

## 1. Definición, generalidades y ejemplos

### Operación binaria

Sea  $\mathcal{G}$  un conjunto, una operación binaria en  $\mathcal{G}$  es una aplicación  $\oplus: \mathcal{G} \times \mathcal{G} \longrightarrow \mathcal{G}$  dada por  $\oplus(a,b) = a \oplus b \quad \forall a, b \in \mathcal{G}$ . Realmente la denotaremos por la yuxtaposición.

Algunos ejemplos:

i) Sumas y productos en  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$

ii) Dado  $\mathcal{X}$  un conjunto, consideramos  $(\cup: P(\mathcal{X}) \times P(\mathcal{X}) \longrightarrow P(\mathcal{X}))$  así como  $\cap$ .

### Monoïdes

Definimos un monoïde como un conjunto no vacío junto con una operación binaria que verifica:

i) Asociatividad  $(xy)z = x(yz) \quad \forall x, y, z \in \mathcal{G}$

ii) Existencia de elemento neutro  $\exists e \in \mathcal{G} \mid ex=x \quad \forall x \in \mathcal{G}$  (por izq y por drch)

No denotaremos como  $(\mathcal{G}, \oplus, e)$ .

Neutral

En un monoïde, el elemento neutro es único.

Algunos ejemplos de monoïdes tenemos:

i)  $(\mathbb{N}, +, 0), (\mathbb{N}, \times, 1)$

ii)  $(P(\mathcal{X}), \cap, P(\emptyset)), (P(\mathcal{X}), \cup, \emptyset)$

### Grupo

Definimos un grupo como un conjunto no vacío junto con una operación binaria que verifica:

i) Asociatividad  $(xy)z = x(yz) \quad \forall x, y, z \in \mathcal{G}$

En definitivo es

ii) Existencia de elemento neutro.  $\exists e \in \mathcal{G} \mid ex=x \quad \forall x \in \mathcal{G}$

un elemento tal que

iii) Existencia de elemento inverso:  $\forall x \in \mathcal{G} \exists y \in \mathcal{G} \mid yx=e$

la op. binaria cumple

Si además se cumple

la existencia inverso

iv) Conmutativa:  $xy = yx \quad \forall x, y \in \mathcal{G}$

diremos que  $\mathcal{G}$  es un grupo abeliano o conmutativo

Destacaremos las siguientes observaciones:

i) Por abuso del lenguaje, denotaremos por  $\mathcal{G}$  al grupo  $(\mathcal{G}, \oplus, e)$

ii) Usaremos notación multiplicativa luego independientemente

de qué operación sea usaremos la composición.

(ii) Por (i) el neutro será 1 y el simétrico  $x^{-1}$ .

(iii) En el caso que usemos la función aditiva, usaremos  $x+y$ , el neutro será 0 y el simétrico será el opuesto  $(-x)$ .

Pocos ejemplos de notación:

i)  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  y  $C$  con la suma serán grupos abelianos.

ii)  $\mathbb{Q}^*, \mathbb{R}^*$  y  $C^*$  con el producto serán también abelianos.

iii)  $\{1, -1, i, -i\} \subset \mathbb{C}$  con el producto también será abeliano.

iv)  $(M_2(\mathbb{R}), +)$  es un grupo abeliano.

v)  $(\mathbb{G}_2(\mathbb{R}), *)$  es un grupo (el producto de matrices regulares no es conmutativo).

Un grupo lineal de orden 2 con el producto, matrices regulares de orden 2.

vi)  $(\mathbb{Z}_n, +)$  es un grupo abeliano.

vii)  $\mathcal{Z}((\mathbb{Z}_n)) = \{[a] \in \mathbb{Z}_n \mid \text{mcd}(a, n) = 1\}$  con la multiplicación de clases es un grupo abeliano.

viii)  $\cup_{i=1}^n M_n =$  raíces complejas de  $x^n - 1 = \{ \alpha_n = e^{2\pi i k/n} + i \operatorname{sen} \frac{2\pi k}{n}, \text{ para } k = 0, 1, 2, \dots, n-1 \}$  es un grupo abeliano con el producto

ix)  $SL_2(\mathbb{K})$ , matrices regulares sobre el cuerpo  $\mathbb{K}$  con el producto de matrices es un grupo.  $SL$  es grupo especial.

x) Sean  $G$  y  $H$  grupos,  $G \times H$  es un grupo donde  $*: (g, h) \mapsto gh$  es la operación  $(a, b)(c, d) \mapsto (ac, bd)$

biunaria llamada producto directo es un grupo.

xi) Si  $S$  es un conjunto vacío, consideramos  $S(x) = \{f: S \rightarrow S \mid f \text{ es biyectiva}\}$  para funciones de  $S$  con la composición es un grupo. A este grupo lo llamaremos  $S$ , donde  $|S|$ .

xii) Sea  $g$  un grupo y  $X$  un conjunto, consideramos  $A_p(X, g) = g^X = \{f: X \rightarrow g \text{ aplicaciones de } X \text{ en } g\}$  con la operación biunaria  $(f * g)(x) = f(g(x)) \forall x \in X$ . En este caso, el simétrico de un elemento  $f$  será  $f^* g^*$  tal que  $f^*(x) = (f(x))^{-1}$ . Si  $X = \emptyset$  entonces  $g^{\emptyset} = \{g\}$  y si  $X = \{x\}$  entonces  $g^x$  identifica con  $g_x$ .

Lema

Op. biunaria }  
- Asoc  
- Elemento por izq  
- Elemento por der

Sea  $g$  un grupo, entonces se cumple.

i)  $x x^{-1} = e \in g$

ii)  $x e = x \in g$

iii)  $\exists! e \in g \mid ex = x \in g$

iv)  $\exists! x' \in g \mid xx' = e \vee x'g$

v) (Propiedad cancelativa)  $\forall x, y, z \in g \text{ si } xy = xz \text{ y } x \neq e \text{ entonces } y = z \text{ y } x = z$

-Demostración -

i)  $x^{-1}(xx^{-1}) = (x^{-1}x)x^{-1} = ex^{-1} = x^{-1}$

ii)  $x = x(x^{-1}x) = (x^{-1}x)x = ex = x$

v) Supongamos que  $xy = xz$  entonces  $y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z$ .  $\square$   
Se consigue la segunda.

