PITHAPUR RAJAH'S GOVERNMENT COLLEGE (AUTONOMOUS), KAKINADA 533001-ANDHRA PRADESH

DEPARTMENT OF MATHEMATICS

KURAGANTI SANJI INDIRA PRIYADARSINI
LECTURER IN MATHEMATICS
P.R.G.C (A),KAKINADA.

In 1772, Lagrange initiated the study of the permutations while studying the solutions of algebraic equations.

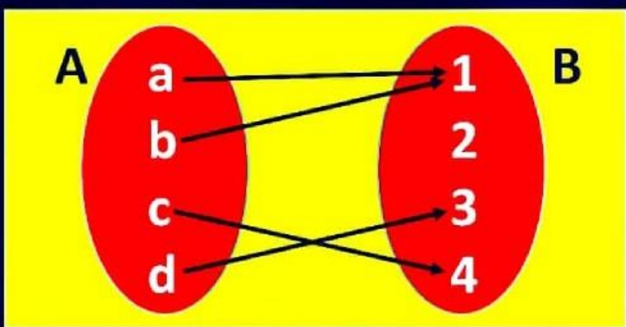
Galois(1812- 1832), first time use the word "Group" in a technical sense.

Basic Concepts

❖ Set: A collection of well-defined objects.

❖ Function : $\forall \ a \in A \ \exists \ a \ unique \ b \in \mathrm{B} \ni$

$$f(a) = b$$



❖ Binary Operation :

A way of computing from $S \times S \rightarrow S$

Group:

Let G be a non empty set and $*$ *be a binary operation on G. Then*

G_1: $\forall a, b \in G, a * b \in G$

G_2: $\forall a, b, c \in G,$

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

G_3: $\forall a \in G, \exists e \in G \ni a * e = e * a = a$

G_4: $If\ a \in G, \exists some\ b \in G \ni$

$$a * b = b * a = e.$$

If G satisfies

G_1 & $G_{2,}$ *then G is called* *semi Group*.

G_1, G_2&$G_{3,}$ *then G is called* *monoid.*

$G_1, G_{2,} G_3$&$G_{4,}$ *then G is called* a Group.

❖ In addition, $\forall a, b \in G, a * b = b * a$, then the group $(G,*)$ is called an abelian group.

Subgroup

Let $(G,*)$ *be a group and H be a non empty subset of G. Then H is said to be a subgroup, if* (H,∗) itself is a group.

Example: Let H={1,-1} sub set of a group G=$\{1, -1, i, -i\}$ *and* "." binary operation on G. Then, (H,.) is a subgroup of group G.
Since H itself is a group w.r.t. binary operation "."

.	1	-1	*i*	*-i*
1	1	-1	*I*	*-i*
-1	-1	1	*-i*	*i*
i	*i*	*-i*	-1	1
-i	*-i*	*i*	1	-1

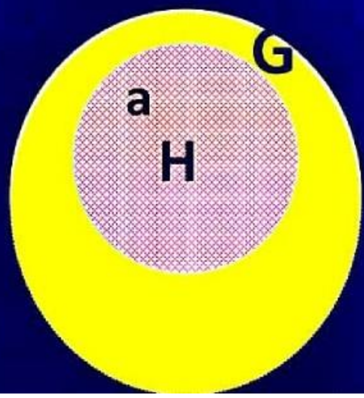
.	1	-1
1	1	-1
-1	-1	1

Cosets

Let $(H,.)$ *be a subgroup of a group* $(G,.)$ *and* $a \in G$. *Then*

$a.H = \{a.h | h \in H\}$ *is called a left Coset*

$H.a = \{h.a | h \in H\}$ *is called a right Coset of H containing a.*



Let $(H,+)$ *be a subgroup of a group* $(G,+)$ *and* $a \in G$. *Then, the left and right cosets are*

$$\boldsymbol{a + H = \{a + h | h \in H\}}$$

$$\boldsymbol{H + a = \{h + a | h \in H\}}$$

Here onwards,

1. G *stands for a group with the binary opeation* "."
2. H *stands for a subgroup of a group* $(G, .)$.
3. We write aH instead of $a.H$ and
4. We write ah instead of $a.h$

<u>Here are a few questions we try to address in this lecture:</u>

1. When is aH = bH or when is Ha = Hb?
2. Are all cosets subgroups? If not, which ones are?
3. $|aH| = |bH|$?
4. Can different cosets have elements in common?
5. Is $|aH| = |Ha|$?

Example 01:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\}$$
$$H = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \ldots\}.$$

$(H,+)$ is subgroup of $(\mathbb{Z},+)$.

Let $1 \in \mathbb{Z}$.

