Clase 2: Centro, Generadores, Morfismos y Teorema de Lagrange

§4. Sub-grupos y generadores (continuación)

(4) **Def/Ejemplo**: Sea G un grupo. El CENTRO de G es el subgrupo

$$Z(G) := \{ h \in G \text{ tq } gh = hg \text{ para todo } g \in G \}$$

⚠ En particular, G abeliano $\iff Z(G) = G$.

Por ejemplo: Si $G = S_n$ con $n \geq 1$ entonces

a) Si $n = 1$ ó 2: $Z(S_n) = S_n$ pues S_1 y S_2 abelianos

b) Si $n \geq 3$: $Z(S_n) = \{Id\}$. Sea $\sigma \neq Id \rightsquigarrow \exists i$ tq $\sigma(i) = j \neq i$

Como $n \geq 3$, $\exists k \in \{1, \ldots, n\}$ tq $i \neq k$ y $j \neq k$. Sea $\tau := (j, k) \in S_n$

$\Rightarrow \sigma\tau(i) = \sigma(i) = j$, $\tau\sigma(i) = \tau(j) = k \rightsquigarrow \sigma\tau \neq \tau\sigma \Rightarrow \sigma \notin Z(S_n)$.

$\boxed{\text{Ejercicio}}$ Probar que $Z(GL_n(k)) = \{\lambda I_n, \ \lambda \in k^{\times}\}$ y calcular $Z(D_n)$.

[Ind: $I_n + E_{ij}$ con $i \neq j$] ↳ homotecias

Queremos imitar el concepto de "familia generadora" que conocemos de Álgebra Lineal:

Proposición 2.1.10. — *Sea A un sub-conjunto de un grupo G. Entonces, existe un sub-grupo de G conteniendo a A el cual es minimal respecto a la inclusión (es decir, el más pequeño posible). Dicho sub-grupo es llamado el* **sub-grupo generado por** *A y lo denotamos por $\langle A \rangle$.*

Dem: $\langle A \rangle \overset{\text{def}}{:=} \bigcap_{\substack{A \subseteq H \\ H \leq G}} H$ verifica lo pedido ✓

Explícitamente

$$\langle A \rangle = \{ x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} , \ n \in \mathbb{N} , \ x_i \in A , \ \varepsilon_i \in \{-1,1\} \} \qquad \blacksquare$$

Obs: Si G es abeliano y usamos la notación aditiva

$$\langle A \rangle = \{ m_1 x_1 + \cdots + m_n x_n , \ n \in \mathbb{N} , \ x_i \in A , \ m_i \in \mathbb{Z} \}$$

Terminología: Sea G un grupo y $A \subseteq G$ un subconjunto (no nec. un subgrupo!). Decimos que:

i) A es un CONJUNTO GENERADOR de G (o que A GENERA G) si $\langle A \rangle = G$

ii) G es FINITAMENTE GENERADO (o DE TIPO FINITO) si $\exists A_0 \subseteq G$ conjunto finito tq $G = \langle A_0 \rangle$

Obs: Si $A_0 = \{g_1, \dots, g_r\} \subseteq G$ conjunto finito, entonces escribimos $\langle A_0 \rangle =: \langle g_1, \dots, g_r \rangle$ al subgrupo generado por $g_1, \dots, g_r$.

Def: Decimos que un grupo G es CÍCLICO si puede ser generado por un elemento, ie, $\exists g \in G$ tal que $G = \langle g \rangle$.

$\boxed{\text{Ejercicio}}$: Probar que si G es cíclico entonces G es abeliano.

Ejemplos:

① Grupos finitos: Todo grupo finito G es finitamente generado, pues $G = \langle G \rangle$.

② Enteros: $(\mathbb{Z}, +)$ es un grupo cíclico generado por 1 o -1.

