Clase 0: Preliminares (recuerdos de 1^{er} y 2^{do} año).

§0. Notación: Durante todo el curso

$\mathbb{N} := \{0, 1, 2, 3, \dots\}$ naturales, $\mathbb{N}^{\geq 1} = \{1, 2, 3, \dots\}$

Similar: $\mathbb{R}^{>0} = \{x \in \mathbb{R} \text{ tal que } x > 0\}$, $\mathbb{R}^{\geq 0}$, $\mathbb{R}^{\leq 0}$, etc.

Dado $x \in \mathbb{C}$, denotamos $x\mathbb{Z} := \{nx, n \in \mathbb{Z}\}$ "múltiplos de x"

$f : A \hookrightarrow B$ (resp. $f : A \twoheadrightarrow B$) indica que f es una función inyectiva (resp. sobreyectiva)

Abreviaciones típicas:

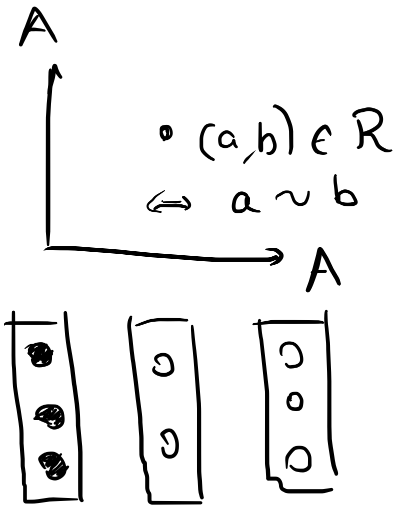
1) cf (confer): "comparar con"
2) eg (exempli gratia): "por ejemplo"
3) ie (id est): "es decir"

§1. Relaciones de equivalencia y cocientes

no-vacío

***Definición 1.1.1* (relación de equivalencia).** — Sea A un conjunto y sea $\mathscr{R}$ una relación en A (es decir, un subconjunto $\mathscr{R} \subseteq A \times A$). Si para todo $(a,b) \in A \times A$ tal que $(a,b) \in \mathscr{R}$ escribimos $a \sim b$, entonces decimos que $\mathscr{R}$ es una **relación de equivalencia** si es:

1. **reflexiva:** $a \sim a$ para todo $a \in A$,
2. **simétrica:** $a \sim b$ si y sólo si $b \sim a$ para todos $a, b \in A$,
3. **transitiva:** si $a \sim b$ y $b \sim c$ entonces $a \sim c$, para todos $a, b, c \in A$.



Ej: "=" es una rel. de equiv.

***Definición 1.1.2* (clase de equivalencia).** — Sea $\mathscr{R}$ una relación de equivalencia en A. Para todo $a \in A$ diremos que el conjunto

$$[a]_{\mathscr{R}} = \{b \in A \mid a \sim b\} = \{b \in A \mid b \sim a\}$$

es la **clase de equivalencia** de $a \in A$ respecto a $\mathscr{R}$, el cual es también denotado $a \bmod \mathscr{R}$. En caso que la relación $\mathscr{R}$ sea clara en el contexto, escribiremos simplemente $[a]$ o bien $\overline{a}$.

Una de las nociones más relevantes del curso:

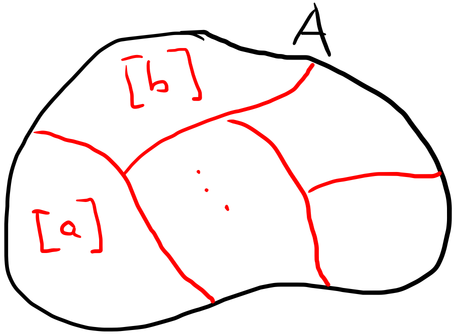
***Definición 1.1.3* (cociente).** — Sea $\mathscr{R}$ una relación de equivalencia en A. El conjunto cuyos elementos son todas las clases de equivalencia es llamado **conjunto cociente** de A por $\mathscr{R}$, y será denotado $A/\mathscr{R}$ (o simplemente $A/\sim$ si la relación $\mathscr{R}$ es clara en el contexto). Explícitamente,

$$A/\mathscr{R} = \{[a]_{\mathscr{R}},\ a \in A\}.$$

Obs: $\pi : A \twoheadrightarrow A/R$, $a \mapsto [a]$ es llamado "proyección canónica"

