Grupos. Parte 2.

Silvio Reggiani

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

02 de octubre de 2018

Definiciones y propiedades básicas

Definición

Un **grupo** es un conjunto G dotado de una operación asociativa $G \times G \to G$, $(g, h) \mapsto gh$ tal que

1. Existe un elemento neutro:

$$\exists e \in G, \forall g \in G, (eg = ge = g).$$

2. Existen los inversos:

$$\forall g \in G, \exists g^{-1} \in G, (gg^{-1} = g^{-1}g = e).$$

Nociones más débiles

- **Semigrupo:** no se piden ni 1 ni 2, solo una operación asociativa.
- **Monoide:** se pide 1 pero no 2.

Grupos abelianos

Definición

Decimos que un semigrupo/monoide/grupo G es **abeliano** o **conmutativo** si

$$\forall g, h \in G, (gh = hg).$$

Notación aditiva

Para grupos abelianos en general se prefiere la notación aditiva por sobre la multiplicativa:

$$gh \longleftrightarrow g + h$$
$$e \longleftrightarrow 0$$
$$g^{-1} \longleftrightarrow -g$$

Proposición

En un grupo G, el elemento neutro (también llamado elemento identidad) y los inversos son únicos.

Demostración.

- Sean $e, e' \in G$ dos neutros. Entonces

$$e' = ee' = e.$$

- Sean $h, k \in G$ dos inversos de $g \in G$. Entonces

$$k = ke = k(gh) = (kg)h = eh = h.$$ □

Observación

La primera parte de la prueba también es válida para monoides.

Ejemplos abelianos

1. $(\mathbb{N}, +)$ es un semigrupo.
2. $(\mathbb{N}_0, +)$ es un monoide.
3. $(\mathbb{Z}, +)$ es un grupo.
4. $B = \{\text{True}, \text{False}\}$.
   - (B, AND) es un monoide con $e = \text{True}$, no es grupo.
   - (B, OR) es un monoide con $e = \text{False}$, no es grupo.
   - (B, XOR) es un grupo: $e = \text{False}$, $\text{True}^{-1} = \text{True}$.

AND	True	False
True	True	False
False	False	False

OR	True	False
True	True	True
False	True	False

XOR	True	False
True	False	True
False	True	False

5. $(\mathbb{R}, +)$, $(\mathbb{R}^{>0}, \cdot)$ son grupos.

Más ejemplos

1. $M(n, \mathbb{R}) := \{\text{matrices } n \times n \text{ con coeficientes en } \mathbb{R}\}$ es un grupo abeliano con la suma de matrices pero es un monoide no abeliano con la multiplicación de matrices.
2. $GL(n, \mathbb{R}) := \{A \in M(n, \mathbb{R}) : \det A \neq 0\}$ es un grupo (continuo) con la multiplicación de matrices (notar que $GL(n, \mathbb{R})$ no es un grupo con la suma de matrices ¿por qué?).
3. Monoide de palabras sobre un alfabeto Σ (no abeliano).

Ejercicio (Leyes de cancelación)

Si G es un grupo, valen

- $\forall a, b, c \in G, (ab = ac \implies b = c)$,
- $\forall a, b, c \in G, (ba = ca \implies b = c)$,
- $\forall a, b \in G, [(ab)^{-1} = b^{-1}a^{-1}]$,
- $\forall a \in G, [(a^{-1})^{-1} = a]$.

Más ejemplos

Ejemplo: grupo opuesto

- Partimos de un grupo $(G, \cdot)$.
- El **grupo opuesto** G^{op} se define como $(G, \cdot_{\mathrm{op}})$, es decir, el conjunto subyacente es el mismo pero con una nueva operación
$$g \cdot_{\mathrm{op}} h := h \cdot g.$$
- Esto puede interpretarse como un objeto dual, lo cual formalizaremos más adelante.
- Observemos que G^{op} tiene el mismo elemento neutro y los mismos inversos que G:
  - $e \cdot_{\mathrm{op}} g = g \cdot e = g = e \cdot g = g \cdot_{\mathrm{op}} e$,
  - $g^{-1} \cdot_{\mathrm{op}} g = g \cdot g^{-1} = e = g^{-1} \cdot g = g \cdot_{\mathrm{op}} g^{-1}$.
- La inversión $\mathrm{inv} : G \to G^{\mathrm{op}}$ es biyectiva y satisface $\mathrm{inv}(g \cdot h) = \mathrm{inv}(g) \cdot_{\mathrm{op}} \mathrm{inv}(h)$ (isomorfismo de grupos).

