$\exists q, t \in Z$ such that $r = mq + t; 0 \leq t < m$
$w = a^r = a^{mq+t} = a^{mq}a^t = (a^m)^q a^t = e.a^t = a^t, t < m$
so $w \in S$, hence $G \subseteq S$. But $O(G) = n$
Thus $n = m$

Corollary:

(1) Let $G = \langle a \rangle$ of order n , then n the smallest positive integer such that $a^n = e$.
(2) Let $G = \langle a \rangle$, if $0(G) = n$ and $a^m = e$, then $n \setminus m$.

Proof: (2)
Applying to the "Division Algorithm", there exist integers q and r such that $m = q_n^n + r$, where $0 \leq r < n$. Thus

$$= (a^n)^q a^r = a^r = a^m = a^{nq+r} = e$$

$$a^m = a^{nq+r}$$

Since n is the smallest positive integer such that $a^n = e, := (a^4)^q a^r$ implies that $r = 0$, hence $m = qn$ or equivalently $n/m_- = e \cdot a^r$

Definition:

Let G be a
Let G be a group and $a \in G$, the order of a is the -order of

Example:

$Z_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$
$0(\overline{5}) = 0 < \overline{5} >= \{\overline{5}, \overline{4}, \overline{3}, \overline{2}, \overline{1}, \overline{0}\} = 6$
$0(\overline{1}) = 6$
$0(\overline{2}) = 0 < \overline{2} >= \{\overline{2}, \overline{4}, \overline{0}\} = 3$
$0(\overline{3}) = \{\overline{3}, \overline{0}\} = 2$

Definition:

Let H and K be a nonempty sugroups of a group G the product of H and K denoted by HK is the set $HK = \{hk: h \in H, k \in K\}$.
In case $H = \{a\}$, then $\{a\}K = aK = \{ak: k \in K\}$

Example:

$G = S_3$, let $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$

$K = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$

$HK = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$

$KH = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$

$HK \neq KH$

Q:Is HK a subgroup of G

HK is not subgroup since

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \notin HK$$

Example:

Let L be a subgroup

$$L = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

KL

$= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -i & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$

LK

$= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$

HL

$= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$

LH

$= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$

Corollary:

(1) Let $G = \langle a \rangle$ of order n , then n the smallest positive integer such that $a^n = e$.

(2) Let $G = \langle a \rangle$, if $0(G) = n$ and $a^m = e$, then $n \setminus m$.

Proof:
Appling to the "Division Algorithm", there exist integers q and r such that $m = qn + r$, where $0 \leq r < n$. Thus

$$e = a^m = a^{nq+r} = (a^n)^q \cdot a^t = a^r$$

Since n is the smallest positive integer such that $a^n = e$, implies that $r = 0$, hence $m = qn$ or equivalently $n \setminus m$

Definition: Let G be a group and $a \in G$, the order of a is the order of $< a >$.

Example: $Z_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$
$0(\overline{5}) = 0 < \overline{5} >= \{\overline{5}, \overline{4}, \overline{3}, \overline{2}, \overline{1}, \overline{0}\} = 6$
$0(\overline{1}) = 6$
$0(\overline{2}) = 0 < \overline{2} >= \{\overline{2}, \overline{4}, \overline{0}\} = 3$
$0(\overline{3}) = \{\overline{3}, \overline{0}\} = 2$
Definition: Let H and K be a nonempty subsets of a group G the product of H and K denoted by HK is the set $HK = \{hk: h \in H, k \in K\}$ in case $H = \{a\}$, then $\{a\}K = aK = \{ak: k \in K\}$
Example: $G = S_3$, let $H = \left\{\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}\right\}$
$K = \left\{\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}\right\}$
$HK = \left\{\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}\right\}$
$KH = \left\{\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix}\right\}$
$HK \neq KH$
Q:Is HK a subgroup of G

HK is not subgroup since
$\begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix} \notin HK$
Example:
$L = \left\{\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix}\right\}$, is a subgroup

$KL = \left\{\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}\right\}$
$LK = \left\{\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix}\right\}$

$LH = \left\{\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix} \cdot \begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}\right\}$

$HL = \left\{\begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix}\right\}$

Theorem: Let H and K be subgroups of a group G then HK is subgroup if and only if HK = KH.

