teoría de grupos

1. Definición de grupos y propiedades

Un grupo es un conjunto G en el que hay definida una operación interna que verifica tres propiedades:

grupo
- i) Asociativa
- ii) Existencia de un elemento neutro (e)
- iii) Todo elemento tiene inverso

Además, se dice que el grupo es abeliano cuando se verifica que:

- iv) El orden de la operación no influye en el resultado

conjunto

$$\boxed{G} \times G \xrightarrow{\circledast} G$$

$a \quad b \qquad\qquad a * b$

$(G,+)$ $e = 0$ $a^{-1} = -a$ (opuesto)

$\circledast$ operación: siempre está definida y el resultado es único

Las tres propiedades cumple:

i) asociativa: $(a * b) * c = a * (b * c) = a * b * c$ (no es necesario el paréntesis)

↑ consecuencia

ii) $\exists e \in G / \begin{cases} a * e = a \\ e * a = a \end{cases} \quad \forall a \in G$ → para todo elemento de G

iii) Cuando hay elemento neutro, se define el inverso de un elemento $a \in G$, a^{-1} como aquel que cumple $a * a^{-1} = e$

$a^{-1} * a = e$

$\forall a \in G \; \exists a^{-1} \in G / \begin{cases} a * a^{-1} = e \\ a^{-1} * a = e \end{cases}$ no tiene por qué ser conmutativo

iv) Además, G es un grupo abeliano (propiedad conmutativa), cuando:

$a * b = b * a \quad \forall a, b \in G$

ejemplo:

$(\mathbb{R}, +)$

1) Asociativo $(17 + e) + 2 = 17 + (e + 2)$
2) elemento neutro $\rightarrow 0$
3) existe inverso
4) Conmutativo $(17 + e) + 2 = (2 + 17) + e$

} Grupo abeliano

$(\mathbb{Q}, +)$ gr. abeliano

$(\mathbb{Z}, +)$ gr abeliano

$(\mathbb{N}, +)$ no es grupo, no cumple que tenga inverso, salvo el 0

incluimos el 0

$(\mathbb{R}, *)$

i) Asociativo $(e * 17) * 6 = e * (17 * 6)$
ii) elemento neutro $\rightarrow 1$
iii) si tienen inverso
iv) es conmutativo $e * 17 = 17 * e$

} grupo abeliano

→ Propiedades

1) Propiedad cancelativa

$a * b = a * c \Rightarrow a * b$ (por la izquierda) $\qquad b * a = c * a \Rightarrow b = c$ (por la derecha)

demostración: $a * b = a * c$

$(a^{-1} * a) * b = (a^{-1} * a) * c$ ⇝ cancelada por la izq.

$e * b = e * c \rightarrow b = c$

2) El elemento neutro es único

demostración: supongamos que hay dos elementos neutros e, f

$e = e * f = f$

3) el inverso es único para cada elemento

demostración: supongamos que $a \in G$ tiene dos inversos $a' = a''$,

entonces $a' * a = e = a'' * a$

aplicando la propiedad cancelativa $a' = a''$

4) $(a^{-1})^{-1} = a$ $a \in G$ entonces existe $a^{-1} \in G$ entonces existe $(a^{-1})^{-1} \in G$, ect

demostración: por un lado $a * a^{-1} = e = \underbrace{(a^{-1})^{-1} * a^{-1}}_{a}$

aplicando la propiedad cancelativa se obtiene que $a = (a^{-1})^{-1}$

5) $(a * b)^{-1} = b^{-1} * a^{-1}$ $\rightsquigarrow \frac{1}{a*b} = b^{-1} * a^{-1}$, $b^{-1} * a^{-1} * a * b$

demostración: vamos a demostrar que $b^{-1} * a^{-1}$ es el inverso de $a * b$

$$b^{-1} * a^{-1} * a * b = b^{-1} * e * b = b^{-1} * b = e$$
$$a * b * b^{-1} * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$$
$$\Big\} (a*b)^{-1} = b^{-1} * a^{-1}$$

ejemplos

1) Matrices cuadradas con determinante distinto de cero, de tamaño n

El grupo lineal $GL(n) = \{A \in M_n(\mathbb{R}) / |A| \neq 0\}$

$B = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}$ $GL(2)$ $\begin{vmatrix} 1 & 2 \\ 3 & 0 \end{vmatrix} = -6 \neq 0$

1) ABC es asociativo

2) hay una matriz especial $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, llamada matriz identidad

$AI = A$ $IA = A$ $\forall A \in GL(2)$

3) toda matriz tiene inverso

$B^{-1} = \frac{1}{|B|} \cdot (B^{ij})^t$ $B^{-1} = -6 \begin{pmatrix} 0 & -3 \\ -2 & 1 \end{pmatrix}$ $B \cdot B^{-1} = I$ $B^{-1} \cdot B = I$

4) No es abeliano

$$C=\begin{pmatrix}1 & -1\\ 0 & 2\end{pmatrix} \qquad D=\begin{pmatrix}0 & 2\\ -1 & 3\end{pmatrix}$$

$$CD=\begin{pmatrix}1 & -1\\ 0 & 2\end{pmatrix}\begin{pmatrix}0 & 2\\ -1 & 3\end{pmatrix}=\begin{pmatrix}1 & -1\\ -2 & 6\end{pmatrix}$$

$$DC=\begin{pmatrix}0 & 2\\ -1 & 3\end{pmatrix}\begin{pmatrix}1 & -1\\ 0 & 2\end{pmatrix}=\begin{pmatrix}0 & 4\\ -1 & 7\end{pmatrix}$$

} No hay conmutividad

2) Congruencias módulo $n \in \mathbb{N}$ $[n \geq 2]$

Tenemos $\mathbb{Z}$. Vamos a agrupar los enteros en subconjuntos de tal manera que 2 números estén en el mismo subconjunto cuando al dividirlos por n, el resto es el mismo

