Unit 4

Group Theory

1. Algebraic Systems : a system consisting of a set S one or more n-ary operations

Properties of Algebraic Systems

Let $\{S, *, \oplus\}$ be an algebraic system, $*$ & $\oplus$ are binary operations ons.

(1) Closure Property

$a, b \in S \Rightarrow a * b \in S$

(2) Associativity

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

(3) Commutativity

$a, b \in S \Rightarrow a * b = b * a$

(4) Identity Element

$a * e = e * a = a$

(5) Inverse Element

$a * a^{-1} = a^{-1} * a = e$

(6) Distributivity

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

(7) Cancellation

$a * b = a * c \Rightarrow b = c$ (Left cancellation)

$b * a = c * a \Rightarrow b = c$ (Right cancellation)

(8) Idempotent Element

$a * a = a$

* Homomorphism

If $\{x, \bullet\}$, $\{y, *\}$ are 2 algebraic systems,

where $\bullet, *$ are n-ary operators,

then $g(x_1 \bullet x_2) = g(x_1) * g(x_2)$

epimorphism: $g: \{x, \bullet\} \to \{y, *\}$ is onto

monomorphism: is one-one

isomorphism: both one-one & onto

endomorphism: $y \subseteq x$

automorphism: $x = y$

* Group

Let G be a non empty set and * a binary op on it.

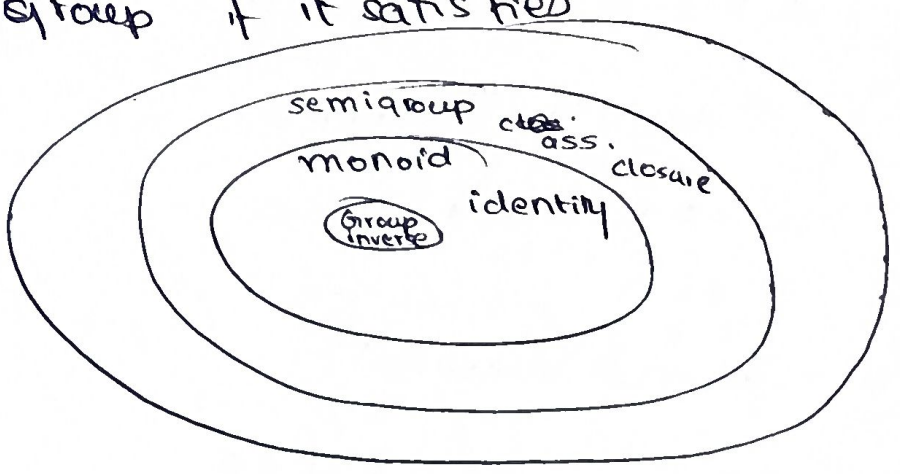
Then $(G, *)$ is said to be a group if it satisfies

(i) closure

(ii) associative

(iii) identity

(iv) inverse



* Semi-Group: satisfies closure & associative property

* Monoid: satisfies closure, associativity and identity

* Abelian group: A group that satisfies commutativity as well.

* Sub-group: A non-empty subset H of a group is a subgroup of G, if $a, b \in H \Rightarrow ab^{-1} \in H$.

Properties of a Group

(1) The inverse element of a group is unique.

Proof :

Let $(G, *)$ be a group

Let $a \in G$ and $e \in G$, where e is the identity element of G.

Let a_1^{-1} and a_2^{-1} be 2 different inverses of the same element a.

Then, $a * a_1^{-1} = a_1^{-1} * a = e$ — (1)

$a * a_2^{-1} = a_2^{-1} * a = e$ — (2)

Consider :

$a_1^{-1} = a_1^{-1} * e$ $\quad (a * e = a)$

$= e * a_1^{-1}$ — (3)

from (2), $e = a_2^{-1} * a$

(3) becomes : $a_1^{-1} = (a_2^{-1} * a) * a_1^{-1}$

using associative property

$a_1^{-1} = a_2^{-1} * (a * a_1^{-1})$

$a_1^{-1} = a_2^{-1} * e$

$\boxed{a_1^{-1} = a_2^{-1}}$

$\boxed{a * a^{-1} = e}$

$\boxed{a^{-1} * e = a^{-1}}$

⇒ This means that the inverse of an element in a group is always unique.

(2) The identity element of a group is unique.

Let $(G, *)$ be a group

Let there be 2 identity elements e_1 & e_2.

Since e_2 is an identity element and $e_1 \in G$

$$e_1 * e_2 = e_1 \quad -(1)$$

Since e_1 is an identity element and $e_2 \in G$

$$e_2 * e_1 = e_2 \quad -(2)$$

from (1), (2)

$$e_1 * e_2 = e_2 * e_1 = e_1 = e_2$$

$$\Rightarrow \boxed{e_1 = e_2}$$

∴ The identity element of a group is unique.

(3) The cancellation laws are true in a group

Let $(G, *)$ be a group.

Let $a, b, c \in G$

To prove: $a * b = a * c \Rightarrow b = c$ Left Cancellation

$b * a = c * a \Rightarrow b = c$ Right Cancellation

(i) $a * b = a * c \Rightarrow b = c$

Multiplying on both sides by a^{-1}

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

by the associative rule

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

$$e * b = e * c \Rightarrow b = c$$

(ii) $b * a = c * a \Rightarrow b = c$

Post multiplying on both sides by a^{-1}

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

using associativity

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

$b * e = c * e$

$\Rightarrow \boxed{b = c}$

(4) (X) Prove that $(a * b)^{-1} = b^{-1} * a^{-1}$ for any $a, b \in G$.

