LAGRANGE’S THEOREM

Definition:
An operation on a set $G$ is a function $*: G \times G \to G$.

Definition:
A group is a set $G$ which is equipped with an operation $*$ and a special element $e \in G$, called the identity, such that
(i) the associative law holds: for every $x, y, z \in G$ we have $x * (y * z) = (x * y) * z$;
(ii) $e * x = x = x * e$ for all $x \in G$;
(iii) for every $x \in G$, there is $x' \in G$ (so-called, inverse) with $x * x' = e = x' * x$.

Definition:
A subset $H$ of a group $G$ is a subgroup if
(i) $e \in H$;
(ii) if $x, y \in H$, then $x * y \in H$;
(iii) if $x \in H$, then $x^{-1} \in H$.

Definition:
If $G$ is a group and $a \in G$, write
$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\text{all powers of } a\};$$
$\langle a \rangle$ is called the cyclic subgroup of $G$ generated by $a$.

Definition:
A group $G$ is called cyclic if $G = \langle a \rangle$ for some $a \in G$. In this case $a$ is called a generator of $G$.

Definition:
Let $G$ be a group and let $a \in G$. If $a^k = 1$ for some $k \geq 1$, then the smallest such exponent $k \geq 1$ is called the order of $a$; if no such power exists, then one says that $a$ has infinite order.

Definition:
If $G$ is a finite group, then the number of elements in $G$, denoted by $|G|$, is called the order of $G$.

Theorem:
Let $G$ be a finite group and let $a \in G$. Then
$$\text{order of } a = |\langle a \rangle|.$$ 

Fermat’s Little Theorem:
Let $p$ be a prime. Then $n^p \equiv n \mod p$ for any integer $n \geq 1$. 

1
**Proof (Sketch):** We distinguish two cases.

*Case A:* Let $p \mid n$, then, obviously, $p \mid n^p - n$, and we are done.

*Case B:* Let $p \not\mid n$.

Consider the group $\mathbb{Z}_p^\times$ and pick any $[a] \in \mathbb{Z}_p^\times$. Let $k$ be the order of $[a]$. We know that $\langle [a] \rangle$ is a subgroup of $\mathbb{Z}_p^\times$ and by the Theorem above we obtain

$$|\langle [a] \rangle| = k.$$

**Lemma (Lagrange’s Theorem):**

If $H$ is a subgroup of a finite group $G$, then

$$|H| \text{ divides } |G|.$$

By Lagrange’s Theorem we get

$$|\langle [a] \rangle| \text{ divides } |\mathbb{Z}_p^\times|,$$

which gives

$$k \mid p - 1,$$

since $|\langle [a] \rangle| = k$ and $|\mathbb{Z}_p^\times| = p - 1$. So

$$p - 1 = kd$$

for some integer $d$. On the other hand, since $k$ is the order of $[a]$, it follows that for any $n \in [a]$ we have

$$n^k \equiv 1 \pmod{p},$$

hence

$$n^{kd} \equiv 1^d \equiv 1 \pmod{p},$$

and the result follows, since $kd = p - 1$. ■

**Definition:**

If $H$ is a subgroup of a group $G$ and $a \in G$, then the coset $aH$ is the following subset of $G$:

$$aH = \{ah : h \in H\}.$$

**Remark:**

Cosets are usually not subgroups. In fact, if $a \not\in H$, then $1 \not\in aH$, for otherwise

$$1 = ah \implies a = h^{-1} \not\in H,$$

which is a contradiction.
Example:
Let $G = S_3$ and $H = \{(1), (12)\}$. Then there are 3 cosets:

$$(12)H = \{(1), (12)\} = H,$$

$$(13)H = \{(13), (123)\} = (123)H,$$

$$(23)H = \{(23), (132)\} = (132)H.$$  

Lemma:
Let $H$ be a subgroup of a group $G,$ and let $a, b \in G.$ Then

(i) $aH = bH \iff b^{-1}a \in H.$

(ii) If $aH \cap bH \neq \emptyset,$ then $aH = bH.$

(iii) $|aH| = |H|$ for all $a \in G.$

Proof:

(i) $\Rightarrow$ Let $aH = bH,$ then for any $h_1 \in H$ there is $h_2 \in H$ with $ah_1 = bh_2.$ This gives

$$b^{-1}a = h_2h_1^{-1} \implies b^{-1}a \in H,$$

since $h_2 \in H$ and $h_1^{-1} \in H.$

$\Leftarrow$) Let $b^{-1}a \in H.$ Put $b^{-1}a = h_0.$ Then

$$aH \subseteq bH,$$ since if $x \in aH,$ then $x = ah \implies x = b(b^{-1}a)h = h_0h = bh_1 \in bH;$$

$$bH \subseteq aH,$$ since if $x \in bH,$ then $x = bh \implies x = a(b^{-1}a)^{-1}h = ah_0^{-1}h = ah_2 \in aH.$

So, $aH \subseteq bH$ and $bH \subseteq aH,$ which gives $aH = bH.$

(ii) Let $aH \cap bH \neq \emptyset,$ then there exists an element $x$ with

$$x \in aH \cap bH \implies ah_1 = x = bh_2 \implies b^{-1}a = h_2h_1^{-1} \in H,$$

therefore $aH = bH$ by (i).

(iii) Note that if $h_1$ and $h_2$ are two distinct elements from $H,$ then $ah_1$ and $ah_2$ are also distinct, since otherwise

$$ah_1 = ah_2 \implies a^{-1}ah_1 = a^{-1}ah_2 \implies h_1 = h_2,$$

which is a contradiction. So, if we multiply all elements of $H$ by $a,$ we obtain the same number of elements, which means that $|aH| = |H|.$
Lagrange’s Theorem:
If $H$ is a subgroup of a finite group $G$, then
$$|H| \text{ divides } |G|.$$  

**Proof:**
Let $|G| = t$ and
$$\{a_1H, a_2H, \ldots, a_tH\}$$
be the family of all cosets of $H$ in $G$. Then
$$G = a_1H \cup a_2H \cup \ldots \cup a_tH,$$
because $G = \{a_1, a_2, \ldots, a_t\}$ and $1 \in H$. By (ii) of the Lemma above for any two cosets $a_iH$ and $a_jH$ we have only two possibilities:

$$a_iH \cap a_jH = \emptyset \quad \text{or} \quad a_iH = a_jH.$$  

Moreover, from (iii) of the Lemma above it follows that all cosets have exactly $|H|$ number of elements. Therefore

$$|G| = |H| + |H| + \ldots + |H| \implies |G| = d|H|,$$
and the result follows. ■

**Corollary 1:**
If $G$ is a finite group and $a \in G$, then the order of $a$ is a divisor of $|G|$.  

**Proof:**
By the Theorem above, the order of the element $a$ is equal to the order of the subgroup $H = \langle a \rangle$. By Lagrange’s Theorem, $|H|$ divides $|G|$, therefore the order $a$ divides $|G|$. ■

**Corollary 2:**
If a finite group $G$ has order $m$, then $a^m = 1$ for all $a \in G$.  

**Proof:**
Let $d$ be the order of $a$. By Corollary 1, $d \mid m$; that is, $m = dk$ for some integer $k$. Thus,

$$a^m = a^{dk} = (a^d)^k = 1.$$  

**Corollary 3:**
If $p$ is a prime, then every group $G$ of order $p$ is cyclic.  

**Proof:**
Choose $a \in G$ with $a \neq 1$, and let $H = \langle a \rangle$ be the cyclic subgroup generated by $a$. By Lagrange’s Theorem, $|H|$ is a divisor of $|G| = p$. Since $p$ is a prime and $|H| > 1$, it follows that

$$|H| = p = |G|,$$
and so $H = G$, as desired. ■
Definition:
An operation on a set $G$ is a function $*: G \times G \rightarrow G$.

