THM

Every subgroup of a cyclic group is cyclic.

proof:- Let $(G,\circ)$ be a cyclic group generated by $a$ and let $(H,\circ)$ be a subgroup of $G$. If $H=G$ there is nothing to prove. We consider two cases.

case-I :- If $H=\{e\}$. since $e^n=e$ for all $n\in Z$

$H=\{e^n : n\in Z\}$

$\therefore H$ is the cyclic group generated by $e$.

case-II :- $H$ is a proper subgroup of $G$ other than the trivial subgroup. Then there is an element $x$ in $H$ such that $x\neq e$. since $x\in G$, $x=a^k$ for some integer $k\neq 0$.

since $H$ is a subgroup $x^{-1}\in H$ and $x^{-1}=a^{-k}$.

so, $a^k$ and $a^{-k}$ both belong to $H$ for some integer $k\neq 0$.

Therefore there are some positive integral power of $a$ in $H$.

Let $m$ be the least positive integer such that $a^m\in H$. such an $m$ exists by well ordering property of the set $N$.

We propose to prove that $a^m$ is a generator of $H$. Let $h$ be an element of $H$. Then $h=a^p$ for some integer $p$. By division algorithm

there exists integers ~~p and~~ q and r such that $p = qm + r$. where $0 \leq r < m$.

since H is a subgroup $a^m \in H \Rightarrow a^{-qm} \in H$

also $a^p \in H$ and $a^{-qm} \in H \Rightarrow a^{p-qm} \in H \Rightarrow a^r \in H$

but $0 \leq r < m$ and $a^r \in H$ are both satisfied only if $r = 0$ because otherwise m fails to be the smallest positive integral power a in H.

consequently, $p = qm$ and therefore $h = \langle a^m \rangle^q$ where q is an integer.

Hence $H = \langle a^m \rangle$ and the proof is complete.

Note-1 :-

If a subgroup H of a finite cyclic group $G = \langle a \rangle$ of order n is generated by $a^m$ then m is a divisor of n.

Note→2 :- For a cyclic group G, the cyclic subgroups generated by different elements of G are the only subgroups of G.

Some Remarks :-

(1) Every cyclic group of prime order has no proper non trivial subgroup.

(2) A cyclic group of finite order n has one and only one subgroup of order d for every positive divisor d of n.

Prove that $(\mathbb{Q}, +)$ is a non cyclic group. Deduce that the group $(\mathbb{R}, +)$ is non cyclic.

Proof:- If possible let $(\mathbb{Q}, +)$ be a cyclic group generated by an element $a$. Then $a$ is a non zero element of $\mathbb{Q}$.

Since $a$ is a generator of the additive cyclic group $(\mathbb{Q}, +)$, every element of $\mathbb{Q}$ must be expressed as $ma$ where $m$ is an integer.

But $\frac{1}{2}a \in \mathbb{Q}$ and $\frac{1}{2}a$ cannot be expressed as $ma$ for some integer $m$. Therefore $a$ is not a generator of $(\mathbb{Q}, +)$

This proves that $(\mathbb{Q}, +)$ is not a cyclic group.

$(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$. If $(\mathbb{R}, +)$ be cyclic then $(\mathbb{Q}, +)$ being a subgroup of the cyclic group $(\mathbb{R}, +)$ must be cyclic

But $(\mathbb{Q}, +)$ is not cyclic and therefore $(\mathbb{R}, +)$ is not cyclic.

Let $n$ be a positive integer and let $S$ be the set of $n$th roots of unity. Show that $(S, \cdot)$ is a cyclic group. Find all possible generators.

The elements of $S$ are $1, \alpha, \alpha^2, \cdots \alpha^{(n-1)}$ where $\alpha = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

$S$ be a finite group with respect to multiplication and $o(S) = n$. $n$ is the least

positive integer such that $a^n = 1$

$\therefore O(a) = n$

since S is a finite group containg n elements and $a \in S$ with $O(a) = n$ ; $(S, \cdot)$ is a cyclic group generated by $a$.

If r is a positive integer then $a^r$ is a generator of the group iff r is less than n and prime to n.

THM Let G be an infinite cyclic group generated by a. prove that a and $a^{-1}$ are the only generators of the group.

proof:- Let b be a generator of the group. since $b \in G$ and a is a generator, $b = a^m$ for some integer m.

since $a \in G$ and b is a generator, $a = b^p$ for some integer p.

so, $a = b^p = (a^m)^p$ this implies $a^{(mp-1)} = e$ where e being the identity element.

since $G = \langle a \rangle$ and $O(G)$ is infinite, $O(a)$ is infinite

since $O(a)$ is infinite and $a^{(mp-1)} = e$ so $mp = 1$

so either $m = 1$ and $p = 1$ or $m = -1$ and $p = -1$

$\therefore b = a$ or $b = a^{-1}$ and the proof is complete.