Teorema.

Sea $G=\langle g\rangle$ un grupo cíclico finito de orden n. Entonces G contiene exactamente $\varphi(n)$ elementos de orden n y éstos son los elementos g^r con $r\in U_n$.

Dem:

Notemos que $G=\{e, g, g^2, \dots, g^{n-1}\}$

Debemos probar que $o(g^r)=n \iff mcd(r,n)=1$

$\Rightarrow$| Sup $mcd(r,n)>1$. Entonces $d=\frac{n}{mcd(r,n)}<n$

Note que $g^{rd}=g^{\frac{rn}{mcd(r,n)}}=(g^n)^{\frac{r}{mcd(r,n)}}=\underline{e}$. Por lo tanto $o(g^r)\mid d$. Esto implica que

$o(g^r)\leq d<n$.

$\Leftarrow$ Sup. que $\mcd(r,n)=1$. Sea $t>0$ mínimo con la propiedad de que $g^t \in \langle g^r \rangle$. Por un lema anterior $t \mid r$. Por otro lado $g^n = e \in \langle g^r \rangle$ Por el mismo lema, $t \mid n$. Entonces $t \mid \mcd(r,n)=1$, así que $t=1$. Esto implica $g \in \langle g^r \rangle$ y así $G = \langle g \rangle = \langle g^r \rangle$ Por lo tanto $o(g^r)=n$.

Teorema.

Sean B y C grupos cíclicos finitos de orden n. Entonces $B \cong C$ y hay exactamente $\varphi(n)$ isomorfismos diferentes de B en C.

Dem:

Fijamos $b \in B$ tal que $B = \langle b \rangle$ y tomamos un iso $\theta : B \to C$. Entonces, dado $\underline{c = \theta(b)}$ se tiene que $\theta(b^m) = c^m \ \forall m \in \mathbb{Z}$. Por lo tanto θ está totalmente determinado por su valor en b. Dado $x \in C$, existe $b^m \in B$ tal que $c^m = \theta(b^m) = x$. Por lo tanto c es un generador de C.

$$\{\theta : B \to C \mid \theta \text{ iso}\} \longrightarrow \{\text{generadores de } C\}$$
$$\theta \longmapsto \theta(b) = c$$

Esta asignación es inyectiva. Sea c un generador de C, ie, $C = \langle c \rangle$. Sea $\theta : B \to C$ definido como $\theta(b^m) = c^m \ \forall m \in \mathbb{Z}$

Notemos que

$$b^m = b^l \iff m \equiv l \bmod n \iff c^m = c^l \iff \theta(b^m) = \theta(b^l)$$

Por lo tanto θ está bien definida y es inyectiva. Como $|B| = |C| = n$, θ es biyectiva

Falta ver que θ es un isomorfismo de grupos

Sean $b^l, b^m \in B$. Entonces

$$\theta(b^l b^m) = \theta(b^{l+m}) = c^{l+m} = c^l c^m = \theta(b^l)\theta(b^m)$$

Esto prueba que hay tantos isomorfismos entre B y C como generadores de C, es decir, hay $\varphi(n)$ isomorfismos. ∎

Notemos que $(\mathbb{Z}, +)$ y $(\mathbb{Z}/n\mathbb{Z}, +)$ (con $n>1$) son grupos cíclicos.

Como para cada $n \geq 1$, está el grupo cíclico $(\mathbb{Z}/n\mathbb{Z}, +)$ de enteros módulo

El teorema anterior me dice que un grupo cíclico G de orden $n \geq 2$ es isomorfo

a $\mathbb{Z}/n\mathbb{Z}$

∎

Notemos que todo grupo cíclico es abeliano. En general no todo grupo abeliano es cíclico y un contraejemplo es $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(x,y) \mid x,y \in \mathbb{Z}_2\}$ con la suma coordenada a coordenada. Es decir, $(x,y)+(x',y') = (x+x', y+y')$

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(1,0),(0,1),(1,1)\}$ $\quad |\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$

$(1,0)+(1,0) = (1+1,0) = (0,0)$ $\quad \mathbb{Z}_2 = \{0,1\}$

$(0,1)+(0,1) = (0,1+1) = (0,0)$

$\theta(1,0) = 2 = \theta(0,1) \quad \therefore |\langle(1,0)\rangle| = 2 = |\langle(0,1)\rangle|$

Esto implica que $\mathbb{Z}_2 \times \mathbb{Z}_2$ no puede ser cíclico.

Si tenemos un grupo en general, nos interesa saber que tan "abeliano" es. Dado un grupo G y $g \in G$ se define el centralizador de g en G como el subconjunto de G: