

# ESTRUCTURAS ALGEBRAICAS

## 1.1.a. Grupos y subgrupos

• Grupo: por  $(G, *)$  donde  $G$  es un conjunto no vacío y  $*$  es una operación interna que verifica:

- propiedad asociativa  $(a * b) * c = a * (b * c)$

-  $\exists$  e neutro:  $e \in G$  s.t.  $a * e = a$

-  $\exists$  inverso:  $a^{-1} \in G$  s.t.  $a^{-1} * a = e$

Se dice que  $(G, *)$  es un grupo abeliano si además verifica la propiedad commutativa:  $a * b = b * a$

• orden del grupo  $q = |G| =$  cardinal del gto. q. Si  $(G, *)$  es un grupo finito de operación se puede describir con una tabla (Tabla de Cayley)

$$4 * (2 * 5) = 7 \quad ( = 1 * 6 = 7 )$$

$$(4 * 2) * 5 = 6 \quad ( = 5 * 5 = 6 )$$

Es  $(G, *)$  grupo?

•  $a * b = \text{mcd}(a, b)$

> Es asociativa,

> ¿Es neutro?  $\forall a \in \mathbb{Z}$   $\text{mcd}(q, a) = a \Rightarrow a|a$ ,  $a|a \Rightarrow a = a$   $\Rightarrow$  No hay elemento neutro

$\Rightarrow \text{mcd}(q, a) = a \forall a \in \{1, 2, 4, 8\} \rightarrow \{1, 2, 4, 8\} \models a * b = \text{mcd}(a, b)$

> Es euclídea

	1	2	4	8
1	1	1	1	1
2	1	2	2	2
4	1	2	4	4
8	1	2	4	8

(operación)  $\models$

elemento neutro

elemento neutro  
No hay  
No es grupo

Alguna vez todo es  
tene uno el cojunto

$\{1, 2, 4, 8\}$

$\Rightarrow \text{mcd}(q, a) = a \forall a \in \{1, 2, 4, 8\} \Rightarrow a = a$

$\models$

$a * a = a \forall a \in \{1, 2, 4, 8\} \models$

$\Rightarrow$  Para encontrar el inverso tendríamos que buscar por ejemplo  $\text{mcd}(a, 1) = 1$   $\Rightarrow$  no hay, luego el 1 no tiene inverso. El 2 y el 4 no tienen tampoco inverso, pero el 8 si  $\Rightarrow$  NO es grupo.

$$\circ * : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

Es asociativa, tiene elemento neutro (1) pero no tiene inverso (para 2,  $\frac{1}{2}$ ,  $\frac{-1}{2}$ )

$$\forall b \in \mathbb{Z} \text{ tq } b \cdot 2 = 1 \text{ (no) que determina los enteros}$$

$$\circ : \{-1, 1\} \times \{-1, 1\} \rightarrow \{-1, 1\}$$

*	-1	1
-1	1	-1
1	-1	1

Si es grupo y ademá es abeliano

Lema 1: Si  $*$  es una operación asociativa en  $G$  entonces:

$$(a * b) * (c * d) = (a * (b * c)) * d$$

$$m * (c * d) = (m * c) * d \text{ por la asociatividad}$$

$$m = a * b$$

$$\Rightarrow (a * b) * (c * d) = ((a * b) * c) * d = (a * (b * c)) * d$$

$\uparrow$   
property  
associative

Lema 2: Sea  $(G, *)$  grupo con elemento neutro  $e$ . Todo elemento  $b \in G$  tal que  $b * b = e$

$$\begin{aligned} \text{existe } e. \quad & \text{Hipótesis: } b * b = b \\ & \exists b' \in G \text{ tq } b' * b = e? \quad \left. \right\} \Rightarrow b' * (b * b) = b' * b = e \\ & b' * (b * b) = e \Rightarrow (b' * b) * b = e \\ & \Rightarrow e * b = e \Rightarrow b = e \end{aligned}$$

TEOREMA 1 INVERSO Y NEUTRO PARA LA

OPERACIÓN

- si  $a, a' \in G$  tq  $a' * a = e$ , se verifica  $a * a' = e$   
 - si  $a \in G$ , se verifica  $a * e = a$

$$\textcircled{1} \quad da * a' = e? \quad \text{Hipótesis: } a' * a = e$$

$$\begin{aligned} & d(a * a') * (a * a') = a * a' ? \quad \text{Usar el Lema 1 y otra hipótesis:} \\ & \underline{(a * a') * (a * a')} = (a * (a' * a)) * a' = (a * e) * a' = a * a' = a * a' \end{aligned}$$

$$\begin{aligned} & (a * a') * (a * a') = a * a' \quad \checkmark \\ & b = a * a' \quad \checkmark \\ & \text{dado que es (formal)} \end{aligned}$$

$$\left. \begin{aligned} & \Rightarrow b * b = b \Rightarrow b = e : a * a' = e \\ & \uparrow \\ & \text{Lema 2} \end{aligned} \right\} \beta$$

• Teorema 2: UNICIDAD DEL NEUTRO Y DEL INVERSO

1. En todo grupo  $(G, *)$  el elemento neutro es único

→ Sean  $e_1, e_2 \in G$  dos elementos neutros de  $G$ :

$$e_1 * e_2 = e_2 = e_2 * e_1 = e_1 \Rightarrow e_1 = e_2$$

Cel. e. neutro va primero en la operación - not necessary

2. En todo grupo  $(G, *)$  el inverso de cada elemento  $a \in G$  es único

→ Sean  $b_1, b_2 \in G$  dos inversos de  $a \in G$ :

$$\begin{aligned} \text{d} b_1 = b_2? & (b_1 * a) * b_2 = a * b_2 = b_2 \\ & b_1 * (a * b_2) = b_1 * a = b_1 \end{aligned} \Rightarrow b_2 = b_1$$

• Notación: Ver hoja 1.1)

• Propiedades cancelativas: por la dcha. y por la izqda.:

Sea  $(G, *)$  un grupo,  $\forall a, b, x \in G$

- Si  $x * a = x * b$  entonces  $a = b$

$$\rightarrow x^{-1} * (x * a) = x^{-1} * (x * b)$$

$$(x^{-1} * x) * a = (x^{-1} * x) * b$$

$$e * a = e * b$$

$$\underline{a = b}$$

- Si  $a * x = b * x$  entonces  $a = b$

(demonstración análoga a la anterior)

1.1.b

• Grupos de congruencia módulo  $n$ :  $(\mathbb{Z}_n, +_n)$  y  $(\mathbb{U}_n, \cdot_n)$

relación de equivalencia

congruencia módulo  $n$ :

$$a \equiv_n b \Leftrightarrow n \mid (b-a)$$

↑  
grupo abeliano

$$\text{prop: } [a_n] + [b_n] = [a+b]_n$$

↑  
grupo abeliano tb, y tb. grupo  
de unidades módulo  $n$

$$\mathbb{U}_n = \{[r_n] \in \mathbb{Z}_n : \text{Mcd}(r, n) = 1\}$$

• Grupos  $(\mathbb{Q}, +)$ ,  $(\mathbb{Q}^*, \cdot)$

(chequear hoja 1.1.b)

1. En  $\mathbb{Q}$  se define la operación suma,  $\frac{a}{n} + \frac{b}{m} = \frac{ma+nb}{mn}$ .  $(\mathbb{Q}, +)$  es abeliano.

2. Sea  $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ , se define  $\frac{a}{n} \cdot \frac{b}{m} = \frac{ab}{mn} \cdot (\mathbb{Q}^*, \cdot)$  es abeliano

$$\mathbb{U}_{10} = \left\{ \left[\frac{1}{10}\right], \left[\frac{3}{10}\right], \left[\frac{7}{10}\right], \left[\frac{9}{10}\right] \right\}$$

$\frac{a}{10}$	1	3	7	$a$
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

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

$\frac{a}{10}$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Dato q. el resto 27, se guarda la lista de  $[7]_{10}$  ( $1^{\circ}$  q. tal que  $\text{Mcd}(n^2, 10) = 1$ )

## • Producto directo de grupos

sea  $(a_1, \star_1), (a_2, \star_2)$ , para  $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$

$$\text{prod. cartesiano: } (a_1, a_2) * (b_1, b_2) = (a_1 \underset{\substack{\text{operación} \\ \text{de } G_1}}{\star_1} b_1, a_2 \underset{\substack{\text{operación} \\ \text{de } G_2}}{\star_2} b_2)$$

$(G_1 \times G_2, \star)$  es un producto directo de  $(G_1, \star_1)$  y  $(G_2, \star_2)$

ti- $G_1$

ti- $G_2$

si los dos son abelianos, el producto directo también es y se llama suma directa:  $G_1 \oplus G_2$

## • Subgrupos ( $H \leq G$ )

sea  $(G, \star)$  un grupo y  $H \subseteq G$ ,  $H$  es subgrupo de  $(G, \star) \Leftrightarrow (H, \star)$  es un grupo. (dato)

L subgrupo propio: subgrupo  $H \leq G$  se dice proprio de  $(G, \star)$  si  $H \neq G$  y  $H \neq \{e\}$ .

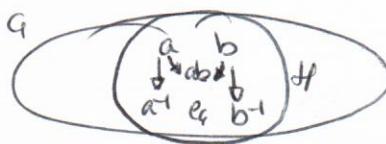
L subgrupo trivial: sea  $e_G \in G$  el e. neutro del grupo  $(G, \star)$ :

$$H_0 = \{e_G\} \leq G \rightarrow \text{subgrupo trivial}$$

## • Definición equivalente de subgrupo // condiciones para los subgrupos

- el elemento neutro de  $G$  pertenece a  $H$ :  $e_G \in H$
- la operación  $\star$  existe en  $H$ :  $\forall a, b \in H, a \star b \in H$  (op. int. de  $G$ )
- $\forall a, a^{-1} \in H$  ( $a^{-1}$  es el inverso de  $a$  en  $G$ , y  $b \cdot a^{-1} \in H$  debe estar en  $H$ )

en dibujo, estos 3:



otras condiciones: grupo  $\left\{ \begin{array}{l} \text{asociativa} \\ \text{neutral} \\ \text{inverso} \end{array} \right.$ ; subgrupo (y por tanto grupo)  $\left\{ \begin{array}{l} \text{operación interna} \\ \text{neutral} \\ \text{inverso} \end{array} \right.$

" $\Rightarrow$ " si  $H \leq G \Rightarrow (H, \star)$  el grupo  $\Rightarrow \forall a, b \in H, a \star b \in H$  (Op. interna)  $\checkmark$ ,  $e_H \in H \checkmark$ ,  $a^{-1} \in H \checkmark$   $\cancel{\Rightarrow H \star H \rightarrow H}$  la operación interna

" $\Leftarrow$ " si se verifica  $\textcircled{sg}_1$ ,  $\textcircled{sg}_2$  y  $\textcircled{sg}_3 \Rightarrow \star: H \star H \rightarrow H$  es operación interna por  $\textcircled{sg}_1$ ,  $\star(H, \star)$  es grupo?

- $\forall a, b, c \in H \rightarrow a, b, c \in G$ ;  $a \star (b \star c) = (a \star b) \star c$   $\checkmark$  asociativa
- $\textcircled{sg}_2 \rightarrow \exists e \in H \checkmark$
- $\textcircled{sg}_3 \rightarrow \forall a \in H \exists a^{-1} \in H \checkmark$

el grupo  $\checkmark$

comprobar que es grupo: // lo hacemos con las condiciones de subgrupo, y así no tenemos que demostrar la asociatividad

$$SL_n(\mathbb{R}) = \{ A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in \mathbb{R}^{n \times n} : \det(A) = 1 \} \subset GL_n(\mathbb{R})$$

subgrpo  
del grpo general  
de matrices cuadradas  
que tienen  $\det 1$

operación interna

- $\det(A) = 1$
  - $\det(B) = 1$
- $\Rightarrow \det(A * B) = \det(A) * \det(B) = 1 * 1 = 1$
- $\exists e \in ?$  matriz  $I \Rightarrow \det(I) = 1 \in SL_n(\mathbb{R})$
- $\exists A^{-1} \forall A \in SL_n(\mathbb{R})$

$$\det(A^{-1}) = (\det(A))^{-1} = 1^{-1} = 1 \in SL_n(\mathbb{R})$$

en subgrpo y por tanto srgro

comprobar que el subgrupo

En el grpo  $(\mathbb{Z}_6, +_6)$  se considera el subconjunto:  $H = \{0, 2, 4\}$

$H$  es L (centros red. 6)

~~$\mathbb{Z}_6$  puede ser subgrupo de  $\mathbb{Z}_6$  (es propio)~~, comprobando las condiciones de subgrupo:

$$\text{elems } \mathbb{Z}_6: \{ [0], [1], [2], [3], [4], [5] \}_6$$

• operación interna ( $+_6$ ):  $a \in \mathbb{Z}_6,$

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$b \in \mathbb{Z}_6,$   
 $a+b \in \mathbb{Z}_6?$

✓

• neutro?:  $0 \in H$  (o.e. de  $\mathbb{Z}_6$ )

• inverso?:  $2^{-1} = 4$   
 $4^{-1} = 2$   
 $0^{-1} = 0$  en  $\mathbb{Z}_6$ , y ademá

tb están en  $H$

por tanto, con  
estos 3,  $H$  es subgrpo,  
y con ello grpo.

### Caracterización de subgrpo

si  $(G, *)$  es un grpo y  $H \subseteq G$  entonces

$$H \leq G \Leftrightarrow \forall a, b \in H \text{ se verifica } a * b^{-1} \in H$$

demo:

$$\begin{array}{l} \xrightarrow{H \text{ es subgrpo}} \\ \xrightarrow{\text{si } H \leq G} H \neq \emptyset \text{ porque es el e.neutro y además} \\ \text{(partimos de 3)} \quad \forall a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a * b^{-1} \in H \end{array}$$

$\xleftarrow{\text{partimos de 2}}$   $\text{tf } \emptyset, \text{ sea } a \in H \Rightarrow a, a \in H \Rightarrow a * a^{-1} = e_g \in H$

sea  $b \in H \Rightarrow e_g * b \in H \Rightarrow e_g * b^{-1} = b^{-1} \in H$

$\forall a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H \Rightarrow a * b \in H$

■ Comprobar que es grupo (con esta última condición):

grupo ortogonal:

$$O_n(\mathbb{R}) = \{ A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in \mathbb{R}^{n \times n} : A^T A = I \} \subset G L_n(\mathbb{R})$$

(grupo de matrices ortogonales)

Primeros:  $O_n(\mathbb{R}) = \emptyset$ ? No, tenemos la matriz  $I$  (elem. neutro en  $G$  y  $O_n$ )

Respecto a esta pregunta, ante que cualquier elemento buscamos el elemento neutro, porque así si no lo encontramos ya sabremos que no es gnp.