Then left & right cosets are

$$1 + H = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$$
$$H + 1 = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$$

Example: Let $G = \{1, -1, i, -i\}$ be a group and $H = \{1, -1\}$ be a subgroup of G. Then

Left cosets	Right cosets
$1H = \{1, -1\}$	$H1 = \{1, -1\}$
$-1H = \{-1, 1\}$	$H(-1) = \{-1, 1\}$
$iH = \{i, -i\}$	$Hi = \{i, -i\}$
$-iH = \{-i, i\}$	$H(-i) = \{-i, i\}$

Remark.

1. For an abelian group G,
   $aH = Ha$, i.e. right and left cosets of any subgroup coincide.
2. The subgroup H itself is always one of its left cosets and right cosets (since $eH = He = H$).

Theorem:01

Let H be a subgroup of a group G and $a \in G$. Then 1. $a \in aH$
2. $a \in Ha$.

Proof:

Since H is a sub group of group G, we have $e \in H$.

Then $a = ae \in aH$.

Similarly, we prove that $a \in Ha$.

Theorem:02

Let H be a subgroup of a group G and $a \in G$. *Then* $\mathbf{a \in H \Leftrightarrow aH = H.}$

Proof: *Suppose* $aH = H$.

By Theorem 01, $a \in aH$. But $aH = H$

Thus, we get $a \in H$.

Conversely, Suppose $a \in H$.

Claim: $aH = H\ (aH \subseteq H\ \&\ H \subseteq aH)$.

Let $ah \in aH$ *for some* $h \in H$.

Since H is a subgroup & a,h∈ H, *we get* $ah \in H$. Thus $aH \subseteq H$.

Let $h \in H$.

Since $a \in H$ *and* H *is a sub group,* we get that $a^{-1} \in H \ni aa^{-1} = e$.

$$\text{Now } h = eh = (aa^{-1})h$$
$$= a(a^{-1}h) \in aH.$$

Thus $H \subseteq aH$. *Hence* $H = aH$.

Theorem 04: Let H be a subgroup of a group G and $a, b \in G$. Then

1. $a \in bH \Leftrightarrow aH = bH$
2. $a \in Hb \Leftrightarrow Ha = Hb$.

Proof: Suppose $aH = bH$.

If $a \in aH$, then $a \in bH$

$(\because aH = bH)$.

Conversely, Suppose $a \in bH$.

$$\begin{aligned} Then\ b^{-1}a &\in b^{-1}bH \\ \Rightarrow b^{-1}a &\in eH \\ \Rightarrow b^{-1}a &\in H \\ \Rightarrow bH &= aH. \end{aligned}$$

Similarly, we can prove $a \in Hb \Leftrightarrow Ha = Hb$.

Example: Let $H = \{1, -1\}$ be a sub-group of a group $G = \{1, -1, i, -i\}$.
Then the left cosets are

$$1H = \{1, -1\}$$
$$-1H = \{-1, 1\}$$
$$iH = \{i, -i\}$$
$$-iH = \{-i, i\}$$

Here $1H = \{1, -1\} = -1H$

$iH = \{i, -i\} = -iH$

Theorem 05: *Let H be a subgroup of a group G and $a, b \in G$. Then any two left(right) cosets either identical or disjoint (or)*

If aH, bH be two left cosets of H in G, then either $aH \cap bH = \phi$ or $aH = bH$.

Proof: Let aH, bH be two left coests of H in G.

$Suppose\ aH \cap bH = \phi.$

Then nothing to prove.

Suppose aH $\cap\, bH \neq \phi.$

$$Then\ c \in aH \cap bH$$
$$\Rightarrow c \in aH\ \&\ c \in bH$$
$$\Rightarrow cH = aH\ \&\ cH = bH$$
$$(\because \text{ by Theorem } 04)$$
$$\Rightarrow aH = bH.$$

Similarly, we can prove either

$$Ha \cap Hb = \phi \text{ or } Ha = Hb.$$

Theorem 07: *Let H be a subgroup of a group G. Then there exists a bijection between the set of distinct left cosets of H in G and the set of distinct right cosets of H in G*

$Proof$: *Let*

$L_H =$ the set of all left cosets of H in G

$R_H =$ the set of all right cosets of H in G

Define f: $L_H \rightarrow R_H$ by $f(aH) = Ha^{-1}$, $\forall a \in G$.

