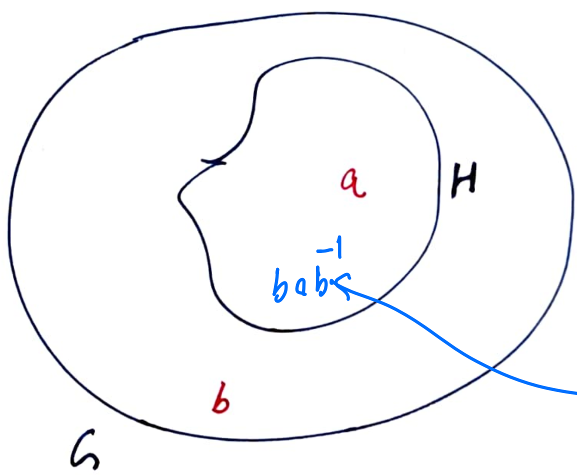
Lecture 13 – Introduction to Group Theory

February 04, 2022

Normal Subgroup. A subgroup H of a group G is called a **normal subgroup** if for every $a \in H$, and every $b \in G$ $bab^{-1} \in H$.

[bab^{-1} : conjugate of a by b]



$\forall\, a \in H$ and $\forall\, b \in G$

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

One of the aim to define normal subgroup is to define quotient structure [G/H].

Examples of normal subgroup.

1. $\varphi : G \longrightarrow G'$ group homomorphism, then

$H = \ker\varphi = \{ a \in G \text{ such that } \varphi(a) = 1_{G'} \}$ is a normal subgroup.

Proof. Let $a \in \overset{H}{\ker\varphi}$ and $b \in G$, then we should show that $bab^{-1} \in \ker\varphi$.

$\left[\text{i.e. } \varphi(bab^{-1}) = 1_{G'} \right]$

Artin Exercise

$$\boxed{\begin{aligned}&\varphi(g_1 \cdots g_k)\\ &= \varphi(g_1) \cdots \varphi(g_k)\end{aligned}}$$

$$\begin{aligned}\varphi(bab^{-1}) &= \varphi(b)\varphi(a)\varphi(b^{-1}) \\ &= \varphi(b) \cdot 1_{G'} \cdot \underset{\varphi(b)^{-1}}{\varphi(b^{-1})} \\ &= 1_{G'}\end{aligned}$$

[Use associativity,
$\varphi(b^{-1}) = \varphi(b)^{-1}$

(i) Define $\varphi : GL_n(\mathbb{R}) \longrightarrow (\mathbb{R} - \{0\}, \cdot)$ group homomorphism

$A \longmapsto \det(A)$

$$\ker\varphi = \{ A \in GL_n(\mathbb{R}) \text{ such that } \det(A) = 1 \} = SL_n(\mathbb{R}).$$

Hence $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$.

(ii) Any subgroup H of an abelian group G is normal.

Let $a \in H$ and for any $b \in G$, write

$$bab^{-1} = abb^{-1} \qquad [\text{Since } ba = ab]$$
$$= a \in H$$

(iii) Define $\varphi : (\mathbb{Z}, +) \longrightarrow G$

$$n \longmapsto \varphi(n) = a^n \text{ ; where } a \text{ is some fixed element in } G.$$

$\ker \varphi = \{ n \in \mathbb{Z} \text{ such that } a^n = 1_G \}$ is a normal subgroup of G.

Definition. Let G be a group. The center of a group is

$$Z(G) = \{ b \in G \text{ such that } ba = ab \text{ for all } a \in G \}$$

Exercise. $Z(G)$ is a subgroup of G.

Exercise. $Z(G)$ is a normal subgroup of G.

Proof. Let $H = Z(G)$, then $a \in H$ and for any $b \in G$,

$$\underbrace{ba}b^{-1} = abb^{-1}$$
$$= a \in H = Z(G)$$

(i) Does $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in Z(GL_2(\mathbb{R}))$?

(ii) Does $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in Z(GL_2(\mathbb{R}))$?

(iii) Does $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in Z(GL_2(\mathbb{R}))$?

Relation. A relation on a non-empty set A is a subset R of $A \times A$, and we write $a \sim b$ if $(a, b) \in R$.

denote it by symbol $\sim$ tilde

Equivalence relation. Let $X \neq \phi$ and $\sim$ a relation on X. Then $\sim$ is an equivalence relation if it is

Reflexive, symmetric and transitive.