$\square$

Teorema (Propiedades del inverso)

Sea  $g$  un grupo entonces:

i)  $e^{-1} = e$

ii)  $(x^{-1})^{-1} = x \quad \forall x \in g$

iii)  $(xy)^{-1} = y^{-1}x^{-1} \quad \forall x, y \in g$

-Demostración -

i)  $e^{-1} = ee^{-1} = e$

ii)  $x^{-1}(x^{-1})^{-1} = e = x^{-1}x \text{ entonces } (x^{-1})^{-1} = x$

iii)  $(y^{-1}x^{-1})(xy) = y^{-1}x^{-1}xy = y^{-1}ey = y^{-1}y = e \Rightarrow (y^{-1}x^{-1}) = (xy)^{-1}$   $\square$

Teorema

Sea  $g$  un conjunto no vacío con una operación binaria asociativa, son equivalentes:

i)  $g$  es un grupo

ii)  $\forall a, b \in g$ , las ecuaciones  $ax=b$ ,  $xa=b$  tienen solución en  $g$ , es decir,

$\exists c, d \in g \mid ac = b \wedge da = b$  soluciones de la ecuación

-Demostración -

i)  $\Rightarrow$  ii)

$$ax = b \Rightarrow c = a^{-1}b$$

$$xa = b \Rightarrow d = ba^{-1}$$

ii)  $\Rightarrow$  i) Tomemos la ecuación  $ax = a$  cuya solución será  $e_a$  (por ii). Por otro lado,  $\forall b \in g \quad xb = b$  tiene solución, que llamaremos  $x \in g \mid xb = b$

En este caso,  $be_a = xae_a = xa = b$ , por tanto,  $e_a = e$  es unidimensional por la derecha (y consecuentemente por la izquierda)

Como  $ax = e$  tiene solución y por tanto, todo elemento va a tener un inverso.

## definición asociativa general

Sea  $\mathcal{G}$  un grupo,  $\forall x \in \mathcal{G}$  y  $u, v \in \mathbb{Z}$ , se cumple que

$$\left(\prod_{i=1}^u x_i\right) \left(\prod_{i=u+1}^v x_i\right) = \prod_{i=1}^v x_i$$

Gracias a esto, podemos definir las potencias de forma que, para cada  $x \in \mathcal{G}$  se define

$$x^u : \mathcal{G}, \mathbb{Z} \longrightarrow \mathcal{G} \quad \begin{cases} x^u & u > 0 \\ e & u = 0 \\ (x^{-1})^{-u} & u < 0 \end{cases}$$
$$(x, u) \mapsto x^u$$

En consecuencia,  $x^{u+v} = x^u x^v \quad \forall u, v \in \mathbb{Z}$ .

## Grupos finitos

Sea  $\mathcal{G}$  un grupo, si  $\mathcal{G}$  tiene un número finito de elementos, se dice que  $\mathcal{G}$  recibe el nombre de **grupo finito** y a ese número de elementos se le llama **orden del grupo** y lo denotaremos por  $|G|$ .

Además, dado un grupo finito  $\mathcal{G} = \{x_1, \dots, x_n\}$  se llama **tabla de Cayley** (o tabla de multiplicación) a la matriz  $A_{n \times n}, n \in \mathbb{N}$  cuya entrada  $(i, j)$  es  $x_i * x_j$ .

Algunos ejemplos tenemos:

i)  $\mathcal{G} = \{e, x\}$

*	0	1
0	0	1
1	1	0

ii)  $\mathcal{G} = \{e, x, x^2\}$

*	0	1
0	0	0
1	0	1

En definitiva, es una operación bivaluada asociativa, con neutro y inverso para cada elemento que define al grupo.

Algunas propiedades de las tablas de Cayley son:

i) Todas las entradas de una tabla de Cayley de un grupo abeliano son simétricas

ii) Todas las entradas aparecen en todas las filas y columnas, pues en caso contrario, dados  $a, b \in \mathcal{G}$  las ecuaciones  $ax=b$  y  $xa=b$  no tendrían solución.

iii) Una fila de las entradas responde el criterio para que respete la existencia de neutro.

Al igual que hablamos de orden de un grupo  $\mathcal{G}$ , podemos definir el orden de un elemento  $x \in \mathcal{G}$

como el número natural  $n$  más, si existe, tal que  $x^n = e$ . En caso de que no exista, dicho orden

será infinito y notaremos por  $0(x)=\infty$

→ Puede no existir

Si encontramos  $w \in \mathbb{N}$ , tal que para todo  $x$  dado cumple  $O(x) = w$ , cumpliendo  $x^w = 1$   
entonces  $w$  divide a  $m$ .

Algunos ejemplos de esto son:

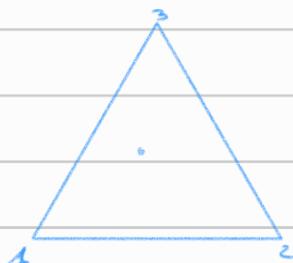
- i)  $O(x) = 1 \Leftrightarrow x = 1$
- ii)  $O(x) = O(x^{-1}) \forall x \in \mathbb{R} \setminus \{0\}$
- iii)  $\forall x \neq 0, x \in \mathbb{Z} \cup \mathbb{Q} \cup \mathbb{R} \quad O(x) = \infty$
- iv) En  $\mathbb{C}^*$   $O(i) = 4$
- v)  $\mathbb{Z}_7 \quad O(6) = 3$
- vi)  $\mathbb{Z}_7 = \langle \langle \mathbb{Z}_7 \rangle, O(2) = 3 \text{ y } O(3) = 6 \rangle$

Ejercicio: Construimos  $(\mathbb{Z}, *)$  donde  $a * b = a + b + 1$ . Probar que es un grupo abeliano.

- i) Asociativa:  $(a * b) * c = (a + b + 1) * c = a + b + c + 2 = a * (b * c)$
- ii) Neutro:  $a * e = a + e + 1 = a \Rightarrow e = -1$
- iii) Inverso:  $a * a^{-1} = -1 \Rightarrow a + a^{-1} + 1 = -1 \Rightarrow a^{-1} = -a - 2$
- iv) Comunitativa: se deduce de  $\mathbb{Z}$ .

## 2. Grupos diédricos

Los grupos diédricos se definen como isometrías de un polígono regular que dejó fija la figura. Por ejemplo con el triángulo:



### i) Rotaciones

- Identidad

- Rotación de  $\frac{2\pi}{3}$  en sentido horario  $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} (r)$

- Rotación de  $\frac{4\pi}{3}$  en sentido horario  $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} (r^2)$

### ii) Simetrías axiales:

- Las tres reflexiones por cada recta que pasa por el punto medio:

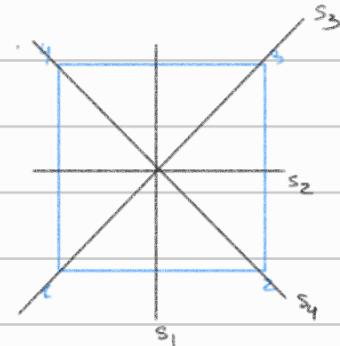
$$s_1: \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad (\text{lado } 1/2) \quad (s_1)$$

$$s_2: \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix} \quad (sr)$$

$$s_3: \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \quad (sr^2)$$

De aquí vemos que todas las isometrías se deducen de  $s_1$  y  $r$ , por composición.

