**6. More Results of Subgroups**

**Cyclic Group:**

 **Definition(6-1)**Let $(G,\*)$ be a group and $a\in G$, the cyclic subgroup of $G$ generated by $a$ is denoted by $\left〈a\right〉$ and defined as

$$\left〈a\right〉=\left\{a^{k}:k\in Z\right\}=\{…, a^{-1}, a^{0}, a^{1},…\}$$

If $G=\left〈a\right〉$, then $G$ is called a cyclic group.

**Definition(6-2):** A group $(G,\*)$ is called cyclic group generated by $a$ iff$ ∃a\in G\ni G=\left〈a\right〉=\left\{a^{k}:k\in Z\right\}$.

**Example(6-3):** In $(Z\_{9},+\_{9})$, find the cyclic subgroup generated by $2,3,1$.

**Solution:** $\left〈2\right〉=\left\{2^{k}, k\in Z\right\}=\{…,2^{-3},2^{-2},2^{-1},2^{0},2^{1},2^{2},2^{3},…\}$

$$=\left\{…,3,5,7,0,2,4,6,…\right\}=\left\{0,1,2,…,8\right\}=Z\_{9}$$

$⟹Z\_{9}$ is a cyclic group generated by$ 2$.

$$\left〈3\right〉=\left\{…,3^{-3},3^{-2},3^{-1},3^{0},3^{1},3^{2},3^{3},…\right\}$$

$$ =\{…,3,6,0,3,6,…\}$$

 $ =\{0,3,6\}$ is a cyclic subgroup of $ Z\_{9}$.

$$\left〈1\right〉=\left\{…,1^{-3},1^{-2},1^{-1},1^{0},1^{1},1^{2},1^{3},…\right\}$$

$$ =\{…,6,7,8,0,1,2,3,…\}$$

 $ =$ $Z\_{9}$ is generated by $1$.

**Example(6-4):** In $(Z,+)$, find a cyclic group generated by $1,2,-1$.

**Solution:** $\left〈1\right〉=\left\{1^{k}, k\in Z\right\}=\{…,1^{-3},1^{-2},1^{-1},1^{0},1^{1},1^{2},1^{3},…\}$

$$ =\left\{…, -3,-2,-1,0,1,2,3,…\right\}=Z$$

$$\left〈2\right〉=\left\{2^{k}, k\in Z\right\}=\{…,2^{-3},2^{-2},2^{-1},2^{0},2^{1},2^{2},2^{3},…\}$$

 $=\left\{…,-6,-4,-2,0,2,4,6,…\right\}\ne Z\_{9}$

$$\left〈-1\right〉=\left\{(-1)^{k}, k\in Z\right\} =\{…,(-1)^{-3},(-1)^{-2},(-1)^{-1},(-1)^{0},(-1)^{1},(-1)^{2},(-1)^{3},…\} =\left\{…, 2,1,o,-1,-2,…\right\}=Z$$

$⟹(Z,+)$ is a cyclic group generated by $1$ and $-1$.

**Example(6-5):** Is$(S\_{3},∘)$ a cyclic group?

**Solution:**$ \left〈f\_{1}\right〉=\left\{f\_{1}^{k}, k\in Z\right\}=\{…,f\_{1}^{-3},f\_{1}^{-2},f\_{1}^{-1},f\_{1}^{0},f\_{1}^{1},f\_{1}^{2},f\_{1}^{3},…\}$

$$ =\left\{f\_{1}\right\}\ne S\_{3}$$

$$\left〈f\_{2}\right〉=\left\{f\_{2}^{k}, k\in Z\right\}=\{…,f\_{2}^{-2},f\_{2}^{-1},f\_{2}^{0},f\_{2}^{1},f\_{2}^{2},…\}$$

$$ =\{…,f\_{2}, f\_{3}, f\_{1}, f\_{2},f\_{3},…\}$$

 $ =\{ f\_{1}, f\_{2},f\_{3}\}\ne S\_{3}$

$$\left〈f\_{3}\right〉=\{f\_{1}, f\_{2},f\_{3}\}\ne S\_{3}$$

$$\left〈f\_{4}\right〉=\{f\_{1}, f\_{4}\}\ne S\_{3}$$

$$\left〈f\_{5}\right〉=\{f\_{1}, f\_{5}\}\ne S\_{3}$$

$$\left〈f\_{6}\right〉=\{f\_{1}, f\_{6}\}\ne S\_{3}$$

$⟹(S\_{3},∘)$ is not a cyclic group.

