# Cauchy's Theorem in Group Theory

Cauchy's Theorem establishes a useful connection between a group's order and the existence of elements of specific orders.

**Theorem**

If $G$ is a finite group and $p$ is a prime number dividing the order of $G$ (denoted $|G|$), Then $G$ contains an element of order $p$.

Some prelimanaries will be introduced:

(I.) order of an element

↳ the order of an element $g \in G$ is the smallest positive integer $n$ such that $g^n = e$, where $e$ is the identity element of $G$. If no such $n$ exists, $g$ has infinite order.

(II.) group order

↳ Denoted as $|G|$, group order is the number of elements in a group $G$.

(III.) prime divisors

↳ A prime $p$ divides $G$ if there exists an integer $k$ such that $|G| = kp$

(IV.) action of groups

↳ if $G$ acts on a set $X$, there exists a map $G \times X \longrightarrow X$ (the action) such that for all $g, h \in G$ and $x \in X$

(i) $e \cdot x = x$ where $e$ is the identity element of $G$

(ii) $(gh) \cdot x = g \cdot (h \cdot x)$

↳ the action respects the group operation

Necessary results

**Theorem** (Lagrange's)

If $G$ is a finite group and $H$ is a subgroup, then $|H|$ divides $|G|$

**Theorem** (Orbit - Stabilizer)

If $G$ is a group acting on a set $X$ and $x \in X$, then

$$|G| = |O(x)| \cdot |S(x)|$$

where $O(x)$ denotes the orbit of an element $x$, the set of all elements in $X$ that can be reached from $x$ by the action of any element in $G$.

and $S(x)$ denotes the stabilizer of an element $x$, the set of all elements in $G$ that leave $x$ alone under the action

**Definition** (cyclic subgroups)
A cyclic subgroup of group $G$ is a subgroup generated by a single element. In other words, if $g \in G$, then the cyclic subgroup generated by $g$ is the set

$$\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$$

If the order of $g$ is $p$, then $\langle g \rangle$ consists of the elements $\{ e, g, \dots, g^{p-1} \}$

Finally, we prove the result.

**Proof** (Cauchy's Theorem)
Let $G$ be a finite group with order $n$.
$p$ be a prime such that $p \mid n$, i.e. $p$ divides $n$.
We'll aim to show $G$ contains an element of order $p$.
Define a set $X$ consisting of all subsets of $G$ containing $p$ elements.

$$X = \{ A \subseteq G \mid |A| = p \}$$

The size of this set is the number of ways to choose $p$ elements from $n$, namely,

$$|X| = \binom{n}{p} = \frac{n(n-1)\dots(n-p+1)}{p!}$$

This is obviously finite.
Now define a group action of $G$ on the set $X$ by left multiplication.
Specifically, for $g \in G$ and $A \in X$, we have

$$g \cdot A = \{ ga \mid a \in A \}$$

That is, $g$ acts on subset $A$ by multiplying each of its elements from the left by $g$.
A quick observation reveals, this action preserves $|A|$
We now apply the Orbit-Stabilizer Theorem.
By it, the size of the orbit of $A$ is given by

$$|O(A)| = \frac{|G|}{|S(A)|}$$

Since $p$ divides $|G|$, we know from Lagrange's Theorem that the size of the orbit of any subset $A$ must be a divisor of $|G|$.
This implies one of the orbits has size $p$, since $p$ divides $|G|$.

If the size of an orbit is exactly $p$, the elements of it correspond to a cyclic subgroup of $G$ of order $p$. Specifically, there exists $g \in G$ such that the orbit of $\{e\}$ under the action of $G$ consists of the elements $\{e, g, g^2, \ldots, g^{p-1}\}$.

This orbit is cyclic, and $g$ has order $p$, meaning $g^p = e$ and $g^k \neq e$ for $k < p$

Thus, the group $G$ contains an element $g$ of order $p$, as desired. $\blacksquare$