Equivalence class. Let $\sim$ be an equivalence relation on a non-empty set X. The equivalence class of $a \in X$ is

$$[a] = \{ b \in X \text{ such that } b \sim a \}.$$

Another notation $\;\bar{a}$ $\quad$ [Artin notation C_a]

Exercise. (Artin Exercise, Section 5)

1. Is the intersection of two equivalence relations an equivalence relation? True / False

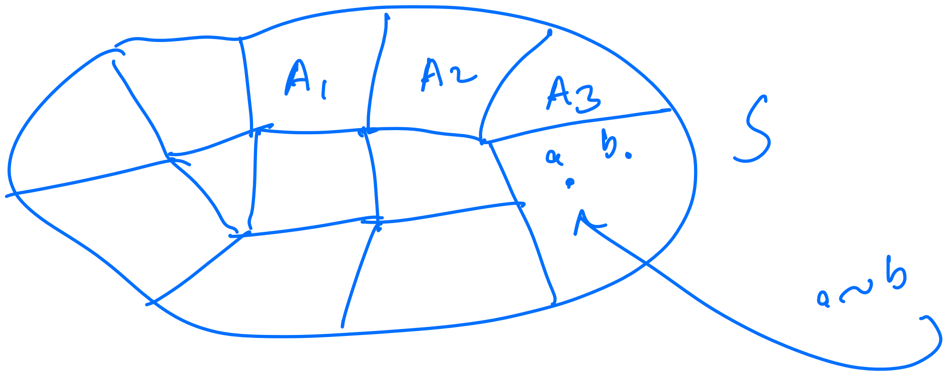
2. Is the union of two equivalence relations an equivalence relation? True / False

3. Determine the number of equivalence relations on a set $\{1,2,3,4,5\}$. Think about this!

Partition of a set. A partition $\mathcal{P}$ of a set S is a collection of subsets A_i, $i \in I$ such that

(i) $\bigcup A_i = S$ [A_i covers S]

(ii) If $i \neq j$, then $A_i \cap A_j = \phi$ [A_i's are pairwise disjoint]



A partition $\wp$ of S is a collection of subsets A_i s.t.

$$\bigcup A_i = S \quad \text{and} \quad A_i \cap A_j = \phi \text{ if } i \neq j$$

$\Uparrow$ $\Downarrow$

Given a partition $\wp$ on S, define equivalence relation on S

$a \sim b$ if $a, b \in A_i$ for some i (some subset of the partition)

$\Leftarrow$

Given an equivalence relation define a partition $\wp$ on S, the subset containing a [say $a \in A_i$],

$\xleftrightarrow[\text{correspondence}]{1-1}$

$A_i = \{ b \in S \text{ such that } b \sim a \}$

[Exercise. $\sim$ is an equivalence relation]