Pensando en el cuadrado.



- Rotaciones

$$r_1: (g_{\frac{\pi}{2}}) : (1 \ 2 \ 3 \ 4) \quad (r_1) \text{ Se informa} \rightarrow \text{biene su rotación}$$

$$r_2: (g_{\pi}) : (1 \ 3)(2 \ 4) \quad (r_2)$$

$$r_3: (g_{\frac{3\pi}{2}}) : (1 \ 4 \ 3 \ 2) \quad (r_3)$$

$$(r'') = id$$

- Simetrías

$$\begin{aligned} s_1 &: (1 \ 2)(3 \ 4) \quad (s_1) \\ s_2 &: (1 \ 4)(2 \ 3) \quad \left. \begin{array}{l} s_1^2 = id \\ s_2^2 = id \end{array} \right. \\ s_3 &: (2 \ 4) \\ s_4 &: (1 \ 3) \end{aligned}$$

En este caso, no se cumple que sea abeliano pues  $rs \neq sr$  pero si que  $sr = r^3s$ . Poco aprendizaje constructivo la tabla de Cayley de  $D_4$  (isometrías del cuadrado)

	1	r	$r^2$	$r^3$	s	$sr$	$s r^2$	$s r^3$
1	1	r	$r^2$	$r^3$	s	$sr$	$s r^2$	$s r^3$
r	r	$r^2$	$r^3$	1	$s r^3$	s	$sr$	$s r^2$
$r^2$	$r^2$	$r^3$	1	r	$s r^2$	$s r^3$	s	$sr$
$r^3$	$r^3$	1	r	$r^2$	s	$s r^2$	$s r^3$	s
s	s	$s r$	$s r^2$	$s r^3$	1	r	$r^2$	$r^3$
$sr$	$sr$	$s r^2$	$s r^3$	s	$r^3$	1	r	$r^2$
$s r^2$	$s r^2$	$s r^3$	s	$sr$	$r^2$	$r^3$	1	r
$s r^3$	$s r^3$	s	$sr$	$s r^2$	r	$r^2$	$r^3$	1

Es importante tener en cuenta que

$$rs = r^3s$$

y por ende

$$sr = s r^3$$

De forma general, dado  $n \in \mathbb{N}$ , se define como el conjunto de las isometrías que dejan fijo un polígono regular de  $n$  lados,  $|D_n| = 2n$  donde:

•  $u$  rotaciones dadas por giros de  $\frac{2k\pi}{n}$ ,  $k=0, \dots, n-1$

•  $u$  simetrías

Nº par de lados



Nº impar de lados



Para fijar una rotación daremos por  $r$  a la rotación de  $\frac{2\pi}{n}$  rotaciones. De la misma forma, daremos para  $s$  la simetría que pasa por el origen de coordenadas y el vértice

que hagamos visto por 1.

Línea

Se cumple que, para  $D_n, n \in \mathbb{N}$

- i)  $1, r, r^2, \dots, r^{n-1}$  son todos distintos y  $r^{n-1} = 1$ . Entonces  $O(r) = n$
- ii)  $s^2 = 1$  luego  $O(s) = 2$ .
- iii)  $s \cdot r^i \in \{r, \dots, r^{n-1}\}$  ( $s$  fija 1 pero  $r^{(i+1)} \neq r^i, \dots, r^{n-1}$ )
- iv)  $s \cdot r^i$  o  $s \cdot s \cdot r^i$  son simetrías en los ejes de simetría ( $s, \dots, s_n$ ) y además,  $s \cdot r^i \cdot s = r^{(n-i)}$
- v)  $s \cdot r = r^i \cdot s$ , o en general,  $s \cdot r^i = r^i \cdot s \quad \forall i \in \{0, \dots, n-1\}$

De esta manera se describen todos los grupos finitos  $D_n, n \in \mathbb{N}$ .

Como ejemplo de esta construcción:

$$\text{i) Para } D_{12} \quad s_1^9 s_1^6 = r^9$$

Definición

Un conjunto de generadores de un grupo  $g$  es un subconjunto  $S \subseteq g$  tal que todo elemento de  $g$  puede escribirse como producto finito de elementos de  $S$  y sus inversos de dos maneras por  $g = \langle S \rangle$  o si  $S = \{x_1, \dots, x_m\}$  entonces  $g = \langle x_1, \dots, x_m \rangle$

En ese caso, diremos que  $g$  es generado por  $S$  y cualquier elemento lo podemos expresar de la siguiente:

$$x \in g \Leftrightarrow x = \prod_{i=1}^m s_i^{\gamma_i} \mid \gamma_i = \pm 1, s_i \in S.$$

Como ejemplos:

i)  $g = \langle x \rangle, S = \{x\}$  será un grupo cíclico

$$\mathbb{Z} = \langle 1 \rangle$$

ii)  $D_n = \langle r, s \rangle \quad \forall n \in \mathbb{N}$

Si  $g = \langle S \rangle$  y existe un conjunto de rotaciones generadas por  $R_1, \dots, R_m$  donde esas rotaciones son igualdades entre elementos de  $S \cup S^{-1}$  tal que cualquier rotación entre los elementos de  $S$  puede deducirse de estas. Entonces, diremos que estos generadores y rotaciones constituyen una presentación de  $g$  y lo escribiremos  $g = \langle S \mid R_1, \dots, R_m \rangle$

## Clases ejemplos finitos:

i)  $D_6 = \langle r, s / rs = sr^{-1}, r^3 = 1, s^2 = 1 \rangle$  tiene orden 6

ii)  $D_8 = \langle r, s / r^2 = s^2 = 1, rs = sr \rangle = \langle 1, r, s, rs \rangle$

iii)  $\mathbb{Z}_n = \langle x / x^n = 1 \rangle$  grupo cíclico de orden  $n \in \mathbb{N}$

iv)  $V^{\text{abs}} = \langle x, y / x^2 = 1, y^2 = 1, (xy)^2 = 1 \rangle = \langle 1, xy, xy^2 \rangle$  grupo de Klein abstracto

v)  $Q_2^{\text{abs}} = \langle x, y / x^4 = 1, x^2 = y^2, xyx^{-1} = y^3 = 1, xy, x^3y, x^3y^2 \rangle$

Si nos fijamos en los ordenes de los elementos

$O(x^4), O(x^2) = 2$  y los demás tienen orden 4 a excepción del 1 que tiene orden 1

