

### 3 SUBGRUPOS, GENERADORES, RETÍCULOS Y GRUPOS CÍCLICOS

#### 3.1 Subgrupos

Dados dos grupos  $g$  y  $H$ , se dice que  $H$  es un subgrupo de  $g$  y lo denotamos por  $H \subset g$ , si  $H$  es subconjunto de  $g$  y la inclusión  $H \hookrightarrow g$  es un homomorfismo de grupos donde  $\hookrightarrow \omega = x$ .

Dentro de un grupo cualquiera siempre habrá dos subgrupos conocidos como subgrupos propios que son {}{1} y el total. A todos los demás, en caso de que los haya, los llamaremos subgrupos propios.

Algunos ejemplos son:

i)  $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +)$

ii) Rotaciones  $\{ \in D_n \}$  se cumple pues las rotaciones son un grupo <sup>a-isomorfo</sup>

iii)  $n\mathbb{Z} \subset \mathbb{Z}$

iv)  $SL_n(\mathbb{IF}) \subset GL_n(\mathbb{IF})$

v)  $(\mathbb{Q}^*, \cdot) \not\subset (\mathbb{R}, +)$  pues el anillo es distinto. (no generalizar con división)

vi)  $(\mathbb{Z}^+, +) \not\subset (\mathbb{Z}, +)$  pues  $\mathbb{Z}^+$  no es un grupo.

vii)  $D_6 \not\subset D_8$  pues  $r^6=1$  pero  $r^6 \neq 1$  en  $D_8$  y  $D_6 \not\cong D_8$

Viii) Transitividad. Si  $K \subset H \subset g \Rightarrow K \subset g$

#### Proposición

Dado  $g$  un grupo y  $H \subset g$  uovacío. Entonces

1. Son equivalentes

i)  $H \subset g$

ii) Se verifican tres condiciones

a)  $\forall x, y \in H \Rightarrow xy \in H$

b)  $1 \in H$

c)  $\forall x \in H \Rightarrow x^{-1} \in H$

iii)  $\forall x, y \in H, xy^{-1} \in H$

2 Si  $g$  es finito, son equivalentes.

i)  $H \subset g$

ii)  $\forall x, y \in H \Rightarrow xy \in H$

### - Demostración -

1.  $\text{ii} \Rightarrow \text{iii}$ : Si  $H \subset g \Rightarrow \forall x, y \in H \Rightarrow \exists x, y^{-1} \in H \Rightarrow xy^{-1} \in H$

(Sup. Ind.)

iii)  $\exists u \in H \neq \emptyset \Rightarrow \exists x \in H \mid x^{-1} \in H$  luego  $x \in H$ . Entonces  $x^{-1} = 1 \cdot x^{-1} \in H$  y  $xy = x(y^{-1})^{-1} \in H$

$\Rightarrow \text{iii}$  Es trivial  $\square$

2.  $\text{c} \Rightarrow \text{ii}$  Es por definición

$\text{ii} \Rightarrow \text{i}$  Como  $g$  es finito  $\forall x, y \in g$   $\exists u \in g \mid x^{-1} = u^{-1}$  pero  $1 = x^{-1} \in H$  luego basta

i.ii) y por tanto 1.i)

Veamos algunos ejemplos con los que vamos a trabajar:

i)  $A \subset S_n$ , pues el producto de permutaciones pares es par y  $S_n$  es finito

ii) Si  $a \in \mathbb{Z} \Rightarrow a \in \mathbb{Z}$  (múltiplos de  $a$ ) couple que  $a \in \mathbb{Z} \subset \mathbb{Z}$ . Ademáis, todo subgrupo de  $\mathbb{Z}$  es  $a\mathbb{Z}$  para algún  $a \in \mathbb{N}$ .

iii)  $V \subset S_4$ , pues  $S_4$  es finito y el producto de elementos de  $V$  es de  $V$ .

iv)  $D_{n,k} \subset D_n \Leftrightarrow n \mid k$

### Proposición

Sea  $f: G \rightarrow G'$  (homomorfismo) de grupos. Entonces:

i) Si  $H \subset G \Rightarrow f_*(H) = \{f(x) \mid x \in H\} \subset G'$  (imagen directa) "Im( $f$ )"  
 $\text{Im}(f)(H)$

ii) Si  $H' \subset G' \Rightarrow f^*(H') = \{x \in G \mid f(x) \in H'\} \subset G$  (imagen inversa) "Im( $f$ )<sup>-1</sup>"

En particular  $\text{Im}(f) = f_*(G) \subset G'$  y  $\text{Ker}(f) = f^*(\{1\}) \subset G$

