Equivalence relation on S.

* Reflexive : $a R a \ \forall a \in S$
* Symmetric : $aRb \Rightarrow bRa \ \forall a, b \in S$.
* Transitive : $aRb, bRc \Rightarrow aRc \ \forall a, b, c \in S$.

$[a] = \{x \in S : aRx\}$

i) $[a] = [b]$ or $[a] \cap [b] = \phi$ [empty set]

ii) $\bigcup_{a \in S} [a] = S$.

{1, 2, 3} $/R_2$

$[1] : C_2 \{R, G, O\}$

$[R] \cup [G] \cup [O]$

Lagrange's theorem

Definition (congruence of H) :

G - group. H - subgroup.

$a, b \in G$, $a \equiv b \pmod H \Leftrightarrow ab^{-1} \in H$.

(congruent)

Lemma 1 : The relation $a \equiv b \pmod H$ is an equivalence relation.

Proof :

* Reflexive : $a \equiv a \pmod H \Rightarrow aa^{-1} = e \in H$.
* Symmetric : Assume $a \equiv b \pmod H$ Then $ab^{-1} \in H$.

(It hai inverse. $\therefore (ab^{-1})^{-1}$)

To prove $b \equiv a \pmod H$

$\because$ H is a sub group,

$(ab^{-1})^{-1} \in H$.

$(ab^{-1})^{-1} = (b^{-1})^{-1} a^{-1} = ba^{-1} \in H$.

$= b \equiv a \pmod H$

* Transitive : Assume $a \equiv b \pmod H$ and $b \equiv c \pmod H$

To prove : $a \equiv c \pmod H$

Then $ab^{-1} \in H$ & $bc^{-1} \in H$.

If we multiply both it belongs to H.

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

$= aec^{-1}$

$= ac^{-1} \in H$.

$\therefore a \equiv c \pmod H$

Lemma 2:

$Ha = [a] = \{x \in G : a \equiv x \pmod{H}\}$

Proof:

To prove: (i) $Ha \subseteq [a]$

(ii) $[a] \subseteq Ha$

(i) Let $x \in Ha$

Then $x = ha$ for some $h \in H$.

To prove: $a \equiv x \pmod{H}$

$a \equiv ha \pmod{H}$

$a(ha)^{-1} \in H$

$(a(ha)^{-1})^{-1} \in H$

$(ha)a^{-1} \in H$

$h(aa^{-1}) = he = h \in H$.

$\therefore Ha \subseteq [a]$

$a(ha)^{-1}$

$a(a^{-1}h^{-1})$

$aa^{-1}h^{-1}$

$h^{-1} \in H$

$h \in H$

$a \equiv x \pmod{H} \Rightarrow x \in [a]$

(ii) Let $x \in [a]$

Then $a \equiv x \pmod{H}$

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

$(ax^{-1})^{-1} \in H$;

$xa^{-1} \in H$.

$\Rightarrow xa^{-1} = h$ for some h.

$xa^{-1}a = ha$

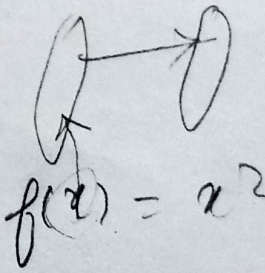
$x = ha$ for some h.

$\Rightarrow x \in Ha$. $\therefore [a] \subseteq Ha$.

Lemma 3:

There exists a one-one correspondence between any two right cosets. i.e $O(Ha) = O(Hb)$

↳ order.



Proof:

Let $f : Ha \to Hb$ be defined by

$f(ha) = hb$.

f is one-one

~~Let $x, y \in G$ and $x \neq y$.~~

~~To prove~~ Let $h_1a, h_2a \in H$

~~$f(x) \neq f(y)$~~ To prove: $f(h_1a) \neq f(h_2a)$

$f(h_1a) = h_1b$

$f(h_2a) = h_2b$

$h_1b \neq h_2b$

$f(h_1a) \neq f(h_2a)$ ∴ f is one-to-one

f is onto

Let $hb \in Hb$

Then there exists $ha \in Ha$

Such that $f(ha) = hb$ ∴ f is onto.