Este grupo lo podemos ver dentro de  $S_{\ell_2}(\mathbb{C}) = \{f \in M_2(\mathbb{C}) \mid \det(f) \neq 0\}$  realizando la siguiente identificación

$$1 = \text{Id}_2 \quad x = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad x^2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad x^3 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

$$xy = \begin{pmatrix} 0 & -1 \\ -i & 0 \end{pmatrix} \quad x^2y = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix} \quad x^3y = \begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix}$$

los cuaternios,  $Q_2 = \{ \pm 1, \pm i, \pm j, \pm k \}$  cumpliendo  $i^2 = j^2 = k^2 = -1$ ,  $ij = k$ ,  $jk = i$ ,  $ki = j$  y cambiando el orden cambia el signo  $ji = -k$ ,  $kj = -i$ ,  $ik = -j$ . Con esta descripción podemos identificar con los elementos de  $Q_2^{\text{abs}}$  de la siguiente forma:

$$\begin{array}{llll} 1 = 1 & x = i & y = j & x^2 = -1 \quad x^3 = -i \\ xy = k & x^2y = -j & x^3y = -k & x^3y^2 = -k \end{array}$$

## 3. Grupos simétricos ( $S_n$ )

Dado un conjunto  $X$ , diremos de  $S(X) = \{f : X \rightarrow X \text{ biyectivas}\}$  que denominaremos como Perm( $X$ ). Considerando ahora  $X$  finito, que podemos identificar como  $X = \{1, \dots, n\} \subset \mathbb{N}$  de forma que  $S(X) = S_n$  y llamaremos  $n$ -ésimo grupo simétrico cuyo orden será  $|S_n| = n!$   $\forall n \in \mathbb{N}$ . Siempre trabajaremos sobre la composición.

Dado ahora  $n \in \mathbb{N}$ , trabajaremos por  $\sigma \in S_n$  a los elementos de  $S_n$ . Además, usaremos una representación matricial para representar los elementos de  $S_n$ .

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

Esto define perfectamente a  $\sigma : X \rightarrow X$  biyectiva

Veamos un contraejemplo que muestra que  $S_n$ , en general, no es abeliano.

•) Considerando  $S_5$ ,  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$   $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$

Se cumple que  $\sigma \tau \neq \tau \sigma$

•)  $S_0 = S_1$  y  $S_2$  son abelianos, los demás no

En ocasiones, usaremos la representación de ciclos para representar los permutaciones, considerando  $\sigma$  y  $\tau$  ciclos de  $S_n$ , como en el ejemplo:

$$\sigma = (1 \ 2 \ 3 \ 4 \ 5)$$

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

A este tipo de representación la denominaremos representación en ciclos disjuntos; de hecho, si algún elemento no se permuta no aparecerá en esta representación.

Sea  $\sigma \in S_n$ ,  $a \in \mathbb{N}$  tal que  $\sigma(a_1) = a_{i+1}$ ,  $\sigma(a_m) = a_i$ . Dicimos, a esto movimiento, lo llamaremos ciclo de longitud  $m \in \mathbb{N}$  y lo representaremos por:

$$\sigma = (a_1 \ a_2 \ \dots \ a_m) = (a_2 \ \dots \ a_m \ a_1) = \dots = (a_m \ a_1 \ a_2 \ \dots \ a_{m-1}) \text{ Notación de ciclos Taura I}$$

Dado el número de ciclos de longitud  $m$  será  $\frac{m}{m}$  para  $m \in \mathbb{N}$ .

El orden de un ciclo de longitud  $m \in \mathbb{N}$  es  $m$  como cabía esperar pues  $\sigma^m = id$ . De la misma forma, si  $\sigma = (a_1 \ \dots \ a_m)$  es un ciclo de longitud  $m$  sabemos que  $\sigma^{-1} = id$  luego  $\sigma^l = (a_m \ a_{m-1} \ \dots \ a_1)$ . A los dos-ciclos  $(a_1 \ a_2)$  los llamaremos transposiciones y tienen orden dos.

Dado  $\sigma \in S_n$  tal que  $\sigma = (a_1 \ \dots \ a_m)$  con  $m \in \mathbb{N}$ , lo podemos descomponer en ciclos disjuntos pues

$\sigma = (a_1, \dots, a_{m_1}) (a_{m_1+1}, \dots, a_{m_2}) \dots (a_{m_k}, \dots, a_n)$  donde  $m_i < m_{i+1}$ ,  $m_1$  y donde para cada subciclo, su longitud será menor que  $m$  cumpliendo que la suma de las longitudes debe ser  $m$ .

Veamos algunos ejemplos:

i) Consideremos  $S_{13}$ , es decir, el grupo simétrico de ciclos de longitud 13 son los dada

por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix}$$

cuya representación en ciclos disjuntos es:

no se solo par

$$\sigma = (1 \ 12 \ 8 \ 10 \ 4) (2 \ 13) (3) (5 \ 11 \ 7) (6 \ 9)$$

Si no escribimos los uno-ciclos pediremos ver que  $\sigma \in S_n$  y  $\sigma \in S_m$  para  $n \in \mathbb{N}$ .

solo los que cumplen el orden

En el caso de disponer de la representación en ciclos disjuntos de  $\sigma \in S_n$   $n \in \mathbb{N}$ , para calcular  $\sigma^{-1}$  bastaría con obtener  $\sigma_i^{-1}$   $\forall i$ . Por tanto:

$$\sigma \in S_n, \sigma = \sigma_1 \cdots \sigma_k \Leftrightarrow \sigma^{-1} = \sigma_1^{-1} \cdots \sigma_k^{-1}$$

### Teorema

Toda permutación  $\sigma \in S_n, n \in \mathbb{N}, n \neq 1$  se expresa de la forma  $\sigma = \tau_1 \cdots \tau_k$ , donde  $\tau_i, i=1, \dots, k$  son ciclos disjuntos de longitud mayor o igual que 2.

Además, esta descomposición es única salvo el orden de los factores, es decir:

$$\tau_1 \cdots \tau_k = \tau_2 \tau_k \tau_3 \cdots \tau_{k-1} \tau_1 \text{ por ejemplo.}$$

### - Demostración -

Sea  $\Sigma = \{1, \dots, n\}$  y  $\sigma \in S_n$  como así definimos la relación de equivalencia en  $\Sigma$ :

$$y R x \Leftrightarrow \exists m \in \mathbb{Z} \mid y = \sigma^{m \cdot u}(x) \quad \forall x, y \in \Sigma$$

Entonces, disponemos de las clases de equivalencia dadas por:

$$[x] = \{\sigma^{m \cdot u}(x) \mid m \in \mathbb{Z}\} \quad \forall x \in \Sigma$$

que cumplen  $|[x]| = n, n \in \mathbb{N}$ ; es decir, como  $\Sigma$  es finito  $[x]$  es finito.