Morfismos de (semi)grupos

Definición

Sean G, H dos semigrupos/grupos. Una función $\varphi : G \to H$ se dice un **morfismo** de semigrupos/grupos si

$$\forall g, g' \in G, [\varphi(gg') = \varphi(g)\varphi(g')].$$

Además, si φ es

- inyectiva, φ se dice un **monomorfismo**;
- sobreyectiva, φ se dice un **epimorfismo**;
- biyectiva, φ se dice un **isomorfismo**.

Observación

Para monoides la definición es diferente, como veremos más adelante.

Ejemplos

- Ya mencionamos el isomorfismo de grupos $D_3 \to S_3$ que asigna a cada simetría de un triángulo equilátero la correspondiente permutación de sus vértices.
- $D_4 \to S_4$ es un monomorfismo, pero no es sobreyectiva (ídem).
- $(\mathbb{N}, +) \hookrightarrow (\mathbb{Z}, +)$ es un morfismo de semigrupos.
- $\text{len} : \text{str}(\Sigma) \to (\mathbb{N}_0, +)$ es un morfismo de monoides. ATENCIÓN: todavía no definimos formalmente qué es un morfismo de monoides.
- $\exp : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$ es un isomorfismo (continuo) de grupos.

Proposición

Sea $\varphi : G \to H$ un morfismo de grupos. Entonces,

- $\varphi(e_G) = e_H$.
- $\forall g \in G, \varphi(g^{-1}) = \varphi(g)^{-1}$.

Demostración.

Para el primer ítem observamos que

$$\varphi(e_G)e_H = \varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$$

y por cancelación a izquierda sigue que $e_H = \varphi(e_G)$.

Para el segundo ítem tenemos que

$$\varphi(g)\varphi(g)^{-1} = e_H = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$$

y por cancelación a izquierda sigue que $\varphi(g)^{-1} = \varphi(g^{-1})$. □

Observación importante

El primer ítem de la demostración no es válido para monoides. ¿Por qué?: para demostrar las leyes de cancelación se usa la existencia de inversos.

Contraejemplo

- $\{a\}$ es monoide (grupo): $aa = a$
- $\{a, b\}$ semigrupo sin identidad:

	a	b
a	a	a
b	a	a

- monoidizamos en $\{e, a, b\}$:

	e	a	b
e	e	a	b
a	a	a	a
b	b	a	a

- $\varphi : \{a\} \hookrightarrow \{a, b, e\}$ morfismo de semigrupos que no preserva la identidad.

Morfismos de monoides

Definición

Sean G, H dos monoides. Una función $\varphi : G \to H$ se dice un **morfismo de monoides** si

- $\varphi(e_G) = e_H$,
- $\forall g, g' \in G, \varphi(gg') = \varphi(g)\varphi(g')$.

Observación

Uno podría pensar en

- **Semigrupo:** $(G, \cdot)$ un conjunto con una operación binaria asociativa (producto);
- **Monoide:** $(G, \cdot, e_G)$ un conjunto con una operación binaria asociativa (producto) y una operación 0-aria (neutro);
- **Grupo:** $(G, \cdot, e_G, (\ )^{-1})$ un conjunto con una operación binaria asociativa (producto), una operación 1-aria (inversos) y una operación 0-aria (neutro);

y definir morfismos como las funciones que preservan estas operaciones. Lo que probamos en la proposición anterior es que, para grupos, si una función preserva el producto, entonces preserva las otras dos operaciones y, por lo tanto, nuestras dos definiciones son equivalentes. Como ya vimos, con monoides la situación es distinta (morfismo de semigrupo no implica morfismo de monoide).