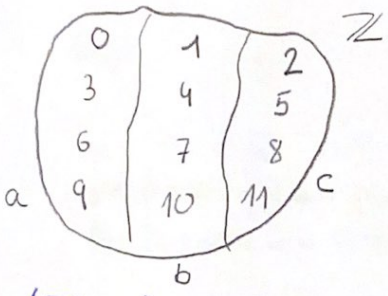
Es decir, $a, b \in \mathbb{Z}$

$a \sim b$ (relacionado) cuando $\begin{cases} a = c_1 n + r_1 \\ b = c_2 n + r_2 \end{cases}$ (cociente) $\qquad r_1 = r_2$

$a - b = \dot{n}$ (múltiplo)

$$a \sim b = a - b = c_1 n + r_1 - (c_2 n + r_2) = (c_1 - c_2) n = \dot{n}$$

ejemplo: $\mathbb{Z}_3$ $n=3$



$n = 3$ - divisor

$0 = 0 \cdot 3 + 0$

$1 = 0 \cdot 3 + 1$

$2 = 0 \cdot 3 + 2$ (resto)

$3 = 1 \cdot 3 + 0$

$4 = 1 \cdot 3 + 1$

(cociente)

$\vdots$

0 | 3

0 0

$\mathbb{Z}_3$ es el conjunto de los subconjuntos (clases) que se han formado

$\bar{6}$ representa a un conjunto de subconjuntos (=clases) representantes de 6 $= \bar{0}, \bar{3}, \bar{6}, \bar{9}$

$(\mathbb{Z}, +)$ $n = 3$

$\mathbb{Z}_3 \times \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$

$a \quad b \qquad a, b, c$

$\bar{6} = \bar{0}$ * $\qquad \bar{4} \qquad \bar{6} + \bar{4} = \bar{10}$

$\bar{11} \qquad \bar{11} \qquad \bar{9} + 7 = \bar{16}$

$\bar{9} \qquad \bar{7}$

} $10 - 16 = -\dot{6} = -2 \cdot 3$

↑ multiplo de n

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \bar{3} \dots n-\bar{1}\}$ $\quad n = \dot{0}$, $n - 0 = \dot{n}$

$n - 1 \neq \bar{0}$

$n - 1 - 0 = n - 1 \neq \dot{n}$

$\mathbb{Z}_2 = \{\bar{1}, \bar{2}\} = \{\bar{8}, \bar{9}\} = \{-\bar{1}, \bar{4}\}$

→ ejemplo

$(\mathbb{Z}_n, +)$

$$\begin{array}{ccccc} \mathbb{Z}_n & \times & \mathbb{Z}_n & \xrightarrow{+} & \mathbb{Z}_n \\ \bar{a} & & \bar{b} & & \overline{a+b} \end{array}$$

¿está bien definido? La operación está bien definida cuando la operación no depende de los representantes

dem: sea $\begin{cases} \bar{a} = \bar{c} \\ \bar{b} = \bar{d} \end{cases}$ queremos ver que $\overline{a+b} = \overline{c+d}$

entonces... $a - c = \dot{n} = \alpha n$

$b - d = \dot{n} = \beta n$ $\quad \alpha, \beta \in \mathbb{Z}$

luego... $a + b - (c+d) = a - c + b - d = \alpha n + \beta n = \alpha + \beta (n)$

$\alpha + \beta \in \mathbb{Z}$ operación interna

Por lo tanto este grupo es abeliano por:

i) Operación interna
ii) asociativa
iii) elemento neutro (0)
iv) opuesto $\bar{a} = -\bar{a}$

} grupo conmutativo

quitamos al cero

→ ejemplo 2 $(\mathbb{Z}^{*}_{n}, \cdot)$

$(\mathbb{Z}, \cdot)$ esto NO es un grupo porque el 0 no tiene inverso

$$\mathbb{Z}_{\bar{a}} \times \mathbb{Z}_{\bar{b}} \xrightarrow{\cdot} \mathbb{Z}_{\overline{a \cdot b}}$$

* Lo que quiero llegar a demostrar es: $\overline{a \cdot b} = \overline{c \cdot d}$

i) Demostramos que está bien definido

representante

$\bar{a} = \bar{c}$, $\bar{b} = \bar{d}$

$\bar{a} - \bar{c} = \alpha n$

$\bar{b} - \bar{d} = \beta n$ $\quad \alpha, \beta \in \mathbb{Z}$

$a \cdot b = c\,d$, $a \cdot b - c\,d = (c + \alpha n)(d + \beta n) - cd =$

$= \cancel{cd} + c\beta n + \alpha n d + \alpha n \beta n - \cancel{cd} = \boxed{(\beta c + \alpha d + \alpha \beta n) n} \in \mathbb{Z}$

Por lo tanto... $\overline{a \cdot b} = \overline{c \cdot d}$

ii) Es un grupo asociativo

iii) Existe un elemento neutro $\bar{1}$

iv) Tiene inverso en $\mathbb{Z}^{*}$

$(\mathbb{Z}^{*}_{p}, \cdot)$ grupo abeliano p nº primo

3) Permutaciones de n elemento $P_n = n!$

Una permutación es una reordenación de n elementos

$n=4$ S_4

$P_4 = 4!$

	notación clásica	notación cíclica	ℓ (longitud de un ciclo) nº de elmtos. que tiene el ciclo
	$i=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$	i	
	$\alpha=\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}$	$\alpha=(1\ 3\ 4\ 2)$ 1 ciclo	$\ell=4$
	$\beta=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$	$\beta=(1\ 4\ 3)$ 1 ciclo	$\ell=3$
	$\gamma=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$	$\gamma=(1\ 2)(3\ 4)$ 2 ciclos	$\ell_1=2\ \ell_2=2$
	$\pi=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$	$\pi=(2\ 4\ 3)$ 1 ciclo	$\ell=3$