∴ f is bijection. ⇒ $O(Ha) = O(Hb)$

Statement: Let G be a finite group and H be a subgroup of G then $O(H)$ divides $O(G)$

Proof: From lemma 2, $\bigcup_{a \in G} Ha = G$

$$\Rightarrow \sum O(Ha) = O(G)$$

Let K be the no. of distinct right cosets.

then $$\sum_{i=1}^{K} O(Ha) = O(G)$$

$$\Rightarrow K\, O(Ha) = O(G)$$

W.K.T. $O(Ha) = O(H)$

$$\therefore K\, O(H) = O(G)$$

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

What are the possible orders of the sub groups of a group of order 36?

$O(G) = 36$

$O(H) = 1, 2, 3, 4, 6, 9, 12, 18, 36$

Index of G in H, $i_H G$ = no. of distinct right cosets of H in G.

$$= \frac{O(G)}{O(H)}$$

$O(G) = 45$, $O(H) = 5$

$\therefore i_H G = \frac{45}{5} = 9.$

$O(G) = 100$

$O(H) = 25 \quad O(K) = 50.$

$O(H \cap K) = 1, 5, 25.$

$$O(HK) = \frac{O(H) \cdot O(K)}{O(H \cap K)} = \frac{25 \times 50}{1}$$ (not possible)

$HK = \{hk, h \in H, k \in K\}$

$$= \frac{25 \times 50^{10}}{5} = 250 > 100.$$ (not possible)

$$= \frac{25 \times 50}{25} = 50.$$

~~$\therefore O(HK) \geq 50.$~~ $O(H \cap K) = 25.$ $O(HK) = 50.$

Left coset:

$aH = \{ah : h \in H\}$ → left

$Ha = \{ha : h \in H\}$ → right

$aH = Ha \Rightarrow ?$

If $aH = Ha$ then the groups are called as Normal sub groups.

Normal sub groups:

$Na = aN \quad \forall \; a \in G$

$Ng = gN \quad \forall \; g \in G.$

Let G be abelian and N - Sub group.

$Ng = \{ng : n \in N\}$ left coset.

$= \{gn : n \in N\}$ right coset.

$= gN.$

$Ng = gN \quad \forall g \in G.$

∴ Every sub group of a abelian group is normal.

Eg. $(n\mathbb{Z}, +)$ is normal for $(\mathbb{Z}, +)$.

$Ng = gN \quad \forall g \in G.$

$g^{-1}Ng = g^{-1}gN$ (or) $Ngg^{-1} = gNg^{-1}$

$g^{-1}Ng = N$ (or) $N = gNg^{-1}$

$\Rightarrow g^{-1}ng \in N$ (or) $gng^{-1} \in N. \quad \forall g \in G$ $n \in N.$

Eg. $G = \{GL_2(\mathbb{R}), \cdot\}$

$N = \{A \in GL_2(\mathbb{R}) : |A| = 1\}$

We already proved that N is a sub group of G

∴ T.P : N is normal, i.e. $g^{-1}ng \in N$.

Let $A \in G$ and $B \in N$, i.e. $|B| = 1$.

T.P : $ABA^{-1} \in N$. i.e. $|ABA^{-1}| = 1$.

$|ABA^{-1}| = |A|\,|B|\,|A^{-1}|$

$= |A|\,|B|\,\frac{1}{|A|}$

$= |B|$

$= 1.$

∴ N is a normal sub group of G.

$G = \{M_2(R), +\}$

$N = \{A \in M_2(R) : \text{trace of } A = 0\}$.

To prove, N is normal.

∵ the given group is abelian, N is a normal sub group.

$G = \{GL_2(R), \cdot\}$

$N = \{A \in GL_2(R) \mid A = A^T\}$

Let $A \in G$ and $B \in N \Rightarrow B = B^T$.

i.e. $ABA^{-1} = (ABA^{-1})^T$

$(ABA^{-1})^T = (A^{-1})^T B^T A^T$

$= (A^{-1})^T B A^T$

$\neq ABA^{-1}$

∴ The given group is not a normal sub group.

Theorem:

A group G has no proper sub group ⇔ G is cyclic and O(G) = p(prim

Result:

Product of two right cosets of N in G is again a right coset ⇔ N is normal in G.

i.e. $Na\,Nb \overset{①}{=} Nab \Leftrightarrow N$ is normal $\overset{②}{\longrightarrow} Na = aN \quad \forall a \in G$.

② ⇒ ① $(Na)(Nb) = (Na)(bN)$ ∵ N is normal

$= (Nab)N$

$= (ab)(abN)N$

$= abN$

$= Nab$

① ⇒ ② Assume $NaNb = Nab$ $\forall\ a, b \in G$.

To prove: N is normal. i.e $gng^{-1} \in N$.

