# Ejercicio 1

c. Hallar elementos $a, b \in \mathbb{Z}_2 \times \mathbb{Z}$ que cumplan: $o(a) = o(b) = \infty$, $o(a+b)$ finito y mayor a 1. La operación del grupo es la suma coordenada a coordenada.

$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ $\quad \bar{x} + \bar{y} = \overline{x+y}$

el neutro es $\bar{0}$

$\rightarrow o(\bar{0}) = 1$

$o(\bar{1}) = 2$ $\qquad \bar{0} = \{0, 2, -2, 4, -4, \ldots\}$

$\bar{1} \neq \bar{0}$

$\bar{1}^2 = \bar{1} + \bar{1} = \overline{1+1} = \bar{2} = \bar{0}$

$\mathbb{Z}_2 \times \mathbb{Z} = \{(\bar{0},0), (\bar{0},1), (\bar{0},-1), (\bar{0},2), \ldots, (\bar{1},0), (\bar{1},1), (\bar{1},-1), (\bar{1},2) \ldots\}$

$\rightarrow$ la operación es la suma coordenada a coordenada

$$(\bar{x}, n) + (\bar{y}, m) = (\overline{x+y}, n+m)$$

neutro de $\mathbb{Z}_2 \times \mathbb{Z}$ es $(\bar{0}, 0)$

$$(\bar{x}, n) + (\bar{0}, 0) = (\bar{x}, n)$$

$*$ buscamos $a \in \mathbb{Z}_2 \times \mathbb{Z}$ tal que $o(a)$ sea infinito

$a = ( \;\; , 0)$ $\rightarrow$ $a = (\bar{0}, 0) \leftarrow$ orden 1

$\uparrow$ $\qquad \rightarrow$ $a = (\bar{1}, 0) \leftarrow$ orden 2

$$(\bar{1},0) + (\bar{1},0) = (\overline{1+1}, 0+0) = (\bar{0}, 0)$$

para que a tenga infinito la segunda entrada no puede ser 0

$a = (\bar{0}, 1)$

$a + a = (\bar{0}, 1) + (\bar{0}, 1) = (\bar{0}, 2)$

$a + a + a = (\bar{0}, 1) + (\bar{0}, 1) + (\bar{0}, 1) = (\bar{0}, 3)$

$$a^n = \underbrace{(\bar{0},1) + (\bar{0},1) + \cdots + (\bar{0},1)}_{n \text{ veces}} = (\bar{0}, n)$$

$a^n = (\bar{0}, n)$

entonces $a^n \neq (\bar{0}, 0)$ para todo $n \in \mathbb{Z}^+$

$\Rightarrow$ a tiene orden infinito

* buscamos b tal que: $o(b) = \infty \rightarrow b = ( \; , \; )$ distinta de 0

$1 < \underbrace{o(a+b) < \infty}_{a+b = ( \; , 0)}$

$a = (\bar{0}, 1)$

$b = ( \; , -1)$

$\rightarrow b = (\bar{0}, -1) \rightsquigarrow a+b = (\bar{0}, 1) + (\bar{0}, -1) = (\bar{0}, 0)$

$\rightarrow o(a+b) = 1$

$\rightarrow b = (\bar{1}, -1)$

$\rightarrow a+b = (\bar{0}, 1) + (\bar{1}, -1) = (\bar{1}, 0)$

$(\bar{1}, 0) \neq (\bar{0}, 0)$

$(\bar{1}, 0) + (\bar{1}, 0) = (\overline{1+1}, 0+0) = (\bar{0}, 0)$

$\Rightarrow o((\bar{1}, 0)) = 2$

$a = (\bar{0}, 1)$

$b = (\bar{1}, -1)$

$$\rightarrow \begin{cases} o(a) = \infty \\ o(b) = \infty \\ o(a+b) = 2 \end{cases}$$

## Grupos cíclicos

$(G, *, e)$ un grupo

$g \in G$

el conjunto de potencias de g es

$$\langle g \rangle = \{ g^n : n \in \mathbb{Z} \} = \{ g, \overbrace{g^2}^{g*g}, \overbrace{g^3}^{g*g*g}, \dots, g^0, g^{-1}, g^{-2}, \dots \}$$

$\langle g \rangle$ es un subgrupo de G llamado subgrupo generado por G

* $o(g) < \infty$

$$\langle g \rangle = \{ \underbrace{g, g^2, g^3, \dots, \overbrace{g^{o(g)}}^{e}}, \overbrace{g^{o(g)+1}}^{g}, \overbrace{g^{o(g)+2}}^{g^2}, \dots \}$$