Segundo: Si  $A, B \in O_n(\mathbb{R})$ ,  $A * B^{-1} \in O_n(\mathbb{R})$ ?

$$\text{se sabe que } \begin{cases} A^T \cdot A = I \\ B^T \cdot B = I \end{cases} \Rightarrow \begin{cases} A^T = A^{-1} \\ B^T = B^{-1} \end{cases}$$

$$(A \cdot B^{-1})^T \cdot (A \cdot B^{-1}) = ? =$$

$$= (B^{-1})^T \cdot A^T \cdot A \cdot B^{-1} = (B^{-1})^T \cdot B^{-1} =$$

$$= B \cdot B^{-1} = I \quad \checkmark$$

④ ojo al condicón de orden

■ Comprobar que el subgrupo (con la ult. condición 4b)

se considera el grupo  $(\mathbb{Z}_3 \times \mathbb{Z}_2, +_3 \times +_3)$  y el subconjunto  $H = \{(0,0), (0,1), (0,2)\}$

$$(0,0) - (0,0) = (0,0)$$

$$(0,0) - (0,1) = (0,2)$$

$$(0,0) - (0,2) = (0,1) \quad (-2 \text{ en } \mathbb{Z}_3 = [1]_3)$$

$$(0,1) - (0,0) = (0,1)$$

$$(0,1) - (0,1) = (0,0)$$

$$(0,1) - (0,2) = (0,2) \quad (-1 \text{ en } \mathbb{Z}_3 = [2]_3)$$

$$(0,2) - (0,0) = (0,2)$$

$$(0,2) - (0,1) = (0,1)$$

$$(0,2) - (0,2) = (0,0)$$

$$\begin{matrix} -6 & -5 & -4 \\ -3 & -2 & -1 \\ [0]_3 & [1]_3 & [2]_3 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{matrix}$$

$$A * B^{-1} \in \mathbb{Z}_3$$

\* Uso el - por el inverso / cuando el + solo comprobó la operación interna, y se hace con la primera condición (3 prop.) en vez de con la anterior.

■ Obtener el mínimo subgrupo que contiene a  $a \in \mathbb{Z}_6$

en el grupo  $(\mathbb{Z}_6, +_6)$

$$\begin{array}{l} ① a=1 \\ ② a=2 \\ ③ a=3 \end{array} \left. \right\} \in \mathbb{Z}_6$$

↓ El subgrupo en  $\mathbb{Z}_6$  más pequeño que contiene a  $a = \{ \}$ ?

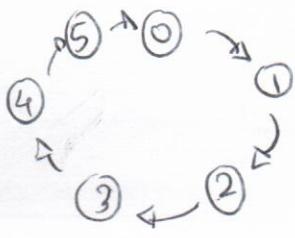
$\mathbb{Z}_6$  (entero), pq tiene que contener al 1 y  $+_6$  a 1+1, 1+1+1, etc

↓ El subgrupo en  $\mathbb{Z}_6$  más pequeño que contiene a  $a = 2$ ?

$$H_2 = \{2, 4, 0\}; \text{ tiene que contener } 2, 2+2, 2+2+2, \text{ etc}$$

↓ El subgr. en  $\mathbb{Z}_6$  más pequeño que contiene a  $a = 3$ ?

$$H_3 = \{3, 0\}; 3, 3+3, 3+3+3, \text{ etc}$$



1.2.a

$$3^2 \text{ (operación de } z_6 : +_6) = 3+3$$

$$\begin{aligned} |3| &= 2 \quad (3+3=6=0_6) && \text{ctb. resto es 6} \\ |5| &= 6 \quad (5+5=10=0_6) && \text{pero 3 en el menor} \\ |6| &= 6 \quad (6+6=12=0_6) \end{aligned}$$

### • Orden de un elemento

sea  $(G, *)$  un grupo y  $a \in G$

- orden de  $a$  es el menor entero positivo  $r \in \mathbb{Z}^+$  tq  $a^r = e_q$

- si para todo  $n \in \mathbb{N}$ ,  $a^n \neq e_q$  se dice que el orden de  $a$  es infinito

se escribe  $\cdot |a|=r$  o  $\cdot |a|=\infty$

### • (Caracterización) de orden de un elemento

sea  $(G, *)$  grupo y  $a \in G$ , para todo  $k \in \mathbb{Z}$  se verifica  $a^k = e_q \Leftrightarrow |a| \text{ divide a } k$

" $\Rightarrow$ " sea  $|a|=n$  y  $a^k = e_q \Rightarrow n \mid k?$

$$k = n \cdot q + r \quad 0 \leq r \leq n \quad \Rightarrow \quad a^k = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$$

$$a^k = e \Leftrightarrow e^r = e \quad \text{siendo} \quad 0 \leq r \leq n \quad \left\{ \begin{array}{l} r=0 \\ n=|a| \end{array} \right. \Rightarrow \underline{\underline{r=0}}$$

" $\Leftarrow$ " si  $|a|=n$  divide a  $k \Rightarrow k = nq \Rightarrow a^k = (a^n)^q = e^q = e$

¶ obtener el orden de los elementos indicados

$(G, \circ_2)$  siendo  $G = \{(a, b) : a, b \in \mathbb{Z}_7, a \neq 0\}$

Operación  $(*) = \circ_7 = \text{producto en } \mathbb{Z}_7$

$$\cdot A = \begin{pmatrix} 6 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 6 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}; \quad \begin{pmatrix} 6 & 1 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \quad \dots \quad \begin{pmatrix} 6 & 1 \\ 0 & 1 \end{pmatrix}^7 = \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix} \xrightarrow{\text{en } \mathbb{Z}_7} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$|A|=7$  (elem. neutro)

$$\cdot B = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix} \text{ et...} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \text{ en } \mathbb{Z}_7$$

$$\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ 0 & 1 \end{pmatrix} \quad \dots$$

$$\dots \quad \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^6 = \begin{pmatrix} 15 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ en } \mathbb{Z}_7 \quad (\text{directamente})$$

$|B|=6$  identidad

### Sistema de generadores:

- subgrupo generado por un conjunto: sea  $(G, *)$  un grupo y  $A \subseteq G$  subconjunto no vacío de  $G$ . Se denomina subgrupo de  $G$  generado por  $A$  al menor subgrupo de  $(G, *)$  que contiene a  $A$ :

$$\langle A \rangle = \{a_1^{r_1} * \dots * a_n^{r_n} : a_i \in A, r_i \in \mathbb{Z}, n \in \mathbb{N}\}$$

- sistema de generadores: un cjto.  $A \subseteq G$ , se llama sistema de generadores del grupo  $(G, *)$  si verifica:  $G = \langle A \rangle$

- grupo cíclico: el grupo  $(G, *)$  es cíclico si tiene un sistema de generadores formado por un único elemento: existe  $a \in G$  tq:

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\} \quad \text{en notación aditiva:}$$

$$G = \langle a \rangle = \{na : n \in \mathbb{Z}\}$$

### El orden de un elemento coincide con el orden del subgrupo que genera

sea  $(G, *)$  un grupo y  $a \in G$ :  $|a| = |\langle a \rangle|$

$$\rightarrow |a| = n \Rightarrow \{a, a^2, \dots, a^n, a^n = e\} \quad \text{y}$$

$$\text{suponemos que } a^i = a^j \quad 0 < i < j \leq n \Rightarrow a^i + a^{j-i} = e \Rightarrow a^{j-i} = e$$

siendo  $0 < j-i < n$   
contradicción con  $|a| = n$

$$\langle a, a^2, \dots, a^n = e \rangle \subset \langle a \rangle \Rightarrow |\langle a \rangle| \geq n$$

$$\text{d} \langle a \rangle \subset \langle a, a^2, \dots, a^n = e \rangle ?$$

$$\begin{aligned} \text{sea } b \in \langle a \rangle &\Rightarrow b = a^k \quad \text{sea } k = n \cdot q + r \quad 0 \leq r < n \Rightarrow \\ &\Rightarrow b = a^k = (a^n)^q \cdot a^r = e \cdot a^r = a^r \Rightarrow b = a^r \in \langle a, a^2, \dots, a^{n-1}, e = a^n \rangle \end{aligned}$$

Tener en cuenta then: El orden de un elemento coincide con el orden del grupo que genera  
(subgrupo)

### Diagrama de Cayley de un grp:

sea  $(G, *)$  un grupo finito de orden  $n$  con generadores  $\{g_1, \dots, g_r\}$ .

$(G, *)$  puede representarse mediante un digrafo  $\mathcal{D} = (V, E)$  con  $V = G = \{a_1, \dots, a_n\}$  y para cada generador  $g_k$  hay un arco  $(a_i, a_j) \in E$  etiquetado  $g_k \Leftrightarrow$

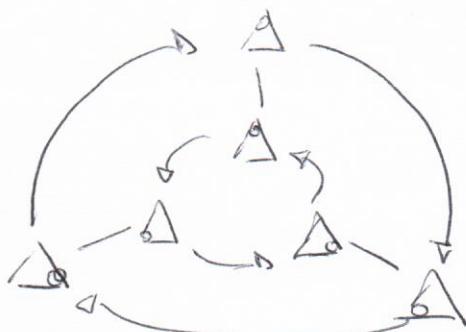
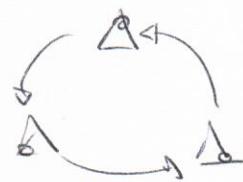
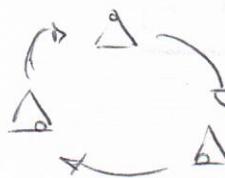
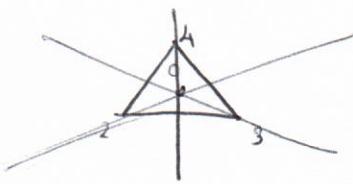
(cont.)

$$g_k * a_i = a_j$$

④ obtener los subgrupos aditivos propios no triviales?.

④ construir la tabla de Cayley del grupo

grupo de simetría del triángulo (grupo diédrico 3)



trasladando la vuelta, se ve los diámetros

$$\text{DGA} \\ \text{Op } g \cdot s^2 = e \\ s \cdot g^2 = g$$

*	e	g	$g^2$	s	$gs$	$g^2s$
e	e	g	$g^2$	s	$gs$	$g^2s$
g	g	$g^2$	e	$gs$	$g^2s$	s
$g^2$	$g^2$	e	g	$g^2s$	s	$g^2$
s	s	$g^2s$	$gs$	e	$s^2$	g
$gs$	$gs$	g	$g^2s$	g	e	$g^2$
$g^2s$	$g^2s$	gs	s	$g^2$	g	e

ver pag. siguiente

el otro(s) estípulos, cuál?

### • Grupos de cuaterniones y grupos diédricos

- Grupo de cuaterniones:  $Q_8$ , grupo generado por dos elementos de orden 4,  $a, b \in Q_8$  tales que  $bab = a^{-1}b$  y  $b^2 = a^2$ .

$$\rightarrow Q_8 = \langle a, b : |a| = 4, b^2 = a^2, bab = a^{-1}b, |b| = 4 \rangle$$

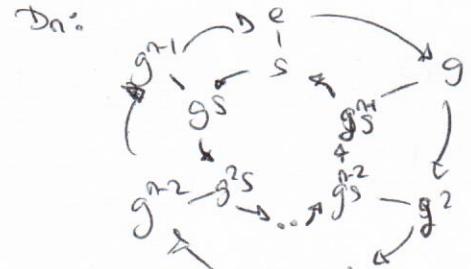
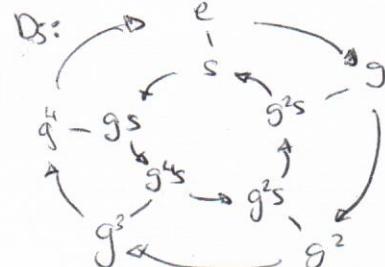
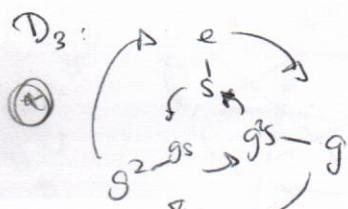
- Para todo  $n > 2$ , se llama grupo diédrico  $D_n$  al grupo de las simetrías de un polígono regular de  $n$  lados. su orden es  $2n$  y está generado por un elemento  $a \in D_n$  de orden  $n$  y un elemento  $b \in D_n$  de orden  $2 + \frac{n}{2}$ .  $bab = a^{-1}b$ .

$$\rightarrow D_n = \langle a, b : |a| = n, |b| = 2, bab = a^{-1}b \rangle$$

III  
III mismo, para lo de la cuarta:

para todo  $n > 2$  se llama grupo diédrico  $D_n$  a un grupo, de orden  $2n$ , generado por dos

$$g, s \in D_n$$
 tales que  $|g| = n$ ,  $|s| = 2$  y  $sg = g^{-1}s$



(cont.)

• Propiedades de grupos cíclicos

① Todo grupo cíclico es abeliano

demo: sea  $(G, *)$  un grupo cíclico  $\forall a, b \in G$ , da  $a * b = b * a$ ?

$$G = \langle g \rangle \text{ para } g \in G$$

una de generadora  $\rightarrow a = g^r$  y  $b = g^s \rightarrow a * b = g^r * g^s = g^{r+s} = g^{s+r} = g^s * g^r = b * a \quad \checkmark$

② Todo subgrupo de un grupo cíclico es cíclico

demo:  $(G, *)$  es cíclico y  $H \leq G$ 

$$G = \langle g \rangle$$

$$\rightarrow H \subseteq G \rightarrow \forall a \in H, a = g^h$$

- si  $H = \langle e_G \rangle = \{e_G\}$  es cíclico

- si  $H \neq \{e_G\}$ , sea  $g^r \in H$  tq r el menor positivo con  $g^r \in H$ , d  $H = \langle g^r \rangle$ ?

$$\text{sea } b \in H \rightarrow b \in G \rightarrow b = g^h \quad \text{d} b = g^h = (g^r)^q ?$$

$dh = r \cdot q$ ? dividimos h entre r:  $h = q \cdot r \rightarrow s, 0 \leq s < r \rightarrow$

$$\begin{matrix} b = g^h = & (g^r)^q \cdot g^s \\ \uparrow H & \underbrace{\qquad}_{\in H} \end{matrix} \rightarrow g^s = (g^r)^q \quad \text{d} b \in H \rightarrow s = 0 \rightarrow$$

$$\rightarrow h = r \cdot q \quad \checkmark$$

Estudiar si es cíclico:

 $(\mathbb{Z}_8, +_8)$  obtener todos sus subgrupos y el orden que tiene cada uno de ellos.

$\mathbb{Z}_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$$1, 1+1, 1+1+1, \dots \text{ etc}$$

$$H_1 = \langle 1 \rangle = \mathbb{Z}_8 \Rightarrow \text{orden: 8}$$

$$H_2 = \langle 2 \rangle = \langle 2, 4, 6, 0 \rangle \Rightarrow \text{orden: 4}$$

$$H_3 = \langle 3 \rangle = \langle 3, 6, 1, 7 \rangle \Rightarrow \text{orden: 8} \quad (3) = \frac{8}{\text{mcd}(3, 8)} = 8$$

$$H_4 = \langle 4 \rangle = \langle 4, 0 \rangle \quad (4) = \frac{8}{\text{mcd}(4, 8)} = 4 \quad \text{orden: 4}$$

$$H_5 = \langle 5 \rangle = \mathbb{Z}_8 \quad \text{orden: 8}$$

$$H_6 = \langle 6 \rangle = \langle 6, 4, 2, 0 \rangle \quad \text{orden: 4}$$

$$H_7 = \langle 7 \rangle = \mathbb{Z}_8 \quad \text{orden: 8}$$

$$H_8 = \langle 0 \rangle = \langle 0 \rangle \quad \text{orden: 1}$$

obtener todos los subgrupos cíclicos, propios, triviales (?)