Consider $gng^{-1} = egng^{-1}$ (N, G, N, G)

$eg \in Ng$ and $ng^{-1} \in Ng^{-1}$

$(eg)(ng^{-1}) = NgNg^{-1} = Ngg^{-1} = Ne = N$

$\therefore gng^{-1} \in N. \Rightarrow$ N is normal.

Quotient group:

$$\frac{G}{N} = \{Na : a \in G\}$$

Recap: If G is a group. For N to be a normal sub group if $gng^{-1} \in N$.

Collection of all right cosets (Na) also forms a group.

$Na \cdot Nb = Nab$

To prove: Center of a group is a normal sub group.

Proof: Let $N = Z(G)$

To prove: $gng^{-1} \in N = Z(G)$ $\forall\ n \in N$ and $g \in G$.

Since, $n \in N = Z(G)$ $ng = gn$.

NOW, $gng^{-1} = ngg^{-1}$

$= ne$

$= n \in N = Z(G)$

Hence proved.

The set $\frac{G}{N} = \{Na : a \in G\}$ // collection of all right cosets

$$O\left(\frac{G}{N}\right) = \frac{O(G)}{O(N)}$$

1, 5, 9, 13, ...

Prove that $\frac{G}{N}$ is a group

↓

quotient group.

Proof: $\frac{G}{N} = \{Na : a \in G\}$

* binary:

product of 2 right cosets is a right coset.

* Associative:

Let $Na, Nb \& Nc \in \frac{G}{N}$

$(NaNb)Nc = Na(NbNc)$

$(Nab)Nc = Na(Nbc)$

$Nabc = Nabc$

* Identity:

$Na\,Ne = Nae = Na.$

* Inverse:

$Na\,Na^{-1} = Ne$

$Naa^{-1} = Ne$

$Ne = Ne.$

$\therefore \frac{G}{N}$ is a group.

$G = (Z, +)$, $N = (4Z, +)$ Determine $\frac{G}{N}$ i.e $\frac{Z}{4Z}$

$\frac{G}{N} : \frac{Z}{4Z} = \{4Z + a \mid a \in Z\}$

As $O(G)$ and $O(N)$ are infinite, it's impossible to find no. of right cosets i.e $\frac{O(G)}{O(N)}$

Use trial and error:

$a = 4Z + 0 = 4Z$

$4Z + 4 = 4Z$

$a = 4Z + 1 = \{1, 5, 9, 13, \ldots$
$-3, -7, -11 \ldots\}$

$a = 4Z + 2 = \{2, 6, 10, \ldots$
$-2, -6, -10 \ldots\}$

$a = 4Z+3 = \{3, 7, 11, 15, \ldots$
$-1, -5, -9, \ldots\}$

For all $a \geq 3$, they can be written as $a = 4R + r$

$r \in [0, 3]$

$4Z + a = 4(Z+R) + r$

$= 4Z + r, \quad 0 \leq r \leq 3$

Thus, $\frac{Z}{4Z}$ has right cosets as $\{4Z, 4Z+1, 4Z+2, 4Z+3\}$

Note: $\frac{Z}{nZ}$ has $\underbrace{\{nZ, nZ+1, nZ+2, \ldots nZ+(n-1)\}}_{n\text{-elements.}}$

$\therefore O\left(\frac{Z}{nZ}\right) = n.$

Consider $G = (Z_{18}, \oplus_8)$ $N = \{0, 6, 12\}$ Find $\frac{G}{N}$

$G = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\}$

$N \oplus_{18} 0 = \{0, 6, 12\}$
$= \{n \oplus_{18} 0, \ n \in N\}$

$N \oplus_{18} 1 = \{1, 7, 13\}$
$N \oplus_{18} 2 = \{2, 8, 14\}$
$N \oplus_{18} 3 = \{3, 9, 15\}$
$N \oplus_{18} 4 = \{4, 10, 16\}$
$N \oplus_{18} 5 = \{5, 11, 17\}$
$N \oplus_{18} 6 = \{6, 12, 18\}$
$N \oplus_{18} 7 = \{7, 13, 19\}$
$N \oplus_{18} 8 = \{8, 14, 20\}$
$N \oplus_{18} 9 = \{9, 15, 21\}$
$N \oplus_{18} 10 = \{10, 16, 22\}$
$N \oplus_{18} 11 = \{11, 17, 23\}$
$N \oplus_{18} 12 = \{12, 18, 24\}$
$N \oplus_{18} 13 = \{13, 19, 25\}$
$N \oplus_{18} 14 = \{14, 20, 26\}$
$N \oplus_{18} 15 = \{15, 21, 27\}$

