**Definition 2.41:** [g.c.d(x,y)] القاسم المشترك الاكبر

A positive integer c is said to be a greatest common divisor of two non-zero number x and y iff

**(1)** $c \mid x \wedge c \mid y$

**(2)** If $a \mid x \wedge a \mid y \Rightarrow a \mid c$

(g.c.d(x, y) = c)

**Examples 2.42:** Find (g.c.d.(12, 18))

**Solution:**

g.c.d(12, 18) = 6 since

**(1)** $6|12 \wedge 6|18$

**(2)** $3|12 \wedge 3|18 \Rightarrow 3|6$

or $2|12 \wedge 2|18 \Rightarrow 2|6$

**Remark 2.43:** If $(G, *)$ is finite cyclic group of order $n$ generated by $a$ , then the generators of G is $a^k$ such that g.c.d $(k, n) = 1$.

**Examples 2.44:** Find all generators of $(Z_6, +_6)$

**Solution:**

$o(Z_6) = 6$ , $Z_6 = <\bar{1}>$

$Z_6 = <(\bar{1})^k>$ s.t. g.c.d $(k, 6) = 1$, $k = 1, 2, 3, 4, 5$

$k = 1 \Rightarrow$ g.c.d$(1, 6) = 1 \Rightarrow Z_6 = <\bar{1}>$

$k = 2 \Rightarrow$ g.c.d$(2, 6) \neq 1 \Rightarrow Z_6 \neq <(\bar{1})^2> = <\bar{2}>$

$k = 3 \Rightarrow$ g.c.d$(3, 6) \neq 1 \Rightarrow Z_6 \neq <(\bar{1})^3> = <\bar{3}>$

$k = 4 \Rightarrow$ g.c.d$(4, 6) \neq 1 \Rightarrow Z_6 \neq <(\bar{1})^4> = <\bar{4}>$

$k = 5 \Rightarrow$ g.c.d$(5, 6) = 1 \Rightarrow Z_6 = <(\bar{1})^5> = <\bar{5}>$

The generators of $Z_6$ are $\{\bar{1}, \bar{5}\}$.

**Examples 2.45:** Find all generators of $(Z_7, +_7)$ **(H. W.)**

**Theorem 2.46:** If $(G, *)$ is an infinite cyclic group generated by $a$, then:

**(1)** $a$ and $a^{-1}$ are only generators of G

**(2)** Every subgroup of G except {e} is an infinite subgroup.

**Proof (1):**

Let G = $<a>$ . To prove, G = $<a^{-1}>$

Let $a \in G \ni G = <a> = \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\}$

Let $b \in G \ni G = <b> = \{\dots, b^{-2}, b^{-1}, b^0, b^1, b^2, \dots\}$

$a \in G = <b> \Rightarrow a = b^r, \; r \in Z$ …(1)

$b \in G = <a> \Rightarrow b = a^s, \; s \in Z$ …(2)

Put (1) in (2) $\Rightarrow b = (b^r)^s \Rightarrow b^1 = b^{rs} \Rightarrow b^1 = b^{rs}$

$1 = rs \Rightarrow r = s = 1$ or $r = s = -1$

If $r = s = 1 \Rightarrow a = b \Rightarrow G = <a>$

If $r = s = -1 \Rightarrow b = a^{-1} \Rightarrow G = <a^{-1}>$

**Proof (2):**

Let (H, ∗) be a subgroup of (G, ∗) ∋ H ≠ {e}.

To prove, (H, ∗) is an infinite.

Suppose that (H,∗ ) is finite ∋ o(H) = k, then

(H, ∗) is cyclic subgroup

$H = <a^m> = \{(a^m)^1, (a^m)^2, \dots, (a^m)^k = e\}$

$a^{mk} = e \Rightarrow o(a) = mk$

∴ o(a) = o(G) C!!!!! تناقض (G = $<a>$, G is finite)

∴ (H, ∗) is infinite.

**Definition 2.47:** المجموعات المشاركة للزمرة الجزئية H

Let (H, ∗) be a subgroup of a group (G,∗) and a ∈ G.

The set **a∗H= {a ∗ h : h ∈ H}** of G is the left coset of H containing a, while the set **H∗ a= { h∗ a : h ∈ H}** is the right coset of H containing a.

**Examples 2.48:** If $(Z_6, +_6)$, a = $\bar{1}$ and a = $\bar{3}$, H = $\{\bar{0}, \bar{2}, \bar{4}\}$, then

$\bar{1} +_6 H = \{\bar{1}, \bar{3}, \bar{5}\}$ , $H +_6 \bar{1} = \{\bar{1}, \bar{3}, \bar{5}\}$

$\bar{3} +_6 H = \{\bar{3}, \bar{5}, \bar{1}\}$, $H +_6 \bar{3} = \{\bar{3}, \bar{5}, \bar{1}\}$.

**Notes 2.49:**

**(1)** a∗H is not subgroup in general. Give an example **(H.W.)**

**(2)** a∗H ≠ H ∗a in general, for example

$(S_3, \circ)$, $H = \{f_1, f_4\}$ , $a = f_2$

$f_2 \circ H = \{f_2, f_5\}$ , $H \circ f_2 = \{f_2, f_6\}$

$f_2 \circ H \neq H \circ f_2$

**Theorem 2.50:** Let $(H, *)$ be a subgroup of $(G, *)$ and $a \in G$, then

**(1) H is itself left coset of H in G.**

**Proof (1):** $e \in G$, $e*H = \{e*h : h \in H\} = H$

**(2) If $(G, *)$ is abelian group, then $a*H = H*a$**

**Proof (2):** $a*H = \{a*h : h \in H\} = \{h*a : h \in H\} = H*a$

**The converse is not true,** for example: $(S_3, \circ)$, $H = \{f_1, f_2, f_3\}$, $a = f_4$

$f_4 \circ H = \{f_4, f_5, f_6\}$ and $H \circ f_4 = \{f_4, f_6, f_5\}$

$\therefore f_4 \circ H = H \circ f_4$, but $(S_3, \circ)$ is not abelian group.

**(3) $a \in a*H$**

**Proof (3):** $a = a*e \in a*H$

**(4) $a*H = H \Leftrightarrow a \in H$**

**Proof (4):** $(\Rightarrow)$ Suppose $a*H = H$, then by (3) we get $a \in H$

$(\Leftarrow)$ Suppose $a \in H$. To prove, $a*H = H$

We must prove that $a*H \subseteq H \wedge H \subseteq a*H$

To prove, $a*H \subseteq H$

Let $x \in a*H \Rightarrow x = a*h \in H$ (since $a \in H \wedge h \in H$)

$\therefore a*H \subseteq H$

To prove, $H \subseteq a*H$

Let $b \in H \Rightarrow b = e*b$

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

$$= a*\underbrace{(a^{-1}*b)}_{\in H} \Rightarrow b \in a*H$$

$\therefore H \subseteq a*H$

Thus, $a*H = H$