Grado de centralidad  $Q_8 = \{a, b : |a|=4, |b|=4, b^2=a^2, ba=a^{-1}b\}$

e	a	$a^2$	$a^3$	b	ab	$a^2b$	$a^3b$
e	$a^3$	$a^2$	a	b	ab	$a^2b$	$a^3b$
a	$a^2$	$a^3$	e	ab	$a^2b$	$a^3b$	b
$a^2$	$a^3$	a	e	$a^2b$	$a^3b$	b	ab
$a^3$	a	$a^2$	a	$a^3b$	b	ab	$a^2b$
b	$b^2$	$a^3b$	$a^2b$	ab	$a^2$	a	$a^3$
ab	ab	b	$a^3b$	$a^2b$	$a^3$	$a^2$	a
$a^2b$	$a^2b$	$a^3b$	b	ab	e	$a^3$	$a^2$
$a^3b$	$a^3b$	$a^2b$	ab	b	a	e	$a^3$

(revisar esto: que el an  
pero que cada grupo (theta  
diédrico))

misma q el  
anterior

29-2-2018



EJERCICIOS TEMA 1.1 y 1.2

hoja 1.3

27/2/2018

Grados de permutación

> Grupo simétrico:

El conj.  $S_x = \{f : X \rightarrow X \text{ aplicación biyectiva}\}$  de las aplicaciones biyecciones definidas en  $X \neq \emptyset$ , con la operación composición de aplicaciones, es un grupo que se denomina grupo simétrico sobre  $X$  y se nota:

$(S_x, \circ)$

demo:  $(S_x, \circ)$  es grupo

$\forall f, g \in S_x \Rightarrow f, g : X \rightarrow X \text{ son biyectivas} \Rightarrow f \circ g : X \rightarrow X \text{ y es biyectiva}$

demo: la composición es asociativa

$f, g, h : X \rightarrow X$

$$f \circ (g \circ h) = (f \circ g) \circ h$$

$$\forall x \in X \quad f[g[h(x)]] = \overbrace{f(g[h(x)])}^{(\text{const.})}$$

$\xrightarrow{\hspace{1cm}}$   
(const.)

$$D_4 = \{g, g^2, g^3, e, s, gs, g^2s, g^3s\} \quad (|g|=n=4 \quad |s|=2 \quad sg = g^{-1}s)$$

Grupo cuarto de Klein:  $D_2$ , con grupo de orden 4, generado por dos elementos  $g, s \in D_2$  tq  $D_2 = \langle g, s : |g|=2, |s|=2, sg = gs \rangle$

Leyenda:  $\begin{matrix} \text{Leyenda} \\ \text{de Cayley} \end{matrix}$

$e$	$a$	.	$e$	$g$	$s$	$gs$
$ $	$ $		$e$	$e$	$g$	$s$
$b$	$-ab$		$g$	$g$	$e$	$gs$
$ $	$ $		$s$	$s$	$gs$	$e$
			$gs$	$gs$	$s$	$g$

GOT IT : en este p.ej:  $|g|=2, |s|=2;$

-  $gs \cdot g = g^2s$  pero  $g^2$  no puede ser pq no es max,  $g^n \leq 2$

||  
es =  $s$

-  $gs \cdot gs = g^2 \cdot s^2 \Rightarrow e \cdot e = e$

-  $s \cdot gs = g \cdot s^2 \Rightarrow g \cdot e = g$

U  
cardinal  
(en este  
caso maximo  
para g y  
s)

ver resto ejemplos  
( $\neq$  cardinales y didácticos)  
grupos

(hoja 1.2.b)

III Encontrar subgrupos ciclicos propios no (palabra)

$D_3 = \{e, g, g^2, s, gs, g^2s\}$  el orden <sup>“”</sup> de cada uno de los elem.

$$H_1 = \langle e \rangle = \{e\}$$

$$H_2 = \langle g \rangle = \{g, g^2, e\}$$

$$H_3 = \langle g^2 \rangle = \{g^2, g^4, e\} \Rightarrow |g^2| = \frac{|g|}{\text{mcd}(2, 3)} = 3$$

$$H_4 = \langle s \rangle = \{s, e\}$$

$$H_5 = \langle ss \rangle = \{ss, e\}$$

$$H_6 = \langle g^2s \rangle = \{g^2s, e\}$$

$$H_7 = \langle g, s \rangle = D_3$$

$$H_8 = \langle gs, s \rangle = \langle g, s \rangle$$

$$H_9 = \langle gs, g^2s \rangle = \langle g, ss \rangle$$



$$\begin{aligned} ba &= a^{-1}b \\ gsgs &= \cancel{(gs)^2} = (gs)^{-1}gs = g^2s \cdot gs = g^3s^2 = e \quad (\text{en } D_3) \\ g^2sg^2s &= e \\ (gs)^{-1} \cdot gs &= e \end{aligned}$$

grupos formados por dos elementos en el total:  $D_3$

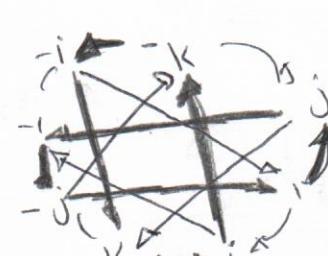
IV Encontrar generadores del grupo

$$G = \{1, j, i, k, -1, -i, -j, -k\}$$

compararlo con el grupo de cuaterniones

.	1	i	j	k	-1	-i	-j	-k
1	1	i	j	k	-1	-i	-j	-k
i	i	-1	-k	-j	-i	1	-k	-j
j	j	-k	-1	-i	-j	k	1	-i
k	k	j	i	-1	-k	-j	-i	1
-1	-1	-i	-j	-k	1	i	j	k
-i	-i	1	-k	-j	-1	-k	-j	-i
-j	-j	k	1	-i	-j	-k	i	-1
-k	-k	j	i	1	-k	-j	-i	-1

$$\begin{aligned} ij &= k & ji &= -k \\ jk &= i & ki &= -i \\ kj &= -j & ik &= -i \\ kj &= j & ik &= -i \\ kj &= -i & ik &= -s \end{aligned}$$



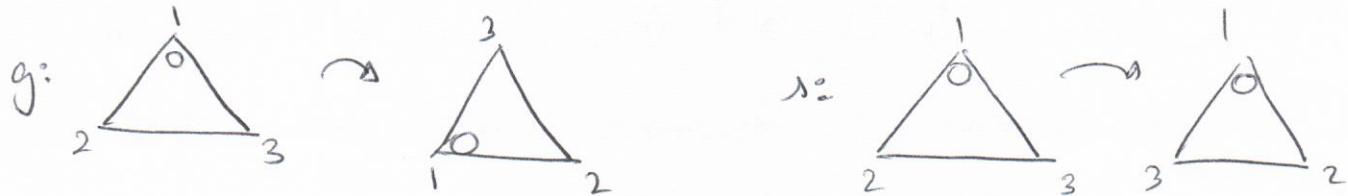
no lo  
paso,  
para el  
examen  
revisarlo  
lo  
compruebo  
y clavo.)

Relaciones entre grupos  $(S_3, \circ)$  y  $(D_3, \circ)$   $\xrightarrow{g \in S_3, s \in D_3}$   
permutaciones

$D_3 = \{g, s : |g|=3, |s|=2, sg = g^{-1}s\}$  / diédrico

$S_3 = \text{(ej. anterior)}$

Estableciendo una biyección entre los elementos



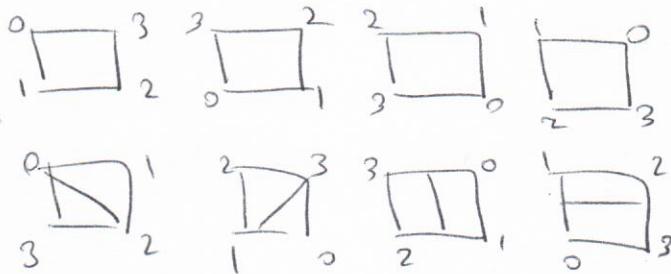
$$D_3 = \{e, g, g^2, 1, g^3, g^21\}$$

$\begin{matrix} \xrightarrow{\text{rel. 19}} & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \xrightarrow{\text{rel. 19}} \\ \text{rel. 19} & \begin{pmatrix} 3 & 1 & 2 \end{pmatrix} & \begin{pmatrix} g & g \\ 3 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \end{matrix}$

Estudia una posible relación entre los grupos  $(S_4, \circ)$ ,  $(D_4, \circ)$

$D_4 = \text{(ej. anterior, pero para 4)}$

Calculo el orden de cada uno de los grupos.



recordar:

$$D_n = \{g, s ; |g|=n, |s|=2, sg = g^{-1}s\}$$

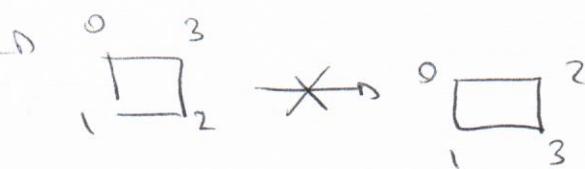
elementos:

$$D_n = \{e, s, g, g^2, g^3, g^4, \dots, g^{n-1}\}$$

$$|D_4| = 8$$

$$\nexists$$
  

$$|S_4| = 24$$



$$D_4 \leq S_4$$

(cont.)

demo: tiene elem. neutro

$$\text{id}_X: X \rightarrow X \quad \text{id}_X(x) = x \quad \forall x \in X$$

demo: todo elem. tiene opuesto o inverso

$$f \in S_X \quad f: X \rightarrow X \text{ biyectiva} \Rightarrow f^{-1} \in X \quad \forall x \in X \quad f^{-1}$$

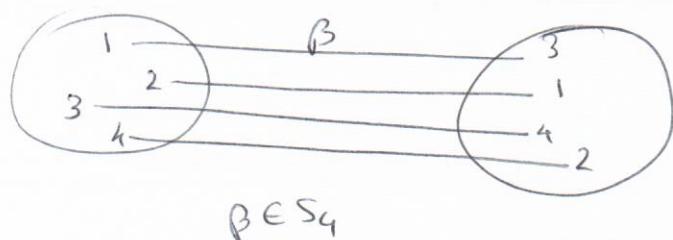
$$f(x) = z \text{ se define } f^{-1}(z) = x \quad \text{y } f^{-1} \text{ es biyectiva}$$

> Grupo permutaciones:

cuando el conj.  $X$  del grupo simétrico está formado por un nº finito de enteros consecutivos, a ese grupo se le da el nombre Grupo de permutaciones.

permutaciones posibles (ithink)

hay  $n!$  elementos en el grupo de permutaciones  $S_n: |S_n| = n!$



$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

• calcular los productos  $\alpha\beta$  y  $\beta\alpha$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$$

$$\alpha\beta = \begin{pmatrix} 1 & 3 & 2 & 5 & 1 & 4 & 2 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$$

// la composición van de derecha a izqdo !

• completar tabla de  $(S_3, \circ)$

$$S_3 = \left\{ P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

	$P_0$	$P_1$	$P_2$	$\mu_1$	$\mu_2$	$\mu_3$
$P_0$	$P_0 P_0$	$P_0 P_1$	$P_0 P_2$			
$P_1$		$P_1 P_1$				
$P_2$			$P_2 P_2$			
$\mu_1$				$\mu_1 \mu_1$		
$\mu_2$					$\mu_2 \mu_2$	
$\mu_3$						$\mu_3 \mu_3$

etc.

demo:

$$\textcircled{1} \quad f^k(a_i) = a_{(i+k) \bmod r} ?$$

inducción:

$$k=1: \quad f(a_i) = a_{(i+1) \bmod r} \quad \checkmark$$

$$\text{sup: } ((k-1) \text{ cierto: } f^{k-1}(a_i) = a_{(i+(k-1)) \bmod r} \text{ cierto} \\ \text{y} \\ f^k(a_i) = f(f^{k-1}(a_i)) = f(a_{(i+(k-1)) \bmod r}) = a_{(i+k) \bmod r}$$

$$\textcircled{2} \quad f^r(a_i) = a_{i+r \bmod r} = a_i \quad \left| \begin{array}{l} \text{por tanto} \\ k=r \Rightarrow f^r = id \end{array} \right.$$

llego r es el orden

↓ inverso de un ciclo de longitud r

$$\tau = (a_0, a_1, \dots, a_{r-1}) \quad \text{el inverso es } \tau^{-1} = \sigma^r$$

demo:

$$\tau^r = id \rightarrow \tau^{r-1} \cdot \tau = id \rightarrow \tau^{-1} = \sigma^{r-1} \quad \checkmark$$

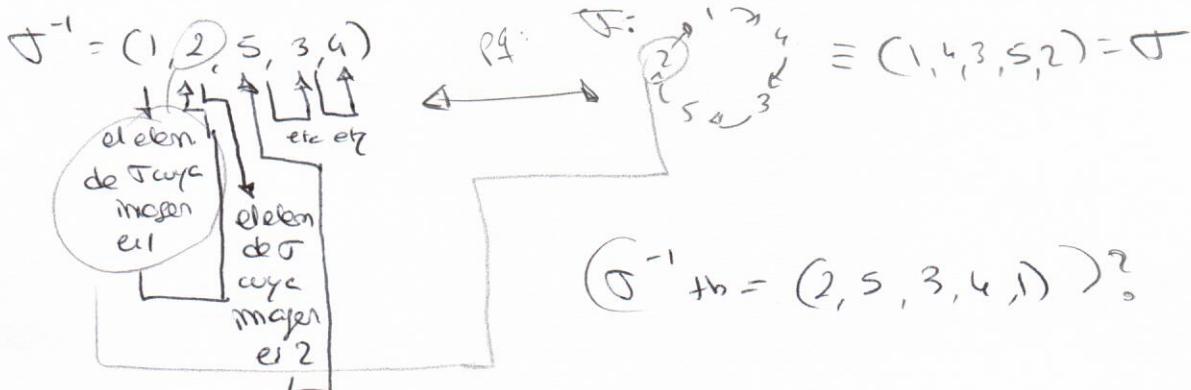
¶ calcular  $\tau^{-1}$

$$\tau = (1, 4, 3, 5, 2)$$

$$r=5 \quad \text{long} (= \text{orden})$$

¿De cuanta forma se puede operar  $\tau^{-1}$ ?

es más rápido calcular la inversa de la aplicación que hacer  $\sigma^4 (= f^{-1})$



> Ciclos y transposiciones:

Sea  $\sigma \in S_n$ . Se dice que  $\sigma$  es un ciclo de longitud  $r$  si existen  $a_0, \dots, a_{r-1} \in \{1, \dots, n\}$  tales que:

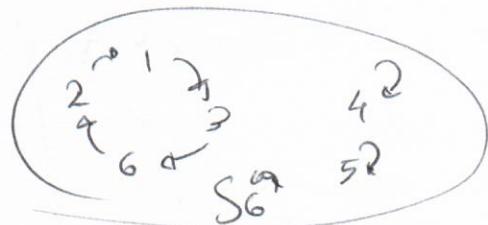
$$\sigma(a_0) = a_1, \sigma(a_1) = a_2, \dots, \sigma(a_{r-2}) = a_{r-1}, \sigma(a_{r-1}) = a_0.$$

y  $K \in \{1, \dots, n\}$  tal que  $K \notin \{a_0, \dots, a_{r-1}\}$  y  $\sigma(K) = K$ .

