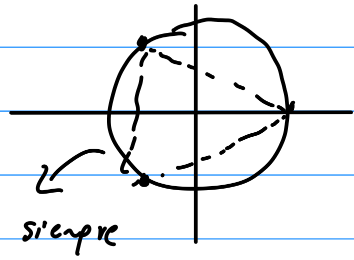
Grupos cíclicos

un grupo se dice cíclico si está generado por un único elemento.

t.q. $\exists\, g \in G : \langle g \rangle = G$

- $\odot \left\{ e^{\frac{2\pi i k}{n}},\ k=0,1,\dots \right\}$



da siempre un polígono regular

↳ se llama raíces n-ésimas de 1.

↳ $x = \sqrt[3]{1}$

$x^3 = -1$

$x^3 - 1 = 0$

- $\odot\ \mathbb{Z} = \langle 1 \rangle$.
- $\odot\ V_4$ no es cíclico.
- $\odot\ \mathbb{Z}_m = \langle 1 \rangle$
- $\odot\ \mathbb{Z}_p^{\times}$ ⇝ grupo multiplicativo de un campo.
  - ↳ todos sus elementos son invertibles.

otra forma de dar la def.

Obs $\odot$ Un grupo G es cíclico sii contiene un elemento de orden n.

$\odot$ Cíclico $\Rightarrow$ abeliano.

$G = \langle g \rangle, \quad h_1, h_2 \in G$

$\exists\, n_1, n_2 \in \mathbb{Z} : h_1 = g^{n_1},\ h_2 = g^{n_2}$

$$h_1 h_2 = g^{n_1} \cdot g^{n_2} = g^{n_1+n_2} = g^{n_2+n_1} = g^{n_2} \cdot g^{n_1} = h_2 h_1$$

! recuerde que todo grupo tiene subgrupo(s) cíclico(s)

Teorema: Sea G un grupo cíclico de orden finito $n < \infty$.

Luego, para cualquier divisor m de n existe un único subgrupo cíclico H de orden m y $H = \langle g^{\frac{n}{m}} \rangle$ si $G = \langle g \rangle$

Dem: Sea $H \leq G$, llamamos k al menor entero positivo t.q. $g^k \in H$.

Vamos a demostrar $H = \langle g^k \rangle$

orden del subgrupo.

Esto equivale a mostrar que $g^l \in H \Leftrightarrow k \mid l$.

$(\Leftarrow)$ $l = kq$, $g^l = g^{kq} = (g^k)^q \in H$.

$(\Rightarrow)$ Sean q, r:

$$l = kq + r$$

$$0 \leq r \leq k$$

$$g^l = g^{kq+r} = g^{kq} \cdot g^r$$

$$g^r = g^{l-kq} \in H$$

Pero $r < k$ y k es el menor entero positivo $(\Rightarrow\Leftarrow)$ lo que contradice la elección de k, luego r debe ser cero.

Para acabar: $\boxed{g^n} = \boxed{1 \in H} \rightarrow n$ debe estar en H.

el orden de un elemento es g^n t.q es 1.

$\Leftrightarrow k \mid n$, $\exists m : km = n \Leftrightarrow k = \frac{n}{m}$

Homomorfismos de grupos

Sean H, G grupos. Un homomorfismo de grupos $\varphi : G \to H$

$$\varphi(\underbrace{g_1 g_2}_{\text{operación en } G}) = \varphi(g_1) \underbrace{\cdot}_{\text{operación en } H} \varphi(g_2)$$

$\forall\, g_1, g_2 \in G$. De la def. sigue:

$$\varphi(1_G) =$$

$$\varphi(g^{-1})$$

Un homomorfismo invertible se llama isomorfismo.

Dos grupos son isomorfos si existe un isomorfismo entre ellos y en este caso $G \cong H$.

Teorema: Dos grupos cíclicos con el mismo orden son isomorfos. (es un sii).

Dem: Sean $G = \langle g \rangle$, $H = \langle h \rangle$, cilíndricos del mismo orden.

Definimos $\varphi : G \to H$, $g^m \mapsto h^m$ → de un generador a otro.