### Proposición

Sea  $\{H_i\}_{i \in I}$  una familia de subgrupos de  $G$ , entonces  $\bigcap_{i \in I} H_i \subset G$

### - Demostración -

Como  $H_i \subset G \quad \forall i \in I \Rightarrow 1 \in H_i \quad \forall i \in I$  luego  $1 \in \bigcap_{i \in I} H_i$  luego  $\bigcap_{i \in I} H_i \neq \emptyset$ . Ahora  $\forall x, y \in \bigcap_{i \in I} H_i \Rightarrow$

$x, y \in H_i \quad \forall i \in I \Rightarrow x^{-1} \in H_i \quad \forall i \in I \Rightarrow x^{-1} \in \bigcap_{i \in I} H_i$

$\square$

En general, la unión de subgrupos no es un subgrupo pues como contraejemplo  $2\mathbb{Z} \cup 3\mathbb{Z}$  no es un subgrupo pues  $5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ .

Sea  $S$  un grupo y  $S \subseteq G$ , entonces el subgrupo generado por  $S$ , que lo denotaremos por  $\langle S \rangle$ , es la intersección de todos los subgrupos de  $G$  que contienen a  $S$ , es decir, es el menor subgrupo que contiene a  $S$ .

## Proposición

Sea  $G$  un grupo,  $\langle S \rangle$  entonces:

- i) Si  $S = \emptyset$  entonces  $\langle S \rangle = \{1\}$ , el trivial =  $\{1\}$   $\rightarrow$  Dado ser un grupo u paralelo infinito
- ii) Si  $S \neq \emptyset$  entonces  $\langle S \rangle = \{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m} \mid m \geq 1, x_i \in S, \alpha_i = \pm 1, \forall i \geq 1\}$  donde  $S = \{x_1, x_2, \dots\}$
- iii) Si  $G$  es finito entonces Si también basta y si  $S \neq \emptyset$  se cumple que  $\langle S \rangle = \{1\}$  productos finitos de elementos de  $S$  ( $\Rightarrow \langle S \rangle = \{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m} \mid m \in \mathbb{N}, x_i \in S, \alpha_i = \pm 1 \forall i \geq 1\}$ )

Algunos ejemplos son:

i)  $D_n$ ,  $S = \{r\} \subset D_n$  y  $\langle S \rangle = \langle r \rangle = \{1, r, r^2, \dots, r^{n-1}\} \subset D_n$

ii)  $D_n$ ,  $S = \{s\} \subset D_n$  luego  $\langle S \rangle = \langle s \rangle = \{1, s\}$

iii)  $S_4$ ,  $S = \{(12)(34), (13)(24)\}$

$$\langle S \rangle = V \subset S_4$$

iv)  $S_3$ ,  $S = \{(x_1 x_2 x_3); x_1, x_2, x_3\}$

$$\langle S \rangle = A_3 \subset S_3$$

v)  $GL_2(\mathbb{C})$ ,  $S = \{( \begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix} ), (\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}) \}$

$$Q_2 \cong \langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rangle \subset gl_2(\mathbb{C})$$

vi) En el caso de que  $\langle S \rangle = G$  entonces  $S$  será un sistema de generadores.

vii) Si  $G$  es finito,  $\langle S \rangle = G$ , diremos que  $G$  es finitamente generado. Recibido que no es igual a esp. verbales

viii) Si  $S = \{a\}$  y  $\langle S \rangle = G$  entonces  $G$  es cíclico. ( $\mathbb{Z}$  es cíclico pues  $\mathbb{Z} = \langle 1 \rangle$ )

## Definición

Sea  $\{H_i\}_{i \in S}$ ,  $H_i \in \mathcal{G}(G)$ ; llamaremos conjunto de los subgrupos  $H_i$ , lo denotaremos por  $\bigvee H_i$ , al sobgrupo generado por  $S = \bigvee_{i \in S} H_i$ . En el caso de que  $S$  sea finito lo denotaremos por  $H_1 \vee \dots \vee H_n$ .

## 3.2. Retículos

En este caso, un retículo será un grafo dirigido en el que las aristas vienen dadas por las relaciones de inclusión.

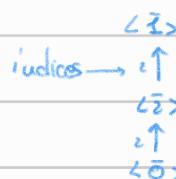
Nos servirá para representar las operaciones y dar más información de forma sencilla y visual.

Para construirlos usaremos todos los subgrupos ordenados de manera que, de abajo a arriba, se aumentará su orden, de esa forma hemos establecido una orden. En definitiva.

- i) Si  $H_1 < H_2 \Rightarrow$
- $\begin{array}{c} H_2 \\ \uparrow \\ H_1 \end{array}$
- ii) El grupo más inferior sería el trivial
- iii) El subgrupo más superior sería el total.

