Si nuestro conjunto X es finito, digamos $X=\{a,b,c\}$, entonces escribimos $\langle X\rangle=\langle a,b,c\rangle$.

Def: Un grupo G es llamado cíclico si existe $g\in G$ tal que $G=\langle g\rangle$.

Cor. Sea $g\in G$. Entonces $\langle g\rangle=\{g^n \mid n\in\mathbb{Z}\}$.

Lema: Sea $G=\langle g\rangle$ cíclico. Sea $H\leq G$ y sea $n\geq 1$ el menor natural tal que $g^n\in H$. Entonces

a) $g^m\in H$ si y solo si $n|m$.

b) $H=\langle g^n\rangle$

Unas observaciones: Si $o(g)=\infty$ y $H=e$, entonces no existe tal n.

En cualquier otro caso, ya sea $o(g)<\infty$ ó $H\neq e$. Si $o(g)<\infty$, ent $g^{o(g)}=e\in H$. Por buen orden puedo encontrar el menor natural ≥ 1 y. $g^n\in H$.

Si $H \neq e$, entonces existe $e \neq h \in H$. Como $G = \langle g \rangle$ entonces $g^r = h \in H$. Por lo tanto existe $n \geq 1$ mínimo con la propiedad $g^n \in H$.

Dem:

a) $\Rightarrow$ Sup. $g^m \in H$. Por el algoritmo de la división $m = nq + r$ con $r = 0$ ó $r < n$. Entonces

$$g^r = g^{m-nq} = g^m (g^n)^{-q} \in H$$ contradiciendo la minimalidad de n. $\therefore r = 0$ y así $n \mid m$.

$\Leftarrow$ Sup que $n \mid m$ i.e. $\exists q \in \mathbb{Z}$, $nq = m$. Así

$g^m = g^{nq} = (g^n)^q \in H$.

b) Como $g^n \in H$, $\langle g^n \rangle \subseteq H$. Sea $h \in H$. Como $G = \langle g \rangle$, $h = g^r$. Por (a), n/r ie $nq = r$. Por lo tanto $h = g^r = g^{nq} = (g^n)^q \in \langle g^n \rangle$ $\therefore H = \langle g^n \rangle$.

Cor. Todo subgrupo de un grupo cíclico es cíclico.

Dem:
$H \leq \langle g \rangle$. Si $H = e$ ✓ Si $H \neq e$, existe $n \geq 1$ mínimo tal que $g^n \in H$. $\therefore H = \langle g^n \rangle$.

Lema: Sea $g \in G$ con $o(g) = n < \infty$. Entonces

a) $g^m = e$ si y solo si $n | m$.

b) $g^m = g^l$ si y solo si $m \equiv l \mod n$

c) $|\langle g \rangle| = n$

Dem:

a) Tomemos el subgrupo $\langle g \rangle$ y sea $H = \{e\} \leq \langle g \rangle$.
Entonces $g^n = e$ y n es el menor con esta propiedad.
Por el lema anterior, $g^m = e \iff n \mid m$

b) $g^m = g^l \iff (g)^{m-l} = e \underset{(a)}{\iff} n \mid m-l \iff m \equiv l \mod n$.

c) Por (b) hay una biyeccion entre los elementos de $\langle g \rangle$ y las clases de equivaleneia de enteros módulo n. Por lo tanto, $|\langle g \rangle| = n$.

Teorema:

Sea G un grupo cíclico de orden n. Entonces G tiene exactamente un subgrupo de orden d para cada divisor d de n; y esos son todos los subgrupos de G.

Dem:

Sup. $G=\langle g\rangle$. Por el lema anterior $o(g)=n$.
Sea d un divisor de n, ie, $dt=n$ con $t\in\mathbb{Z}$.
Sea $H_d=\langle g^t\rangle$. Tenemos que $(g^t)^d=g^{dt}=g^n=e$
Entonces $o(g^t)\mid d$. Esto implica $o(g^t)\leq d$.
Por lo tanto, $o(g^t)t\leq dt=\underline{n}$. Pero
$(g^t)^{o(g^t)}=g^{o(g^t)t}=e$. Como $o(g)=n$,

$o(g^t)\,t = n = dt$. Así $o(g^t) = d$. Por el lema anterior, $|\langle g^t \rangle| = |H| = d$.

Ahora, sea $H \leq G$. Como G es cíclico, H también. Entonces $H = \langle g^d \rangle$, tal que $d \mid m$ para cualquier potencia $g^m \in H$. En particular, $g^n = e \in H$. Por lo tanto $d \mid n$. ∎

Recordemos que dados dos enteros a y b (alguno distinto de cero) el máximo común divisor de a y b es un entero d que cumple:

i) $d|a$ y $d|b$

ii) Si $g|a$ y $g|b$ entonces $g|d$.

y es denotado como $d=mcd(a,b)$.

Para un entero positivo n, podemos considerar el conjunto de todos los enteros positivos primos relativos con n y menores que n, es decir,

$$U_n = \{0 \leq r < n \mid mcd(r,n)=1\}$$

La función φ de Euler, se define para $n>0$ como $\varphi(n)=|U_n|$.