- Si $|G| = \infty$, también $|H| = \infty$ entonces $g^{m_1} \neq g^{m_2}$ $\forall\, m_1 \neq m_2$ y φ está bien def.

⊙ Si $|G| = n = |H|$

$$g^k = g^l \iff g^{k-l} = 1$$
$$\iff n \mid k-l$$
$$\iff h^{k-l} = 1$$
$$\iff h^k = h^l$$

está bien def.

⊙ Quiero decir φ homomorfismo:

$$\varphi(g^k \cdot g^l) = \varphi(g^{k+l}) = h^{k+l}$$
$$= h^k \cdot h^l = \varphi(g^k) \cdot \varphi(g^l)$$

⊙ φ es sobreyectiva:

Sea $h^l \in H$, $\varphi(g^l) = h^l$

⊙ φ es inyectiva:

- Si $|G| = |H| = \infty$, $g^{m_1} \neq g^{m_2}$, $h^{m_1} \neq h^{m_2}$
- Si $|G| = n = |H|$ y

$$\varphi(g^{m_1}) = \varphi(g^{m_2})$$
$$h^{m_1} = h^{m_2}$$

$\rightsquigarrow$ si dos elemen son iguales tienen la misma imagen.

Obs: el único (a menos de isomorfismo) grupo cíclico de orden n se denota C_n

ej: C_{12} $\to$ todos los divisores de 12

$$\begin{tikzcd}
 & C_{12} \arrow[dl, dash] \arrow[dr, dash] & \\
C_6 \arrow[d, dash] \arrow[drr, dash] & & C_4 \arrow[d, dash] \\
C_3 \arrow[dr, dash] & & C_2 \arrow[dl, dash] \\
 & C_1 &
\end{tikzcd}$$

$C_2 \leq C_6 \leq C_{12}$

$\to$ Cada arista significa subgrupo

ej: $\mathbb{Z} \to \mathbb{Z}$ $\to$ ¿Como hacer isomorfismo de ciclos?

$\leftarrow$ tomar el generador de uno y mandarlo al otro generador.

Kernel de grupos

Sea $\varphi: G \to H$ homomorfismo. luego:

① $Im(\varphi) = \{ h \in H : \exists_g \in G \ \varphi(g) = h \}$

② $\ker \varphi \leq G$, y además si $x \in \ker \varphi$ y $g \in G$

$$g x g^{-1} \in \ker \varphi$$

③ $\varphi(g_1) = \varphi(g_2) \iff g_1 g_2^{-1} \in \ker \varphi$.

Dem: ① Sean $h_1, h_2 \in Im \varphi$

luego existen $g_1, g_2 \in G$: $\varphi(g_1) = h_1$, $\varphi(g_2) = h_2$

$$\begin{aligned} h_1 \cdot h_2^{-1} &= \varphi(g_1) \cdot \varphi(g_2)^{-1} \\ &= \varphi(g_1) \cdot \varphi(g_2^{-1}) \\ &= \varphi(g_1 \cdot g_2^{-1}) \end{aligned}$$

$h_1 h_2^{-1} \in \operatorname{Im} \varphi$. $\operatorname{Im}\varphi \leq H$.

② Sean $g_1, g_2 \in \ker \varphi$

$$\varphi(g_1 g_2^{-1}) = \varphi(g_1) \cdot \varphi(g_2)^{-1}$$
$$= 1_H \cdot 1_H^{-1}$$
$$= 1_H$$

$g_1, g_2^{-1} \in \ker \varphi$ y $\ker \varphi \leq G$

Sean $x \in \ker \varphi$ $= \varphi(g) \cdot \varphi(x) \cdot \varphi(g^{-1})$
$$= \varphi(g) \cdot 1_H \cdot \varphi(g^{-1})$$
$$= 1_H$$

Subgrupo Normal Un subgrupo normal H de G es normal si $\forall\, h \in H$, $g \in G$ $ghg^{-1} \in H$. en este caso se escribe

$$H \trianglelefteq G.$$

Tarea Demostrar que $V_4 \cong C_2 \times C_2$.