Sri SAI RAM ENGINEERING COLLEGE
INSTITUTE OF TECHNOLOGY
West Tambaram, Chennai - 44

SAIRAM DIGITAL RESOURCES

YEAR II

SEM III

MA8351

DISCRETE MATHEMATICS

(Common to CSE & IT)

UNIT IV

ALGEBRAIC STRUCTURES

4.4 HOMOMORPHISM AND NORMAL SUBGROUPS

SCIENCE & HUMANITIES

Normal Subgroup:

A subgroup $(H,*)$ of a group $(G,*)$ is said to be a normal subgroup, if for every $a \in G$ where $aH = Ha$.

The Necessary and Sufficient condition for a subgroup H of a group G is a normal subgroup:

A subgroup H of a group G is a normal subgroup if and only if

$a * h * a^{-1} \in H \;\forall\; a \in G \;\&\; h \in H$.

Proof:

Let H be a normal subgroup of G.

By Definition: $aH = Ha \;\; \forall\; a \in G$

Now, $h * a \in Ha = aH$

Pre-multiply by a^{-1},

$h*a*a^{-1}=a*h*a^{-1}$,

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

Since $h\in H$,

$\Rightarrow h*e=a*h*a^{-1}\in H\ \forall\ a\in G$.

Conversely, assume $a*h*a^{-1}\in H\ \forall\ a\in G\ \&\ h\in H$,

(i) Let $a*h*a^{-1}\in H$,

$\Rightarrow (a*h*a^{-1})*a\in Ha$

$(a*h)*(a^{-1}*a)\in Ha$,

$(a*h)*e \in Ha$,

$(a*h) \in Ha$.

Since $a*h \in aH$,

$\Rightarrow aH \subseteq Ha$ ......(1)

(ii) Since $a \in G \Rightarrow a^{-1} \in G$

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

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

Post-multiply by a on both sides

$a*(a^{-1}*h*a) \in aH$

$\Rightarrow (a * a^{-1}) * (h * a) \in aH$

$\Rightarrow e * (h * a) \in aH$

$\Rightarrow h * a \in aH$

Since $h * a \in Ha$

$\Rightarrow Ha \subseteq aH \quad ......(2)$

From (i) & (ii),

$\Rightarrow Ha = aH$

Therefore H is a normal subgroup of G.

Theorem:

Intersection of two normal subgroups is again a normal subgroup.

Proof:

- Let G be a group.
- Let the subgroups H_1 and H_2 of G is also a normal subgroup of G.
- Since H_1 is a normal subgroup of G, hence $a*h*a^{-1} \in H_1 \; \forall \; a \in G \;\&\; h \in H_1$.
- Since H_2 is a normal subgroup of G, hence $a*h*a^{-1} \in H_2 \; \forall \; a \in G \;\&\; h \in H_2$.
- Since $a \in H_1$ and $a \in H_2 \Rightarrow a \in H_1 \cap H_2$.

  $a*h*a^{-1} \in H_1$ and $a*h*a^{-1} \in H_2$.

  $\Rightarrow a*h*a^{-1} \in H_1 \cap H_2 \quad \forall\, h \in H_1 \cap H_2 \;\&\; a \in G$
- $\Rightarrow H_1 \cap H_2$ is a normal subgroup of G.

Group Homomorphism:

Let $(G,*)$ and $(G,\oplus)$ be two groups, then mapping $f:G\to G'$ is called Group Homomorphism.

$f(a*b)=f(a)\oplus f(b)$.

Theorem:

If $f:G\to G'$ is a group homomorphism from $(G,*)$, $(G,\oplus)$ then

(i) $f(e)=e'$, $e\in G$ & $e'\in G'$

(i.e) f preserves identity element.

(ii) $f(a^{-1})=(f(a))^{-1}\ \forall a\in G$

(i.e) f preserves identity element.

Proof:

(i) $f(e)=f(e*e)$, since f is homomorphism $f(a*b)=f(a)\oplus f(b)$.

$=f(e)\oplus f(e)$

$\Rightarrow f(e)\oplus f(e)=f(e)$ ......(1)

Since e' is the identity element of G'

$f(e)*e'=f(e)$ ......(2)

Since identity element is unique,

From (1) & (2), we get

$f(e)=e'$.