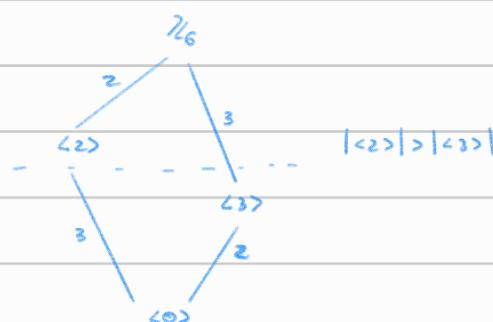
Pocos ejemplos:

i)  $\mathbb{Z}_4 = \{0, \bar{1}, \bar{2}, \bar{3}\}$  cuyos subgrupos son  $\{\bar{0}\}$ ,  $\langle \bar{1} \rangle = \mathbb{Z}_4$ ,  $\langle \bar{2} \rangle = \{0, \bar{2}\}$ ,  $\langle \bar{3} \rangle = \mathbb{Z}_4$ . Luego el retículo es:



Nota: consideramos clases de equivalencia.

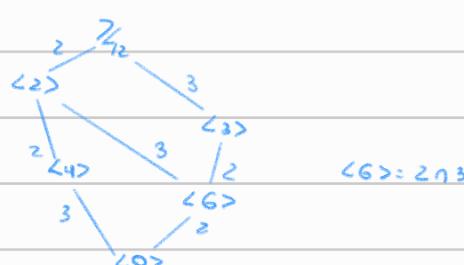
ii)  $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$  cuyos subgrupos son:  $\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_6$ ,  $\langle 2 \rangle = \{0, 2, 4\} = \langle 4 \rangle$ ,  $\langle 3 \rangle = \{0, 3\}$



iii)  $\mathbb{Z}_8$  con subgrupos  $\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \mathbb{Z}_8$ ,  $\langle 2 \rangle = \{0, 2, 4, 6\}$ ,  $\langle 4 \rangle = \{0, 4\}$

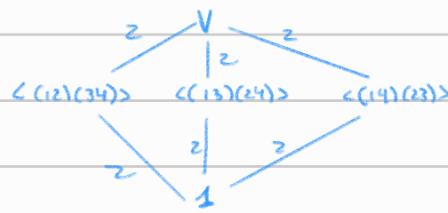


iv)  $\mathbb{Z}_{12}$  con subgrupos:  $\langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$ ,  $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$ ,  $\langle 3 \rangle = \{0, 3, 6, 9\}$ ,  $\langle 4 \rangle = \{0, 4, 8\}$ ,  $\langle 6 \rangle = \{0, 6\}$

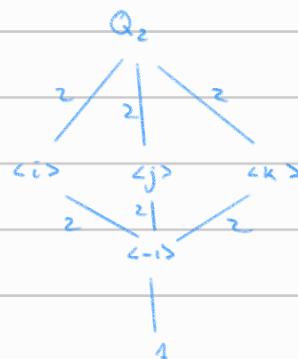


Es importante ver que el orden de los subgrupos es divisor del orden del grupo.

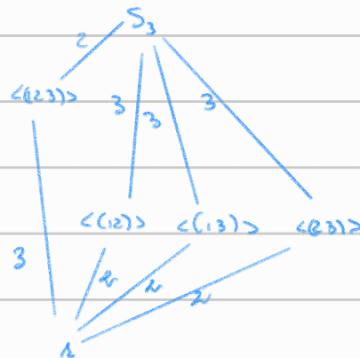
v)  $V = \{1, (12)(34), (13)(24), (14)(23)\}$



