Mathematical foundation

>> Coset' and Lagrange's theorem

Let G be a group and H be a subgroup of G.

Define a relation $a \rho b$ if and only if $a^{-1} b \in H$

$\forall a, b \in H$.

Then ρ is an equivalence relation

$a^{-1}x = h$
$a(a^{-1}x) = ah$
$= (aa^{-1})x = ah$
$\Rightarrow ex = ah$
$= x = ah$

$[a]_\rho = \{x \in G : a \rho x \text{ holds}\} = \{x \in G : a^{-1}x \in H\}$

$= \{x \in G : x = ah \text{ for some } h \in H\} = aH$

$aH = \{ah : h \in H\}$

$\downarrow$

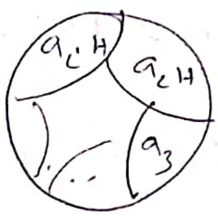
Left coset of H in G.

$a \rho b \Leftrightarrow ab^{-1} \in H$

$[a]_\rho = Ha = \{ha : h \in H\}$

$\downarrow$

Right coset of H in G.



$G = \bigcup_{a_i \in G} a_i H$ $\quad a_i H = a_j H$

$a_i H \cap a_j H = \phi$

$L_H = \{aH : a \in G\}$. $\quad |L_H| = |R_H|$

$R_H = \{Ha : a \in G\}$

$\phi : L_H \to R_H$

$\phi(ah) = ha \quad \forall\, ah \in aH.$

$[G : H] = (aH) = |H|$.

index of H in G.

Lagrange's Theorem

Let G be a <u>finite</u> group and H be a subgroup of G. Then $|H|$ divides $|G|$ where $|H|$ is order of H.

Since G is finite, let $G = \{a_1, a_2, \ldots, a_n\}$ then G has finite no of n cosets $a_1H, a_2H, \ldots, a_nH$

Let G has a distinct left cosset such that

$a_1H, a_2H, \ldots, a_rH$. (r distinct coset)

Then $[G : H] = r$ Now $G = \cup a_iH \quad i = 1, 2, \ldots r.$

Then $|G| = |a_1H| + |a_2H| + \cdots + |a_rH|.$

$= |H| + |H| + \cdots + |H| = r|H|$

$= [G : H]\,|H|$ (proved).

Converse of Lagranges theorem (CLT)

Let G be a finite group of order n. then corresponding to every divisor of m of n then there exists a subgroup of order m.

For cyclic group converse of lagrange's theorem is always true. For commutative group CLT also holds

Normal subgroup and Quotient Group

Let G be a group and H be a subgroup of G.

Then $aH \neq Ha$ for $a \in G$.

but if $aH = Ha$ then H is a normal subgroup.

for commutative group every subgroup is a normal subgroup. but in non commutative group every subgroup is not normal subgroup.

S_n

A_n is a normal subgroup of S_n.

Let G be a group and H be a subgroup of G such that $[G: H]=2$

then H is a normal subgroup of G.

$SL(n, \mathbb{R})$ is a normal subgroup of $GL(n, \mathbb{R})$

$aH = Ha \ \forall a \in G$

Necessary and sufficient condition

Let G be a group and H be a subgroup of G then H is a normal subgroup of G if and only if $ghg^{-1} \in H \ \forall g \in G$ and $h \in H$.

Let $A \in GL(n, \mathbb{R})$

$B \in SL(n, \mathbb{R})$

$ABA^{-1} \in SL(n, \mathbb{R})$

$GL(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$

$SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : \det A = 1\}$

$\det(ABA^{-1})$

$= \det A . \det B . \det A^{-1}$

$= \det A . (\det A^{-1})$

$= \det A \times \frac{1}{\det A}$

$= 1$

Let G be a group then the centre of G is denoted by $Z(G)$ and is defined by $Z(G) = \{ a \in G : ab = ba \ \forall b \in G\}$

If H is commutative $Z(G) = G$.

$Z(G) \leq G$. $Z(G)$ is a subgroup of G.

$(S, *)$

Quotient Set of a set

Let $S \neq \phi$ ~~set~~ be a set.

Define an equivalence relation ρ on S.

$$[a]_\rho = \{x \in S : a \rho x \text{ holds}\}$$

$S/\rho = \{[a]_\rho : a \in S\}$ $[a]_\rho = \{x \in S : a \rho x \text{ holds}\}$

ρ → congruence relation.

$a \rho b \Rightarrow a * c \ \rho \ b * c$

$c * a \ \rho \ c * b \quad \forall \ c \in G$.

Let H be a normal subgroup of G.

$a \rho b \Leftrightarrow a^{-1} b \in H$

$G/H = \{aH : a \in G\}$

$(G/H, *)$ → Quotient group of G. $(aH) * (bH) = (ab)H$

Group $\quad$ $\forall aH_c$

Let G be a group and H be a normal subgroup of G. Consider $G/H = \{aH : a \in G\}$ Define a binary relation $*$ on G/H by $(aH) * (bH)$ $= (ab)H$ $\forall$ $aH, bH \in G/H$. Then $(G/H, *)$ forms a group. This group is called a quotient group of G.