Proposición

Sea $\varphi : M \to M'$ un morfismo de monoides biyectivo. Entonces $\varphi^{-1} : M' \to M$ es un morfismo de monoides. En particular, la inversa de un isomorfismo de grupos es un morfismo de grupos.

Demostración.

- $\varphi(e) = e' \implies \varphi^{-1}(e') = e.$
- $\forall m', n' \in M', \exists m, n \in M : \begin{cases} \varphi(m) = m' \\ \varphi(n) = n' \end{cases}$

$$\begin{aligned} \varphi(\varphi^{-1}(m')\varphi^{-1}(n')) &= \varphi(mn) \\ &= \varphi(m)\varphi(n) \\ &= m'n' \\ \implies \varphi^{-1}(m'n') &= \varphi^{-1}(m')\varphi^{-1}(n'). \end{aligned}$$

□

Proposición

Sea $\varphi : G \to H$ un morfismo de grupos. Entonces φ es un monomorfismo de grupos si y sólo si

$$\forall g \in G, [\varphi(g) = e_H \implies g = e_G].$$

Demostración.

$\implies$ Por inyectividad.

$\impliedby$ Si $\varphi(g) = \varphi(h)$ entonces

$$\begin{aligned} e_H &= \varphi(g)\varphi(h)^{-1} \\ &= \varphi(g)\varphi(h^{-1}) \\ &= \varphi(gh^{-1}). \end{aligned}$$

Luego $gh^{-1} = e_G$ y por ende $g = h$. $\square$

Subgrupos

Definición

Sea G un grupo. Un subconjunto $H \subset G$ se dice un subgrupo si:

- $H \neq \varnothing$;
- $\forall h_1, h_2 \in H, h_1 h_2^{-1} \in H$.

Proposición

Sean G un grupo y $H \subset G$ un subconjunto. Las siguientes afirmaciones son equivalentes:

1. *H es un subgrupo de G;*
2. *$H \neq \varnothing$ y $\forall h_1, h_2 \in H, \begin{cases} h_1^{-1} \in H \\ h_1 h_2 \in H \end{cases}$ (o sea H es cerrado por inversos y multiplicaciones);*
3. *H es un grupo y la inclusión $i : H \hookrightarrow G$, $i(h) = h$, es un morfismo de grupos.*

Demostración.

- $1 \iff 2$: Ejercicio.
- $2 \implies 3$: Las operaciones son cerradas en H, en particular $e = hh^{-1} \in H$ (puedo elegir $h \in H$ pues $H \neq \varnothing$). Luego H es un grupo con las operaciones heredades de G y se tiene que $i(h_1 h_2) = h_1 h_2 = i(h_1) i(h_2)$ es un morfismo de grupos.
- $3 \implies 2$: Supongamos que existe una operación binaria $\cdot_H$ en H tal que $(H, \cdot_H)$ es un grupo e $i : (H, \cdot_H) \hookrightarrow (G, \cdot)$ es un morfismo de grupos. En particular tenemos:
  - $\cdot_H$ tiene elemento neutro e_H, luego $H \neq \varnothing$;
  - $\forall h \in H$,

$$h^{-1_H} = i(h^{-1_H}) = i(h^{-1}) = h_1^{-1} \in H;$$

  - $\forall h_1, h_2 \in H$,

$$h_1 \cdot_H h_2 = i(h_1 \cdot_H h_2) = i(h_1) i(h_2) = h_1 h_2 \in H. \qquad \square$$

Ejemplo

Si G es un grupo, entonces $\{e\}$ (subgrupo trivial) y G son subgrupos de G. Un subgrupo H de G se dice **propio** si $\{e\} \subsetneqq H \subsetneqq G$.

