Subgroups and Lagrange's Theorem

Let $(G, *)$ be a group

<u>Definition</u> $H \subset G$ is a <u>subgroup</u> if

- $e \in H$ (Identity)
- $x, y \in H \Rightarrow x * y \in H$ (Closure under composition)
- $x \in H \Rightarrow x^{-1} \in H$ (Closure under inverses)

<u>Examples</u>

1/ Given $m \in \mathbb{N}$, $m\mathbb{Z} := \{ma \mid a \in \mathbb{Z}\} \subset \mathbb{Z}$

2/ V real vector space, $W \subset V$ a subspace

$\Rightarrow (W, +)$ a subgroup of $(V, +)$

3/ orthogonal matrices

$O_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R}) \mid A^T = A^{-1}\} \subset GL_n(\mathbb{R})$

trivial subgroup

4/ $\{e\} \subset G$, $G \subset G$

<u>Definition</u> Let $H \subset G$ be a subgroup. A <u>left coset</u> of H in G is a <u>subset</u> of the form

$$xH := \{x * h \mid h \in H\} \subset G$$

for some $x \in G$.

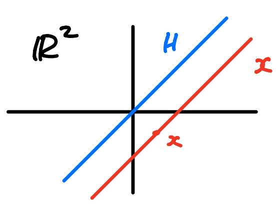
<u>Examples</u>

Group under + | Remainder class of x modulo m

1/ $x \in \mathbb{Z}, H = m\mathbb{Z}, G = \mathbb{Z} \Rightarrow xH = \{x + ma \mid a \in \mathbb{Z}\} = [x]$

2/ $x = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, $H = \{\lambda \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mid \lambda \in \mathbb{R}\}$, $G = \mathbb{R}^2$ group under addition

$\Rightarrow xH = \{\begin{pmatrix} 1 \\ -1 \end{pmatrix} + \lambda \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mid \lambda \in \mathbb{R}\}$ = Straight line parallel to H containing x



Proposition The left cosets of H in G form a partition of G

Proof

- Let $x \in G$

$e \in H \Rightarrow x = x * e \in xH \Rightarrow \bigcup_{x \in G} xH = G$

- Let $x, y \in G$ such that $xH \cap yH \neq \emptyset$

$\Leftrightarrow \exists\, h_1, h_2 \in H$ such that $x * h_1 = y * h_2$

$\Leftrightarrow x^{-1} * y = h_2 * h_1^{-1}$ $\quad (h_1, h_2 \in H \Rightarrow h = h_2 * h_1^{-1} \in H)$

So $xH \cap yH \neq \emptyset \Leftrightarrow x^{-1} * y \in H$

$x^{-1} * y = h \Rightarrow y = x * h$ and $x = y * h^{-1}$ in H

Let $k \in H$, then $y * k = x * (h * k) \in xH \Rightarrow yH \subset xH$

Similarly, $x * k = y * (h^{-1} * k) \in yH \Rightarrow xH \subset yH$ (in H)

Hence $xH \cap yH \neq \emptyset \Leftrightarrow xH = yH$

$\square$

Definition We denote the collection of left cosets of H in G by G/H. ← "G quotient H"

If $|G/H| < \infty$ we say H is finite order in G

Examples $\mathbb{Z}/m\mathbb{Z}$ finite, $\mathbb{R}^2 / \{\lambda \binom{1}{1} \mid \lambda \in \mathbb{R}\}$ infinite

Remarks 1) xH = equivalence class containing x under the following equivalence relation: $x \sim y \Leftrightarrow x^{-1} * y \in H$. Hence $y \in xH \Leftrightarrow yH = xH$

2) Left cosets are <u>not</u> subgroups in general.

$e \in xH \Leftrightarrow eH = xH \Leftrightarrow x \in H$.

Proposition The map $f : H \longrightarrow xH$ is a <u>bijection</u>.
$$h \longrightarrow x * h$$

In particular, if $|H| < \infty$ then $|H| = |xH|$

Proof

f surjective by definition of xH

Let $h, k \in H$

$$f(h) = f(k) \Rightarrow x * h = x * k \overset{(C.L.)}{\Rightarrow} h = k \Rightarrow f \text{ injective}$$

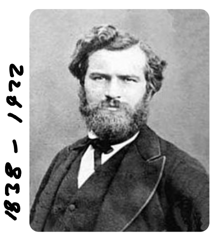
$\square$

Lagrange's Theorem Let G be a <u>finite</u> group and $H \subset G$ a subgroup

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

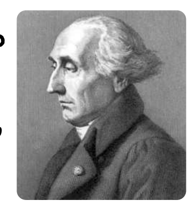
proved general case

1838 - 1922



Jordan

1736 - 1813



Lagrange

Proof

$|G| < \infty \Rightarrow |H| < \infty$

Hence $|xH| = |H| \quad \forall x \in G$

Number of sets in partition

Each has size

The left cosets partition $G \Rightarrow |G| = |G/H| \cdot |H|$

$\square$

Remarks

1/ $|G| < \infty$, $H \subset G$ subgroup $\Rightarrow \left|G/H\right| = \dfrac{|G|}{|H|}$

2/ $|G| = p$, a prime, $H \subset G$ subgroup $\Rightarrow H = \{e\}$ or $H = G$

3/ <u>Warning</u>: If $m \,\big|\, |G|$ it is <u>not</u> in general true that $\exists H \subset G$ a subgroup such that $m = |H|$.

We'll see examples later.