Orden de un elemento

$(G, *, e)$ un grupo

$g \in G$

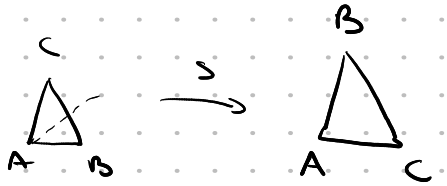
definimos el orden de g:

* si $g^n \neq e$ para todo $n \in \mathbb{Z}^+$ decimos que $o(g) = \infty$
* si no definimos $o(g) = \min\{n \in \mathbb{Z}^+ : g^n = e\}$

ejemplo:

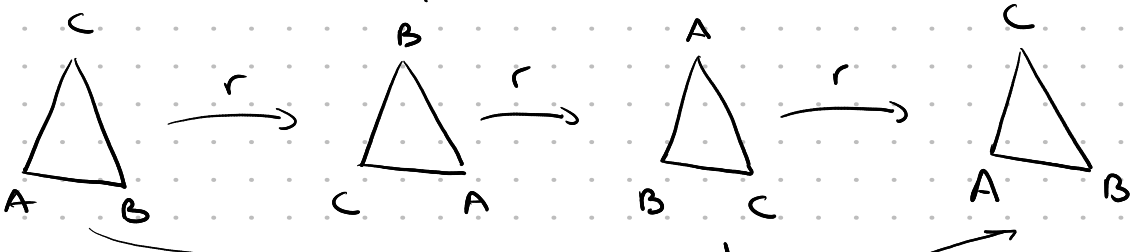
* $(\mathbb{Z}, +) \rightsquigarrow o(1) = \infty$
* $(D_3, \circ) \rightsquigarrow o(s) = ?$

s simetría



$s^2 = e \Rightarrow o(s) = 2$

$o(r) = ?$



$r^2 \neq id$

$r^3 = id$

$\Rightarrow o(r) = 3$

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) $G = GL_2(\mathbb{R})$

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

* $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $\quad o(A) = ?$

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

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

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

$$\left.\begin{array}{l} A^4 = I \\ A \neq I,\ A^2 \neq I,\ A^3 \neq I \end{array}\right] \Rightarrow o(A) = 4$$

* $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ $\quad o(B) = ?$

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

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

$$\left.\begin{array}{l} B^3 = I \\ B \neq I,\ B^2 \neq I \end{array}\right] \Rightarrow o(B) = 3$$

* $o(AB) = ?$

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

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

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

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

→ vamos a probarlo por inducción

caso base: $n = 1$

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

paso inductivo: suponemos que se cumple para k y probamos que se cumple para $k+1$

Hipótesis: $(AB)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$

Tesis: $(AB)^{k+1} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}$

$$(AB)^{k+1} = (AB)^k (AB) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix} \checkmark$$

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

$\Rightarrow o(AB) = \infty$

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

para ver que AB tiene orden finito tenemos que encontrar algún $k \in \mathbb{Z}^+$ tal que $(AB)^k = e$

Sean $n = o(A)$ y $m = o(B)$

$\Rightarrow A^n = e$ y $B^m = e$

$$(AB)^{nm} = \underbrace{AB\,AB \cdots AB}_{nm \text{ veces}} = AA\cdots BB\cdots B = A^{nm}B^{nm}$$

(G es abeliano)

$$= (A^n)^m (B^m)^n$$
$$= e^m e^n$$
$$= e$$

$(AB)^{nm} = e \Rightarrow o(AB)$ es finito

$o(AB) \leq nm$

(G abeliano)

$$(AB)^{\max\{n,m\}} = (AB)^m = A^m \underbrace{B^m}_{e} = A^m = A^{n+k} = \underbrace{A^n}_{e} A^k = A^k$$

supongamos $\max\{n,m\} = m$

$$(AB)^{mcm(n,m)} = A^{mcm(n,m)} B^{mcm(n,m)} = A^{nq} B^{mq'} = (A^n)^q (B^m)^{q'} = e^q e^{q'} = e$$

(G abeliano)

$(AB)^{mcm(n,m)} = e \Rightarrow o(AB)$ es finito y $o(AB) \leq mcm(n,m)$

Grupo de los enteros modulo n

$n = 3$

ser congruentes modulo 3 es una relación de equivalencia

- reflexiva: $x \equiv x \pmod 3$ para todo $x \in \mathbb{Z}$
- simétrica: $x \equiv y \pmod 3 \Rightarrow y \equiv x \pmod 3$
- transitiva: $\left.\begin{array}{l} x \equiv y \pmod 3 \\ y \equiv z \pmod 3 \end{array}\right\} \Rightarrow x \equiv z \pmod 3$

→ podemos considerar las clases de equivalencia

$\bar{0} = \{ x \in \mathbb{Z} : x \equiv 0 \pmod 3 \}$ ← los enteros que tienen resto 0 al dividir entre 3

$\bar{1} = \{ x \in \mathbb{Z} : x \equiv 1 \pmod 3 \}$ ← los enteros que tienen resto 1 al dividir entre 3

$\bar{2} = \{ x \in \mathbb{Z} : x \equiv 2 \pmod 3 \}$ ← los enteros que tienen resto 2 al dividir entre 3

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

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

definimos la suma

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

↖ suma de $\mathbb{Z}$

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

$$\left.\begin{array}{l} \bar{1} = \bar{4} \\ \bar{2} = \bar{5} \end{array}\right\} \Rightarrow \overline{1+2} = \overline{4+5}$$

$$\bar{1} + \bar{2} = \overline{4+5} = \bar{9} = \bar{0}$$

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

veamos que está bien definida

$$\left.\begin{array}{l} \bar{a} = \bar{a'} \\ \bar{b} = \bar{b'} \end{array}\right\} \Rightarrow \overline{a+b} = \overline{a'+b'}$$

$\bar{a} = \bar{a'} \Rightarrow a \equiv a' \pmod 3$

$\bar{b} = \bar{b'} \Rightarrow b \equiv b' \pmod 3$

$\Rightarrow a+b \equiv a'+b' \pmod 3$

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

$\mathbb{Z}_3$ con la suma es un grupo

el neutro es $\bar{0}$

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

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

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

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

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

en general $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ es un grupo con $\bar{a}+\bar{b} = \overline{a+b}$ (↑ suma de $\mathbb{Z}$)