vi)  $\mathbb{Q}_2 = \{1, i, -i, j, -j\}$

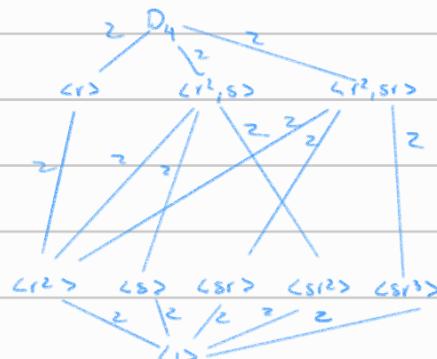


vii)  $S_3 = \{1, (12), (13), (23), (123), (132)\}$



$$H = \{(123)\} = \{1, (12)(132)\} \Rightarrow S_3 / H \cong \{H, (123)\}$$

viii)  $D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$



$$\langle r \rangle = \{r, r^2, r^3, 1\} = \langle r^2 \rangle$$

$$\langle r^2 \rangle = \{1, r^2\}$$

$$\langle sr^2 \rangle = \{1, sr^2\}$$

$$\langle s \rangle = \{1, s\}$$

$$\langle sr^3 \rangle = \{1, sr^3\}$$

$$\langle sr \rangle = \{1, sr\}$$

$$\langle r^2, sr \rangle = \{1, r^2, sr, sr^2\}$$

$$\langle r^2, sr^2 \rangle = \{1, r^2, sr^2\}$$

$$\langle r^2, sr^3 \rangle = \{1, r^2, sr^3\}$$

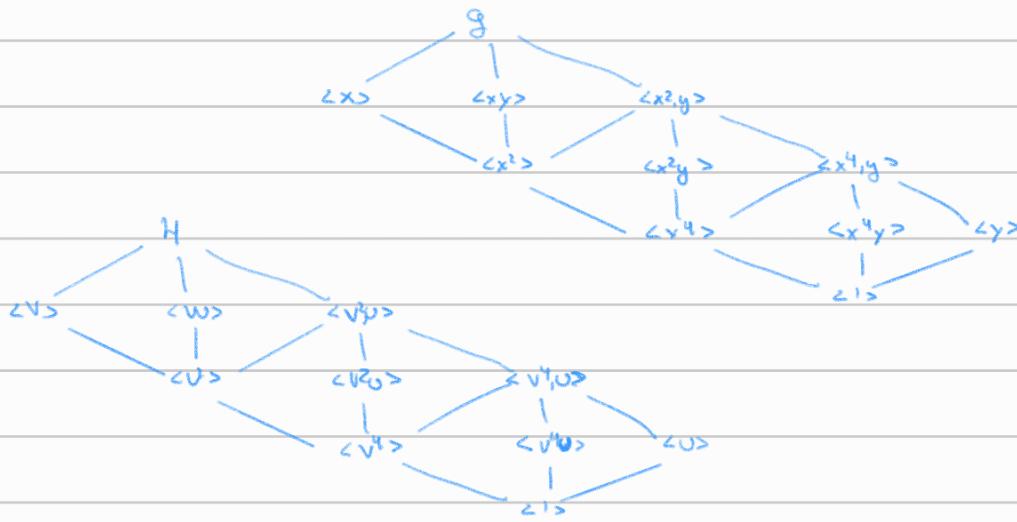
## Observación

Sean  $H, G$  grupos tales que  $H \cong G$  entonces sus retículos son isomorfos.

Grado modular de orden 16

Como ilustración tenemos que, considerando  $G = \langle x, y \mid x^8 = y^2 = 1, xy = yx \rangle$  y  $H = \langle u, v \mid u^2 = v^8 = 1, vu = uv \rangle$  pero  $G \cong C_8 \times C_2$  y dispone de 3 subgrupos de orden 8 ( $\langle x^2, y \rangle \cong C_4 \times C_2$ ,  $\langle x^4 \rangle \cong C_8$ ,  $\langle xy \rangle \cong C_2$ ) y 8 de orden 2 ( $\langle x, y^2 \rangle \cong C_2 \times C_4$ ,  $\langle y \rangle \cong C_2$ ,  $\langle xy^2 \rangle \cong C_8$ ). Los retículos

Son:



Por tanto, el reciproco es falso

Pero  $G$  es abeliano y  $H$  no; aun así sus retículos son isomorfos. Además, como ya hemos citado antes, el orden de los subgrupos divide el orden del grupo, pero no todos los divisores del orden del grupo se corresponden con el orden de algún subgrupo. Pensemos en el ejemplo:

$$|A_4| = \frac{12}{2} = 12$$

pero  $A_4$  tiene 4 subgrupos de orden 3, 1 de orden 4 y 3 de orden 2 por un grupo de orden 6 pero a que 6/12.

Supongamos  $\exists H \subset A_4 \mid |H|=6$ , entonces  $H$  tiene al menos un 3-ciclo  $(x_1 x_2 x_3)$  entonces, por ser subgrupo dispone de inverso; sin tener más de orden 3 entonces  $H = \{(x_1 x_2 x_3), (x_3 x_2 x_1), 1, (x_2 x_3), (x_3 x_1), (x_1 x_3)\}$  pero esto nos dice que  $|H| = 6 \neq 4 \times 6$ . Si hubiera otro elemento  $(x_1 x_2 x_4)$  entonces  $H = \{(x_1 x_2 x_3), (x_1 x_3 x_2), (x_1 x_2 x_4), (x_1 x_4 x_3), (x_3 x_2 x_1)\}$  pero  $(x_1 x_2 x_3)(x_1 x_4 x_3) = (x_1 x_4 x_3)$  luego realmente  $H = \{(x_1 x_2 x_3), (x_1 x_3 x_2), (x_1 x_2 x_4), (x_1 x_4 x_3), (x_3 x_2 x_1), 1\}$  que tiene 7 elementos !!.

