$(G, *, e)$ un grupo, $g \in G$

$\langle g \rangle = \{ g^n : n \in \mathbb{Z} \}$ subgrupo generado por g

$\rightarrow \quad |\langle g \rangle| = o(g)$

G es un grupo cíclico si existe $g \in G$ tal que $\underset{\substack{\uparrow \\ \text{generador de } G}}{\langle g \rangle} = G$

Si G es finito, entonces

G es cíclico $\Leftrightarrow$ existe $g \in G$ tal que $o(g) = |G|$

$$\left.\begin{array}{l} o(g) = |\langle g \rangle| \\ o(g) = |G| \end{array}\right\} \Rightarrow |\langle g \rangle| = |G| \Rightarrow \langle g \rangle = G$$

Ejercicio 9. Considere los grupos $\mathbb{Z}_4$, $U(5)$ y $U(6)$. Para cada uno de estos grupos:

a. Hallar el orden de cada uno de los elementos del grupo.

b. Determinar si el grupo es cíclico.

c. En caso de que el grupo sea cíclico, calcular todos sus elementos generadores.

(1) $\mathbb{Z}_4 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \}$

$\bar{a} + \bar{b} = \overline{a+b}$

neutro: $\bar{0}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\bar{1} + \bar{1} = \overline{1+1} = \bar{2}$

$\bar{1} + \bar{3} = \bar{4} = \bar{0}$

* el orden de $\bar{0}$ $\rightarrow o(\bar{0}) = 1$
* el orden de $\bar{1}$

$\bar{1}^2 = \bar{1} + \bar{1} = \bar{2}$

$\bar{1}^3 = \bar{1} + \bar{1} + \bar{1} = \bar{3}$

$\bar{1}^4 = \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{0}$ $\qquad \bar{1}^5 = \bar{1}^4 + \bar{1}^1 = \bar{0} + \bar{1} = \bar{1}$

$\Rightarrow 4 = \min \{ n \in \mathbb{Z}^+ : \bar{1}^n = \bar{0} \}$

$\Rightarrow o(\bar{1}) = 4 = |\mathbb{Z}_4| \Rightarrow \mathbb{Z}_4$ es cíclico

$\langle \bar{1} \rangle = \{ \bar{1}, \bar{2}, \bar{3}, \bar{0} \} = \mathbb{Z}_4$

$\Rightarrow \mathbb{Z}_4$ es un grupo cíclico y $\bar{1}$ es un generador

* orden de $\bar{2}$

$\bar{2}^2 = \bar{2} + \bar{2} = \bar{0}$

$\Rightarrow o(\bar{2}) = 2 < |\mathbb{Z}_4|$

$\langle \bar{2} \rangle = \{ \bar{2}, \bar{0} \}$ $\Rightarrow \bar{2}$ no es generador de $\mathbb{Z}_4$

* orden de $\bar{3}$

$\bar{3}^2 = \bar{3} + \bar{3} = \bar{2}$

$\bar{3}^3 = \bar{3} + \bar{3} + \bar{3} = \bar{1}$

$\bar{3}^4 = \bar{3} + \bar{3} + \bar{3} + \bar{3} = \bar{2} + \bar{2} = \bar{0}$

$4 = \min \{ n \in \mathbb{Z}^+ : \bar{3}^n = \bar{0} \}$

$\Rightarrow o(\bar{3}) = 4 = |\mathbb{Z}_4|$

$\langle \bar{3} \rangle = \{ \underset{\bar{3}}{\bar{3}^1}, \underset{\bar{2}}{\bar{3}^2}, \underset{\bar{1}}{\bar{3}^3}, \underset{\bar{0}}{\bar{3}^4} \} = \mathbb{Z}_4$ $\Rightarrow \bar{3}$ es un generador de $\mathbb{Z}_4$

② $U(5)$ = enteros invertibles modulo 5

$\mathbb{Z}_5 = \{ \cancel{\bar{0}}, \underbrace{\bar{1}, \bar{2}, \bar{3}, \bar{4}}_{\text{coprimos con } 5} \}$

