Clase 1:

Definición: un grupo es un par $(G,\cdot)$ donde $G \neq \emptyset$ y $\cdot : G \times G \to G$ cumple:

1) $(ab)c = a(bc)$
2) $\exists e \in G \,/\, a.e = e.a = a, \forall a \in G$ (elem. neutro)
3) $\forall a \in G, \exists a^{-1} \in G \,/\, aa^{-1} = e = a^{-1}a$ (elem. inverso)

Además G es abeliano si:

4) $ab = ba$

Ejemplo:

1) $(\mathbb{Z},+), (\mathbb{Q},+), (\mathbb{R},+), (\mathbb{C},+)$
$(\mathbb{Q}-\{0\},\cdot), (\mathbb{R}-\{0\},\cdot), (\mathbb{C}-\{0\},\cdot)$

2) V un $\mathbb{K}$-esp. vectorial $\Rightarrow (V,+)$ es grupo. abeliano

3) En $\mathbb{Z}$ consideremos:

$$a \sim b \Leftrightarrow n \mid a-b$$

$$\mathbb{Z}_n = \mathbb{Z}/_{\sim} = \{[0],[1],\ldots,[n-1]\}$$

$a \sim a', b \sim b'$
$\Rightarrow a+b \sim a'+b'$

$$[a]+[b] = [a+b]$$
$$[a].[b] = [a.b]$$

están bien definidas

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

$(\mathbb{Z}_n^{\times},\cdot)$ es grupo abeliano, $\mathbb{Z}_n^{\times} = \{[a] \,/\, [a] \text{ tiene inverso}\}$

4) A, B grupos $\Rightarrow A \times B$ es grupo (prod. directo)

$$(a,b) \cdot (c,d) = (a \cdot c, b \cdot d)$$

Proposición: sea $(G, \cdot)$ un grupo:

1) $e \in G$ es único.
2) $\forall a \in G$, a^{-1} es único.
3) $(a^{-1})^{-1} = a$
4) $(ab)^{-1} = b^{-1}a^{-1}$
5) $a_1 \dots a_n$ no depende de paréntesis (inducción)

Demostración: Ejercicio.

Proposición: $(G, \cdot)$ un grupo, $a, b \in G$

$$au = av \Rightarrow u = v$$
$$ub = vb \Rightarrow u = v$$

$\Big(au = av$
$u = 1 \cdot u = (a^{-1}a)u$
$= a^{-1}(au) = a^{-1}(av)$
$= v \Big)$

Notación:

1) $(G, +) \rightsquigarrow e = 0$, $a^{-1} = -a$, $nx = \underbrace{x + \dots + x}_{n \text{ veces}}$

2) $(G, \cdot) \rightsquigarrow e = 1$, $a^{-1} = a^{-1}$, $x^n = \underbrace{x \dots x}_{n \text{ veces}}$ ✓ $x^{-n} = (x^{-1})^n$, $x^0 = e$

Definición: $(G, \cdot)$ grupo:

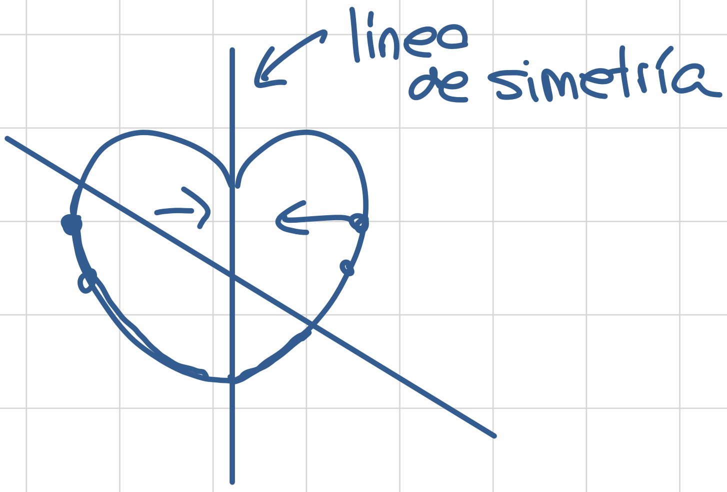
1) El orden de G es $|G|$ → finito / → ∞ ✓ $(\mathbb{Z}, +)$
2) El orden de $a \in G$ es:

$$|a| = n = \min \{ m \in \mathbb{Z} \,/\, x^m = 1 \}$$

Si no existe $m \,/\, x^m = 1 \Rightarrow |a| = \infty$

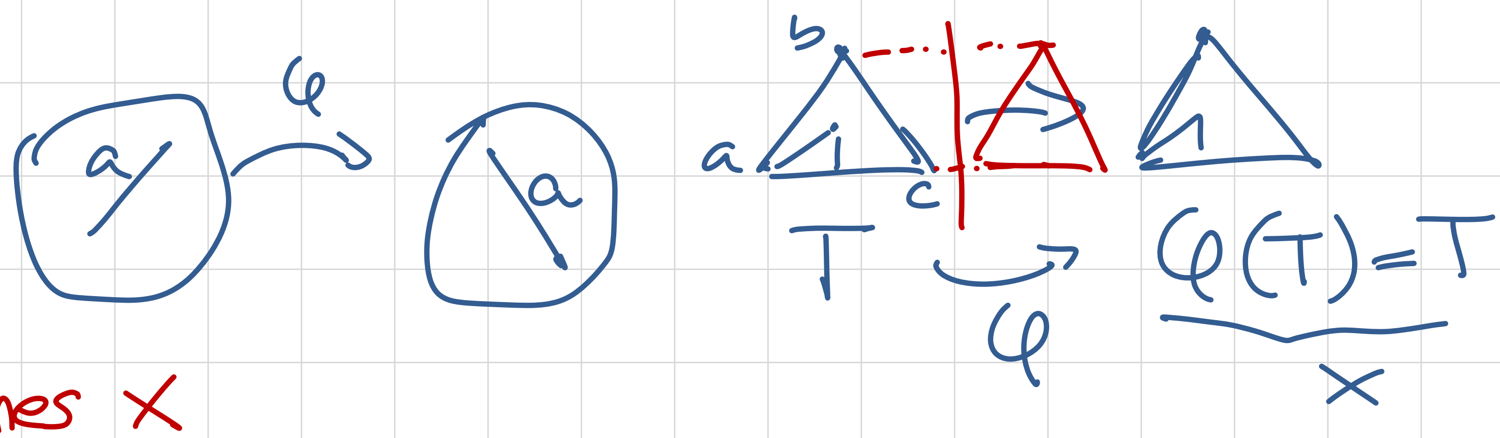
Grupo diedral:

¿Simetría?



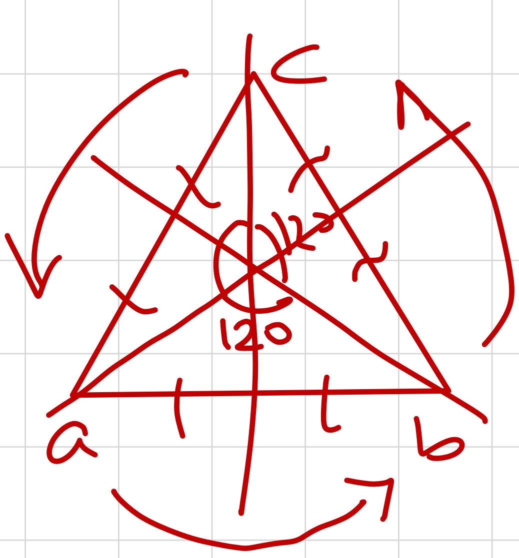
En el contexto general:

isometría $\varphi: \mathbb{R}^2 \to \mathbb{R}^2$, $\|\varphi(x)-\varphi(y)\| = \|x-y\|$



