Subgroup. G is a group.

Recall: $\phi \neq H \subset G$ is a subgroup if H is closed under multiplication and inverse.

More examples:

- subgroups of $(\mathbb{Z}, +)$

  Let n be a positive integer. The subset $n\mathbb{Z}$ is the set of integers divisible by n.
  $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$

- $G = S_n$, consider H consisting of all the permutations that fix n.

  H is a subgroup.

  $H = \{ \sigma \in Perm(n) \mid \sigma(n) = n \}$.

  ① $H \neq \phi$ because $e \in H$.

  ② $\forall\ \sigma_1, \sigma_2 \in H$,

  $\sigma_1 \cdot \sigma_2 (n) = \sigma_1(\sigma_2(n)) = \sigma_1(n) = n$.

  $\Rightarrow \sigma_1 \sigma_2 \in H$.

③ $\forall \sigma \in H$, $\sigma^{-1}(n) = m$.

m is the unique element in $\{1, \dots n\}$ such that $\sigma(m) = n$. Since $\sigma(n) = n$, $\Rightarrow m = n$.

So $\sigma^{-1} \in H$.

H is isomorphic to S_{n-1}

The elements in H are essentially permutations of $\{1, 2, \dots n-1\}$.

$$\rho: H \longrightarrow S_{n-1}$$

$$\sigma \longrightarrow \sigma\Big|_{\{1,2,\dots n-1\}} : \{1,2,\dots n-1\} \to \{1,2\dots n-1\}$$

restriction of σ to the subset $\{1, 2, \dots n-1\}$.

$|H| = (n-1)!$

$|G| = n!$ $\qquad (n-1)! \mid n!$

In other words, we can view Perm $(n-1)$ as a subgroup S_n .
(G)

• $(\mathbb{Z}/n\mathbb{Z}, +)$ Let m be a positive integer dividing n. The subset $H = \{\overline{mk} \mid k = 0, 1, \dots \frac{n}{m} - 1\}$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$. $|H| = \frac{n}{m}$. $|G| = n$.

$\frac{n}{m} \mid n$

Thm: Let G be a finite group and $H \subset G$ a subgroup.

(group with finitely many elements)

Then the number of elements divides the number of elements in G. $(|H| \mid |G|)$.

In the proof of this theorem. we need another important construction the set of cosets. G/H. $H \subset G$ subgroup.

Defn (coset). A right H-coset in G is a subset of G with the form

$gH = \{g \cdot h \mid h \in H\}$ for some $g \in G$.

In other words, g_1, g_2 are in the same coset iff $g_1^{-1} g_2 \in H$.

if and only if.

Example: $G = \mathbb{Z}$, $H = n\mathbb{Z}$, $g = k \in \mathbb{Z}$.

So the right coset $k + n\mathbb{Z}$

$= \{k + m \mid m \in n\mathbb{Z}\} = \{k + ln \mid l \in \mathbb{Z}\}$.

$= \{x \in \mathbb{Z} \mid x \equiv k \mod n\}$.

We can get $\underbrace{0 + n\mathbb{Z} = n\mathbb{Z},\ 1 + n\mathbb{Z},\ \ldots\ (n-1) + n\mathbb{Z}}_{n \text{ different right cosets.}}$

<u>Why "iff"</u>.

If $g_1, g_2 \in G$, satisfies $g_1^{-1} g_2 \in H$.

Then. we look at coset $g_1 H$.

$g_1 = g_1 \cdot e \in g_1 H$

$g_2 = (g_1 \cdot g_1^{-1}) \cdot g_2 = g_1 \underbrace{(g_1^{-1} g_2)}_{\uparrow \text{ in } H.} \in g_1 H$.

"Only if": if $g_1, g_2 \in gH$. then

$g_1 = g h_1$ for some $h_1 \in H$

$g_2 = g h_2$ for some $h_2 \in H$.

$$g_1^{-1} g_2 = (g h_1)^{-1} \cdot g h_2 = h_1^{-1} g^{-1} g h_2 = h_1^{-1} h_2$$

$h_1^{-1} h_2$ is in H.

Remark: $(gh)^{-1} = h^{-1} g^{-1}$.