Además, considerando  $\tau_{[x]}(x) = \sigma(x), \sigma(\sigma(x)) = \sigma^2(x), \dots, \sigma^{n-1}(x)$  es una permutación de  $S_n$  de forma que

$$\tau_{[y]}(y) = \begin{cases} \sigma(y) & y \in [x] \\ y & y \notin [x] \end{cases} \quad \begin{matrix} \hookrightarrow \tau_{[x]} \text{ es ciclo de } [x] \\ \text{Definición de ciclo} \end{matrix} \quad \tau_{[x]} : \Sigma \longrightarrow \Sigma$$

De esta forma, podemos determinar una partición de  $\Sigma$  en función de clases de equivalencia, por tanto

$$\Sigma = \bigcup_x [x]$$

$$\text{de forma que } \tau_{[y]}(y) = \begin{cases} \sigma(y) & y \in [x] \\ y & y \notin [x] \end{cases}$$

Debemos ver que  $\tau_{[x]} \cap \tau_{[y]} = \emptyset$  pero esto se cumple porque la partición es disjunta pues si  $y \in \tau_{[x]}$

entonces  $\tau_{[y]}(y) = \sigma(y)$  pero  $\tau_{[x]}(y) = y$  pues  $x \in [x] \in [y] \in \tau_{[y]}(y) \in \tau_{[x]}(y) = y$ . Por tanto, los ciclos son disjuntos.

De esta forma  $\sigma = \prod_{[x]} \tau_{[x]}$  y para  $y \in [y]$   $\sigma(y) = \prod_{[x]} \tau_{[x]}(y) \stackrel{\text{pues sólo habrá un }}{=} \tau_{[y]}(y) = \sigma(y)$

La unicidad la obtenemos gracias a la partición por reducción al absurdo  $\square$

### Corolario

El orden de cualquier permutación es el u.c.m. de las longitudes de los ciclos disjuntos en los que se descompone

### - Demostración -

Sea  $\sigma = \tau_1 \cdots \tau_k, n \in \mathbb{N}$ , como los ciclos son disjuntos conmutan luego

$$\sigma^m = \tau_1^m \tau_2^m \cdots \tau_k^m \quad \forall m \in \mathbb{N}$$

$$S_i \circ_i^{(u)} \Rightarrow O(\sigma_i) = u \text{ ó } O(\sigma_i) = u \mid u = u$$

De esta forma,  $\sigma^{(u)} = \sigma$  si y solo si  $\sigma_i^{(u)} = \sigma_i$  ( $i \in \{1, \dots, n\}$ ). Entonces  $O(\sigma_i) | u$  si y solo si  $u = u$

Vemos algunos ejemplos de permutaciones:

$$(i) \pi = \{1, 2, 4\}, S_2 = \{\text{id}, (12)\}$$

$$(ii) \pi = \{1, 2, 3\}, S_3 = \{\text{id}, (12), (23), (13), (123), (132)\} \cong D_3$$

$$(iii) \pi = \{1, 2, 3, 4\}, S_4 = S_3 \cup \{(1234), (2134), (2314), (1324), (1242), (1243), (14), (24), (34), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

Una forma intuitiva de ver los elementos es agrupar por particiones; por ejemplo para  $S_4$ , podemos agrupar  $(1, 1, 1, 1), (2, 1, 1), (3, 1), (4), (2, 2)$  donde cada número representa el número de elementos de cada subconjunto.

Proposición

Sea  $\tau \in S_n$  con  $n \in \mathbb{N}$  un ciclo de longitud  $m \in \mathbb{N}$ , también lo es su conjugado; esto es, todo elemento de la forma  $\tau \circ \tau^{-1} \forall \tau \in S_n$ . (En la definición de conjugado basta reemplazar  $\tau$  por  $\tau^{-1}$ )

-Demostración-

Sea  $\tau = (x_1, \dots, x_m)$  veremos que  $\tau \circ \tau^{-1} = (\tau(x_1), \dots, \tau(x_m))$ . Por tanto, supongamos  $y \in \{1, \dots, n\}$

entonces hay tres posibilidades

$$(i) \tau^{-1}(y) = x_i \quad i=1, \dots, m-1$$

$$(ii) \tau^{-1}(y) = x_m$$

$$(iii) \tau^{-1}(y) = x_j, x_j \neq x_i, \forall i \in \Delta_m$$

Vemos cada caso:

$$(i) \quad y \xrightarrow{\tau^{-1}} x_i \xrightarrow{\tau} x_{i+1} \xrightarrow{\tau} \tau(x_{i+1})$$

$$(ii) \quad y \xrightarrow{\tau^{-1}} x_m \xrightarrow{\tau} x_1 \longrightarrow \tau(x_1)$$

$$(iii) \quad y \xrightarrow{\tau^{-1}} x \xrightarrow{\tau} x \longrightarrow \tau(x) = y$$

Por lo tanto, se cumple lo que queríamos ver □

Vemos algunos ejemplos de conjugados

$$(i) \tau = (2453), \sigma = (134) \Rightarrow \sigma \circ \tau \circ \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} = (1542)$$

Sea  $\sigma \in S_n$  tal que  $\sigma = \sigma_1 \dots \sigma_k$ , para un  $\sigma_i$  fijo, podemos obtener el conjugado obteniendo

para cada  $\sigma_i$   $i \in \{1, \dots, k\}$  pues  $\sigma_1 \dots \sigma_k$  son ciclos que se interponen en ciclos disjuntos, es decir

$$\sigma \circ \sigma^{-1} = \sigma_1 \circ \sigma^{-1} \dots \sigma_k \circ \sigma^{-1}$$

Por ejemplo, para  $\sigma = (1 \ 12 \ 8 \ 10 \ 4)(2 \ 13)(5 \ 11 \ 7)(6 \ 9)$  y  $\sigma = (4 \ 8 \ 12 \ 7 \ 6 \ 9)$

es fácil ver que  $\sigma \circ \sigma^{-1} = (4 \ 8 \ 12 \ 7 \ 6 \ 9)(1 \ 12 \ 8 \ 10 \ 4)(2 \ 13)(5 \ 11 \ 7)(6 \ 9)(9 \ 5 \ 7 \ 12 \ 8 \ 4)$

$$\sigma \circ \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 7 & 13 & 3 & 6 & 9 & 4 & 12 & 1 & 11 & 8 & 5 & 10 & 2 \end{pmatrix} = (1\ 7\ 12\ 10\ 8)(2\ 13)(4\ 6)(5\ 9\ 11)$$

Podemos obtener  $\sigma \circ \sigma^{-1}$  usando  $\sigma \circ \sigma^{-1} = (\sigma(x_i) \dots)$

### Proposición

Toda permutación es un producto de trasposiciones.

-Demostración-

Para mostrar  $\exists x_1, \dots, x_n \in S_n$  tal que  $\sigma = \sigma_1 \dots \sigma_k$  entonces basta ver que cualquier ciclo es producto de trasposiciones.

Si  $\sigma = (x_1, \dots, x_m)$  entonces  $\sigma = (x_1, x_m)(x_1, x_{m-1}) \dots (x_1, x_2)(x_2, x_3) \dots (x_{m-1}, x_m)$   
y queda así demostrado lo pedido

↑  
!Es un producto!