Los ciclos de longitud 2 se denominan transposiciones.

$$\sigma = \{a_0, a_1, \dots, a_{r-1}\}$$

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



• Estudiar el ciclo:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 9 & 8 & 2 & 4 & 5 & 7 \end{pmatrix}$$

$$\beta = (1, 3, 6, 2)$$

$$\alpha = (4, 9, 7)$$

$$\lambda = (5, 6) \quad \text{(Transposición)} \\ \text{ciclo, long. 2.}$$

NO ES CICLO (hay 3, y todos de + de 1 elem, si hubiere 1 y el resto de 1 elem, o solo 1, si reír a do)

Es permutación.

> Toda permutación se puede escribir como producto de ciclos disjuntos

> Orden de un ciclo:

sea  $\sigma = (a_0, \dots, a_{r-1})$  un ciclo, entonces:

$$\textcircled{1} \quad a^k(a_i) = a_{(i+k) \bmod r} \quad \forall i \in \{0, \dots, r-1\} \quad k \in \mathbb{N}$$

( $r = \text{const}(\text{long. ciclo})$ )

$$\textcircled{2} \quad \text{El orden de } \sigma \text{ es su largo: } |\sigma| = r$$

demas.

Exhibir como producto de transposiciones

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

11

$$\alpha = (1, 6, 4, 2) \quad (3, 8, 5, 7) \quad // \text{ciclos disjuntos}$$

$$(1, 6, 4, 2) = (1, 6) (6, 4) (4, 2) \quad // \text{NO DISJUNTOS} \Rightarrow \text{NO COMMUTAN}$$

$$(3, 8, 5, 7) = (3, 8) (8, 5) (5, 7) \quad // \text{4}$$

u

> Toda permutación se puede expresar como producto de transposiciones.

que  $\in S_n$ , con

$n \geq 2$

$$(a_0, a_1, \dots, a_n) = (a_0, a_1) (a_1, a_2) \dots (a_{n-1}, a_n)$$

$$\text{ej: } \alpha = (1, 6, 4, 2) \quad (3, 8, 5, 7)$$

$$\alpha = (1, 6) (6, 4) (4, 2) \quad (3, 8) (8, 5) (5, 7)$$

(2 ciclos disjuntos)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 4 & 6 & 3 & 5 & 7 & 8 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 6 & 8 & 9 & 3 & 4 & 7 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 4 & 6 & 8 & 3 & 5 & 7 & 9 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 3 & 9 & 5 & 2 & 6 & 8 \\ 1 & 4 & 3 & 9 & 7 & 5 & 2 \end{pmatrix} (6, 8)$$

~~$\alpha \beta = \beta \alpha$~~

$$\alpha \beta = (1, 2, 4) (3, 8) (1, 2, 4, 5) (3, 9, 7) (6, 8)$$

11

$$\underline{(1, 4, 3, 9, 7, 5, 2)} (6, 8)$$

▷ calcular el producto de  $\alpha \beta$

$$\alpha = (1, 2, 4) \quad (3, 8)$$

$$\beta = (1, 2, 4, 5) (3, 9, 7) (6, 8)$$

▷ Estudiar si es posible hacer de la primera a la segunda:

$$\begin{array}{|c|c|c|} \hline & L & I \\ \hline B & R & O \\ \hline S & V & E \\ \hline \end{array} \xrightarrow{\text{OE, P}} (O, E)$$

$$\begin{array}{|c|c|c|} \hline & L & I \\ \hline B & R & E \\ \hline S & V & O \\ \hline \end{array} \xrightarrow{\text{e}} (E, O)$$

- Movimiento válido al multiplicar

-  $(V, X_1) (V, X_{n-1}) \dots (V, X_n)(OE) = e$  por la transposición  $(V, X)$

- n es par porque acaba en el mismo sitio que ha empezado

$$(V, X_1) (V, X_{n-1}) \dots (V, X_n)(OE) \xrightarrow{\text{Pero } n \text{ impar}} e = e$$

como e es par y el producto es impar, entonces el problema no tiene solucion.

$\rightarrow$  ciclos disjuntos

dos ciclos:  $\sigma = (a_0, \dots, a_r)$ ,  $\beta = (b_0, \dots, b_s) \in S_n$ ,

son disjuntos si  $(a_0, \dots, a_r) \cap (b_0, \dots, b_s) = \emptyset$

demo:

$$\sigma = (a_0, \dots, a_r)$$

$$\beta = (b_0, \dots, b_s) \Rightarrow \text{sup: } s_n = \{a_0, \dots, a_r, b_0, \dots, b_s, c_0, \dots, c_t\}$$

$$\underbrace{\{1, \dots, n\}}$$

terminos q  
no estén en  
ninguno de  
los dos

$\rightarrow$  si  $\sigma, \beta \in S_n$  son dos ciclos disjuntos,

entonces:  $\sigma\beta = \beta\sigma \equiv$  los ciclos disjuntos  
comutan

$\square$  Escribir como producto de ciclos disjuntos

$$\beta = (1 \ 2 \ 3 \ 4 \ 8 \ 6 \ 7 \ 9 \ 5 \ 4)$$

$$\beta = (1326)(497)(58)$$

Aplicación de todo esto:

$$\begin{array}{ccccccc} 1 & 2 & 3 & & 1 & 5 & 9 \\ 4 & 5 & 6 & & 2 & 6 & 10 \\ 7 & 8 & 9 & & 3 & 7 & 11 \\ 10 & 11 & 12 & \xrightarrow{\text{ciclos}} & 4 & 8 & 12 \\ & & \text{"se oponen"} & & & & \\ & & \text{(se juntan y}\\ & & \text{las pone en)} & & & & \\ & & \text{"como columnas"} & & & & \end{array} \quad \begin{array}{ccccccc} 1 & 6 & 11 & & 1 & 6 & 11 \\ 5 & 10 & 4 & & 5 & 10 & 4 \\ 9 & 3 & 8 & & 9 & 3 & 8 \\ 2 & 7 & 12 & & 2 & 7 & 12 \end{array}$$

$$\sigma \left( \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 4 & 7 & 10 & 2 & 5 & 8 & 11 & 3 & 6 & 9 & 12 \end{array} \right) \left( \begin{array}{c} \xrightarrow{\text{se convierte}} \\ 2 \end{array} \right)$$

11

$$\frac{(2, 4, 10, 6, 5)}{\alpha} \quad \frac{(3, 7, 8, 11, 9)}{\beta} \quad (\text{prod. de ciclos disjuntos})$$

orden de  $\sigma = 5$ : por tanto:

$$\sigma = \alpha \cdot \beta \quad \text{comutan pq son ciclos disjuntos}$$

$$\sigma^2 = \alpha \beta \alpha \beta = \alpha \alpha \beta \beta = \alpha^2 \beta^2$$

$$\sigma^3 = \alpha^2 \beta^2 \alpha \beta = \alpha^3 \beta^3$$

⋮

$$\sigma^5 = \alpha^5 \beta^5 = \underline{\underline{e}}$$

## > Identidad como producto de transposiciones

La identidad solo puede ser expresada como producto de un no par de transposiciones.

Sea  $e \in S_n$  la permutación identidad y sea  $T_1, \dots, T_r$  transposiciones de  $S_n$  tq.  $e = T_1, T_2, \dots, T_r$ . Entonces  $r \equiv 0 \pmod{2}$

Demo: por inducción sobre  $r$ :

- 1) La identidad no se puede escribir como una transposición pero si como producto d' dos  $(ab)(ab) = e, (ab)^2 = e$ .
- 2) Ave. q el resultado es cierto  $\Leftrightarrow$  producto de un  $n^o$   $s < r$  de transposiciones
- 3) Si  $e = T_1, \dots, T_r \Rightarrow e = T_1, \dots, T_s$ 
  - a)  $r \equiv s \pmod{2}$
  - b)  $s < r$  y a no aparece  $\Rightarrow$  p.ej. el resultado es cierto
  - c)  $s < r$  y a solo aparece en  $T_1 \Rightarrow e(a) = c \neq a$   
 $\Rightarrow e \neq e$  la identidad

## > Paridad de una permutación

Si  $\sigma \in S_n$  se puede expresar como producto de  $r$  transposiciones, y como producto de  $s$  transposiciones, entonces  $r \equiv s \pmod{2}$

Demo:  $\sigma = T_1, \dots, T_r = \alpha_1, \dots, \alpha_s$  transposiciones  $\alpha_i \cdot \alpha_j = e$

$$\Rightarrow T_1, \dots, T_r \alpha_s \alpha_{s-1} \dots \alpha_1 = e \Rightarrow r + s \equiv 0 \pmod{2} \Rightarrow$$

$$\Rightarrow r \equiv s \pmod{2}$$

## > Grupo alternado

$A_n \triangleq \mathbb{Z}$ , sea  $A_n$  el cjs. de todas las permutaciones pares de  $S_n$ , entonces:  $A_n \leq S_n$  y  $|A_n| = \frac{n!}{2}$

El grupo  $(A_n, \circ)$  se denomina grupo alternado.

Demo:  $A_n \neq \emptyset \quad e \in A_n$

$$\sigma, \tau \in A_n \Rightarrow \sigma^{-1} \tau^{-1} \text{ tambien es par} \Rightarrow \sigma^{-1} \tau^{-1} \in A_n$$

## > Reordenación de componentes de transposiciones

Dado un producto de transposiciones  $T_1 \dots T_r$ , existe otro producto de transposiciones  $\sigma_1 \dots \sigma_s$  tales que:

$$\textcircled{1} \quad \sigma_1 \sigma_2 \dots \sigma_s = T_1 T_2 \dots T_r$$

$$\textcircled{2} \quad s \equiv r \pmod{2}$$

\textcircled{3} se verifica una de las dos condiciones siguientes:

•  $s < r$  y la 1<sup>a</sup> componente de  $T_r$  no aparece en ninguna transposición  $\sigma_i$

•  $s < r$  y la 1<sup>a</sup> componente de  $T_r$  solo aparece en  $\sigma_1$

¶ Expressar como producto de no más de 6 transposiciones

$$(12)(53)(34)(56)(51)(31)$$

De manera que  $s$  aparece a lo sumo en la primera de las transposiciones y se conserve la paridad.

$$(12)(53)(34)(56)(51)(31)$$

los cambios  $\overset{\text{100}}{\text{disjuntores}}$  entre  $\sigma_1$  y  $T_r$  se cancelan y el signo

$$(12)(53)(34)(51)(6)(31) = (12)(53)(34)(51)(16)(31) =$$

$$= (12)(53)(51)(34)(16)(31) = (12)(51)(3)(34)(16)(31) =$$

$$= (12)(51)(13)(34)(16)(31) = (521)(13)(34)(16)(31) =$$

$$= (52)(1)(13)(34)(16)(31) \quad \checkmark$$

## ¶ Permutaciones pares e impares

Una permutación <sup>dijo</sup> par o impar según pueda ser expresada como el producto de un n° par o de un n° impar de transposiciones respectivamente.

$$T_1 = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8) \quad \checkmark_1 = (1 \ 7 \ 3 \ 4 \ 5 \ 6 \ 7 \ 2)$$

$$T_1 = (136)(28)(57)$$

$$(13)(36)(28)(84)(45)(57)$$

par

$$T_2 = (13)(36)(62)(78)(64)(45)(57)$$

impar

Lema a) demo que  $\varphi$  es biyectiva:

(ex  $a^m = a^n \Leftrightarrow m = n \Leftrightarrow \varphi(a^m) = \varphi(a^n) \Leftrightarrow \varphi(a^m) = \varphi(a^n)$ )

y bien de (inversa)

por lo tanto  $m = n$ , no divide a,  $n-m$  y  $a^{n-m}$  divide a, por tanto  $n-m=0$

$\varphi(a^m) = \varphi(a^n) \Leftrightarrow a^m = a^n \Leftrightarrow a^{m-n} = 1 \Leftrightarrow a^{m-n} = a^0 \Leftrightarrow m-n = 0$

(ex  $b \in G = \langle a \rangle \Rightarrow b = a^m$  para algún  $m \in \mathbb{Z} \Rightarrow b = \varphi(a^m)$ )

b) Vamos a ver ahora que conserva la operación

$$\varphi(a^{m+n}) = a^{m+n} = a^m \cdot a^n = \varphi(a^m) * \varphi(a^n)$$

Por tanto en isomorfismo (cumple a y b)

demo ②: sea  $(G, *)$  cíclico de orden n  $\Rightarrow G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$

se define  $\varphi: \mathbb{Z}_n \rightarrow G$

$$[r]_n \rightarrow \varphi([r]_n)$$

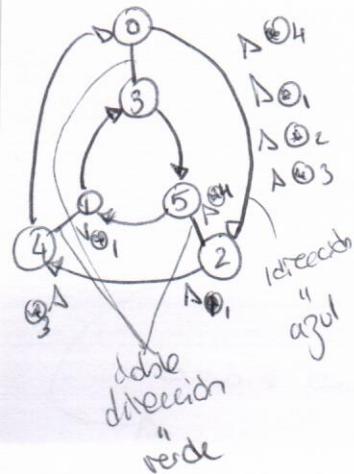
a) demo. que  $\varphi$  es biyectiva:

- $\varphi([r]_n) = \varphi([s]_n) \Leftrightarrow a^r = a^s \Leftrightarrow r \equiv s \pmod{n} \Leftrightarrow [r]_n = [s]_n$
- $\forall b \in G, b = a^r \Rightarrow b = \varphi([r]_n)$

b) demo. que  $\varphi$  conserva la operación

$$\varphi([r]_n + [s]_n) = \varphi([r+s]_n) = a^{r+s} = a^r * a^s = \varphi([r]_n) * \varphi([s]_n)$$

estudiar si el grupo dado por la diagonal de Cayley es isomorfo:



$*_2$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$$\begin{aligned} AAV &= 1 & \textcircled{1}, \\ A &= 2 & \textcircled{2}, \\ AA &= 4 & \textcircled{3}, \\ AV &= 5 & \textcircled{4} \end{aligned}$$

1.4

## Isomorfismos en grupos

Dos grupos  $(G, *)$  y  $(G', *)'$  son isomorfos, y se escribe  $G \cong G'$ , si existe una aplicación biyectiva  $\phi: G \rightarrow G'$  para todos  $x, y$  se verifica que  $\phi(x * y) = \phi(x) *' \phi(y)$

La aplicación  $\phi$  se llama isomorfismo de grupos

1)

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	6	5	4	3
3	3	4	5	6	1	2
4	4	3	2	1	6	5
5	5	6	1	2	3	4
6	6	5	4	3	2	1

Re-escribir la tabla, cambiando el orden de los elementos, y comparar la tabla obtenida con la tabla del grupo  $(\mathbb{Z}_3, +)$

*	e	r	r <sup>2</sup>	s	r s	r <sup>2</sup> s
e	e	r	r <sup>2</sup>	s	r s	r <sup>2</sup> s
r	r	r <sup>2</sup>	e	r s	r <sup>2</sup> s	s
r <sup>2</sup>	r <sup>2</sup>	e	r	r <sup>2</sup> s	s	r s
s	s	r s	r <sup>2</sup> s	e	r <sup>2</sup> r	r
r s	r s	r <sup>2</sup> s	s	r	e	r <sup>2</sup>
r <sup>2</sup> s	r <sup>2</sup> s	s	r s	r <sup>2</sup>	r	e

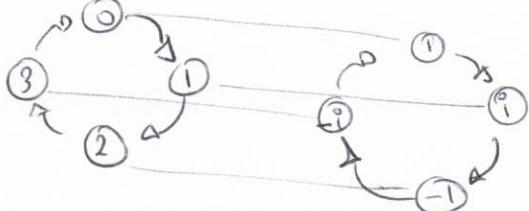
Nueva  
tabla  
(icosahedro)  
→

*	1	3	5	2	4	6
1	1	3	5	2	4	6
3	3	5	1	4	6	2
5	5	1	3	6	2	4
2	2	6	4	1	5	3
4	4	2	6	3	1	5
6	6	4	2	5	3	1

modific:  $\begin{array}{l} e \rightarrow 1 \\ r \rightarrow 3 \\ r^2 \rightarrow 5 \\ s \rightarrow 2 \\ rs \rightarrow 4 \\ r^2s \rightarrow 6 \end{array}$

(Q, 0)  
↑D

2)



&gt; Isomorfismo en grupos cíclicos

- ① Todo grupo cíclico  $(G, *)$  de orden infinito, es isomorfo a  $(\mathbb{Z}, +)$
- ② Todo grupo cíclico  $(G, *)$  de orden  $n$ , es isomorfo a  $(\mathbb{Z}, +_n)$

demo ①: sea  $(G, *)$  cíclico de orden  $n \Rightarrow G = \langle a \rangle = \{a^n; n \in \mathbb{Z}\}$

se define  $\varphi: \mathbb{Z} \rightarrow G$   
 $n \rightarrow \varphi(n) = a^n$

¿ $\varphi$  es isomorfismo de grupos?

