Grupos. Parte 2.

Silvio Reggiani

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

20 de octubre de 2020

Kernel

La definición de núcleo de un morfismo de grupos es ligeramente distinta a la de núcleo de una función: no se define como una relación de equivalencia sino como un subgrupo. Más adelante veremos que se puede ir y volver entre estos dos conceptos.

Definición

El **núcleo** o **kernel** de un morfismo de grupos $\varphi : G \to H$ se define como

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

Observación

- $\ker \varphi$ es un subgrupo de G:
  - $\varphi(e_G) = e_H \implies e_G \in \ker \varphi$
  - $g_1, g_2 \in \ker \varphi \implies \varphi(g_1) = \varphi(g_2) = e_H \implies \varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_H \implies g_1 g_2^{-1} \in \ker \varphi$.
- Con la definición anterior $\ker \varphi$ es la relación de equivalencia $g_1 \sim g_2 \iff \varphi(g_1) = \varphi(g_2)$. Con la nueva definición, $\ker \varphi$ es la clase de equivalencia de e para $\sim$.

Coclases

Congruencia módulo n en $\mathbb{Z}$

$$x \equiv y \mod n \overset{\cdot}{\iff} n \mid (x - y)$$

- Es lo mismo que decir que x e y tienen el mismo resto cuando los dividimos por n.
- Es lo mismo que decir que $x - y \in n\mathbb{Z}$. O sea, podemos decir que son congruentes módulo el subgrupo $n\mathbb{Z}$.
- Es una relación de equivalencia en $\mathbb{Z}$.
- El conjunto de clases de equivalencia $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$. forma un grupo tal que la proyección $\pi : \mathbb{Z} \to \mathbb{Z}_n$ es un epimorfismo de grupos.
- $\ker \pi = n\mathbb{Z}$.

Es interesante estudiar la congruencia en cualquier grupo, aunque hay algunas dificultades que aparecen cuando tratamos de adaptar estas ideas.

Congruencia a izquierda vs. congruencia a derecha

Dados G un grupo y H un subgrupo de G, tenemos dos posibles formas de definir la congruencia módulo H.

- **A izquierda:**

$$g_1 \equiv_\ell g_2 \mod H \iff g_1 g_2^{-1} \in H.$$

- **A derecha:**

$$g_1 \equiv_r g_2 \mod H \iff g_1^{-1} g_2 \in H.$$

Proposición

1. *$- \equiv_\ell -$ $\text{mód } H$ y $- \equiv_r -$ $\text{mód } H$ son relaciones de equivalencia en G.*
2. *La clase de equivalencia de g para la congruencia a izquierda es*
$$\bar{g}^\ell = Hg = \{hg : h \in H\}.$$
3. *La clase de equivalencia de g para la congruencia a derecha es*
$$\bar{g}^r = gH = \{gh : h \in H\}.$$

Observación

- Las clases de equivalencia de las congruencias a izquierda y derecha se llaman **coclases** a izquierda y derecha, respectivamente.
- En general $Hg \neq gH$ (veremos ejemplos más adelante).

Demostración de la Proposición.

Prueba de 1

- Haremos la prueba para la congruencia a izquierda. La otra queda como ejercicio (¿se puede usar dualidad?).
- Reflexividad: $g \equiv_\ell g \mod H \iff gg^{-1} = e \in H$ ✓
- Simetría:

$$\begin{aligned} g_1 \equiv_\ell g_2 \mod H &\iff g_1 g_2^{-1} \in H \\ &\iff (g_1 g_2^{-1})^{-1} = g_2 g_1^{-1} \in H \\ &\iff g_2 \equiv_\ell g_1 \mod H \quad \checkmark \end{aligned}$$

- Transitividad: $g_1 \equiv_\ell g_2 \mod H$ y $g_2 \equiv_\ell g_3 \mod H$ implica

$$g_1 g_3^{-1} = \underbrace{g_1 g_2^{-1}}_{\in H} \underbrace{g_2 g_3^{-1}}_{\in H} \in H \iff g_1 \equiv_\ell g_3 \mod H \quad \checkmark$$

- Usamos fuertemente que H es un subgrupo.

Demostración de la Proposición (cont.)