□

Además esta descomposición ya la hemos visto que es única. De hecho, lo decimos que la única en común es la paridad del número de trasposiciones, es decir, si el nº de trasposiciones necesarias es par o impar.

### Signatura

Sea  $\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in \mathbb{Z}[x_1, \dots, x_n]$  y  $\sigma \in S_n$  entonces  $\sigma(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$ . Veamos un ejemplo de esto:

i)  $n=4$  y tomamos  $\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$ ,  $\sigma = (1\ 2\ 3\ 4)$

entonces  $\sigma(\Delta) = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1)$ . Aquí podemos

ver que los factores son los mismos salvo el signo de algunos de ellos.

Además, lo de el ejemplo se cumple para todo  $\sigma \in S_n$ . Definimos entonces la signatura de una permutación, que es el valor que le asigna la aplicación

$$\begin{aligned} \varepsilon : S_n &\longrightarrow \{-1, 1\} \\ \sigma &\longmapsto \varepsilon(\sigma) = \begin{cases} 1 & \text{si } \sigma(\Delta) = \Delta \\ -1 & \text{si } \sigma(\Delta) = -\Delta \end{cases} \end{aligned}$$

De esta manera, se cumple que  $\sigma(\Delta) = \varepsilon(\sigma)\Delta$  y diremos que:

1.  $\sigma$  es par si  $\varepsilon(\sigma) = 1$

2.  $\sigma$  es impar si  $\varepsilon(\sigma) = -1$

En el ejemplo dado  $\varepsilon(\sigma) = -1$  pues hay un número impar de cambios de signo

### Proposición

La aplicación  $\varepsilon : S_n \longrightarrow \{-1, 1\}$  cumple que  $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$   $\forall \sigma, \tau \in S_n$

Esta proposición nos permite verificar que la siguiente cumple la regla de los signos, es decir:

- i) par · par = par
- ii) impar · impar = par
- iii) par · impar = impar

} + - - y esas suertes

### Corolario

Las transposiciones son permutaciones impares.  $\sigma: S_n \rightarrow S_n$  si es sobreyectiva.

-Demostración:

Considerando  $\Delta$  el polinomio concreto general y  $\sigma \in S_n$ ,  $\sigma = (i\ j)$  se cumple que

- si  $(x_a - x_b) \in \Delta$  |  $(a, b) \neq (i, j)$  lo dejó falso.
- si  $(x_a - x_b) \in \Delta$  |  $(a, b) = (i, j) = \sigma(x_a - x_b) = -(x_i - x_j)$

luego necesariamente habrá un número impar de transposiciones, pues al final se compensan salvo  $(x_i - x_j)$

Dispongo de la identidad para obtener la sobredefinición

### Corolario

Dada  $\sigma \in S_n$ ,  $n \in \mathbb{N}$  se cumple la siguiente equivalencia:

$E(\sigma) = 1 \iff \sigma$  se descompone en un número par de transposiciones

$E(\sigma) = -1 \iff \sigma$  se descompone en un número impar de transposiciones

Ade más, para un ciclo de longitud  $m \geq 3$  es par si y solo si  $m$  es impar. Lógicamente, será impar cuando sea par.

Por último, un n-ciclo es producto de  $n-1$  transposiciones

### Corolario

Una permutación es par si y solo si sus n-ciclos de longitud par en su descomposición es par. Lógicamente será impar si y solo si sus n-ciclos de longitud par en su descomposición es impar.

### Como ejemplo:

- $\sigma = (1\ 2\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$  es par pues tiene 2 ciclos pares.

#### 4. El grupo alterno

Se define el grupo alterno de grado  $n \in \mathbb{N}$ , denotado por  $A_n$ , es el grupo formado por las permutaciones pares de  $S_n$ .

- El producto de permutaciones pares es par.  $\Rightarrow$  bien definido
- Neutro  $\rightarrow$  identidad
- Inverso  $\rightarrow$  sea  $\sigma \in A_n, \sigma^{-1} \in A_n$  pues tiene la misma longitud luego se mantiene la paridad
- Asociativa  $\rightarrow$  inducida de  $S_n$

Ade más, el orden del grupo alterno cumple que:

$$O(S_n) = 2 O(A_n) \quad \forall n \in \mathbb{N} \quad \rightsquigarrow \text{Biyección con los cuatros los pares}$$

Luego se tiene que  $O(A_n) = \frac{n!}{2} \quad \forall n \in \mathbb{N}$

Algunos ejemplos son:

i) Para  $n=3 \quad S_3 = \{(1), (12), (13), (23), (123), (132)\}$  luego  $A_3 = \{(1), (123), (132)\}$

ii) Para  $n=4 \quad A_4 = \{(1), (12), (123), (134), (132), (142), (143), (234), (243), (12)(34), (24)(31)\}$

12 elementos

Proposición

Para  $n \in \mathbb{N}$  dado.

a)  $S_n = \{(12), (23), \dots, (n-1\ n)\}$

b)  $S_n = \{(12), (12\dots n)\}$

c)  $S_n = \{(12), (13), \dots, (1..n)\}$

d)  $A_n = \{(x_1, x_2, x_3) \mid x \in S_n\}$

e)  $A_n = \{(1\ x_4) \mid x \in S_3\}$

- Interpretación - (vale como demostración)

a) Cada toda permutación se obtiene para un conjunto de trasposiciones cíclicas

$$S_n = \{(i\ j) \mid i, j \in \{1, \dots, n\}\}$$

Sea  $i, j$ , es fácil ver que

$$(i\ j) = (i\ i+1)(i+1\ i+2) \dots (j-2\ j-1) \dots (j-1\ j)(j-1\ j-2) \dots (i+1\ i)$$

Como ejemplo  $S_3 = \{(12), (23)\}$  pues  $(13) = (12)(23)(21)$  o  $S_4 = \{(12), (23)(34)\}$

pues  $(14) = (12)(23)(34)(32)(21)$

b)  $S_n = \{(12), (1\dots n)\}$  pues dado  $\sigma = (1\dots n)$  obtenemos  $\sigma^{i-1}(1) = i \wedge \sigma^{i-1}(2) = i+1 \quad \forall i \in \{1, \dots, n\}$

de donde deducimos que  $\sigma^{i-1}(1\ z)\sigma^{i-1}(z) = (i\ z)$ ; basta probar con cada elemento  $(i\ z)$

Además,  $\sigma^{i-i}(j) = j \quad \forall j \neq i, i+1$ .