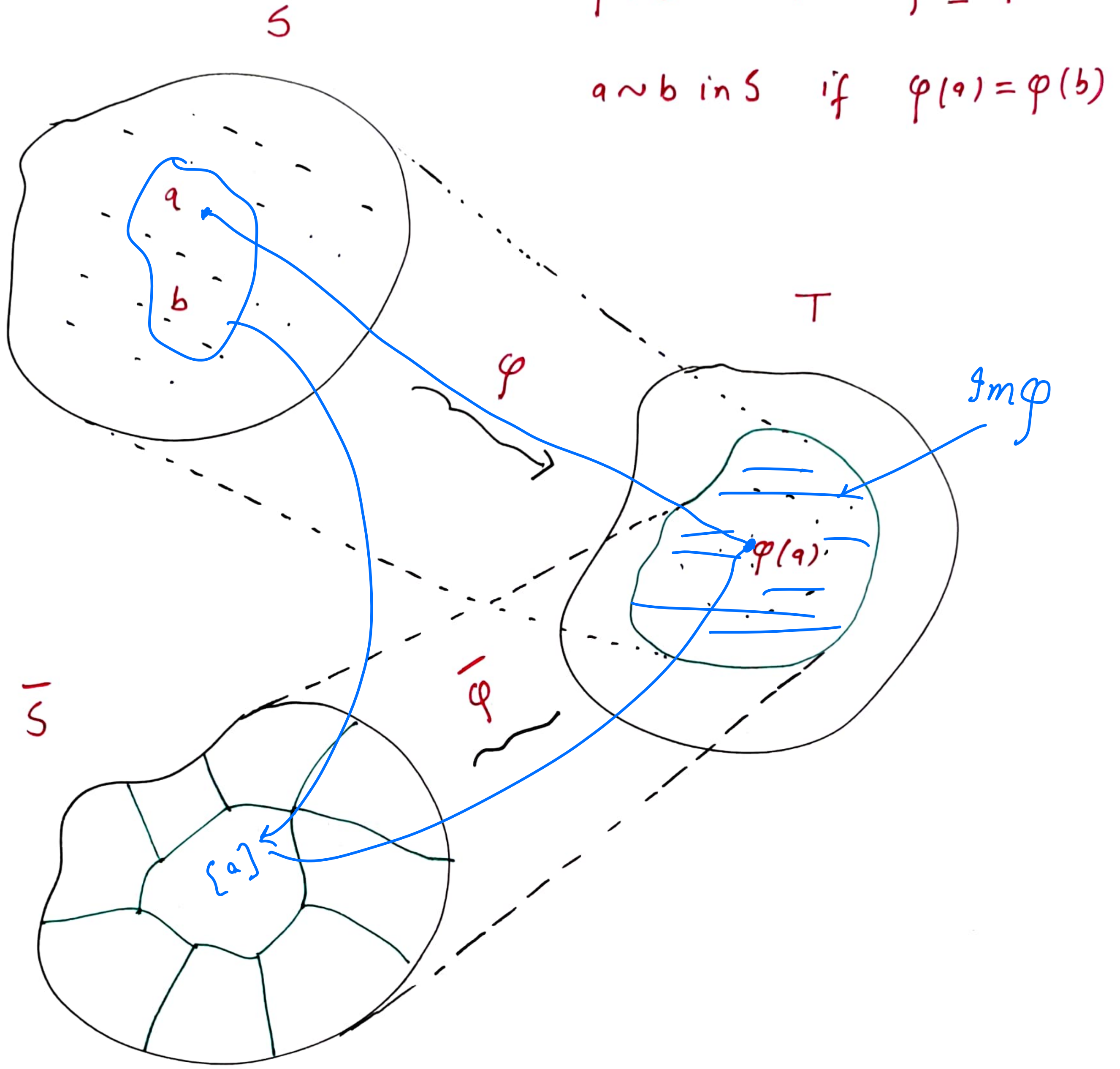
Equivalence relation determined by the map :

Let S and T be sets. A map $\varphi : S \longrightarrow T$ defines an equivalence relation on the domain S by $\varphi(S) \subseteq T$

$a \sim b$ in S if $\varphi(a) = \varphi(b)$.

