Ejercicio 3. Sea G un grupo. Probar que $o(xy) = o(yx)$, $\forall\, x, y \in G$.

$n = o(xy) \rightarrow (xy)^n = e_G$ y n es la mínima potencia ≥ 1 que cumple esto

$m = o(yx) \rightarrow (yx)^m = e_G$ y m es la menor potencia ≥ 1 que cumple esto

Queremos probar que $n = m$

vamos a probar que $n \geq m$ y que $m \geq n$

* $n \geq m$ para ver esto vamos a probar $(yx)^n = e_G$

$$(xy)^n = e_G \Rightarrow xyxyxy \cdots xy = e_G$$
$$\Rightarrow x^{-1}xyxyx \cdots xyx = x^{-1}e_G x$$
$$\Rightarrow yxyx \cdots yx = e_G$$
$$\Rightarrow (yx)^n = e_G$$

$$\left.\begin{array}{l} (yx)^n = e_G \\ o(yx) = m \end{array}\right\} \Rightarrow m \leq n$$

* $n \leq m \rightarrow$ vamos a probar que $(xy)^m = e_G$

$$(yx)^m = e_G \Rightarrow yxyx \cdots yx = e_G$$
$$\Rightarrow y^{-1}yxyx \cdots yxy = y^{-1}e_G y$$
$$\Rightarrow xyxy \cdots xy = e_G$$
$$\Rightarrow (xy)^m = e_G$$

$$\left.\begin{array}{l} (xy)^m = e_G \\ o(xy) = n \end{array}\right\} \Rightarrow m \geq n$$

Otra forma:

$$(xy)^k = e_G \Leftrightarrow xyxy \cdots xy = e_G$$
$$\Leftrightarrow x^{-1}xyxy \cdots xyx = x^{-1}e_G x$$
$$\Leftrightarrow (yx)^k = e_G$$

$\{k \in \mathbb{Z}^+ : (xy)^k = e_G\} = \{k \in \mathbb{Z}^+ : (yx)^k = e_G\}$

$\Rightarrow o(xy) = o(yx)$

Ejercicio 11. Sea G un grupo, con $G \neq \{e\}$. Probar las siguientes afirmaciones.

a. Si G es cíclico, todo subgrupo de G también es cíclico. Sugerencia: sea g un generador de G. Dado un subgrupo H, considere la menor potencia $m \geq 1$, tal que $g^m \in H$.

b. Si los únicos subgrupos de G son los triviales, entonces G es cíclico, finito y $|G|$ es primo.

G un grupo, $G \neq \{e\}$

b) los únicos subgrupos de G son los triviales

H subgrupo de $G \Rightarrow H = \{e\}$ o $H = G$

1 G cíclico $\leftarrow$ buscamos $x \in G$ tal que $\langle x \rangle = G$

sea $x \in G$, $x \neq e_G$

$\langle x \rangle$ es un subgrupo de G

como $x \neq e_G$ tenemos $\langle x \rangle \neq \{e_G\}$

entonces $\langle x \rangle = G$

$\Rightarrow G$ es cíclico y x es un generador

2 G finito

Supongamos por absurdo que G no es finito.

Sea $x \in G$ tal que $x \neq e_G$

$\Rightarrow \langle x \rangle = G$

$\Rightarrow \boxed{o(x) = \infty}$

$x^2 \neq e_G$

por lo que probamos en 1, x^2 es un generador

$\langle x^2 \rangle = G$

entonces $x \in \langle x^2 \rangle$

$\Rightarrow x = (x^2)^k$ para algún $k \in \mathbb{Z}$

$\Rightarrow x = x^{2k}$

$\Rightarrow x x^{-1} = x^{2k} x^{-1}$

$\Rightarrow \boxed{e_G = x^{2k-1}} \Rightarrow o(x) \leq 2k-1$ Absurdo!

③ $|G|$ es primo

Supongamos por absurdo que $|G|$ no es primo

$|G| = ab$ con $a, b \neq 1$

sea $x \in G$, $x \neq e_G$

por lo que probamos en ①, x es generador de G

$$\langle x \rangle = G$$

$o(x) = |\langle x \rangle| = |G|$

$\langle x \rangle = G \Rightarrow o(x) = |G| = ab$

buscamos subgrupo no trivial de G

buscamos $\langle y \rangle$ con

$1 < o(y) < ab$

$x^{ab} = e_G$

$(x^a)^b = e_G$

$\Rightarrow o(x^a) \leq b$

tenemos $\times$ $o(x) = ab \Rightarrow x^a \neq e_G \Rightarrow \{e\} \subsetneq \langle x^a \rangle$

$\times$ $o(x^a) \leq b \Rightarrow |\langle x^a \rangle| \leq b < |G| \Rightarrow \langle x^a \rangle \subsetneq G$

$\langle x^a \rangle$ es un subgrupo no trivial

Absurdo!

Grupo cociente

construcción de $\mathbb{Z}_n$

$(\mathbb{Z}, +)$ grupo

definimos la relación de equivalencia

$a \sim b$ sii $a \equiv b \pmod n \Leftrightarrow a - b = nq$

$\mathbb{Z}_n = \{ \overline{a} : a \in \mathbb{Z} \}$ conjunto de clases de equivalencia

$(\mathbb{Z}_n, +)$ es un grupo

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

otra forma de ver la construcción de $\mathbb{Z}_n$

$(\mathbb{Z},+)$ grupo

$n\mathbb{Z} = \{nq : q \in \mathbb{Z}\}$ multiplos de n

$n\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$ (subgrupo normal)

definimos la relación de equivalencia

$a \sim b$ sii $a-b \in n\mathbb{Z}$

$\mathbb{Z}/_{n\mathbb{Z}} = \{\bar{a} : a \in \mathbb{Z}\}$

$\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n$

$(\mathbb{Z}/n\mathbb{Z}, +)$ en un grupo con la suma $\bar{a} + \bar{b} = \overline{a+b}$

Generalizamos

G un grupo

H subgrupo normal de G

definimos la relación de equivalencia

$x \sim y$ sii $xy^{-1} \in H$ sii $x \in Hy$

$G/_H = \{\bar{x} : x \in G\}$ conjunto de clases de equivalencia

queremos que $G/_H$ sea un grupo con la operación

$$\bar{x}\bar{y} = \overline{xy}$$

$\rightarrow$ la operación está bien definida:

$$\left.\begin{array}{l}\bar{x} = \bar{x'} \\ \bar{y} = \bar{y'}\end{array}\right\} \Rightarrow \underbrace{\overline{xy} = \overline{x'y'}}$$ $\Leftarrow$ $xy \sim x'y' \Leftarrow (xy)(x'y')^{-1} \in H$

$\bar{x} = \bar{x}' \Rightarrow x \sim x' \Rightarrow x(x')^{-1} \in H$

$\Rightarrow x(x')^{-1} = h_1$ para algún $h_1 \in H$

$\Rightarrow x = h_1 x'$

$\bar{y} = \bar{y}' \Rightarrow y \sim y' \Rightarrow y(y')^{-1} \in H \Rightarrow y(y')^{-1} = h_2$ con $h_2 \in H$

$\Rightarrow y = h_2 y'$

$$xy = h_1 x' h_2 y' = h_1 x' h_2 (x')^{-1} x' y'$$

$$\Rightarrow xy(x'y')^{-1} = h_1 \underbrace{x' h_2 (x')^{-1}}_{\in H} \in H \,?$$

H subgrupo normal : $gHg^{-1} = H \;\; \forall g$