Mod-5. Algebraic structures.

Notations

$N = \{1, 2, 3 \ldots \infty\}$

$W = \{0, 1, 2, 3 \ldots\}$

$I/Z = \{0, \pm 1, \pm 2 \ldots\}$

$Q = \{a/b : a \,\&\, b$ are integers, $b \neq 0\}$

$R = Q \cup$ set of irrationals

$C = \{a + ib : a, b \in R\}$

Binary operation

→ Binary operation $*$ on a set S;

$* : S \times S \rightarrow S$

$*(a, b) = a * b \qquad (a, b) \in S \times S$

→ $+, -, \times$ binary op. on R

$+, \times$ " on N (not '$-$')

→ properties :- closure

Associative

commutative

Algebraic system/structure

A set S together with binary op. $*$

$(S, *)$

① Semigroup – $(S, *)$

- $*$ closure
- $*$ associative

② Monoid – $(M, *, e) / (M, *)$

- $*$ closure
- $*$ associative
- $*$ identity element w.r.t $*$

Note :- Every monoid is a semigroup

$(N, -) \rightarrow$ not semigroup.

$(Z, +)$, $(R, +)$ } monoid.

$(N \cup \{0\}, +) \rightarrow$ monoid

$(N, +) \rightarrow$ not a monoid. $N\{1, \infty$

③ Group. – $(G, *)$

- $*$ closure
- $*$ associativity
- $*$ identity
- $*$ inverse.

Order of a group – $|G|$

Abelian group → Group + commutativity

$(I, +)$ is abelian group.

$*$ composition table (refer note)

4^{th} roots of unity $\rightarrow 1, -1, i, -i\}$

cube roots of unity $\rightarrow 1, \omega, \omega^2$

$*$ $(Z_n, +_n)$ is abelian group

$n \in Z^+ \qquad x +_n y = \frac{x+y}{n}$

$(x+y) \bmod n$

- power
- cyclic monoid

$(M, *, e)$

for any $x \in M$, $x = a^n$ $\quad$ $a \rightarrow$ generator of cyclic monoid.

commutative semigroup/Abelian semigroup

Semigroup + commutativity.

Abelian monoid

monoid + commutative

Note: Every cyclic monoid is abelian

identity w.r.t $+$ → Additive identity – 0

" $\times$ → Multiplicative identity – 1

Subsemigroup

$(S,*)$ → semigroup

$T \subseteq S$, if $(T,*)$ is a subsemigroup of $(S,*)$

Submonoid

$(M,*,e)$ → monoid

$T \subseteq M$, if $(T,*,e)$ is submonoid of $(M,*,e)$

eg: $(Z,+)$ → semigrp
$(Z^+,+)$ → subsemigrp of $(Z,+)$

$(R,\times,1)$ → monoid
$(N,\times,1)$ → submonoid

Note:- Set of idempotent elements of M for any abelian monoid $(M,*)$ forms a submonoid

Note: $(N,+,0)$ is an infinite cyclic monoid.

⇒ Properties - group.
1. Identity of G is unique
2. Inverse of each element of G is unique
3. cancellation law holds good
   * left cancellation property
   * right cancellation "
4. for any $a,b \in G$, $(a*b)^{-1} = b^{-1} * a^{-1}$.
5. $\langle G,*\rangle$ cannot have an idempotent element except Identity element

Cyclic group $(G,*)$

for any $x \in G$, $x = a^n$

Note:- cyclic group is abelian

eg: $(Z_m, +_m)$ is cyclic group

Subgroup.

$(G,*)$ → group

$H \subseteq G$, if $(H,*)$ → group then it is the subgroup of $(G,*)$

Direct product of groups

$(G,\circ)$ and $(H,*)$ ⇒ groups

binary operation $\circ$ on $G \times H$

$(G \times H, \circ)$ ⇒ group of direct product of G and H

$(g_1,h_1) \circ (g_2,h_2) = (g_1 \circ g_2, h_1 * h_2)$

$g_1, g_2 \in G$ $h_1, h_2 \in H$

Functions

one-one, onto,

Homomorphism

$(X,\circ)$ and $(Y,*)$ → 2 algebraic systems

$f: X \to Y$ is homomorphism from $(X,\circ)$ to $(Y,*)$ if for $a,b \in X$, we have, $f(a \circ b) = f(a) * f(b)$

$f: X \to Y$ be a homomorphism

1. If $f: X \to Y$ is onto, f is epimorphism
2. If $f: x \to y$ is one-one, f is monomorphism
3. If $f: X \to Y$ is one-one & onto, f is isomorphism.

Semigroup homomorphism

$(S, *)$, and $(T, \Delta) \Rightarrow$ 2 semigrp

$g: S \to T$ for any elements $a, b \in S \Rightarrow g(a*b) = g(a) \Delta g(b)$

Monoid homomorphism

$(M, *, e_M)$ and $(T, \Delta, e_T) \Rightarrow$ 2 monoids.

$g: M \to T$ for any elements $a, b \in M \Rightarrow g(a*b) = g(a) \Delta g(b)$

$g(e_M) = e_T$

Homomorphism of groups

$(G, *)$ and $(T, \Delta) \Rightarrow$ 2 groups.

$g: G \to T$ for any $a, b \in G \Rightarrow g(a*b) = g(a) \Delta g(b)$

Note:- Every cyclic group of order n is isomorphic to group $(Z_n, +_n)$

Note:- Every subgroup of a cyclic group is cyclic

cosets

H is a subgrp of G, for each $a \in G$, set $aH = \{ah / h \in H\}$ is left coset of H in G

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

Lagrange's theorem

Order of a subgroup of a finite group divides order of group.