$$\varphi : S \longrightarrow \operatorname{Im}\varphi \subseteq T$$

$a \sim b$ in S if $\varphi(a) = \varphi(b)$



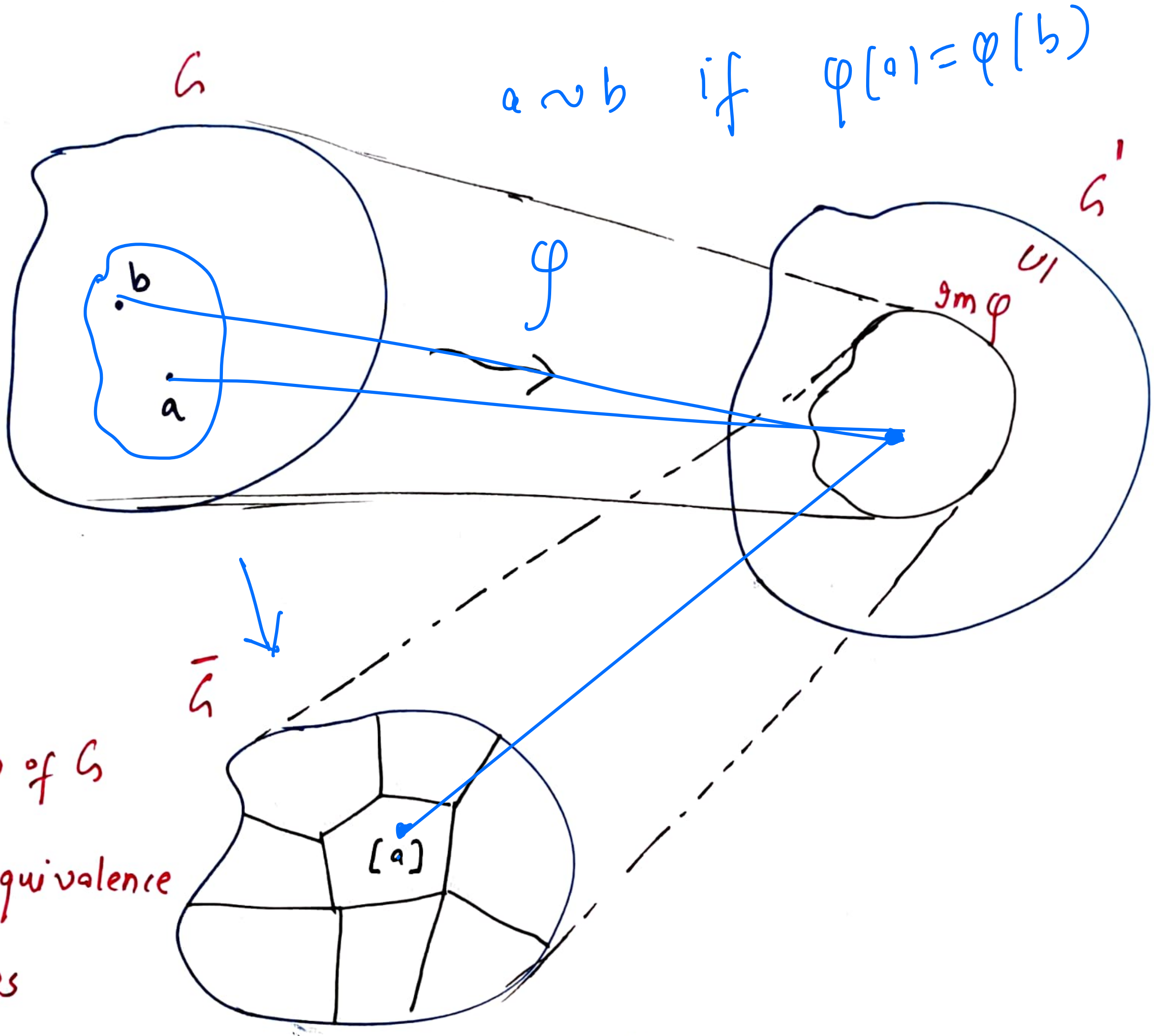
$\bar{S}$ forms partition of S by equivalence classes

$$\bar{\varphi} : \bar{S} \longrightarrow \operatorname{Im}\varphi$$

$$[a] \longmapsto \varphi(a)$$

Exercise. Let $x, y \in S$, then either $[x] \cap [y] = \phi$ or $[x] = [y]$.

Let $\varphi : G \longrightarrow G'$ be a group homomorphism.



Partition of G into equivalence classes

$\left[\, a \sim b \text{ if } \varphi(a) = \varphi(b) \,\right]$

$$\varphi : G \longrightarrow \operatorname{Im}\varphi \subseteq G'$$
$$a \longmapsto \varphi(a)$$

$$\bar{\varphi} : \bar{G} \longrightarrow \operatorname{Im}\varphi$$
$$[a] \longmapsto \varphi(a)$$

$$[a] = \{ b \in G \text{ such that } b \sim a \}$$

Proposition. Let $\varphi : G \longrightarrow G'$ be a group homomorphism with $\ker\varphi$. Let $a, b \in G$. Then

[$a \sim b$ if $\varphi(a) = \varphi(b)$]

$$\varphi(a) = \varphi(b) \iff b = an \text{ for some } n \in \ker\varphi$$

$$\iff a^{-1}b \in \ker\varphi.$$

Proof.