→ Las permutaciones como grupo

$\lambda = \beta \circ \alpha = \begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$ notación clásica

$\lambda = \beta \circ \alpha = (1\ 4\ 3)(1\ 3\ 4\ 2) = (2\ 4)$ 1 ciclo $\ell=2$ transposición por ser de longitud 2

→ Esto es una composición que es una operación interna, asociativa, tiene un elemento neutro y un elemento inverso

→ elemento inverso $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = i$

$\alpha^{-1} = \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}$

$\alpha \circ \alpha^{-1} = \begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&2\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} i$

S_8 $\alpha = (2\ 5\ 7\ 1\ 3)(6\ 8)$ · $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 2 & 4 & 7 & 8 & 1 & 6 \end{pmatrix}$] ciclos disjuntos

$\beta = (5\ 4\ 2\ 8)(2\ 3\ 4\ 1\ 7)(3\ 2)(1\ 8\ 7\ 5\ 3)$] ciclos no disjuntos

$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 7 & 1 & 3 & 6 & 4 & 8 \end{pmatrix} = \underbrace{(1\ 5\ 3\ 7\ 4) = (3\ 7\ 4\ 1\ 5)}_{\text{ciclos iguales}}$

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

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

$S_2 = \{1, 2\}$

$\alpha \cdot \alpha = \alpha^2 = (2\ 5\ 7\ 1\ 3)(6\ 8)(2\ 5\ 7\ 1\ 3)(6\ 8)$

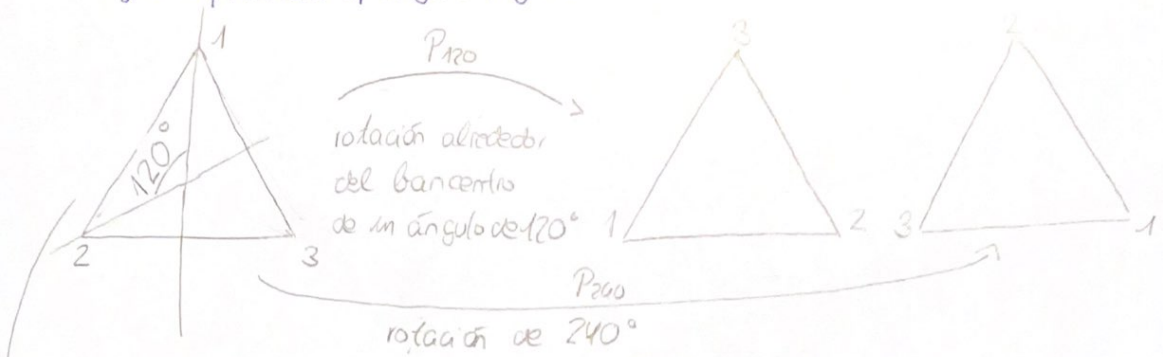
Propiedades:

1) No es abeliano
2) ciclos disjuntos conmutal S_{22}

ejemplo 4: Grupo Dihédrico

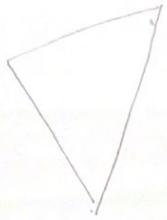
Son las simetrías de un polígono regular de n lados (D_n)

i) triángulo equilátero (polígono regular de tres lados



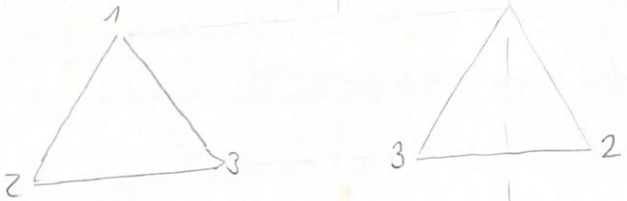
* Una simetría es un movimiento que deja la figura invariante

Rotación de 60° no es una simetría

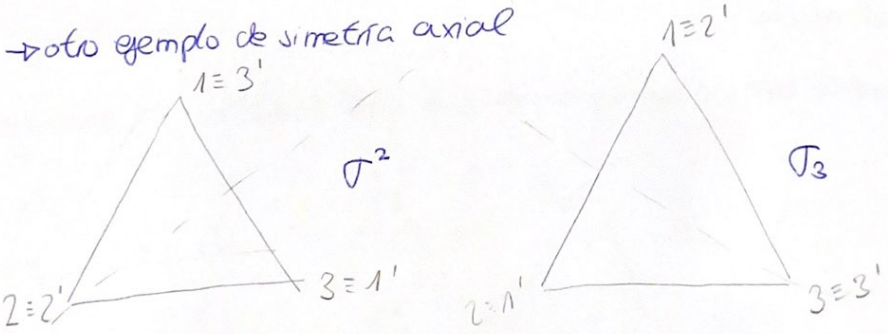


* un ejemplo trivial, es la identidad I.

