UNIT - 4

Algebraic Structure

Algebraic System:-

A non empty set G together with one (or) more n- ary operations say * (Binary) is called Algebraic system It is denoted by $(G, *)$

Notations:-

1) N: Set of all Natural numbers. $\{1, 2, 3 \ldots \infty\}$
2) W: Set of all whole numbers $\{0, 1, 2, 3 \ldots \infty\}$
3) Z: Set of all integers $\{-\infty, \ldots -3, -2, -1, 0, 1, \ldots \infty\}$
4) Q: set of rational numbers.

   Eg: A number which is in the form of $\frac{a}{b}$, $b \neq 0$

5) C: set of All complex number

   Eg: A number which is in the form of $a+ib$, $a, b \in R$

6) R: set of all real number (All come under Real number)

* Operations:-

1) Unary operation:

   It is an operator which operates single element

   Eg: LCM & GCD

2) Binary operation:

It is an operator which operates using two elements

Eg: Add, Sub, Mult, Div, GCD, LCM.....

Properties of Binary operations:-

Let the binary operation be $* : G \times G \to G$ then the following property exists

1. closure Property:

Let A, B follows $\in$ G, then $a * b = c \in G$

2. Associative property:

Let $A, B, C \in G$, then $a * b * c = A * (b * c) \forall a, b, c \in G$

3. Identity element:

Let $A \in G$, then $a * e = e * a = a$

4. Inverse element:

Let $A, e \in G$, then $a * a^{-1} = a^{-1} * A = e \forall a, e \in G$.

5. Commutative Property:

Let $A, B. \in G$, then $\underset{a}{a} * \underset{b}{b} = b * a \forall a, b \in G$

Semi Group:-

A not empty set S together with

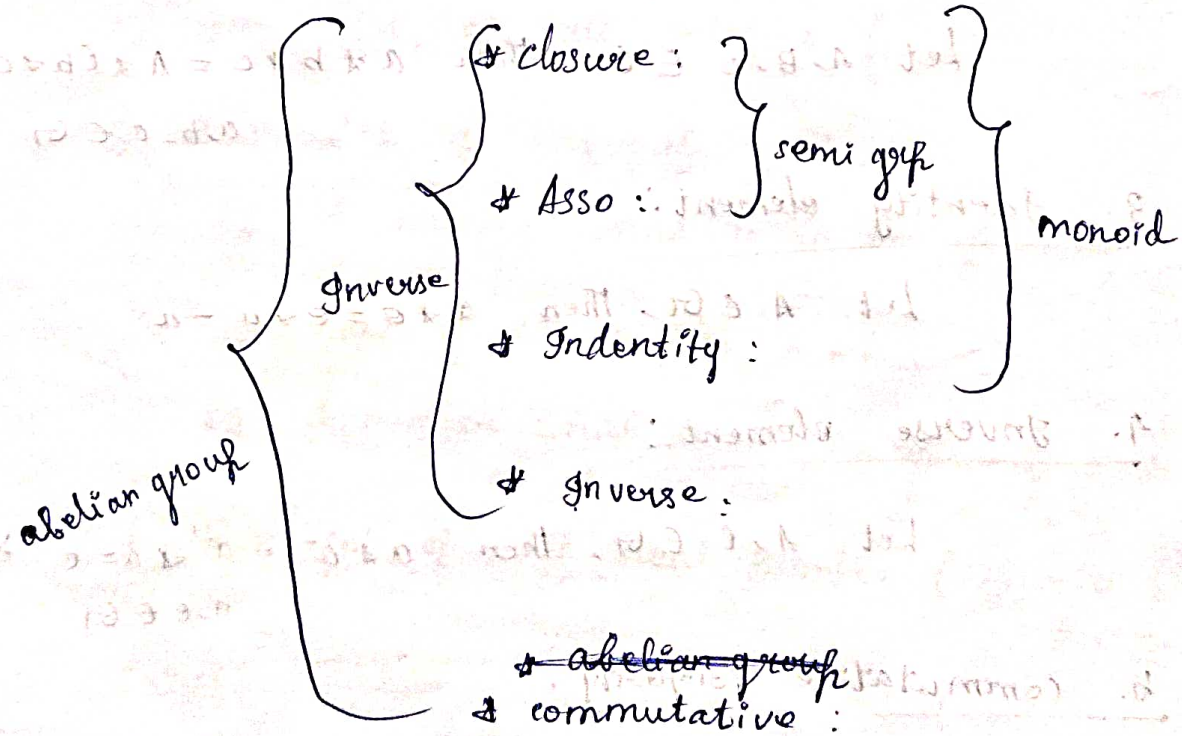
the binary operation $*$ satisfying the following Properties

