Cyclic groups الزمر الدورية (أو الزمر الدائرية)

Def. Let $(G,*)$ be a gp. and $a \in G$, the cyclic subgroup of G generated by a is denoted by $\langle a \rangle$ and defined as

$$\langle a \rangle = \{ a^k : k \in Z \} = \{ \dots, a^{-1}, a^0, a^1, \dots \}.$$

ستسمى الزمرة دورية او دائرية

If $G = \langle a \rangle$ then G is called cyclic gp. generated by a.

اذا امكن توليدها من عنصر واحد.
او اذا وجد عنصر يولدها.

Def. A group $(G,*)$ is called cyclic gp. generated by a iff $\exists a \in G$ such that $G = \langle a \rangle = \{ a^k : k \in Z \}$.

ex.① In $(Z_9, +_9)$, find the cyclic subgp. generated by $\bar{2}, \bar{3}, \bar{7}$.

$$\langle \bar{2} \rangle = \{ \bar{2}^k : k \in Z \} = \{ \dots, \bar{2}^{-3}, \bar{2}^{-2}, \bar{2}^{-1}, \bar{2}^0, \bar{2}^1, \bar{2}^2, \bar{2}^3, \dots \}$$
$$= \{ \dots, \bar{5}, \bar{7}, \bar{0}, \bar{2}, \bar{4}, \bar{6}, \dots \}$$
$$= \{ \bar{0}, \bar{1}, \bar{2}, \dots, \bar{8} \} = Z_9$$

$\therefore Z_9$ is cyclic gp. generated by $\bar{2}$.

$$\langle \bar{3} \rangle = \{ \dots, \bar{3}^{-3}, \bar{3}^{-2}, \bar{3}^{-1}, \bar{3}^0, \bar{3}^1, \bar{3}^2, \bar{3}^3, \dots \}$$
$$= \{ \dots, \bar{3}, \bar{6}, \bar{0}, \bar{3}, \bar{6}, \bar{0}, \dots \}$$
$$= \{ \bar{0}, \bar{3}, \bar{6} \}$$ is cyclic subgp. of Z_9.

$$\langle \bar{1} \rangle = \{ \dots, \bar{1}^{-3}, \bar{1}^{-2}, \bar{1}^{-1}, \bar{1}^0, \bar{1}^1, \bar{1}^2, \bar{1}^3, \dots \}$$
$$= \{ \dots, \bar{6}, \bar{7}, \bar{8}, \bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots \} = Z_9$$ is generated by $\bar{1}$.

ex.① In $(\mathbb{Z}, +)$, find cyclic gp. generated by $1, \bar{2}, -1$.

$$\langle 1 \rangle = \{ 1^k : k \in \mathbb{Z} \} = \{ \cdots, \bar{1}^3, \bar{1}^2, \bar{1}^1, \bar{1}^0, \bar{1}^1, \bar{1}^2, \bar{1}^3, \cdots \}$$
$$= \{ \cdots, -3, -2, -1, 0, 1, 2, 3, \cdots \}$$
$$= \mathbb{Z}$$

$$\langle \bar{2} \rangle = \{ 2^k : k \in \mathbb{Z} \} = \{ \cdots, \bar{2}^3, \bar{2}^2, \bar{2}^1, \bar{2}^0, \bar{2}^1, \bar{2}^2, \bar{2}^3, \cdots \}$$
$$= \{ \cdots, -6, -4, -2, 0, 2, 4, 6, \cdots \} = E$$
$$\neq \mathbb{Z}$$

$$\langle -1 \rangle = \{ (-1)^k : k \in \mathbb{Z} \} = \{ \cdots, (-1)^{-2}, (-1)^{-1}, (-1)^0, (-1)^1, (-1)^2, \cdots \}$$
$$= \{ \cdots, 2, 1, 0, -1, -2, \cdots \}$$
$$= \mathbb{Z}$$

$\therefore (\mathbb{Z}, +)$ is cyclic gp. generated by 1 and -1

---

ex.② Is (S_3, o) cyclic gp.?