Como ejemplo de esto tenemos que  $S_3 = \langle (12)(123) \rangle$ , pues  $(23) = (123)^2$  y  $(12) = (1234)^{-1}$ , pues  $(23) = (1234)(12)(1234)^{-1}$  y  $(34) = (1234)^2(12)(1234)^{-2}$

c)  $S_u = \langle (12)(13) \dots (1u) \rangle$  pues la permutación  $\sigma = (12 \dots u) = (1u)(1u-1) \dots (13)(12)$

d)  $A_u = \langle (x_1 x_2 x_3) \rangle$  para  $x_1 < x_2 < x_3$  y podemos suponer  $x_1 < x_2 < x_3$  pues si  $\sigma = (x_1 x_3 x_2)$  sabemos que  $\sigma = (x_1 x_2 x_3)^2$ .

Sea ahora  $\tau \in A_u$  para  $u \in \mathbb{N}$ .  $\tau$  será producto de un número par de transposiciones y distinguiremos casos:

• Si hay elementos comunes

$$(x_1 x_2)(x_3 x_4) = (x_1 x_2 x_3 x_4)^2$$

• Si no hay elementos comunes

$$(x_1 x_2)(x_3 x_4) = (x_1 x_2 x_3)(x_2 x_3 x_4)$$

Por ejemplo, para  $u=4$  tenemos que  $A_4 = \{1, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$  de donde podemos deducir que

$$A_4 = \langle (123), (124), (134), (234) \rangle$$

e)  $A_u = \langle (1 \times 1) \rangle$  con  $u \geq 3$  pues  $(x_1 x_2 x_3) = (1 x_3 x_2)(1 x_1 x_2)(1 x_1 x_3)$ ; por tanto

$$A_4 = \langle (123), (124), (134) \rangle$$

## 5 Grupos de matrices

Sea  $\mathbb{F}$  un cuerpo y  $M_n(\mathbb{F})$  las matrices cuadradas de orden n que con la suma y el producto es un anillo. Además, nos quedaremos con el grupo multiplicativo

$$G_{M_n}(\mathbb{F}) = \{A \in M_n(\mathbb{F}) \mid A \text{ tiene inversa}\}$$

dónde se cumple que

$A$  tiene inversa  $\Leftrightarrow \exists B \in M_n(\mathbb{F}) \mid AB = BA = I \Leftrightarrow \det(A) \neq 0 \Leftrightarrow$  las columnas de  $A$  son l.i.

En este caso se cumple que  $G_{M_n}(\mathbb{F})$  es el grupo general para cualquier  $n \in \mathbb{N}$ . No serán

grupos finitos pues si  $|\mathbb{F}| = k, k \in \mathbb{N}$  obtenemos que  $|G_{M_n}(\mathbb{F})| = (k^n - 1)(k^n - k) \dots (k^n - k^{n-1})$

Veamos algunos ejemplos:

1.  $GL_2(\mathbb{Z}_2) = \{(1\ 0), (1\ 1), (0\ 1), (0\ 0), (1\ 0), (0\ 1)\}$

$$|GL_2(\mathbb{Z}_2)| = (2^2-1)(2^2-2) = 6$$

2.  $GL_3(\mathbb{Z}_2)$ :

$$|GL_3(\mathbb{Z}_2)| = 168$$

3.  $GL_2(\mathbb{Z}_3)$ :

$$|GL_2(\mathbb{Z}_3)| = 48$$

Si tomamos el conjunto de las matrices con determinante 1 obtendremos el grupo lineal

general y lo notaremos por  $SL_n(\mathbb{F})$ . Dado que  $|SL_n(\mathbb{F})| = \frac{|GL_n(\mathbb{F})|}{q-1}$  si  $|F|=q$ .

Como ejemplos:

1.  $SL_2(\mathbb{Z}_2) = GL_2(\mathbb{Z}_2)$

2.  $|SL_2(\mathbb{Z}_3)| = 24$

## 6. Homomorfismos de grupos

Dados dos grupos,  $g$  y  $H$ , un homomorfismo de grupos de  $g$  en  $H$  es una aplicación  $f: g \rightarrow H$

que verifica que  $\forall x, y \in g \quad f(xy) = f(x)f(y)$ . Llamaremos dominio a  $g$  y codominio a  $H$ .

Lema.

Si  $f: g \rightarrow H$  es un homomorfismo de grupos, entonces:

i)  $f(1)=1$

ii)  $f(x^{-1}) = (f(x))^{-1} \quad \forall x \in g$

- Demostración:

i)  $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \xrightarrow{\text{Prop. canónica}} f(1) = 1$

ii)  $1 = f(1) = f(x \cdot x^{-1}) = f(x)f(x^{-1}) \Rightarrow (f(x))^{-1} = f(x^{-1})$

Veamos tener dos subconjuntos bien distinguidos

c)  $\text{Ker } f = \{x \in g \mid f(x) = 1\}, \text{Ker } f \subset g$

ii)  $\text{Im } f = \{f(x) \mid x \in g\}$

Como ejemplos de homomorfismos de grupos tenemos:

i)  $\text{Id}: g \rightarrow g, f(g)=x$

ii)  $f: g \rightarrow H$  dado por  $f(g)=1_{\text{H}} \forall g$  (homomorfismo trivial)

iii)  $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot)$  dado por  $\exp(x)=e^x \forall x \in \mathbb{R}$

iv)  $\det: GL_n(\mathbb{C}) \rightarrow \mathbb{C}^*$  dado por  $\det(A)=1 \forall A \in GL_n(\mathbb{C})$

v)  $\varepsilon: S_n \rightarrow \{-1, 1\} = \mathbb{Z}/(2\mathbb{Z})$  (signatura)  
 $\sigma \mapsto \varepsilon(\sigma)$

vi) La composición de homomorfismos de grupos es homomorfismo de grupos

Dados dos grupos  $g$  y  $H$ , la aplicación  $f: g \rightarrow H$  homomorfismo de grupos. Diremos que:

i)  $f$  es monomorfismo si como aplicación es inyectiva

ii)  $f$  es epimorfismo si como aplicación es sobreyectiva

iii)  $f$  es isomorfismo si como aplicación es bijectiva

iv) Si  $g=H$  diremos que  $f$  es endomorfismo

v) Si  $f$  es isomorfismo y endomorfismo diremos que es automorfismo

Proposición

Sea  $f: g \rightarrow H$  un homomorfismo de grupos. Entonces:

i)  $f$  es monomorfismo  $\Leftrightarrow \text{Ker } f = \{1\}$

ii)  $f$  es isomorfismo  $\Leftrightarrow f$  tiene inverso  $\Leftrightarrow \exists g: H \rightarrow g \mid fg = \text{Id}_H \wedge gf = \text{Id}_g$  y lo demostraremos por  $f^{-1}$

-Demostración-

i)  $\Rightarrow$  Si  $x \in \text{Ker } f \Rightarrow f(x)=1$  pero  $f(1)=1$ , como  $f$  es inyectiva tenemos que  $x=1$

$\Leftarrow$  Sean  $x, y \in g \mid f(x)=f(y) \Rightarrow f(x)f(y)^{-1}=1 \Rightarrow f(xy^{-1})=1 \Rightarrow xy^{-1}=1 \Rightarrow x=y \Rightarrow f$  es inyectiva

ii)  $f$  isomorfismo  $\Leftrightarrow f$  es aplicación biyectiva  $\Leftrightarrow \exists f^{-1}$  biyectiva  $\Rightarrow f$  homomorfismo

Como ser isomorfo es una relación de equivalencia podemos construir las Tablas de clasificación.

