Álgebra II Práctica (clase 3)

Guido Arnone

Universidad de Buenos Aires

21 de Abril de 2020

Prerrequisitos

Para leer estas diapositivas se recomienda haber leído el apunte teórico hasta el Teorema 1.6.10 de la Sección 1.6.

Coclases

Recordar: dado un subgrupo H de un grupo G, las coclases a izquierda de G con respecto a H son los conjuntos $gH = \{gh : h \in H\}$ para cada $g \in G$, y el cociente de G por H es el conjunto de coclases $G/H = \{gH\}_{g \in G}$.

Coclases

Recordar: dado un subgrupo H de un grupo G, las coclases a izquierda de G con respecto a H son los conjuntos $gH = \{gh : h \in H\}$ para cada $g \in G$, y el cociente de G por H es el conjunto de coclases $G/H = \{gH\}_{g \in G}$.

Las coclases forman una partición de G, y en particular se tiene la relación de equivalencia

$$\begin{aligned} s \sim t \iff sH = tH \iff s^{-1}tH = H \\ \iff s^{-1}t \in H \iff t = sh \text{ para algún } h \in H. \end{aligned}$$

Coclases

Recordar: dado un subgrupo H de un grupo G, las coclases a izquierda de G con respecto a H son los conjuntos $gH = \{gh : h \in H\}$ para cada $g \in G$, y el cociente de G por H es el conjunto de coclases $G/H = \{gH\}_{g \in G}$.

Las coclases forman una partición de G, y en particular se tiene la relación de equivalencia

$$\begin{aligned} s \sim t \iff sH = tH \iff s^{-1}tH = H \\ \iff s^{-1}t \in H \iff t = sh \text{ para algún } h \in H. \end{aligned}$$

A veces notaremos $[s]$ o $\overline{s}$ a la coclase sH, pues es la clase de equivalencia de $s \in G$ con respecto a esta relación.

Coclases

Recordar: dado un subgrupo H de un grupo G, las coclases a izquierda de G con respecto a H son los conjuntos $gH = \{gh : h \in H\}$ para cada $g \in G$, y el cociente de G por H es el conjunto de coclases $G/H = \{gH\}_{g \in G}$.

Las coclases forman una partición de G, y en particular se tiene la relación de equivalencia

$$\begin{aligned} s \sim t \iff sH = tH \iff s^{-1}tH = H \\ \iff s^{-1}t \in H \iff t = sh \text{ para algún } h \in H. \end{aligned}$$

A veces notaremos $[s]$ o $\overline{s}$ a la coclase sH, pues es la clase de equivalencia de $s \in G$ con respecto a esta relación.
Lo anterior nos dice que $[s] = [t]$ si y sólo si $t = sh$ para algún $h \in H$.
Intuitivamente, dos elementos son equivalentes (es decir, están la misma coclase) si "difieren en un elemento de H".

Coclases - Ejemplos

Veamos algunos ejemplos:

Coclases - Ejemplos

Veamos algunos ejemplos:

- Si tomamos $H = \{1\}$, entonces $gH = \{g\}$ para cada $g \in G$ y $G/H = \{\{g\}\}_{g \in G}$.
  Si en cambio $H = G$, es $gH = gG = G$ para todo g en G, así que $G/H = \{G\}$.

Coclases - Ejemplos

Veamos algunos ejemplos:

- Si tomamos $H = \{1\}$, entonces $gH = \{g\}$ para cada $g \in G$ y $G/H = \{\{g\}\}_{g \in G}$.
  Si en cambio $H = G$, es $gH = gG = G$ para todo g en G, así que $G/H = \{G\}$.

- Dado $n \in \mathbb{N}$ y $n\mathbb{Z} \leq \mathbb{Z}$, sabemos que

  $$s(n\mathbb{Z}) = t(n\mathbb{Z}) \iff t - s \in n\mathbb{Z} \iff n | t - s \iff t \equiv s \pmod{n}$$

  así que hay una coclase por cada resto en la división por n,

  $$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

Coclases - Ejemplos (cont.)

