

Grupos. Parte 3.

Silvio Reggiani

Complementos de Matemática II (LCC)
Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Universidad Nacional de Rosario

27 de octubre de 2020

Ejemplo no abeliano

- ▶ $G = GL(2, \mathbb{R})$ matrices invertibles 2×2 ,
- ▶ $H = SL(2, \mathbb{R}) = \{A \in GL(2, \mathbb{R}) : \det A = 1\}$,
- ▶ $H < G$: $A, B \in H \implies \det(AB^{-1}) = (\det A)(\det B)^{-1} = 1$,
- ▶ $H \triangleleft G$: si $A \in H$ y $B \in G$, entonces

$$\det(BAB^{-1}) = (\det B)(\det A)(\det B)^{-1} = \det A = 1$$

y por ende $BAB^{-1} \in H$.

- ▶ ¿Qué grupo es $GL(2, \mathbb{R})/SL(2, \mathbb{R})$?

Ejemplo

- ▶ Sea D_n el grupo de simetrías de un polígono regular de n lados.
- ▶ $D_n = \langle R, \tau \rangle$.
- ▶ R = rotación en $\frac{2\pi}{n}$ radianes.
- ▶ τ = una reflexión.
- ▶ $H := \langle R \rangle \triangleleft D_n$. En efecto,

$$[D_n : H] = \frac{|D_n|}{|H|} = \frac{2n}{n} = 2 \xRightarrow{\text{ejercicio}} H \triangleleft D_n.$$

- ▶ $D_n/H \simeq \mathbb{Z}_2$ (es la única posibilidad).

Ejemplo

Si $\varphi : G \rightarrow H$ es un morfismo de grupos, entonces

$$\ker \varphi = \{g \in G : \varphi(g) = e\} \triangleleft G.$$

En efecto,

- ▶ si $\varphi(k) = e$, entonces $\forall g \in G$,

$$\begin{aligned}\varphi(gkg^{-1}) &= \varphi(g)\varphi(k)\varphi(g^{-1}) \\ &= \varphi(g)\varphi(g^{-1}) \\ &= \varphi(g)\varphi(g)^{-1} \\ &= e.\end{aligned}$$

- ▶ ¿Qué grupo es $G/\ker \varphi$?

Teoremas de isomorfismo

Teorema (de factorización)

Sean $H \triangleleft G$ y $\varphi : G \rightarrow K$ un morfismo de grupos tal que $H \subset \ker \varphi$. Entonces existe un único morfismo de grupos $\bar{\varphi} : G/H \rightarrow K$ tal que $\bar{\varphi} \circ \pi = \varphi$.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & K \\ & \searrow \pi & \nearrow \exists! \bar{\varphi} \\ & G/H & \end{array}$$

Demostración.

- Definimos $\bar{\varphi}(gH) := \varphi(g)$. (Esto implica la **unicidad**.)
- Buena definición:

$$\begin{aligned}g_1H = g_2H &\implies g_1^{-1}g_2 \in H \\&\implies \varphi(g_1^{-1}g_2) = e && [H \subset \ker \varphi] \\&\implies \varphi(g_1)^{-1}\varphi(g_2) = e \\&\implies \varphi(g_1) = \varphi(g_2).\end{aligned}$$

- $\bar{\varphi}$ es morfismo:

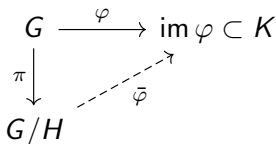
$$\begin{aligned}\bar{\varphi}((g_1H)(g_2H)) &= \bar{\varphi}((g_1g_2)H) \\&= \varphi(g_1g_2) \\&= \varphi(g_1)\varphi(g_2) \\&= \bar{\varphi}(g_1H)\bar{\varphi}(g_2H).\end{aligned}$$



Corolario (primer teorema de isomorfismo)

Si $\varphi : G \rightarrow K$ es un morfismo de grupos entonces $\text{im } \varphi \simeq G / \ker \varphi$.
En particular, si φ es un epimorfismo, entonces $K \simeq G / \ker \varphi$.

Demostración.



- Aplicamos el teorema anterior a $H = \ker \varphi$.
- Debemos ver que $\bar{\varphi}$ es inyectiva.

$$\begin{aligned}\bar{\varphi}(g_1 H) = \bar{\varphi}(g_2 H) &\iff \varphi(g_1) = \varphi(g_2) \\ &\iff \varphi(g_1)^{-1} \varphi(g_2) = e \\ &\iff \varphi(g_1^{-1} g_2) = e \\ &\iff g_1^{-1} g_2 \in H = \ker \varphi \\ &\iff g_1 H = g_2 H.\end{aligned}$$



Corolario (segundo teorema de isomorfismo)

Si G, H son subgrupos de un grupo K y H es normal en K , entonces

$$\frac{GH}{H} \simeq \frac{G}{G \cap H}. \quad (1)$$

Demostración.

Antes que nada notemos que los cocientes (1) son efectivamente grupos. En efecto,

- ▶ $H \triangleleft K \implies H \triangleleft GH \implies GH/H$ es grupo.
- ▶ Si $h \in G \cap H$ y $g \in G$, entonces $ghg^{-1} \in H$ pues $H \triangleleft K$ y $ghg^{-1} \in G$ pues H es subgrupo. Luego $ghg^{-1} \in G \cap H$ y por lo tanto $G \cap H$ es normal en G .

Demostración (cont.).

- Definimos $\varphi : G \rightarrow GH/H$ como sigue

$$\begin{array}{ccccc} G & \hookrightarrow & GH & \xrightarrow{\pi} & \frac{GH}{H}. \\ & & \searrow \varphi & & \uparrow \end{array}$$

- $\ker \varphi = G \cap H$. (En realidad esto implica que $G \cap H \triangleleft G$, por lo que no hacía falta probarlo antes.)
- φ es sobre: cualquier elemento en GH es de la forma gh . En efecto, en primer lugar notemos que si $g \in G, h \in H$, entonces

$$hg = gg^{-1}hg = gh', \quad h' \in H. \quad (2)$$

IMPORTANTE: esto sólo se puede hacer porque H es normal.

Demostración (cont.).

- ▶ Como un elemento genérico en GH tiene la forma $x = a_1 a_2 \cdots a_n$ con $a_i \in G \cup H$ podemos usar (2) para reescribir

$$x = a'_1 \cdots a'_s a''_1 \cdots a''_t, \quad a'_i \in G, a''_j \in H.$$

- ▶ Finalmente,

$$\frac{G}{\ker \varphi} \simeq \frac{G}{G \cap H} \simeq \operatorname{im} \varphi = \frac{GH}{H}.$$



Corolario (tercer teorema de isomorfismo)

Sean $K \subset H \subset G$ subgrupos tales que $K \triangleleft G$, $H \triangleleft G$. Entonces

$$G/H \simeq \frac{G/K}{H/K}.$$

Ejercicio importante

Sea $K \triangleleft G$. Probar que:

- ▶ Los subgrupos de G/K son todos de la forma H/K con H subgrupo de G tal que $K \subset H$;
- ▶ si $H \triangleleft G$ y $K \subset H$, entonces $H/K \triangleleft G/K$.

Usando este ejercicio vemos que todos los cocientes en el enunciado del corolario son grupos.

Demostración.

$$\begin{array}{ccc} G & \xrightarrow{\pi_H} & G/H \\ \pi_K \downarrow & \nearrow \exists! \varphi & \\ G/K & & \end{array}$$

► $K = \ker \pi_K \subset H = \ker \pi_H \implies \exists! \varphi.$

► $\pi_H \text{ epi} \implies \varphi \text{ epi}.$

► $\ker \varphi = H/K$. En efecto,

$$\varphi(gK) = \varphi(\pi_K(g)) = \pi_H(g) = gH$$

y por ende

$$\varphi(gK) = e (= eH) \iff g \in H.$$

Luego,

$$G/H = \text{im } \varphi \simeq \frac{G/K}{\ker \varphi} = \frac{G/K}{H/K}.$$



Ejemplos

Ejemplo

Si G es un grupo cíclico, entonces $G \simeq \mathbb{Z}$ o $G \simeq \mathbb{Z}_n$. En efecto,

- ▶ $G = \langle g \rangle$.
- ▶ Defino $\varphi : \mathbb{Z} \rightarrow G$, $\varphi(n) = g^n$ (epi de grupos).
- ▶ Analizamos el núcleo de φ :
 - ▶ $\ker \varphi = \{0\} \implies G \simeq \mathbb{Z}/\{0\} = \mathbb{Z}$.
 - ▶ $\ker \varphi \neq 0 \implies (\exists n, \ker \varphi = n\mathbb{Z}) \implies G \simeq \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Ejemplo

► $\text{cis} : \mathbb{R} \rightarrow \mathbb{C} - \{0\},$

$$\text{cis}(t) := e^{2\pi it} = \cos(2\pi t) + i \sin(2\pi t).$$

- cis es morfismo de grupos: $e^{2\pi i(t_1+t_2)} = e^{2\pi it_1} e^{2\pi it_2}$ (probarlo como ejercicio). Recordar que \mathbb{R} es un grupo con la suma y $\mathbb{C} - \{0\}$ es un grupo con la multiplicación.
- $\text{im cis} = S^1 = \{z \in \mathbb{C} : |z| = 1\}.$
- $\text{ker cis} = \{t \in \mathbb{R} : e^{2\pi it} = 1\} = \mathbb{Z}.$
- Por el 1er teorema de isomorfismo tenemos que

$$S^1 = \mathbb{R}/\mathbb{Z}.$$

Ejemplo

- ▶ $\det : GL(2, \mathbb{R}) \rightarrow \mathbb{R} - \{0\}$ es epi de grupos ¿por qué?
- ▶ $\ker \det = \{A \in GL(2, \mathbb{R}) : \det A = 1\} = SL(2, \mathbb{R})$.
- ▶ $GL(2, \mathbb{R})/SL(2, \mathbb{R}) \simeq \mathbb{R} - \{0\}$.

Ejemplo

El mismo argumento funciona para matrices (cuadradas) de cualquier tamaño:

$$\frac{GL(n, \mathbb{R})}{SL(n, \mathbb{R})} \simeq \mathbb{R} - \{0\},$$

incluso se pueden cambiar los reales por otro cuerpo, por ejemplo

$$\frac{GL(n, \mathbb{C})}{SL(n, \mathbb{C})} \simeq \mathbb{C} - \{0\}.$$

Comentario

Estos grupos continuos son muy importantes en geometría.

Ejemplo

$$\frac{\mathbb{Z}_{mn}}{\mathbb{Z}_m} \simeq \mathbb{Z}_n.$$

- ▶ Lo primero que hay que entender es **qué significa que \mathbb{Z}_m sea un subgrupo de \mathbb{Z}_{mn} .**
- ▶ \mathbb{Z}_m es un subgrupo cíclico de orden m y el único subgrupo cíclico de orden m en \mathbb{Z}_{mn} es el generado por n , es decir, $n\mathbb{Z}/mn\mathbb{Z}$.
- ▶ Luego,

$$\frac{\mathbb{Z}_{mn}}{\mathbb{Z}_m} = \frac{\mathbb{Z}/mn\mathbb{Z}}{n\mathbb{Z}/mn\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n \quad [3er \text{ Teor. Isom.}].$$

Ejercicio

Si G es un grupo cíclico de orden n y $q \mid n$, entonces G tiene exactamente un subgrupo (cíclico) de orden q .

Ejemplo (grupo producto)

- G, H grupos $\implies G \times H$ es un grupo definiendo

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2) \quad (\text{ejercicio}).$$

- $G_1 \triangleleft G, H_1 \triangleleft H \implies G_1 \times H_1 \triangleleft G \times H$. En efecto,

$$\begin{aligned}(g, h)(g_1, h_1)(g, h)^{-1} &= (g, h)(g_1, h_1)(g^{-1}, h^{-1}) \\ &= (\underbrace{gg_1g^{-1}}_{\in G_1}, \underbrace{hh_1h^{-1}}_{\in H_1}) \in G_1 \times H_1.\end{aligned}$$

► $\frac{G \times H}{G_1 \times H_1} \simeq \frac{G}{G_1} \times \frac{H}{H_1}$

$$\begin{array}{ccc} G \times H & \xrightarrow{\pi_G \times \pi_H} & \frac{G}{G_1} \times \frac{H}{H_1} \\ \pi \downarrow & \nearrow \exists! \text{ iso} & \\ \frac{G \times H}{G_1 \times H_1} & & \end{array}$$

Grupo libre

Sea X un conjunto. El **grupo libre** F_X en X consiste de todas las palabras

$$x_1 x_2 \cdots x_n$$

en donde aplican las siguientes reglas:

- ▶ $x \in X \implies x^{-1} \notin X$,
- ▶ $x_i \in X$ ó $x_i \in X^{-1} := \{x^{-1} : x \in X\}$,
- ▶ $() = e$ (notación).
- ▶ **Multiplicación:** yuxtaposición de palabras.
- ▶ **Reglas de reducción:** $\forall x \in X$,
 - ▶ $xx^{-1} = e$,
 - ▶ $x^n = xx \cdots x$ (n veces).

Palabras reducidas

Se simplifica todo lo que se pueda simplificar. Por ejemplo, si

$x, y, z \in X$,

- ▶ $xy^3x^{-1}zxy$, xy , x , yx^2 son palabras reducidas;
- ▶ x^3x , $x^3yy^{-1}x$, $xy^2zy(zy)^{-1}x^{-1}$ no son palabras reducidas.

Proposición

F_X es un grupo.

Observación

- ▶ $X = \emptyset \implies F_X = \{e\}$.
- ▶ $X = \{*\} \implies F_X \simeq \mathbb{Z}$.
- ▶ $|X| \geq 2 \implies F_X$ es no abeliano.

Definición

Un grupo G se dice **libre** si existe un conjunto X tal que $G \simeq F_X$.

Proposición (propiedad universal)

Sean X un conjunto, G un grupo y $f : X \rightarrow G$ una función.

Entonces existe un único morfismo de grupos $\varphi : F_X \rightarrow G$ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} X & \xrightarrow{f} & G \\ & \searrow & \nearrow \exists! \varphi \\ & F_X & \end{array}$$

Más aún, F_X está unívocamente determinado, salvo isomorfismo, por esta propiedad.

Aclaración

Decir que un grupo \tilde{F} tiene la misma propiedad universal que F_X significa que en el diagrama anterior podemos reemplazar F_X por \tilde{F} y \hookrightarrow por una función inyectiva $i : X \rightarrow \tilde{F}$.

Idea de la prueba.

- ▶ Para $x \in X$ definimos

$$f(x^{-1}) = f(x)^{-1}.$$

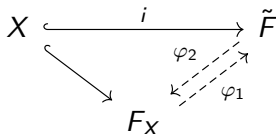
- ▶ Dada una palabra $x_1x_2 \cdots x_n \in F_X$ chequear que

$$\varphi(x_1x_2 \cdots x_n) := f(x_1)f(x_2) \cdots f(x_n)$$

está bien definida y es un morfismo de grupos (observar que el lado derecho garantiza la unicidad).

Idea de la prueba (cont.)

- Si un grupo \tilde{F} tiene la misma propiedad universal que F_X , podemos construir morfismos



- $\varphi_2 \circ \varphi_1 = \text{id}_{F_X}$ (coinciden en todo $x \in X$).
- $\varphi_1 \circ \varphi_2 = \text{id}_{\tilde{F}}$ (coinciden en todo $i(x) \in i(X)$).
- φ_1 isomorfismo con inversa φ_2 .



Corolario

Si X es biyectivo con Y , entonces $F_X \simeq F_Y$.

Demostración.

- ▶ Sea $f : X \rightarrow Y$ una biyección.
- ▶ Construimos un morfismo

$$\begin{array}{ccccc} X & \xrightarrow{f} & Y & \hookrightarrow & F_Y \\ & \searrow & & \nearrow \varphi & \\ & & F_X & & \end{array}$$

- ▶ φ es un isomorfismo (ejercicio).

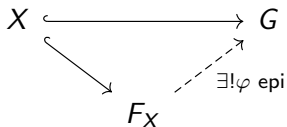


Corolario

Cualquier grupo G es imagen mórfica de un grupo libre.

Demostración.

- ▶ Considerar X un conjunto de generadores de G y F_X el grupo libre en X .
- ▶ Construimos un epimorfismo



Comentario

Uno puede hacer la construcción anterior eligiendo los generadores de G de manera más inteligente.

Generadores y relaciones

Presentamos una forma de construir el grupo “más libre posible” en una familia de generadores sujetos a ciertas relaciones (es decir, que satisfacen ciertas ecuaciones).

- ▶ Sea S un conjunto, F_S el grupo libre en S y \mathcal{R} una familia de “relaciones” que involucran elementos de S . Por ejemplo,
 - ▶ $S = \{a, b\}$, $\mathcal{R} = \{ab = ba\}$;
 - ▶ $S = \{a, b, c\}$, $\mathcal{R} = \{a^3 = b^2 = abc^{-1} = e\}$.
- ▶ Cualquier familia de relaciones \mathcal{R} puede escribirse como

$$\{E_1 = E_2 = \cdots = e\},$$

en donde los E_i son elementos de F_S , y por ende, es común identificar \mathcal{R} con $\{E_1, E_2, \dots\}$.