* Simetría especular o axial σ_1



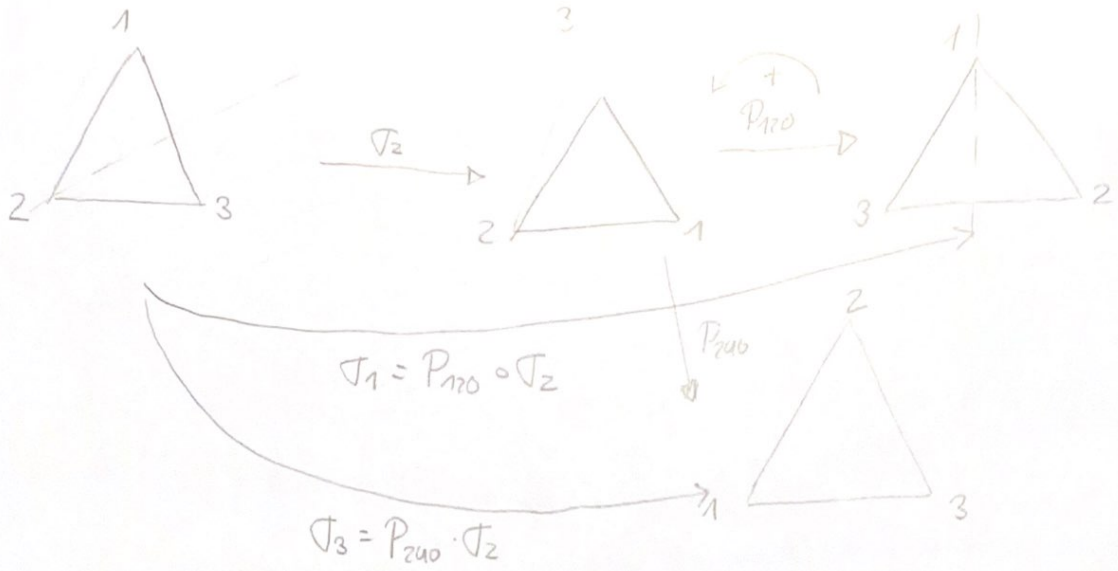
→ otro ejemplo de simetría axial



$D_3 = \{ I, P_{120}, P_{240}, \sigma_1, \sigma_2, \sigma_3 \}$

estos elementos se operan componiendo uno detrás de otro

ejemplo de operación



La operación de componer es interna

¡¡¡ con una simetría y las rotaciones, se consiguen otras simetrías

esto permite utilizar la siguiente descripción de este conjunto

$$D_3 = \{ I, P, P^2, \sigma, P\sigma, P^2\sigma \}$$

Además, la composición es asociativa (como con las funciones)

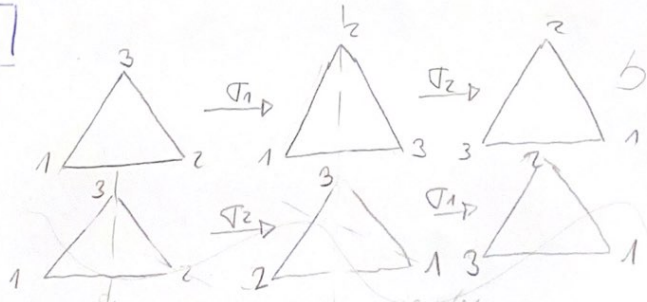
$$(f \circ g) \circ h = f \circ (g \circ h)$$

La identidad es el neutro $P^3 \circ P^2 = I$

Toda simetría tiene su inverso $P^{-1} = P^2$ $\sigma^{-1} = \sigma$ $(P^2)^{-1} = P$

D_3 es grupo

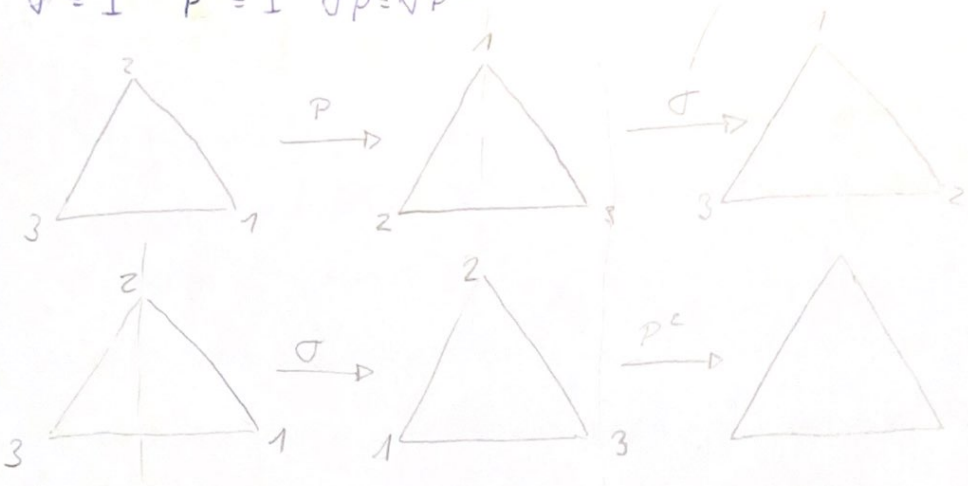
¿es abeliano?
conmutativo



no es abeliano !!! a ojo tendrían que ser iguales

Podemos observar las siguientes relaciones

$\sigma^3 = I \quad \rho^2 = I \quad \sigma\rho = \sigma\rho^2$



2a tabla del grupo

$1^o \backslash 2^o$	I	ρ	ρ^2	σ	$\rho\sigma$	$\rho^2\sigma$
I	I	ρ	ρ^2	σ	$\rho\sigma$	$\rho^2\sigma$
ρ	ρ	ρ^2	I	$\rho\sigma$	$\rho^2\sigma$	σ
ρ^2	ρ^2	I	ρ	$\rho^2\sigma$	σ	$\sigma\rho$
σ	σ	$\sigma\rho$	$\sigma\rho^2$	I	$\sigma\rho$	$\sigma\rho^2$
$\rho\sigma$	$\rho\sigma$	$\sigma\rho^2$	σ	$\sigma\rho^2$	I	$\sigma\rho$
$\rho^2\sigma$	$\rho^2\sigma$	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho$	I

$X = \sigma\rho^2 = \sigma \cdot \rho\rho = \rho^2 \cdot \sigma \cdot \rho =$

$= \rho^2\rho^2\sigma = \rho^4\sigma = \rho\sigma$

$Y = \rho\sigma\rho^2\sigma = \rho\rho^2\sigma\rho\sigma = \rho^3\rho^2\sigma\sigma =$

$= \rho^2$

$= \rho\sigma\sigma\rho = \rho\sigma^2\rho = \rho^2$

$Z = \sigma\rho = \rho^2\sigma$

~~$\sigma\rho^2 = \sigma\rho^2\sigma$~~

* Si el grupo fuese abeliano la tabla sería simétrica respecto de la diagonal principal

* En una fila o columna están todos los elementos sin repetirse

$A^3 = I$, $B^2 = I$ e $B \circ I = A^2 \circ B$

Subgrupos

Dado un grupo G y un subgrupo H de G, diremos que H es un subgrupo de $(G, *)$, y escribiremos $(H, *) \leq (G, *)$. si H es un grupo con respecto a la operación $*$ definida en G.

