We apply the concept of congruence in the group setting.
Although will use the multiplicative notation for the binary operation in a group, the additive version of congruence is similar.

**Definition.** Let $K$ be a subgroup of a group $G$. For $a, b \in G$, we say that $a$ is congruent to $b$ modulo $K$, written $a \equiv b \pmod{K}$, if $ab^{-1} \in K$.
Otherwise, $a$ is not congruent to $b$, written $a \not\equiv b \pmod{K}$.

**Example.** For the group $D_4$ and the subgroup $K = \{r_0, r_1, r_2, r_3\}$ (the rotations), the element $d$ is congruent to $h$ (two reflections, the first across the $x$-axis, the second across the line $y = x$) because $dh^{-1} = dh = r_3 \in K$.
The element $r_1$ is congruent to $v$ (reflection across the line $y = -x$) because $r_1v^{-1} = r_1v = d \not\in K$.

Congruence in a group modulo a subgroup is an equivalence relation.

**Theorem 8.1.** For a subgroup $K$ of a group $G$, congruence modulo $K$ is
(1) reflexive: $a \equiv a \pmod{K}$ for all $a \in G$,
(2) symmetric: $a \equiv b \pmod{K}$ implies $b \equiv a \pmod{K}$, and
(3) transitive: $a \equiv b \pmod{K}$ and $b \equiv c \pmod{K}$ implies $a \equiv c \pmod{K}$.

**Proof.** (1) Since $aa^{-1} = e \in K$, we have $a \equiv a \pmod{K}$.
(2) If $a \equiv b \pmod{K}$, then $ab^{-1} \in K$, and since $K$ is a subgroup, the inverse $(ab^{-1})^{-1} \in K$, whence $ba^{-1} = (ab^{-1})^{-1} \in K$, so that $b \equiv a \pmod{K}$.
(3) If $a \equiv b \pmod{K}$ and $b \equiv c \pmod{K}$, then $ab^{-1} \in K$ and $bc^{-1} \in K$, and since $K$ is a subgroup, the product $(ab^{-1})(bc^{-1}) = ac^{-1}$ is in $K$, so that $a \equiv c \pmod{K}$. □

We may therefore talk about the equivalence classes in $G$ for congruence modulo $K$.

**Definitions.** For a subgroup $K$ of a group $G$, the congruence class of $a \in G$ modulo $K$ is
$$\{b \in G : a \equiv b \pmod{K}\} = \{b \in G : ba^{-1} \in K\}.$$ 
For $ba^{-1} \in K$, there is $k \in K$ such that $ba^{-1} = k$, which by right multiplication of $a^{-1}$ gives $b = ka$ for some $k \in K$.
The congruence class of $a$ is then
$$\{b \in G : b = ka \text{ for some } k \in K\} = \{ka : k \in K\}.$$ 
The notation we use for the congruence class of $a$ modulo $K$ is the right coset of $a$ is $K a = \{ka : k \in K\}$.

In additive notation, the congruence class of $a$ is $K + a$.

Now we present results about congruence that we have seen before.
Theorem 8.2. For a subgroup $K$ of a group $G$, we have $a \equiv c \pmod{K}$ if and only if $Ka = Kc$.

Corollary 8.3. For a subgroup $K$ of a group $G$, two right cosets of $K$ are either identical or disjoint.

Recall that an equivalence relation on a set partitions the set into nonempty disjoint subsets whose union of the set.

In the group setting, we can say more about the partition given by right cosets.

Theorem 8.4. Let $K$ be a subgroup of a group $G$.

1. $G$ is the union of the right cosets of $K$ in $G$:
   $$G = \bigcup_{a \in G} Ka.$$

2. For each $a \in G$, there is a bijection $f : K \to Ka$, and so each right coset has the same cardinality as $K$.

Proof. (1) Since each right coset $Ka$ is a subset of $G$, we have $\bigcup_{a \in G} Ka \subseteq G$.

So it remains to show the opposite inclusion.