Prueba de 2

- $k \in Hg \implies k = hg$ para algún $h \in H$. Luego

  $$gk^{-1} = g(hg)^{-1} = gg^{-1}h^{-1} = h^{-1} \in H$$

  y por tanto $Hg \subset \bar{g}^{\ell}$.
- Recíprocamente, $k \equiv_{\ell} g \mod H \implies kg^{-1} = h$ para algún $h \in H$. Luego $k = hg \in Hg$ y por lo tanto $\bar{g}^{\ell} \subset Hg$.
- Así, $\bar{g}^{\ell} = Hg$.

Prueba de 3: ejercicio. $\square$

Notación para los cocientes

- $H\backslash G = \{Hg : g \in G\}$ (coclases a izquierda).
- $G/H = \{gH : g \in G\}$ (coclases a derecha).

Proposición

1. *Todas las coclases (a izquierda o derecha) tienen la misma cantidad de elementos. Es decir, tienen la cardinalidad de H.*
2. *Existe una biyección entre $H\backslash G$ y G/H.*

Observación

H es la coclase de e, tanto a izquierda como a derecha.

Demostración.

Prueba de 1. La hacemos sólo para coclases a izquierda.

- Dado $g \in G$ definimos la función $R_g : H \to Hg$, $R_g(h) = hg$.
- R_g es sobre (¿por qué?).
- R_g es inyectiva:

$$R_g(h_1) = R_g(h_2) \implies h_1 g = h_2 g \implies h_1 = h_2.$$

- Luego $|Hg| = |H| = |He|$.

Demostración (cont.)

Prueba de 2: hay que definir una biyección $\varphi : H\backslash G \to G/H$.

- Lo que NO funciona: $\varphi(Hg) = gH$ ¿por qué?
- Lo que SÍ funciona: $\varphi(Hg) = g^{-1}H$.
  - Buena definición: $Hg_1 = Hg_2 \overset{?}{\Longrightarrow} g_1^{-1}H = g_2^{-1}H$.

$$\begin{aligned} Hg_1 = Hg_2 &\iff g_1g_2^{-1} \in H \\ &\iff (g_1^{-1})^{-1}g_2^{-1} \in H \\ &\iff g_1^{-1}H = g_2^{-1}H. \end{aligned}$$

  - φ es sobre, pues todo elemento de G es de la forma g^{-1} .
  - φ es inyectiva:

$$\begin{aligned} \varphi(Hg_1) = \varphi(Hg_2) &\implies g_1^{-1}H = g_2^{-1}H \\ &\implies (g_1^{-1})^{-1}g_2^{-1} = g_1g_2^{-1} \in H \\ &\implies Hg_1 = Hg_2. \end{aligned}$$

$\square$

Índice

Definición

El **índice** de un subgrupo H de G es

$$[G : H] = |H \backslash G| = |G/H|.$$

El índice es un invariante algebraico que no depende de la elección de la congruencia.

Teorema (Lagrange)

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

Observación

Cuando los cardinales de G y H son finitos, el teorema de Lagrange se puede expresar diciendo que el cardinal del cociente es el cociente de los cardinales: $|G/H| = [G : H] = |G|/|H|$.

Demostración.

G es unión disjunta de $[G : H]$ coclases (clases de equivalencia) y cada una de estás coclases tiene la cardinalidad de H. $\square$

El teorema de Lagrange es un resultado muy simple, pero tiene aplicaciones importantes.

Definición

- El **orden de un subgrupo** H de G es $|H|$.
- El **orden de un elemento** $g \in G$ es $|g| := |\langle g \rangle|$.

Corolario (Importante)

Si G es un grupo finito y H es un subgrupo de G, entonces $|H| \mid |G|$ (el orden de H divide al orden de $|G|$). En particular, el orden de un elemento de G divide a $|G|$.

Ejemplo

Sea $(G, +)$ un grupo abeliano y H un subgrupo de G,

- La congruencia a izquierda módulo H coincide con la congruencia a derecha módulo H:

$$x - y \in H \iff y - x = -(x - y) \in H.$$

- Coclases a izquierda coinciden con coclases a derecha:

$$\forall x \in G, H + x = x + H :$$

- **Ejercicio:** $H \backslash G = G/H$ es un grupo definiendo

$$(x + H) + (y + H) = (x + y) + H.$$

- La proyección al cociente $\pi : G \to G/H$, $\pi(x) = x + H$ es un (epi)morfismo de grupos.