- Fijemos V un $\mathbb{k}$-espacio vectorial, que podemos considerar como grupo con su suma, y sea $S \leq V$ un subespacio (en particular, un subgrupo de V). Cada coclase $v + S = \{v + s : s \in S\}$ se corresponde con trasladar a S por v.

Coclases - Ejemplos (cont.)

- Fijemos V un $\mathbb{k}$-espacio vectorial, que podemos considerar como grupo con su suma, y sea $S \leq V$ un subespacio (en particular, un subgrupo de V). Cada coclase $v + S = \{v + s : s \in S\}$ se corresponde con trasladar a S por v. Las observaciones que hicimos sobre las coclases nos dicen que V es la unión disjunta de trasladados de S, y que $v + S = w + S$ si y sólo si $v - w \in S$.

Coclases - Ejemplos (cont.)

- Fijemos V un $\mathbb{k}$-espacio vectorial, que podemos considerar como grupo con su suma, y sea $S \leq V$ un subespacio (en particular, un subgrupo de V). Cada coclase $v + S = \{v + s : s \in S\}$ se corresponde con trasladar a S por v. Las observaciones que hicimos sobre las coclases nos dicen que V es la unión disjunta de trasladados de S, y que $v + S = w + S$ si y sólo si $v - w \in S$.

- Más concretamente, tomemos $V = \mathbb{R}^2$ y $S = \langle (1,0) \rangle = \mathbb{R} \oplus 0$ el "eje x".

Coclases - Ejemplos (cont.)

- Fijemos V un $\mathbb{k}$-espacio vectorial, que podemos considerar como grupo con su suma, y sea $S \leq V$ un subespacio (en particular, un subgrupo de V). Cada coclase $v + S = \{v + s : s \in S\}$ se corresponde con trasladar a S por v. Las observaciones que hicimos sobre las coclases nos dicen que V es la unión disjunta de trasladados de S, y que $v + S = w + S$ si y sólo si $v - w \in S$.
- Más concretamente, tomemos $V = \mathbb{R}^2$ y $S = \langle(1,0)\rangle = \mathbb{R} \oplus 0$ el "eje x". Cada trasladado $L_y := (x, y) + S = \{(x + \lambda, y) : \lambda \in \mathbb{R}\}$ es una recta horizontal de altura y.

Coclases - Ejemplos (cont.)

- Fijemos V un $\mathbb{k}$-espacio vectorial, que podemos considerar como grupo con su suma, y sea $S \leq V$ un subespacio (en particular, un subgrupo de V). Cada coclase $v + S = \{v + s : s \in S\}$ se corresponde con trasladar a S por v. Las observaciones que hicimos sobre las coclases nos dicen que V es la unión disjunta de trasladados de S, y que $v + S = w + S$ si y sólo si $v - w \in S$.

- Más concretamente, tomemos $V = \mathbb{R}^2$ y $S = \langle (1, 0) \rangle = \mathbb{R} \oplus 0$ el "eje x". Cada trasladado $L_y := (x, y) + S = \{(x + \lambda, y) : \lambda \in \mathbb{R}\}$ es una recta horizontal de altura y. Por lo tanto, las coclases son las rectas paralelas a S, estas forman una unión disjunta de $\mathbb{R}^2$, y $(x, y) + S = (x, y') + S$ si y sólo si $y = y'$.

Coclases - Ejemplos (cont.)

- Fijemos V un $\mathbb{k}$-espacio vectorial, que podemos considerar como grupo con su suma, y sea $S \leq V$ un subespacio (en particular, un subgrupo de V). Cada coclase $v + S = \{v + s : s \in S\}$ se corresponde con trasladar a S por v. Las observaciones que hicimos sobre las coclases nos dicen que V es la unión disjunta de trasladados de S, y que $v + S = w + S$ si y sólo si $v - w \in S$.