For $b \in G$, we have $eb \in Kb$ where $Kb \subseteq \bigcup_{a \in G} Ka$, and so $G \subseteq \bigcup_{a \in G} Ka$.

(2) Define a map $f : K \to Ka$ by $f(x) = xa$.

Since $Ka = \{ka : k \in K\}$, the map $f$ is surjective.

If $f(x) = f(y)$, then $xa = ya$ which by cancelation implies $x = y$, so that $f$ is injective.

Thus $K$ and $Ka$ have the same cardinality for each $a \in G$. 

We ask how many distinct right cosets of a subgroup $H$ of $G$ are there in $G$?

Definition. For a subgroup $H$ of a group $G$, the number of distinct right cosets of $H$ in $G$ is denoted by $[G : H]$.

If $G$ is a finite group, then there can be only a finite number of right cosets of a subgroup.

If $G$ is an infinite group, then there can be a finite number or and infinite number of right cosets of a subgroup.

Examples. (a) Let $H = \langle 5 \rangle$, the cyclic subgroup of $\mathbb{Z}$.

There are five distinct right cosets of $H$ in $\mathbb{Z}$, namely $H + 0$, $H + 1$, $H + 2$, $H + 3$, and $H + 4$.

So $[\mathbb{Z} : H] = 5$.

(b) Let $H = \mathbb{Z}$ which is a subgroup of $\mathbb{R}$.

For each $a \in [0, 1)$, the right coset $H + a$ is distinct, since the difference any two distinct real numbers in $[0, 1)$ is not an integer.
Thus \( \mathbb{R} : \mathbb{Z} = \infty \).

There is strong connection between the order of a subgroup and the order of a finite group, and it involves the index of the subgroup.

**Lagrange’s Theorem.** If \( K \) is a subgroup of a finite group \( G \), then the order of \( K \) divides the order of \( G \), specifically

\[ |G| = |K| [G : K]. \]

**Proof.** Suppose that \( [G : K] = n \).

There are \( n \) distinct elements \( c_1, c_2, \ldots, c_n \in G \) such that the collection of right cosets \( Kc_1, Kc_2, \ldots, Kc_n \) are pairwise distinct, and hence mutually disjoint by Corollary 8.3.

By Theorem 8.4 we have

\[ \bigcup_{i=1}^{n} Kc_i = G. \]

Since for disjoint sets \( A \) and \( B \) we have \( |A \cup B| = |A| + |B| \) (where \( |A| \) is the cardinality of \( A \)), we have

\[ |G| = |Kc_1| + |Kc_2| + \cdots + |Kc_n|. \]

By Theorem 8.4 we have that \( |Kc_i| = |K| \) for all \( i = 1, 2, \ldots, n \), and so

\[ |G| = \underbrace{|K| + |K| + \cdots + |K|}_{n} = n|K|. \]

Since \( n = [G : K] \) we obtain \( |G| = |K| [G : K] \). \( \square \)

Lagrange’s Theorem tells us that there is only a finite number of possibilities for the orders of subgroups of a finite group.

Warning about Lagrange’s Theorem: just because \( n \) divides the order of \( G \), it does not mean that there is a subgroup of \( G \) of order \( n \).

**Example.** The group \( A_4 \) has order \( 4!/2 = 12 \), but does not have a subgroup of order 6.

Lagrange’s Theorem also limits the orders of elements of a finite group.

**Corollary 8.6.** Let \( G \) be a finite group.

1. The order of \( a \in G \) divides \( |G| \).
2. For each \( a \in G \), we have \( a^k = e \) for \( k = |G| \).

**Proof.**

1. For each \( a \in G \), the order of the cyclic subgroup \( \langle a \rangle \) is the order of \( a \).

By Lagrange’s Theorem \( |\langle a \rangle| \) divides \( |G| \).

2. If \( |G| = k \) and \( |a| = n \), then \( n \mid k \) by part (a).

Thus \( k = nt \) for some \( t \in \mathbb{Z} \), and so

\[ a^k = a^{nt} = (a^n)^t = e^t = e. \]

This holds for any \( a \in G \). \( \square \)