Proposición 1.1.4. — *Sea $\mathscr{R}$ una relación de equivalencia en A. Entonces:*

1. *Para todo $a \in A, a \in [a]_{\mathscr{R}}$. En particular, $[a]_{\mathscr{R}} \neq \emptyset$.*
2. *Si $b \in [a]_{\mathscr{R}}$ entonces $a \in [b]_{\mathscr{R}}$. Además, en este caso tenemos que $[a]_{\mathscr{R}} = [b]_{\mathscr{R}}$.*
3. *Para todos $a, b \in A$ ya sea $[a]_{\mathscr{R}} = [b]_{\mathscr{R}}$ o bien $[a]_{\mathscr{R}} \cap [b]_{\mathscr{R}} = \emptyset$. En particular, A es la unión disjunta de las clases $[a]_{\mathscr{R}}$.*



Idea (Ejercicio: Completar los detalles):

① $a \sim a \iff a \in [a]$ (reflex.)

② $b \in [a] \overset{\text{def}}{\iff} b \sim a \overset{\text{sim}}{\iff} a \sim b \overset{\text{def}}{\iff} a \in [b]$

Además, $c \in [a] \iff \begin{matrix} c \sim a \\ b \sim a \end{matrix} \underset{\text{trans.}}{\implies} c \sim b \overset{\text{def}}{\iff} c \in [b]$

ie, $[a] \subseteq [b]$. Similar: $[b] \subseteq [a]$ ✓

③ Vimos: $a \sim b \overset{① \,\&\, ②}{\iff} [a] = [b]$

Por otro lado, si $[a] \cap [b] \neq \emptyset \leadsto \exists\, c \in [a] \cap [b]$

ie, $c \sim a$ y $c \sim b$

$\overset{\text{trans}}{\implies} a \sim b$ ✓

Ejemplo (muy importante): Sea $n \in \mathbb{N}^{\geq 1}$ y definamos la rel en $\mathbb{Z}$ dada por: $a \sim b \overset{\text{def}}{\iff} n$ divide $a-b$ ← Notación: $n \mid (a-b)$

$\overset{\text{def}}{\iff} \exists\, k \in \mathbb{Z}$ tq $a-b = nk$

Hecho/Ejercicio: $\sim$ es una relación de equiv. en $\mathbb{Z}$ ✓

⚠ **Notación típica**:
1) $a \sim b \rightsquigarrow a \equiv b \pmod{n}$
2) $[a]_n := \{ b \in \mathbb{Z} \text{ tq } a \equiv b \pmod{n} \}$
3) $\mathbb{Z}/n\mathbb{Z} := \mathbb{Z}/\sim = \{ [a]_n, \ a \in \mathbb{Z} \}$

Eg. $(n=2)$:
$$[0]_2 = \{ b \in \mathbb{Z} \text{ tq } 0 \equiv b \pmod{2} \}$$
$$= \{ b \in \mathbb{Z} \text{ tq } b = 2k \text{ para algún } k \in \mathbb{Z} \}$$
$$= \{ \ldots, -2, 0, 2, 4, 6, \ldots \}$$

$$[1]_2 = \{ \ldots, -3, -1, 1, 3, 5, \ldots \}$$

Recuerdo (División Euclidiana): Para todos $a, b \in \mathbb{Z}$ tal que $b \neq 0$ existen <u>únicos</u> $q, r \in \mathbb{Z}$ tales que

$$a = bq + r \quad , \quad \text{con} \quad 0 \leq r < |b| .$$

↳ <u>Muy útil</u>! (cf. Algoritmo de Euclides)

<u>Ejemplo</u>: La división euclidiana implica que

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$$

$(b=n)$ ↳ $a = qn + r$, ie, $a \equiv r \pmod n$, $r \in \{0, 1, \ldots, n-1\}$

<u>Ejercicio</u>: Probar que $\forall a, b \in \mathbb{Z}$ si $a \equiv a' \pmod n$ y $b \equiv b' \pmod n$
$\Rightarrow a + b \equiv a' + b' \pmod n$ y $ab \equiv a'b' \pmod n$.

