a \cdot 3^b$

$y = 2^c 3^d$

$z = 2^e \cdot 3^f$

RHS: $(x \cdot (y \cdot z)) = 2^a 3^b \left((2^c 3^d)(2^e 3^f) \right)$

$= 2^a 3^b \cdot (2^{c+e} \cdot 3^{d+f})$

$= 2^{a+c+e} \cdot 3^{b+d+f}$.

LHS = RHS

Existence of identity: Let $x \in G$; we have

$e = 2^0 3^0 \in G$; since $0 \in \mathbb{Z}$

$x \cdot e = x = e \cdot x$

$(2^a \cdot 3^b)(2^0 \cdot 3^0) = 2^{a+0} \cdot 3^{b+0} = 2^a \cdot 3^b = x$

$\Rightarrow e \cdot x = x$

$e = 2^0 3^0$ is the identity element in G.

Existence of Inverse

Let $y = 2^{-a} \cdot 3^{-b}$ exists

$\because -a, -b \in \mathbb{Z}$

$\exists\ x \cdot y = e = y \cdot x \quad \forall x = 2^a 3^b \in G$

$\because a, b \in \mathbb{Z}$

$(2^a \cdot 3^b)(2^{-a} \cdot 3^{-b}) = 2^0 3^0 \quad (\because e = 2^0 3^0)$

$\Rightarrow y \cdot x = 2^0 3^0 = e$

$\therefore (G, \cdot)$ is a group.

20/01/2023

*Note:

① If G is an additive group, $a+b = a+c$

$\Rightarrow b = c$ & $b+a = c+a \Rightarrow b = c$

② In a semi group cancellation laws may not hold

Let S be the set of all 2×2 matrices over integers and let matrix multiplication be the binary operation defined on S. Then S is a semi group of the above operation

If $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$; $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$; $C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ then $A, B, C \in S$ and $AB = AC$ we observe that left cancellation law is not true in the semi group

③ $(N, +)$ is a semi group

But $(N, +)$ is not a group

Ex: If every element of a group G is its own inverse. Show that G is an abelian group.

Soln: Let $a, b \in G$

By hypothesis

$a^{-1} = a$, $b^{-1} = b$

Then $ab \in G$ & hence $(ab)^{-1} = ab$

Now $(ab)^{-1} = ab$

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

$\therefore$ G is an abelian group.

Note: The converse of the above not true.

Ex: $(R, +)$ where R is the set of all real numbers is abelian group; but no element except 0 is its own inverse

* Prove that if $a^2 = a$; then $a = e$; a being an element of a group G.

Proof: Let a be an element of a group G such that $a^2 = a$

To prove that $a = e$.

G.T. $a^2 = a$

$\Rightarrow a \cdot a = a$

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

$a(aa^{-1}) = e \quad \because aa^{-1} = e$

$ae = e \quad (\because ae = a)$

$a = e$

* In a group G having more than one elem If $x^2 = x$ for every $x \in G$ prove that G is abelian.

Soln: Let $a, b \in G$

Under the given hypothesis; we have $a^2 = a$, $b^2 = b$

$(ab)^2 = ab$

$a(ab)b = (aa)(bb) = a^2b^2 = ab = (ab)^2$

$= (ab)(ab)$

$= a(ba)b$

$ab = ba$ (Using cancellation laws)

$\therefore$ G is abelian.

* Show that in a group G, for $a, b \in G$
$(ab)^2 = a^2b^2 \iff G$ is abelian

Soln Let $a, b \in G$ & $(ab)^2 = a^2b^2$ to prove that G is abelian

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

$(ab)(ab) = (aa)(bb)$

$a(ba)b = a(ab)b$ (By associative law)

$ba = ab$ (by cancellation laws)

$\therefore G$ is abelian

Conversely; Let G be abelian;

to prove that $(ab)^2 = a^2b^2$

then $(ab)^2 = (ab)(ab) = a(ba)b$

$= a(ab)a$ ($\because$

$= a^2b^2$

* If a, b are any 2 elements of a group $(G, \cdot)$ which commute show that

(1) a^{-1} & b commute

(2) b^{-1} & a commute

(3) a^{-1} & b^{-1} commute

Soln 1) $(G, \cdot)$ is a group & such that $ab = ba$

(1) $ab = ba$

$a^{-1}(ab) = a^{-1}(ba)$ [premultiply by a^{-1} on both sides)

$(a^{-1}a)b = a^{-1}(ba)$ [By associative]

$eb = (a^{-1}b)a$ ($\because a^{-1}a = e$ & associative)

$b = (a^{-1}b)a$ ($eb = b$ by identity)

$ba^{-1} = [(a^{-1}b)a]a^{-1}$ (post multiply by a^{-1})

$= (a^{-1}b)(aa^{-1})$ (Associative)