### Definición

Sea  $H, K$  grupos tales que  $H \trianglelefteq G, K \trianglelefteq G$ . Entonces se define  $HK = \{hk \mid h \in H, k \in K\}$

### Proposición

$HK$  es un subgrupo  $\Leftrightarrow HK = KH$ . En particular,  $HK = H \vee K$

- Demostración.  $H, K$  son grupos para ser subgrupos

$$\Rightarrow \forall h \in H, k \in K, hk = (h^{-1}k^{-1})^{-1} \in HK \Rightarrow KH \subseteq HK. \text{ Al revés, } h^{-1}k^{-1} \in HK \Rightarrow \exists h_1, k_1 \in H, K \mid h_1^{-1}k_1^{-1} = h^{-1}k^{-1}$$

$$\Rightarrow h_1^{-1}k_1^{-1} = (h^{-1}k^{-1})^{-1} = (h, k)^{-1} \in KH \Rightarrow HK \subseteq KH$$

$$\Leftrightarrow \forall h_1, h_2, k_1, k_2 \in HK, (h_1k_1)^{-1} = h_1^{-1}k_1^{-1} = h_2^{-1}k_2^{-1} \in KH \Rightarrow HK \subseteq KH$$

↑  
Bueno este combate vale?

Por lo tanto  $HK$  es el menor subgrupo que contiene a  $H \vee K$  entonces  $HK = KH$ .

Inciso Obtener el retículo de  $A_4$

dos subgrupos son:

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

$$\langle (23) \rangle = \{1, (23), (13)\}$$

$$\langle (12) \rangle = \{1, (12), (14)\}$$

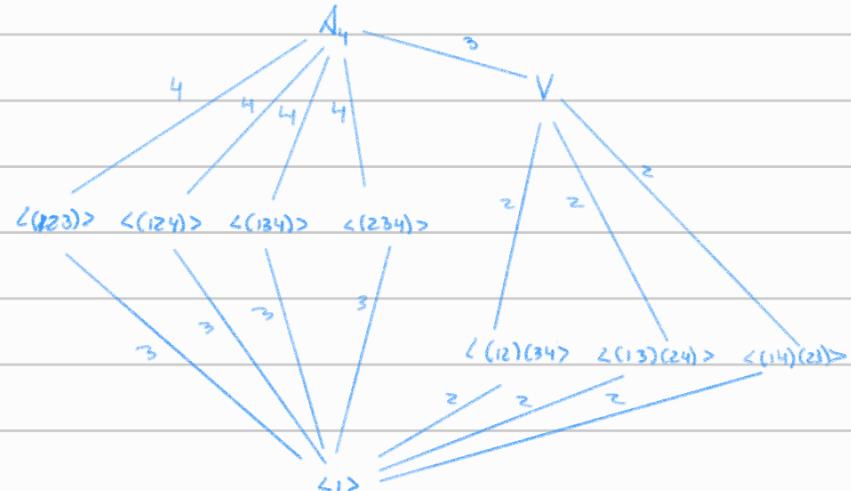
$$\langle (23) \rangle = \{1, (23), (24)\}$$

$$\langle (12)(34) \rangle = \{1, (12)(34)\}$$

$$\langle (13)(24) \rangle = \{1, (13)(24)\}$$

$$\langle (14)(23) \rangle = \{1, (14)(23)\}$$

$$\langle (12)(34)(13)(24) \rangle = \{1\}$$



### Definición

Sea  $G$  un grupo y  $H \trianglelefteq G$ ; se definen las relaciones binarias

i) una relación  $y \sim_H x \Leftrightarrow x^{-1}y \in H$

ii) una relación  $y \sim_H x \Leftrightarrow yx^{-1} \in H$

Además es de equivalencia cuyas clases se definen por

i)  $[x] = xH = \{xh \mid h \in H\}$  (clase lateral por la izquierda de  $H \trianglelefteq G$ ) que resaltó anteriormente

un conjunto cociente  $G/H = \{xH \mid x \in G\}$

ii)  $[x] = Hx = \{hx \mid h \in H\}$  (clase lateral por la derecha de  $H$  en  $G$ ) que nos permite obtener un conjunto cociente  $G/H = \{Hx \mid x \in G\}$

Es claro que en ambos casos dichas clases determinan una partición de  $G$ .

