Grupo de enteros modulo n

n=3

ser congruentes módulo 3 es una relación de equivalencia

podemos considerar las clases de equivalencia

$$\bar{0} = \{x \in \mathbb{Z} : x \equiv 0 \pmod 3\} = \{x \in \mathbb{Z} : x = 3k \text{ con } k \in \mathbb{Z}\}$$
$$= \{\dots -6, -3, 0, 3, 6 \dots\}$$

$$\bar{1} = \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\} = \{x \in \mathbb{Z} : x = 3k+1 \text{ con } k \in \mathbb{Z}\}$$
$$= \{\dots -2, 1, 4, 7 \dots\}$$

$$\bar{2} = \{x \in \mathbb{Z} : x \equiv 2 \pmod 3\} = \{x \in \mathbb{Z} : x = 3k+2 \text{ con } k \in \mathbb{Z}\}$$
$$= \{\dots -1, 2, 5, 8, \dots\}$$

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

queremos darle estructura de grupo a $\mathbb{Z}_3$:

definimos una suma:

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

(suma en $\mathbb{Z}$)

$\bar{2} + \bar{2} = \bar{4} = \bar{1}$

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

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

esta operación es asociativa y el neutro es $\bar{0}$

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

En general, $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ es un grupo con la suma

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

Grupo de los invertibles módulo n

queremos definir un producto en $\mathbb{Z}_n$

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

↖ producto en $\mathbb{Z}$

este producto: * es asociativo

* tiene neutro: $\bar{1}$
* $\bar{0}$ no tiene inverso

$$\bar{0}\,\bar{b} = \overline{0b} = \bar{0} \neq \bar{1}$$

$\bar{a}$ es invertible en $\mathbb{Z}_n \iff$ existe $b \in \mathbb{Z}$ tq $\bar{a}\,\bar{b} = \bar{1}$

$\iff ab \equiv 1 \pmod n$

$\iff$ a y n son coprimos

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

$U(n)$ es un grupo con el producto $\bar{a}\,\bar{b} = \overline{ab}$

$U(n)$ tiene $\varphi(n)$ elementos

Orden

Sea $(G, *, e)$ un grupo y $g \in G$. Definimos el orden de g:

- Si $g^n \neq e$ para todo $n \in \mathbb{Z}^+$, $o(g) = \infty$
- Si no definimos $o(g) = \min\{n \in \mathbb{Z}^+ : \underbrace{g^n}_{g*g*g*\cdots*g} = e\}$

por ejemplo

* $(\mathbb{Z}, +)$, $o(1) = \infty$
* $(\mathbb{Z}_3, +)$, $o(\bar{1}) = 3$ $\quad \bar{1} + \bar{1} = \bar{2}$ $\quad \bar{1} + \bar{1} + \bar{1} = \bar{0} \leftarrow$ neutro

Ejercicio 1.

a. Sean $G = \mathrm{GL}(2,\mathbb{R})$ el grupo multiplicativo de las matrices invertibles 2×2 con coeficientes en $\mathbb{R}$, $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ y $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$. Probar que $o(A) = 4$, $o(B) = 3$, y que AB tiene orden infinito.

b. Sea $(G, \cdot)$ un grupo conmutativo. Probar que si $o(A)$ y $o(B)$ son finitos, entonces $o(AB)$ es finito.

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.

a) $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

$A^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \neq I$

$A^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \neq I$

$A^4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

$\rightsquigarrow 4 = \min\{n \in \mathbb{Z}^+ : A^n = I\} \Rightarrow o(A) = 4$

$B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

$B^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \neq I$

$B^3 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

$\rightsquigarrow 3 = \min\{n \in \mathbb{Z}^+ : B^n = I\} \Rightarrow o(B) = 3$

$AB = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$(AB)^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \neq I$