$\underline{f \text{ is well} - \text{define}}$:

Suppose $aH = bH$

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

$\Rightarrow (a^{-1}b)^{-1} \in H$ ($\because$ H is a sub gp)

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

$\Rightarrow Ha^{-1} = Hb^{-1}$

$\Rightarrow f(aH) = f(bH)$

$\underline{f \text{ is one} - \text{one}}$:

Suppose $Ha^{-1} = Hb^{-1}$

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

$\Rightarrow a^{-1}b \in H$ ($\because$ H is a sub gp)

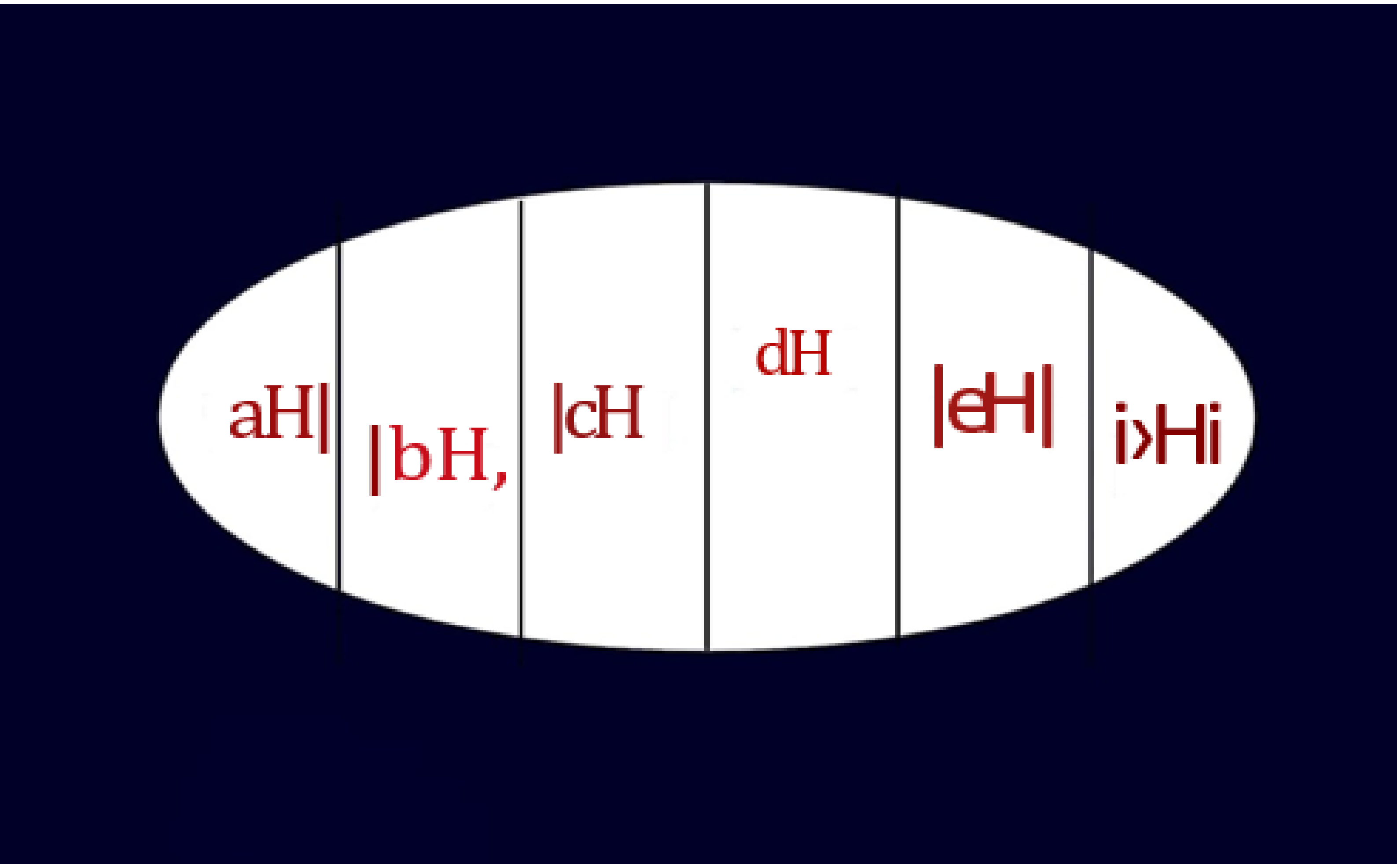
$\Rightarrow aH = bH$

$\underline{f \text{ is onto}}$:

For $Ha \in R_H$. Since $a \in G$, we get $a^{-1} \in G$ and hence $a^{-1}H \in L_H$.

Thus $f(a^{-1}H) = H(a^{-1})^{-1} = Ha$

$\therefore$ f is onto and hence f is bijective.



Recap:

1. $a \in aH$
2. $aH = H \Leftrightarrow a \in H$
3. $a \in Hb \Leftrightarrow Ha = Hb$
4. Either $aH = bH$ or $aH \cap bH = \phi$
5. $aH = bH \Leftrightarrow a^{-1}b \in H$
6. $|aH| = |bH|$
7. $|aH| = |Hb|$