1. closure property
2. Associative property
3. is called a semi group and it is denoted by $(S, *)$

(am)

Monoid :-

A semi group $(S, *)$ with an identity element with respect to $*$ is called Monoid and it is denoted by $(M, *)$.



Note:

1. the additive identity is always zero (0)
2. the Multiplicative identity is always one (1)

3 the additive inverse of 'a' is '-a'.

4. the Multiplicative inverse of 'a' is 'a^{-1}'.

(1) verify $(N, +)$ is a Monoid.

Let N, + represents set of all natural numbers with additive operator. we have to verify the following properties namely.

1. closure
2. Associative
3. Identity

i. closure property

Let $a, b \in N$, then

now, $a + b = c, c \in N$.

∴ closure Property satisfies.

ii. Associative Property.

Let $a, b, c \in N$,

$(a+b)+c = a+(b+c)$ is true.

∴ Associative Property satisfies.

iii. Identity Property.

we know that. the additive identity is zero but zero doesn't belongs to ~~one~~ $\notin N$

∴ identity element doesn't exist

∴ $(N, +)$ is not a Monoid.

(2) Verify $(E, +)$ is a Monoid.

i) closure property

Let $a, b \in E$, then.

Let $(E, +)$ represent set of all even number with additive operator. we have to verify the following Property namely

1. closure property
2. Associative Property
3. Identity property

i) closure property

Let $a, b \in E$, then

not $a + b = c$, $c \in E$

$\therefore$ closure property satisfy

ii) Associative Property

Let $a, b, c \in E$,

$(a+b)+c = a+(b+c)$ is true

$\therefore$ Associative Property satisfy

iii) Identity element

we know that the additive Identity is zo

but $0 \notin F$

$\therefore$ Identity element doesn't exist

$\therefore (F, +)$ is not a Monoid.

(cyclic) Monoid:

A Monoid $(M, *)$ is said to be cyclic if every element of M is of the form (a^n), where $a \in M$ and n is an integer

Sm (1) Every cyclic Monoid is commutative

Sol:

Let $(M, *)$ be a Monoid

Let $x, y \in M$ now, $x = a^n$, $y = a^m$, $a \in M$, $n, m \in Z$

since M is cyclic we need verify $(M, *)$ is commutative.

That is

(i.e) $x * y = y * x$

LHS

$$x * y$$
$$= a^n \cdot a^m$$
$$= a^{n+m}$$
$$= a^{m+n}$$
$$= a^m \cdot a^n$$
$$= y * x.$$

$\therefore$ LHS = RHS.

$\therefore$ Commutative Property satisfy

$\therefore (m, *)$ is commutative.

① Let $a, b \in G_1$ and $*$ is defined as $a * b = a + b + ab$. verify $(G_1, *)$ is abelian

Sol:

Let $a, b \in G_1$ and $*$ is defined as $a * b = a + b + ab$

To verify $(G_1, *)$ is an abelian we need to verify the following properties namely

1) closure
2) Associative
3) existence of identity element
4) " inverse element
5) commutative

i) closure:

Let $a, b \in G_1$

$a * b = a + b + ab \in G_1$

$\therefore$ closure Property satisfy.

ii) Associative.

Let $a, b, c \in G_1$

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

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

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

$\therefore$ LHS = RHS.