$(AB)^3 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \neq I$

$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

Vamos a probarlo por inducción:

caso base: $n=1$

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

paso inductivo: suponemos que $(AB)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$

y queremos probar que $(AB)^{k+1} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}$

$$(AB)^{k+1} = (AB)^k (AB)$$

$$= \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix} \checkmark$$

$$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq I \text{ para todo } n \in \mathbb{Z}^+$$

$$\Rightarrow o(AB) = \infty$$

b) G un grupo conmutativo, $a, b \in G$

$$\left.\begin{array}{l} o(a) < \infty \\ o(b) < \infty \end{array}\right\} \Rightarrow o(ab) < \infty$$

para probar que $o(ab) < \infty$ alcanza con encontrar un $k \in \mathbb{Z}^+$ tal que $(ab)^k = e$

$$o(a) = n \Rightarrow a^n = e$$

$$o(b) = m \Rightarrow b^m = e$$

$$(ab)^{nm} \overset{\uparrow}{=} a^{nm} b^{nm} = (\underbrace{a^n}_{\overset{\|}{e}})^m (\underbrace{b^m}_{\overset{\|}{e}})^n = e \checkmark$$

$\uparrow$ G es conmutativo

G es abeliano

$$(ab)^{n+m} = (ab)^n (ab)^m = \overbrace{a^n}^{\overset{\|}{e}} b^n a^m \overbrace{b^m}^{\overset{\|}{e}} = b^n a^m$$

$\uparrow$ G conmutativo

c) $\mathbb{Z}_2 \times \mathbb{Z}$, la operación es la suma coordenada a coordenada

buscamos $a, b \in \mathbb{Z}_2 \times \mathbb{Z}$ tales que: $\begin{cases} o(a) = \infty \\ o(b) = \infty \\ 1 < o(a+b) < \infty \end{cases}$

$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ $\quad o(\bar{1}) = 2 \quad\quad \bar{1} + \bar{1} = \bar{2} = \bar{0}$

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

el neutro es $(\bar{0}, 0)$

* buscamos a tq $o(a) = \infty$

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

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

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

$\Rightarrow o(a) = \infty$

* buscamos b tq $o(b) = \infty$ y $o(a+b) < \infty$

$o(a+b) < \infty \Rightarrow a + b = (\ , 0)$

$\left.\begin{array}{l} a = (\bar{0}, 1) \\ a + b = (\ , 0) \end{array}\right\} \Rightarrow b = (\ , -1)$

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

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

$b^n = \underbrace{b + b + \dots + b}_{n \text{ veces}} = \underbrace{(\bar{1},-1) + (\bar{1},-1) + \dots (\bar{1},-1)}_{n \text{ veces}}$

$b^2 = (\bar{1}, -1) + (\bar{1}, -1) = (\bar{0}, -2)$

$b^3 = (\bar{1}, -1) + (\bar{1}, -1) + (\bar{1}, -1) = (\bar{1}, -3)$

$$b^n = \begin{cases} (\bar{0}, -n) & \text{si } n \text{ es par} \\ (\bar{1}, -n) & \text{si } n \text{ es impar} \end{cases}$$

$b^n \neq (\bar{0}, 0)$ para todo $n \in \mathbb{Z}^+ \Rightarrow o(b) = \infty$

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

$(a+b)^2 = (\bar{1}, 0) + (\bar{1}, 0) = (\bar{0}, 0) \leftarrow$ neutro

$\Rightarrow o(a+b) = 2$

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

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

$= \{ g, g^2, g^3, g^4, g^{-1}, g^{-2}, g^0, \dots \}$

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

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

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

$$\langle g \rangle = G$$

ejemplo: $(\mathbb{Z}_3, +)$ es cíclico?

$\mathbb{Z}_3 = \{ \bar{0}, \bar{1}, \bar{2} \}$ $\quad |\mathbb{Z}_3| = 3$

$\langle \bar{1} \rangle = ?$ $\quad \bar{1}, \ \bar{1} + \bar{1} = \bar{2}, \ \bar{1} + \bar{1} + \bar{1} = \bar{0}$

$\langle \bar{1} \rangle = \{\bar{1}, \bar{2}, \bar{0}\} = \mathbb{Z}_3$ $\rightsquigarrow$ $\mathbb{Z}_3$ es cíclico y es generado por $\bar{1}$

$o(\bar{1}) = 3$

Si G es un grupo finito entonces es cíclico sii existe un elemento $g \in G$ tal que $o(g) = |G|$.

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