Definition:
A group is a set $G$ which is equipped with an operation $*$ and a special element $e \in G$, called the identity, such that

(i) the associative law holds: for every $x, y, z \in G$ we have $x*(y*z) = (x*y)*z$;
(ii) $e*x = x = x*e$ for all $x \in G$;
(iii) for every $x \in G$, there is $x' \in G$ (so-called, inverse) with $x*x' = e = x'*x$. 
**Definition:**
A subset $H$ of a group $G$ is a **subgroup** if

(i) $e \in H$;
(ii) if $x, y \in H$, then $x \ast y \in H$;
(iii) if $x \in H$, then $x^{-1} \in H$. 
Definition:
If $G$ is a group and $a \in G$, write
$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\text{all powers of } a\}$; 
$\langle a \rangle$ is called the cyclic subgroup of $G$ generated by $a$.

Definition:
A group $G$ is called cyclic if $G = \langle a \rangle$ for some $a \in G$. In this case $a$ is called a generator of $G$. 
**Definition:**
Let $G$ be a group and let $a \in G$. If $a^k = 1$ for some $k \geq 1$, then the smallest such exponent $k \geq 1$ is called the order of $a$; if no such power exists, then one says that $a$ has infinite order.

**Definition:**
If $G$ is a finite group, then the number of elements in $G$, denoted by $|G|$, is called the order of $G$. 
Theorem:
Let $G$ be a finite group and let $a \in G$. Then
order of $a = |\langle a \rangle|$.

Fermat’s Little Theorem:
Let $p$ be a prime. Then $n^p \equiv n \pmod{p}$ for any integer $n \geq 1$. 
Proof (Sketch): We distinguish two cases.

Case A: Let $p \mid n$, then, obviously, $p \mid n^p - n$, and we are done.
Case B: Let

\[ p \nmid n. \]

Consider the group \( \mathbb{Z}_p^\times \) and pick any \([a] \in \mathbb{Z}_p^\times\). Let \( k \) be the order of \([a]\). We know that \( \langle [a] \rangle \) is a subgroup of \( \mathbb{Z}_p^\times \) and by the Theorem above we obtain

\[ |\langle [a] \rangle| = k. \]

Lemma (Lagrange’s Theorem):

If \( H \) is a subgroup of a finite group \( G \), then

\[ |H| \text{ divides } |G|. \]
By Lagrange’s Theorem we get

\[ |\langle [a] \rangle| \text{ divides } |\mathbb{Z}_p^\times|, \]

which gives

\[ k \mid p - 1, \]

since \( |\langle [a] \rangle| = k \) and \( |\mathbb{Z}_p^\times| = p - 1 \). So

\[ p - 1 = kd \]

for some integer \( d \). On the other hand, since \( k \) is the order of \([a]\), it follows that for any \( n \in [a] \) we have

\[ n^k \equiv 1 \mod p, \]

hence

\[ n^{kd} \equiv 1^d \equiv 1 \mod p, \]

and the result follows, since \( kd = p - 1 \). ■
Definition:
If \( H \) is a subgroup of a group \( G \) and \( a \in G \), then the coset \( aH \) is the following subset of \( G \):
\[
aH = \{ ah : h \in H \}.
\]

Remark:
Cosets are usually not subgroups. In fact, if \( a \not\in H \), then \( 1 \not\in aH \), for otherwise
\[
1 = ah \implies a = h^{-1} \not\in H,
\]
which is a contradiction.
Example:
Let $G = S_3$ and $H = \{(1), (12)\}$. Then there are 3 cosets:

$(12)H = \{(1), (12)\} = H,$

$(13)H = \{(13), (123)\} = (123)H,$

$(23)H = \{(23), (132)\} = (132)H.$
Lemma:
Let $H$ be a subgroup of a group $G$, and let $a, b \in G$. Then

(i) $aH = bH \iff b^{-1}a \in H$.

(ii) If $aH \cap bH \neq \emptyset$, then $aH = bH$.

