# Clase 2:

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$$

$$S_n = \{ \sigma : \{1, \dots, n\} \to \{1, \dots, n\} \ / \ \sigma \text{ es biyección} \}$$

**Subgrupo:** $H \subseteq G$ tq $(H, \cdot|_{H\times H})$ es grupo

$$\emptyset \neq H \text{ es subgrupo} \iff \forall x, y \in H : xy^{-1} \in H$$

**Ejemplos:**

1) $\mathbb{Z} \leq \mathbb{Q}$, $\mathbb{Q} \leq \mathbb{R}$
2) Dado un grupo $G$, $\{1\}$, $G$ son subgrupos
3) $H = \{1, r, \dots, r^{n-1}\} \leq D_{2n}$
4) Sea $\mathbb{K}$ un cuerpo

grupo general lineal $\rightarrow$ $GL_n(\mathbb{K}) = \{ (a_{ij}) \in \mathbb{K}^{n\times n} \ / \ \det(a_{ij}) \neq 0 \}$

$$SL_n(\mathbb{K}) = \{ A \in GL_n(\mathbb{K}) \ / \ \det(A) = 1 \} \leq GL_n(\mathbb{K})$$

5) $S^1 = \{ z \in \mathbb{C} \ / \ |z| = 1 \} \subseteq \mathbb{C}$

$$U_n = \{ z \in \mathbb{C} \ / \ z^n = 1 \},\ n \in \mathbb{N} \text{ fijo}$$

$$U = \{ z \in \mathbb{C} : \exists n \in \mathbb{N} \ / \ z^n = 1 \} \subseteq \mathbb{C}$$

$$U_n \leq U \leq S^1$$

**Proposición:** $\{H_\alpha\}$ familia de subgrupos de $G$

$$\Rightarrow \bigcap_{\alpha \in I} H_\alpha \leq G$$

**Definición:** $\emptyset \neq A \subseteq G$ subconjunto, defino:

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H$$

subgrupo generado por $A$

* $A \subseteq \langle A \rangle$
* Si $A = \{a_1, \dots, a_n\} \Rightarrow \langle A \rangle = \langle a_1, \dots, a_n \rangle$
* Si $A, B \subseteq G \Rightarrow \langle A \cup B \rangle = A \vee B = \langle A, B \rangle$

**Proposición:** $\emptyset \neq A \subseteq G$, entonces

$$\langle A \rangle = \{ \underbrace{a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \;/\; \epsilon_i \in \{-1, 1\}, a_i \in A, n \in \mathbb{N}}_{\bar{A}} \}$$

**Demostración:**

1) $\bar{A}$ es un subgrupo de $G$, $\bar{A} \neq \emptyset$

2) $A \subseteq \bar{A}$ ✓

$\Big\} \langle A \rangle \subseteq \bar{A}$

3) $a = a_1^{\epsilon_1} \dots a_n^{\epsilon_n} \in \bar{A} \leadsto a_1^{\epsilon_1}, \dots, a_n^{\epsilon_n} \in \langle A \rangle$

$\leadsto a \in \langle A \rangle$ ∎

Se puede tener

$$baa\,a\cdot a^{-1} = ba^3 \quad , a\cdot a^{-1}\cdot a = a$$

Entonces:

$$\langle A\rangle = \{ a_1^{\alpha_1} \dots a_n^{\alpha_n} \,/\, \alpha_i \in \mathbb{Z},\ a_i \neq a_{i+1},\ n\in\mathbb{N} \}$$

Si G es abeliano:

$$\langle A \rangle = \{ a_1^{\alpha_1} \dots a_n^{\alpha_n} \,/\, \alpha_j \in \mathbb{Z},\ a_i \in A,\ n\in\mathbb{N} \}$$

Por ejemplo:

$$\langle a\rangle = \{ a^n \,/\, n\in\mathbb{Z} \}$$

Grupos cíclicos:

Definición un grupo $G$ es cíclico si $G = \langle a\rangle$, para algun $a\in G$

* $G = \langle x\rangle \Rightarrow G = \langle x^{-1}\rangle$

Proposición: Si $H$ es ciclico $\Rightarrow$ es abeliano

Ejemplos:

1) $\mathbb{Z}_n = \langle \bar{1}\rangle$

2) $G = D_{2n}$, $H = \langle r\rangle$ y como $|r| = n$

$$\Rightarrow H = \{1, r, r^2, \dots, r^{n-1}\}$$

$$\Rightarrow |H| = n$$

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

Todo subgrupo de $\mathbb{Z}$ es de la forma $\underset{\langle n \rangle}{n\mathbb{Z}}$

En efecto, sea $H \leq \mathbb{Z}$ con $H \neq \{0\}$

$$\Rightarrow \exists n \in H \;/\; \underbrace{n}_{n \cdot 1} \neq 0 \checkmark$$

Consideremos:

$$m = \min\{n \in \mathbb{Z} - \{0\} \;/\; n \in H\}$$

Afirmación: $H = \langle m \rangle = \{k \cdot m \;/\; k \in \mathbb{Z}\} = m\mathbb{Z}$

($\supseteq$) Es evidente porque $m \in H \Rightarrow k \cdot m = \underbrace{m + \dots + m}_{k \text{ veces}} \in H$

($\subseteq$) Sea $h \in H$, Por alg. de la división:

$$h = q \cdot m + r, \quad r \in \{0, 1, \dots, m-1\}$$

Si $r = 0 \Rightarrow h = q \cdot m \in \langle m \rangle \checkmark$

Si $r \neq 0 \Rightarrow r = \underbrace{h}_{\in H} - q \cdot \underbrace{m}_{\in H} \in H$ pero $r < m$

esto es imposible pues $m$ es mínimo

Proposición: Todo subgrupo de un grupo cíclico es cíclico

$H \leq G$

Si $G = \langle a \rangle \Rightarrow H = \langle a^m \rangle$

$m = \min\{\underbrace{n \;/\; a^n \in H}\}$

## Clasificación de Grupos cíclicos:

**Proposición:** Sea $G = \langle x \rangle$ y $|x| = n \Rightarrow |G| = n$

Mas aún:

1) Si $|G| = n < \infty \Rightarrow G = \{1, x, \ldots, x^{n-1}\}$

2) Si $|G| = \infty \Rightarrow x^n \neq 1, \forall n \in \mathbb{N}$
$x^a \neq x^b, a \neq b$

**Demostración:**

1) Si $|x| = n$

- $1, x, \ldots, x^{n-1}$ son diferentes

  [Si $x^a = x^b$, $a < b \in \{0, \ldots, n-1\} \Rightarrow x^{b-a} = 1$
  imposible porque $b - a < n$ ]

- $\{1, x, \ldots, x^{n-1}\} \subseteq G = \langle x \rangle$

- Sea $a \in G \Rightarrow a = x^m$, por alg. de div.