Como la operación es asociativa en G, también será asociativa en H de G.

$(H, *)$ es un subgrupo de $(G, *)$ si cumple las siguientes condiciones:

i) $*$ es cerrada en H.

ii) el neutro de G pertenece a H.

iii) si $x \in H$, su inverso x^{-1} también pertenece a H.

ejemplo 1: $(\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Q}, +)$ y este, a su vez, es un subgrupo de $(\mathbb{R}, +)$

ejemplo 2: $(\mathbb{Q}^*, \cdot)$ es un subgrupo de $(\mathbb{R}^*, \cdot)$ se ha eliminado el 0

ejemplo 3: si $n\mathbb{Z}$ es el conjunto de los múltiplos enteros del número natural n, es decir $n\mathbb{Z} = (nx : x \in \mathbb{Z})$, se tiene que $(n\mathbb{Z}, +)$ es un subgrupo $(\mathbb{Z}, +)$

* Todo grupo G, posee al menos dos subgrupo: el formado por el neutro de G y el subgrupo formado por todos los elementos de G

ejemplo 4: $(\mathbb{Z}_4, +)$ $\quad \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\bar{1} + \bar{1} = \bar{2} \in H$, $\bar{3} + \bar{3} = \bar{2} \in H$, $\bar{3} + \bar{3} + \bar{3} + \bar{3} = \bar{0} \in H$

Teorema:

Sea $(G, *)$ un grupo y H un subconjunto de G

$H \leq G \iff \forall x, y \in H \quad x * y^{-1} \in H$!

suponemos...

$\Rightarrow \forall x, y \in H$ por hipótesis $y^{-1} \in H$, por tanto $x * y^{-1} \in H$

suponemos que se cumple la última parte de la proposición

$x \in H$, $x * x^{-1} = e \in H$, como $e \in H$, $e * x^{-1} = x^{-1} \in H$

finalmente, si $x, y \in H$, $y^{-1} \in H$ y entonces $x * y = x * (y^{-1})^{-1} \in H$.

Como se cumple las propiedades de un subgrupo, queda comprobado que

$(H, *)$ es un subgrupo de $(G, *)$

ejercicio 14 demostrar que son $(G, *)$

$h \in G$, $C_h = \{ g \in G / g * h = h * g \}$ centralizador de h

todos los elementos que conmutarán

$\Rightarrow$ Tenemos que demostrar $C_h \leq G \ \forall h \in G$

Sea $x, y \in C \quad x * y^{-1} \in C_h$

$x * y^{-1} * h = h * x * y^{-1}$:

$y \in C_h \quad y h = h y \Rightarrow h y^{-1} = y^{-1} h$ *

$\Rightarrow x y^{-1} h = x h y^{-1} = h x y^{-1}$

$x \in C_h$

23,15
31 +€

Teorema: G finito

El orden de un elemento $x \in G$ es el menor número natural / $x^n = e$

Sea $k \in \mathbb{N}$. Si $x^k = e \Rightarrow n \mid k$, $k = \dot{n}$. $k = \lambda n \ \lambda \in \mathbb{Z}$

orden

dem: $\langle x \rangle = \{x, x^2, x^3, \dots x^{-1}, x^{-2}, \dots\}$

como G finito, en algún punto se repiten $x^l = x^r$, $l \neq r$, $l > r$

luego, $x^{l-r} = x^0 = e$. Hay una potencia de x que alcanza el neutro (e)

Entonces, definimos n como el menor número que tiene esa propiedad

entonces... $\langle x \rangle = \{x, x^2, x^3, \dots, x^n = e, x^{-1}, x^{-2}, \dots\}$

Además, dividiendo en $\mathbb{N} \subset \mathbb{Z}$ se tiene que $-1 = (-1)\,n + r \quad 0 \leq r < n$

$-3 = -1 \cdot 5 + 2$ tiene $r > 0$ $\quad -3 \mid 5$; $-2 \quad -1$

$x^{-1} = x^{-1 \cdot n + n(-1)} = (x^n)^{-1} \cdot x^{n-1} = e x^{n-1} = x^{n-1} \quad n - 1 > 0$

$-k = c \cdot n + r \quad 0 \leq r < n \quad x^{-k} = x^{cn+r} = (x^n)^c x^r = e x^r = x^r \quad n > r \geq 0$

luego... $\langle x \rangle = \{x, x^2, x^3, \dots x^n = e\}$

$|x| = |\langle x \rangle| = n$

- Si $x^k = e$, por definición $k > n$

Dividimos en $\mathbb{Z}$ $k = cn + r \quad 0 \leq r < n$

$e = x^k = (x^n)^e x^r = e x^r = x^r$

r también lleva x al neutro y es más pequeño que n $\Rightarrow r = 0$,

entonces $k = c \cdot n$

el orden de un elemento divide a cualquier elemento múltiplo del mismo

16 G abeliano $a, b \in G$ $|a| = m$ $|b| = n$

mcm(m,n)