③ Enteros módulo n: Sea $n \in \mathbb{N}^{\geq 2}$, entonces $\mathbb{Z}/n\mathbb{Z}$ es un grupo cíclico: $\mathbb{Z}/n\mathbb{Z} = \langle [k]_n \rangle$ para cualquier $k \in \mathbb{Z}$ tq $\mathrm{mcd}(k,n) = 1$.

En efecto: Por Bézout, $\exists x, y \in \mathbb{Z}$ tq $xn + yk = \mathrm{mcd}(k,n) = 1$ $(\star)$
$(\Rightarrow yk \equiv 1 \pmod{n} \underset{n\geq 2}{\Longrightarrow} y \not\equiv 0 \mod n)$
Sea $m \in \{0, 1, \dots, n-1\}$ arbitrario y consideramos $m(\star)$:
$mxn + myk = m \Rightarrow m \equiv lk \pmod{n}$, con $l = ym$. $\blacksquare$

④ Con la notación de la Clase 1, el grupo diedral

$$D_n = \{ I_2, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s \}$$

está generado por r y s, ie, $D_n = \langle r, s \rangle$

⑤ El grupo simétrico S_n está generado por todas las transposiciones (pues toda permutación se escribe como producto de transposiciones!)

$\boxed{\text{Ejercicio}}$ Probar que:

i) Las trasposiciones $(1,2), (2,3), \ldots, (n-1,n)$ generan S_n.

ii) La transposición $(1,2)$ y el "ciclo" $(2,3,\ldots,n,1)$ generan S_n.

$\boxed{\text{Ejercicio}}$ Probar que todo grupo finitamente generado es NUMERABLE.

↳ Recuerdo: Un conjunto $X \neq \emptyset$ es NUMERABLE si $\exists f : \mathbb{N} \xrightarrow{\text{sobre}} X$

$\Longleftrightarrow$ (Sub-ejercicio) $\exists f : S \twoheadrightarrow X$ con S numerable $\Longleftrightarrow \exists g : X \hookrightarrow S$ inyectiva con S numerable.

⑥ $(\mathbb{Q},+)$ <u>NO</u> es finitamente generado.

(En part, no todo grupo numerable es fin. generado !)

En efecto: Sup. que $A_0 = \left\{\frac{p_1}{q_1}, \dots, \frac{p_r}{q_r}\right\} \subseteq \mathbb{Q}$ es un conj. generador, con $\mathrm{mcd}(p_i,q_i)=1$.

Sea l un primo que NO divide $q_1\cdots q_r$.

$\Rightarrow$ $1/l \in \mathbb{Q}$ <u>NO</u> puede ser generado por A_0:

Los elementos de $\langle A_0\rangle$ son de la forma

$$m_1\frac{p_1}{q_1}+\dots+m_r\frac{p_1}{q_r} = \frac{(\cdots)}{q_1\cdots q_r} \qquad \text{con } m_1,\dots,m_r\in\mathbb{Z}$$

pero $\dfrac{(\cdots)}{q_1\cdots q_r} = \dfrac{1}{l} \Rightarrow l \mid q_1\cdots q_r$ ↯ $\blacksquare$

$\boxed{\text{Ejercicio}}$ Sea G el subgrupo de $GL_2(\mathbb{Q})$ generado por las matrices

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad y \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(En part, $G = \langle A, B \rangle$ es fin. generado). Demostrar que el subgrupo $H \leq G$ formado por los elementos de G cuyos coeficientes en la diagonal son todos iguales a 1 NO es finitamente generado.

Consecuencia: Un sub-grupo de un grupo finitamente generado NO es necesariamente finitamente generado!

↳ cf. Espacios vectoriales: Si $\dim_{\mathbb{R}}(V) < +\infty$ y $W \subseteq V$ sub-ev $\Rightarrow \dim_{\mathbb{R}}(W) < +\infty$.