To prove that $(a * b)^{-1} = b^{-1} * a^{-1}$, it is enough to prove that

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

using associativity

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

$a * e * a^{-1}$

$a * a^{-1}$

$= e$

(5) In a group $(a^{-1})^{-1} = a$

Let $(G, *)$ be a group

Let a be an element, and let a^{-1} be its inverse.

e is the identity element

$a * a^{-1} = e$ or $a^{-1} * a = e$

multiply by $(a^{-1})^{-1}$ on both sides

$$\left((a^{-1})^{-1} * a^{-1} \right) * a$$

$$e * a$$

$$= a$$

(6) For any group a, if $a^2 = e$, with $a \neq e$, then G is an abelion group. (or)

If every element of a group is its own inverse than G is abelion. Is the converse true?

Ans. Let $(G, *)$ be a group

if $a, b \in G$, then $(a * b) \in G$

given that $a = a^{-1}$ and $b = b^{-1}$

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

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

$$= b * a$$

$\Rightarrow a * b = b * a$.

the commutative property is true

$\therefore$ an abelion group

The converse need not be true since $(\mathbb{Z}, +)$ is an abelian group. However, no element other element in G is its own inverse.

* If $\{G, *\}$ is an Abelion group, p.t

$(a*b)^n = a^n * b^n$, $\forall a, b \in G$, where n is a +ve integer.

Ans. Since $\{G, *\}$ is an abelion group,

$a * b = b * a$

Proof using Mathematical Induction

for $n = 1$

LHS $a * b$

RHS $= a' * b' = a * b$

$P(1)$ is true.

assume that $P(k)$ is true.

i.e $(a*b)^k = a^k * b^k$

To prove: $P(k+1)$ is true

i.e $(a*b)^{k+1} = a^{k+1} * b^{k+1}$

$$\text{LHS} = (a*b)^{k+1}$$

$$= (a*b)^k * (a*b)$$

$$= a^k * b^k * (a*b)$$

$$= (a * a^k) * (b * b^k)$$

$$= a^{k+1} * b^{k+1}$$

Hence, by induction, the result is true for all +ve integer values of n

* The intersection of 2 subgroups of a group G is also a subgroup.

G is a group

Ans. Consider 2 subgroups H_1 and H_2.

To prove: $H_1 \cap H_2$ is a subgroup of G

let $a, b \in H_1 \cap H_2$

$\Rightarrow a, b \in H_1 \;, a, b \in H_2$

The necessary & sufficient conditions for a subgroup are.

$a * b^{-1} \in H$

here $a * b^{-1} \in H_1$ and $a * b^{-1} \in H_2$

$\Rightarrow a * b^{-1} \in H_1 \cap H_2$

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

* The union of 2 subgroups need not be a subgroup

Consider $H_1 = \{x : x = 2n, n \in Z\} = \{0, \pm 2, \pm 4 \ldots\}$

$H_2 : \{x : x = 3n, n \in Z\} = \{0, \pm 3, \pm 6 \ldots\}$

consider $2 \in H_1$

$3 \in H_2$

however $2 + 3 = 5 \notin H_1 \cup H_2$

hence proved

condition to be a subgroup: $H_1 \subseteq H_2$

or $H_2 \subseteq H_1$

Homomorphism

$$f(a * b) = f(a) \Delta f(b)$$

Theorem 1: If e is the identity of $\langle G, * \rangle$, p.t $f(e) = e'$, where e' is the identity of $\langle G', \Delta \rangle$

Consider an element $a \in G$.

$f(a)$ belongs to G' (f is a group homomorphism)

Consider $f(a) \Delta e'$

$= f(a)$ {e' is the id element in G'}

$= f(a * e)$

$= f(a) \Delta f(e)$

$f(a) \Delta e' = f(a) \Delta f(e)$

using left cancellation

$$\boxed{e' = f(e)}$$

Theorem 2: $f(a^{-1}) = [f(a)]^{-1}$

Since G is a group

$a \in G$

$a^{-1} \in G$

$a * a^{-1} = a^{-1} * a = e$

$f(e) = e'$

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

$e' = f(a) \Delta f(a^{-1})$

also consider

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

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

Theorem 3: $f(G)$ is a subgroup of G'.

Let a', b' belong to $f(G)$

$\Rightarrow f(a') = a$ and $f(b') = b$

condition for a subgroup : $a * b^{-1} \in H$

Consider $a' \Delta (b')^{-1}$

$= f(a) \Delta [f(b)]^{-1}$

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

$= \in G$

For any $a', b' \in f(G)$

$a' \Delta (b')^{-1} \in f(G)$

$f(G)$ is a subgroup of G'

* **Kernel of Homomorphism**

If $f: G \to G'$ is a group homomorphism from $\{G, *\}$ to $\{G', \Delta\}$, then the set of elements mapped to e' is called the kernel of homomorphism.

Theorem: The kernel of a homomorphism f from a group $\{G, *\}$ to another group $\{G', \Delta\}$ is a subgroup of $\{G, *\}$

Proof $f(e) = e'$

$e \in \ker f()$

Let $a, b \in \ker(f)$

To prove: $a * b^{-1} \in \ker(f)$

$$f(a) = e' \qquad f(b) = e'$$

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

$$= f(a) \Delta \{f(b)\}^{-1}$$

$$= e' \Delta (e')^{-1}$$

$$= e'$$

$\therefore \quad a * b^{-1} \in \ker(f)$

$\Rightarrow$ $\ker(f)$ is a subgroup of $\{G, *\}$

For eg. $f : (Z, +) \to (Z, +)$ defined by $f(x) = 2x$

The $\ker(f) = \{0\}$

$f : (R^+, .) \to (R^+, .)$ defined by $f(x) = \{x\}$.

$\ker\{f\} \Rightarrow \quad \{1\}$