**Example(6-6):** In $(Z\_{6},+\_{6})$, find a cyclic subgroup generated by $1,2,5$. (**Homework**)

**Theorem(6-7):** Every cyclic group is an abelian.

**Proof:** let $(G,\*)$ be a cyclic group, $⟹∃a\in G\ni G=\left〈a\right〉=\left\{a^{k}, k\in Z\right\}$

To prove $G$ is an abelian group

Let $x,y\in G$, to prove$ x\*y=y\*x ∀ x,y\in G$

$$x\in G=\left〈a\right〉⟹x=a^{m}\ni m\in Z$$

$$y\in G=\left〈a\right〉⟹y=a^{n}\ni n\in Z$$

$$x\*y=a^{m}\*a^{n}=a^{m+n}=a^{n+m}=a^{n}\*a^{m}=y\*x$$

$⟹G$ is an abelian group.

**Note(6-8):** The converse of above theorem is not true in general, for example.

$$\left(G=\left\{e,a,b,c\right\},\*\right)\ni a^{2}=b^{2}=c^{2}=e$$

$$a^{2}=e⟹a\*a=e⟹a^{-1}=a$$

$$b^{2}=e⟹b\*b=e⟹b^{-1}=b$$

$$c^{2}=e⟹c\*c=e⟹c^{-1}=c$$

$$e^{-1}=e⟹x^{-1}=x ∀ x\in G$$

$⟹(G,\*)$ is an abelian group, but $(G,\*)$ is not a cyclic group, since

$$\left〈e\right〉=\{e\}\ne G$$

$$\left〈a\right〉=\left\{a^{k}, k\in Z\right\}=\{e,a\}\ne G$$

$$\left〈b\right〉=\left\{b^{k}, k\in Z\right\}=\{e,b\}\ne G$$

$$\left〈c\right〉=\left\{c^{k}, k\in Z\right\}=\{e,c\}\ne G$$

$⟹(G,\*)$ is not a cyclic.

**Theorem(6-9):** $\left〈a\right〉=\left〈a^{-1}\right〉 ∀ a\in G$.

**Proof:** $\left〈a\right〉=\left\{a^{k}, k\in Z\right\}=\left\{(a^{-1})^{-k}, -k\in Z\right\}$

$=\left\{(a^{-1})^{m}, m=-k\in Z\right\}=\left〈a^{-1}\right〉$.

**Theorem(6-10):** If $(G,\*)$ is a finite group of order $n$ generated by$ a$, then $G=: \left〈a\right〉=\left\{a^{k}, k\in Z\right\}=\{a^{1},a^{2},…,a^{n}=e\}$, such that $n$ is the least positive integer $\ni a^{n}=e$, this means $O\left(a\right)=n=O(G)$.

**Example(6-11):** Show that $(Z\_{n},+\_{n})$ is a cyclic group.

**Solution:** $Z\_{n}=\{0,1,…,n-1\}$

$O(Z\_{n})=n$, to prove $Z\_{n}=\left〈1\right〉$

$$\left〈1\right〉=\left\{1^{k}, k\in Z\right\}=\{1,1^{2}, 1^{3},…,1^{n}=0\}$$

$$=\left\{1,2,3,…,n=0\right\}=Z\_{n}$$

$⟹Z\_{n}=\left〈1\right〉$ and $O(Z\_{n})=O\left(1\right)=n$.

**Definition(6-12):** (Division Algorithm for $Z$)

If $a,b$ are integers, with $b>0$. Then there is a unique pair of integers$q,r\ni a=bq+r, 0\leq r<b$.

The number $q$ is called the quotient and $r$ is called the remainder when $a$ is divided by $b$.