$(m,n) = 1$ son primos entre sí

dem. $|ab| = mn$ ← esto es lo que hay q demostrar

$(ab)^{mn} = a^{mn} \cdot b^{mn} = (a^m)^n (b)^{nm} = e^n e^n = e$ → esto no nos asegura que el orden sea el menor número natural

esto me hace que tenga que recurrir

Sea h el menor n^o / $(ab)^h = e$ ($h = |ab|$)

$e = a^h b^h$

$$\begin{cases} e = e^m = (ab)^{hm} = (a^m)^h b^{mh} = e b^{mh} = b^{mh} \\ n \mid mh \Rightarrow n \mid h \end{cases}$$

→ $m \cdot h$ es múltiplo de n

$$\begin{cases} e = e^n = (ab)^{hn} = a^{hn} (b^n)^h = a^{hn} e = a^{hn} \\ m \mid nh \Rightarrow m \mid h \end{cases}$$

(el orden de $A(m)$ divide a hn)

$h = mcm(m,n) = m \cdot n$ (Teoría de nº)

demostración de teoría de números

$a \mid xy$ $(a,x) = 1 \Rightarrow a \mid y$

$xy = \lambda a$ ↑ los factores primos de x están en λ $\lambda = mx$ $(a,x) = 1$

$\lambda \in \mathbb{Z}$

Th. fundamental de la aritmética (TFA)

mcd mcm

$(m,n)[m,n] = (m,n)$

luego...

calcula los órdenes $\mathbb{Z}_8, S$

teorema de La Grange (1736-1813)

$(G, \cdot)$ grupo

Def: El orden de un grupo $|G|$ es el número de elementos que tiene

ejemplo:

$|GL(n)| = \infty$

$|\mathbb{Z}(n)| = n$

$|S_n| = n!$

$|D_3| = 6 \longrightarrow |D_n| = 2n \qquad |D_4| = 8$

def: unos elementos del grupo $(x_1, x_2, \dots, x_k) \in G$ generan el grupo cuando al operarlos entre sí de cualquier manera se obtienen todos los demás $G = \langle \{x_1, x_2, x_3, \dots x_k\} \rangle$

ejemplo:

- $\mathbb{Z}_8$ $\{\bar{2}\}$ $\bar{2}, \bar{2}+\bar{2} = \bar{4}, \bar{2}+\bar{2}+\bar{2} = \bar{4}+\bar{2} = \bar{6}, \bar{2}+\bar{2}+\bar{2}+\bar{2} = \bar{0}$

  $\{\bar{3}\}$ $\bar{3}, \bar{3}+\bar{3} = \bar{6}, \bar{3}+\bar{6} = \bar{1}, \bar{3}+\bar{1} = \bar{4}, \bar{3}+\bar{4} = \bar{7}, \bar{3}+\bar{7} = \bar{2},$

  $\bar{3}+\bar{2} = \bar{5}, \bar{3}+\bar{5} = \bar{0}$

  $\{\bar{3}, \bar{6}, \bar{1}, \bar{4}, \bar{7}, \bar{2}, \bar{5}, \bar{0}\} = \mathbb{Z}_8 = \langle \bar{3} \rangle$ $\quad \mathbb{Z}_8 = \langle \bar{5} \rangle$

- $D_3 = \{\rho, \rho^2, i, \sigma, \rho\sigma, \rho^2\sigma\}$ no es cíclico

  $\rho, \rho^2, \rho^2 \circ \rho = \rho^3 = i, \rho \circ i = \rho, \quad \langle \rho \rangle \neq D_3$

  $\langle \{\rho, \sigma\} \rangle = \{\rho, \sigma, \rho^2, i, \rho\sigma, \rho^2\sigma\} = D_3$

def: G cíclico cuando está generado por un solo elemento

$G = \langle x \rangle$ el resto no genera grupo

G cíclico $\Rightarrow$ G abeliano

$G = \langle x \rangle = \{x, x^2, x^3, \dots x^{-1}, x^e\}$

$x^n \cdot x^k = x^{n+k} = x^k \cdot x^n \Rightarrow$ por esto es abeliano

Observación: todo elemento genera un subgrupo

$\langle x \rangle = \{x, x^2, x^3, \dots x^{-1}, x^{-2}, \dots\}$

ejemplo:

$S_4 \quad \sigma = (1,2\,4)$

$\langle \sigma \rangle = \{(1\,2\,4), (1\,4\,2), i\} \leq S_4$

$\sigma \cdot \sigma = (1\,2\,4)(1\,2\,4) = (1\,4\,2)$

$\sigma \cdot \sigma^2 = (1\,2\,4)(1\,4\,2) = i$

$\sigma^2 \sigma = (1\,4\,2)(1\,2\,4) = i$

$\sigma^2 \cdot \sigma^2 = (1\,4\,2)(1\,4\,2) = (1\,2\,4)$

def: el orden de un elemento $|x|$ es el orden del grupo generado por él

$|x| = |\langle x \rangle|$

ejemplo: $\mathbb{Z}_8$

$\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{6}, \bar{0}\} \quad |\bar{2}| = 4 \quad |\bar{3}| = 8 \quad |\bar{5}| = 8$

- $S_4 \quad |\sigma| = 3$
- $D_3 \quad |\rho| = 3 \quad |\sigma| = 2 \quad |\rho\sigma| = 2$

10 compre...