§5. Morfismos de grupos

Del mismo modo que consideramos aplicaciones lineales entre espacios vectoriales, tenemos:

Terminología "moderna" (cf. Teoría de Categorías)

Def: Un MORFISMO de grupos (o HOMOMORFISMO) es una aplicación $f: G \to G'$ entre grupos tal que

$$f(g_1 g_2) = f(g_1) f(g_2) \quad \text{para todos } g_1, g_2 \in G.$$

$\boxed{\text{Obs / Ejercicio}}$:

1°) Necesariamente $f(e_G) = e_{G'}$. [Indicación: $e_G \cdot e_G = e_G$]

2°) Si f es un morfismo de grupos BIYECTIVO, entonces $f^{-1}: G' \to G$ también es un morfismo de grupos (i.e., $f^{-1}(g_1' g_2') = f^{-1}(g_1') f^{-1}(g_2')$ $\forall g_1', g_2' \in G'$).

3°) Si G, G' son abelianos y usamos la notación aditiva:

$$f(g_1 + g_2) = f(g_1) + f(g_2)$$

Terminología: Sea $f: G \to G'$ un morfismo de grupos.
Decimos que:

1) $f: G \xrightarrow{\sim} G'$ es un ISOMORFISMO si f es biyectivo $\rightsquigarrow G \cong G'$
2) $f: G \to G$ es un ENDOMORFISMO si $G = G'$
3) $f: G \xrightarrow{\sim} G$ es un AUTOMORFISMO si es un endomorfismo biyectivo.

Tal como para el caso de espacios vectoriales, definimos

$$\ker(f) := \{g \in G \text{ tq } f(g) = e_{G'}\} \quad \text{e} \quad \mathrm{Im}(f) := \{f(g),\ g \in G\}$$

En part, f inyectivo (resp. sobreyectivo) si y sólo si $\ker(f) = \{e_G\}$ (resp. $\mathrm{Im}(f) = G'$). Más aún, $\ker(f) \leq G$ e $\mathrm{Im}(f) \leq G'$ son subgrupos! $\underbrace{f(g \cdot g^{-1})}_{=f(e)=e} = \underbrace{f(g)}_{=e} f(g^{-1}) \Rightarrow f(g^{-1}) = e$ etc.

Mejor todavía:

$\boxed{\text{Ejercicio}}$ Sea $f: G \to G'$ morfismo de grupos, y sean $H \leq G$ y $H' \leq G'$ subgrupos. Probar que $f^{-1}(H') \leq G$ y $f(H) \leq G'$ son subgrupos.

Ejemplos:

① Sea $n \in \mathbb{N}^{\geq 1}$. La proyección canónica

$$\pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}, \quad m \longmapsto [m]_n$$

es un morfismo sobreyectivo. Además, $\ker(\pi) = n\mathbb{Z}$.

② La signatura $\varepsilon : S_n \longrightarrow \{\pm 1\}$ ← grupo mult., $\sigma \longmapsto \varepsilon(\sigma)$ es un morfismo ($\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$) de grupos, sobreyectivo si $n \geq 2$.

El kernel de ε, conformado por todas las permutaciones <u>pares</u> de S_n, es llamado el GRUPO ALTERNANTE, $A_n := \ker(\varepsilon)$ $\xleftrightarrow{\text{Latex}}$ $\mathfrak{A}_n$

$\boxed{\text{Ejercicio}}$ Sup. que $n \geq 3$. Probar que A_n está generado por los "3-ciclos" (a,b,c) (← permutación $a \mapsto b \mapsto c$ y fija el resto)

[Indicación: $(a,b)(a,c) = (a,c,b)$ y $(a,b)(c,d) = (a,c,d)(a,c,d)$.]

③ La exponencial

$$\exp : (\mathbb{C}, +) \twoheadrightarrow (\mathbb{C}^\times, \cdot) \quad , \quad z \mapsto e^z$$

es un morfismo sobreyectivo. Además, $\ker(\exp) = 2\pi i \mathbb{Z} \leq \mathbb{C}$.

