Recall: S_n is the group of permutations on n objects, i.e. the collection of bijective functions from the set of n objects to itself.

Theorem: (Cayley's Theorem) Let G be a group w/ $\#G = n$. Then G is isomorphic to a subgroup of S_n.

Proof. Goal is to find an injective homomorphism $\varphi: G \longrightarrow S_n$. We get $G \cong \operatorname{im}\varphi = \varphi(g)$, which is a subgroup of S_n. From recall, our n objects are the n elements of the group $\{g_1, g_2, \ldots, g_n\}$.

For $g \in G$, define $L_g: G \longrightarrow G$, $h \longmapsto gh$.

Claim: L_g is a permutation of G, i.e. a bijective function.

$\rightarrow$ Let $h_1, h_2 \in G$. Assume $L_G(h_1) = L_G(h_2)$. So $gh_1 = gh_2$, and since G is a group, $g^{-1} \in G$. Hence $g^{-1}gh_1 = g^{-1}gh_2$ i.e. $h_1 = h_2$. Thus L_G is injective.

$\rightarrow$ Let $h \in G$. Observe $g^{-1}h \in G$ and $L_G(g^{-1}h) = g(g^{-1}h) = h$. Thus L_G is surjective.

We have a map $\varphi: G \longrightarrow S_n$, $g \longmapsto L_g$.
Let $g_1, g_2 \in G$. W.T.S. $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$.
We have $\varphi(g_1 g_2) = L_{g_1 g_2}$ and $\varphi(g_1) \circ \varphi(g_2) = L_{g_1} \circ L_{g_2}$.
W.T.S. these two functions are equal. Let $h \in G$. We have $L_{g_1 g_2}(h) = (g_1 g_2)h$ and $(L_{g_1} \circ L_{g_2})(h) = L_{g_1}(L_{g_2}(h))$ $= L_{g_1}(g_2 h) = g_1 g_2 h$. Thus $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$, i.e. φ is a homomorphism.

It only remains to show φ is injective. Let $g \in \operatorname{Ker}\varphi$. So $\varphi(g) = id_{S_n}$ = identity in S_n = identity map.

$S_n = \{\varphi: G \to G \mid \varphi \text{ is bijective}\}$, $id(g) = g$.

So that means L_G is the identity map. So for any $h \in G$, $L_G(h) = h$. But then $gh = h$ for every $h \in G$. So g is the identity of G. Thus $\operatorname{Ker}\varphi = \{e_G\}$ i.e. φ is injective.
Since φ is a mapping between two groups of equal order, φ is also a surjection. So $\varphi: G \xrightarrow{\sim} \operatorname{Im}(\varphi) \leq S_n$. $\square$

Exercise: 1) Prove $\operatorname{im}\varphi = \{\varphi(g) \in H : g \in G\}$ is a subgroup of H if $\varphi: G \to H$ is a homomorphism.

$\operatorname{im}\varphi \neq \emptyset$ since $\varphi(e_G) \in \operatorname{im}\varphi$.

Let $h_1, h_2 \in \operatorname{im}\varphi$. $\exists g_1, g_2 \in G$ so that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. Note $h_1 h_2^{-1} = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_2^{-1})$

$= \varphi(g_1 g_2^{-1}) \in \operatorname{Im}\varphi$.

2) What subgroup in S_4 is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?

Check draft.

Example: Consider $G = \mathbb{Z}$, $H = n\mathbb{Z}$. Know $n\mathbb{Z} \subseteq \mathbb{Z}$.

$$\mathbb{Z}/n\mathbb{Z} = G/H = \{[a]_n : 0 \leq a \leq n\}, \quad [a]_n = \{b \in \mathbb{Z} : n \mid (a-b)\}$$
$$= \{b \in \mathbb{Z} : b = a + nk, k \in \mathbb{Z}\}$$
$$= \{a + nk : k \in \mathbb{Z}\}$$
$$= a + n\mathbb{Z}.$$

So
$$\mathbb{Z}/n\mathbb{Z} = G/H = \{a + n\mathbb{Z} : 0 \leq a \leq n-1\}$$
$$= \{g + H : 0 \leq g \leq n-1\}.$$

$\longrightarrow$ $\underbrace{a + n\mathbb{Z}}_{=[a]_n} = \underbrace{b + n\mathbb{Z}}_{=[b]_n}$ iff $n \mid (a-b)$ iff $a - b \in n\mathbb{Z}$.

$a \equiv b \pmod{n}$
$a - b \equiv 0 \pmod{n}$
$n \mid a - b$

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

- A left coset of H is a set of the form $gH = \{gh : h \in H\}$ for $g \in G$.
- A right coset of H " " $Hg = \{hg : h \in H\}$ "
- Denote the collection of left cosets as G/H and right cosets by $H\backslash G$.