$$m = nq + r, \quad 0 \leq r \leq n-1$$

$$\Rightarrow x^m = (x^n)^q \cdot x^r$$

$$\Rightarrow a = x^r, \quad \underline{r \leq n-1}$$

$$\Rightarrow a \in \{1, x, x^2, \ldots, x^{n-1}\}$$

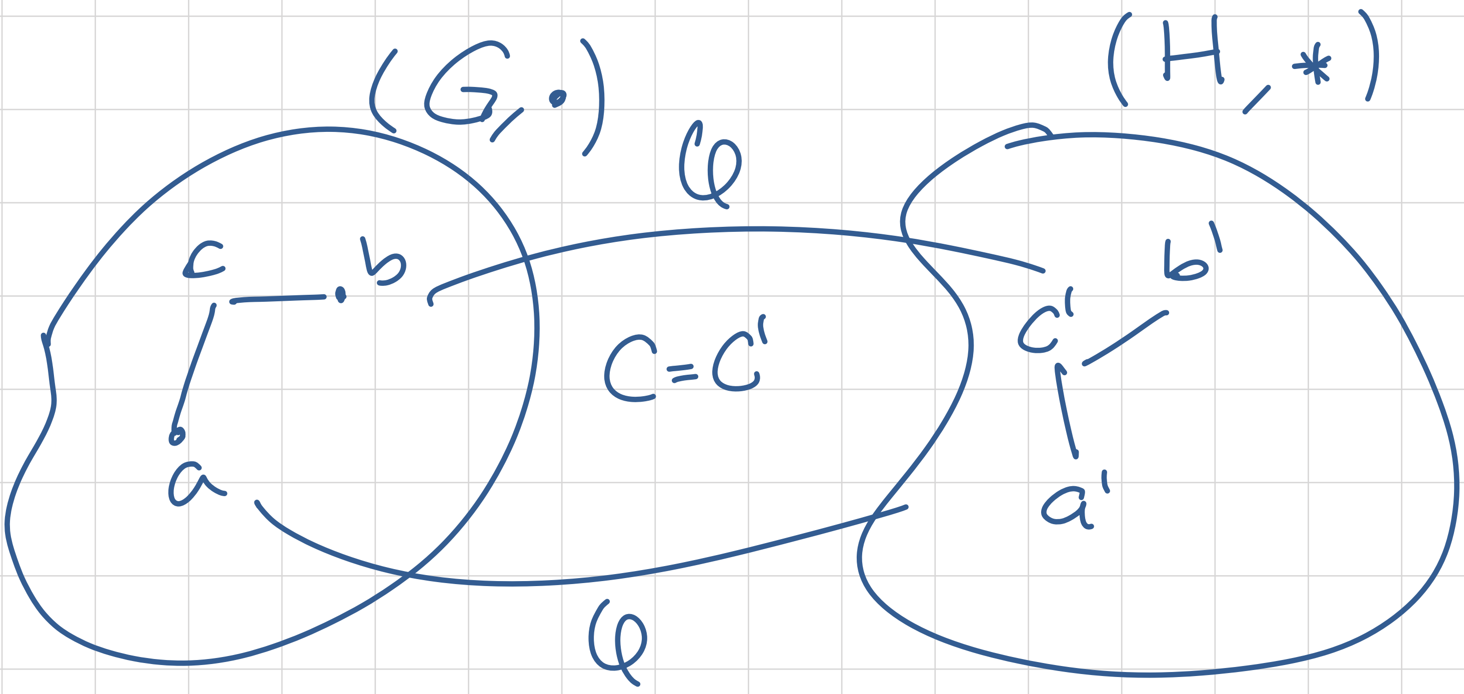
2) Si $|x| = \infty$

* $x^n \neq 1, \forall n \in \mathbb{Z}$ ✓

* $x^a \neq x^b, \forall a \neq b$

[Sup. que existen $a \neq b$ tq' $x^a = x^b$, por ejemplo $a < b \Rightarrow x^{b-a} = 1$ ($\Rightarrow\Leftarrow$)]

Entonces $G = \langle x \rangle = \{x^n / n \in \mathbb{Z}\} \Rightarrow |G| = \infty$ ▨




$$\varphi(\underbrace{ab}_{c}) = c' = \varphi(a)\varphi(b)$$

**Definición:** Sean G, H grupos, un homomorfismo de G en H es una función

$$\varphi : G \rightarrow H$$

tal que: $\varphi(ab) = \varphi(a) \cdot \varphi(b), \forall a, b \in G$

Si $\varphi$ es biyectiva, diremos que es un isomorfismo y G, H serán isomorfos ($G \cong H$)

Si $H$ es cíclico $\leadsto \overset{\text{clasif.}}{\text{¿}} H = ?$

Teorema: (Clasif. de grupos cíclicos)

Todo par de grupos cíclicos del mismo orden son isomorfos

Más aún:

1) Si $G=\langle x\rangle$, $H=\langle y\rangle$ son cíclicos de orden $n<\infty$

$$\Rightarrow \varphi: G \to H$$
$$x^n \mapsto y^n$$

es un isomorfismo. $(G\cong H)$

2) Si $G=\langle x\rangle$ y $|G|=\infty$

$$\Rightarrow \varphi: \mathbb{Z} \to G$$
$$n \mapsto x^n$$

es un isomorfismo $(\mathbb{Z}\cong G)$

Demostración:

1)
$$\varphi: \underset{\langle x\rangle}{\overset{\|}{G}} \to \underset{\langle y\rangle}{\overset{\|}{H}}$$
$$x^n \mapsto y^n$$

* $\varphi$ está bien definida:

Si $x^n = 1 \Rightarrow |x| \mid n$

En efecto:
$n = q|x| + r$, $\underbrace{0 \le r < |x|}$

$\Rightarrow x^n = (x^{|x|})^q \cdot x^r \Rightarrow x^r = 1$ $(\Rightarrow\Leftarrow)$

$\Rightarrow r = 0 \Rightarrow |x| \mid n$

Tenemos que ver:

$$\underbrace{X^r = X^s}_{X^{r-s}=1} \Rightarrow \varphi(X^n) = \varphi(X^m)$$

Por lo anterior $\Rightarrow n \mid r-s \Rightarrow r-s = kn$

$\Rightarrow r = s+kn$

Luego: $\varphi(X^r) = Y^r = Y^s \cdot \underbrace{Y^{kn}}_{(Y^n)^k} = Y^s = \varphi(X^s)$ ✓