Subgrupos de $S_3 \simeq D_3$

- Las rotaciones forman un subgrupo

$$\{(1,2,3),(2,3,1),(3,2,1)\}.$$

- Cada reflexión determina un subgrupo de dos elementos

$$\{(1,2,3),(1,3,2)\} \quad \{(1,2,3),(3,2,1)\} \quad \{(1,2,3),(2,1,3)\}.$$

- Si un subgrupo H contiene dos reflexiones distintas, entonces $H = S_3$. Por ejemplo,

$$\underbrace{(1,3,2)}_{\text{reflexión}}\underbrace{(3,2,1)}_{\text{reflexión}} = \underbrace{(2,3,1)}_{\text{rotación}}.$$

Subgrupos de $(\mathbb{R}, +)$

"Topológicamente" podemos distinguir dos grandes clases, que sin embargo pueden ser muy distintas desde un punto de vista "algebraico".

Subgrupos discretos

- $G_\rho = \rho\mathbb{Z} = \{\rho n : n \in \mathbb{Z}\}$.
- Sus elementos están igualmente espaciados.

$$\longleftarrow \boxed{-2\rho} \text{ —— } \boxed{-\rho} \text{ —— } \boxed{0} \text{ —— } \boxed{\rho} \text{ —— } \boxed{2\rho} \longrightarrow$$

- Son todos isomorfos si $\rho \neq 0$ (ejercicio).
- Están generados por un solo elemento.

Subgrupos densos

- Elementos arbitrariamente próximos a cualquier número real.
- Ejemplo 1: $\mathbb{Q}$.
  - Este grupo no se puede generar con una cantidad finita de elementos (ejercicio).
  - Por ejemplo: con $\frac{2}{3}$ y $\frac{5}{4}$ sólo puedo generar $G_{\frac{1}{12}}$:

$$m\frac{2}{3} + n\frac{5}{4} = \frac{8m + 15n}{12} \in \frac{1}{12}\mathbb{Z}$$

  - Para obtener $\frac{1}{12}$ podemos tomar $m = 2$, $n = -1$.
- Ejemplo 2: $\mathbb{Z}[\sqrt{2}] := \{m + \sqrt{2}n : m, n \in \mathbb{Z}\}$.
  - Está generado por 1 y $\sqrt{2}$.
  - Ejercicio*: es denso.

Subgrupos de $\mathbb{R}^2$

Pueden ser

- Discretos e.g. $\mathbb{Z} \times \mathbb{Z}$.
- Densos e.g. $\mathbb{Q} \times \mathbb{Q}$.
- Ninguno de los dos:

$$G_\alpha = \{(t, \alpha t) : t \in \mathbb{R}\} \qquad \text{(recta de pendiente } \alpha\text{)}.$$

Comentario

Se puede hace una construcción tipo "pacman" en el plano con estos subgrupos: restringiéndonos a un cuadrado de lado 1 e identificando lados opuestos. Las rectas G_α se "enroscan" sobre el cuadrado en segmentos de rectas paralelas (porque lo que sale por un lado, vuelve a entrar por el lado opuesto) y según α sea racional o irracional el subgrupo se cierra sobre si mismo, o es denso y nunca vuelve a cortarse. Formalizaremos más adelante.

Propiedades de los subgrupos

Proposición

Sea G un grupo y $\{H_i\}_{i\in I}$ una familia de subgrupos de G. Entonces $H = \bigcap_{i\in I} H_i$ es un subgrupo de G.

Demostración.

- $(\forall i \in I, e \in H_i) \implies e \in H \implies H \neq \varnothing$.
- si $g, h \in H$ entonces $g, h \in H_i$ para todo i, por lo tanto $gh^{-1} \in H_i$ para todo i. Es decir $gh^{-1} \in H$.
- Luego, H es un subgrupo de G. □

Definición

Sea G un grupo y X un subconjunto de G. El **subgrupo generado** por X es el menor subgrupo que contiene a H:

$$\langle X \rangle := \bigcap_{\substack{H \text{ subgrupo de } G \\ X \subset H}} H.$$

Ejemplos/Definiciones

- $\langle \varnothing \rangle = \{e\}$.
- **Grupos/subgrupos cíclicos:** G se dice cíclico si

$$G = \langle g \rangle := \langle \{e\} \rangle$$

para algún $g \in G$.