- Más concretamente, tomemos $V = \mathbb{R}^2$ y $S = \langle(1,0)\rangle = \mathbb{R} \oplus 0$ el "eje x". Cada trasladado $L_y := (x,y) + S = \{(x+\lambda, y) : \lambda \in \mathbb{R}\}$ es una recta horizontal de altura y. Por lo tanto, las coclases son las rectas paralelas a S, estas forman una unión disjunta de $\mathbb{R}^2$, y $(x,y) + S = (x,y') + S$ si y sólo si $y = y'$. En particular un sistema de representantes para la relación dada por las coclases es $\{(0,y)\}_{y \in \mathbb{R}}$, y

$$\mathbb{R}^2/\mathbb{R} \oplus 0 = \{(0,y) + \langle(1,0)\rangle : y \in \mathbb{R}\}.$$

Coclases - Ejemplos (cont.)

- Consideremos ahora $A_n \leq S_n$, para $n \geq 2$. Tenemos que

  $$\sigma A_n = \tau A_n \iff \sigma^{-1}\tau \in A_n \iff \mathrm{sg}(\sigma)^{-1}\mathrm{sg}(\tau) = \mathrm{sg}(\sigma^{-1}\tau) = 1,$$

  así que dos permutaciones pertenecen a la misma coclase si y sólo si tienen el mismo signo.
  Hay entonces dos coclases, correspondientes a las permutaciones de signo 1 y -1 respectivamente, y

  $$S_n/A_n = \{1 \cdot A_n, \sigma \cdot A_n\}$$

  con $\sigma \in S_n$ de signo -1 (por ejemplo, podemos tomar $\sigma = (12)$).

Coclases - Ejemplos (cont.)

- Consideremos ahora $A_n \leq S_n$, para $n \geq 2$. Tenemos que
$$\sigma A_n = \tau A_n \iff \sigma^{-1}\tau \in A_n \iff \mathrm{sg}(\sigma)^{-1}\mathrm{sg}(\tau) = \mathrm{sg}(\sigma^{-1}\tau) = 1,$$
así que dos permutaciones pertenecen a la misma coclase si y sólo si tienen el mismo signo.
Hay entonces dos coclases, correspondientes a las permutaciones de signo 1 y -1 respectivamente, y
$$S_n/A_n = \{1 \cdot A_n, \sigma \cdot A_n\}$$
con $\sigma \in S_n$ de signo -1 (por ejemplo, podemos tomar $\sigma = (12)$).
- Más en general, dado un morfismo de grupos $f : G \to G'$, sabemos que $H = \ker f$ es un subgrupo de G. Aquí es
$$yH = xH \iff y^{-1}x \in \ker f \iff f(y)^{-1}f(x) = f(y^{-1}x) = 1_{G'},$$
así que $xH = yH \iff f(x) = f(y)$. Aplicando esto a $\mathrm{sg} : S_n \to G_2$ obtenemos el ejemplo anterior.

El teorema de Lagrange

Recordemos que dado un subgrupo H de un grupo G, su índice es

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

El teorema de Lagrange

Recordemos que dado un subgrupo H de un grupo G, su índice es

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

El teorema de Lagrange relaciona el índice de H en G con los órdenes de tanto H como G,

El teorema de Lagrange

Recordemos que dado un subgrupo H de un grupo G, su índice es

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

El teorema de Lagrange relaciona el índice de H en G con los órdenes de tanto H como G,

Teorema (Lagrange)

Si G es un grupo y H un subgrupo de G, entonces $|G| = [G : H]|H|$.

El teorema de Lagrange

Recordemos que dado un subgrupo H de un grupo G, su índice es

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

El teorema de Lagrange relaciona el índice de H en G con los órdenes de tanto H como G,

Teorema (Lagrange)

Si G es un grupo y H un subgrupo de G, entonces $|G| = [G : H]|H|$.

En particular, de los ejemplos anteriores y el teorema resulta que $|S_n| = 2|A_n|$, como habíamos visto la clase pasada. En general,

El teorema de Lagrange

Recordemos que dado un subgrupo H de un grupo G, su índice es

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

El teorema de Lagrange relaciona el índice de H en G con los órdenes de tanto H como G,

Teorema (Lagrange)

Si G es un grupo y H un subgrupo de G, entonces $|G| = [G : H]|H|$.