Coclases en S_3

- $G = S_3$, $H = \{(1,2,3),(2,3,1),(3,1,2)\}$ (rotaciones).
- $He = eH = H$.
- $H(1,3,2) = \{(1,3,2),(3,2,1),(2,1,3)\} = (1,3,2)H$. O sea, la coclase a izquierda de $(1,3,2)$ coincide con la coclase a derecha y consiste de todas las reflexiones. A esto lo sabemos pues las coclases son disjuntas (y en este caso tienen 3 elementos).
- $S_3 \backslash H = H/S_3$ tiene estructura de grupo definiendo

  $$(H(1,3,2))(H(1,3,2)) = H(1,3,2)^2 = H(1,2,3) = H$$

  y se cumple que la proyección al cociente es un morfismo de grupos (pensar porqué esto está bien definido).
- $S_3/H \simeq \mathbb{Z}_2$.

Coclases en S_3

- $G = S_3$, $H = \{(1,2,3),(1,3,2)\}$ (subgrupo generado por la reflexión $(1,3,2)$).
- Coclases a izquierda:
  - $He = H = \{(1,2,3),(1,3,2)\}$
  - $H(2,3,1) = \{(2,3,1),(3,2,1)\}$
  - $H(3,1,2) = \{(3,1,2),(2,1,3)\}$
- Coclases a derecha:
  - $eH = H = \{(1,2,3),(1,3,2)\} = He$
  - $(2,3,1)H = \{(2,3,1),(2,1,3)\} \neq H(2,3,1)$
  - $(3,1,2)H = \{(3,1,2),(3,2,1)\} \neq H(3,1,2)$
- **Ejercicio:** no se puede definir un producto en el cociente tal que la proyección sea un morfismo de grupos.

Ejemplo

En S_3 la composición de dos reflexiones es una rotación.

- A esto ya lo vimos haciendo las cuentas explícitamente. Ahora veremos otra forma usando el teorema de Lagrange (y sin hacer cuentas).
- Llamemos τ_1, τ_2, τ_3 a las tres reflexiones en S_3 y supongamos por el absurdo que $\tau_1\tau_2 = \tau_3$ no es una rotación.
- Luego $H = \langle \tau_1, \tau_2 \rangle = \{e, \tau_1, \tau_2, \tau_3\}$ es un subgrupo de S_3 de orden 4.
- Lagrange $\implies |H| = 4$ divide a $|S_3| = 6$. Absurdo.

Ejemplo

¿Cuál es el máximo orden posible para un elemento en S_4?

- Por el teorema de Lagrange el orden de un elemento de S_4 divide a $|S_4| = 24$. O sea, los posibles órdenes son $\{1, 2, 3, 4, 6, 8, 12, 24\}$.
- 24 no puede ser pues S_4 no es cíclico (¿por qué?).
- Hay elementos de orden 2, por ejemplo
  - $(2, 1, 3, 4)$: una trasposición;
  - $(2, 1, 4, 3) = (2, 1, 3, 4)(1, 2, 4, 3)$: la composición de dos transposiciones que intercambian subconjuntos disjuntos de elementos.
- Hay elementos de orden 3, por ejemplo $(1, 3, 4, 2)$: una permutación con un punto fijo que rota los otros tres elementos (se puede pensar como un elemento de S_3).
- Hay elementos de orden 4, por ejemplo (2, 3, 4, 1): una rotación.

Ejemplo (cont.)

- No hay elementos de orden 6. Supongamos que existe $\sigma \in S_3$ tal que $\sigma^6 = e$ pero $\sigma^k \neq e$ para $1 \leq k < 6$.
  - Si σ tiene un punto fijo, entonces puede pensarse como un elemento de S_3. Luego $S_3 = \langle \sigma \rangle \simeq \mathbb{Z}_6$ (abeliano). Absurdo.

  Por ende σ mueve todos los elementos.
  - Si σ rota todos los elementos, entonces tiene orden 4. Absurdo.
  - Si σ no rota todos los elementos, entonces los intercambia de a pares, es decir, es la composición de dos trasposiciones disjuntas

    $$\sigma = \tau_{ij}\tau_{i'j'}$$

    y por lo tanto tiene orden 2. Absurdo.
- No hay elementos de orden 12: si σ tuviera orden 12, entonces σ^2 tendría orden 6. Absurdo.
- No hay elementos de orden 8 (ejercicio).
- Luego, el máximo orden posible para un elemento de S_4 es 4.