$\rightsquigarrow e^{2\pi i k} = 1$

④ Sea k un cuerpo. El determinante

$$\det : GL_n(k) \twoheadrightarrow k^\times \quad , \quad M \longmapsto \det(M)$$

es un morfismo sobreyectivo. Definimos

$$SL_n(k) := \ker(\det) \overset{\text{def}}{=} \{ M \in GL_n(k) \text{ tq } \det(M) = 1 \}.$$

$\rightsquigarrow$ GRUPO ESPECIAL LINEAL.

⑤ Sea G un grupo. Entonces

$$\mathrm{Aut}(G) := \{ f : G \xrightarrow{\sim} G \text{ automorfismo} \}$$

ley de grupos: composición de funciones

es el GRUPO DE AUTOMORFISMOS DE G.

$\boxed{\text{Obs / Ejercicio}}$ Dado $g \in G$, la aplicación $\iota_g : G \to G$, $x \mapsto g x g^{-1}$ es un automorfismo de G. $\rightsquigarrow$ "AUTOMORFISMO INTERNO"

Más aún, $\iota : G \to \mathrm{Aut}(G)$, $g \mapsto \iota_g$ es un morfismo de grupos, con $\ker(\iota) = Z(G)$ el centro de G.

§6. Clases laterales

Para fijar ideas: $G = \mathbb{Z}$, $H = n\mathbb{Z}$

Sea G un grupo y $H \leq G$ un subgrupo. Consideremos la sgte relación de equivalencia en G:

$$g_1 \sim g_2 \overset{\text{def}}{\Longleftrightarrow} \exists\, h \in H \text{ tal que } g_2 = g_1 h$$

Denotamos por $gH := \{gh,\ h \in H\}$ la clase de equiv. de $g \in G$.

→ "CLASE LATERAL IZQUIERDA"

El cociente $G/\sim$, formado por las clases laterales izquierdas de G, será denotado

$$G/H \overset{\text{def}}{=} \{gH,\ g \in G\}$$

Notación importante: $[G:H] :=$ Cardinal de G/H ⇝ ÍNDICE de H en G.

⚠ También podemos considerar $Hg := \{hg,\ h \in H\}$ "CLASES LATERALES DERECHAS" y el respectivo cociente $H\backslash G := \{Hg,\ g \in G\}$.

__Observación clave:__

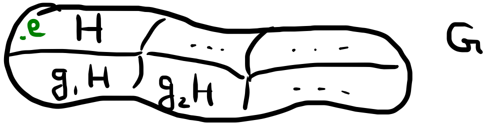
① $\Phi : G \xrightarrow{\sim} G$, $g \mapsto g^{-1}$ envía gH en Hg^{-1} (pues $(gh)^{-1} = h^{-1}g^{-1}$)

$\Longrightarrow$ Hay una biyección $G/H \xrightarrow{1:1} H\backslash G$ ✓

② Dado $g \in G$, la aplicación $H \longrightarrow G$, $h \mapsto gh$ induce una biyección $H \xrightarrow{1:1} gH$ ✓ (con inversa $gh \xmapsto{g^{-1}\cdot} h$)

↪ En part, si H finito: $\mathrm{Card}(gH) = \mathrm{Card}(H) \overset{\text{def}}{=} |H|$ ← constante! (indep. de g)

Dado que las clases laterales $\{gH, g \in G\}$ forman una partición de G y dado que $\mathrm{Card}(G/H) \overset{\text{def}}{=} [G:H]$, deducimos:



Teorema 2.1.17 (Teorema de Lagrange). — *Sea H un sub-grupo de un grupo finito G. Entonces*

$$|G| = |H|[G:H].$$

$\Longleftrightarrow [G:H] = \dfrac{|G|}{|H|}$.

En particular, el orden de un sub-grupo de G divide el orden de G.

(Lagrange 1771, Gauss 1801, Cauchy 1844, Jordan 1861)