The converse of this theorem is not true, for example:

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

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

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

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

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

$\therefore$ (G, $*$) is commutative group

But (G, $*$) is not cyclic group since:

$< e > = \{e\} \neq G$

$< a > = \{a^k : k \in Z\} = \{e, a\} \neq G$

$< b > = \{b^k : k \in Z\} = \{e, b\} \neq G$

$< c > = \{c^k : k \in Z\} = \{e, c\} \neq G$

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

Theorem 2.29: Let (G, $*$) be a group, then $<a> = <a^{-1}> \ \forall \ a \in G$

Proof:

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

Theorem 2.30: If (G, $*$) is a finite group of order n generated by a, then G = $< a > = \{a^k : k \in Z\} = \{a^1, a^2, \ldots\ldots, a^n = e\}$ such that n is least positive integer $\ni a^n = e$.

(i.e,) o(a) = n = o(G) (رتبة العنصر الذي يولد الزمرة = رتبة الزمرة)

Examples 2.31: Show that (Z_n, $+_n$) is cyclic group.

Solution:

$Z_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ بما ان الزمرة منتهية فتكتب بالشكل :

o(Z_n) = n . To prove, $Z_n = <\bar{1}>$

$$<\bar{1}> = \{(\bar{1})^k : k \in Z\} = \{(\bar{1})^1, (\bar{1})^2, (\bar{1})^3, \ldots\ldots, (\bar{1})^{n-1}, (\bar{1})^n = \bar{0}\}$$
$$= \{\bar{1}, \bar{2}, \bar{3}, \ldots, \bar{n} = \bar{0}\} = Z_n$$

$Z_n = <\bar{1}>$ and o(Z_n) = o($\bar{1}$) = n.

Definition 2.32: (Division Algorithm for Z) **خوارزمية القسمة**

Let a and b be two integer numbers with b > 0, then there is a unique pair of integer's q and r such that:

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

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

Examples 2.33: Find the quotient q and remainder r when 38 is divided by 7 according to the division algorithm.

Solution: $38 = 7(5) + 3 \quad 0 \le 3 \le 7$

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

Examples 2.34: If a = 23 , b = 7

$23 = 7(3) + 2 \quad 0 \le 2 \le 7 \quad \Rightarrow \quad q = 3 \ , r = 2.$

Examples 2.35: If a = 15 , b = 2

$15 = (2)(7) + 1 \quad 0 \le 1 \le 2 \quad \Rightarrow \quad q = 7 \ , \ r = 1$

Theorem 2.36: Any subgroup of acyclic group is cyclic.

Proof: (Without proof)

Corollary 2.37: If (G, $*$) is a finite cyclic group of order n generated by a , then every subgroup of G is cyclic generated by $a^m \ \ni \ m|n$

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

$G = < a > = \{a^1, a^2, \dots\dots, a^n = e\}$

Let (H, $*$) be a subgroup of (G, $*$). Then (H,$*$) is cyclic (by Theorem 2.35) such that $H = <a^m>$

To prove, $m|n$ ($n = mg$, $g \in Z$)

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

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

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

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

But $0 \le r < m \quad \Rightarrow \quad r = 0 \ \Rightarrow \ n = mg$

$\therefore \ m|n$

Examples 2.38: Find all subgroup of $(Z_{15}, +_{15})$

Solution: $o(Z_{15}) = 15$, $H = <(\bar{1})^m> \ni m|n$

$$H = <(\bar{1})^m > \ni m|15$$

$m = 1, 3, 5, 15$

If $m = 1 \Rightarrow H_1 = <\bar{1}> = Z_{15}$

If $m = 3 \Rightarrow H_2 = <(\bar{1})^3> = \{\bar{3}, \bar{6}, \bar{9}, \overline{12}, \bar{0}\}$

If $m = 5 \Rightarrow H_3 = <(\bar{1})^5> = \{\bar{5}, \overline{10}, \bar{0}\}$

If $m = 15 \Rightarrow H_4 = <(\bar{1})^{15}> = \{\bar{0}\} = <\bar{0}>$

(H.W.) Find all subgroup of $(Z_8, +_8)$.

Corollary 2.39: If $(G, *)$ is finite cyclic group of prime order, then G has no proper subgroup.

Proof: Let $(G, *)$ be a finite group such that $o(G) = p$ (p prime number)

$G = <a> = \{a^1, a^2, \ldots\ldots, a^p = e\}$

Let $(H, *)$ be cyclic subgroup

$\therefore H = < a^m> \ni m|p \Rightarrow m = 1$ or $m = p$

If $m = 1 \Rightarrow H = <a> = G$ (not proper subgroup)

If $m = p \Rightarrow H = <a^p = e> = \{e\}$ (not proper subgroup)

$\therefore$ G has no proper subgroup.

Examples 2.40: Find all subgroup of $(Z_7, +_7)$

Solution: $o(Z_7) = 7$, let $H = <(\bar{1})^m > \ni m|7$

$\therefore m = 1$, $m = 7$

If $m = 1 \Rightarrow H_1 = <\bar{1}> = Z_7$

If $m = 7 \Rightarrow H_2 = <(\bar{1})^7> = \{\bar{0}\}$.