Algunos ejemplos:

i)  $S_3$  con  $H = \langle (12) \rangle$  son clases de equivalencia:

$$G/H = \{H, (12)H, (23)H\}$$

$$H = \{1, (12)\}$$

$$(23)H = \{(23), (23)(12)\}$$

$$(13)H = \{(13), (13)(12)\}$$

Intuitivo por la derecha  $\rightarrow$  No son el causas porque  $S_3$  no es abeliano.

Por lo general, estos conjuntos no serán grupos.

Proposición:

Sea  $g$  un grupo y  $H \trianglelefteq g$ . Entonces:

i)  $\forall x \in g, x^{-1}Hx \subseteq Hx$

ii)  $\forall x \in g$ , los conjuntos  $H, x^{-1}Hx$  son biyectivos (biyectivo)

iii) Los conjuntos cociente  $G/H$  y  $G_{/\sim_H}$  de clases laterales son biyectivos.  
*(No son grupos)*

-Demostración:

i)  $x = x \cdot 1 \in xH, x^{-1} = 1^{-1}x \in Hx$

ii)  $xH$  es biectivo  $H$  es biectivo  $Hx$   
 $xH \longleftrightarrow H \longleftrightarrow Hx$

iii)  $G/H \longrightarrow G_{/\sim_H}$

$$xH \longmapsto Hx^{-1}$$

Ver eugectividad y sobregeneralidad

Definición:

El cardinal del conjunto  $G/H$  (o  $G_{/\sim_H}$ ) se llama índice de  $G$  en  $H$  y se denota  $[G:H]$

Teorema de Lagrange

Sea  $g$  un grupo finito y  $H \trianglelefteq g$ . Entonces  $|H|$  divide  $|g|$  y además se tiene que

$$|g| = [g:H]|H|$$

-Demostración-

Es claro que  $g$  es unidimensional de las clases de  $g_{/H}$ ; supongamos que  $b_1^H, \dots, b_n^H$  son los representantes de las clases. Luego  $|g| = |\bigcup_{i=1}^n Hx_i| = \sum_{i=1}^n |Hx_i| = n|H|$  donde  $n = [g:H]$

Por ende disjunta

El reciproco visto que  $u$  era cierto, es decir, no todos los divisores del orden de un grupo dan lugar a un subgrupo.

Gracias al Teorema, si  $g$  es finito es cierto que  $[g:H] = \frac{181}{|H|}$  pero en el caso infinto existirían dos casos:

- i) Si  $H$  es finito debemos hacerlo de forma primitiva obteniendo el conjunto cociente  $\mathbb{Z}$  con  $59$ .
- ii) Si  $H$  es finito pasa igual pues bastaría tomar  $\mathbb{Z}$  con  $u\mathbb{Z}$  o?

### Corolario

El orden de un elemento de un grupo finito divide al orden del grupo.

-Demostración-

Si  $x \in g$ ,  $o(x) = l(x)$  pues el orden de  $x$  es el orden del subgrupo cíclico que genera. Luego por el Tº del grupo  $O(x) | O(g)$

### Corolario

Si  $g$  es finito y  $K \subset H \subset g$  entonces  $[g:K] = [g:H][H:K]$

-Demostración-

$$|g| = [g:K]|K|$$

$$|g| = [g:H]|H| = [g:H][H:K]|K|$$

$$\Rightarrow [g:K] = [g:H][H:K]$$

### 3.3 Propiedades de los grupos cíclicos

Recordemos que un grupo  $g$  es cíclico cuando  $g = \langle a \rangle = \{b \cdot a^n \mid n \in \mathbb{Z}\}$  para algún  $a \in g$ .

### Lema

Si  $g$  es un grupo finito de orden primo. Entonces es cíclico.

-Demostración-

Sea  $a \in g, a \neq 1$ . Dicás?

$a > 1 \Rightarrow |a| > 1 \mid |g|$  pero  $|g|$  es primo  $\Rightarrow |a| = 1 \mid |g|$

Lema

Sea  $g$  un grupo y  $x \in g$ ,  $a \in \mathbb{N}$ . Entonces  $x^a = 1 \Leftrightarrow a \mid n$  → Ya lo vimos pero Lagrange lo da más fácil

-Demostración.

$\Rightarrow$  Ya lo hicimos por def. de orden

$$\Leftrightarrow \text{Si } a \mid n \Rightarrow n = at \Rightarrow x^n = x^{at} = 1^t = 1$$

Lema

Sea  $g$  un grupo,  $x \in g$ . Entonces,

$$i) \text{ Si } O(x) = \infty \text{ se tiene que } x^k = x^m \forall k, m \in \mathbb{Z}$$

$$ii) \text{ Si } O(x) = n \text{ se tiene que } \langle x \rangle = \{1, x, \dots, x^{n-1}\} \subset g \text{ y } x^c = x^j \Leftrightarrow a \mid c - j$$

-Demostración-

$$i) \text{ Si } \exists i, j : x^i = x^j \Rightarrow x^{i-j} = 1 \Rightarrow O(x) < \infty !!$$

$$ii) \text{ Si } x^c = x^j \Rightarrow x^{c-j} = 1 \Rightarrow a \mid c - j$$

↳ Por un corolario del Tº de Lagrange.