1 cont. →

$$\frac{mn}{\text{mcd}(m,n)} (a,b) = (0,0) \Rightarrow \text{mcd}(m,n) = 1$$

↑  
 $|(a,b)| = mn$

L  $\Leftrightarrow$  imp. que  $\text{mcd}(m,n)=1$   
 ¿ $\mathbb{Z}_m + \mathbb{Z}_n$  euclídeo?

$$([1]_m, [1]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n \quad (\text{divide})$$

$$|(1,1)| = \text{mcm}([1]_m, [1]_n) = m(m|m,n)$$

Q) Estudiar si los isomorfismos

$$(\mathbb{Z}_4 \times \mathbb{Z}_2, +_4 \times +_2) \rightarrow U_{15} = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}$$

$t_4 x + 2$	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)	
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)	→ 1
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)	(3,1)	(3,0)	→ 2
(1,0)	(1,0)	(1,1)	(2,0)	(2,1)	(2,0)	(3,1)	(0,0)	(0,1)	→ 4
(1,1)	(1,1)	(1,0)	(2,1)	(2,0)	(3,1)	(3,0)	(0,1)	(0,0)	→ 4
(2,0)	(2,0)	(2,1)	(3,0)	(3,1)	(0,0)	(0,1)	(1,0)	(1,1)	→ 2
(2,1)	(2,1)	(2,0)	(3,1)	(3,0)	(0,1)	(0,0)	(1,1)	(1,0)	→ 2
(3,0)	(3,0)	(3,1)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	→ 4
(3,1)	(3,1)	(3,0)	(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)	→ 4

$^o_{15}$	1	2	4	7	8	11	13	14	
1	1	2	4	7	8	11	13	14	$ 1 =1$
2	2	4	8	4	1	7	11	13	$ 2 =4$
4	4	8	1	13	2	14	7	11	$ 4 =2$
7	7	14	13	4	11	2	1	8	$ 7 =4$
8	8	1	2	11	4	12	14	7	$ 8 =4$
11	11	7	14	2	13	1	8	4	$ 11 =2$
13	13	11	7	1	14	8	4	2	$ 13 =4$
14	14	13	11	8	7	4	2	1	$ 14 =2$

$$\begin{aligned} H &= \{1, 2, 4, 8\} = \langle 2 \rangle \\ K &= \{1, 11\} = \langle 11 \rangle \\ U_{15} &\cong H \times K \end{aligned}$$

Q) Escribir como producto directo interno

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12} \quad | \quad \mathbb{Z}_2 \times \mathbb{Z}_6 \not\cong \mathbb{Z}_{12}$$

cont.

(aqui empiezan aps. Alicia)

■ Estudiar si son isomorfos

$$(\mathbb{Z}_2, +) \text{ y } (\mathbb{Z}_3, +)$$

$$\begin{aligned} 2\mathbb{Z} &= \langle 2 \rangle = \{2n : n \in \mathbb{Z}\} \\ 3\mathbb{Z} &= \langle 3 \rangle = \{3n : n \in \mathbb{Z}\} \end{aligned} \quad \begin{array}{l} \text{tienen orden infinito} \\ \Rightarrow \text{no son isomorfos} \end{array}$$

$$\Rightarrow \begin{cases} 3\mathbb{Z} \cong (\mathbb{Z}_3, +) \\ 2\mathbb{Z} \cong (\mathbb{Z}_2, +) \end{cases} \quad \{ (\mathbb{Z}_2, +) \cong (\mathbb{Z}_3, +)$$

son isomorfos  
a  $(\mathbb{Z}_2, +)$

juechicht! solo se ve

■ Estudiar si es isomorfismo a algún grupo aditivo

$$(U_{18}, -)$$
 no se si es o no

-	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

$$\begin{array}{lll} |1|=1 & |17|=3 & |13|=3 \\ |5|=6 & |11|=6 & |1|=2 \end{array}$$

$$U_{18} \cong \mathbb{Z}_6$$

$$|U_6| = \frac{6}{\text{mcd}(6, u)} \quad \begin{array}{l} 6 \text{ dñ mcd}(6, u)=1 \\ \text{dñ } u \in \{5, 1\} \text{ en } (\mathbb{Z}_6, +) \end{array}$$

$$\text{en } \mathbb{Z}_6: \quad |0|=1 \quad |2|=3 \quad |3|=2 \\ |4|=3 \quad |5|=6 \quad |1|=6$$

> Productos de grupos aditivos

El grupo  $(\mathbb{Z}_m \times \mathbb{Z}_n, +_m \times +_n)$  es isomorfo a  $(\mathbb{Z}_{mn}, +_{mn})$  si y solo si  $\text{mcd}(m, n)=1$ .

demo:

$\Rightarrow$  Supongamos que  $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$  (es decir  $\mathbb{Z}_m \times \mathbb{Z}_n$  es cíclico)

¿  $\Rightarrow \text{mcd}(m, n)=1$  ?

sea  $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$  con  $|(a, b)| = mn$

$$\begin{aligned} m \cdot a &= 0 \text{ en } \mathbb{Z}_m \\ n \cdot b &= 0 \text{ en } \mathbb{Z}_n \end{aligned}$$

$$|a| = \frac{m}{\text{mcd}(a, m)}$$

$$m = |a| \cdot \text{mcd}(a, m)$$

$$\Rightarrow |b| = \frac{n}{\text{mcd}(b, n)} \Rightarrow n = |b| \cdot \text{mcd}(b, n)$$

El orden de  $a$  es el min. entero no negativo tq  $a + \dots + a = e$ ,

$$a + a + \dots + a = 0 \Rightarrow r \cdot a = 0$$

$$|a| * a = 0 \Rightarrow ma = 0$$

$$|b| * b = 0 \Rightarrow nb = 0$$

## Tema 2

**2.1** (continuar, dividido en 42 secciones)

(3) - Teorema de Lagrange (importante) (demo + b)

1º ( $G, \cdot$ ) es un grupo finito y  $H \leq G$  entonces  $|H|$  es un divisor de  $|G|$  y se verifica que:

$$\frac{|G|}{|H|} = [G : H]$$

(1) - Relación de equivalencia determinada por un subgrupo

sea  $(G, \cdot)$  un grupo y  $H$  un subgrupo de  $G$ . La relación  $a \sim_H b \Leftrightarrow a^{-1} * b \in H$  es una relación de equivalencia en  $G$ .

La clase de equivalencia de un elemento  $a \in G$  se denomina clase lateral izquierda, y se define:  $[a]_H = aH = \{a * h : h \in H\}$

demo: relación de equivalencia módulo  $H$

①  $\sim_H$  es reflexiva

$\forall a \in G$  se verifica que  $a^{-1} * a = e_G \in H \rightarrow a \sim_H a$

②  $\sim_H$  es simétrica

$\forall a, b \in G$  todo  $a \sim_H b \Rightarrow a^{-1} * b \in H \Rightarrow (a^{-1} * b)^{-1} \in H \Rightarrow b^{-1} * a \in H \Rightarrow b \sim_H a$

③  $\sim_H$  es transitiva

$\forall a, b, c \in G$  tales que  $\begin{matrix} a \sim_H b \\ b \sim_H c \end{matrix} \Rightarrow \begin{matrix} a^{-1} * b \in H \\ b^{-1} * c \in H \end{matrix} \Rightarrow (a^{-1} * b)(b^{-1} * c) \in H \Rightarrow a^{-1} * c \in H \Rightarrow a \sim_H c$

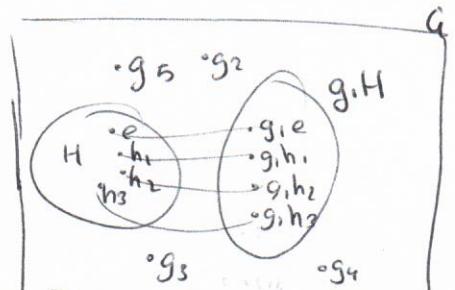
(2) - Índice de un grupo sobre un subgrupo

sea  $H$  un subgrupo de  $(G, \cdot)$ , se llama índice de  $G$  sobre  $H$  al nº de clases laterales izquierdas de  $H$  en  $G$  y se nota por  $[G : H]$ .

nº de clases de equivalencia

- clases laterales izquierdas ej:

$$\begin{aligned} [a]_H &= \{b \in G : a \sim_H b\} = \{b \in G : a^{-1} * b \in H\} = \\ &= \{b \in G : a^{-1} * b = h \in H\} \quad \{b \in G : b = a * h \text{ para } h \in H\} = \\ &= \{a * h : h \in H\} = aH \end{aligned}$$



$$H = \{e, h_1, \dots, h_m\}$$

$$g_1H = \{g_1, g_1h_1, \dots, g_1h_m\}$$

$$aH = \{a, ah_1, \dots, ah_m\}$$

cont.

$$\mathbb{Z}_{12} \cong H \times K$$

$$\textcircled{1} \quad H \cap K = \{(0,0)\}$$

$$\textcircled{2} \quad \underbrace{(h_1, m)}_{\in H} + \underbrace{(k_1, k_2)}_{\in K} = (k_1, k_2) + (h_1, m_2)$$

$$H = \{(0,0), (1,0), (2,0)\}$$

$$K = \{(0,0), (0,1), (0,2), (0,3)\}$$

$$\mathbb{Z}_{12} \cong H \times K$$

2) Construir un isomorfismo con un grupo de simetrías

$$(G, *)$$

$\cdot 12$	1	5	7	11
1	1	5	7	11
5	5	1	11	2
7	7	11	1	5
11	11	7	5	1

$$(U_{12}, \cdot')$$

$S_{U_{12}}$	$T_1$	$T_5$	$T_7$	$T_{11}$
$T_1$	$T_1$	$T_5$	$T_7$	$T_{11}$
$T_5$	$T_5$	$T_1$		
$T_7$	$T_2$			
$T_{11}$	$T_{11}$			

$$S_G = \left\{ \begin{array}{l} e \\ T_1 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 2 \end{pmatrix}, \\ T_5 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{pmatrix}, T_7 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{pmatrix}, \\ (1,5)(7,11) \quad T_{11} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{pmatrix} \end{array} \right\} \begin{array}{l} (1,7)(5,11) \\ (1,11)(5,7) \end{array}$$

> Teorema de Cayley:

Todo grupo de orden  $n \in \mathbb{N}$  es isomorfo a un grupo de permutaciones

dem: Dado  $g \in (G, *)$  grupo  $S_n = \langle \sigma \leq S_n : \sigma_j(k) = j \Leftrightarrow g * k = j \rangle$   
 si  $|G| = n$

- dem. teorema de Lagrange:

demos que todos los claves de equivalencia tienen el mismo n<sup>o</sup> de elementos, para demostrar el t. de Lagrange:

① Veamos que  $\forall a \in G \quad |H| = |\alpha H|$

Definimos  $\varphi : H \rightarrow \alpha H$   
 $h \mapsto \varphi(h) = ah$

a)  $\varphi$  es app. y es biyectiva:

$$\varphi(h) = \varphi(k) \Leftrightarrow ah = ak \Leftrightarrow h = k$$

b)  $\varphi$  es suryectiva:  $\forall b \in \alpha H$ , sea  $g = a^{-1}b \Rightarrow \varphi(g) = \varphi(a^{-1}b) = a(a^{-1}b) = b$

$$\varphi(h) = ah$$

$$\varphi(\frac{a^{-1}b}{h}) = a(\frac{a^{-1}b}{h})$$

$$\Rightarrow |G| = \sum_{a_i \in \{a_1, \dots, a_n\}} |\alpha H| = |G:H| |H|$$

2.2. (ver observaciones en la hora)

- Subgrupos normales

sea  $(G, *)$  un grupo y  $N \subseteq G$ . El subgrupo  $N \subseteq G$  se dice que es normal en  $G$  si para todo  $a \in G$  se verifica:

$$aN = \{a * h : h \in N\} = [a]_N = \{h * a : h \in N\} = Na$$

se escribe:  $N \trianglelefteq G$

↑  
clase lateral  
derecha

Estudiar si  $H$  es un subgrupo normal de  $G$

$$a = \{1, -1, i, -i, j, -j, k, -k\} \quad H = \{1, -1\}$$

$$|H| = \{1, -1\} = -1H$$

$$iH = \{i, -i\} = -iH$$

$$jH = \{j, -j\} = -jH$$

$$kH = \{k, -k\} = -kH$$

aquí el índice es 1

h.k clases laterales  
para G sobre H

$$H1 = \{1, -1\} = H \cdot -1$$

$$Hi = \{i, -i\} = H \cdot -i$$

$$Hj = \{j, -j\} = H \cdot -j$$

$$HK = \{k, -k\} = H \cdot -k$$

subgrupo  
normal



■ Obtener las claves laterales de  $H$  en  $Q$

$$(Q, \cdot) = (\mathbb{Z}_6, +_6) \quad , \quad H = \langle 2 \rangle$$

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$$H = \langle 2 \rangle = \{0, 2, 4\} \text{ (en } \mathbb{Z}_6)$$

clase de  
equivalencia  
del 0.  
neutral

$$[0]_H = 0H = \{0 +_6 H\} = H = \{0, 2, 4\}$$

$$[1]_H = 1H = \{1 +_6 H\} = \{1, 3, 5\} \quad [= \{0+1, 2+1, 4+1\}]$$

$$[2]_H = 2H = \{2, 4, 0\}$$

$$[3]_H = 3H = \{3, 5, 1\}$$

$$[4]_H = 4H = \{4, 0, 2\}$$

$$[5]_H = 5H = \{5, 1, 3\}$$

■ Obtener las claves laterales de  $H$  en  $Q$

$$(Q, \cdot) = (\mathbb{Z}_{12}, +_{12}) \quad H = 3$$

$$\mathbb{Z}_{12} = \{0, \dots, 26\}$$

$$H = \{0, 3, 6, 9, 12, 15, 18, 21, 24\}$$

se hace igual que el anterior

■ Calcular claves laterales de  $H$  en  $Q$

$$(Q, \cdot) = (\mathbb{D}_3, \circ) \quad H = \langle f \rangle$$

$$\mathbb{D}_3 = \{e, r, r^2, f, rf, r^2f\}$$

$$H = \{e, f\}$$

$$[e]_H = \{e\}$$

$$[r]_H = \{e, r\}$$

$$[r^2]_H = \{r^2, r^4\}$$

$$[f]_H = \{f, e\}$$

$$[rf]_H = \{rf, r\}$$

$$[r^2f]_H = \{r^2f, r^4\}$$

■ Obtener el grupo cociente  $G/H$

$$(G, \Delta) = (2, +) \quad , \quad H = 672 \quad , \quad H = \{6k, k \in \mathbb{Z}\}$$