$U(5) = \{ \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$

$\bar{a}\,\bar{b} = \overline{ab}$

neutro: $\bar{1}$

$\times$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\bar{2} \times \bar{2} = \overline{2 \cdot 2} = \bar{4}$

$\bar{2} \times \bar{3} = \overline{2 \cdot 3} = \bar{6} = \bar{1}$

$\bar{2} \times \bar{4} = \overline{2 \cdot 4} = \bar{8} = \bar{3}$

* orden de $\bar{2}$

$\bar{2}^2 = \bar{2} \times \bar{2} = \bar{4}$

$\bar{2}^3 = \bar{4} \times \bar{2} = \bar{3}$

$\bar{2}^4 = \bar{3} \times \bar{2} = \bar{1}$

$\Rightarrow o(\bar{2}) = 4$

$\langle \bar{2} \rangle = \{ \bar{2}^1, \bar{2}^2, \bar{2}^3, \bar{2}^4 \} = U(5)$

$\bar{2}^1 = \bar{2}$, $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{3}$, $\bar{2}^4 = \bar{1}$

$\Rightarrow$ $U(5)$ es cíclico y $\bar{2}$ es un generador

*orden de $\bar{4}$

$\bar{4}^2 = \bar{4} \times \bar{4} = \bar{1}$

$o(\bar{4}) = 2$

$\langle \bar{4} \rangle = \{ \bar{4}^1, \bar{4}^2 \} = \{ \bar{4}, \bar{1} \}$

$\bar{4}^1 = \bar{4}$, $\bar{4}^2 = \bar{1}$

$\Rightarrow$ $\bar{4}$ no es generador de $U(5)$

* orden de $\bar{3}$

$6 = 2 \cdot 3$

② $U(6) = \{ \bar{1}, \bar{5} \}$ $\quad |U(6)| = \varphi(6) = 6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 6 \frac{1}{2} \frac{2}{3} = 2$

$\mathbb{Z}_6 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$

$\bar{1}$: coprimo con 6

$\bar{0}, \bar{2}, \bar{3}, \bar{4}$: no son coprimos con 6

$\bar{5}$: coprimo con 6

orden de $\bar{5}$

$\bar{5}^2 = \bar{5} \times \bar{5} = \bar{1}$

$o(\bar{5}) = 2 = |U(6)|$ $\Rightarrow$ $U(6)$ es cíclico y $\bar{5}$ es generador

$\langle \bar{5} \rangle = \{ \bar{5}^1, \bar{5}^2 \} = \{ \bar{5}, \bar{1} \} = U(6)$

Ejercicio 4. Sea G un grupo. Probar que $a^n = e_G \Leftrightarrow o(a)|n$.

G un grupo, $a \in G$

$a^n = e_G \iff o(a) | n$

$a^{o(a)} = e_G$

$(\Rightarrow)$ tenemos $a^n = e_G$

$n = o(a)q + r$ con $\underbrace{0 \leq r < o(a)}$ queremos probar que $r = 0$

$a^n = e_G \Rightarrow a^{o(a)q + r} = e_G$

$\Rightarrow a^{o(a)q} a^r = e_G$

$\Rightarrow \underbrace{(a^{o(a)})^q}_{e_G} a^r = e_G$

$\left.\begin{array}{l} \Rightarrow a^r = e_G \\ 0 \leq r < o(a) \end{array}\right] \Rightarrow r = 0 \Rightarrow n = o(a)q \Rightarrow o(a) | n$

$(\Leftarrow)$ $o(a) | n$ queremos ver que $a^n = e_G$

$o(a) | n \Rightarrow n = o(a) q$ con $q \in \mathbb{Z}$

$a^n = a^{o(a)q} = (\underset{\underset{e_G}{\shortparallel}}{a^{o(a)}})^q = e_G$

Ejercicio 5. Considere un grupo cíclico finito G de orden n, con **generador** $g \in G$.

a. Probar que $g^k = g^m$ si y solo si $k \equiv m \pmod{n}$

b. Sea $d = \operatorname{mcd}(m, n)$. Sean n^* y m^* los cofactores de m y n. Es decir: $n = dn^*$, $m = dm^*$ y $\operatorname{mcd}(m^*, n^*) = 1$. Probar que el orden de g^m es n^*. Es decir: $o(g^m) = \frac{n}{d} = \frac{o(g)}{\operatorname{mcd}(m, o(g))}$.

c. Probar que g^m es también un generador de G si y solo si $\operatorname{mcd}(m, n) = 1$.

d. Usando la parte anterior, probar que G tiene $\varphi(n)$ generadores.