$\therefore$ Asso Property satisfied

iii) Identity element

Let $a \in G$, $a * e = a$

$$a + e + ae = a$$

$$e + ae = 0$$

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

$$e = \frac{0}{1+a}$$

$$\boxed{e = 0 \in G}$$

iv) Inverse element

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

$$a + a^{-1} + aa^{-1} = 0$$

$$a + a^{-1}(1+a) = 0$$

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

$$\boxed{a^{-1} = \frac{-a}{1+a}}$$

V) commutative

Let $a, b \in G$, $a * b = b * a$

LHS:

$$= a * b$$

$$= a + b + ab$$

$$= b + a + ab$$

$$= b + a + ba$$

$$= b * a$$

$$= RHS$$

$\therefore$ LHS = RHS

$\therefore$ commutative property satisfied

$\therefore$ $(G, *)$ is abelian.

(2) Let $(a, b) \in G_1$ and $*$ is defined as $a * b = a+b+2ab$. , verify $(G, *)$ is abilian

Sol:

closure Let $a, b \in G_1$ and $*$ is defined as

$a * b = a+b+2ab$.

To verify $(G_1, *)$ is an Abelian we need to verify the following properties namely

1. closure
2. Associative
3. Identity
4. inverse
5. Commutative

1. closure.

Let $a, b \in G_1$.

$a * b = a+b+2ab \in G_1$

$\therefore$ closure Property satisfied.

2. Associative

Let $a, b, c \in G_1$

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

$(a+b+2ab) * c = a * (b+c+2bc)$

$a+b+2ab+c+2ac+2bc+4abc = a+b+c+2bc+2ab+2ac+4abc$

$\therefore$ LHS $\neq$ RHS.

$\therefore$ Associative property satisfied.

3. Identity.

Let $a \in G$, $a * e = a$

$$a + e + 2ae = a$$

$$e + 2ae = 0$$

$$e(1 + 2a) = 0$$

$$e = \frac{0}{1+2a}$$

$$\boxed{e = 0}$$

iv) inverse

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

$$a + a^{-1} + 2aa^{-1} = 0$$

$$a^{-1} + 2aa^{-1} = -a$$

$$a^{-1}(1 + 2a) = -a$$

$$\boxed{a^{-1} = \frac{-a}{1+2a}}$$

v) Commutative

Let $a, b \in G$ then $a * b = b * a$

$$a * b$$
$$= a + b + 2ab$$
$$= b + a + 2ab$$
$$= b + a + 2ba$$
$$= b * a$$

$\therefore$ LHS = RHS.

$\therefore$ commutative properties satisfied.

$\therefore$ $(G, *)$ is abelian.

tqabc

Model

Show that $\{1,3,7,9\}$ is an abilian group under Multiplication Modulo 10.

sol:

cayley table

$\cdot_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$9 \times 9 = 81$ ↓ above 10

$81/10$ $10\overline{)81}$ 8, 80, 1

$10\overline{)91}$

Given:

$\{1,3,7,9\}$ under the operator multiplycation Modulo 10 we need to Prove the set is abilian.

the following Properties should be verified namely

1. closure Property
2. associative Property
3. identity element
4. inverse element
5. commutative Property

1. closure Property:

since the elements present in the cayley table are from the given set.

∴ closure Property satisfy

2. Associative Property

to verify $(a \cdot_{10} b) \cdot_{10} c = a \cdot_{10} (b \cdot_{10} c)$

$(3 \cdot_{10} 7) \cdot_{10} 9 = 3 \cdot_{10} (7 \cdot_{10} 9)$

$(1) \cdot_{10} 9 = 3 \cdot_{10} (3)$

$9 = 9.$ ∴ Associative Property verify

3) Identity element

$a * e = a$

from the cayley table we observed the '1' is the identity element

4. Inverse element

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

The inverse of 1 is 1

The inverse of 3 is 7

The inverse of 7 is 3

The inverse of 9 is 9

∴ inverse element exist

5. Commutative Property

To verify Commutative Property

(i.e) $a \cdot_{10} b = b \cdot_{10} a$

$3 \cdot_{10} 9 = 9 \cdot_{10} 3$

$7 = 7$.

∴ commutative property satisfies

since the given set under the operation Multiplication Modulo 10 satisfy all the above properties

∴ It is abilian (commutative = abilian

Verify Z_4 is a commutative group under addition Modulo.

Sol:

given set $Z_4 = \{0, 1, 2, 3\}$

under the operation addition Modulo

(i.e) $(Z_4, +_4)$

To verify $(Z_4, +_4)$ is the commutative group (Abelian) we have to verify the following properties namely.

1. closure
2. Asso
3. Identity
4. Inverse
5. Commutative

Cayley table

$+_4$	0	1	2	3 ↓
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3 →	3	0	1	2

↓ above 4

$3+3=6$

$6-4=2$

i) closure

ii) ~~Associative~~ Property

The elements present in the caley table belongs to the set Z_4

∴ closure Property verify

ii) Associative Property

Let $a, b, c \in Z_4$

To verify $(a +_4 b) +_4 c = a +_4 (b +_4 c)$.

∴ Associative property satisfy

iii) identity element

From the cayley table it is observed that '0' is the Additive Modulo identity

iv) Inverse element

The inverse of 0 is 0

The inverse of 1 is 3

The inverse of 2 is 2

The inverse of 3 is 1

∴ inverse element exist

v- commutative Property

let $A, B \in Z_4$

To verify $a +_4 b = b +_4 a$

∴ commutative Property satisfy

since $(Z_4, +_4)$ satisfy all the above property

∴ $Z_4 +_4$ is a commutative group (abilian)

Verify Z_7 is a commutative group under addition Modulo

Property 1:

The identity element of a group is unique

Proof:

Let $(G, *)$ be a group. Let e_1 and e_2 be the two identity element in G.

Suppose e_1 be the identity element then,

$$e_2 * e_1 = e_1 * e_2 = e_2 \quad \text{(case 1)}.$$

Suppose e_2 be the identity element then,

$$e_1 * e_2 = e_2 * e_1 = e_1 \quad \text{(case 2)}$$

From (1) & (2) $e_1 = e_2$ Therefore identity element is unique.

Property 2:

The inverse element of a group is unique

Proof:

Let $(G, *)$ be a group. Let a_1 follow G and e be the identity element in G.

Let a_1^{-1} and a_2^{-1} be the two different inverse of the same element.

By definition, we get $a_1 * a_1^{-1} = a_1^{-1} * a_1 = e \rightarrow (1)$

$a_1 * a_2^{-1} = a_2^{-1} * a_1 = e \rightarrow (2)$

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

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

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

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

element inverse identity

$\therefore$ Inverse element is unique.

Property:

Let G be a group. if a, b follows G then $(a * b)^{-1} = b^{-1} * a^{-1}$

(or) the inverse of Product of two elements is equal to the

Product of their inverse in reverse order

Let A, B follows G_1 then $A * B$ follows G_1

To Prove that $(A * B)^{-1} = B^{-1} * a^{-1}$

It is enough to Prove $(a * b) * (b^{-1} * a^{-1}) = e$.

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

LHS :

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

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

$a * e * a^{-1}$ ~~Identity~~ Inverse

$(a * e) * a^{-1}$ Asso

$a * a^{-1}$ Identity

e Inverse

$= RHS$.

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

$\therefore (a * b)^{-1} = b^{-1} * a^{-1} \quad \forall a, b \in G_1$.

gm

Property :

Let $(G, *)$ is an abilian group then show that $(a * b)^n = a^n * b^n$. $\forall a, b \in G$., where n is a positive integer

Proof :

Let as we improve by mathematical induction Let as assume

$P(n) : (a * b)^n = a^n * b^n \quad \forall n \in Z$

Step : 1 :

To prove P(1) is true.

Put n = 1

$P(1) : (a * b)^1 = a^1 * b^1$

$\therefore P(1)$ is true

Step 2: Let us assume P(k) is true.