En particular, de los ejemplos anteriores y el teorema resulta que $|S_n| = 2|A_n|$, como habíamos visto la clase pasada. En general,

Corolario

Si G es un grupo finito y H un subgrupo de G, el orden de H divide al orden de G. En particular, si $x \in G$ entonces $\operatorname{ord}(x) = |\langle x \rangle|$ divide al orden de G.

El teorema de Lagrange - Aplicaciones

Ejercicio

Exhibir un grupo G *y* $n \in \mathbb{N}$ *que divida a* $|G|$ *pero tal que no existan elementos de orden* n *en* G.

El teorema de Lagrange - Aplicaciones

Ejercicio

Exhibir un grupo G *y* $n \in \mathbb{N}$ *que divida a* $|G|$ *pero tal que no existan elementos de orden* n *en* G.

Antes de seguir, veamos una aplicación del teorema de Lagrange:

Proposición

Si $n, m \in \mathbb{N}$, *entonces* $n! \cdot m!$ *divide a* $(n + m)!$.

Ejercicio

Exhibir un grupo G y $n \in \mathbb{N}$ que divida a $|G|$ pero tal que no existan elementos de orden n en G.

Antes de seguir, veamos una aplicación del teorema de Lagrange:

Proposición

Si $n, m \in \mathbb{N}$, entonces $n! \cdot m!$ divide a $(n+m)!$.

Idea de la demostración:

El teorema de Lagrange - Aplicaciones

Ejercicio

Exhibir un grupo G y $n \in \mathbb{N}$ que divida a $|G|$ pero tal que no existan elementos de orden n en G.

Antes de seguir, veamos una aplicación del teorema de Lagrange:

Proposición

Si $n, m \in \mathbb{N}$, entonces $n! \cdot m!$ divide a $(n+m)!$.

Idea de la demostración:

- Si $\sigma \in S = S_n$ y $\tau \in T = S(\{n+1, \ldots, n+m\})$, podemos definir una permutación $i(\sigma, \tau) \in S_{n+m}$ por $i(\sigma, \tau)(t) = \sigma(t)$ si $t \leq n$ e $i(\sigma, \tau)(t) = \tau(t)$ si $t > n$, que "permuta $\{1, \ldots, n\}$ como σ y $\{n+1, \ldots, n+m\}$ como τ".

El teorema de Lagrange - Aplicaciones

Ejercicio

Exhibir un grupo G y $n \in \mathbb{N}$ que divida a $|G|$ pero tal que no existan elementos de orden n en G.

Antes de seguir, veamos una aplicación del teorema de Lagrange:

Proposición

Si $n, m \in \mathbb{N}$, entonces $n! \cdot m!$ divide a $(n+m)!$.

Idea de la demostración:

- Si $\sigma \in S = S_n$ y $\tau \in T = S(\{n+1, \ldots, n+m\})$, podemos definir una permutación $i(\sigma,\tau) \in S_{n+m}$ por $i(\sigma,\tau)(t) = \sigma(t)$ si $t \leq n$ e $i(\sigma,\tau)(t) = \tau(t)$ si $t > n$, que "permuta $\{1, \ldots, n\}$ como σ y $\{n+1, \ldots, n+m\}$ como τ". Esto define un morfismo de grupos inyectivo $(\sigma,\tau) \in S \times T \mapsto i(\sigma,\tau) \in S_{n+m}$.

El teorema de Lagrange - Aplicaciones

Ejercicio

Exhibir un grupo G y $n \in \mathbb{N}$ que divida a $|G|$ pero tal que no existan elementos de orden n en G.

Antes de seguir, veamos una aplicación del teorema de Lagrange:

Proposición

Si $n, m \in \mathbb{N}$, entonces $n! \cdot m!$ divide a $(n+m)!$.