$\langle \rho \rangle = \{\rho, \rho^2, i\} \quad \langle \sigma \rangle = \{\sigma, \sigma^2\}$

- $(\mathbb{Z}, +) \quad |\mathbb{Z}| = \infty$ No

teorema de Lagrange:

El orden de un subgrupo H divide al orden del grupo G

división exacta

$$|H| \,\big|\, |G|$$

dem:

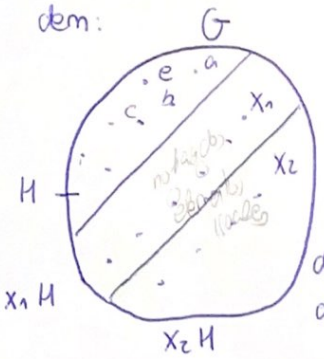


diagrama de Venn

H_1

sea $x_1 \notin H$ y forma $\{x_1 h \,/\, h \in H\}$

Sea $x_2 \notin H, x_1 H$ y forma $\{x_2 h \,/\, h \in H\}$.

hasta que no haya más elementos libres

$H, x_1 H, x_2 H, \ldots, x_k H$

Estos subconjuntos forman una partición:

1) La unión es el total

2) Son disjuntos: sea $a \in x_1 H$ y $b \in x_2 H$

si fueran iguales $x_1 \cdot h = a = b = x_2 h'$

entonces $x_1 \underbrace{h (h')^{-1}}_{\in H} = x_2 \Rightarrow x_2 \in x_1 H$ contradicción

Además cada subconjunto tiene el mismo número de elementos, porque no tiene elementos repetidos.

Supongamos que $a, b \in x_1 H$ son iguales

$x_1 h = a = b = x_1 h' \Rightarrow h = h'$

propiedad cancelativa

Sea $x_1 h$ y $x_1 h'$ distintos, luego $h \neq h'$

entonces NO pueden ser iguales:

$x_1 h = x_1 h' \Rightarrow h = h'$ contradicción

con esto... → partición

$|G| = |H| + |x_1 H| + |x_2 H| + \ldots + |x_k H|$

$|G| = |H| + |H| + |H| + \ldots |H| \rightarrow |G| = n \cdot |H| \quad |H| \,\big|\, |G|$

también hay otra partición...

$H, Hy, Hy_2, \cdots, Hy_k$

obs: $|x|/|G|$

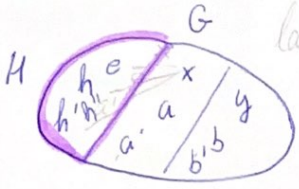
ej: $|D_3| = 6$

$|\mathbb{Z}_8| = 8$

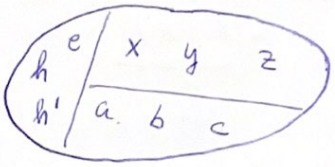
$|x| = \{1, 2, 4, 8\}$

Subgrupos normales

$(G, \circ)$ grupo $H \leq$ subgrupo h.



las particiones son disjuntas



$[G:H] = 3$

$Hx = Hy = Hz$

$Ha = Ha' = Hb$

$H \quad xH = \{xh / h \in H\}$ y H adjuntos por la derecha

$aH = a'H \quad bH = b'H$

$H \quad Hx = \{hx / h \in H\}$ Ha adjuntos por la izquierda

Def: el índice de un subgrupo H, es el número de particiones a las que da lugar $[G:H]$

* queremos identificar los elementos de una misma partición o subconjuntos:
  - → Queremos manejarlos como si fueran uno solo, es decir, queremos operar con ellos como si fueran uno solo
  - → Queremos dar una estructura de grupo a las particiones, a los adjuntos:

$$xH * yH = xyH = \{xyh / h \in H\}$$

¿con esta operación sale un grupo?

1) ¿es una operación interna? Sí porque operamos en G

2) Es asociativa

$$(xH * yH) * zH = xyH * zH = xyzH$$

$$xH * (yH * zH) = xH * yzH = xyzH$$

3) Hay elemento neutro

$$eH = H \qquad eH * xH = exH = xH$$

$$eH = \{eh / h \in H\} = H$$

4) Hay elemento inverso

$$(xH)^{-1} = x^{-1}H \qquad xH * x^{-1}H = xx^{-1}H = eH = H$$

$$x^{-1}H * xH = x^{-1}xH = eH = H$$

- Esta definición DEPENDE de los elementos en determinar los adjuntos.

Es decir. $xH = aH$

Como $a \in xH$ quiere decir que $a = xh$

Luego si formemos aH vuelve a salir los elementos de xH $ah'' = \underbrace{xhh''}_{H} \in xH$

- Pero entonces si usamos otros elementos para fijar los adjuntos ¿el resultado será igual?

si $xH = aH$; $yH = bH$ $\quad xH * yH = xyH$ $\quad$ ¿es $xyH = abH$?

$$aH * bH = abH$$

En general no hay solución, es decir no hay manera de arreglarlo. Es decir esto no se puede hacer.

Entonces, al revés, vamos a poner condiciones sobre H, para que esto tenga sentido.

Vamos a ver el problema más detalladamente:

$$xH * yH = xyH$$

$$\left.\begin{array}{l} a \in xH,\ aH = xH,\ a = xh \\ b \in yH,\ bH = yH,\ b = yh' \end{array}\right\}$$

$$aH * bH = abH = xhyh'H = xyh''h'H = xyH = xH * yH$$

$h \in H$; $=$; $\uparrow$?

$\forall y$ si pedimos $Hy = yH$ estamos pidiendo que

$$hy \in yH$$

es decir que $hy = yh'''$

↑ podemos intercambiar la y i poo con distinto $h \in H$

En resumen, si pedimos que las clases adjuntas por la derecha sean iguales que las clases adjuntas por la izquierda tendrás bien definida la operación

definición: $(G, *)$ grupo $H \leq G$

H es normal cuando sus adjuntos por la derecha coinciden con sus adjuntos por la izquierda.

