Cosets and Lagrange's Theorem

(Section 2.5)

Q: (order of subgroups) Let G be a group, $H \leq G$. Does $|H|$ have any connection to $|G|$? In particular what can we say if $|G| < \infty$?

Definition: (left/right cosets) Let G be a group, $H \leq G$. We define the set of all **left cosets** of H to be

$$\{xH \mid x \in G\}$$

where

$$xH = \{xy \mid y \in H\}.$$

Similarly, the **right cosets** of H,

$$\{Hx \mid x \in G\},$$

is comprised of all

$$Hx = \{yx \mid y \in H\}.$$

Observations: 1) If G is abelian, then $xH = Hx \ \forall \ x \in G$, i.e., left cosets are right cosets.

2) $H \trianglelefteq G$ if and only if $xH = Hx \ \forall \ x \in G$.

Example 1: Let $G = D_4$ = the symmetries of a square.

$$D_4 = \{ R^k J^m \mid 0 \le k \le 3, m \in \{0,1\} \}$$

and

$$R^4 = e$$

$$J^2 = e$$

$$JR = R^3 J$$

Let $H \le G$,

$$H = \langle J \rangle = \{ e, J \}.$$

Then we list all left cosets of H:

1) $eH = \{e, J\} = H$

2) $JH = \{J \cdot e, J \cdot J\} = \{J, e\} = H$

3) $RH = \{R \cdot e, R \cdot J\} = \{R, R \cdot J\}$

4) $R^2H = \{R^2 \cdot e, R^2 \cdot J\} = \{R, R^2 J\}$

5) $R^3 H = \{R^3 \cdot e, R^3 \cdot J\} = \{R^3, R^3 J\}$

6) $JRH = \{JR \cdot e, \underbrace{JR}_{R^3 J} \cdot J\} = \{JR, R^3\}$

$= \{R^3 J, R^3\}$

$= R^3 H$

7) $JR^2H = \{JR^2 \cdot e, JR^2 \cdot J\}$

$$= \{\underline{JR^2 \cdot e, \ R^2}\} = R^2 H$$

8) $JR^3H = \{JR^3 \cdot e, JR^3 \cdot J\}$

$$= \{\underline{JR^3, \ R}\}$$

$$= RH$$

These are all the left cosets of H.

Proposition: (equivalences) Let G be a group, $H \leq G$. The following conditions are equivalent for $x, y \in G$:

1) $x \in yH$

2) $y \in xH$

3) $xH = yH$

4) $y^{-1}x \in H$

5) $x^{-1}y \in H$

proof: $1 \Rightarrow 2$

if $x \in yH$, $\exists\ z \in H$

$x = yz$.

Then multiplying on the right by z^{-1},

$xz^{-1} = y$, so

$y \in xH$

Since $H \leq G \Rightarrow z^{-1} \in H$.

$2 \Rightarrow 1$ same proof, interchange x and y.

$2 \Rightarrow 3$ Show $xH = yH$

Since $1 \Leftrightarrow 2$, we may assume either one. Let $t \in xH$. Then $\exists\, w \in H$,

$t = xw$

from 1), $\exists\ z \in H$,

$x = yz$, so

$t = (yz)\cdot w = y\cdot(z\cdot w) \in yH$

Since $H \leq G \Rightarrow z\cdot w \in H$.

This shows $xH \subseteq yH$ if

$y \in xH$ ($\Leftrightarrow x \in yH$).

The reverse containment is similar.

$3 \Rightarrow 4$ We know $xH = yH$

Then since $e \in H$,

$\boxed{x \in xH}$.

But $xH = yH$, so $\exists\ z \in H$,

$x = yz$

$\Rightarrow y^{-1}x = z \in H$

$4 \Rightarrow 5$ If $y^{-1}x \in H$, $\exists\ s \in H$,

$y^{-1}x = s$.

Then
$x^{-1}y = (y^{-1}x)^{-1} = s^{-1} \in H$

since $H \leq G$.

$5 \Rightarrow 1$ Suppose $x^{-1}y \in H$. Then

$\exists\ q \in H$,
$x^{-1}y = q \Rightarrow$
$xq = y \Rightarrow x = yq^{-1} \in yH$

$\square$

Proposition: Let G be a group, $H \leq G$.

Then if $x, y \in G$,

1) Either $xH = yH$ or

$xH \cap yH = \emptyset$

2) $xH \neq \emptyset \quad \forall x \in G$

and $\displaystyle\bigcup_{x \in G} xH = G$.

proof: 1) Suppose $xH \cap yH \neq \emptyset$.

We want to show $xH = yH$.

Take $z \in xH \cap yH$.

Then $\exists \; s, t \in H$

$$z = xs$$

$$z = yt .$$

Then

$$xs = z = yt , \quad \text{so}$$

$$xs = yt ,$$

$$x = yts^{-1} \quad (\text{multiply by } s^{-1} \text{ on the right})$$

$$\Rightarrow x \in yH$$

since $H \leq G \Rightarrow ts^{-1} \in H .$

But this is 1) in the previous proposition, so according to the equivalence 1) $\Leftrightarrow$ 3),

$$xH = yH .$$

2) Since $H \leq G$, $H \neq \emptyset$.

In particular, $e \in H$, so

$$\boxed{x \in xH} \Rightarrow xH \neq \emptyset.$$

The statement regarding unions is then trivial.

Theorem: (Lagrange) Let G be a group, $H \leq G$, and assume $|G| < \infty$. Then $|H|$ divides $|G|$.

proof: We know from the previous proposition that if $x, y \in G$, $xH = yH$ or $xH \cap yH = \phi$.

Then using the second part of the proposition,

$$G = \bigcup_{x \in G} xH = x_1 H \cup x_2 H \cup \cdots \cup x_n H$$

where $x_i H \cap x_j H = \phi$ if $i \neq j$, for some $n \in \mathbb{N}$.

Then $G = \bigsqcup_{i=1}^{n} x_i H$.

However, the map

$$z \mapsto xz \qquad (z \in H)$$

establishes a bijection from H to xH $\forall x \in G$.

Then $|x_i H| = |H|$

$\forall\ 1 \leq i \leq n$.

Then $|G| = \left| \bigsqcup_{i=1}^{n} x_i H \right|$

$= n\,|H|$

$\Rightarrow |H|$ divides $|G|$ $\square$