Thus it could be concluded as

$N \oplus_{18} 1 = N \oplus_{18} 7 = N \oplus_{18} 13$
$N \oplus_{18} 2 = N \oplus_{18} 8 = N \oplus_{18} 14$
$N \oplus_{18} 3 = N \oplus_{18} 9 = N \oplus_{18} 15$
$N \oplus_{18} 4 = N \oplus_{18} 10 = N \oplus_{18} 16$
$N \oplus_{18} 5 = N \oplus_{18} 11 = N \oplus_{18} 17$

$\therefore \frac{G}{N} = \{N \oplus_{18} 0, N \oplus_{18} 1, N \oplus_{18} 2, N \oplus_{18} 3, N \oplus_{18} 4, N \oplus_{18} 5\}$

$O\left(\frac{G}{N}\right) = \frac{O(G)}{O(N)} = \frac{18}{3} = 6.$

1) $G = (Z_{18}, \oplus_{18})$

(i) $N = \{0, 2, 4, 6, 8, 12, 14, 16, 10\}$

$$O\left(\frac{G}{N}\right) = \frac{O(G)}{O(N)} = \frac{18}{9} = 2.$$

$$\frac{G}{N} = \{N \oplus_{18} 0,\ N \oplus_{18} 1\}$$

(ii) $N = \{0, 3, 6, 9, 12, 15\}$

$$O\left(\frac{G}{N}\right) = \frac{O(G)}{O(N)} = \frac{18}{6} = 3.$$

$$\frac{G}{N} = \{N \oplus_{18} 0,\ N \oplus_{18} 1,\ N \oplus_{18} 2\}$$

Group Homomorphism

Let G $(G, *)$ and $\bar{G}$ $(\bar{G}, \bar{*})$ be two groups and $f: G \to \bar{G}$ be a function, f is said to be a group homomorphism if

$$f(a * b) = f(a) \bar{*} f(b) \quad \forall\ a, b \in G.$$

G & $\bar{G}$ can be equal

Example 1. Let $G = (Z, +)$ & $\bar{G} = (Z, +)$

$f: G \to \bar{G}$.

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

LHS: $f(a * b) = f(a + b)$

$= 2(a + b)$

$= 2a + 2b$

RHS: $f(a) \bar{*} f(b) = f(a) + f(b)$

$= 2a + 2b$

$\therefore$ f is homomorphism.

Example 2. Let $G = (R, +)$ & $\bar{G} = (R - \{0\}, \cdot)$

$f: G \to \bar{G}$ defined by $f(x) = 2^x$

LHS: $f(a * b) = f(a + b)$

$= 2^{a+b}$

$= 2^a \cdot 2^b$

RHS: $f(a) \bar{*} f(b) = 2^a \cdot 2^b$

$\therefore$ f is homomorphism.

Example 3. $f : (R, +) \to (R, +)$ by $f(x) = x + 1$.

LHS: $f(a * b) = f(a + b)$

$= a + b + 1$

RHS: $f(a) \bar{*} f(b) = a + 1 + b + 1$

$= a + b + 2$

$\therefore$ f is not homomorphism.

Example 4. $f : (R - \{0\}, \cdot) \to (C - \{0\}, \cdot)$ by $f(x) = x + ix$

LHS: $f(a * b) = f(a \times b)$

$= ab + iab$

RHS: $f(a) \bar{*} f(b) = (a + ia) \times (b + ib)$

$= (ab - ab) + i(ab + ba) = 2abi$

$\therefore$ f is not a homomorphism.

Example 5. $f : (R, +) \to (C, +)$ by $f(x) = x + ix$.

LHS: $f(a * b) = f(a + b)$

$= (a + b) + i(a + b)$

RHS: $f(a) \bar{*} f(b) = a + ia + b + ib$.

$= (a + b) + i(a + b)$

$\therefore$ f is homomorphism.

Example 6. $f : (C - \{0\}, \cdot) \to (R - \{0\}, \cdot)$ by $f(x) = |x|$

LHS: $f(a * b) = f(a \cdot b)$

$= |a \cdot b| = |ab|$

RHS: $f(a) \bar{*} f(b) = |a| \cdot |b|$

$= |a||b|$

$= |ab|$

$\therefore$ f is homomorphism.