↳ consecuencia: $[a]_n + [b]_n := [a+b]_n$ bien definido ! $\rightsquigarrow (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$
$[a]_n \cdot [b]_n := [ab]_n$

↳ anillo

Lema 1.1.8 (Bézout). — *Sean $a, b \in \mathbb{Z}$ no nulos. Entonces existen $x, y \in \mathbb{Z}$ tales que $ax + by = \operatorname{mcd}(a, b)$.*

Muy útil !

Dem:

$S := \{ax + by,\ \text{con } x, y \in \mathbb{Z}\} \rightsquigarrow S \cap \mathbb{N}^{\geq 1} \neq \emptyset$

$\rightsquigarrow d := \min(S \cap \mathbb{N}^{\geq 1})$. Obs que $d \mid a$: $a = dq + r$, $\underline{0 \leq r < d}$

$a, d \in S \Rightarrow r = a - dq \in S \Rightarrow r = 0$ pues d minimal

ie, $d \mid a$ ✓

Análogo: $d \mid b$. Si d' divide a a y $b \Rightarrow d' \mid s\ \forall s \in S$

En part, $d' \mid d \Rightarrow d' \leq d$. , ie, $d = \operatorname{mcd}(a, b)$ ∎

Corolario 1.1.9. — *Sea p un número primo. Entonces para todo $a \in \mathbb{Z}$ tal que $p \nmid a$, existe $b \in \mathbb{Z}$ tal que $p \nmid b$ tal que $ab \equiv 1 \pmod{p}$.*

Dem: $p \nmid a \Rightarrow mcd(a, p) = 1 \overset{\text{Bézout}}{\Longrightarrow} \exists\, x, y \in \mathbb{Z}$ tq $ax + py = 1$

$\Leftrightarrow ax - 1 = p(-y) \overset{\text{dy}}{\Longleftrightarrow} ax \equiv 1 \pmod{p} \rightsquigarrow b := x$ ✓ ∎

Obs: $p \nmid a \Longleftrightarrow a \not\equiv 0 \pmod{p}$

Consecuencia importante: Sea p un número primo, entonces

$$\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot) \text{ es un cuerpo. (de } p \text{ elementos)}$$

Eg ($p = 3$): $\mathbb{F}_3$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

" $2^{-1} \equiv 2$ en $\mathbb{F}_3$ "

§ 2. Permutaciones

***Definición 1.2.1* (permutación).** — Sea $n \in \mathbb{N}^{\geq 1}$. Una **permutación** del conjunto $\{1, 2, \ldots, n\}$ es una función biyectiva

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

La denotaremos mediante

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

ó simplemente

$$\sigma = (\sigma(1), \sigma(2), \ldots, \sigma(n)).$$

$$\sigma : \begin{cases} 1 \longmapsto \sigma(1) \\ 2 \longmapsto \sigma(2) \\ \vdots \\ n \longmapsto \sigma(n) \end{cases}$$

Eg $(n=4)$: $\sigma = (2,3,4,1)$ es $\sigma : \begin{cases} 1 \longmapsto 2 \\ 2 \longmapsto 3 \\ 3 \longmapsto 4 \\ 4 \longmapsto 1 \end{cases}$ ó $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

En part, $\sigma^{-1} : \begin{cases} 1 \longmapsto 4 \\ 2 \longmapsto 1 \\ 3 \longmapsto 2 \\ 4 \longmapsto 3 \end{cases}$, i.e., $\sigma^{-1} = (4,1,2,3)$

Notación 1.2.3. — El conjunto de todas las permutaciones de $\{1,\ldots,n\}$ será denotado $\mathfrak{S}_n$. Además, si $\sigma,\tau\in\mathfrak{S}_n$, entonces denotamos $\sigma\tau := \sigma\circ\tau$ (composición de funciones) y como σ^{-1} a la función inversa de σ.