Proposición

Sea  $g$  un grupo,  $a \in g$  entones existe un homomorfismo de grupos  $\varphi_a : \mathbb{Z} \rightarrow g$  |  $\varphi_a(1) = a$  y

$$\text{Im}(\varphi_a) = \langle a \rangle$$

-Demostración-

Distintos casos:

$$i) \text{ Si } a = 0, \varphi_a(u) = \varphi_a(u+1) = \varphi_a(1)^u = 0^u \rightarrow \text{definido así}$$

$$ii) \text{ Si } a \neq 0, \varphi_a(-u) = \varphi_a(-u)^{-1} = (a^{-u})^{-1} = a^u$$

{Está bien definido}

Luego  $\varphi_a(u) = a^u \forall u \in \mathbb{Z}$ . → Porque lo ha definido así.

$$\varphi_a(u+m) = a^{u+m} = a^u a^m = \varphi_a(u) \varphi_a(m) \text{ luego } \text{Im} \varphi_a = \{a^u \mid u \in \mathbb{Z}\} = \langle a \rangle$$

↳ prop. vistas Teoría 2.

Tarea:

Si  $g$  es un grupo cíclico,  $g \cong \mathbb{Z}$  o  $g \cong \mathbb{Z}_n$  para algún  $n \in \mathbb{N}$

-Demostración-

Si  $g$  es cíclico entonces  $\varphi_a : \mathbb{Z} \rightarrow g$  es un homomorfismo sobreyectivo pues  $\text{Im}(\varphi_a) = g$  → prop. anterior que es inyectivo.

- Si  $O(a) = n \Rightarrow \exists k \in \mathbb{Z} \mid a^k = 1 \Rightarrow \text{Ker}(\varphi_a) = \{0\} \Rightarrow \text{Im}(\varphi_a) = g \Rightarrow \varphi_a$  inyectivo

Luego es isomorfismo

- Si  $\text{O}(a)=u$ ,  $u \in \mathbb{N} \Rightarrow \exists u > 1, u = 1 \Rightarrow \text{Ker}(\bar{\phi}_a) \neq \{0\}$  luego definimos  $\rightarrow \cong \mathbb{Z}_u$

$$\begin{aligned}\bar{\phi}_a : \mathbb{Z}_u &\longrightarrow g \\ r &\longmapsto \bar{\phi}_a(r) = a^r\end{aligned}$$

Bien definida, si  $r = s \Rightarrow r - s \in \mathbb{Z} \Rightarrow a^{r-s} = a^{u-t} = 1 \Rightarrow a^{r-s} = 1 \Rightarrow a^{r-s} \in \{1\}$ . Se puede

comprobar que es homomorfismo de grupos sobreyectivo pues  $g = \text{ca} = \text{Im}(\bar{\phi}_a)$

Para ver la ruedatividad, si  $\bar{\phi}_a(r) = a^r = 1 \Rightarrow r = 0$  luego  $\text{Ker}(\bar{\phi}_a) = \{0\}$   
por tanto  $g \cong \mathbb{Z}_u$

### Proposición

Si  $g$  es un grupo cíclico con  $|a|=u$ . Entonces para cada divisor  $w$  de  $u$  existe un único  
subgrupo de  $g$  de orden  $w$  que es el cíclico  $\langle a^{\frac{u}{w}} \rangle$ . Y estos son los únicos subgrupos de  $g$ .

### Demotstración

Verificar que existe y es único  
que  $a^{\frac{u}{w}} = 1 \Rightarrow a^{\frac{uw}{w}} = 1$  es un grupo cíclico de orden  $w$  porque  $(a^{\frac{uw}{w}})^w = a^{uw} = 1$  y si  $\exists t \in \mathbb{Z} \mid (a^{\frac{uw}{w}})^t = 1$   
entonces  $a^{\frac{ut}{w}} = 1 \Rightarrow a^{\frac{ut}{w}} = a^{\frac{uw}{w}} \Rightarrow ut = uw \Rightarrow u(t-w) = 0$  lo que contradice la condición de que  $w$  sea primo.