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

$ba^{-1} = a^{-1}b$

$\therefore a^{-1}$ & b commute

2) $ab = ba$

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

$a(bb^{-1}) = (ba)b^{-1}$

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

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

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

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

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

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

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

b^{-1} and a commute

3) $ab = ba$

$(ab)^{-1} = (ba)^{-1}$

$b^{-1}a^{-1} = a^{-1}b^{-1}$

a^{-1} & b^{-1} are commute

*Ring Structure

If R is a non-empty set and '+', '·' are 2 binary operations defined on R then $(R,+,\cdot)$ is said to be a Ring if it satisfies the following properties

1) $(R,+)$ is an abelian group

(i) Closure: $\forall a,b \in R, a+b \in R$

(ii) Associative: $\forall a,b,c \in R \; (a+b)+c = a+(b+c)$

(iii) Identity: $\forall a \in R, \exists x \in R \Rightarrow a+x = a = x+a$

(iv) Inverse: $\forall a \in R \; \exists x \in R \Rightarrow a+x = e = x+a$

(v) abelian: $\forall a,b \in R, a+b = b+a$

2) $(R,\cdot)$ is a semi group:

(i) closure: $\forall a,b \in R \;\; a.b \in R$

(ii) Associative: $\forall a,b,c \in R \;\; (a\cdot b)\cdot c = a\cdot(b\cdot c)$

3) $(R,+,\cdot)$ is distributive

$\forall a,b,c \in R \Rightarrow a\cdot(b+c) = a\cdot b + a\cdot c$

& $(b+c)\cdot a = b\cdot a + c\cdot a$

* Commutative Ring: In addition to the above if $(R,+,\cdot)$ satisfies the commutative property under '·'

i.e. $\forall a,b \in R, \; a\cdot b = b\cdot a$ then $(R,+,\cdot)$ is said to be Commutative Ring

*Commutative Ring with Unity:

In addition to the above if $(R,+,\cdot)$ satisfies the identity property under multiplication i.e. $\forall a \in R \; \exists 1 \in R \Rightarrow$

$a\cdot 1 = a = 1\cdot a$ then 1 is called as unit element (or) unity and is the multiplicative identity

* Determine whether $(Z, \oplus, \odot)$ is a ring with the binary operations $x \oplus y = x+y-7$ & $x \odot y = x+y-3xy$ $\forall x,y \in Z$

Sol^n: To show $(Z,\oplus)$ is an abelian group:

closure: $\forall x,y \in Z$

$x \oplus y = x+y \rightarrow \in Z$

$(\because x+y \in Z, x+y-7 \in Z)$

Associative: $\forall x,y,z \in Z$

$x \oplus (y \oplus z) = x \oplus (y+z-7)$

$= x+y+z-7-7$

$= (x+y-7)+(z-7)$

$= x \oplus y + (z-7)$

$= x \oplus y \oplus z$

Identity $\forall x \in z, \exists e \in z \Rightarrow x \oplus e = e \oplus x = x$

Consider $x \oplus e = x+e-7 = x$

$e = 7$ which is identity element

Inverse $\forall x \in z \; \exists \; y \in z \ni x+y = e$

$x+y-7 = 7 \quad (\because e = 7)$

$y = 14 - x$

is the inverse of x

Commutative $\forall x, y \in z$

$x \oplus y = y \oplus z$

Consider $x \oplus y = x+y-7$

$= y+x-7$

$= y \oplus x$

$\therefore (z, \oplus)$ is an abelian

→ To show $(z, \odot)$ is associative:

Let $x, y, z \in z$

Consider $x \odot (y \odot z) = x \odot (y+z-3yz)$

$= x+y+z-3yz-3x(y+z-3yz)$

$= x+y+z-3(xy+yz+zx-3xyz)$

$(x \odot y) \odot z = (x+y-3xy) \odot z$

$= x+y-3xy+z-3(x+y-3xy)z$

$= x+y+z-3(xy+yz+zx-3xyz)$

$\therefore x \odot (y \odot z) = (x \odot y) \odot z$

* To show $(z, \oplus, \odot)$ is distributive:

Consider $x \odot (y \oplus z) = x \odot (y+z-7)$

$= x+(y+z-7)-3x(y+z-7)$

$= 2x+y+z-3xy-3xz-7$

Now $(x \odot y) \oplus (x \odot z)$

$= (x+y-3xy) \oplus (x+z-3xz)$

$= x+y-3xy+x+z-3xz-7$

$= 2x+y+z-3xy-3xz-7$

So if $a \neq 0$, $x \odot (y \oplus z)$

$\neq (x \odot y) \oplus (x \odot z)$

Distributive fails

$\therefore (z, \oplus, \odot)$ is not a ring

* Zero divisors of a ring:

If 'R' is a ring and $a \neq 0, b \neq 0 \in R$ such that $ab = 0$ then a & b are the divisors of '0' (zero divisors). In particular 'a' is the left divisor and 'b' is the right divisor.