Pf: $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1}$
$= g \cdot e \cdot g^{-1} = g \cdot g^{-1}$
$= e$

$(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g) \cdot h$
$= h^{-1} \cdot e \cdot h = h^{-1}h$
$= e$.

Example $H \subset S_n$ is the subgroup of permutations fixing n.

There are n different right H-cosets.

They are $X_m = \{ \sigma \in \mathrm{Perm}(n) \mid \sigma(n) = m \}$

$m = 1, 2, \cdots n$.

Pick $\sigma \in X_m$. We want to prove.

$\tau \in X_m$ if and only if $\tau = \sigma \cdot h$ for some $h \in H$.

"if". $\tau = \sigma h$, $h \in H$,

$\Rightarrow$ $\tau(n) = \sigma(h(n)) = \sigma(n) = m$.

"only if". $\tau \in X_m$. $\tau = \sigma \cdot (\sigma^{-1} \tau)$

define $h = \sigma^{-1} \tau$. $h(n) = \sigma^{-1}(\tau(n))$

$= \sigma^{-1}(m)$

$\sigma(n) = m \Rightarrow$ $= n$.

$\Rightarrow h \in H$

Defn: The set of all right H-cosets form a new set G/H.

$H \subset \text{perm}(n)$. $G/H = \{X_1, X_2 \cdots X_n\}$.

$|G/H| = n$. $n \cdot (n-1)! = n!$

Thm (Lagrange). $|G| = |H| \cdot |G/H|$.

pf: ① Claim: all the right cosets have the same number of elements.

There is a bijection between H and gH

$$f: H \longrightarrow gH.$$
$$h \longmapsto gh.$$

surjective from definition of gH.

injective because. $h_1, h_2 \in H$, if $gh_1 = gh_2$.

then $g^{-1}gh_1 = g^{-1}gh_2 \Rightarrow h_1 = h_2$.

② G is the disjoint union of all the right H-cosets.

If $g_1H \cap g_2H \neq \phi$. take $g \in g_1H \cap g_2H$

$\Rightarrow$ $g_1 . g \in g_1H \Rightarrow g_1^{-1}g \in H$.

$\Rightarrow \quad g_2, g \in g_2 H. \Rightarrow g_2^{-1} g \in H.$

$$\Rightarrow \quad g_1^{-1} g_2 = g_1^{-1} g g^{-1} g_2$$

$$= (g_1^{-1} g) \cdot (g_2^{-1} g)^{-1} \in H$$

$$\Rightarrow \quad g_1 H = g_2 H.$$

$$G = \bigsqcup_{gH \in G/H} gH \quad \Rightarrow \quad |G| = |H| \cdot |G/H|.$$

Products

Defn: Let G_1, G_2 be two groups. Consider the set of pairs $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$. It has a natural group structure by component-wise products.

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 h_1, g_2 h_2).$$

Identity element $= (e_1, e_2)$. e_1 unit in G_1, e_2 unit in G_2.

$$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$$

$G_1 \times G_2$ is called the product of G_1 and G_2.

We have the same definition for products of several groups $G_1, G_2, \dots G_n$.

$$G_1 \times G_2 \times \cdots \times G_n.$$

Example: Pick two positive integers n_1, n_2. $n = n_1 + n_2$. Product group $Perm(n_1) \times Perm(n_2)$ is isomorphic to a subgroup of $Perm(n)$

$$H = \{ \sigma \in Perm(n) \mid \sigma \text{ maps } \{1, \dots n_1\} \text{ to } \{1, \dots n_1\} \text{ itself} \}$$

σ also maps $\{n_1+1 \cdots n_1+n_2\}$ to itself.

$$\rho : H \longrightarrow Perm(n_1) \times Perm(n_2)$$

$$\sigma \longmapsto (\sigma|_{\{1,\dots n_1\}}, \sigma|_{\{n_1+1, \dots n_1+n_2\}})$$

From Lagrange. $|H| = n_1! \cdot n_2!$

$$\text{Perm}(n) = n!$$

$$\Rightarrow \quad \frac{(n_1+n_2)!}{n_1!\, n_2!} \text{ is an integer.}$$

and it is equal to $|G/H|$.

Q: Find an enumeration proof of $|G/H| = \binom{n}{n_1}$