Todo grupo cíclico es finito si tienen

Si  $H \subset g$ , por el T<sup>a</sup> de Lagrange  $|H| \mid |g|$  de manera que si  $|H| = w = u/w$ . Veamos  
que  $H = \langle a^{\frac{u}{w}} \rangle$ ; para ello, sea  $K = \langle a^{\frac{u}{w}} \rangle \cap H$  entonces  $a^{\frac{u}{w}} \in K \subseteq H$ . Sea ahora  $b \in H \setminus g$   
entonces  $b = a^k$  para algún  $k \in \mathbb{N} \Rightarrow b \in K$  con  $0 \leq k < w \Rightarrow a^k = a^{\frac{uw}{w}-kw} \in H$   
Por tanto,  $b \in K$  y  $s = u/w$  luego  $b = (a^u)^{\frac{1}{w}} \in \langle a^{\frac{u}{w}} \rangle$ . Luego,  $H = \langle a^{\frac{u}{w}} \rangle$ .

¿Por qué? → porque si es el mínimo luego existe  $\frac{1}{w} \in K$ .

Veamos ahora que  $w = u/w$ ; pero como  $a^u = 1$  y  $H \subset g \Rightarrow 1 \in H \Rightarrow u \in K$  luego  $O(a^{\frac{u}{w}}) \cdot \frac{u}{w} = u \Rightarrow w = \frac{u}{w}$   
 $|H| = u \Rightarrow 1^{\text{o}}$  punto de demostración

Como ejemplo constituyentes  $C_{1,2} = \langle x^1 \rangle, \langle x^2 \rangle$ ,  $\text{Div}(x) = \{2, 3, 4, 6\}$  luego disponemos de los siguientes  
subgrupos:

1. Un grupo de orden 2  $\langle x^2 \rangle$

2. Un grupo de orden 3  $\langle x^3 \rangle$

3. Un grupo de orden 4  $\langle x^4 \rangle$

4. Un grupo de orden 6  $\langle x^6 \rangle$

En el caso de tener un cílico de orden  $p^u$  siendo  $p$  un número primo tenemos subgrupos cíclicos  
no triviales de orden  $p^i$   $1 \leq i < u$ , es decir, las potencias de  $p$

### Proposición

Sea  $g$  un grupo y  $a \in g$  tal que  $O(a) = u$ . Entonces si  $v \geq u$  se tiene que  $\langle a^u \rangle = \langle a^v \rangle$  donde  $d$  es el orden de  $\langle a^u \rangle$  como divisor de  $u$  y, ademas,  $O(a^u) = \frac{u}{d}$ .

-Demostración-

$$\text{Porque } u = dt \Rightarrow a^u = a^{dt} \in \langle a^d \rangle \text{ luego } \langle a^u \rangle \subseteq \langle a^d \rangle$$

$$\text{Porque } d = \text{mcd}(u, v), \text{ usando la igualdad de Bezout, } \exists u, v \mid ua + v = d \text{ luego } a^d = a^{ua+v} = a^{ua} \cdot a^v = (a^u)^d = \langle a^u \rangle^d \subseteq \langle a^u \rangle$$

por ser subgrupo de grupo cíclico  $\langle a^u \rangle$

por qué esto

$$\text{Si } \langle a^u \rangle = \langle a^d \rangle \Rightarrow O(a^u) = O(a^d) \text{ pero } O(a^d) = \frac{u}{d} \text{ pues } (a^d)^{u/d} = 1. \text{ Ademas, si } (a^d)^e = 1 \Rightarrow a^{ed}$$

pues  $O(a) = u \Rightarrow a^u = 1$

Para ejemplo, los divisores primos que en  $\mathbb{Z}_8$  tienen el 8 como apareció pues  $\langle \bar{8} \rangle = \langle \bar{4} \rangle \supseteq \langle \bar{2} \rangle = \langle \bar{2} \cdot \bar{2} \rangle$  y  $O(\bar{2}) = 4 \wedge \text{mcd}(6, 4) = 2 \Rightarrow O(\bar{6}) = 3$

### Corolario

Si  $g$  es un grupo y  $a \in g$  con  $O(a) = u$ ; entonces  $\langle a^i \rangle = \langle a^j \rangle$  si y solo si  $\text{mcd}(u, i) = \text{mcd}(u, j)$

### Corolario

Si  $g$  es un grupo cíclico con  $O(a) = u$ . Entonces

$$g = \langle a^u \rangle \Leftrightarrow \text{mcd}(u, u) = 1 \rightarrow \text{Para sacar los subgrupos } \langle a^i \rangle \text{ o } \langle a^j \rangle$$

que será el número de generadores de  $g$  es la  $\varphi$  de Euler,  $\varphi(u) = \{n \in \mathbb{N} \mid \text{mcd}(u, n) = 1\}$