($\Rightarrow$) Assume that $\varphi(a) = \varphi(b)$. Then

$$\varphi(a)^{-1} \cdot \varphi(a) = \varphi(a)^{-1}\varphi(b)$$

$$\Rightarrow \quad 1_{G'} = \varphi(a^{-1})\varphi(b) \qquad [\because \varphi(a)^{-1} = \varphi(a^{-1})]$$

$$1_{G'} = \varphi(a^{-1}b)$$

$$\Rightarrow \quad a^{-1}b \in \ker\varphi$$

$\Leftarrow$ Assume $b = an$ for some $n \in \ker\varphi$

Then $\varphi(b) = \varphi(an) = \varphi(a)\varphi(n) = \varphi(a) \cdot 1_{G'}$

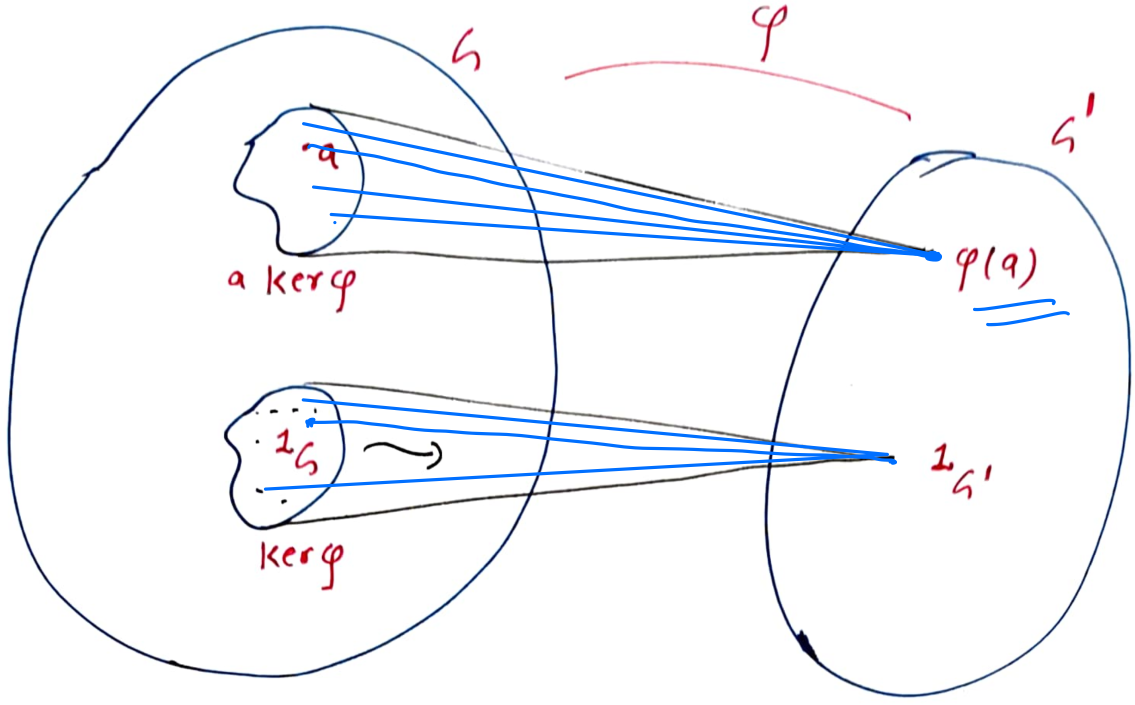
$= \varphi(a).$

Notation. $\varphi : G \longrightarrow G'$ group homomorphism

$$a\ker\varphi = \{g \in G \text{ such that } g = an \text{ for some } n \in \ker\varphi\}$$

$$\parallel$$

$$a \cdot H = \{an \text{ such that } n \in \ker\varphi\}$$



Here, $a \sim b$ in G if $\varphi(a) = \varphi(b)$ partitions the group G into congruence classes $a \ker\varphi$.

COSETS. Let H be a subgroup of G. A left coset is a subset of the form [Wikipedia]

$$\underset{\overset{\shortparallel}{a * H}}{aH} = \{ \underset{\overset{\shortparallel}{a*h}}{ah} \text{ such that } h \in H \}.$$

Note.

(i) $1_G \cdot H = H$ [Subgroup H is itself a coset]

(ii) aH need not be a subgroup

Examples.

1. $G = (\mathbb{Z}/9\mathbb{Z}, +)$, and $H = \{[0], [3], [6]\}$.