⚠ La notación puede variar en algunos textos! (eg. S_n)

Eg $(n=4)$: $\sigma=(2,3,4,1)$ y $\tau=(1,4,3,2)$ en S_4

$1\xmapsto{\tau}1\xmapsto{\sigma}2$; $2\xmapsto{\tau}4\xmapsto{\sigma}1$; $3\xmapsto{\tau}3\xmapsto{\sigma}4$; $4\xmapsto{\tau}2\xmapsto{\sigma}3$

$\sigma\tau=(2,1,4,3)$ y $\tau\sigma=(4,3,2,1)$

Proposición 1.2.5. — *El cardinal de $\mathfrak{S}_n$ es $n! = 1\cdot 2\cdots n$.*

(Idea: 1° → n opciones
2° → $n-1$ "
⋮
n° → 1 ")

Idea: Inducción en n : OK para $n=1$ ✓

Sup. que $|S_n| = n!$ y notamos

$\{\sigma=(a_1,\ldots,a_{n+1})\in S_{n+1}$ tq $a_k=n+1\}\xleftrightarrow{\text{biy}}\{\tau=(a_1,\ldots,a_{k-1},a_{k+1},\ldots,a_n)\in S_n\}$

$\hookrightarrow \#\{\ldots\} =: A_k \underset{\text{Hip}}{=} n!$

$\rightsquigarrow |S_{n+1}| = \sum_{k=1}^{n+1} A_k = n!\underbrace{\sum_{k=1}^{n+1} 1}_{=n+1} = (n+1)!$ ∎

***Definición 1.2.6* (transposición).** — Una permutación $\tau \in \mathfrak{S}_n$ que sólo cambia dos elementos de $\{1, \ldots, n\}$ es llamada una **transposición**.

Notación 1.2.7. — Sea $n \geq 2$. Para todos $i, j \in \{1, \ldots, n\}$ tales que $i \neq j$, denotamos por $\tau = (i, j)$ a la transposición tal que $\tau(i) = j$, $\tau(j) = i$ y $\tau(k) = k$ para todo k distinto de i y de j.

← "Abuso de notación"

Obs: 1) Hay que tener cuidado en que n está implícito en la notación

2) Se tiene $\tau = (i,j) = (j,i) = (i,j)^{-1}$ y luego $\tau^2 := \tau \circ \tau = Id$

Ejemplo: $S_3 = \{ Id, (1,2), (2,3), (1,3), (2,3,1), (3,1,2) \}$

Id fija todo ✓

Fijan 0 elementos: $\begin{pmatrix} 1 & 2 & 3 \\ \bigcirc & \bigcirc & \bigcirc \end{pmatrix}$

$\rightsquigarrow (3,1,2)$

$\rightsquigarrow (2,3,1)$

Fijan 1 elemento:

$1 \rightsquigarrow (2,3)$

$2 \rightsquigarrow (1,3)$

$3 \rightsquigarrow (1,2)$

***Definición 1.2.10* (inversión).** — Sea $\sigma \in \mathfrak{S}_n$ y sean $i, j \in \mathbb{N}^{\geq 1}$ tales que $1 \leq i < j \leq n$. Decimos que σ **invierte** i y j si $\sigma(i) > \sigma(j)$.

Ejemplos: 1) $Id = (1, 2, \dots, n) \rightsquigarrow 0$ inversiones

2) $(1,2) \in S_n \rightsquigarrow 1$ inversión

3) $(1, n) \in S_n \rightarrow \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & 2 & \cdots & n-1 & 1 \end{pmatrix} \rightarrow \begin{array}{l} n-1 \\ + \, n-2 \\ = 2n-3 \text{ inv.} \end{array}$

4) $(2,3,1), (3,1,2) \in S_3 \rightsquigarrow 2$ inv.