$\Rightarrow |\langle g\rangle| = o(g)$

$\# \langle g \rangle$

* decimos que $G$ es cíclico si existe algún $g \in G$ tq

$\langle g \rangle = G$

$\rightarrow$ $g$ es un generador de $G$

ejemplo: suma

* $\mathbb{Z}$ es cíclico? $\langle 1 \rangle = \{1, 1+1, 1+1+1, \dots, \underset{\substack{\shortparallel \\ 0}}{1^{0}}, -1, -1-1, -1-1-1, \dots\}$

$\langle 1 \rangle = \mathbb{Z}$ $\rightarrow$ $\mathbb{Z}$ es cíclico y $1$ es un generador

* $\mathbb{Z}_2$ es cíclico? $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

$\langle \bar{1} \rangle = \{\bar{1}, \bar{1}+\bar{1}\} = \{\bar{1}, \bar{0}\} = \mathbb{Z}_2$

$\mathbb{Z}_2$ es cíclico y $\bar{1}$ es un generador

* un grupo $G$ finito es cíclico si existe $g \in G$ tal que $o(g) = |G|$

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

$\Rightarrow \langle g \rangle = G$

porque $G$ tiene que ser finito?

$\mathbb{Z}$ con la suma

$o(2) = \infty$

$\langle 2 \rangle =$ los enteros pares $\Rightarrow$ $2$ no es generador de $\mathbb{Z}$

**Ejercicio 7.** 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.

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

para ver si $\mathbb{Z}_4$ es cíclico buscamos un elemento de orden 4

$o(\bar{0}) = 1$

$$\left.\begin{aligned} \bar1+\bar1&=\bar2\\ \bar1+\bar1+\bar1&=\bar3\\ \bar1+\bar1+\bar1+\bar1&=\bar4=\bar0 \end{aligned}\right\} \Rightarrow o(\bar1)=4$$

$\langle\bar1\rangle=\{\bar1,\bar2,\bar3,\bar0\}$

$\Rightarrow \mathbb{Z}_4$ es cíclico y $\bar1$ lo genera

$\bar2+\bar2=\bar4=\bar0$

$\Rightarrow o(\bar2)=2$

$$\langle\bar2\rangle=\{\bar2,\overset{\bar0}{\overset{\shortparallel}{\overline{\bar2+\bar2}}}\}=\{\bar2,\bar0\}$$

$$\left.\begin{aligned} \bar3+\bar3&=\bar6=\bar2\\ \bar3+\bar3+\bar3&=\bar9=\bar1\\ \bar3^4=\bar3+\bar3+\bar3+\bar3&=\overline{12}=\bar0 \end{aligned}\right\} \Rightarrow o(\bar3)=4$$

$\langle\bar3\rangle=\{\bar3,\bar2,\bar1,\bar0\}=\mathbb{Z}_4$

$\Rightarrow \bar3$ genera $\mathbb{Z}_4$

---

## Grupo de invertibles modulo n

queremos definir un producto en $\mathbb{Z}_n=\{\bar0,\bar1,\bar2,\dots,\overline{n-1}\}$

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

$\nwarrow$ producto de $\mathbb{Z}$

→ esta operación es asociativa

→ el neutro es $\bar1$

$$\bar a\,\bar1=\overline{a\cdot1}=\bar a$$

→ el problema son los inversos

$\bar0$ tiene inverso? $\underbrace{\bar0\,\bar x}_{=\overline{0x}=\bar0}=\bar1$

a es invertible modulo n sii $mcd(a,n)=1$

$$ax\equiv b \pmod n$$

$$a'a\equiv 1 \pmod n$$

$U(n) = \{ \bar{a} \in \mathbb{Z}_n : \text{mcd}(a,n) = 1 \}$

$\uparrow$

grupo de invertibles modulo n

$|U(n)| = \varphi(n)$

para ver si $U(n)$ es cíclico buscamos un elemento con orden igual a $\varphi(n)$

$\mathbb{Z}_5 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$

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

$\varphi(5) = 4$

$\rightarrow o(\bar{1}) = 1$

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

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

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

$\bar{2}^4 = \bar{2}^3 \cdot \bar{2} = \bar{3} \cdot \bar{2} = \bar{6} = \bar{1}$

$\Rightarrow o(\bar{2}) = |U(5)|$

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

$\langle \bar{2} \rangle = \{ \bar{2}, \bar{4}, \bar{3}, \bar{1} \}$

$\rightarrow o(\bar{3}) = 4 \rightarrow \bar{3}$ es otro generador de $U(5)$

$\bar{3}^2 = \bar{3} \cdot \bar{3} = \bar{9} = \bar{4}$

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

$\bar{3}^4 = \bar{3}^3 \cdot \bar{3} = \bar{2} \cdot \bar{3} = \bar{6} = \bar{1}$

$\rightarrow o(\bar{4}) = 2 \rightarrow \bar{4}$ no genera $U(5)$

$\bar{4}^2 = \bar{4} \cdot \bar{4} = \overline{16} = \bar{1}$

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