(i.e) $P(k): (a*b)^k = a^k * b^k \; \forall k \in Z$

Step 3:

To prove P(k+1) is true

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

LHS:

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

$= (a*b)^k * (a*b)^1$

$= (a^k * b^k) * (a*b)$ (by step 2)

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

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

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

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

$=$ RHS.

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

$\therefore P(k+1)$ is true

$\therefore P(n)$ is true for $n \in Z$

Sub group

Definition:

Let $(G,*)$ be a group. $(H,*)$ is said to be a sub group of $(G,*)$, if $(a*b^{-1} \in H)$

Theorem: statement

The necessary and ~~state~~ sufficient condition that a non empty subset H of a group G, to be a sub group is $a*b^{-1} \in H$

Proof:

Necessary condition:

Let us assume that H is a sub group of G since H itself a group then $a, b \in H \Rightarrow a * b \in H$

(closure Property)

Since $b \in H \Rightarrow b^{-1} \in H$

$\therefore$ for $a, b \in H \rightarrow a, b^{-1} \in H$

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

Sufficient Part;

Let $a * b^{-1} \in H \; \forall \; a, b \in H$

Now, we have to prove H is a subgroup of G.

i) identity

Let $a \in H \Rightarrow a^{-1} \in H$

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

$\Rightarrow e \in H$

Hence identity element $e \in H$

ii) inverse:

Let $a^{-1} e \in H$.

$\Rightarrow e * a^{-1} \in H$

$\Rightarrow a^{-1} \in H$.

$\therefore$ Every element 'a' of H has its inverse 'a-1' belongs to H

iii) closure:

Let $b \in H$

$\Rightarrow b^{-1} \in H$.

$\therefore$ Let $a, b \in H \Rightarrow a, b^{-1} \in H$

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

$\Rightarrow a * b \in H$

$\therefore$ H is a subgroup of G

Theorem :

The intersection of two subgroup of a group is also a subgroup.

Proof :

Since H_1 and H_2 are sub group of G.

$\therefore H_1 \cap H_2 \neq \phi$

Since H_1 is a sub group.

$\Rightarrow a, b \in H_1$

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

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

Since H_2 is a sub group.

$\Rightarrow a, b \in H_2$

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

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

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

$\therefore H_1 \cap H_2$ is a subgroup of G_1.

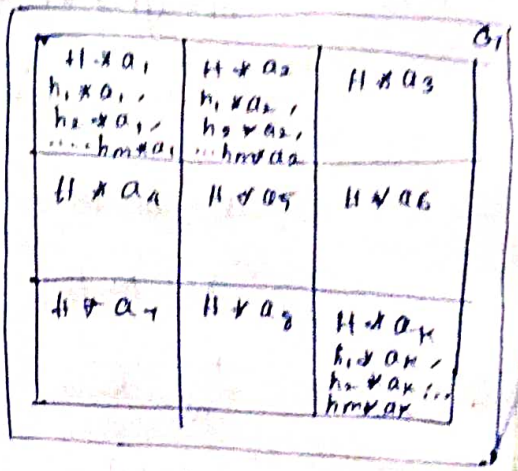
Coset :

Let $(H, *)$ be a sub group of $(G, *)$ for any $a \in G$, the left coset of H is denoted by $(a * H)$ then the set $a * H = \{a * h / a \in G, h \in H\}$.

(a : sub grp, h : element)

Similarly the right coset of H is denoted by $H * a$ then the set $H * a = \{h * a / h \in H, a \in G\}$

Lagrange Theorem



~~Proof~~

Statement: Let G be a finite group of order n and H be any sub group of G. Then order of H divides order of G

(i.e) $o(H) / o(G)$

(or)

$o(G) / o(H)$

Proof: Let $(G, *)$ be a group of order n

(i.e) $o(G) = n$

Let $(H, *)$ be any sub group of G whos order is 'm'.

(i.e) $o(H) = m$

Let $(h_1, h_2 \cdots h_m)$ be the 'm' different (distinct) elements of H.

The right coset $(H * a)$ of H in G is difined by $(H * a) = \{h_1 * a, h_2 * a \cdots h_m * a\}$ where $a \in G$

since there exist a one to one correspondence b/w the elements of H & $H * a$, the elements of $H * a$ are distinct

Hence each right coset of H in G has 'm' distinct element.