G grupo cíclico finito

$|G| = n$

g un generador de G $\Rightarrow o(g) = n$

$o(g) = |\langle g \rangle| = |G| = n$

$g^{\alpha} = e_G \iff o(g) \mid \alpha$

orden de g

a) $g^k = g^m \iff \underbrace{k \equiv m \pmod{n}}_{n \mid k-m}$

$(\Rightarrow)$ $g^k = g^m \Rightarrow g^k g^{-m} = g^m g^{-m}$

$\Rightarrow g^{k-m} = e_G$

$\Rightarrow n \mid k-m$ porque $n = o(g)$

$\Rightarrow k \equiv m \pmod{n}$

$(\Leftarrow)$ $k \equiv m \pmod{n} \Rightarrow n \mid k-m$

$\Rightarrow g^{k-m} = e_G$ porque $n = o(g)$

$\Rightarrow g^{k-m} g^m = e_G g^m$

$\Rightarrow g^k = g^m$

b) Sea $d = \mathrm{mcd}(m,n) \rightsquigarrow \begin{cases} n = dn^* \\ m = dm^* \\ \mathrm{mcd}(n^*, m^*) = 1 \end{cases} \rightsquigarrow g^{dn^*} = e_G$

Queremos probar que $o(g^m) = n^*$

$*$ $(g^m)^{n^*} = e_G$?

$$(g^m)^{n^*} = (g^{dm^*})^{n^*} = (g^{dn^*})^{m^*} = (\underbrace{g^n}_{e_G})^{m^*} = e_G$$

$*$ Sea $k \in \mathbb{Z}^+$ tal que $(g^m)^k = e_G$, queremos ver que $k \geq n^*$

$(g^m)^k = e_G$

$(g^m)^{n^*} = e_G$

$\Rightarrow (g^m)^{n^*} = (g^m)^k \Rightarrow g^{mn^*} = g^{mk}$

entonces $n \mid mn^* - mk$ $\qquad mn^* = mk \pmod{n}$

$$mn^* = mk \pmod{n}$$

$$dm^*n^* \equiv dm^*k \pmod{n}$$

$$m^*n^* \equiv m^*k \pmod{n^*}$$

$$n^* \equiv k \pmod{n^*}$$

$$\left.\begin{array}{l} k > 1 \\ k \text{ multiplo de } n^* \end{array}\right\} k \geq n^*$$

Probamos: $o(g^m) = \dfrac{n}{mcd(m,n)}$ donde $n = o(g)$

c) $\underbrace{g^m \text{ también es generador de } G}_{o(g^m) = n} \Leftrightarrow mcd(m,n) = 1$

($\Leftarrow$) $\quad o(g^m) = \dfrac{n}{\underbrace{mcd(m,n)}_{=1}} = n$

$$\Rightarrow o(g^m) = n \Rightarrow g^m \text{ es un generador}$$

($\Rightarrow$) Supongamos que $mcd(m,n) > 1$

$$o(g^m) = \dfrac{n}{\underbrace{mcd(m,n)}_{>1}} < n$$

$$o(g^m) < |G| \Rightarrow \langle g^m \rangle \subsetneq G$$

$\Rightarrow g^m$ no es generador absurdo!

a) G tiene $\varphi(\overset{n}{\overset{\shortparallel}{|G|}})$ generadores

$$G = \langle g \rangle = \{e, g, g^2, g^3, \ldots\ldots, g^{\overset{|G|-1}{\overbrace{o(g)-1}}}\}$$

g^m es generador de G sii $mcd(m, \underset{|G|}{\underset{\shortparallel}{n}}) = 1$

$$\# \text{ generadores} = \# \{ m : 1 \leq m \leq |G| - 1 \ , \ \text{mcd}(m, |G|) = 1 \}$$

$$= \varphi(|G|)$$

$$= \varphi(n)$$