  - Los grupos cíclicos son abelianos.
  - $\mathbb{Z}$ es cíclico.
  - Si G es cíclico entonces $G = \{g^n : n \in \mathbb{Z}\}$ (pero no necesariamente G es infinito).

- $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$ es un grupo (cíclico) definiendo

$$x + y := \text{resto}(x + y, n).$$

- **Grupo finitamente generado:**
  $\exists g_1, \ldots, g_k \in G : G = \langle \{g_1, \ldots, g_k\} \rangle$.

Definición

Si H, K son dos subgrupos de G, se define

$$HK = \langle H \cup K \rangle.$$

Es decir, HK es el menor subgrupo de G que contiene a H y K.
Notación aditiva: $H + K$.

Ejemplo (retículo de subgrupos)

Si G es un grupo, definimos el **retículo de subgrupos** de G por

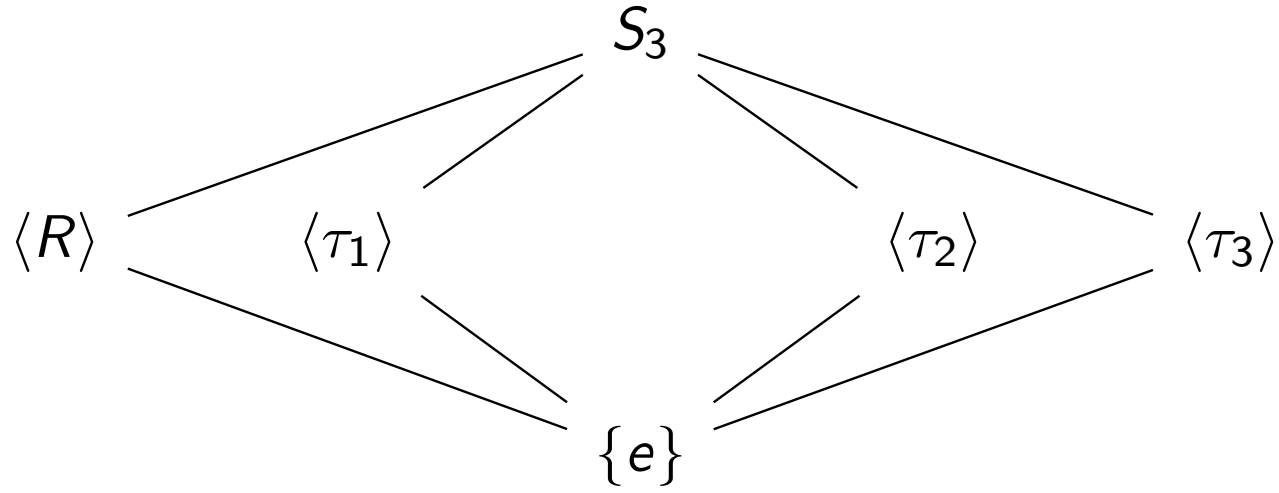
$$\mathcal{L}(G) := \{H \in \mathcal{P}(G) : H \text{ es subgrupo de } G\}.$$

$\mathcal{L}(G)$ es efectivamente un retículo con las operaciones

- $H \vee K = HK$,
- $H \wedge K = H \cap K$.

Ejemplos concretos/Ejercicios

- $\mathcal{L}(\mathbb{Z}_n) = (D_n, |)$
- $\mathcal{L}(S_3)$



- $\mathcal{L}(D_4) = ?$ (grupo de simetrías del cuadrado, 10 subgrupos)
- $\mathcal{L}(\mathbb{Z}) = ?$
- $\mathcal{L}(S_4) = ?$

Observación

$\mathcal{L}(G)$ no necesariamente es

- modular,
- distributivo,
- complementado.
- etc.

Teorema (Ore)

$\mathcal{L}(G)$ *es distributivo* $\iff$ G *es localmente cíclico.*

Localmente cíclico: todo subgrupo finitamente generado es cíclico.