(iii) $|aH| = |H|$ for all $a \in G$. 
Proof:
(i) \( \Rightarrow \) Let \( aH = bH \), then for any \( h_1 \in H \) there is \( h_2 \in H \) with \( ah_1 = bh_2 \). This gives
\[
b^{-1}a = h_2h_1^{-1} \implies b^{-1}a \in H,
\]
since \( h_2 \in H \) and \( h_1^{-1} \in H \).
\(\Leftarrow\) Let \(b^{-1}a \in H\). Put \(b^{-1}a = h_0\). Then

\[
aH \subset bH, \text{ since if } x \in aH, \text{ then } x = ah
\]

\[
\Downarrow
\]

\[
x = b(b^{-1}a)h = bh_0h = bh_1 \in bH
\]

and

\[
bH \subset aH, \text{ since if } x \in bH, \text{ then } x = bh
\]

\[
\Downarrow
\]

\[
x = a(b^{-1}a)^{-1}h = a h_0^{-1}h = ah_2 \in aH.
\]

So, \(aH \subset bH\) and \(bH \subset aH\), which gives \(aH = bH\).
(ii) Let $aH \cap bH \neq \emptyset$, then there exists an element $x$ with

$$x \in aH \cap bH$$

$$\Downarrow$$

$$ah_1 = x = bh_2$$

$$\Downarrow$$

$$b^{-1}a = h_2h_1^{-1} \in H,$$

therefore $aH = bH$ by (i).
(iii) Note that if \( h_1 \) and \( h_2 \) are two distinct elements from \( H \), then \( ah_1 \) and \( ah_2 \) are also distinct, since otherwise

\[
\begin{align*}
ah_1 &= ah_2 \\
\downarrow \\
 a^{-1}ah_1 &= a^{-1}ah_2 \\
\downarrow \\
 h_1 &= h_2,
\end{align*}
\]

which is a contradiction. So, if we multiply all elements of \( H \) by \( a \), we obtain the same number of elements, which means that \(|aH| = |H|\). ■
Lagrange’s Theorem:
If $H$ is a subgroup of a finite group $G$, then

$|H|$ divides $|G|$. 
Proof:
Let \(|G| = t\) and 
\[ \{a_1H, a_2H, \ldots, a_tH\} \]
be the family of all cosets of \(H\) in \(G\). Then 
\[ G = a_1H \cup a_2H \cup \ldots \cup a_tH, \]
because \(G = \{a_1, a_2, \ldots, a_t\}\) and \(1 \in H\). By (ii) of the Lemma above for any two cosets \(a_iH\) and \(a_jH\) we have only two possibilities:
\[ a_iH \cap a_jH = \emptyset \quad \text{or} \quad a_iH = a_jH. \]
Moreover, from (iii) of the Lemma above it follows that all cosets have exactly \(|H|\) number of elements. Therefore 
\[ |G| = |H| + \ldots + |H| \quad \iff \quad |G| = d|H|, \]
and the result follows. ■
**Corollary 1:**

If $G$ is a finite group and $a \in G$, then the order of $a$ is a divisor of $|G|$.

**Proof:**

By the Theorem above, the order of the element $a$ is equal to the order of the subgroup

$$H = \langle a \rangle.$$

By Lagrange’s Theorem, $|H|$ divides $|G|$, therefore the order $a$ divides $|G|$. ■
Corollary 2:
If a finite group $G$ has order $m$, then

$$a^m = 1$$

for all $a \in G$.

Proof:
Let $d$ be the order of $a$. By Corollary 1, $d \mid m$; that is,

$$m = dk$$

for some integer $k$. Thus,

$$a^m = a^{dk} = (a^d)^k = 1.$$
Corollary 3:

If $p$ is a prime, then every group $G$ of order $p$ is cyclic.

Proof:

Choose $a \in G$ with $a \neq 1$, and let

$$H = \langle a \rangle$$

be the cyclic subgroup generated by $a$. By Lagrange’s Theorem, $|H|$ is a divisor of $|G| = p$. Since $p$ is a prime and $|H| > 1$, it follows that

$$|H| = p = |G|,$$

and so $H = G$, as desired. ■