(ii) $\Rightarrow f(a * a^{-1}) = f(a) \oplus f(a^{-1})$

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

$e' = f(a) \oplus f(a^{-1})$ ......(1) $[\because f(e) = e']$

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

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

$e' = f(a^{-1}) \oplus f(a)$ ......(2)

From (1) & (2),

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

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

Example:

If $S = N \times N$ is a set of all positive integer with operation ' * ' is defined as $(a,b)*(c,d) = (ad + bc, bd)$.

$$f : (S,*) \to (Q,*) \qquad f(a,b) = \frac{a}{b}$$

Prove that f is a semi-group homomorphism.

Solution:

- To Prove: $(S,*)$ is a semi-group.
- Clearly $(S,*)$ satisfies closure property.
- It is enough to verify Associate property.

Associate Law:

(i) $(a,b)*((c,d)*(e,f))$

$=(a,b)*(cf+de,df)$

$=(adf+b(cf+de),bdf)$ ....(1)

(ii) $((a,b)*(c,d))*(e,f)$

$=(ad+bc,bd)*(e,f)$

$=(adf+bcf+bde,bdf)$ ....(2)

Therefore (1)=(2).

To prove: f is homomorphism

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

$$f((a,b)*(c,d))=f(ad+bc,bd)$$

$$=\frac{ad+bc}{bd}$$

$$=\frac{ad}{bd}+\frac{bc}{bd}$$

$$=\frac{a}{b}+\frac{c}{d}$$

$$=f(a,b)+f(c,d).$$

Kernel of Homomorphism:

- Let $(G,*)$, $(G,\oplus)$ be two groups.
- Let $f : G \to G'$ be a homomorphism, then the kernel of f is defines as the set of elements of g which maps to the identity element of G'.

Theorem:

Kernal of f is a normal subgroup.

Proof:

To prove kernel of f is a normal subgroup.

(i.e) $a * h * a^{-1} \in \ker(f) \forall a \in G \;\&\; h \in \ker(f)$

It is enough to prove,

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

Since $h \in \ker(f) \Rightarrow f(h) = e'$

$\Rightarrow f(a * h * a^{-1}) = f(a) \oplus f(h) \oplus f(a^{-1})$ [Since f is homomorphism]

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

$= f(a) \oplus [f(a)]^{-1}$ [Since f preserves inverse]

$= e'$.

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

$\Rightarrow a*h*a^{-1} \in \ker(f)$

Hence proved.

Theorem:

Let $f : h \to a'$ be a group homomorphism, then f is one to one if and only if $\ker(f) = \{e\}$.

Proof:

Let us assume $f \; is \, 1-1$.

$[f \; is \, 1-1 \Rightarrow f(x) = f(y), \; then \; x = y.]$

Let $x, y \in G$

Since $f \; is \, 1-1$,

$f(x) = f(y)$.

To prove: $\ker(f) = \{e\}$.

If $x \in \ker(f)$

$f(x) = e' \quad ....(1)$

We know that $f(e) = e'$ ....(2)

From (1) and (2),

$f(x) = f(e)$

Since $f\ is\ 1-1$

$\Rightarrow x = e$

$\Rightarrow \ker(f) \in \{e\}$

Conversely let us assume $\Rightarrow \ker(f) \in \{e\}$

To prove: $f\ is\ 1-1$

Assume $f(x) = f(y)$

$f(x) * f(y)^{-1} = f(y) \oplus f(y)^{-1}$

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

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

$$\Rightarrow x * y^{-1} \in Ker(f) = \{e\}$$

$$\Rightarrow x * y^{-1} = e$$

$$x * y^{-1} * y = e * y$$

$$x * e = y$$

$$x = y.$$

$$\Rightarrow f \; is \; 1-1.$$

Examples:

Let $f:(R,+)\to(R,\bullet)$ be a mapping defined as $f(a)=2^a\ \forall\ a\in R$. Verify f is homomorphism and also prove that $f\ is\ 1-1$.

Solution:

To prove: $f(a+b)=f(a).f(b)$

Let $a,b\in R$

$\Rightarrow f(a)=2^a$

$\Rightarrow f(b)=2^b$

$\Rightarrow f(a+b)=2^{a+b}=2^a.2^b=f(a).f(b)$.

Therefore f is homomorphism.

To prove: $f\ is\ 1-1$

It is enough to prove,

$\ker(f) \in \{e\}$

Since $e' = 1$

$f(a) = e' = 1$

$2^a = 1$

$\Rightarrow a = 0 = e$

$\Rightarrow \ker(f) = \{0\}$.

Hence $f\ is\ 1-1$.