- ▶ Sea $N_{\mathcal{R}}$ el **subgrupo normal generado por \mathcal{R}** :

$$N_{\mathcal{R}} := \bigcap_{\mathcal{R} \subset H \triangleleft F_S} H.$$

Definición

El grupo presentado por los generadores S y las relaciones \mathcal{R} es

$$\langle S \mid \mathcal{R} \rangle := F_S / N_{\mathcal{R}}.$$

Observación/Ejercicio

- ▶ $\langle S \mid \mathcal{R} \rangle$ está generado por $\{\pi(s) : s \in S\}$, en donde $\pi : F_S \rightarrow F_S / N_{\mathcal{R}}$ es la proyección al cociente.
- ▶ Todas las relaciones o ecuaciones de \mathcal{R} se satisfacen en $\langle S \mid \mathcal{R} \rangle$.

Ejemplo

- ▶ $\langle S \mid \emptyset \rangle = F_S$.
- ▶ $\langle a, b \mid ab = ba \rangle = \langle a, b \mid aba^{-1}b^{-1} \rangle \simeq \mathbb{Z} \times \mathbb{Z}$.

Para probar esto es útil el siguiente resultado.

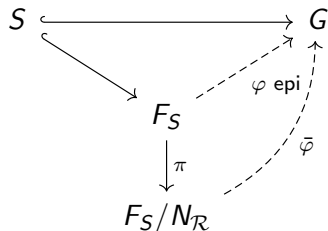
Proposición

Sea G un grupo. Supongamos que $G = \langle S \rangle$ y que los elementos de S satisfacen las relaciones de \mathcal{R} . Entonces existe un epimorfismo de grupos

$$\varphi : \langle S \mid \mathcal{R} \rangle \rightarrow G.$$

En otras palabras, $\langle S \mid \mathcal{R} \rangle$ es el grupo más general posible que está generado por S en el que se cumplen las relaciones de \mathcal{R} .

Idea de la prueba (completar los detalles como ejercicio).



- φ existe por la propiedad universal del grupo libre F_S .
- $\bar{\varphi}$ existe por teorema de factorización. En efecto,

$$\mathcal{R} \subset \ker \varphi \implies N_{\mathcal{R}} \subset \ker \varphi. \quad \square$$

Ejemplo

Volvamos al ejemplo $\langle S \mid \mathcal{R} \rangle = \langle a, b \mid aba^{-1}b^{-1} \rangle \simeq \mathbb{Z} \times \mathbb{Z}$.

- En primer lugar, sabemos que $\mathbb{Z} \times \mathbb{Z}$ está generado por $a = (1, 0)$, $b = (0, 1)$ y satisfacen la relación $aba^{-1}b^{-1} = e$, que en notación aditiva es

$$a + b - a - b = 0.$$

O sea, tenemos un grupo abeliano generado por a y b .

- Por la proposición sabemos que existe un epimorfismo

$$\varphi : \langle S \mid \mathcal{R} \rangle \rightarrow \mathbb{Z} \times \mathbb{Z}.$$

- Todo elemento en $\langle S \mid \mathcal{R} \rangle$ tiene la forma $x = a^m b^n$, pues a y b conmutan.
- $x \in \ker \varphi \iff (0, 0) = \varphi(x) = \varphi(a^m b^n) = (m, n)$. Luego $\ker \varphi = \{e\}$ y por ende $\langle S \mid \mathcal{R} \rangle \simeq \text{im } \varphi = \mathbb{Z} \times \mathbb{Z}$.

Ejemplo/Ejercicio

- ▶ $\langle a \mid a^n = e \rangle \simeq \mathbb{Z}_n$.
- ▶ $\langle a, b \mid a^3 = b^2 = (ab)^2 = e \rangle \simeq D_3$.
- ▶ $\langle a, b \mid a^n = b^2 = (ab)^2 = e \rangle \simeq D_n$.

La construcción por generadores y relaciones también sirve para construir grupos con “ciertas propiedades” deseables. Por ejemplo,

- ▶ $D_\infty := \langle a, b \mid b^2 = (ab)^2 = e \rangle$ (chequear que $|D_\infty| = \infty$).

Ejercicio

Pensar en una presentación por generadores y relaciones para el grupo simétrico S_n .