**Example(6-13):** Find the quotient $q$ and remainder$ r$, when $38$ is divided by $7$according to the division algorithm.

**Solution:**  $38=7\left(5\right)+3, 0\leq 3<7$

$⟹q=5, r=3$.

**Example(6-14):** $a=23, b=7$.

**Solution:**  $23=7\left(3\right)+2, 0\leq 2<7$

$⟹q=3, r=2$.

**Example(6-15):** $a=15, b=2$.

**Solution:**  $15=2\left(7\right)+1, 0\leq 1<2$

$⟹q=7, r=1$.

**Theorem(6-16):** A subgroup of a cyclic group is a cyclic.

**Proof:** let $G$ be a cyclic group generated by $a$ and let $H$ be a subgroup of $G$

If $H=\{e\}$, then $H=\left〈e\right〉$ is a cyclic

If $H\ne \{e\}$ and $H\ne G$ ($H$ is a proper subgroup), then

$$x\in H⟹x=a^{m}, m\in Z$$

$$x^{-1}\in H⟹x^{-1}=a^{-m}, -m\in Z$$

Let $m$ be a least positive integer such that $a^{m}\in H$

to prove $H=\left〈a^{m}\right〉=\{\left(a^{m}\right)^{g}:g\in Z\}$

to prove $H⊆\left〈a^{m}\right〉,\left〈a^{m}\right〉⊆\left〈a^{m}\right〉 $

let $y\in H⟹y=a^{s}, s\in Z$

by division algorithm of $s$ and $m$

$$s=mg+r⟹r=s-mg$$

$$a^{r}=a^{s-mg}=a^{s}\*\left(a^{-m}\right)^{g}, 0\leq r<m$$

$a^{r}\in H$ but $0\leq r<m⟹r=0⟹s=mg$

$$a^{s}=\left(a^{m}\right)^{g}\in \left〈a^{m}\right〉$$

$$y=a^{s}\in \left〈a^{m}\right〉⟹H⊆\left〈a^{m}\right〉$$

To prove $\left〈a^{m}\right〉⊆H$

Let $x\in \left〈a^{m}\right〉⟹x=\left(a^{m}\right)^{g}, g\in Z$

$$a^{m}\in H⟹\left(a^{m}\right)^{g}\in H⟹x\in H⟹\left〈a^{m}\right〉⊆H$$

$⟹(H,\*)$ is a cyclic subgroup.

**Corollary(6-17):** If $(G,\*)$ is a finite cyclic group of order $n$ generated by$ a$, then every subgroup of $G$ is a cyclic generated by $a^{m}\ni \frac{n}{m}$.

**Proof:** suppose $(G,\*)$ is a finite, $O\left(G\right)=n$

$$G=\left〈a\right〉=\{a,a^{2},…,a^{n}=e\}$$

Let $(H,\*)$ be a subgroup of $(G,\*)$, then$(H,\*)$ is a cyclic

such that $H=\left〈a^{m}\right〉$, to prove $\frac{n}{m} (n=mg, g\in Z)$

$e\in H⟹a^{n}\in H$, by division algorithm of $n,m$

$$⟹n=mg+r, 0\leq r<m$$

$$r=n-mg⟹a^{r}=a^{n}\*(a^{m})^{-g}$$

$a^{r}\in H$, but $0\leq r<m$

If $r=0⟹n=mg⟹\frac{n}{m}$.

**Example(6-18):** Find all subgroups of $(Z\_{15},+\_{15})$.

**Solution:** $ O\left(Z\_{15}\right)=15$, $H=\left〈1^{m}\right〉, \frac{15}{m}$

If $m=1⟹H\_{1}=Z\_{15}$

If $m=3⟹H\_{2}=\{3,6,9,12\}$

If $m=5⟹H\_{3}=\{5,10,0\}$

If $m=15⟹H\_{4}=\{0\}$.