$\mathbb{Z}/9\mathbb{Z} = \{[0], [1], [2], \dots [8]\}$

Is H a subgroup of G?

Cosets of H in G are

$$[0] + H = \{[0], [3], [6]\} = H$$

$$[1] + H = \{[1], [4], [7]\}$$

$$[2] + H = \{[2], [5], [8]\}$$

$$[3] + H = \{[0], [3], [6]\} = [0] + H$$

$$[4] + H = [1] + H \underline{= [7] + H}$$

Similarly $[5] + H = [2] + H = [8] + H$

Note. If $h \in H$, then $h + H \in H$, and hence $h + H = H$.

2. Let $G = (\mathbb{Z}, +)$ and $H = m\mathbb{Z}$ for some m.

Cosets of H in G are

$$0 + H = H = \{\dots, -m, 0, m, \dots\}$$

$$1 + H = \{\dots, -m+1, 1, m+1, \dots\}$$

$$\vdots$$

$$m-1 + H = \{\dots, -1, m-1, m+m-1, \dots\}$$

3. Cosets of $2\mathbb{Z}$ in $\mathbb{Z}$.

$0 + 2\mathbb{Z} = \{\cdots, -4, -2, 0, 2, 4, \cdots\}$ even numbers

$1 + 2\mathbb{Z} = \{\cdots, -3, -1, 1, 3, \cdots\}$ odd numbers

Note that

$2 + 2\mathbb{Z} = 0 + 2\mathbb{Z} = 2\mathbb{Z}$

$3 + 2\mathbb{Z} = 1 + 2 + 2\mathbb{Z} = 1 + 2\mathbb{Z}$

Thus, $0 + 2\mathbb{Z}$ and $1 + 2\mathbb{Z}$ are the only distinct cosets.

4. $G = (\mathbb{R} - \{0\}, \cdot)$ and $H = \{1, -1\}$.

Cosets of H in G are

$aH = \{a, -a\}$ for every $a \in \mathbb{R} - \{0\}$.

5. $G = S_3$ and $H = \{e, (12)\}$

Corollary. The left cosets of a subgroup H partitions the group G.

$aH = \{ ah \text{ such that } h \in H \}$ (left coset)

Define $a \sim b$ in G if $b = ah$ for some $h \in H$.

[We also use $a \equiv b$ for $a \sim b$]