The number of distinct right coset of H in G is finite (say k).

The union of k distinct right coset of H in G is equal to G.

Let these k distinct right cosets are $H * a_1$, $H * a_2$, ... $H * a_k$.

$G = (H * a_1) \cup (H * a_2) \cdots \cup (H * a_k)$ (set)

$o(G) = o(H * a_1) + o(H * a_2) + \cdots + o(H * a_k)$ (element in set)

$n = m.m \ldots\ldots m$ (K times)

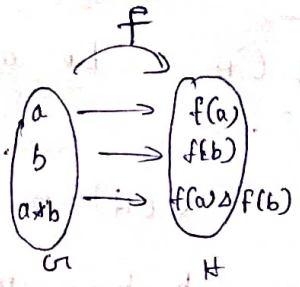
$n = m.K$

$\frac{n}{m} = K$

$\frac{o(G)}{o(H)} = K$.

where K is any positive integer

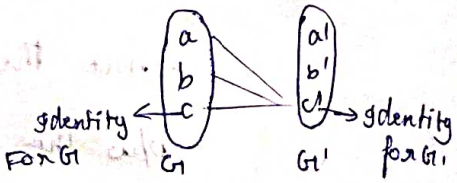
$\therefore o(H) / o(G)$



Homo morphism

Let $(G, *)$ and (H, Δ) be any two groups, a mapping $f: G \to H$ is said to be Homomorphism if $f(a * b) = f(a) \Delta f(b) \quad \forall a, b \in G$

Kernal of a Homorphism



Let $f: G \to G'$ be a group homo. morphism. The set of element of G which are mapped into e' (identity element in G') is called the kernal of f and it is denoted by Ker (f).

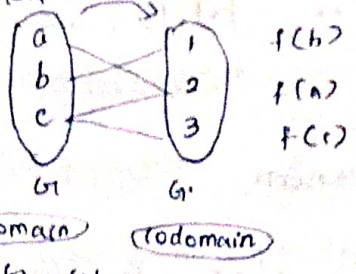
$$\text{Ker}(f) = \{ x \in G / f(x) = e' \}$$

normal subgroup

Let H be a sub group of G under star then H is said to be a normal sub group of G for

every element $x \in G$ (group) and for $h \in H$ (subgroup) then $x * h * x^{-1} \in H$

Basics of functions



1. one to one (injective)

for each element in domain it should have a unique image in codomain eg: $f(c) = 3$ (for a element 'c' in domain the image is '3' in codomain)

2. on to (subjective)

for every element in co-domain the preimage exist in domain and need not to be unique

3. Bijective :

If a function is injective and subjective then it is called as bijective

Theorem:

Let $f : (G, *) \to (G', *)$ be a homomorphism

The prove that $\ker(f)$ is a normal subgroup

Proof:

we know that $\ker(f) = \{ x \in G / f(x) = e' \}$

$\therefore$ $\ker(f)$ is non empty in G

Let H be a normal sub-Group of G which contains the elements $pqp^{-1} \in H$, where $q \in H$, $p \in G$.

Now $f(p * q * p^{-1}) = f(p) * f(q) * f(p^{-1})$ homo.

$= e' * e' * e'$ ker (f)

$= (e' * e') * e'$ (Asso)

$= e' * e'$ (Iden)

conclusion:

$\therefore$ ker(f) is a normal sub group of G

Theorem:

Let $f:(G,*)\to(G',*)$ be a homomorphism then prove that ker(f) is ~~non empty~~ sub group

Proof:

We know that $\ker(f)=\{x\in G / f(x)=e'\}$

$\therefore$ ker(f) is non empty in G

Let H be a sub group of G which contains the element $a*b^{-1}$ ~~$\in H$~~

now,

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

$= e'*e'$ (ker f)