Idea de la demostración:

- Si $\sigma \in S = S_n$ y $\tau \in T = S(\{n+1, \ldots, n+m\})$, podemos definir una permutación $i(\sigma,\tau) \in S_{n+m}$ por $i(\sigma,\tau)(t) = \sigma(t)$ si $t \leq n$ e $i(\sigma,\tau)(t) = \tau(t)$ si $t > n$, que "permuta $\{1, \ldots, n\}$ como σ y $\{n+1, \ldots, n+m\}$ como τ". Esto define un morfismo de grupos inyectivo $(\sigma,\tau) \in S \times T \mapsto i(\sigma,\tau) \in S_{n+m}$.
- Por Lagrange $n! \cdot m! = |S \times T| = |\mathrm{im} f|$ divide a $|S_{n+m}| = (n+m)!$.

El teorema de Lagrange - Aplicaciones (cont.)

Quedan como ejercicio también las siguientes aplicaciones del teorema:

El teorema de Lagrange - Aplicaciones (cont.)

Quedan como ejercicio también las siguientes aplicaciones del teorema:

Ejercicio

Probar que si G *es un grupo de orden* p^s *con* p *primo y* $s \geq 1$, *todo subgrupo de* G *tiene orden* p^r *con* $0 \leq r \leq s$.

El teorema de Lagrange - Aplicaciones (cont.)

Quedan como ejercicio también las siguientes aplicaciones del teorema:

Ejercicio

Probar que si G es un grupo de orden p^s con p primo y $s \geq 1$, todo subgrupo de G tiene orden p^r con $0 \leq r \leq s$.

Esto puede ser útil para probar una propiedad sobre los grupos de orden p^k inductivamente.

El teorema de Lagrange - Aplicaciones (cont.)

Quedan como ejercicio también las siguientes aplicaciones del teorema:

Ejercicio

Probar que si G es un grupo de orden p^s con p primo y $s \geq 1$, todo subgrupo de G tiene orden p^r con $0 \leq r \leq s$.

Esto puede ser útil para probar una propiedad sobre los grupos de orden p^k inductivamente.

Ejercicio

Sea G un grupo finito y $H, K \leq G$ dos subgrupos. Probar que:

(i) *Si los órdenes de H y K son coprimos, entonces $H \cap K = \{1\}$.*

(ii) *Si H y K tienen orden p con p un primo, entonces $H = K$ ó $H \cap K = \{1\}$.*

Subgrupos Normales

Recordar: un subgrupo H de un grupo G se dice normal si para cada $g \in G$ se tiene que $gHg^{-1} \subset H$. En tal caso notamos $H \triangleleft G$.

Subgrupos Normales

Recordar: un subgrupo H de un grupo G se dice normal si para cada $g \in G$ se tiene que $gHg^{-1} \subset H$. En tal caso notamos $H \triangleleft G$.

¿Por qué nos interesan los subgrupos normales?

Subgrupos Normales

Recordar: un subgrupo H de un grupo G se dice normal si para cada $g \in G$ se tiene que $gHg^{-1} \subset H$. En tal caso notamos $H \triangleleft G$.

¿Por qué nos interesan los subgrupos normales?

- Si $f : G \to G'$ es un morfismo de grupos, sabemos que $\ker f$ es normal en G.

Subgrupos Normales

Recordar: un subgrupo H de un grupo G se dice normal si para cada $g \in G$ se tiene que $gHg^{-1} \subset H$. En tal caso notamos $H \triangleleft G$.

¿Por qué nos interesan los subgrupos normales?

- Si $f : G \to G'$ es un morfismo de grupos, sabemos que $\ker f$ es normal en G.
- Si H es normal en G, podemos dotar al cociente G/H de una estructura de grupo a través de la operación $gH \cdot g'H := gg'H$.

Subgrupos Normales

Recordar: un subgrupo H de un grupo G se dice normal si para cada $g \in G$ se tiene que $gHg^{-1} \subset H$. En tal caso notamos $H \triangleleft G$.

¿Por qué nos interesan los subgrupos normales?