Ejercicio

¿Cuál es el máximo orden posible para un elemento de S_5?

- Tiene que ser un divisor de $5! = 120$.
- Hay elementos de orden 5: $(2,3,4,5,1)$, una rotación.
- Pero también hay elementos de orden 6, por ejemplo

$$\sigma = (2,1,4,5,3) = \underbrace{(2,1,3,4,5)}_{\text{orden 2}}\underbrace{(1,2,4,5,3)}_{\text{orden 3}}$$

  que es la composición de un elemento de orden 2 con uno de orden 3 que conmutan.
- ¿Es 6 el máximo orden posible para un elemento en S_5?

Subgrupos normales, grupo cociente

Pregunta

¿Cuándo G/H admite una estructura de grupo tal que la proyección al cociente $\pi : G \to G/H$ sea un morfismo de grupos? En otras palabras, si G es un grupo y H es un subgrupo, ¿cuándo se tiene que

$$(g_1 H)(g_2 H) = (g_1 g_2)H$$

define una estructura de grupo en G/H?

- **Buena definición:** $\left.\begin{array}{l} g_1 H = \tilde{g}_1 H \\ g_2 H = \tilde{g}_2 H \end{array}\right\} \overset{?}{\Longrightarrow} (g_1 g_2)H = (\tilde{g}_1 \tilde{g}_2)H$
- $g_1 H = \tilde{g}_1 H \iff g_1^{-1}\tilde{g}_1 \in H$, $g_2 H = \tilde{g}_2 H \iff g_2^{-1}\tilde{g}_2 \in H$
- $(g_1 g_2)H = (\tilde{g}_1 \tilde{g}_2)H \iff (g_1 g_2)^{-1}\tilde{g}_1 \tilde{g}_2 \in H$
- $(g_1 g_2)^{-1}\tilde{g}_1 \tilde{g}_2 = g_2^{-1} g_1^{-1}\tilde{g}_1 \tilde{g}_2 = \underbrace{g_2^{-1}\underbrace{g_1^{-1}\tilde{g}_1}_{\in H} g_2}_{\in H?} \underbrace{g_2^{-1}\tilde{g}_2}_{\in H}$

Definición

Un subgrupo H de un grupo G se dice **normal** si

$$\forall g \in G, gHg^{-1} \subset H.$$

Notación

- **Subgrupo:** $H < G$
- **Subgrupo normal:** $H \triangleleft G$
- **Conjugado** de H por $g \in G$: gHg^{-1}. **Ejercicio:** gHg^{-1} es un subgrupo de G.

Proposición (ejercicio)

Sea $H < G$. Son equivalentes:

- $H \triangleleft G$;
- $\forall g \in G, gHg^{-1} = H$;
- $\forall g \in G, gH = Hg$. *Es decir* $H \backslash G = G/H$.

En otras palabras: *H es un subgrupo normal de G si y sólo si la congruencia izquierda módulo H coincide con la congruencia a derecha módulo H.* Más aún,

Proposición

Si $H \triangleleft G$, entonces

$$(g_1H)(g_2H) = (g_1g_2)H$$

define una estructura de grupo en G/H tal que la proyección al cociente $\pi : G \to G/H$ es un epimorfismo de grupos.

Demostración.

No hay que hacer mucho. La buena definición la vimos antes de definir subgrupo normal. Chequear que G/H es efectivamente un grupo con este producto. $\square$

Ejemplos

- Todo subgrupo H de un grupo abeliano G es normal:

$$H + x = x + H.$$

- $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ (¿por qué?).
- $\mathbb{R}/\mathbb{Z} \simeq$ círculo $= S^1 := \{z \in \mathbb{C} : |z| = 1\}$ (intuitivamente debería ser claro, pero cuando veamos los teoremas de isomorfismos lo justificaremos un poco mejor).
- $\mathbb{Q}/\mathbb{Z}$ es un ejemplo medio raro: es infinito pero todo elemento tiene orden finito.