One more proposition about Kernels.

<u>Proposition</u>: Let $\varphi: G \to H$ be a homomorphism of groups. Then $\varphi$ is injective iff $\ker(\varphi) = \{e_G\}$.

<u>Proof</u>: If $\varphi$ is injective, $e_H$ has at most one preimage. Since $\varphi(e_G) = e_H$, we have $\ker(\varphi) = \varphi^{-1}(\{e_H\}) = \{e_G\}$.

Suppose $\ker(\varphi) = \{e_G\}$. Let $a, b \in G$ and suppose $\varphi(a) = \varphi(b)$ then $\varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = \varphi(a)^{-1}\varphi(b) = e_H$ then $a^{-1}b \in \ker(\varphi)$ so $a^{-1}b = e_G$, so $b = ae_G = a$. Thus $\varphi(a) = \varphi(b) \Rightarrow a = b$, and $\varphi$ is injective. $\blacksquare$

<u>Cosets</u>: $S_n$ = permutations of $\{1, 2, \dots, n\}$.

Consider $H = \{\sigma \in S_n \mid \sigma(1) = 1\}$ = permutations that fix 1. Then $H$ is a subgroup - check it yourself.

Next consider set $\{\sigma \in S_n \mid \sigma(1) = 2\}$. This is <u>not</u> a subgroup.
$(12), (123), (34)(12), \dots$

Now observe: if $\sigma, \tau \in S_n$ and $\sigma(1) = 2$ and $\tau(1) = 2$
Then $\tau^{-1}(2) = 1$, so $\tau^{-1}\sigma(1) = \tau^{-1}(2) = 1$
Thus $\tau^{-1}\sigma \in H$.
That is to say, $\tau^{-1}\sigma = h$ or $\sigma = \tau h$ for some $h \in H$.

In fact, <u>every</u> element of the set $\tau H = \{\tau h \mid h \in H\}$ takes $1 \to 2$
$\tau h(1) = \tau(1) = 2$.

Thus
$\{\sigma \in S_n \mid \sigma(1) = 2\} = \tau H$ where $\tau$ is <u>any</u> particular element with $\tau(1) = 2$.

E.g. $\{\sigma \in S_n \mid \sigma(1) = 2\} = (12)H$

More generally $\{\sigma \in S_n \mid \sigma(1) = j\} = (1j)H$.

<u>Definition</u> Let $G$ be a group, $H \leq G$ a subgroup.
For $g \in G$, define subsets
$gH = \{gh \mid h \in H\}$, a <u>Left coset</u> of $H$;
$Hg = \{hg \mid h \in H\}$, a <u>Right coset</u> of $H$.

<u>Proposition</u> Let $H \leq G$, $a, b \in G$. The following are equivalent.

(1) $a \in bH$
(2) $b \in aH$
(3) $aH = bH$
(4) $b^{-1}a \in H$
(5) $a^{-1}b \in H$

<u>Proof</u> <u>(1) ⇒ (2)</u>: If $a \in bH$, $(\exists h \in H)(a = bh)$
then $ah^{-1} = b$ so $b \in aH$

<u>(2) ⇒ (1)</u>: follows swapping roles of $a, b$.

<u>(1) ⇒ (3)</u>: $(\exists h \in H)(a = bh)$
so $\forall h' \in H$, $ah' = bhh' = b(hh') \in bH$
thus $aH \subseteq bH$. Since $b \in aH$,
we have $bH \subseteq aH$ as well, so (3) holds.

<u>(3) ⇒ (1)</u> $a = ae$ and $e \in H$, so $a \in H$.
If $aH = bH$, then $a \in aH = bH$, so (1) holds.

<u>(1) ⇒ (4)</u>: $a \in bH$ means $a = bh$ for some $h \in H$, so $b^{-1}a = h \in H$

<u>(4) ⇒ (5)</u>: $b^{-1}a \in H$ means $(b^{-1}a)^{-1} = a^{-1}b \in H$ since $H$ is subgrp.

<u>(5) ⇒ (2)</u>: $a^{-1}b \in H$ means $a^{-1}b = h \in H$ so $b = ah \in aH$.