- ① Clauer lateraler
  - ②  $G/H = \{aH : a \in G\}$
  - ③  $(G/H, \cdot_H)$

$$\begin{aligned} ① \quad 0H &= \{6u, u \in \mathbb{Z}\} \\ 1H &= \{1+6u, u \in \mathbb{Z}\} \\ 2H &= \{2+6u, u \in \mathbb{Z}\} \\ 3H &= \{3+6u, u \in \mathbb{Z}\} \\ 4H &= \{4+6u, u \in \mathbb{Z}\} \\ 5H &= \{5+6u, u \in \mathbb{Z}\} \end{aligned}$$

$$\textcircled{2} \quad G_H = \{ [0]_H, [1]_H, [2]_H, [3]_H, [4]_H, [5]_H \} \approx 72$$

## Y la operación:

una clase opera de cerca  
otra clase, en la clase  
de la operación de los  
representantes?

$$[2]_H \bowtie [4]_H = [2+4]_H = [6]_H =$$

$$\textcircled{3} \quad (\gamma_{L_6}, +_6) = G/H$$

$$c_{\alpha} \text{ (1)} = \underline{\underline{[0]}}_H$$

para la operación  
 $a_N +_N b_N = (a+b)_N$   
 de  $+_G$  (lo que se acaba  
 para q esto sea así)

Teorema de Cayley:  $c(x) \in \mathbb{R}$  implica  
pero si  $c(x)$  faltan  $\rightarrow$  Notas

## 2.1 (cont, uJin)

- Corolarios del teorema de Lagrange

① Si  $(G, \cdot)$  es un grupo finito de orden primo, entonces  $G$  es cíclico.

demo:  $|G| = p$  primo sao a CG tq a  $\neq e_G$

$$|a| = |\langle a \rangle|_p \Rightarrow |a| \in \langle 1, p \rangle \Rightarrow |a| = p \Rightarrow \langle a \rangle = G \Rightarrow G$$

es  
cyclic

② Si  $(G, *)$  es un grupo finito con  $|G|=n$  entonces  $\forall a \in G$ ,  $a^n = e$ .

demo:  $|G| = n \Rightarrow \forall a \in G \quad a^n = e_G$

$$|a| = |\langle a \rangle| = h \Rightarrow h/n \Rightarrow n < q_1 \Rightarrow a^n = (a^h)^q \stackrel{?}{=} e_a^{q^2} = e_q$$

$(a) = h$

③ Si  $H$  y  $K$  son subgrupos de  $(G, \cdot)$  tales que  $K \trianglelefteq H$ , entonces  $|H| = h$

$$[G : K] = [G : H][H : K]$$

En el ejemplo anterior de  $c$  y  $f$ :  $f(x) = H(x)$ ?

$$Hr = \{ e+r, \underbrace{\} + r}_\text{esta es pergo} \} = \{ r, r^2 \} \neq \{ r, r^3 \} = rH$$

no es subgroup normal X

$Dn = \{ g \cdot s : |g|=n, |s|=2, \underline{sg=g^{-1}s} \}$

$\Downarrow \quad g \cdot r = r^l \}$

$4 \in D_3 : r^l = r^2 \text{ pq } r \cdot r^2 = e$

- Teorema del grupo (det) cociente

Sea  $(G, *)$  un grupo y  $N \trianglelefteq G$ . Entonces si en el conjunto de las clases laterales de  $N$  en  $G$ :  $G/N = \{gN : g \in G\}$  se define la operación  $aN *_N bN = (a * b)N$ , se verifica que:

$(G/N, \cdot_N)$  es un grupo de orden  $|G/N| = |G:N|$

Dicho grupo recibe el nombre de grupo caliente de q sobre N.

demo: ① La operación está bien definida.

$$aN = a'N \quad \text{and} \quad bN = b'N \quad \Rightarrow \quad (a+b)N = (a'+b')N$$

$$\text{ii) } \begin{cases} aN = a'N \\ bN = b'N \end{cases} \Rightarrow a = a'n \quad n \in N \quad \begin{cases} \Rightarrow b = b'm \quad m \in N \end{cases} \Rightarrow a+b = (a'n) + (b'm) = a' (n+b)m$$

$$\text{como } N \trianglelefteq G \Rightarrow b'N = Nb' \Rightarrow nb' \in Nb' = b'N \Rightarrow nb' = b'n' \in BN \Rightarrow$$

$$\Rightarrow ab = a'(nb')m = (a'b')(n'm) \in \underline{(a'b')N}$$

$$\Rightarrow \boxed{\underline{abN = a'b'N}} \quad \text{clase} \quad \text{classe}$$

② El ej. anterior, c/d N, con los op. productos módulo N,  $*_N$ , el grupo:

a) asociativa

$(\alpha_{(N)}, \beta_N)$  ergnjo

$$(aN) \star_N (bN \star_N cN) = aN \star_N (b \star c)N = (a \star (b \star c))N = \\ = ((a \star b) \star c)N = (aN \star_N bN) \star_N cN \checkmark$$

b) here e. neutro

$$eN \cdot \star_N aN = (e \star a) N = aN \quad \checkmark$$

c) todo elemento tiene inverso

$\forall a \in G/N \quad a \in G \rightarrow \exists a' \in G$

$$aN *_N \bar{a}'N = (a * \bar{a}')N = eN$$

clare del  
elem neutro

" $\text{I} \Rightarrow \text{II}$ "  $aNa^{-1} \subseteq N \forall a \in G$  d'  $aNa^{-1} = N \forall a \in G$ ?

$\exists aNa^{-1} \subseteq N \forall a \in G$ ?  $a \in G \Rightarrow \exists n \in aNa^{-1}$ ?

$$\begin{aligned} a^{-1} = b \in G &\Rightarrow bNb^{-1} \subseteq N \Rightarrow bNb^{-1} = N \in N \Rightarrow \\ \Rightarrow n = b^{-1}n'b &= an'a^{-1} \in aNa^{-1} \end{aligned}$$

" $\text{II} \Rightarrow \text{I}$ "  $aNa^{-1} = N \forall a \in G$  d'  $aN = Na \forall a \in G$ ?

" $c$ " d'  $aN = Na \forall a \in G$ ?  $a \in G, n \in N$  d'  $na \in aN$ ?

$$ana^{-1} = n \in N \Rightarrow an = n'a \in Na$$

" $\text{II}$ " d'  $Na \subseteq aN$ ?  $a \in G, n \in N$  d'  $na \in aN$ ?

$$\begin{aligned} b = a^{-1} \in G &\Rightarrow bNb^{-1} = N, bnb^{-1} = n \in N \Rightarrow a^{-1}na = n \in N \Rightarrow \\ \Rightarrow na &= an' \in aN \end{aligned}$$

■ Estudiar si  $H$  es un grupo normal de  $G$

$$(G, *) = (\mathbb{Z}_3, +_3) ; H = \{0, 2, 4, 6\} \quad \mathbb{Z}_3 = \{0, 1, 2\}$$

$$0H = \{0, 2, 4, 6\}$$

$$1H = \{1, 3, 5, 7\}$$

$$0H +_3 H = (0 +_3 0)H$$

$$0H +_3 1H = (0 +_3 1)H$$

$$1H +_3 1H = (1 +_3 1)H = 2H = 0H$$

$+_3 H$	$0H$	$1H$
$0H$	$0H$	$1H$
$1H$	$1H$	$0H$

- Todo subgrupo con índice 2 es normal

si  $(G, *)$  es un grupo finito y  $H \leq G$  tq  $[G:H]=2$ , entonces  $H \trianglelefteq G$ .

DUDA!:  $\{0\}$  no es normal en  $\mathbb{Z}_3$  pq  $2 \in \mathbb{Z}_3$ .

■ Estudiar si  $H$  es un subgrupo normal de  $\mathbb{D}_5$

$$(\mathbb{D}_5, \circ) = \{r, s, |r|=5, |s|=2, sr=r^4s\}$$

$$H = \langle r \rangle = \{e, r, r^2, r^3, r^4\}$$

$$\mathbb{D}_5 = \{e, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$$

cont.

### - Teorema de Fermat

Si  $p \in \mathbb{N}$  es primo y  $a \not\equiv 0 \pmod p$ , entonces  $a^{p-1} \equiv 1 \pmod p$

demo:  $\Psi_p = \{r \in \{1, \dots, p\} : \gcd(r, p) = 1\} \Rightarrow |\Psi_p| = p-1$

$$(\Psi_p, p) \Rightarrow \forall a \in \Psi_p \quad a^{p-1} \equiv 1$$

### - Teorema de Euler

Si  $\gcd(a, m) = 1$  y  $\varphi$  es la función de Euler, entonces  $a^{\varphi(m)} \equiv 1 \pmod m$

$$\varphi(m) = m \prod_{\substack{p \in \mathbb{N} \\ \text{divisor primo} \\ \text{de } m}} \left(1 - \frac{1}{p}\right)$$

demo:  $\Psi_m = \{r \in \{1, \dots, m\} : \gcd(r, m) = 1\}$

$$\varphi(m) = |\Psi_m|$$

$$(\Psi_m, m) \Rightarrow \forall a \in \Psi_m \quad a^{\varphi(m)} \equiv 1$$

### - Teorema de Cauchy

sea  $(G, *)$  un grupo de orden  $n \in \mathbb{N}$ . Si  $p \in \mathbb{N}$  es un divisor primo de  $n \Rightarrow$  existe  $a \in G$  tal que  $|a|_p = p$ .

## 12.2 (cont, fin)

### - Caracterización de los subgrupos normales

sea  $(G, *)$  un grupo y  $N \subseteq G$ . Las siguientes proposiciones son equivalentes:

- i)  $aN = Na \quad \forall a \in G$
- ii)  $aNa^{-1} \subseteq N \quad \forall a \in G$
- iii)  $aNa^{-1} = N \quad \forall a \in G$

"i  $\Rightarrow$  ii": hipótesis:  $aN = Na \quad \forall a \in G$

•  $aNa^{-1} \subseteq N \quad \forall a \in G$ ?

sea  $a \in G, n \in N$ .  $\exists a \bar{a} \in G$

$$an \in aN = Na \Rightarrow an = n'a \quad \begin{cases} \uparrow \\ \text{hip.} \end{cases} \quad \begin{cases} \text{n' } \in N \\ \end{cases} \Rightarrow a\bar{a} = n' \in N$$

12.3

## > Homomorfismos de grupos

Una opp  $\varphi: G \rightarrow G'$  entre los grupos  $(G, *)$  y  $(G', \circ)$  es un homomorfismo de grupos si para todos  $a, b \in G$  se verifica:

$$\varphi(a * b) = \varphi(a) \circ \varphi(b)$$

## > Núcleo de un homomorfismo

Si  $\varphi: G \rightarrow G'$  es un homomorfismo de grupos, núcleo de  $\varphi$ :

$$\begin{aligned} \vartheta(1_G) &= \vartheta(1) \circ \vartheta(1) \\ \vartheta(-1) &= \vartheta(1) \circ \vartheta(2) \\ &\text{etc} \end{aligned}$$

$$\text{Ker}(\varphi) = \{a \in G : \varphi(a) = e_{G'}\} = \varphi^{-1}(\{e_{G'}\})$$

## > Imagen de un homomorfismo

$$\varphi(G) = \{\varphi(a) : a \in G\} \quad \begin{array}{l} \text{(toda lo} \\ \text{dicho transformado} \\ \text{por la aplicación)} \end{array}$$

(Todos los elem  
que se transforman  
en el e. neutro')



## > Propiedades

Sean  $(G, *)$  y  $(G', \circ)$  grupos y  $\varphi: G \rightarrow G'$  homomorfismo. Se tiene:

Imagen del e. neutro de  $G$  = e. neutro  $G'$  ( $G$  grupo inicial,  $G'$  grupo de la transformación o tránsf. o op.)

①  $\varphi(e_G) = e_{G'}$  siendo  $e_G \in G$  y  $e_{G'} \in G'$  los e. neutros de  $(G, *)$  y  $(G', \circ)$

demo: si  $a = \varphi(e_G) \Rightarrow a = \varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G) \circ \varphi(e_G) = a \circ a \Rightarrow a = a \cdot a \Rightarrow a = e_{G'}$

②  $\varphi(a^{-1}) = \varphi(a)^{-1} \forall a \in G$

demo:  $e_{G'} = \varphi(e_G) = \varphi(a^{-1} * a) = \varphi(a^{-1}) \circ \varphi(a) \Rightarrow \varphi(a^{-1}) \circ \varphi(a) = e_{G'} \Rightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$

caracte-  
rización  
de los  
május-  
nos

{ ③  $\varphi$  es inyectivo  $\Leftrightarrow \text{Ker}(\varphi) = \{e_G\}$

demo: " $\Rightarrow$ " si  $\varphi$  es inyectiva  $\rightarrow \text{Ker}(\varphi) = \{e_G\}$ ? : sea  $a, b \in G$  y  $\varphi(a) = \varphi(b)$   
 $\varphi(a) = e_{G'} \Rightarrow a = e_G \Rightarrow \varphi$  es inyectiva //

" $\Leftarrow$ "  $\text{Ker}(\varphi) = \{e_G\} \rightarrow \varphi$  inyectiva? : sea  $a, b \in G$  tg  $\varphi(a) = \varphi(b)$   
 $\varphi(a) = \varphi(b) \Rightarrow a = b$  cont.

cont.

$$|D_5|=10$$

$$|H|=5$$

$$[D_5 : H] = \frac{10}{5} = 2 \Rightarrow H \trianglelefteq D_5$$

Grupo cociente:

$$eH = \{e, r, r^2, r^3, r^4\}$$

$$sH = \{s, r^4s, r^2s, r^3s, rs\}$$

$$D_5/H = \{eH, sH\} \leftarrow \text{DUOA!} \rightarrow$$

$$eH \circ_H eH = (e \circ e)H = eH$$

$$eH \circ_H sH = (e \circ s)H = sH$$

$$sH \circ_H eH = (s \circ e)H = sH$$

$$sH \circ_H sH = (s \circ s)H = eH$$

DH	eH	sH
eH	eH	sH
sH	sH	eH

how & why

- Los subgrupos únicos en un orden son normales

si  $(G, *)$  es un grupo finito y  $H \leq G$  es el único grupo de  $G$  cuyo orden es  $|H|$ , entonces  $H \trianglelefteq G$ .

