def Un conjunto no vacío G se dice **semigrupo** si tiene una operación binaria

$$\cdot : G \times G \to G$$
$$(a, b) \mapsto a \cdot b$$

- es asociativa

) Un semigrupo se dice monoide si existe $e \in G$ llamado neutro que cumple:

$$e \cdot a = a \cdot e = a \quad \forall a \in G$$

·) Un grupo es un monoide G tq

$$\forall a \in G \ \exists b \in G \ / \ a \cdot b = b \cdot a = 1$$

ejemplos 1) $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$ son semigrupo

$(\mathbb{N}, +)$ no es monoide. $(\mathbb{N}, \cdot)$ sí

$(\mathbb{N}, \cdot)$ no es grupo

2) X no vacío $\mathcal{F}(X) = \{f : X \to X\}$ es monoide y no es grupo si $|X| > 1$

3) $\mathfrak{S}(X) = \{f : X \to X \ / \ f \text{ biyectiva}\}$ es grupo con la composición ($\mathfrak{S}$ viene de simetría)

Def Sea G un (semi) grupo se dice conmutativo (abeliano) si $a.b = b.a \quad \forall a,b \in G$

ejemplos

1) Son conmutativos

2) Si $|X| \geq 3 \Rightarrow \mathcal{D}$ no es conmutativo

$$f(x) = \begin{cases} x_2 & \text{si } x = x_1 \\ x_1 & \text{si } x = x_2 \\ x & cc \end{cases} \qquad f \circ g(x) = \begin{cases} x_2 & \text{si } x = x_1 \\ x_3 & \text{si } x = x_2 \\ x_1 & \text{si } x = x_3 \\ x & cc \end{cases}$$

$(x_1\ x_2\ x_3)$

notación permutaciones

$$g(x) = \begin{cases} x_2 & \text{si } x = x_3 \\ x_3 & \text{si } x = x_2 \\ x & cc \end{cases} \qquad g \circ f(x) = \begin{cases} x_3 & x = x_1 \\ x_1 & x = x_2 \\ x_2 & x = x_3 \\ x & cc \end{cases}$$

$(x_1\ x_3\ x_2)$

·) $\mathcal{S}(X)$ se lo llama grupo simétrico de X

cuando $X = \{1, 2, \dots n\} \quad (n > 1)$

$\Rightarrow \mathcal{S}(X)$ se lo denota $\mathcal{S}_n$ y se lo llama grupo simetrico de grado n

4) $|S_n| = n!$ En general el cardinal de un grupo se lo llama orden

Obs S_3 es un grupo de orden 6 no abeliano

ejemplos 1) S^1 grupo abeliano infinito

los complejos son conmutativos

2) $(\mathbb{Z}, +)$ grupo abeliano

$(\mathbb{Z}_n, +)$ grupo abeliano de orden n

$D_3, \mathbb{Z}_6$ son grupos "distintos" no identificables de orden 6

3) $(\mathbb{Z}, \cdot)$ monoide pero no grupo

$(\mathbb{Z}_n, \cdot)$ tambien

(0 no es inversible)

$(M, \cdot, e)$ monoide

$\mathcal{U}(M) (= M^*) = \{g \in M \mid g \text{ es inversible}\}$

$\mathcal{U}(M)$ es un grupo con la operación de M

·) $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$

$\mathcal{U}(\mathbb{Z}_n) = \{0 \leq k \leq n-1 \mid (k, n) = 1\} = \mathcal{U}_n$

Coprimos

·) $|\mathcal{U}_n|$ se denota $\varphi(n)$ indicador de euler

$\varphi(p) = p - 1$ (p primo)

4) A anillo (por ejemplo A cuerpo)

$(M_n(A), \cdot)$ es monoide no conmutativo si $n \geq 2$

$\mathcal{U}(M_n(A))$ grupo con el producto de matrices

$\mathcal{U}$

$GL(n, A) = \{M \in M_n(A) \mid M \text{ es inversible}\}$

grupo no abeliano si $n \geq 2$

·) Grupo lineal general de grado n con coeficientes en A

es finito $\Leftrightarrow$ A finito

·) Recordemos que $\mathbb{Z}_p$ cuerpo (p primo)

