Cosets and Lagrange's Theorem

Def. Let H be a subgroup of G. The subset $aH = \{ah | \ h \in H\}$, where $a \in G$ is called the **left coset** of H containing a.

The subset $Ha = \{ha | \ h \in H\}$, where $a \in G$ is called the **right coset** of H containing a.

Ex. Find the left cosets and right cosets of the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$.

$$4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}.$$

The left coset containing $m \in \mathbb{Z}$ is set

$$m + 4\mathbb{Z} = \{\dots, m-12, m-8, m-4, m, m+4, m+8, m+12, \dots\}$$

$m = 0$: $0 + 4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$

$m = 1$: $1 + 4\mathbb{Z} = \{\dots, 1-12, 1-8, 1-4, 1, 1+4, 1+8, 1+12, \dots\}$

$= \{\dots, -11, -7, -3, 1, 5, 9, 13, \dots\}$

$m = 2$: $2 + 4\mathbb{Z} = \{\dots, -10, -6, -2, 2, 6, 10, 14, \dots\}$

$m = 3$: $3 + 4\mathbb{Z} = \{\dots, -9, -5, -1, 3, 7, 11, 15, \dots\}$

$m = 4$: $4 + 4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$

So the left cosets start repeating. Thus there are 4 distinct left cosets:
$4\mathbb{Z}$, $1 + 4\mathbb{Z}$, $2 + 4\mathbb{Z}$, and $3 + 4\mathbb{Z}$.

Notice that cosets are either identical to another coset or disjoint (they have no common elements) and the union of the disjoint cosets is exactly the group $\mathbb{Z}$. This is a feature of all cosets of a subgroup. This is called a **partition** of a group into the cosets of a subgroup. The cosets aH and bH will either be the same (e.g. $0 + 4\mathbb{Z}$ and $4 + 4\mathbb{Z}$) or disjoint (e.g. $(0 + 4\mathbb{Z}) \cap (1 + 4\mathbb{Z}) = \phi$) and the union of all disjoint cosets is the original set G.

Notice that $\mathbb{Z}, +$ is an abelian group. Thus the left coset $m + 4\mathbb{Z}$ and the right coset $4\mathbb{Z} + m$ are the same sets. So all of the left cosets are the same as the right cosets. If G is not abelian aH need not be the same as Ha (although it might be).

Ex. Find the partition of $\mathbb{Z}_6$ into cosets of the subgroup $H = \{0,3\}$.

Left (or right since $\mathbb{Z}_6$ is abelian) cosets of H will be of the form:

$m + H$ where $m \in \mathbb{Z}_6$.

$m = 0$: $0 + H = \{0, 3\} = H$ (the set H is always a coset associated with the identity element in G)

$m = 1$: $1 + H = \{1, 4\}$

$m = 2$: $2 + H = \{2, 5\}$

$m = 3$: $3 + H = \{3, 0\} = \{0, 3\} = H$

$m = 4$: $4 + H = \{4, 1\} = 1 + H$

$m = 5$: $5 + H = \{4, 2\} = 2 + H$

So $0 + H,\ 1 + H,\ 2 + H$ are the three distinct and disjoint cosets of H and notice that:

$\mathbb{Z}_6 = \{0 + H\} \cup \{1 + H\} \cup \{2 + H\} = \{0,3\} \cup \{1, 4\} \cup \{2, 5\}$.

Notice that all of the cosets of H have the same number of elements as H. This is always the case.

Ex. Let $G = S_3$ and H be the subgroup $\{\rho_0, \mu_2\}$ where:

$$\rho_0 = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} \qquad \mu_1 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

$$\rho_1 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} \qquad \mu_2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

$$\rho_2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} \qquad \mu_3 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

Find the partitions of S_3 into left cosets and right cosets.

Left cosets: $H = \{\rho_0, \mu_2\}$

$$\rho_1 H = \{\rho_1\rho_0, \rho_1\mu_2\} = \{\rho_1, \mu_1\}$$

Since $\rho_1\mu_2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} = \mu_1$

$$\rho_2 H = \{\rho_2\rho_0, \rho_2\mu_2\} = \{\rho_2, \mu_3\}$$

Since $\rho_2\mu_2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = \mu_3$

Notice $\mu_1 H = \{\rho_1, \mu_1\}$ since

$\mu_1\mu_2 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \rho_1$

$\mu_2 H = \{\rho_0, \mu_2\}$ since

$\mu_2^2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = \rho_0$

and $\mu_3 H = \{\rho_2, \mu_3\}$ since

$\mu_3\mu_2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \rho_2$

So $S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\} = \{\rho_0, \mu_2\} \cup \{\rho_1, \mu_1\} \cup \{\rho_2, \mu_3\}$.

The right cosets are:

$H = \{\rho_0, \mu_2\}, \quad H\rho_1 = \{\rho_0\rho_1, \mu_2\rho_1\} = \{\rho_1, \mu_3\}, \quad H\rho_2 = \{\rho_0\rho_2, \mu_2\rho_2\} = \{\rho_2, \mu_1\}$

and $S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\} = \{\rho_0, \mu_2\} \cup \{\rho_1, \mu_3\} \cup \{\rho_2, \mu_1\}.$

Notice that the right cosets apart from H are different from the left cosets. However, the number of left cosets is the same as the number of right cosets (which will always be the case) and the number of elements in any coset is the same as the number of elements in H.

Lagrange's Theorem: Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

This follows from the fact that the cosets (left or right) form a partition of G (i.e. G is the union of disjoint cosets) and each coset has the same number of elements as H.

All cosets have the same number of elements as H because:

$\phi: H \to gH; \ \ g \in G$ by

$\phi(h) = gh$ is 1-1 and onto.

It's 1-1 because if:

$$\phi(h_1) = \phi(h_2)$$
$$gh_1 = gh_2$$
$$g^{-1}gh_1 = g^{-1}gh_2$$
$$h_1 = h_2.$$

It's onto because given any element $gh \in gH, \ \ \phi(h) = gh.$

Corollary: If $|G| = p$, a prime number, then G is cyclic.

Proof: Assume $|G| = p$, a prime number.

Let $a \in G$ with $a \neq e$.

Then the cyclic subgroup generated by a, $< a >$ has at least 2 elements, a and e. By Lagrange's Theorem the order of $< a >$ must divide $|G| = p$. That means $|< a >| = p$ and G is cyclic.

Theorem: The order of an element of a finite group divides the order of the group

Proof: The order of an element $a \in G$ is the order of the cyclic subgroup generated by a.

Thus by Lagrange's Theorem the order of a must divide the order of G.

Def. $H \leq G$. The number of left (or right) cosets of H in G is the **index** of H in G, written $(G: H)$.

Ex. Let $G = S_3$ and $H = \{\rho_0, \mu_2\}$. The number of cosets of H in G was 3 (which equals $\frac{|G|}{|H|}$). So the index of H in G is 3.

The index of H in G may be finite or infinite. However, If G is finite then:

$$(G: H) = \frac{|G|}{|H|}.$$

Ex. Let $G = \mathbb{Z}$ and $H = 4\mathbb{Z}$. As we saw earlier, H has 4 cosets in $\mathbb{Z}$ so $(G:H) = 4$.

Ex. Let $G = \mathbb{R}$ and $H = \mathbb{Z}$, then $(G:H)$ is infinite since $m\sqrt{2} + \mathbb{Z}$ are distinct cosets when $m \in \mathbb{Z}$ and $m\sqrt{2} \in \mathbb{R}$.