* Integral Domain:

A Ring with atleast 2 elements is called an Integral domain if it

(i) is commutative (ii) has unit element (iii) is without zero divisors i.e. $ab = 0$

$\Rightarrow$ either $a = 0$ (or) $b = 0$

Ex:

1) The ring of integers $(z, +, \cdot)$ is an integral domain since it is commutative ring with unity and $\forall\ a, b \in z$, $ab = 0$ either $a = 0$ & $b = 0$

2) The ring of real numbers $(R, +, \cdot)$ is an integral domain.

3) The ring of even integers $(2z, +, \cdot)$ is not an integral domain; since it doesn't contain the unit element, though if it is without zero divisors.

*Field: A ring 'R' with atleast 2 elements is called a field if it ① is commutative ② has unity and ③ is such that every non-zero element has multiplicative inverse in R

i.e. $(R, +, \cdot)$ is a field if

① $(R, +)$ is an abelian group

② $(R, \cdot)$ is a commutative group with $R = R - \{0\}$

③ if satisfies distributive laws.

i.e. $a(b+c) = ab + ac$

$(b+c)\ a = ba + ca$

Ex: 1) The set '$\mathbb{C}$' of all complex numbers is a field ~~since it is a commutative~~

2) The ring of rational numbers $(Q, +, \cdot)$ is a field since it is a commutative ring with unity and every non-zero

element has a multiplicative inverse

3) The set 'R' of all real numbers is a field

* Theorem:

Prove that every field is an integral domain:

Proof:

Let 'F' be a field

Since a field is a commutative ring with unity, therefore it is enough to prove that this field 'F' has no zero divisors which proves that 'F' is an integral domain

To show 'F' has no zero divisors

Let $a, b \in F$ $a \neq 0$ such that $ab = 0$, we have to prove $b = 0$

Consider $ab = 0$

Premultiply by a^{-1} on both sides

$$(a^{-1})(ab) = a^{-1} \cdot 0$$
$$(a^{-1}a)b = 0$$
$$e \cdot b = 0 \quad (b = 0)$$

Now consider $ab = 0$ & $b \neq 0$

We now prove that $a = 0$

post multiply by b^{-1} on both sides

$$(ab)b^{-1} = 0 \cdot b^{-1}$$
$$a(bb^{-1}) = 0$$
$$a \cdot e = 0$$
$$a = 0$$

$\therefore ab = 0 \Rightarrow a = 0$ or $b = 0$

$\therefore$ A field has no zero divisors.

Hence every field is an integral domain

Note:

The converse of the above property is not true. i.e. "Every integral domain is not a field".

Ex: The Ring of integers is an integral domain but it is not a field.

The only invertible elements are 1 & -1.

*Subring: If $(R, +, \cdot)$ be a ring and A be a non-empty subset of R then $(A, +, \cdot)$ will be called as a subring if $(A, +, \cdot)$ is itself a ring under the same composition of addition and multiplication as in R i.e. $(A, +, \cdot)$ is a subring of $(R, +, \cdot)$ if

(i) $A \neq \phi$

(ii) $(A, +)$ is a subgroup of $(R, +)$

(iii) 'A' is closed under multiplication
i.e. $\forall a, b \in A \Rightarrow a.b \in A$

Note:

Every ring $(R, +, \cdot)$ has 2 subrings $(\{0\}, +, \cdot)$ & $(R, +, \cdot)$ which are called as Improper (or) Trivial subrings of R

Any other subrings of R are called as proper (or) non-trivial subrings

Ex: The ring of integers is a subrings of the ring of rational numbers which is a subring of Real numbers

The ring of even integers is a subring of ring of integers

*Ring Homomorphism:

If $(R, +, \cdot)$ and $(S, \oplus, \odot)$ are 2 rings and $f: R \to S$ is a function such that

$\forall a, b \in R$ ① $f(a+b) = f(a) \oplus f(b)$
and ② $f(a.b) = f(a) \odot f(b)$

then f is said to be a Ring homomorphism
When 'f' is onto then we say that 's' is a homo image of R

Also if $f: R \to S$ is a Ring homomorphism and is one to one and onto then f is called a ring homomorphism

Theorem:

Given a Ring $(R, +, \cdot)$ a non-empty 's' of 'R' is a subring of R iff (i) $\forall a, b \in S$ we have $a+b, ab \in S$ on R
i.e. 's' is closed under '+' & '.'
and (ii) $\forall a \in S, -a \in S$

Proof:

Given $(R, +, \cdot)$ is a Ring

Firstly suppose that 's' is a non-empty subset of 'R' which is a subring of R

We now prove ① & ②

Since 's' is a subring by defn of subring it is clear that it satisfies closure under '+' & additive inverse properties → ① & ② are true.

Conversely, suppose that ① & ② are true.

We now prove that 's' is a subring of R

closure under addition, associative, distributive & commutative under '+' & '.' of a ring are inherited by the elements of 'S'; because they are also elements of R. Now it is enough to show that identity element under '+' exists.

Now $s \neq 0$; so there is an element $a \in S$ by

② $a \in S$

also by ① & above $a + (-a) = 0 \in S$

∴ Hence S is a subring of R