Estudiar si  $A_3$  es un subgrupo normal de  $S_3$ .

$$(S_3, \circ) \quad A_3 = \{(1), (1, 2, 3), (1, 3, 2)\}$$

$$S_3 = \{p_0 = (1), p_1 = (1, 2, 3), p_2 = (1, 3, 2), \mu_1 = (2, 3), \mu_2 = (1, 3), \mu_3 = (1, 2)\}$$

- Tiene índice 2  $[S_3 : A_3] = \frac{6}{3} = \frac{|S_3|}{|A_3|} = 2$

- El grupo cociente tiene orden 2  
por tanto es  $\mathbb{Z}_2$

- Los subgrupos de un grupo abeliano son normales

si  $(G, *)$  es un grupo abeliano y  $H \leq G$ , entonces  $H \trianglelefteq G$ .

- Grupos simples

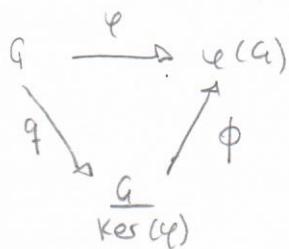
Un grupo  $(G, *)$  se dice que es simple si no tiene subgrupos normales propios ni triviales (equivalente al n° primo)

Propiedad:  $\text{im } \varphi = \text{Zn}$  // todo elem de  $\text{Zn}$  tiene un elemento de  $\text{ZL}$  cuya imagen está en  $\text{Zn}$   
 (por  $f$ )  
 // (suficiente)

## > Primer teorema de Isomorfía

sea  $\varphi: G \rightarrow G'$  un homomorfismo de grupos, entonces:

$$G / \text{Ker } \varphi \cong \varphi(G) = \text{im } \varphi$$



"El nuclo mide de alguna manera lo parecido que son el grupo inicial y el grupo final"

$$\text{demo: } \phi: \frac{G}{\text{Ker } \varphi} \rightarrow \varphi(G)$$

$$\phi(g \text{Ker } \varphi) = \varphi(g)$$

$$\text{hip: } g \text{Ker } \varphi = h \text{Ker } \varphi \Leftrightarrow$$

$$\Leftrightarrow g^{-1}h \in \text{Ker } \varphi \Leftrightarrow \varphi(g^{-1}h) = e_{G'} \Leftrightarrow \varphi(g)^{-1}\varphi(h) = e_{G'} \Leftrightarrow \varphi(g) = \varphi(h)$$

$$\Leftrightarrow \phi(g \text{Ker } \varphi) = \phi(h \text{Ker } \varphi) \Rightarrow \phi \text{ es biyeccin y es inyectiva.}$$

Tambien es suryectiva:  $\forall b \in \varphi(G) \Rightarrow \exists a \in G \text{ tq } b = \varphi(a)$

$$\Rightarrow b = \phi(a \text{Ker } \varphi) \quad \checkmark$$

es homomorfismo de grupos + b? Tendrá que conservar la operación:

$$\begin{aligned} \phi(a \text{Ker } \varphi) \phi(b \text{Ker } \varphi) &= \varphi(a) \varphi(b) = \varphi(a * b) = \\ &= \phi(a * b) \text{Ker } \varphi \quad \checkmark \end{aligned}$$

## ■ Calcular el núcleo y la imagen

$$f: (\mathbb{S}_n, \circ) \rightarrow \{(1, -1)\}$$

$$\begin{aligned} \text{pos: } f(\alpha) &= 1 && \text{si } \alpha \text{ par} \\ f(\alpha) &= -1 && \text{si } \alpha \text{ impar} \end{aligned}$$

Establecer el isomorfismo dado por el primer teorema de isomorfismo.

$$\text{Ker } f = \{\sigma \in \mathbb{S}_n : \sigma \text{ es par}\} = A_n$$

$$\text{Im } f = \{1, -1\}$$

$$\frac{\mathbb{S}_n}{A_n} = \{eA_n, (1, 2)A_n\} \xrightarrow{d} \{1, -1\} = \text{Imagen}$$

(sabíamos que su orden es 2 [ver teoría grupo caro])

$$\begin{array}{ccc} (\text{permuto } \sigma) & \xrightarrow{eA_n} 1 & \\ (\text{permuto } \sigma) & \xrightarrow{(1, 2)A_n} -1 & \end{array}$$

por tanto

$$\sigma \in A_n \Leftrightarrow d(\sigma) = 1 \in \text{Im } f$$

carac-  
teriza -  
cion de  
isomorfis-  
mos

(1)  $\varphi$  es suprayectivo  $\Leftrightarrow \varphi(G_e) = G'$

Demo (3)  
 $\varphi(a) \cdot \varphi(b)^{-1} = e_{G'}$   $\Rightarrow \varphi(ab^{-1}) = e_{G'}$   
 $\Rightarrow ab^{-1} \in \text{Ker } \varphi \Rightarrow ab^{-1} = e_G$   
 $\Rightarrow a = b$

Subgrupo n\'ucleo y subgrupo imagen

Si  $\varphi : G \rightarrow G'$  es un homomorfismo de grupos entonces:

- ①  $\text{Ker } \varphi \trianglelefteq G$  (subgrupo normal)
- ②  $\varphi(G) \leq G'$  (subgrupo)

Demo ①

a)  $\text{Ker } \varphi \neq \emptyset$   $\varphi(e_G) = e_{G'} \Rightarrow e_G \in \text{Ker } \varphi$

b)  $\forall a, b \in \text{Ker } \varphi \quad \exists ab^{-1} \in \text{Ker } \varphi?$   
 $\varphi(ab^{-1}) = \varphi(a) \cdot \varphi(b)^{-1} = e_{G'} \cdot e_{G'}^{-1} = e_{G'} \Rightarrow ab^{-1} \in \text{Ker } \varphi$

c)  $\text{Ker } \varphi \trianglelefteq G$   $\forall a \in G \quad \forall h \in \text{Ker } \varphi \quad \exists ah^{-1} \in \text{Ker } \varphi?$

$\Rightarrow \exists a \in \text{Ker } \varphi \quad a^{-1} \in \text{Ker } \varphi?$

$$\varphi(ah^{-1}) = \varphi(a) \cdot \varphi(h) \cdot \varphi(a)^{-1} \stackrel{h \in \text{Ker } \varphi}{=} \varphi(a) \cdot e_{G'} \cdot \varphi(a)^{-1} = \varphi(a) \cdot \varphi(a)^{-1} = e_{G'} \quad \text{subgrupo normal}$$

$\Rightarrow ah^{-1} \in \text{Ker } \varphi$

Demo ②

a)  $\text{im}(\varphi) \neq \emptyset$   $\varphi(e_G) = e_{G'} \Rightarrow e_{G'} \in \text{im } \varphi$

b)  $a', b' \in \text{im } \varphi \Rightarrow \exists a, b \in G \quad a' = \varphi(a) \quad b' = \varphi(b) \quad \exists a'b'^{-1} \in \text{im } \varphi?$

$$\exists a, b \in G \quad \left\{ \begin{array}{l} a' = \varphi(a) \\ b' = \varphi(b) \end{array} \right. \Rightarrow a'b'^{-1} = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(ab^{-1}) \Rightarrow$$

$$\Rightarrow ab^{-1} \in G \Rightarrow a'b'^{-1} \in G' \quad \underline{a'b'^{-1} \in \text{im } \varphi}$$

Calcular el n\'ucleo y la imagen

$f : \mathbb{Z} \rightarrow \mathbb{Z}_n$  definido por:

$$f(x) = [x]_n$$

$$e_{G'} = [0]_n = \{nq : q \in \mathbb{Z}\}$$

$$\text{Ker } f = \{nq : q \in \mathbb{Z}\} = n\mathbb{Z}$$

$\hookrightarrow$  lo que trae la app  $f(x) = [x]_n$  se transforma en  $0 ([0]_n)$

por ser  $n\mathbb{Z}$  el n\'ucleo, es divisor del grupo  $n\mathbb{Z}$ :

$$\frac{\mathbb{Z}}{\text{Ker } f} = \{[0]_{\text{Ker } f}, [1]_{\text{Ker } f}, [2]_{\text{Ker } f}\}$$

(grado) revisar

④ Estudiar si es homomorfismo

$$\varphi: \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{30}$$

$$\text{definido por: } \varphi([a]_{12}) = [3a]_{30}$$

③ Determinar todos los homomorfismos de  $\mathbb{Z}_{12}$  en  $\mathbb{Z}_{30}$

④ Indicar cuál puede ser el orden del subgroupo imagen

$$12 \cdot ? = 36 \not\equiv 0 \pmod{30} \quad \text{No es homomorfismo}$$

②  $\varphi([a]_{12}) = [ka]_{30}$

$$k \cdot 12 \equiv 0 \pmod{30} \iff 12k = 30q \iff 2k = 5q \iff k = 5h$$

$$k \in \{0, 5, 10, 15, 20, 25\}$$

rem: (estamos en  $\mathbb{Z}_{30}$ )

⑤

$$|\varphi(\mathbb{Z}_{12})| \mid \text{mcd}(12, 30) = 6$$

$$|\varphi(\mathbb{Z}_{12})| \in \{1, 2, 3, 6\}$$

Hay 6 posibles homomorfismos que puedes tener:

$$\varphi([a]_{12}) = [ka]_{30}$$

→ corolario 1

Si  $(G, \cdot)$  y  $(G', \circ)$  son dos grupos finitos y  $\varphi: G \rightarrow G'$  es un homomorfismo de grupos entonces:

$|\varphi(G)|$  divide a  $|G'|$  y tambien divide a  $|G|$

$$|\varphi(G)| \leq |G'| \Rightarrow |\varphi(G)| \mid |G'| \quad \{ \text{lógico}$$

$\Downarrow$   
 $\text{im } \varphi$

$$\frac{|G|}{|\ker \varphi|} \approx \text{im } \varphi \Rightarrow \left| \frac{G}{\ker \varphi} \right| = |\text{im } \varphi| \Leftrightarrow \frac{|G|}{|\ker \varphi|} = |\text{im } \varphi| \Leftrightarrow$$

$$\Leftrightarrow |\ker \varphi| \cdot |\text{im } \varphi| = |G| \Rightarrow |\text{im } \varphi| \mid |G|$$

④ Deducir posibles órdenes para  $G$

$(G, \cdot)$  es grupo y

$\varphi: \mathbb{Z}_{12} \rightarrow G$  es un homomorfismo suryectivo

$$\begin{array}{c} \text{y tb} \\ |\ker \varphi| \mid |G| \\ \text{y tb} \\ |\text{im } \varphi| \mid \text{mcd}(|G|, |G'|) \end{array}$$

$$|G| \mid_{12} \Rightarrow |G| \in \{1, 2, 3, 4, 6, 12\}$$

$\left( \begin{array}{c} \text{y tb} \\ |\mathbb{Z}_{12}| \end{array} \right)$

→ Homomorfismos entre grupos cíclicos

La aplicación  $\varphi: \mathbb{Z}_n \rightarrow \mathbb{Z}_m$  es homomorfismo entre  $(\mathbb{Z}_n, +_n)$  y  $(\mathbb{Z}_m, +_m)$   $\Leftrightarrow \varphi([a]_n) = [ak]_m$  siendo  $nk \equiv 0 \pmod m$

demo:  $\overset{\text{u}}{\Rightarrow} \overset{\text{u}}{\varphi}: \mathbb{Z}_n \rightarrow \mathbb{Z}_m$  es homomorfismo  $\Rightarrow \varphi([\sigma]_n) = \varphi([1]_n)$

$$\Leftrightarrow [nk]_m = [nk]_m \Leftrightarrow nk \equiv 0 \pmod m$$

$$\overset{\text{u}}{\Leftarrow} \overset{\text{u}}{\varphi} ([a]_n) = [ak]_m \quad nk \equiv 0 \pmod m$$

$$\begin{aligned} &(\text{para que sea homomorfismo:}) \quad \varphi([a]_n + [b]_n) = \varphi([a+b]_n) = \\ &= \varphi([r]) = [kr]_m \end{aligned}$$

$$\varphi([a]_n) + \varphi([b]_n) = [ka]_m + [kb]_m = [k(a+b)]_m =$$

$$= [k(nq+r)]_m = [knq]_m + [kr]_m =$$

$$(kn \equiv 0 \pmod m) = [0]_m + [kr]_m = [kr]_m$$

$$\begin{aligned} a+b &= nq+r \\ 0 \leq r < n \end{aligned}$$

\* Grupos de orden 6

sea  $(G, *)$  grupo de orden 6  $\rightarrow (G, *)$  es isomorfo a:

$$- (\mathbb{Z}_6, +_6)$$

$$- (D_3, \circ) \approx (S_3, \circ)$$

2.4.

> P-grupos: grupo que tiene de orden potencia de p

sea  $(G, *)$  grupo finito y  $p \in \mathbb{N}$  divisor primo de  $|G|$ .

$H \leq G$  es p-grupo de G  $\rightarrow |H|$  es una potencia de p

> Subgrupos de Sylow: grupo con la máxima potencia de p entre los grupos q tienen

sea  $p \in \mathbb{N}$  primo divisor de  $|G|$  y  $H \leq G$ . H es un p-grupo de Sylow de G  $\Leftrightarrow H$  es p-grupo de G y tiene orden maximal.

⊗ obtener los p-grupos y subgrupos de Sylow:

$$(\mathbb{Z}_{20}, +_{20})$$

$$20 = 2^2 \cdot 5$$

primero que divide a 20!

$$H_0 = \langle 0 \rangle = \{0\} \rightarrow H_0 \text{ es } 2\text{-grupo ni } 5\text{-grupo}$$

$$H_1 = \langle 1 \rangle = \mathbb{Z}_{20} \xrightarrow{\text{orden } 20} \text{no es potencia de } 2 \text{ ni de } 5, 10 \text{ es ni } 2\text{-grupo ni } 5\text{-grupo}$$

$$H_2 = \langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\} \xrightarrow{\text{orden } 10, 9 \text{ no es potencia de } 2 \text{ ni de } 5, 10 \text{ es } 2\text{-grupo}}$$

P q

$$\text{Nod}(3, 20) = 1$$

$$H_3 = \langle 1 \rangle = \mathbb{Z}_{20}$$

$$H_4 = \langle 4 \rangle = \{0, 4, 8, 12, 16\} \xrightarrow{\text{orden } 5, \text{ es } 5\text{-grupo}} \rightarrow 5\text{-grupo de Sylow}$$

→ orden de 3

en 20, sea

otra vez  $\mathbb{Z}_{20}$

$$H_5 = \langle 5 \rangle = \{0, 5, 10, 15\} \rightarrow \text{el } 2\text{-grupo} \rightarrow 2\text{-grupo de Sylow}$$

$$H_{10} = \langle 10 \rangle = \{0, 10\} \rightarrow \text{el } 2\text{-grupo}$$

máximo  
potencia  
(5! [único]),  
 $2^3$ )