Estas tablas nos permiten saber que cualquier grupo abeliano de orden 6 es isomorfo

a  $S_3$ . Nosotros ya sabíamos que:

$$S_3 \cong D_3 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

## Proposición.

c) Si  $f: X \rightarrow Y$  biyectiva se tiene que la aplicación  $\varphi: \text{Per}_f(X) \rightarrow \text{Per}_f(Y)$  es

$$\sigma \mapsto f\sigma f^{-1}$$

un isomorfismo de grupos

- ii)  $(\text{Aut}(g), \circ)$  es un grupo ( $\circ$  es la composición) ( $\text{Aut}(g) = \text{aut}(\varphi_f(g))$ )
- iii) Si  $f$  es un isomorfismo entre  $G$  y  $H$  entonces  $|G| = |H|$
- iv) Si  $G$  y  $H$  son isomorfos  $\Rightarrow G$  es abeliano si y solo si  $H$  es abeliano
- v) Si  $f: G \rightarrow H$  isomorfismo  $\Rightarrow \forall x \in G \quad O(x) = O(f(x))$

## Ejercicio

- Demostración (ideas)

i)  $\varphi^{-1}(\sigma) = f^{-1}\sigma f \leftarrow$  Definición de  $\varphi$

$$\varphi(\sigma z) = \varphi(\sigma)\varphi(z)$$

ii) Hacerse punto

iii) Si  $f: G \rightarrow H$  biyectiva  $\Rightarrow$  mismo cardinal  $\Rightarrow$  mismo orden

iv)  $\Rightarrow \forall x, y \in H \quad xy = f(f^{-1}(xy)) = f(f^{-1}(x)f^{-1}(y)) = f(f^{-1}(y)f^{-1}(x)) = f(f^{-1}(yx)) = yx$   
porque

$\Leftrightarrow$  es igual ( $f^{-1}f$ )

v) Si  $O(x)=n, n \in \mathbb{N} \Rightarrow (f(x))^n = f(x^n) = f(1) = 1$ . Si  $f(x)^m = 1$  para algún  $m$  entonces  $x^m = 1$  y por

inyectividad tenemos que  $x=1$

Luego ser el más pequeño (hipótesis)

## Teatrero de Dyck

Sea  $G$  un grupo finito con una presentación  $g = \langle s_1, R_1, \dots, R_m \rangle$  donde  $s_i = \langle s_{i1}, \dots, s_{in_i} \rangle$ ,  $H$  otro grupo finito y  $\{r_1, \dots, r_m\} \subset H$ . Supongamos que cualquier relación satisfecha en  $G$  por los  $s_i, i=1, \dots, n$  es también satisfecha en  $H$  para los  $r_i, i=1, \dots, m$  (sustituyendo  $s_i$  por  $r_i$ )

Entonces existe un único homomorfismo de grupos  $f: G \rightarrow H$   $f(s_i) = r_i$  ( $i=1, \dots, n$ ).

Si además  $\{r_1, \dots, r_m\}$  es un conjunto de generadores de  $H$  entonces  $f$  es epimorfismo, y si  $|G| = |H|$  entonces  $f$  es isomorfismo.

(No se demuestra por falta de usabilidad)

Algunos ejemplos de aplicación son:

Grado de  $x^n = 1$

$$(i) \mathbb{C}_n = \langle x \mid x^n = 1 \rangle \Rightarrow \exists f: \mathbb{C}_n \rightarrow \mathbb{Z}_n \text{ ademas } x^{\frac{n}{d}} = 1 \Rightarrow \mathbb{Z}_n = \langle \overline{1} \rangle \text{ y ambos grupos tienen orden } n \Rightarrow \text{podemos tener un isomorfismo.}$$

iii)  $V^{\text{abs}} = \langle x, y | x^2=y^2, xy=yx \rangle$  y  $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$  podemos

tenemos  $f(x)=(0,1)$ ,  $f(y)=(1,0)$  y  $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,1), (1,0)\}$

Además,  $V = \langle (12)(34), (13)(24) \rangle = \{(1, (12)(34)), (13)(24), (14)(23)\}$

Luego  $V^{\text{abs}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$

iv)  $D_3 = \langle r, s | r^3=1, s^2=1, sr=r^2s \rangle$

$$\begin{array}{ccc} D_3 & \longrightarrow & S_3 \\ r & \longmapsto & (123) \\ s & \longmapsto & (12) \end{array}$$

y se cumple todo y  $S_3 = \langle (12)(123) \rangle \Rightarrow$  como  $|D_3|=|S_3|$  son isomorfos

v)  $g_{\text{ab}}(\mathbb{Z}) = \{(10), (10), (10), (10), (10), (10)\}$

pues  $r^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \wedge s^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \wedge (10)(10) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Por tanto,  $g_{\text{ab}}(\mathbb{Z}) \cong S_3$

vi) En general  $D_n$  y  $S_n$  no serán isomorfos pues  $|D_n| \neq |S_n|$  pero tenemos un isomorfismo con la asignación  $f(r) = (123 \dots n)$ ,  $f(s) = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}$

vii)  $Q_2^{\text{abs}} = \langle x, y | x^4=1, y^2=x^2, yxy^{-1}=x^{-1} \rangle$

$$f: Q_2^{\text{abs}} \longrightarrow Q_2 = \langle i, j | \rangle = \{\pm 1, \pm i, ij, \pm u\}$$

$$x \longmapsto i$$

$$y \longmapsto j$$

Como  $|Q_2^{\text{abs}}| = |Q_2|$  entonces son isomorfos.

$H = \{z = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, i = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, j = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, u = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\} \subseteq g_{\text{ab}}(\mathbb{C})$  cumple que  $Q_2^{\text{abs}} \cong H$

pues  $g: Q_2^{\text{abs}} \longrightarrow H$

$$x \longmapsto i$$

$$y \longmapsto j$$

viii) Sea  $k \geq 3$  una tenemos que  $f: D_k \rightarrow D_k$  es un epimorfismo

Si  $D_k = \langle r, s | r^k=1, s^2=1, rs=sr^{-1} \rangle$  y  $D_k = \langle r_1, s_1 | r_1^{k-1}, s_1^2=1, r_1s_1=s_1r_1^{-1} \rangle$

$$\begin{array}{ccc} g: D_k & \longrightarrow & D_k \\ r & \longmapsto & r_1 \\ s & \longmapsto & s_1 \end{array}$$