**Corollary(6-19):** If $(G,\*)$ is a finite cyclic group of prime order, then $G$ has no a proper subgroup.

**Proof:** let $ (G,\*)$ be a finite group such that

 $O\left(G\right)=p$ ($p$ is a prime number)

$$G=\left〈a\right〉=\{a,a^{2},…,a^{p}=e\}$$

Let $ (H,\*)$ be a cyclic subgroup

$H=\left〈a^{m}\right〉\ni \frac{p}{m}⟹m=1$ or $m=p$

If $m=1⟹H=\left〈a\right〉=G$ (not a proper subgroup)

If $m=p⟹H=\left〈a^{p}=e\right〉=\{e\}$ (not a proper subgroup)

$⟹G$ has no a proper subgroup.

**Example(6-20):** Find all subgroup of $(Z\_{7},+\_{7})$.

**Solution:** $O(Z\_{7})=7$

Let $H=\left〈1^{m}\right〉, \frac{7}{m}⟹m=1$ or $m=7$

If $m=1⟹H\_{1}=\left〈1\right〉=Z\_{7}$

If $m=7⟹H\_{2}=\left〈1^{7}\right〉=\{0\}$.

**Definition(6-21):** A positive integer $c$ is said to be a greatest common divisor of two non-zero numbers $x, y$ iff

1. $\frac{x}{c} , \frac{y}{c}$
2. If $\frac{x}{a} , \frac{y}{a}⟹\frac{c}{a}$.

**Example(6-22):** Find g. c. d.$ (12,18)$.

**Solution:** g. c. d.$ \left(12,18\right)=6$**,** since

1. $\frac{12}{6}, \frac{18}{6}$
2. $\frac{12}{3}, \frac{18}{3}⟹\frac{6}{3}$

 $\frac{12}{1}, \frac{18}{1}⟹\frac{6}{1}$

 $\frac{12}{2}, \frac{18}{2}⟹\frac{6}{2}$.

**Remark(6-23):** If $(G,\*)$ is a finite cyclic group of order $n$ generated by $a$, then the generator of $G$ is $a^{k} \ni g. c. d. \left(k,n\right)=1$.

**Example(6-24):** Find all generators of $(Z\_{6},+\_{6})$.

**Solution:** $O\left(Z\_{6}\right)=6, Z\_{6}=\left〈1\right〉 $

$$Z\_{6}=\left〈1^{k}\right〉 \ni g. c. d. \left(k,6\right)=1, k=1,2,3,4,5 $$

$$k=1⟹g. c. d. \left(1,6\right)=1⟹Z\_{6}=\left〈1\right〉$$

$$k=2⟹g. c. d. \left(2,6\right)\ne 1⟹Z\_{6}\ne \left〈1^{2}\right〉=\left〈2\right〉$$

$$k=3⟹g. c. d. \left(3,6\right)\ne 1⟹Z\_{6}\ne \left〈1^{3}\right〉=\left〈3\right〉$$

$$k=4⟹g. c. d. \left(4,6\right)\ne 1⟹Z\_{6}\ne \left〈1^{4}\right〉=\left〈4\right〉$$

$$k=5⟹g. c. d. \left(5,6\right)=1⟹Z\_{6}=\left〈1^{5}\right〉=\left〈5\right〉$$

therefore, the generators of $Z\_{6}$are $1,5$.

**Theorem(6-25):** If $(G,\*)$ is an infinite cyclic group generated by $a$, then:

1. The numbers $a, a^{-1}$ are only generators of $G$;
2. Every subgroup of $G$ except$ \{e\}$ is an infinite subgroup.

**Proof:** (1) suppose $G=\left〈a\right〉$, to prove $G=\left〈a^{-1}\right〉$

Let $a\in G\ni G=\left〈a\right〉=\{…,a^{-2},a^{-1},a^{0},a^{1},a^{2},…\}$

Let $b\in G\ni G=\left〈b\right〉=\{…,b^{-2},b^{-1},b^{0},b^{1},b^{2},…\}$

$$a\in G=\left〈a\right〉⟹a=b^{r},r\in Z…1$$

$b\in G=\left〈a\right〉⟹b=a^{s},s\in Z…2$

Substitute $1$ in $2$, we get $b=(b^{r})^{s}⟹b^{1}=b^{rs}$

$1=rs⟹r=s=1$ or $r=s=-1$

If $r=s=1⟹a=b⟹G=\left〈a\right〉$

If $r=s=-1⟹b=a^{-1}⟹G=\left〈a^{-1}\right〉$.