⊗ Encontrar los 2-grupos y 3-grupos de Sylow

$$A_4 = \{e = (1), x = (1, 2)(3, 4), y = (4, 3)(2, 3), z = (1, 3)(2, 4), a = (1, 2, 3), \\ a^2 = (1, 3, 2), b = (1, 3, 4), b^2 = (4, 3), c = (2, 4, 3), c^2 = (2, 3, 4) \\ d = (1, 4, 2), d^2 = (1, 2, 4)\}$$

$$H_0 = \{(1)\} \xrightarrow{\text{2º}} \text{2-grupo y 3-grupo}$$

$$H_1 = \{(1), x\}$$

$$H_2 = \{(1), y\}$$

$$H_3 = \{(1), z\}$$

$$H_4 = \{(1), x, y, z\} \xrightarrow{\text{2º}} \text{2-grupo de Sylow}$$

$$H_5 = \{e, a, a^2\}$$

$$H_6 = \{e, b, b^2\}$$

$$H_7 = \{e, c, c^2\}$$

$$H_8 = \{e, d, d^2\}$$

3º  
3-grupo

3-grupo  
de Sylow



> Grupos abelianos finitos como producto de p-grupos de Sylow

sea  $(G, *)$  grupo abeliano con  $|G| = p^{t_m}$ ,  $p \in \mathbb{N}$  primo y  $\text{mcd}(m, p) = 1$

$$\Rightarrow G \cong W_p \times K$$

tenemos  $W_p = \{x \in G : x^{p^t} = e_G\}$ ,  $K = \{x \in G : x^m = e_G\}$ , con

$$|W_p| = p^t \quad |K| = m$$

demo:

①  $a \in K \Leftrightarrow \forall q \in \mathbb{Q} \quad e_q \in K \Leftrightarrow \{x \in G : x^m = e_G\}$

$a, b \in K \Rightarrow a^m = e_G, b^m = e_G \Rightarrow (ab^{-1})^m = a^m(b^m)^{-1} = e_G \cdot e_G^{-1} = e_G \Rightarrow ab^{-1} \in K$   
a.  $b^{-1} \in K$

②  $W_p \cap K = \{e_G\}$

sea  $a \in W_p \cap K \Rightarrow a^{p^t} = e_G \quad a^m = e_G \Rightarrow |a| \mid p^t \quad |a| \mid m \Rightarrow \dots \dots \text{(casi terminar)}$

③  $G = W_p \times K \quad \forall a \in G, \exists b \in W_p, c \in K \text{ tq } a = bc$

$$a \in G \quad |G| = p^t \cdot m \Rightarrow |a| = p^h \cdot n$$

$$\text{mcd}(p^h, n) = 1 \Rightarrow \exists x, y \in \mathbb{Z} \text{ tq } 1 = x p^h + y n \Rightarrow$$

$$\Rightarrow a = a^1 = a^{xp^h} \cdot a^{yn} \Rightarrow$$

$$\text{sea } c' = a^{p^h} \Rightarrow (c')^m = a^{p^h \cdot m} = (a^{p^h \cdot n})^{\frac{m}{n}} = e_G \Rightarrow c' \in K \Rightarrow (c')^x \in K \Rightarrow$$

$$\Rightarrow c = (c')^x = a^{xp^h} \in K$$

$$\text{sea } b^1 = a^n \Rightarrow (b^1)^{p^t} = ((b^1)^{p^t})^{p^{t-h}} = (a^{np^h})^{p^{t-h}} = e_G^{p^{t-h}} = e_G \Rightarrow$$

$$\Rightarrow b^1 \in W_p \Rightarrow b = (b^1)^y = a^{yn} \in W_p \Rightarrow a = c \cdot b \text{ siendo } c \in K \text{ y } b \in W_p$$

④  $G$  abeliano  $\Rightarrow$  todos los elementos comutan

$$\Rightarrow G \cong W_p \times K$$

$$|G| = |W_p| \cdot |K| = p^t \cdot m \Rightarrow |K| = \frac{p^t}{|W_p|} \cdot m$$

si  $p \mid |K| \Rightarrow \exists a \in K$  con  $|a| = p$ , como  $a^m = e_G \Rightarrow p \mid m$  contrad.

$$\Rightarrow \frac{p^t}{|W_p|} = 1 \Rightarrow p^t = |W_p| \text{ y } m = |K|$$

Caracterización de subgrupos de Sylow de un grupo abeliano

Sea  $(G, +)$  grupo abeliano, con  $|G| = p^m$ ,  $p \in \mathbb{N}$  primo y  $\text{mcd}(p, m) = 1$ , entonces el  $p$ -subgrupo de Sylow de  $(G, +)$  es:

$$W_p = \{x \in G : x^{p^t} = e_G\} \leq G \quad \text{④ p.o.i}$$

(lo conseguimos ver al ver que su orden es potencia de  $p$ , y esto es maximal)

demo:

$$\textcircled{1} \quad \text{d} W_p \leq G? \quad W_p \neq \emptyset \quad \forall q \in \mathbb{N} \quad q \nmid p \Rightarrow e_G \in W_p$$

$$\forall a, b \in N_p \quad \Rightarrow a^{p^t} = e_G \quad \Rightarrow (ab^{-1})^{p^t} = a^{p^t} \cdot (b^{p^t})^{-1} = e_G \cdot e_G^{-1} = e_G$$

↑  
abeliano  
↓

$$\textcircled{2} \quad \text{es un } p\text{-grupo}$$

$$W_p : q \in \mathbb{N} \text{ es primo y } q \mid |W_p| \Rightarrow \exists a \in W_p \text{ con } |a| = q$$

th. Cauchy

$$a \in W_p \Rightarrow a^{p^t} = e_G \quad \Rightarrow$$

$$\textcircled{3} \quad \text{si } K \text{ es } p\text{-grupo y } W_p \leq K \leq G$$

$$\text{d} W_p = K?$$

$$\Rightarrow q \mid p^t \Rightarrow p = q$$

$$\text{sea } a \in K, \text{ como } K \text{ es } p\text{-grupo se verifica que } |K| = p^h \Rightarrow a^{p^h} = e_G \Rightarrow a^{p^t} = (a^{p^h})^{p^{t-h}} = e_G = e_G \Rightarrow a \in W_p$$

↑  
th.  
degrange

■ Obtener subgrupos de Sylow

- $(\mathbb{Z}_8, +_8)$

orden de  $7e$  en  $\mathbb{Z}_8$  → es el 2-grupo de Sylow

$$W_2 = \langle 2 \rangle \quad \text{pues } 8 \text{ es una potencia de } 2, \text{ y a lo visto la máxima potencia.}$$

Todos sus subgrupos son 2-grupos

$$(\mathbb{Z}_{18}, +_{18}) \quad 18 = 2 \cdot 3^2$$

$$W_3 = \langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\} \quad \text{④ p.ei}$$

$$W_2 = \langle 9 \rangle = \{0, 9\}$$

$$H_6 = \langle 0 \rangle \text{ es } 2 \text{ y } 3\text{-grupo}$$

$$H_1 = \langle 1 \rangle \text{ no es ni } 2 \text{ ni } 3\text{-grupo}$$

$$H_2 = \langle 2 \rangle \text{ es } 3\text{-NPG}$$

$$H_3 = \langle 3 \rangle \approx \{0, 3, 6, 9, 12, 15\}$$

orden 6, ni 2 grupo ni 3 grupo

$$H_6 = \langle 6 \rangle = \{0, 6, 12\} \text{ es } 3\text{-grupo}$$

$$H_7 = H_1$$

$$H_8 = H_2$$

$$H_9 = \langle 9 \rangle = \{0, 9\} \text{ es } 2\text{-grupo.}$$

④ p.ei:  $2^{p^t} = 2^3 = 2 \cdot 2 \cdot 2 = 8$

2<sup>p<sup>t</sup></sup> → hacemos  $t = 3$

$$6^3 = 6+6+6 = 18 = [0] = \text{encontrado.} \checkmark$$

② Escribir como producto de grupos de Sylow:

$$(\mathbb{Z}_{12}, \circ_{12}) \quad |12| = 12 = 2^2 \cdot 3$$

a  $\mathbb{Z}_n$ , en este caso concreto

$$\mathbb{Z}_{12} = W_2 \times W_3 \quad |W_2| = 4 \rightarrow W_2 \approx \mathbb{Z}_4$$

$$|W_3| = 3 \rightarrow W_3 \approx \mathbb{Z}_3$$

$$(W_2 = \langle 3 \rangle = \{0, 3, 6, 9\} \approx \mathbb{Z}_4)$$

$$\mathbb{Z}_{12} \approx \mathbb{Z}_4 \times \mathbb{Z}_3$$

ademas, sabemos tb que  $\mathbb{Z}_4 \approx \mathbb{Z}_2 \times \mathbb{Z}_2$  por que

que un grupo sea isomorfo al producto de otros, estos tienen que ser primos entre si  
creo

→ Todo grupo de Sylow abeliano finito es isomorfo a un producto de ciclos

si  $W_p$  es un  $p$ -grupo de Sylow abeliano, de orden  $p^t \Rightarrow$

$$W_p \approx \mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}} \times \dots \times \mathbb{Z}_{p^{r_k}} \text{ con } t = r_1 + r_2 + \dots + r_k$$

③ Expresar el subgrupo de Sylow como producto de grupos cíclicos

$$(\mathbb{U}_{15}, \circ_{15})$$

$$\mathbb{U}_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\} \quad |\mathbb{U}_{15}| = 8 = 2^3$$

$$\mathbb{U}_{15} = W_2 = \langle 2 \rangle \vee \langle 11 \rangle \approx \mathbb{Z}_4 \times \mathbb{Z}_2$$

$$|\langle 2 \rangle| = 4$$

un elem. cualq.  
con orden maximo

~~13~~ (no entra el 3)

$$\langle 2 \rangle = \{1, 2, 4, 8\}$$

un elem. q. tenga  
orden minimo

$$|\langle 11 \rangle| = 2$$

$$|\langle 7 \rangle| = 4$$

$$|\langle 8 \rangle| = 4$$

$$|\langle 1 \rangle| = 2$$

$$|\langle 13 \rangle| = 4$$

$$|\langle 4 \rangle| = 2$$

④ Localizar los subgrupos de Sylow. (Nota: sabemos que el orden del grupo no va a ser exactamente el orden del subgrupo de Sylow)

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_9$$

$$|G| = 2^5 \cdot 3^2$$

$$G \cong W_2 \times W_3 \quad \text{con} \quad |W_2| = 2^5 \quad |W_3| = 3^2$$

$$G \cong \underbrace{(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8)}_{W_2} \times \mathbb{Z}_9 \Rightarrow \text{orden } 9 (= 3^2)$$

remindere:

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm} \quad \text{if} \quad \text{mcd}(n, m) = 1$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$$

④ Dado un grupo abeliano  $(G, *)$  de orden  $|G|=360 = 2^3 \cdot 3^2 \cdot 5$ . Indicar el orden de cada uno de los p-grupos de Sylow y escribir como producto de grupos.

teorema Lema: 2-grupo  
3-grupo  
5-grupo

$$G \cong W_2 \times W_3 \times W_5$$

$$\begin{aligned} |W_2| &= 8 \quad (= 2^3) \\ |W_3| &= 9 \quad (= 3^2) \\ |W_5| &= 5 \quad (= 5) \end{aligned}$$

Cortamos factorizando el 8  
 $W_2 = \left\{ \begin{array}{l} \mathbb{Z}_8 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\ \mathbb{Z}_4 \times \mathbb{Z}_2 \end{array} \right\}$  3 posibles formas q. podra tener el grupo de Sylow

$$W_3 = \left\{ \begin{array}{l} \mathbb{Z}_9 \\ \mathbb{Z}_3 \times \mathbb{Z}_3 \end{array} \right\}$$

$$W_5 = \left\{ \mathbb{Z}_5 \right\}$$

Entender: Todos los posibles grupos que podrían ser:

$$G = \left\{ \begin{array}{l} \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \\ \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\ \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \\ \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \end{array} \right\}$$

## Ejercicios parciales: repeating

2x17

④

- ⓐ Abierto  
orden 120

dN elem y f. inv → sabiendo q tiene 2 elem de orden 2

$$120 = 2^3 \cdot 5 \cdot 3 = w_1 \times w_2 \times w_3$$

$$|w_1| = 2^3$$

→

$\mathbb{Z}_8$

$$|w_2| = 5 - \mathbb{Z}_5$$

$$|w_3| = 3 - \mathbb{Z}_3$$

$$\frac{\mathbb{Z}_4 \times \mathbb{Z}_2}{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2}$$

como tiene 3 elementos  
de orden 2

dN elem:  $\{2, 2, 2, 5, 3\}$

f. inv

why?

- ⓑ orden 63

7-grupo de sylow?

$$63 = 3^2 \cdot 7$$

$$w_3 \times w_7$$

$$|w_3| = 3^2$$

$$|w_7| = 7$$

1º grp

$$\frac{n_2 | 36}{n_2 | 63} \rightarrow \text{why}$$

ya que el orden  
de un subgrupo  
divide el  
orden de W  
grps

$$n_7 \equiv 1 \pmod{7} \rightarrow n_7 = 1$$

$$S_7 \trianglelefteq G$$

$$|S_7| = 7$$

en prop. y rot. trivial

if

G no es  
simple

1 7-grpo sol.

if

solo 1 subgrupo con orden 7

if

$$S_7 \trianglelefteq G$$

otro  
explicacion

## > Teorema de estructura de grupos abelianos finitos

Todo grupo abeliano finito  $(G, *)$  es isomorfo a un producto de grupos cíclicos:

$$G \cong \mathbb{Z}_{q_1^{\beta_1}} \times \mathbb{Z}_{q_2^{\beta_2}} \times \dots \times \mathbb{Z}_{q_r^{\beta_r}}$$

donde  $q_1 \leq q_2 \leq \dots \leq q_r$  primos, no necesariamente distintas.

Se dice que  $(G, *)$  está en función de los divisores elementales.

## > Factores invariantes de un grupo abeliano finito

Dado un grupo abeliano finito  $(G, *)$ , existe una única sucesión de naturales:

$$m_1 \geq m_2 \geq \dots \geq m_k \geq 1$$

tal que  $|G| = m_1 m_2 \dots m_k$ ,  $\forall i \in \{1, \dots, k-1\}$ ,  $m_{i+1} \mid m_i$  y

$$G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$$

$(G, *)$  está en función de sus factores invariantes.

## ¶ Descomponer como producto de los divisores elementales y los factores invariantes

$$\begin{array}{c} \mathbb{Z}_{12} \times \mathbb{Z}_{15} \times \mathbb{Z}_{24} \\ \text{||} \quad \text{||} \quad \text{||} \\ 2^2 \cdot 3 \quad 3 \cdot 5 \quad 2^3 \cdot 3 \end{array}$$

$$(\mathbb{Z}_2^2 \times \mathbb{Z}_3) \times (\mathbb{Z}_3 \times \mathbb{Z}_5) \times (\mathbb{Z}_{2^2} \times \mathbb{Z}_3) =$$

$$\simeq \underbrace{(\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2})}_{W_2} \times \underbrace{(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3)}_{W_3} \times (\mathbb{Z}_5) \stackrel{\text{W5}}{\simeq} \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$\stackrel{\text{max potencia de cada 1}}{\simeq} \mathbb{Z}_{2^3 \cdot 3 \cdot 5} \times (\mathbb{Z}_{2^2}) \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \simeq$$

$$\stackrel{\text{max potencia de cada 1}}{\simeq} \mathbb{Z}_{2^3 \cdot 3 \cdot 5} \times \mathbb{Z}_{2^2 \cdot 3} \times (\mathbb{Z}_3) \simeq \mathbb{Z}_{2^3 \cdot 3 \cdot 5} \times \mathbb{Z}_{2^2 \cdot 3} \times \mathbb{Z}_3$$

factores invariantes

(OK16)

(6 9 5 16) (1 3 6 7) (3 5 1) (3 6)

(1 6) (2 7) (3 8 9 5)  $\oplus_1$  //yc eaten  
toddler elem

$$\text{wcm}(4, 32) = 4$$