* traslaciones ✗
* rotaciones ✓
* reflexiones ✓
* " deslizadas ✗

Simetrías en un polígono reg P_n = isometrías $\varphi: \mathbb{R}^2 \to \mathbb{R}^2$ tq $\varphi(P_n) = P_n$



reflexiones = 3

rotaciones = 3, $\frac{2\pi}{3}$, $\frac{4\pi}{3}$, 0

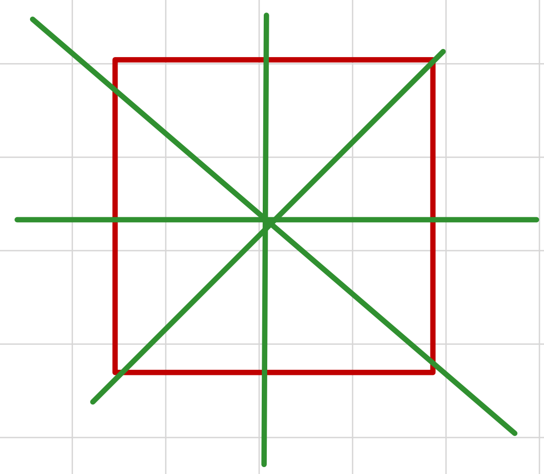
En P_n ⇝ rotaciones = n, $\frac{2\pi k}{n}$, $k \in \{0, \dots, n-1\}$

Polígono de n lados

n impar : n ejes de simetría, que se obtienen uniendo un vértice y el pto. medio del lado opuesto

n par : $n/2$ ejes uniendo vért. opuestos

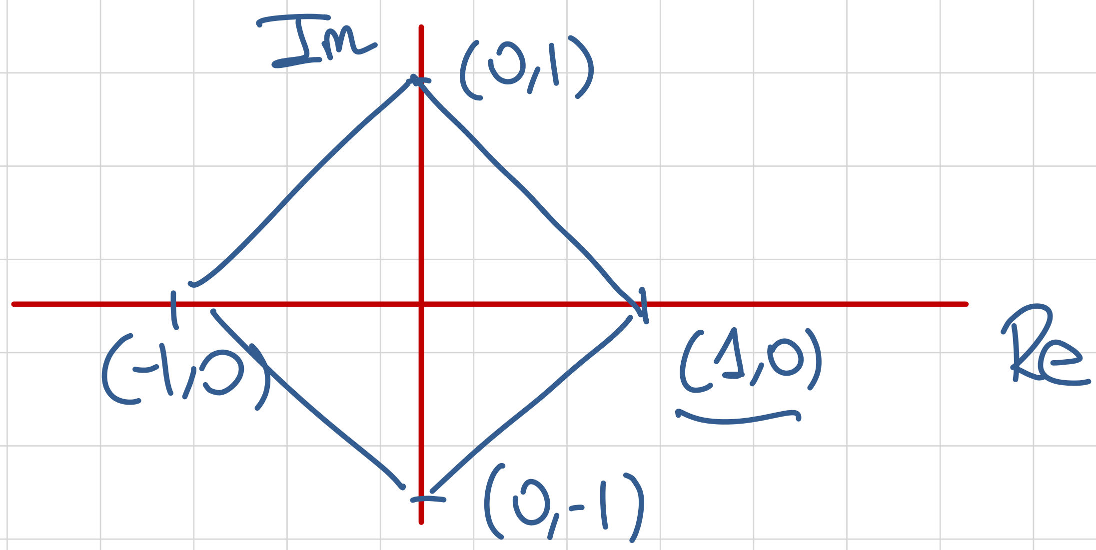
$n/2$ ejes unen ptos. medios de lados opuestos



$D_{2n} = \{\text{simetrías de } P_n\} \rightarrow |D_{2n}| = 2n$

En $\underbrace{\mathbb{C}}_{\mathbb{R}^2}$, $\{z \,/\, z^n = 1\} \approx P_n$

$$z = e^{2\pi i k/n}, \quad k \in \{0, 1, \ldots, n-1\}$$



$D_{2n} = \{ f : \mathbb{C} \to \mathbb{C} \,/\, f(P_n) = P_n, \ f \text{ isometría} \}$

$(D_{2n}, \circ)$ composición de funciones

$$f, g \in D_{2n} \Rightarrow f \circ g \in D_{2n}$$

Proposición: $(D_{2n}, \circ)$ es un grupo con orden $2n$, $n \geq 3$

Demostración:

* $\circ$ asociativa ✓
* $id \in D_{2n}$ ✓, $f \circ (id) = f = (id) \circ f$

* Vamos probar:

$$(*)\ \underbrace{D_{2n} \underset{\supseteq}{=} \{ id, r, r^2, \ldots, r^{n-1}, s, rs, r^2 s, \ldots, r^{n-1} s \}}$$

donde:

$r =$ rotación de $2\pi/n$

$$r: \mathbb{C} \to \mathbb{C} \quad \rightsquigarrow r \in D_{2n}$$
$$z \mapsto z \cdot e^{2\pi i/n}$$

$s =$ reflexión resp. al eje real

$$s: \mathbb{C} \to \mathbb{C} \quad \rightsquigarrow s \in D_{2n}$$
$$z \mapsto \bar{z}$$

Tenemos: $r^n = \underbrace{r \circ r \circ \ldots \circ r}_{n-1 \text{ veces}} = id$, $s^2 = s \circ s = id$

$$\Rightarrow r^{-1} = r^{n-1}, \quad s^{-1} = s \ ✓$$

Prueba de (*):

Sea $f \in D_{2n} \Rightarrow f(1) = \underbrace{e^{\frac{2\pi i k}{n}}}$, para algún $k \in \{0, \ldots, n-1\}$

$$\Rightarrow r^k(1) = e^{2\pi i k/n} = f(1) \Rightarrow (r^{-k} \circ f)(1) = 1$$

$$\Rightarrow (\underbrace{r^{-k} \circ f}_{g})(1) = 1$$

Ahora $g(e^{2\pi i/n}) =$ Vértice del P_n Comparte arista con $g(1)=1$

$$= e^{2\pi i/n} \circ e^{2\pi i\left(\frac{n-1}{n}\right)}$$

* Si $g(e^{2\pi i/n}) = e^{2\pi i\left(\frac{n-1}{n}\right)}$

$$\Rightarrow \begin{cases} (s \circ g)(e^{2\pi i/n}) = e^{2\pi i/n} \\ (s \circ g)(1) = 1 \end{cases} \Rightarrow s \circ g \text{ fija } 1, e^{\frac{2\pi i}{n}}$$

* Si $g(e^{2\pi i/n}) = e^{2\pi i/n}$

$$\Rightarrow g \text{ fija } 1, e^{2\pi i/n}$$

Si $g: \mathbb{C} \to \mathbb{C}$ isometría tq $g(1)=1$, $g(e^{2\pi i/n}) = e^{2\pi i/n}$
$\Rightarrow g(0)=0 \Rightarrow \underline{g = id}$

Así en el 1er caso $\Rightarrow s \circ g = id$
2do caso $\Rightarrow g = id$

Ahora, como $g = r^{-k} \circ f$

* 1er caso $\Rightarrow f = r^{k} \circ s$, $k \in \{0, 1, \dots, n-1\}$
* 2do caso $\Rightarrow f = r^{k}$, k ″

$$\Rightarrow f \in \{id, r, r^2, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}$$

∎

Entonces

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\} \checkmark$$

se denomina el grupo diedral de orden $2n$

$\checkmark\ sr = r^{-1}s \qquad r^n = 1 \checkmark$

$sr^2 = r^{n-2}s \quad \ldots \quad s^2 = 1 \checkmark$

$sr^3 = r^{n-3}s$

$$D_{2n} = \langle \underbrace{r, s}_{\text{generadores}} \mid \underbrace{r^n = s^2 = 1,\ rs = sr^{-1}}_{\text{relaciones}} \rangle$$

Una presentación de D_{2n}

Permutaciones:

Sea $X \neq \emptyset$, definimos

$$\Rightarrow S_X = \{\sigma : X \to X \ / \ \underbrace{\sigma \text{ es biyección}}_{\text{permutación}}\}$$

$(S_X, \circ)$ es un grupo denominado el grupo simétrico de X.

En el caso $X = \{1, \ldots, n\} \rightsquigarrow S_X := S_n$ se denomina el grupo simétrico de orden n.