$GL(n, \mathbb{Z}_p)$. Cada $F_1, \dots, F_n$ es un vector $\mathbb{Z}_p^n$

· $F_1 \in \mathbb{Z}_p^n - \{(0, \dots 0)\} \longmapsto p^n - 1$ opciones

(cero, no invertible)

$$F_2 \in \mathbb{Z}_p^n - \{cF_1 \mid c \in \mathbb{Z}_p\} \longmapsto p^n - p$$

$$F_3 \in \mathbb{Z}_p^n - \{c_1F_1 + c_2F_2 : c_1, c_2 \in \mathbb{Z}_p\}$$

$$\longmapsto p^n - p^2$$

$$\vdots$$

$$F_k \in \mathbb{Z}_p^n - \{\sum_{i=1}^{k} c_i F_i : c_i \in \mathbb{Z}_p\} \longmapsto p^n - p^{k-1}$$

$$|GL(n, \mathbb{Z}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$$

Ejemplo $|GL(2, \mathbb{Z}_3)| = (3^2 - 1)(3^2 - 3) = 48$

$|GL(2, \mathbb{Z}_2)| = (2^2 - 1)(2^2 - 2) = 6$

$GL(2, \mathbb{Z}_2)$ otro grupo no abeliano de orden 6

K cuerpo. $M \in M_n(K)$ invertible $\Leftrightarrow \det(M) \neq 0$

En general M invertible es $\det(M)$ es invertible en K para producto

- $SL(n,K) = \{M \in M_n(K) \mid \det(M) = 1\} \subseteq GL(n,K)$ con el prod de matrices es grupo
- $SL(n,K)$ se llama grupo lineal especial de grado n con coef en K
- Otro ejemplo: grupo ortogonal de grado n con coef en K

$$O(n,K) = \{M \in GL(n,K) \mid M \cdot M^t = M^t \cdot M = Id\}$$

$$SO(n,K) = \{M \in GL(n,K) \mid \det(M) = 1\}$$

→ con -1 no es grupo

Prop: Ser G grupo. Entonces valen las siguientes propiedades

i) El neutro es único

ii) El inverso de cada elemento $a \in G$ es único

Dem: i) Si e, e' neutros

$$ea = ae = a = ae' = e'a \quad \forall a$$

$\Rightarrow a = e'$ $\qquad ee' = e'e = e'$

$a = e$ $\qquad e'e = e \quad \Rightarrow e' = e$

ii) ejercicio

prop Ser G semigrupo, G es grupo sii

i) $\exists e \in G / ea = a \quad \forall a \in G$

ii) $\forall a \in G \ \exists a^{-1} \in G / \ a^{-1}a = e$

dem ($\Rightarrow$) Si G grupo i) y ii) en particular valen pq ya era así inverso

($\Leftarrow$) primero si $c \in G \quad c \cdot c = c$

$\Rightarrow c = e$

dem $c \cdot c = c$

$c^{-1}(c \cdot c) = c^{-1}c$

$(c^{-1}c)c = e$

$ec = e$

$c = e$

Ser $a \in G$ $\quad (aa^{-1})(aa^{-1}) = a(a^{-1}(aa^{-1}))$

$= a((a^{-1}a)a^{-1})$

$= a(ea^{-1})$

$= aa^{-1}$

$\Rightarrow a a^{-1} = e$ (inverso a derecha)

Además $ae = a(a^{-1}a) = (aa^{-1})a$

$= ea = a$

(neutro a derecha)

$\ln(x) = \frac{\ln(b)}{a}$

$x = e^{\frac{\ln(b)}{a}}$

Ejercicio 3

a) G semigrupo, G grupo sii las ecuaciones $ya = b$ y $ax = b$ tienen solución en G $\forall a, b \in G$

($\Rightarrow$) $y = ba^{-1}$ $x = a^{-1}b$ son las únicas sol (tiene sol)

($\Leftarrow$) Sea $a \in G$ y sea $e_a \in G$ solución de $ya = a$. Luego $\forall b \in G$

$e_a(a \cdot b) = (e_a a)b = ab$

(semigrup)

Además $\forall c \in G$, $\exists b \in G$ / $a \cdot b = c$

$\Rightarrow \forall c \in G$ $e_a c = e_a(ab) = ab = c$

$\Rightarrow e_a (= e)$ cumple i) de la prop anterior

.) Usando de nuevo la hipótesis

$\forall a \in G \ \exists a^{-1} \in G \ / a^{-1} a = e$

(prop anteriors) $\Rightarrow G$ grupo

---

obs Sea G grupo y sea $a \in G$

la función $L_a : G \to G$, $L_a(b) = ab$

es biyectiva (pues la ecuación $ax = c$ tiene sol en G)

Análogo $R_a : G \to G$

Parte b) del ej 3): se reduce a probar la recíproca de esta observación (ver 8) i))

G grupo finito

	e	a	b	c
e	e	a	b	c
a	a	aa	ab	ac
b	b	ba	bb	bc
c	e	ca	cb	cc

tabla de multiplicar de G, cada fila/col es una permutación

$\mathbb{Z}_2$

	0	1
0	0	1
1	1	0

$\mathcal{U}(\mathbb{Z})$

	1	-1
1	1	-1
-1	-1	1