* $\varphi$ es homomorfismo y biyectivo ✓

2)
$$\varphi : (\mathbb{Z},+) \to G = \langle x \rangle$$
$$n \mapsto x^n$$

* $X^a \neq X^b, \forall a \neq b \Leftrightarrow \varphi(a) \neq \varphi(b), \forall a \neq b$ ✓
* Sobreyectiva ✓
* Homomorfismo ✓

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

$\blacksquare$

Si H es cíclico $\nearrow$ $|H| = n < \infty$ : $H \cong \mathbb{Z}_n$

$\searrow$ $|H| = \infty$ : $H \cong \mathbb{Z}$

## Generadores de grupos cíclicos:

Si $G = \langle x \rangle$ ¿$G = \langle y \rangle$?

↳ ¿cuales y?

**Ejercicio:** $G$ grupo, $x \in G$, $a \in \mathbb{Z} - \{0\}$

1) Si $|x| = \infty \Rightarrow |x^a| = \infty$

2) Si $|x| = n \Rightarrow |x^a| = \frac{n}{(n,a)}$

Si $a | n \Rightarrow |x^a| = \frac{n}{a}$

1) ✓

2) Si $a|b \wedge b|a \Rightarrow a = b$

Como $(x^a)^{n/(n,a)} = 1$

$$\Rightarrow |x^a| \,\Big|\, \frac{n}{(n,a)}$$

Para la otra:

Si $a|bc$ y $(a,b) = 1 \Rightarrow a|c$

$(x^a)^{|x^a|} = 1 \Rightarrow x^{a|x^a|} = 1$

$$\Rightarrow n \,|\, a|x^a| \quad (*)$$

Sea $d = (n,a) \rightarrow \begin{matrix} n = db \\ a = dc \end{matrix}$, $(b,c) = 1$

Reemplazando: $\cancel{d}b \,|\, \cancel{d}c|x^a| \Rightarrow b \,|\, c|x^a|$

$$\Rightarrow b \,|\, |x^a| \Rightarrow \frac{n}{(n,a)} \,\Big|\, |x^a|$$

**Proposición:** Sea $H = \langle x \rangle$

1) Si $|x| = \infty \Rightarrow H = \langle x^a \rangle \Leftrightarrow a = \pm 1$

2) Si $|x| = n < \infty \Rightarrow H = \langle x^a \rangle \Leftrightarrow (a,n) = 1$

$$\# \text{generadores} = \varphi(n)$$

**Demostración:**

1) $(\Rightarrow)$ $H = \langle x^a \rangle$, consideremos

$$\varphi : \mathbb{Z} \to H$$
$$n \mapsto x^n$$

* $\overset{a\mathbb{Z}}{\mathbb{Z} = \langle a \rangle}$, si $n \in \mathbb{Z} \Rightarrow \varphi(n) \in H$

$(\supseteq)$ ✓

$(\subseteq)$

$$\Rightarrow \varphi(n) = (x^a)^m, \; m \in \mathbb{Z}$$
$$\Rightarrow x^n = x^{am}$$
$$\Rightarrow x^{n-am} = 1$$
$$\Rightarrow n = am$$
$$\Rightarrow n \in \langle a \rangle$$

* $\mathbb{Z}$ solo está generado por $\pm 1$, sup que $\mathbb{Z} = \langle a \rangle$

$$1 = ka, \; k \in \mathbb{Z}$$
$$\begin{matrix} 1 & 1 \\ -1 & -1 \end{matrix}$$

* Como $\mathbb{Z} = \langle a \rangle \Leftrightarrow a = \pm 1$

$\Updownarrow$

$$G = \langle x^a \rangle$$

2) Si $|x| = n \Rightarrow |x^a| = \frac{n}{(n,a)}$   $H = \langle x^a \rangle$

* $x^a$ genera un subgrupo de orden $|x^a| = \frac{n}{(n,a)}$

$H = \langle x^a \rangle \Leftrightarrow |x^a| = |x|$

$\Leftrightarrow \frac{n}{(a,n)} = n$

$\Leftrightarrow (a,n) = 1$

$\blacksquare$

Ejemplo: $\mathbb{Z}_n = \langle \bar{1} \rangle = \langle \bar{a} \rangle$ tq $(a,n) = 1$

