Grupos

Un grupo es un conjunto G junto con una operación $* : G \times G \longrightarrow G$ tal que:

1. la operación es asociativa

$$x * (y * z) = (x * y) * z \quad \text{para todo } x, y, z \in G$$

2. existencia de un neutro:

existe $e \in G$ tal que $e * x = x$ y $x * e = x$ para todo $x \in G$

3. existencia de inversos:

para todo $g \in G$ existe $g^{-1} \in G$ tal que $g * g^{-1} = g^{-1} * g = e$

ejemplos:

- $\underbrace{(\mathbb{Z}, +)}_{\text{es un grupo}}$: la suma es asociativa ✓

  neutro es el 0 ✓

  el inverso de n es $-n$: $n + (-n) = 0$ ✓

- $\underbrace{(\mathbb{Z}, \times)}_{\text{no es un grupo}}$: el producto es asociativo ✓

  el neutro es 1 ✓

  no todo elemento tiene inverso

  → no existe $n \in \mathbb{Z}$ tal que $n \cdot 0 = 1$

  → no existe $n \in \mathbb{Z}$ tal que $n \cdot 5 = 1$

Ejercicio 1. En cada uno de los siguientes casos, investigar si el conjunto y la operación forman un grupo.

a. El conjunto $M_{n\times n}(\mathbb{R})$ con el producto usual de matrices: $A * B = AB$.

b. El conjunto $M_{n\times n}(\mathbb{R})$ con la operación: $A * B = AB + BA$.

c. El conjunto $\mathbb{R}^2$ con la operación: $(x_1, x_2) * (y_1, y_2) = (x_1 y_1, x_2 y_1 + y_2)$.

d. $G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$ con el producto usual de matrices.

e. El conjunto $\{a, b, c\}$, con la operación $*$ definida mediante la tabla:

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

f. El conjunto $\{a, b, c, d\}$, con la operación $*$ definida mediante la tabla:

$*$	a	b	c	d
a	a	b	c	d
b	b	c	a	a
c	c	a	b	b
d	d	a	b	c

g. El conjunto $\mathbb{Z}$ con la operación $\otimes$ definida por: $a \otimes b = ab - 2(a + b) + 6$.

a) $M_{n\times n}(\mathbb{R})$ con el producto usual de matrices $A * B = AB$

① asociativa: $(AB)C = A(BC)$ para todo $A, B, C \in M_{n\times n}(\mathbb{R})$

② existencia del neutro: tenemos la matriz identidad

$AI = A$, $IA = A$ para todo $A \in M_{n\times n}(\mathbb{R})$

③ existencia de inversos: no se verifica

si $\det(A) = 0 \Rightarrow A$ no tiene inversa

$\Rightarrow M_{n\times n}(\mathbb{R})$ con el producto no es un grupo

$GL_n(\mathbb{R}) = \{ M \in M_{n\times n}(\mathbb{R}) : \det(M) \neq 0 \}$ es un grupo con el producto de matrices

$M_{n\times n}(\mathbb{R})$ con la suma de matrices:

① la suma de matrices es asociativa: $(A+B)+C = A+(B+C)$

② el neutro es la matriz nula O_n

③ existencia de inversos: el inverso de M es $-M$

$M + (-M) = O_n$

d) $G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a,b,c \in \mathbb{Z} \right\}$ con el producto usual de matrices

① el producto de matrices es asociativo ✓

② el neutro es $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

③ existencia de inversos:

si $A \in G \Rightarrow \det(A) = 1 \Rightarrow$ existe A^{-1}

falta ver que $A^{-1} \in G$

$$A = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \text{ con } a,b,c \in \mathbb{Z}$$

$$\left(\begin{array}{ccc|ccc} 1 & a & c & 1 & 0 & 0 \\ 0 & 1 & b & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & a & 0 & 1 & 0 & -c \\ 0 & 1 & 0 & 0 & 1 & -b \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\to \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -a & ab-c \\ 0 & 1 & 0 & 0 & 1 & -b \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$A^{-1} = \begin{pmatrix} 1 & -a & ab-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \in G$$

$\Rightarrow G$ es un grupo

e. El conjunto $\{a, b, c\}$, con la operación $*$ definida mediante la tabla:

$*$	a	b	c
a	a	b	c
b	b	c	$\boxed{a}$
c	c	$\boxed{a}$	b

① la operación es asociativa:

- $(a*b)*c \stackrel{?}{=} a*(b*c)$

  $b*c \stackrel{?}{=} a*a$

  $a = a$ ✓

- $(a*c)*b \stackrel{?}{=} a*(c*b)$

  $c*b \stackrel{?}{=} a*a$

  $a = a$ ✓

- $(b * a) * c \stackrel{?}{=} b * (a * c)$

  $b * c = b * c$ ✓

- $(b * c) * a \stackrel{?}{=} b * (c * a)$

  $a * a \stackrel{?}{=} b * c$

  $a = a$ ✓

- $(b * b) * c \stackrel{?}{=} b * (b * c)$

  $c * c \stackrel{?}{=} b * a$

  $b = b$ ✓

- $(c * c) * b \stackrel{?}{=} c * (c * b)$

  $b * b \stackrel{?}{=} c * a$

  $c = c$ ✓

- $(c * b) * c \stackrel{?}{=} c * (b * c)$

etc...

(2) el neutro es a:
$$a * a = a$$
$$a * b = b * a = b$$
$$a * c = c * a = c$$

(3) existencia de inversos:

$b * c = c * b = a$

$\rightarrow$ b es el inverso de c y c es el inverso de b

entonces es un grupo.

si tenemos un grupo finito podemos representar su operación mediante una tabla (tabla de Cayley)

$\rightarrow$ propiedad de Sudoku: cada elemento del grupo aparece una única vez en cada fila y cada columna
es decir las filas y las columnas son una permutación de los elementos del grupo

f. El conjunto $\{a, b, c, d\}$, con la operación $*$ definida mediante la tabla:

$*$	a	b	c	d
a	a	b	c	d
b	b	c	a	a
c	c	a	b	b
d	d	a	b	c

falla la propiedad de sudoku

① asociativa? $(b*c)*d \overset{?}{=} b*(c*d)$

$$a*d \overset{?}{=} b*b$$

$$d = c \quad \times$$

no se verifica la asociatividad $\Rightarrow$ no es un grupo

Ejercicio 2 G es un grupo $f*c=b$, $c*f=a$ $\Rightarrow$ no es conmutativo

b. $G = \{e, a, b, c, d, f\}$ con tabla de Cayley parcial:

·	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

por sudoku es el único lugar de la columna donde puede estar b

$a*b=e \Rightarrow b$ es el inverso de a $\Rightarrow b*a=e$

único lugar en la columna donde puede estar c

$$\underbrace{b}_{a\cdot a}\cdot b = (a\cdot a)\cdot b = a\cdot \underbrace{(a\cdot b)}_{e} = a\cdot e = a$$

$$f\cdot c = b \Rightarrow f\cdot f\cdot c = f\cdot b$$

$$\Rightarrow e\cdot c = f\cdot b$$

$$\Rightarrow c = f\cdot b$$

$$f\cdot b = fcd$$

$$= b\cdot d$$

$$= c$$