Dado $\sigma \in S_n$ se denotan:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

$|S_n| = n!$

Definición: un ciclo (de long. m) en S_n es una permutación

$$\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$$

$$\sigma(a_i) = a_{i+1}$$
$$\sigma(a_m) = a_1$$
$$\sigma(i) = i, \quad \text{otro caso}$$

donde $a_1, \dots, a_m \in \{1, \dots, n\}$. Not. $= (a_1 \dots a_m)$

Ejemplo: En S_5

$$\underset{a_1\ a_2\ a_3\ a_4}{(1\,3\,5\,4)} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$$

Se pueden operar:

$$(1\,3\,5\,4)(1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}$$

Definición: $(a_1 \dots a_m), (b_1, \dots, b_s)$ son ciclos disjuntos si $a_i \neq b_j, \forall i,j$.

Obs: Un ciclo se puede reordenar

$$\begin{aligned}(a_1 a_2 \dots a_m) &= (a_2 a_3 \dots a_m a_1) \\ &= (a_3 a_4 \dots a_{m-1} a_1 a_2) \\ &\ \vdots \\ &= (a_m a_1 \dots a_{m-1})\end{aligned}$$

Ejemplos: Considere

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} \in S_6$$

$1 \to 6 \to 1 \quad (1\,6)$

$2 \to 5 \to 3 \to 2 \quad (2\,5\,3)$

$4 \to 4 \quad (4)$

$\Rightarrow \sigma = (1\,6)(2\,5\,3)$

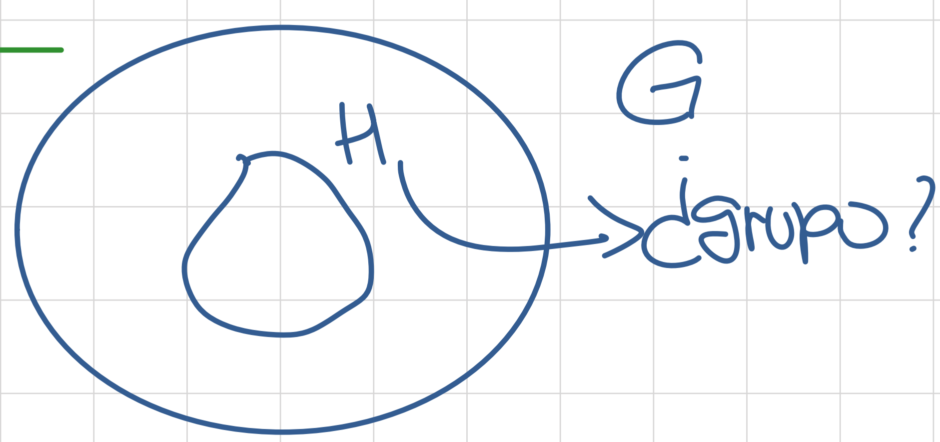
disjuntos

Obs: los ciclos disj. conmutan

Teorema: Toda $\sigma \in S_n$ se expresa como prod. de ciclos disjuntos, esta descomposición es única salvo:

1) El orden de los ciclos
2) reordenamientos de ciclos

Subgrupos:



Querer construir grupos a partir de G

Definición: Sea $(G, \cdot)$ un grupo y $H \subseteq G$. Diremos que H es un subgrupo de G si:

$$(H, \cdot|_{H\times H}) \text{ es grupo} \equiv \forall x,y \in H: \begin{array}{l} xy \in H \\ x^{-1} \in H \end{array}$$

Proposición: $(G, \cdot)$ grupo y $H \subseteq G$ $(H \neq \emptyset)$

$$H \text{ es subgrupo} \Leftrightarrow \forall x,y \in H : xy^{-1} \in H$$

Ejemplos: (H subgrupo, $H \leq G$)

1) $\mathbb{Z} \leq \mathbb{Q}$, $\mathbb{R} \leq \mathbb{C}$ con la adición
2) Si G es grupo ⇝ $\{e\}$, G son subgrupos (triviales)
3) $H = \{1, r, \dots, r^{n-1}\} \leq D_{2n}$

Sea $(G, \cdot)$ un grupo $\Rightarrow$ ¿construir un grupo?

Proposición: sea $\{H_\alpha\}_{\alpha \in I}$ familia de subgrupos de G

$$\Rightarrow \bigcap_{\alpha \in I} H_\alpha \text{ es subgrupo de } G$$

Dado $A \subseteq G$, definimos:

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H \quad \text{es subgrupos}$$

se denomina el subgrupo generado por A