$H = \langle x^a \rangle \Leftrightarrow (a,n) = 1$

$H = \langle ax \rangle \Leftrightarrow (a,n) = 1$

$\mathbb{Z}_n = \langle \bar{a} \rangle \Leftrightarrow (a,n) = 1$

Por ejemplo $\mathbb{Z}_{12} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$

Proposición (# subgrupos de grupos cíclicos)

Sea $H = \langle x \rangle$, entonces:

1) $|H| = \infty$:
- $\to a \neq b \in \mathbb{N} \Rightarrow \langle x^a \rangle \neq \langle x^b \rangle$
- $\to \forall m: \langle x^m \rangle = \langle x^{|m|} \rangle$

# subgrupos de $H = \mathbb{N}$

2) Si $|X| = n < \infty$

- Si $a | n \Rightarrow \exists!$ subgrupo $H$ de orden $a$
más aún ese $H$ tiene la forma

$$H = \langle x^{n/a} \rangle$$

- $\forall m:$ $\langle x^m \rangle = \langle x^{(n,m)} \rangle$ $\rightsquigarrow$ div. de $n$

\# subgrupos de $H$ = \# div. de $n = |H|$

Demostración:

1) a) $a \neq b \in \mathbb{N}:$ $\langle x^a \rangle \neq \langle x^b \rangle$
$(x^n \neq 1, \forall n)$

b) $\forall m:$ $\langle x^m \rangle = \langle x^{|m|} \rangle$
$\left[ (x^m)^n = (x^{-m})^{-n} \right]$

\# subgrupos $= \mathbb{N}$
$1 \mapsto S_1 \leq H$
$2 \mapsto S_2 \leq H$
$\vdots$

a) $\{ \langle x^a \rangle / a \in \mathbb{N} \}$ (*) $\subseteq$ (⊇) $\{$ Conj. de subgrupos de $H$ $\}$

b) Si $H \leq G \rightsquigarrow H$ es cíclico

$$\rightsquigarrow H = \langle x^d \rangle = \langle x^{|d|} \rangle \in (*)$$

2) a) Si $a | n \Rightarrow \exists! H$ tq $|H| = a$

$$H = \langle x^{n/a} \rangle$$

Como $|x| = n \rightsquigarrow |x^a| = \frac{n}{(n,a)} = \frac{n}{a} = d$, $d|n$

Ahora $|\langle x^d \rangle| = \frac{n}{d} = a$

* Unicidad (ejercicio)

b) $\langle x^m \rangle = \langle x^{(n,m)} \rangle$ (ejercicio)

$\{ \langle x^{n/a} \rangle : a|n \} = \{$ Subgrupos de H $\}$

$\blacksquare$

Ejemplo: Calcular los subgrupos de $\mathbb{Z}_{12}$

div 12 = 1, 2, 3, 4, 6, 12

$\rightsquigarrow$ hay 6 subgrupos

* $\mathbb{Z}_{12} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$

* $\langle \bar{2} \rangle = \langle \bar{10} \rangle$ (orden 6)

[ $G = \langle x \rangle \Rightarrow G = \langle x^a \rangle \Leftrightarrow (a,n) = 1$ ✓

$G = \langle \bar{2} \rangle \Rightarrow G = \langle a\bar{2} \rangle \Leftrightarrow (a,6) = 1$
1,5 ]

* $\langle \bar{3} \rangle = \langle \bar{9} \rangle$ (orden 4)

* $\langle \bar{4} \rangle = \langle \bar{8} \rangle$ (orden 3)

* $\langle \bar{6} \rangle$ (orden 2)

* $\langle \bar{0} \rangle$ (orden 1)

# Diag. reticular

$$\begin{tikzcd}
& & \mathbb{Z}_{12} \arrow[dl, dash] \arrow[dr, dash] & \\
& \langle \bar{2} \rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle \bar{3} \rangle \arrow[dl, dash] \\
\langle \bar{4} \rangle \arrow[dr, dash] & & \langle \bar{6} \rangle \arrow[dl, dash] & \\
& \langle \overline{12} \rangle & &
\end{tikzcd}$$

$\langle \bar{2} \rangle \supseteq \langle \bar{4} \rangle$

¿$\langle m \rangle \subseteq \langle n \rangle$?