$$= \{ f_1^k : k \in \mathbb{Z} \} = \{ \cdots, \bar{f}_1^2, \bar{f}_1^1, f_1^0, f_1^1, f_1^2, \cdots \}$$

$$\langle f_1 \rangle = \{ f_1 \} \neq S_3$$

$$\langle f_2 \rangle = \{ f_2^k : k \in \mathbb{Z} \} = \{ \cdots, \bar{f}_2^2, \bar{f}_2^1, f_2^0, f_2^1, f_2^2, \cdots \}$$
$$= \{ \cdots, f_2, f_3, f_1, f_2, f_3, \cdots \}$$
$$= \{ f_1, f_2, f_3 \} \neq S_3$$

$$\langle f_3 \rangle = \{ f_1, f_2, f_3 \} \neq S_3$$
$$\langle f_4 \rangle = \{ f_1, f_4 \} \neq S_3$$
$$\langle f_5 \rangle = \{ f_1, f_5 \} \neq S_3$$
$$\langle f_6 \rangle = \{ f_1, f_6 \} \neq S_3$$

$\therefore (S_3, o)$ is not cyclic gp.

ex④ In $(\mathbb{Z}_6, +_6)$ · Find cyclic subgp. generated by $\bar{1}, \bar{2}, \bar{5}$. (H.W)

Theorem①: Every cyclic group is Commutative.

Proof. Let $(G,*)$ be a cyclic gp.

$\therefore \exists\ a \in G$ s.t. $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$

T.P. G is Comm. gp.

Let $x, y \in G$ T.P. $x * y = y * x \quad \forall x, y \in G$

$\because x \in G = \langle a \rangle \Rightarrow x = a^n \ \exists\ n \in \mathbb{Z}$

and $y \in G = \langle a \rangle \Rightarrow y = a^n \ \exists\ n \in \mathbb{Z}$

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

$\therefore$ G is Comm. gp.

The Convers of this Theorem is not true.

for example: Klien-gp.

$(G = \{e, a, b, c\}, *)$ s.t. $a^2 = b^2 = c^2 = e$

$a^2 = e \Rightarrow a * a = e \Rightarrow \bar{a}^1 = a$

$b^2 = e \Rightarrow b * b = e \Rightarrow \bar{b}^1 = b$

$c^2 = e \Rightarrow c * c = e \Rightarrow \bar{c}^1 = c$

$\bar{e}^1 = e \Rightarrow \bar{x}^1 = x \quad \forall x \in G$

$\therefore (G,*)$ is Comm. gp.

but $(G,*)$ is not cyclic gp. Since:

$\langle e \rangle = \{e\} \neq G$

$\langle a \rangle = \{a^k : k \in Z\} = \{e, a\} \neq G$

$\langle b \rangle = \{b^k : k \in Z\} = \{e, b\} \neq G$

$\langle c \rangle = \{c^k : k \in Z\} = \{e, c\} \neq G$

$\therefore (G, *)$ is not cyclic

Theorem (2): $\langle a \rangle = \langle \bar{a}^1 \rangle \quad \forall a \in G$.

proof: $\langle a \rangle = \{a^k : k \in Z\} = \{(\bar{a}^1)^{-k} : -k \in Z\}$

$= \{(a^{-1})^m : m = -k \in Z\}$

$= \langle \bar{a}^1 \rangle$

Theorem (3): IF $(G, *)$ is a finite gp. of order n generated by a, then $G = \langle a \rangle = \{a^k : k \in Z\}$
$= \{a^1, a^2, \dots, a^n = e\}$ such that n is the least positive integer $\ni a^n = e$ (i.e.)

$o(a) = n = o(G)$.

(رتبة العنصر الذي يولد الزمرة = رتبة الزمرة)

ex. Show that $(Z_n, +_n)$ is cyclic gp.

$Z_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$

بما ان الزمرة منتهية فنكتب بالشكل:

$o(Z_n) \equiv n$, T.P. $Z_n = \langle \bar{1} \rangle$

$\langle \bar{1} \rangle = \{\bar{1}^k : k \in Z\} = \{\bar{1}, \bar{1}^2, \bar{1}^3, \dots, \bar{1}^n = \bar{0}\}$

$= \{\bar{1}, \bar{2}, \bar{3}, \dots, \overline{n} = \bar{0}\} = Z_n$

$Z_n = \langle \bar{1} \rangle$ and $o(Z_n) = o(\bar{1}) = n$

Def. (Division Algorithm for Z) خوارزمية القسمة

If a and b are integers, with $b>0$. Then there is a unique pair of integers q and r such that

$$a = bq + r \quad \text{where } 0 \leq r < b$$

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

ex.① Find the quotient q and remainder r, when $\overset{a}{38}$ is divided by $\overset{b}{7}$ according to the division Algorithm.