- Si $f : G \to G'$ es un morfismo de grupos, sabemos que $\ker f$ es normal en G.
- Si H es normal en G, podemos dotar al cociente G/H de una estructura de grupo a través de la operación $gH \cdot g'H := gg'H$. Más aún, la proyección canónica $\pi : g \in G \mapsto [g] = gH \in G/H$ resulta un morfismo de grupos cuyo núcleo es

$$\ker \pi = \{g \in G : gH = 1H = H\} = \{g \in G : g \in H\} = H.$$

Subgrupos Normales

Recordar: un subgrupo H de un grupo G se dice normal si para cada $g \in G$ se tiene que $gHg^{-1} \subset H$. En tal caso notamos $H \triangleleft G$.

¿Por qué nos interesan los subgrupos normales?

- Si $f : G \to G'$ es un morfismo de grupos, sabemos que $\ker f$ es normal en G.
- Si H es normal en G, podemos dotar al cociente G/H de una estructura de grupo a través de la operación $gH \cdot g'H := gg'H$. Más aún, la proyección canónica $\pi : g \in G \mapsto [g] = gH \in G/H$ resulta un morfismo de grupos cuyo núcleo es

$$\ker \pi = \{g \in G : gH = 1H = H\} = \{g \in G : g \in H\} = H.$$

- En definitiva, lo anterior nos dice que un subgrupo es normal si y sólo si es el núcleo de algún morfismo de grupos.

Subgrupos Normales - Ejemplos

Algunos ejemplos son los siguientes:

Subgrupos Normales - Ejemplos

Algunos ejemplos son los siguientes:

- Los subgrupos $\{1\}$ y G siempre son normales en G.

Subgrupos Normales - Ejemplos

Algunos ejemplos son los siguientes:

- Los subgrupos $\{1\}$ y G siempre son normales en G.
- El grupo alternante A_n es normal en S_n, ya que es el núcleo del morfismo $\mathrm{sg} : S_n \to G_2$.

Subgrupos Normales - Ejemplos

Algunos ejemplos son los siguientes:

- Los subgrupos $\{1\}$ y G siempre son normales en G.
- El grupo alternante A_n es normal en S_n, ya que es el núcleo del morfismo $\mathrm{sg} : S_n \to G_2$.
- En S_3, el subgrupo $H = \langle (12) \rangle = \{1, (12)\}$ no es normal, pues

$$(123)(12)(123)^{-1} = (123)(12)(321) = (13) \notin H.$$

Subgrupos Normales - Ejemplos

Algunos ejemplos son los siguientes:

- Los subgrupos $\{1\}$ y G siempre son normales en G.
- El grupo alternante A_n es normal en S_n, ya que es el núcleo del morfismo $\mathrm{sg} : S_n \to G_2$.
- En S_3, el subgrupo $H = \langle (12) \rangle = \{1, (12)\}$ no es normal, pues

$$(123)(12)(123)^{-1} = (123)(12)(321) = (13) \notin H.$$

- Si G es abeliano, todo subgrupo es normal.

Subgrupos Normales - Ejemplos

Algunos ejemplos son los siguientes:

- Los subgrupos $\{1\}$ y G siempre son normales en G.
- El grupo alternante A_n es normal en S_n, ya que es el núcleo del morfismo $\mathrm{sg} : S_n \to G_2$.
- En S_3, el subgrupo $H = \langle(12)\rangle = \{1, (12)\}$ no es normal, pues

$$(123)(12)(123)^{-1} = (123)(12)(321) = (13) \notin H.$$

- Si G es abeliano, todo subgrupo es normal.
- Las matrices ortogonales $\mathrm{O}(n)$ no son un subgrupo normal de $\mathrm{GL}_n(\mathbb{R})$. Por ejemplo, si $O = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{O}(2)$ y $A = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$, entonces $AOA^{-1} = \begin{pmatrix} 0 & 2 \\ -\frac{1}{2} & 0 \end{pmatrix} \notin \mathrm{O}(2)$.

Un Ejercicio

Pueden relacionar los temas anteriores a través del siguiente ejercicio:

Ejercicio

Sea G un grupo finito de orden $n \cdot m$ y H un subgrupo normal de orden n. Probar que:

(i) *Para todo $g \in G$ se tiene que $g^m \in H$.*

(ii) *Más aún, si m y n son coprimos entonces $H = \{g^m : g \in G\}$.*