Reflexive. $a \sim a$ since $1_G \in H$, $a = a \cdot 1_G$

Symmetric. Suppose $a \sim b \Rightarrow b = ah$ for some $h \in H$

$\Rightarrow a = bh^{-1}$

$\Rightarrow b \sim a$ [If $h \in H$, then $h^{-1} \in H$

Transitive. Suppose $a \sim b$ and $b \sim c$

$\Downarrow$ $\Downarrow$

$b = ah_1$ $c = bh_2$

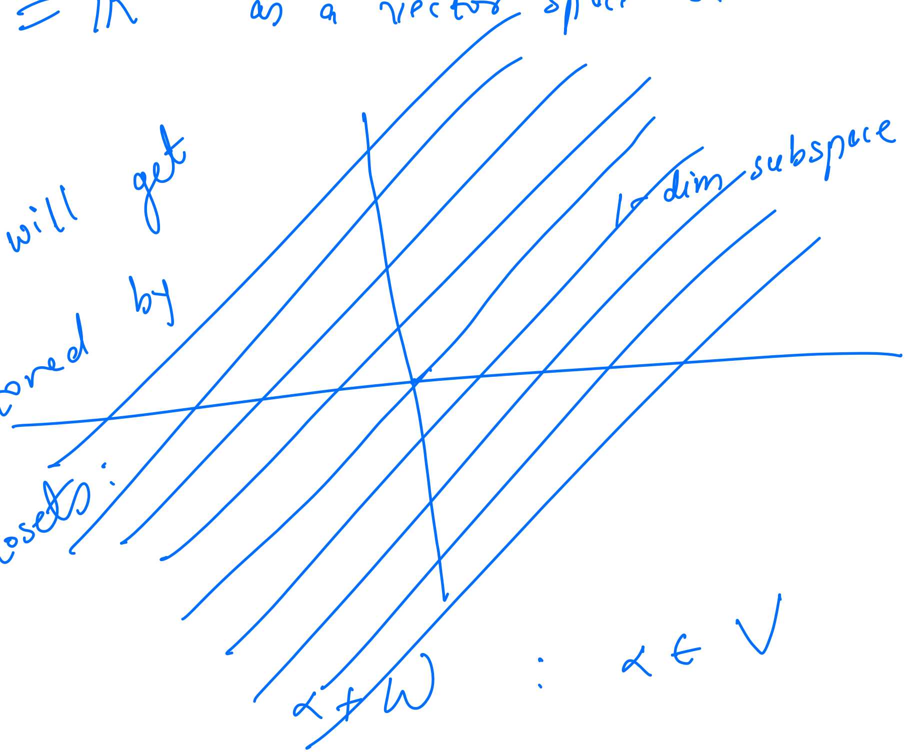
Then

$$
\begin{aligned}
c &= bh_2 \\
&= ah_1h_2 = a \cdot (h') \quad \text{for some } h' \in H.
\end{aligned}
$$

$\Rightarrow a \sim c$.

$V = \mathbb{R}^2$ as a vector space over $\mathbb{R}$

$\mathbb{R}^2$ will get partitioned by cosets:



$\alpha + W \quad : \quad \alpha \in V$

$\boxed{AX = B}$

$AX = 0$ ← vector space under +

Group $(G, +)$

$W = \{ X \mid AX = 0 \}$

$AX = B$

$$\left[A : B \,\middle|\, X \right]^{n \times 1}$$

$\alpha + W$

Cosets provide solution to non-homog. system

Remark. Each coset aH has the same number of elements as H does.

Proof. Define
$$\varphi : H \longrightarrow aH \quad ; \; a \in G$$
$$h \longmapsto \varphi(h) = ah$$

Is φ one-one ?

$$\varphi(h_1) = \varphi(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$$

Is φ onto ?

$$\forall\, ah \in aH \quad \exists\, h \in H \text{ s.t. } \varphi(h) = ah$$

Remark. $|H| = |aH|$ (may be finite or infinite)

If $|G|$ is finite, then $|H|$ is also finite.

Definition. The number of left cosets of a subgroup H is called the index of H in G, and is denoted by $[G:H]$.

Discussion.

If G is a finite group, then

(i) $[G:H]$ is also finite. [no. of left cosets of H in G] is finite.

(ii) H is finite subgroup.

(iii) $|H| = |aH|$ for any $a \in G$.

i.e. no. of elements in H = no. of elements in coset aH

Set-up as in previous discussion:

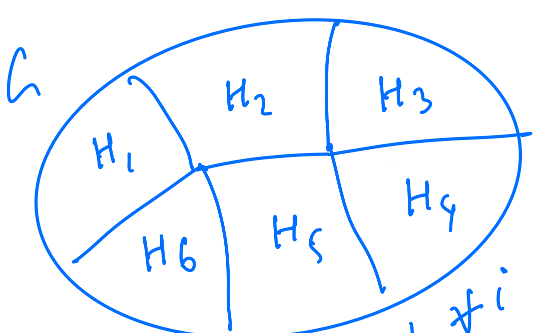
$$\begin{array}{ccccc} |G| & = & |H| & \cdot & [G:H] \\ \| & & \| & & \| \\ n & & m & & k \end{array} \qquad n, m, k \in \mathbb{N}.$$

Cases:

(i) m divides n. [Lagrange's Theorem]

$|H| \mid |G|$

order of subgroup divides the order of group.



$|H_i| = |H|$ $\forall i$, then

$$|G| = 6 \cdot |H| = [G:H] \cdot |H|$$

(ii) Assume that n is prime., i.e. $|G| = n$ (prime)

Then $n = m \cdot k$

$\Rightarrow$ $m = n$ and $k = 1$

[Only one coset]

$\Downarrow$

$G = H$.

(iii) $$[G:H] = \frac{|G|}{|H|}$$

or $|G| = |H| \cdot [G:H]$.

Given H in G, $|H|$ divides $|G|$.

In general, G may not have a subgroup for every divisor of $|G|$.

Remark.

(i). A group of prime order is cyclic.

(ii) Assume $|G|$ is finite. Let $a \in G$, then $|a| \mid |G|$.