We have shown implications
Can get from one to another
by arrows, so all are equivalent. ∎

$$\begin{tikzcd}
 & (1) \arrow[r, Leftrightarrow] \arrow[dr, Rightarrow] \arrow[ddr, Rightarrow] & (2) \\
(5) \arrow[urr, Rightarrow, bend right=80] & & (3) \\
 & (4) \arrow[ul, Rightarrow] &
\end{tikzcd}$$

**Remark** $a(bH) = (ab)H = \{abh \mid h \in H\}$

**Proposition:** Let $H \leq G$, and $a, b \in G$.
(1) $aH \cap bH \neq \emptyset$ iff $aH = bH$
(2) $aH \neq \emptyset$ and $G = \bigcup_{a \in G} aH$.
(3) $L_{ba^{-1}}(x) = ba^{-1}x$ defines a bijective function $aH \to bH$.

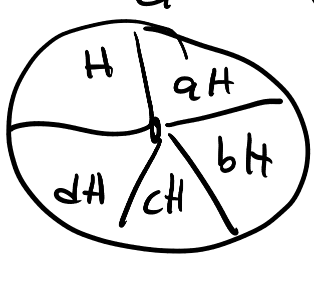
**Proof:** (2): since $e \in H$, $a = ae \in aH$, so $aH \neq \emptyset$.
For any $x \in G$, $x \in xH$, so $x \in \bigcup_{a \in G} aH$. Thus
$G \subseteq \bigcup_{a \in G} aH \subseteq G$ and these sets are equal.

(1) If $aH = bH$ then $aH \cap bH = aH \neq \emptyset$ by (2)
If $aH \cap bH \neq \emptyset$, let $c \in aH \cap bH$. Then
$c \in aH$ so $cH = aH$ and $c \in bH$ so $cH = bH$.
Thus $aH = cH = bH$.

(3) for any $ah \in aH$, $L_{ba^{-1}}(ah) = ba^{-1}ah = bh \in bH$.
So $L_{ba^{-1}} : aH \to bH$.
Swapping roles of $a$ and $b$, get function $L_{ab^{-1}} : bH \to aH$.
These functions are inverses: $L_{ba^{-1}} \circ L_{ab^{-1}} = L_{ba^{-1}ab^{-1}} = L_e$
So each is bijective.

In summary: (1) Distinct cosets are disjoint.
(2) Each coset is nonempty, and they cover all of $G$.
(3) All cosets have same cardinality (number of elements)

$G$




"Cosets slice up $G$ like a pie".

<u>Theorem</u> (Lagrange) Let $G$ be a finite group, $H \leq G$ a subgroup. Then $|H|$ divides $|G|$, and $\frac{|G|}{|H|}$ = # of left cosets of $H$ in $G$.

<u>Proof</u>: Pick $a_1, \dots, a_k \in G$ such that $a_i H \cap a_j H = \emptyset$ for $i \neq j$. And such that $G = \bigcup_{i=1}^{k} a_i H$.

$$\text{Then } |G| = \sum_{i=1}^{k} |a_i H| = \sum_{i=1}^{k} |H| = k|H|. \qquad \blacksquare$$

since all cosets have same cardinality as $eH = H$

<u>Definition</u>: The number of distinct cosets of $H$ in $G$ is called the <u>index of $H$ in $G$</u>, denoted $[G:H]$

Thus if $|G| < \infty$, $[G:H] = \frac{|G|}{|H|}$.

<u>NB</u>: If $G$ and $H$ are infinite, $[G:H]$ may be finite or infinite:

<u>Example</u>: $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\} \leq \mathbb{Z}$ what are cosets?

$a + n\mathbb{Z} = \{a + kn \mid k \in \mathbb{Z}\} = [a]$ is a coset!

So "cosets" are "congruence classes modulo $n$".

The set of cosets is $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$

So $[\mathbb{Z} : n\mathbb{Z}] = |\mathbb{Z}_n| = n$.

**Corollary** Let $p$ be a prime and $G$ a group of order $p$. Then $G$ is cyclic and has no subgroups other than $\{e\}$, $G$.

**Proof:** If $H \leq G$ is a subgroup, $|H| \,\big|\, |G| = p$, so $|H| = 1$ or $|H| = p$ then $H = \{e\}$ or $H = G$.
Let $a \in G$ $a \neq e$. Then $\langle a \rangle \leq G$, and $\langle a \rangle \neq \{e\}$, so $\langle a \rangle = G$, and $G$ is cyclic.

**Corollary:** If $G$ is a finite group, and $a \in G$, then $o(a) \,\big|\, |G|$.
**Proof:** $o(a) = |\langle a \rangle|$ divides $|G|$.