(2) let $(H,\*)$ be a subgroup of$ \left(G,\*\right)\ni H\ne \{e\}$

To prove $(H,\*)$ is an infinite

Suppose that $(H,\*)$ is a finite such that $O\left(H\right)=k$

$(H,\*)$ is a cyclic subgroup

$$H=\left〈a^{m}\right〉=\{\left(a^{m}\right)^{1},\left(a^{m}\right)^{2},…\left(a^{m}\right)^{k}=e\}$$

$a^{mk}=e⟹O\left(a\right)=mk⟹O\left(a\right)=O(G)$, but this is contradiction

$(G=\left〈a\right〉, G$ is a finite)

Thus, $(H,\*)$ is an infinite.

**Definition(6-26):** Let $(H,\*)$ be a subgroup of a group $(G,\*)$. The set $a\*H=\{a\*h:h\in H\}$ of $G$ is the left coset of $H$ containing $a$, while the subset$ H\*a=\{h\*a:h\in H\}$ is the right coset of $H$ containing $a$.

**Example(6-27):** If $\left(Z\_{6},+\_{6}\right), a=1, H=\{0,2,4\}$, then

$$1+\_{6}H=\left\{1,3,5\right\}, H+\_{6}1=\{1,3,5\}$$

$$3+\_{6}H=\left\{3,5,1\right\}, H+\_{6}3=\{3,5,1\}$$

**Notes(6-28):**

1. $a\*H$ is not subgroup ( in general), give an example (**Homework**);
2. $a\*H\ne H\*a$ (in general), for example

$$\left(S\_{3},∘\right), H=\left\{f\_{1}, f\_{4}\right\}, a=f\_{2}$$

$$f\_{2}∘H=\left\{f\_{2}, f\_{5}\right\}, H∘f\_{2}=\left\{f\_{2}, f\_{6}\right\}$$

$⟹f\_{2}∘H\ne H∘f\_{2}$.

**Theorem(6-29):** Let $(H,\*)$ be a subgroup of $(G,\*)$ and $a\in G$, then

1. $H$ is itself left coset of $H$ in $G$.

**Proof:** $e\in G, e\*H=\left\{e\*h:h\in H\right\}=H$.

1. If $(G,\*)$ is an abelian group, then $a\*H=H\*a$.

**Proof:** $a\*H=\left\{a\*h:h\in H\right\}=\left\{h\*a:h\in H\right\}=H\*a$*.*

The converse of above theorem is not true in general, for example

$$\left(S\_{3},∘\right), H=\left\{f\_{1}, f\_{2},f\_{3}\right\}, a=f\_{4}$$

$$f\_{4}∘H=\left\{f\_{4}, f\_{5},f\_{6}\right\}, H∘f\_{4}=\left\{f\_{4}, f\_{6},f\_{5}\right\}$$

$⟹f\_{2}∘H=H∘f\_{2}$, but $\left(S\_{3},∘\right)$ is not an abelian.

1. $a\in a\*H$

**Proof:** $a=a\*e\in a\*H$.

1. $a\*H=H$ iff $a\in H$

**Proof:** $(⟹)$ suppose that$ a\*H=H$, then by $3⟹a\in H$.

$(⟸)$ suppose that $a\in H$, to prove $a\*H=H$

This means $a\*H⊆H$ and $H⊆a\*H$

Let $x\in a\*H⟹x=a\*h\in H⟹a\*H⊆H$

To prove $H⊆a\*H$

Let$ b\in H⟹b=e\*b=\left(a\*a^{-1}\right)\*b=a\*\left(a^{-1}\*b\right)⟹b\in a\*H$

$⟹H⊆a\*H⟹H=a\*H$.