Proof.

(i) $|G| = p$ (prime no.)

Let $a \in G$ and $a \neq 1_G$.

Then consider a group generated by a,

$$\langle a \rangle = H.$$

Then $|H|$ divides $|G|$

$$\Rightarrow \quad |G| = |H| \cdot \underbrace{[G:H]}_{=1} \quad \Rightarrow \quad |H| = |G| = p$$

$$|H| = \langle a \rangle = \langle e, a, a^2, \ldots, a^{p-1} \rangle$$

(ii) Recall

$$|a| = |\langle a \rangle| = |H|$$

[order of a is same as the order of the cyclic group generated by a]

$$\Rightarrow |a| \mid |G|.$$

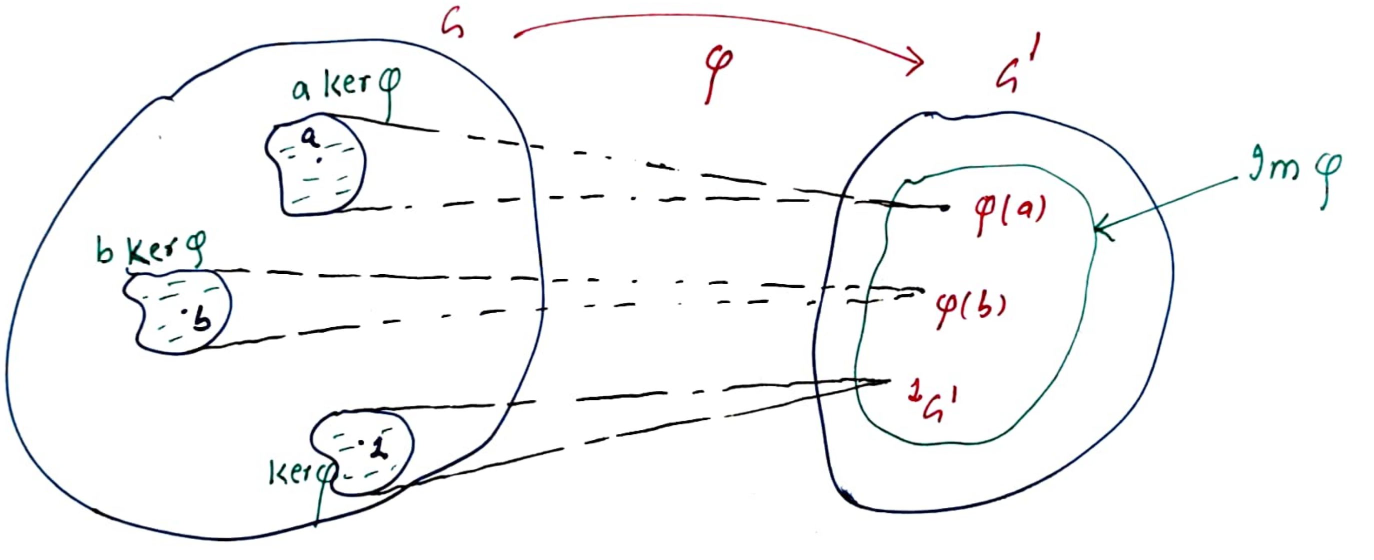
Special Case: $\varphi : G \longrightarrow G'$ group homomorphism,

we know that $\ker\varphi$ is a subgroup of G.

$[G : \ker\varphi]$ = The index of $\ker\varphi$ in G

[number of left cosets of $\ker\varphi$]

$\{a \cdot \ker\varphi\}_{a \in G}$ is collection of left cosets of $\ker\varphi$ in G



Then $G = \bigcup_{b' \in \mathrm{Im}\varphi} \varphi^{-1}(b') = \bigcup_{b \in G} b\ker\varphi$

[$\varphi^{-1}(b')$ is called fibre of b]

It follows that $[G : \ker\varphi] = |\mathrm{Im}\,\varphi|$

Set. If G and G' are finite groups, then

(i) $|G| = |\ker\varphi|\,|\mathrm{Im}\,\varphi|$

(a) $|\ker\varphi|$ divides $|G|$ (b). $|\mathrm{Im}\,\varphi|$ divides both $|G|$ and $|G'|$.