Ans: $38 = 7(5) + 3 \quad 0 \leq 3 < 7$

$\therefore q = 5$ and $r = 3$

ex.② $a = 23$, $b = 7$

$23 = 7(3) + 2 \quad 0 \leq 2 < 7$

$q = 3$, $r = 2$

ex.③ $a = 15$, $b = 2$

$15 = (2)(7) + 1 \quad 0 \leq 1 < 2$

$q = 7$, $r = 1$

Theorem (4): A subgp of a cyclic group is cyclic.

Proof: Let G be a cyclic group generated by a and Let H be a subgp of G.

If $H=\{e\}$, then $H=\langle e\rangle$ is cyclic
If $H\neq\{e\}$ and $H\neq G$ (H is proper subgp.).
Then:
$x\in H \Rightarrow x=a^m$, $m\in Z$
$x^{-1}\in H \Rightarrow x^{-1}=a^m$, $-m\in Z$

Let m be a least positive integer. Such that $a^m\in H$. T.P. $H=\langle a^m\rangle=\{(a^m)^q : q\in Z\}$

T.P. $H\subseteq\langle a^m\rangle \wedge \langle a^m\rangle\subseteq H$
Let $y\in H \Rightarrow y=a^s$, $s\in Z$
By division alg. of s and $m \Rightarrow$
$s=mq+r \Rightarrow r=s-mq$
$\therefore a^r=a^{s-mq}=a^s*(a^m)^q \quad 0\leq r\leq m$
$\because a^r\in H$ but $0\leq r<m$
$\therefore r=0 \Rightarrow s=mq$
$a^s=(a^m)^q\in\langle a^m\rangle$
$\therefore y=a^s\in\langle a^m\rangle \Rightarrow H\subseteq\langle a^m\rangle$

T.P. $\langle a^m\rangle\subseteq H$
Let $x\in\langle a^m\rangle \Rightarrow x=(a^m)^q$, $q\in Z$
$a^m\in H \Rightarrow (a^m)^q\in H$

$\therefore x \in H \Rightarrow \langle a^m \rangle \subseteq H$

$\therefore (H, *)$ is cyclic subgp.

Corollary (1): If $(G, *)$ is a finite cyclic group of order n generated by a, then every subgp of G is cyclic generated by $a^m \ni m|n$.

Proof: Suppose $(G, *)$ is a finite, $o(G) = n$

$G = \langle a \rangle = \{ a, a^2, \ldots, a^n = e \}$

Let $(H, *)$ be a subgp. of $(G, *)$. Then $(H, *)$ is a cyclic (by Th. (4)) such that $H = \langle a^m \rangle$

T.P. $m|n$ $(n = mg, g \in z)$

$a^m \in H$

$e \in H \Rightarrow a^n \in H$, by division Alg. of n and m

$\Rightarrow n = mg + r \quad 0 \leq r < m$

$r = n - mg \Rightarrow a^r = a^n * (a^m)^{-g}$

$\Rightarrow a^r = (a^m)^{-g} \in H$

but $0 \leq r < m$

$\Rightarrow$ if $r = 0 \Rightarrow n = mg$

$\therefore m|n$

---

ex. Find all subgp. of $(Z_{15}, +_{15})$, $Z_{15} = \langle T \rangle$

Ans. $o(Z_{15}) = 15$, $= \langle T^m \rangle \ni m|n$

$H = \langle T^m \rangle \quad m|15$

$m = 1, 3, 5, 15$

If $m = 1 \Rightarrow H_1 = \langle T \rangle = Z_{15}$

If $m=3 \Rightarrow H_2 = \langle T^3 \rangle = \{\bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{0}\}$

If $m=5 \Rightarrow H_3 = \langle T^5 \rangle = \{\bar{5}, \bar{10}, \bar{0}\}$

If $m=15 \Rightarrow H_4 = \langle T^{15} \rangle = \{\bar{0}\} = \langle \bar{0} \rangle$

Corollary ②: If $(G,*)$ is a finite cyclic group of prime order, then G has no proper subgp.