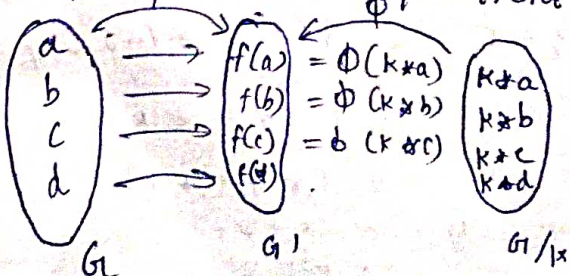
$f(a*b^{-1}) = e'$ (Idem)

$\therefore$ kernal of f is a sub group

Fundamental Theorem on homomorphism of groups

Statement:

every homomorphic image of a group G is isomorphic to some quotient group of G



Proof:

Let f be a homomorphic function from $G \to G'$ $(f : G \to G')$

Let G' be the homo image of the group G. The f is a homo of G onto G'.

Let K be the kernal of this homo clearly K is a normal subgroup of G.

To Prove that $G/K \overset{\sim}{=} G'$ (isomorphic)

(i.e) - $\frac{G}{K}$ is isomorphism to G'

Let for $a \in G$, then $f(a) \in G'$ and $K * a \in G/K$

now consider the mapping $\phi : G/K \to G$.

such that $\phi(K * a) = f(a) \forall a \in G$

i) ϕ is well defined

we have

$K * a = K * b$

$\Rightarrow a * b^{-1} \in K$ e' - identity in G'

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

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

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

$f(a) = f(b)$

$\phi(K * a) = \phi(K * b)$

$\therefore \phi$ is well defined

ii) ϕ is one - one

we know that,

$\phi(K * a) = \phi(K * b)$

$f(a) = f(b)$

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

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

$= f(e)$

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

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

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

$K * a = K * b$

$\therefore \phi$ is one-one

iii) ϕ is onto

Let $y \in G'$ be any element

Then,

$y = f(a)$, $a \in G$ [f is onto G']

Now $K * a \in G/K$

$\Rightarrow \phi(K * a) = f(a) = y$

$\therefore \phi$ is onto.

iv) ϕ is a bijective homomorphism

Now $\phi(K * a * K * b) = \phi(K * a * b)$.

$= f(a * b)$

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

$= \phi(K * a) * \phi(K * b)$

$\therefore \phi$ is a bijective homomorphism

$\therefore \phi$ is an isomorphism b/w G/K to G'

$G/K \cong G'$

Rings

* An Algebraic system $(R, +, \cdot)$ is called a ring if the binary operations $(+, \cdot)$ satisfies the following conditions.

Associative
i) $(a+b)+c = a+(b+c)$ $\forall$ $a, b, c \in R$

* There exist an element $0 \in R$ called zero element such Identity that $a+0 = 0+a = a$ $\forall$ $a \in R$

Inverse
* $a + (-a) = (-a)+a = 0$, $\forall$ $a, 0 \in R$

commutative
* $a+b = b+a$ $\forall$ $a, b \in R$

Asso
* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall$ $a, b, c \in R$.

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

distributive
ii) ~~$(a+b) \cdot c$~~ $(a \cdot b) + c = (a+c) \cdot (b+c)$ $\forall$ $a, b, c \in R$

In other words R is an abelian group under addition with properties (5, 6) then R is a Ring

Eg: $(R, +, \cdot)$

$(Z, +, \cdot)$

$(\mathbb{Z}, +, \cdot)$

Commutative Ring

The ring $(R, +, \cdot)$ is called a commutative ring if $a \cdot b = b \cdot a$ $\forall$ $a, b \in R$

* (Im)

Zero devices

$x, y \neq 0$

$x \cdot y = 0$.

3. $5 = 0$

If a and b are the two non-zero elements of a ring R such that $a.b = 0$, then a and b are called as 0 devices.

Eg: $3 \cdot_5 5 = 0$ $\quad 3 \times 5 = 15$, $15/5 = 0$.

$7 \cdot_2 2 = 0$

Integral domain:

A commutative ring $(R, +, \cdot)$ with identity element and without zero devices is called integral Domain

Eg: $7 \cdot_4 2 = 2 \neq 0$ $\quad 7 \times 2 = 14$, $14/4 = 2$

Field

A commutative ring with identity $(R, +, \cdot)$ is called a field.

