Cosets

Def: Let G be a group and $H \leq G$. A left coset of H in G is a subset of G of the form

$$aH = \{a * x \mid x \in H\}$$

Likewise, a right coset is a subset of the form

$$Ha = \{x * a \mid x \in H\}$$

Notation: if $* = +$, we write $a+H$ instead of aH.

Ex: Let $G = \mathbb{Z}_4$ and $H = \langle 2 \rangle = \{0,2\}$.
Then $0+H = \{0,2\}$ and $1+H = \{1,3\}$ are cosets.
So is $2+H = \{0,2\}$ but we see that this is just the same as $0+H$. In fact the only distinct cosets are $0+H$ and $1+H$.

Ex: Let $G = S_3$ and $H = \langle (12) \rangle = \{(12), e\}$.
The left cosets are:

$$eH = \{(12), e\}$$
$$(12)H = \{e, (12)\} = eH$$
$$(13)H = \{(123), (13)\}$$
$$(23)H = \{(132), (23)\}$$
$$(123)H = \{(13), (123)\} = (13)H$$
$$(132)H = \{(23), (132)\} = (23)H$$

The distinct left cosets are $eH, (13)H, (23)H$.

The right cosets are:

$$He = \{(12), e\}$$
$$H(12) = \{e, (12)\} = He$$
$$H(13) = \{(132), (13)\}$$
$$H(23) = \{(123), (23)\}$$
$$H(123) = \{(23), (123)\} = H(23)$$
$$H(132) = \{(13), (132)\} = H(13)$$

The distinct right cosets are $eH, H(13), H(23)$

Observations:

- each coset has same size
- left cosets are not necessarily right cosets!
- the set of left cosets forms a partition of G
- the set of right cosets forms a partition of G
- # left cosets = # right cosets
- # left cosets = $|G|/|H|$

Let's try to prove some of these things!

Define relations $\sim_L$ and $\sim_R$ on G by

$$a \sim_L b \Leftrightarrow a^{-1}b \in H \quad \text{and} \quad a \sim_R b \Leftrightarrow ba^{-1} \in H$$

Lemma: Both $\sim_L$ and $\sim_R$ are equivalence relations on G.

Proof:

REFLEXIVE: $e = a^{-1}a \in H$ so $a \sim_L a$

SYMMETRIC: $a \sim_L b \Leftrightarrow a^{-1}b \in H$
$\Leftrightarrow (a^{-1}b)^{-1} \in H$
$\Leftrightarrow b^{-1}a \in H \Leftrightarrow b \sim_L a$

TRANSITIVE: $a \sim_L b$ and $b \sim_L c \Rightarrow a^{-1}b \in H$ and $b^{-1}c \in H$
$\Rightarrow a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$
$\Rightarrow a \sim_L c$.

Proof is similar for $\sim_R$ $\square$

Recall: the equivalence classes of an equivalence relation define a partition!

The equivalence class of $a \in G$ for the relation $\sim_L$ is

$$\{x \in G \mid a \sim_L x\} = \{x \in G \mid a^{-1}x \in H\} = \{ah \mid h \in H\} = aH$$

Aha! Equivalence classes of $\sim_L$ are left cosets.
This is why they form a partition.

Likewise, the equivalence class of $a \in G$ for the relation $\sim_R$ is

$$\{x \in G \mid a \sim_R x\} = \{x \in G \mid xa^{-1} \in H\} = \{ha \mid h \in H\} = Ha$$

These are the right cosets, so they too form a partition (potentially different)

<u>Prop</u>: # left cosets = # right cosets.

<u>Proof</u>:

Let $G/H = \{aH \mid a \in G\} \subseteq \mathcal{P}(G)$

$\quad {}_H\backslash G = \{Ha \mid a \in G\} \subseteq \mathcal{P}(G)$

Define $f : G/H \to {}_H\backslash G$

$$S \mapsto S^{-1} = \{s^{-1} \mid s \in S\}$$

Note

$$(aH)^{-1} = \{(ah)^{-1} \mid h \in H\} = \{h^{-1}a^{-1} \mid h \in H\}$$
$$= \{ba^{-1} \mid b \in H\} = Ha^{-1}$$

so f maps left cosets to right cosets and is thus well defined. Since $f(f(S)) = S$, f is its own inverse, so f is bijective

$\square$

<u>Def</u>: The <u>index</u> of H in G is the number of left cosets of H in G.

Notation: $[G:H]$ = index of H in G.

<u>Ex</u>: $G = S_3$, $H = \langle(12)\rangle$, $[G:H] = 3$.

Prop: Each coset has the same cardinality as H.

Proof: Define

$$f: H \to aH \qquad\qquad g: aH \to H$$
$$x \mapsto x \qquad\qquad y \mapsto a^{-1}y$$

Note f and g are inverse functions, so f is bijective. Thus aH and H have the same cardinality $\square$

Theorem (Lagrange): Suppose G has finite cardinality. Then

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

so in particular the order of H divides the order of G.

Proof:

Let $G/H = \{a_1H, a_2H, \dots, a_rH\}$ be the distinct cosets of H in G. Obviously $r = [G:H]$. Since the cosets are a partition

$$\begin{aligned} |G| &= |a_1H \cup a_2H \cup \dots \cup a_rH| \\ &= |a_1H| + |a_2H| + \dots + |a_rH| \\ &= |H| + |H| + \dots + |H| \quad = |H| \cdot r = [G:H] \cdot |H| \end{aligned}$$

$\square$

Some immediate consequences:

Prop: The order of $a \in G$ must divide $|G|$.

Proof: order of a = $|\langle a \rangle|$ which divides $|G|$ by Lagrange's Theorem $\square$

Prop: If $|G| = p$ prime, then $G \cong \mathbb{Z}_p$.

Proof: Choose $x \in G$ different from e. Then the order of x is p so $|\langle x \rangle| = |G|$. $\therefore \langle x \rangle = G$ $\square$.

When are two cosets the same?

Theorem: $aH = bH \iff a^{-1}b \in H$.

Proof:

$$aH = bH \iff a \text{ and } b \text{ have the same equivalence class}$$
$$\iff a \sim_L b \iff a^{-1}b \in H.$$

$\square$

Quest: When are the left cosets also right cosets?

Theorem: Let $\varphi : G \to \tilde{G}$ be a group homomorphism and suppose $H = \ker \varphi$. Then $aH = Ha$ for all $a \in G$.
Moreover $aH = bH \iff \varphi(a) = \varphi(b)$

Proof:

Recall that

$$\ker \varphi = \{x \in G \mid \varphi(x) = \tilde{e}\}.$$

Also notice $\varphi(a^{-1}) = \varphi(a)^{-1}$ and therefore if $x \in \ker(\varphi)$

$$\varphi(axa^{-1}) = \varphi(a)\varphi(x)\varphi(a)^{-1} = \varphi(a)\tilde{e}\varphi(a)^{-1}$$
$$= \varphi(a)\varphi(a)^{-1} = \tilde{e}$$

Thus $axa^{-1} \in \ker(\varphi)$ for all $x \in \ker(\varphi)$. Using this

$$aH = \{ax \mid x \in \ker(\varphi)\}$$
$$= \{(axa^{-1})a \mid x \in \ker(\varphi)\}$$
$$= \{ya \mid y \in \ker(\varphi)\} = Ha$$

$\square$

Corollary: φ is injective if and only if $\ker(\varphi) = \{e\}$

Soon we will realize $H = \ker(\varphi)$ is the ONLY case when the left and right cosets are the same.