Ejercicio: Probar que la transposición $(i,j) \in S_n$ tiene $2|i-j| - 1$ inversiones.

***Definición 1.2.13* (signatura).** — Sea $\sigma \in \mathfrak{S}_n$. Llamaremos al número

$$\varepsilon(\sigma) := (-1)^{\text{número de inversiones de } \sigma}$$

la **signatura** de σ. Decimos que σ es **par** (resp. **impar**) si $\varepsilon(\sigma) = 1$ (resp. $\varepsilon(\sigma) = -1$).

$\rightsquigarrow$ Eg:

1) $\varepsilon(Id) = (-1)^0 = 1$

2) $\varepsilon((i,j)) \overset{Ej}{=} -1$

3) $S_3 \rightsquigarrow$ 3 con $\varepsilon = +1$
3 con $\varepsilon = -1$

Lema 1.2.15. — *Sea $\sigma \in \mathfrak{S}_n$. Entonces,*

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}. =: \tilde{\varepsilon}(\sigma)$$

<u>Dem</u>: Notar que $\varepsilon(\sigma)$ y $\tilde{\varepsilon}(\sigma)$ tienen el mismo signo!

$$\tilde{\varepsilon}(\sigma)^2 = \prod_{i<j} \left(\frac{\sigma(j)-\sigma(i)}{j-i}\right)^2 = \prod_{i \neq j} \left(\frac{\sigma(j)-\sigma(i)}{j-i}\right) \underset{\substack{\uparrow \\ \sigma \text{ biyección}}}{=} 1 \implies \varepsilon(\sigma) = \tilde{\varepsilon}(\sigma) \checkmark \quad \blacksquare$$

Proposición 1.2.16. — *La signatura $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ satisface*

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$$

para todos $\sigma, \tau \in \mathfrak{S}_n$. ← Lo usaremos mucho!

<u>Dem</u>: Notar que $\dfrac{\sigma(j)-\sigma(i)}{j-i} = \dfrac{\sigma(i)-\sigma(j)}{i-j}$ indep. del orden!

$$\implies \varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}$$ y luego tenemos:

$$\varepsilon(\sigma\tau) = \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j-i} \cdot \frac{\tau(j) - \tau(i)}{\tau(j) - \tau(i)} = \varepsilon(\sigma)\,\varepsilon(\tau) \checkmark \quad \blacksquare$$

⚠ Notar que: $S_3 = \{ \underbrace{Id}_{=(1,2)(1,2)}, (1,2), (2,3), (1,3), \underbrace{(2,3,1)}_{=(1,3)(1,2)}, \underbrace{(3,1,2)}_{\| \atop (1,2)(1,3)=(1,3)(2,3)} \}$

Proposición 1.2.17. — *Toda permutación se escribe como producto de transposiciones. Dicha escritura no es única, pero toda descomposición de una permutación par (resp. impar) tiene un número par (resp. impar) de factores.*

Dem (Sketch): Algorítmica ! Veamos un ejemplo (eg. $n=5$):

$\sigma = (5,4,1,3,2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}$. Como $1 \mapsto 5$, componemos (por la izq) con $(1,5)$:

$(1,5)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}$. Como $2 \mapsto 4$ componemos con $(2,4)$:

$(2,4)(1,5)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}$. Como $3 \mapsto 5$ componemos con $(3,5)$:

$(3,5)(2,4)(1,5)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = (4,5) \underset{(3,5)^{-1}=(3,5)}{\rightsquigarrow} (2,4)(1,5)\sigma = (3,5)(4,5)$

$\rightsquigarrow \sigma = (1,5)(2,4)(3,5)(4,5)$ ✓

Finalmente: $\sigma = \tau_1 \cdots \tau_r$ ← transp.

$\Rightarrow \varepsilon(\sigma) = \varepsilon(\tau_1)\cdots\varepsilon(\tau_r) = (-1)^r \rightsquigarrow$ $\varepsilon(\sigma)$ y r tienen la misma paridad ∎