$H \trianglelefteq G$ cuando $xH = Hx \quad \forall x \in G$

observación ⓪J⓪ $xh \in Hx$ es decir $xh = h'x$

o sea x "conmutan" con los elementos de H

definición: $(G, \cdot)$ grupo $H \trianglelefteq G$ subgrupo normal

El grupo cociente es $(G/H, *)$

*Criterios para identificar los subgrupos normales (H tiene que ser subgrupo)

i) $xHx^{-1} \in H$

dem: $H \trianglelefteq G$; $xH = Hx$ como conjuntos; entonces $xHx^{-1} = H$

ii) Si H es el único subgrupo con su número de elementos entonces es normal

dem: xHx^{-1} es un subgrupo: $xHx^{-1} = \{xhx^{-1} / h \in H\}$

$|xHx^{-1}| = |H|$ *

$xHx^{-1} = H$

$xhx^{-1}(xh'x^{-1})^{-1} = xhx^{-1}xh''x^{-1} =$

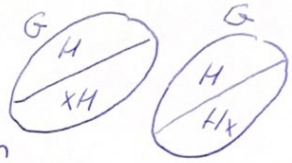
$= xh'''x^{-1} \in xHx^{-1}$

↳ contradicción porque eran elementos distintos

* son elementos distintos $xhx^{-1} = xh'x^{-1} \Rightarrow h = h'$

iii) $[G : H] = 2 \Rightarrow H \trianglelefteq G$, con esta condición NO se demuestra que H sea grupo. Es que a partir de que H es grupo, si el índice es dos entonces es normal

dem: si el índice es 2 es porque solo tiene H, xH como clases adjuntas por la derecha y por la izquierda tiene a H, Hx. En el dibujo se ve que entonces $xH = Hx$



iv) Si G es abeliano entonces cualquier subgrupo es normal

v) El centro de un grupo son todos los elementos que conmutan con todos los elementos del grupo

definición: el retículo de un grupo son los subgrupos ordenados por inclusión

ejemplo: el retículo de $\mathbb{Z}_{12}$

$\mathbb{Z}_{12} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}\}$

genera subgrupo (= divisores

1 Escribe los retículos (subgrupos ordenados por inclusión):

$\mathbb{Z}_{36} = \{\bar{1}, \bar{2}, \bar{3}, \dots \bar{35}\}$

$\langle \bar{1} \rangle = \{\bar{1}, \overline{1+1} = \bar{2}, \overline{1+\bar{1}+\bar{1}} = \bar{3}, \dots\} = \mathbb{Z}_{36}$

$\langle \bar{2} \rangle$

$\langle \bar{3} \rangle = \{\bar{3}, \bar{6}, \bar{12}, \dots, \bar{30}, \bar{33}, \bar{0}\}$

$\langle \bar{4} \rangle = \{\bar{4}, \bar{8}, \bar{12}, \bar{16}, \bar{20}, \bar{24}, \bar{28}, \bar{32}, \bar{0}\}$

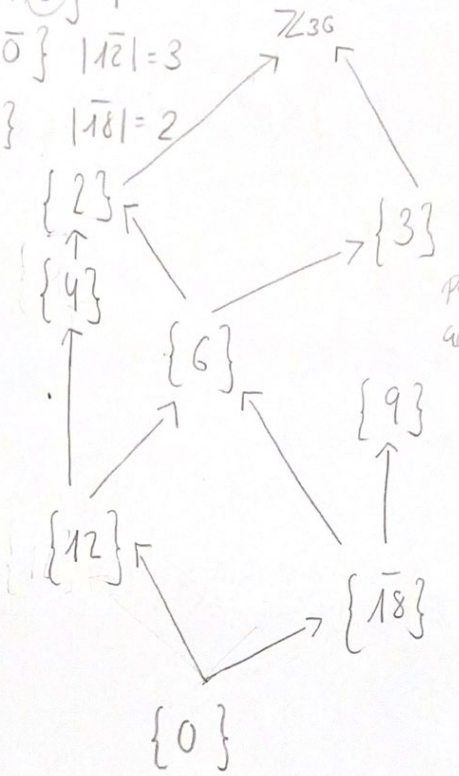
$\langle \bar{5} \rangle = \{$

$\langle \bar{6} \rangle = \{\bar{6}, \bar{12}, \bar{18}, \bar{24}, \bar{30}, \bar{0}\}$ $|\bar{6}| = 6$

$\langle \bar{9} \rangle = \{\bar{9}, \bar{18}, \bar{27}, \bar{0}\}$ $|\bar{9}| = 4$

$\langle \bar{12} \rangle = \{\bar{12}, \bar{24}, \bar{0}\}$ $|\bar{12}| = 3$

$\langle \bar{18} \rangle = \{\bar{18}, \bar{0}\}$ $|\bar{18}| = 2$



↝ no hace falta hacer + flechas porque todos los subgrupos del 6 caben a/3.

$S_3 = \{ i, (123), (132), (12), (23), (32), (31) \}$

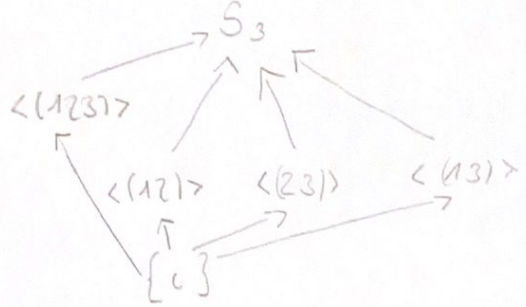
$\langle (132) \rangle$

$\langle (123) \rangle = \{ (123)(132) i \}$ $|(123)| = 3$

$\langle (12) \rangle = \{ (12), i \}$ $|(12)| = 2$

$\langle (23) \rangle = \{ (23) i \}$

$\langle (13) \rangle =$



$D_3 = \{ \rho_1, \rho_2, \sigma_1, \sigma_2, \sigma_3, i \} = \{ \rho, \rho^2, i, \sigma, \rho\sigma, \rho^2\sigma \}$