Proof. Let $(G,*)$ be a finite gp. such that

$o(G) = p$ (p prime number)

$G = \langle a \rangle = \{a^1, a^2, \dots, a^p = e\}$

Let $(H,*)$ be cyclic subgp

$\therefore H = \langle a^m \rangle \ni m \mid p$

$\therefore m = 1$ or $m = p$

If $m=1 \Rightarrow H = \langle a \rangle = G$ (not proper subgp)

If $m=p \Rightarrow H = \langle a^p = e \rangle = \{e\}$ (not proper subgp)

$\therefore G$ has no proper subgp.

Ex: Find all subgp of $(Z_7, +_7)$

Ans: $o(Z_7) = 7$, Let $H = \langle T^m \rangle \ni m \mid 7$

$\therefore m = 1, m = 7$

$m = 1 \Rightarrow H_1 = \langle T \rangle = Z_7$

$m = 7 \Rightarrow H_2 = \langle T^7 \rangle = \{0\}$

Def. [g.c.d(x,y)] القاسم المشترك الأكبر

A positive integer c is said to be a greatest common divisor of two non-Zero number x and y iff ① $c|x \wedge c|y$

② if $a|x \wedge a|y \Rightarrow a|c$

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

ex. Find (g.c.d(12,18))

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

① $6|12 \wedge 6|18$

② if $3|12 \wedge 3|18 \Rightarrow 3|6$

or $1|12 \wedge 1|18 \Rightarrow 1|6$

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

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

ex. Find all generators of $(Z_6, +_6)$.

Ans. $o(Z_6) = 6$, $Z_6 = \langle \bar{1} \rangle$

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

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

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

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

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

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

$\therefore$ the generator of Z_6 is $\{\bar{1}, \bar{5}\} = Z_6$

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

1. a and $\bar{a}^1$ are only generators of G.
2. Every subgroup of G except $\{e\}$ is an infinite subgp.

Proof: ① suppose $G = \langle a \rangle$ T.P. $G = \langle \bar{a}^1 \rangle$

Let $a \in G \ni G = \langle a \rangle = \{\dots, \bar{a}^2, \bar{a}^1, a^0, a^1, a^2, \dots\}$

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

$a \in G = \langle b \rangle \Rightarrow a = b^r, r \in Z$ --- ①

$b \in G = \langle a \rangle \Rightarrow b = a^s, s \in Z$ --- ②

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

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

if $r = s = 1 \Rightarrow a = b \Rightarrow G = \langle a \rangle$

if $r = s = 1 \Rightarrow b = \bar{a}^1 \Rightarrow G = \langle \bar{a}^1 \rangle$

② Let $(H,*)$ be a subgp. of $(G,*) \ni H \neq \{e\}$

T.P. $(H,*)$ is infinite

Suppose that $(H,*)$ is finite $\ni o(H)=k$
$(H,*)$ is cyclic subgp.

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

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

$\therefore o(a)=o(G)$ ⊂! تناقض $(G=\langle a\rangle, G \text{ is finite})$

$\therefore (H,*)$ is infinite.

المجموعات المشاركة للزمرة الجزئية H.

Def. Let $(H,*)$ be a subgp. 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.

$a\in G$.

---

ex. If $(Z_6,+_6)$, $\bar{a}=\bar{1}$, $H=\{\bar{0},\bar{2},\bar{4}\}$, then

$\bar{1}+_6H=\{\bar{1},\bar{3},\bar{5}\}$, $H+_6\bar{1}=\{\bar{1},\bar{3},\bar{5}\}$

$\bar{3}+_6H=\{\bar{3},\bar{5},\bar{1}\}$, $H+_6\bar{3}=\{\bar{3},\bar{5},\bar{1}\}$

Note: ① $a*H$ is not subgp. (in general)
give an example (H.W)

② $a*H\neq H*a$ (in general)

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

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

$\Rightarrow f_4\circ H\neq H\circ f_4$