1. $a\*H=b\*H$ iff $a^{-1}\*b\in H$

**Proof:** $\left(⟹\right) a\*H=b\*H$

$$a^{-1}\*\left(a\*H\right)=a^{-1}\*(b\*H)$$

$$(a^{-1}\*a)\*H=(a^{-1}\*b)\*H)$$

$H=(a^{-1}\*a)\*H$, by $4⟹a^{-1}\*b\in H$

$(⟸)$ suppose that $a^{-1}\*b\in H$

by $4⟹\left(a^{-1}\*b\right)\*H=H⟹b\*H=a\*H$.

1. $a\*H=b\*H$ or $ \left(a\*H\right)∩\left(b\*H\right)=∅$

**Proof:** suppose that $ \left(a\*H\right)∩\left(b\*H\right)\ne ∅$

To prove $a\*H=b\*H$

$∃ x\ni x\in a\*H$ and $x\in b\*H$

$x=a\*h\_{1}$ and $x=b\*h\_{2}\ni h\_{1},h\_{2}\in H$

$$a\*h\_{1}=b\*h\_{2}⟹h\_{1}=a^{-1}\*b\*h\_{2}$$

$$⟹h\_{1}\*h\_{2}^{-1}=a^{-1}\*b\in H$$

by $5⟹a\*H=b\*H$

or suppose $a\*H\ne b\*H$

to prove $\left(a\*H\right)∩\left(b\*H\right)=∅$

suppose $\left(a\*H\right)∩\left(b\*H\right)\ne ∅$

$∃x\in a\*H$ and $x\in b\*H$

$x=a\*h\_{1}$ and $x=b\*h\_{2}$

$$a^{-1}\*b=h\_{1}\*h\_{2}^{-1}⟹a^{-1}\*b\in H$$

$⟹a\*H=b\*H$, but this is contradiction

$⟹ \left(a\*H\right)∩\left(b\*H\right)=∅$.

1. The set of all distinct left coset of $H$ in $G$ form a partition on$ G$.

**Proof:** to prove $G=\bigcup\_{a\in G}^{}a\*H$ and $a\_{i}\*H∩a\_{j}\*H=∅$

$a\_{i}\*H,a\_{j}\*H$ are distinct $⟹a\_{i}\*H∩a\_{j}\*H=∅$

To prove $G=\bigcup\_{a\in G}^{}a\*H$

$a\*H⊆G ∀a\in G$ (by definition of a coset)

$$⟹\bigcup\_{a\in G}^{}a\*H⊆G…1$$

$$∀a\in G⟹a\in a\*H⟹a\in \bigcup\_{a\in G}^{}a\*H$$

$$⟹G⊆\bigcup\_{a\in G}^{}a\*H…2$$

From $1,2$, we have $G=\bigcup\_{a\in G}^{}a\*H$.

**Note(6-30):** Every coset (left or right) of a subgroup $H$ of a group $(G,\*)$ has the same number of elements as $H$.

**Example(6-31):** The group $(Z\_{6},+\_{6})$ is an abelian. Find the partition of $Z\_{6}$ into coset of the subgroup $H=\{0,3\}$.

**Solution:** $0+H=\left\{0,3\right\}=H$

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

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

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

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

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

All the cosets of $H$ are $\left\{0,3\right\},\left\{1,4\right\},\{2,5\}$ and since $(Z\_{6},+\_{6})$ is an abelian group, then the left coset is an equal to the right coset.

**Example(6-32):** In $(S\_{3},∘)$, let $H=\{f\_{1},f\_{4}\}$. Find the partition of $S\_{3}$ into left coset of $H$ and the partition into right coset of $H$. (**Homework**)

**Definition(6-33):** Let $(H,\*)$ be a subgroup of a group $(G,\*)$. The number of left cosets or right cosets of $H$ in$ G$ is called the index of $H$ in $G$ and denoted by$ [G:H]$.