If every non zero element has a multiplicative inverse

Eg: $(R, +, \cdot)$ and $(Q, +, \cdot)$ is a field but $(Z, +, \cdot)$ is not a field

Problem:

To check $(Z_4, +_4, \cdot_4)$ is a ring (or) verify that the set $Z_4 = \{0, 1, 2, 3\}$ is a commutative ring with respect to binary operators ($+_4$ and $\cdot_4$).

(distri, asso, commutative, abilian)

Sol:

Given

$(Z_4, +_4, \cdot_4)$

To verify it is a commutative ring then it

should satisfies the following properties.

first
- i) Associative under (+4)
- ii) Additive identity (+4)
- iii) Additive inverse (+4)
- iv) commutative property under Addition (+4)
- v) Associative property under (·4)
- vi) Distributive Property under (+4 over ·4)

vii) commutative property under (·4)

cayley table

+4	0	1	2	3
0	0+0 = 0	0+1 = 1	0+2 = 2	0+3 = 3 → less than 4
1	1	2	3	1+3 = 0 → 4 greater than 4 (or) = 4−4
2	2	3	0	2+3 = 1 → 5−4 = 1
3	3	0	1	2

·4	0	1	2	3
0	0×0 = 0	0×1 = 0	0×2 = 0	0×3 = 0
1	0	1	2	1×3 = 3
2	0	2	0	2×3 = 2 → 6/4
3	0	3	2	1

To verify Associative property under +4

i) Let $a, b, c \in Z_4$

Then $(a +_4 b) +_4 c = a +_4 (b +_4 c)$

Eg: $1, 2, 3, \in Z_4$

$(1 +_4 2) +_4 3 = 1 +_4 (2 +_4 3)$

$3 +_4 3 = 1 +_4 (1)$

$2 = 2$

∴ Asso Property satisfies under +4.

ii) Existence of Additive identity.

From the cayley table we observed that zero is the

iii) Existance of inverse element

The Additive inverse of 0 is 0

The Additive inverse of 1 is 3

The Additive inverse of 2 is 2

The Additive inverse of 3 is 1

∴ inverse element exist for all the elements in Z_4 under $+_4$

iv) To verify commutative property under $+_4$)

Let $a, b \in Z_4$

Then $a +_4 b = b +_4 a$

Eg: $2 +_4 1 = 1 +_4 2$

$2 = 2$

∴ commutative satisfies under $+_4$

v) To verify Associative Property under $(\cdot_4)$

Let $a, b, c \in Z_4$.

To verify :

$(a \cdot_4 b) \cdot_4 c = a \cdot_4 (b \cdot_4 c)$

Eg: $(1 \cdot_4 2) \cdot_4 3 = 1 \cdot_4 (2 \cdot_4 3)$

$2 \cdot_4 3 = 1 \cdot_4 (2)$

$2 = 2$

∴ Asso Property satisfies under $(\cdot_4)$

vi) To verify Distributive Property ($+_4$ over $\cdot_4$)

Let $a, b, c \in Z_4$

Then $(a +_4 b) \cdot_4 c = (a \cdot_4 c) +_4 (b \cdot_4 c)$

Eg: $(1 +_4 3) \cdot_4 2 = (1 \cdot_4 2) +_4 (3 \cdot_4 2)$

$(0) \cdot_4 2 = 2 +_4 (2)$

$0 = 0.$

$\therefore$ distributive satisfy ($+_4$ over $\cdot_4$)

vii) To verify commutative property under ($\cdot_4$)

Let $a, b \in Z_4$

Then verify $a \cdot_4 b = b \cdot_4 a$

$2 \cdot_4 3 = 3 \cdot_4 2$

$2 = 2$

$\therefore$ commutative property satisfies for ($\cdot_4$).

Since All the above properties are verify and exist

$\therefore (Z_4, +_4, \cdot_4)$ is a commutative ring.