Proof: ⇒) let $y \in HK$, HK is subgroup
then $y^{-1} \in HK$, and $y^{-1} = hk, h \in H, k \in K$
$y = (y^{-1})^{-1} = (hk)^{-1} = k^{-1}\, h^{-1}$ (H,K are subgroups)
then $k^{-1} \in K$ and $h^{-1} \in H$
$y = k^{-1}\, h^{-1} \in KH$, then $HK \subseteq KH$
let $x \in KH$, then $x = kh$
$x^{-1} = h^{-1}k^{-1} \in HK$, but HK is subgroup
then $(x^{-1})^{-1} \in HK$, and $x \in HK$
hence $KH \subseteq HK$
thus HK = KH.
⇔)$HK \neq \emptyset$(since $e \in H, e \in K$)
$e = e.\, e \in HK$
Let $a \in HK \Rightarrow a = h_1k_1; h_1 \in H, k_1 \in K$
$b \in HK \Rightarrow b = h_2k_2; h_2 \in H, k_2 \in K$
$(ab^{-1}) = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1(k_1k_2^{-1})h_2^{-1} = h_1k_3h_3^{-1}$
such that $k_3 = k_1k_2^{-1}$
$k_3\, h_2^{-1} \in KH = HK$
$k_3\, h_2^{-1} \in HK, k_3\, h_2^{-1} = hk; h \in H, k \in K$
hence $ab^{-1} = h_1hk = h_3\dot{k} \in HK (h_3 = h_1h)$

Thus HK is subgroup.
Corollarv: Let H and K be subgroups of an abelian group G then HK is subgroup.

Definition: Let G be a group and H is subgroup of G , for each $a \in G$ the set $aH = \{ah : h \in H\}$ is called the left coset of H in G . The element a is called a representative of aH . In similar way we can define the right coset.

Example: $G = Z_6, H = \{\overline{0}, \overline{2}, \overline{4}\}$
$\overline{0} +_6 \{\overline{0}, \overline{2}, \overline{4}\} = \{\overline{0}, \overline{2}, \overline{4}\}$
$\overline{1} +_6 \{\overline{0}, \overline{2}, \overline{4}\} = \{\overline{1}, \overline{3}, \overline{5}\}$

$\overline{2} +_6 \{\overline{0}, \overline{2}, \overline{4}\} = \{\overline{2}, \overline{4}, \overline{0}\} = \mathrm{H}$
$\overline{3} +_6 \{\overline{0}, \overline{2}, \overline{4}\} = \{\overline{3}, \overline{5}, \overline{1}\}$
$\overline{4} +_6 \{\overline{0}, \overline{2}, \overline{4}\} = \{\overline{4}, \overline{0}, \overline{2}\} = \mathrm{H}$
$\overline{5} +_6 \{\overline{0}, \overline{2}, \overline{4}\} = \{\overline{5}, \overline{1}, \overline{3}\}$
Remark: Let H be a subgroup of a group G , let $a \in G$ then there is (1-1) and onto function from H into aH .
Proof: $\emptyset: \mathrm{H} \longrightarrow \mathrm{aH}$, defined by $\emptyset(\mathrm{h}) = \mathrm{ah}$
To show that $\emptyset$ is $1 - 1$
$x, y \in H, \emptyset(x) = \emptyset(y), ax = ay \Rightarrow x = y$
hence $\emptyset$ is $(1 - 1)$
To show that $\emptyset$ is onto
Let $\mathrm{w} \in \mathrm{aH}, \mathrm{w} = \mathrm{ah}_1; h_1 \in H$
Thus $\emptyset(\mathrm{h}_1) = \mathrm{w}$, and $\emptyset$ is onto
Remark: Let H be a subgroup of G , define $\sim$ on G by $a \sim b$ if and only if $ab^{-1} \in \mathrm{H}$, then $\sim$ equivalence relation.
$\forall a \in G, a \sim a$(since $aa^{-1} = e \in H$)
$a \sim b \Rightarrow b \sim a$
$[ab^{-1} \in H \Rightarrow (ba^{-1})^{-1} \in H \Rightarrow b^{-1}a \in H]$
$a \sim b \Rightarrow ab^{-1} \in H$
$b \sim c \Rightarrow bc^{-1} \in H$, since H is a subgroup

then $(ab^{-1})(bc^{-1}) \in H$
$a(b^{-1}\,b)c^{-1} = ac^{-1} \in H$
This relation is equivalence relation on G,hence partition G into equivalence classes [a]

$$[a] = \{x \in G: a \sim x\}$$

Definition: Let G be a group and H be a subgroup of G , the number of distinct left cosets of H in G is denoted by [G:H] and is called the index of H in G .

Theorem: (Lagrange) Let H be a subgroup of a finite group G , then
$0(G) = 0(H)[G:H]$
Corollary: Let H be a subgroup of a finite group G , then the order of H and index of H divide $0(G)$.

Example: There is no subgroup of order 4 in a group of order 10 .