**Note(6-34):** If $(G,\*)$ is a finite group, then $ \left[G:H\right]=\frac{O(G)}{O(H)}$.

**Example(6-35):** $\left(S\_{3},∘\right), H=\{f\_{1},f\_{2},f\_{3}\}$

$$⟹\left[S\_{3}:H\right]=\frac{O\left(S\_{3}\right)}{O\left(H\right)}=\frac{6}{3}=2$$

**Example(6-36):**$ \left(Z\_{6},+\_{6}\right), H=\{0,3\}$

$$⟹\left[Z\_{6}:H\right]=\frac{O\left(Z\_{6}\right)}{O\left(H\right)}=\frac{6}{2}=3$$

**Theorem(6-37):** (Lagrange Theorem)

Let $H$ be a subgroup of a finite group $(G,\*)$. Then the order of$ H$ is a divisor of the order of $G$.

**Proof:** let $G$ be a finite group$ \ni O\left(G\right)=n$ and $H$ be a subgroup of $G\ni O\left(H\right)=m$

To prove $\frac{O(G)}{O(H)}$ (to prove$\frac{n}{m}, n=mk$)

Since $G$ is a finite $⟹\left[G:H\right]=k$

Let $a\_{1}\*H, a\_{2}\*H,…,a\_{k}\*H$ are left cosets of $H$

$a\_{1}\*H∪a\_{2}\*H∪…∪a\_{k}\*H=G$ and $a\_{i}\*H∩a\_{j}\*H=∅$

$$O(a\_{1}\*H)+ O(a\_{2}\*H)+…+O(a\_{k}\*H)=O(G)$$

$m+m+…+m (k$-times$)=n$

$$mk=n⟹\frac{n}{m}⟹\frac{O(G)}{O(H)}$$

**Corollary(6-38):** If $(G,\*)$ is a finite group, then the order of any element of $G$ divides the order of$ G$.

**Proof:** suppose that $(G,\*)$ is a finite such that $O\left(G\right)=n$

Let $a\in G⟹a$ has a finite order such that $O\left(a\right)=m$

To prove such that $\frac{O(G)}{O(a)}$

Since $a\in G⟹H=\left〈a\right〉$ is a cyclic group

$H=\left\{a,a^{2},…,a^{m}=e\right\}, O\left(a\right)=m⟹\frac{O(G)}{O(H)}$ (by Lagrange Theorem)

$$⟹\frac{O(G)}{O(a)}$$

**Corollary(6-39):** If $(G,\*)$ is a finite group, then $a^{O(G)}=e ∀a\in G$.

**Proof:** suppose that $O\left(G\right)=n$

Let $a\in G\ni O\left(a\right)=m$ (by Corollary of Lagrange)

$$⟹\frac{O\left(G\right)}{O\left(a\right)}⟹\frac{n}{m}⟹n=mk$$

$$a^{O(G)}=a^{n}=(a^{m})^{k}=e^{k}=e$$

$⟹a^{O\left(G\right)}=e ∀a\in G$.

**Corollary(6-40):** Every group of prime order is a cyclic.

**Proof:** let $(G,\*)$ be a finite $\ni O\left(G\right)=p⟹\frac{p}{O\left(a\right)} ∀a\in G$

$O\left(a\right)=1$ or $p$

If $O\left(a\right)=1⟹a=e$

If $O\left(a\right)=p⟹O\left(a\right)=O\left(G\right)⟹G=\left〈a\right〉$

$⟹G $is a cyclic group.

**Corollary(6-41):** Every group of order less than $6$ is an abelian.

**Proof:** let $(G,\*)$ be a finite group $\ni O(G)<6$

$O\left(G\right)=1 $or $2$ or $3$ or $4$ or $5$

If $O\left(G\right)=1⟹G=\{e\}⟹G$ is an abelian

If $O\left(G\right)=2$ or $3$ or $5⟹G$ is a cyclic $⟹G$ is an abelian

If $O\left(G\right)=4⟹\frac{4}{O\left(a\right)}⟹O\left(a\right)=1$ or $2$ or $4$

If $O\left(a\right)=1⟹a=e$

If $O\left(a\right)=2 ∀a\in G⟹a^{2}=e⟹a=a^{-1} ∀a\in G$

$⟹G$ is an abelian

If $O\left(a\right)=4⟹O\left(a\right)=O\left(G\right)⟹G=\left〈a\right〉 $

$⟹G$ is a cyclic $⟹G$ is an abelin.