ÁLGEBRA II

Primer Cuatrimestre – 2020

Clases Prácticas

28 de Abril

Proposición 1. Sea G un grupo y H un subgrupo normal, y notemos $\pi : g \in G \to [g] = gH \in G/H$ a la proyección canónica. Si tenemos $S, T \subset G$ tales que S genera a H y $\pi(T)$ genera a G/H, entonces $S \cup T$ genera a G.

Demostración. Fijemos $g \in G$. Por hipótesis, podemos escribir a $[g] \in G/H$ como producto de elementos de $\pi(T)$ o sus inversos. Esto es, sabemos que existen $t_1, \dots, t_n \in T$ y $\varepsilon_1, \dots, \varepsilon_n \in \{-1, 1\}$ tales que

$$[g] = [t_1]^{\varepsilon_1} \cdots [t_n]^{\varepsilon_n} = [t_1^{\varepsilon_1} \cdots t_n^{\varepsilon_n}].$$

Esta igualdad en el cociente nos dice que tanto g como $t_1^{\varepsilon_1} \cdots t_n^{\varepsilon_n}$ pertenecen a la misma coclase. Por lo tanto, existe $h \in H$ tal que

$$g = t_1^{\varepsilon_1} \cdots t_n^{\varepsilon_n} \cdot h, \tag{1}$$

y como S genera a $H \ni h$, existen a su vez $s_1, \dots, s_m \in S$ y $\delta_1, \dots, \delta_m \in \{-1, 1\}$ tales que $h = s_1^{\delta_1} \cdots s_m^{\delta_m}$.

Reescribiendo **(1)** se obtiene

$$g = t_1^{\varepsilon_1} \cdots t_n^{\varepsilon_n} \cdot s_1^{\delta_1} \cdots s_m^{\delta_m},$$

con cada elemento s_i ó t_j perteneciente a $S \cup T$.

Vemos de esta manera que todo elemento de G se escribe como producto de elementos de $S \cup T$ o sus inversos, lo que concluye la demostración. ■

Ejercicio 1. Probar que:

(i) Una transformación afín $T = A + b$ es inversible si y sólo si A lo es. En tal caso, su inversa es también una transformación afín.

(ii) La composición de transformaciones afines resulta una transformación afín.

Resolución. Hacemos cada inciso por separado. Recordemos que si $A \in \mathsf{M}_n\mathbb{R}$ y $b \in \mathbb{R}^n$, notamos $A + b$ a la transformación afín que envía x a $A \cdot x + b$.

(i) Observemos que las traslaciones son biyectivas. Explícitamente, la inversa de una traslación $S_b(x) := x + b$ es $S_{-b}(x) := x - b$. Por otro lado, sabemos que la composición de biyecciones es una biyección.

Sea ahora $T = A + b$ afín y $L(x) := Ax$. Si A es inversible entonces L lo es, y componiendo por S_b obtenemos que $T = S_b \circ L$ es inversible. Recíprocamente, si $T = A + b$ es inversible, entonces $L = S_{-b} \circ T$ lo es y por lo tanto A también.

Por último, sea $T = A + b$ inversible. Por lo anterior, la matriz A es inversible, así que tiene sentido definir la transformación afín $S := A^{-1} - A^{-1}b$. De esta forma[1] S es la inversa de T, pues

$$(T \circ S)(x) = T(A^{-1}x - A^{-1}b) = A(A^{-1}x - A^{-1}b) + b = x - b + b = x$$

y

$$(S \circ T)(x) = S(Ax + b) = A^{-1}(Ax + b) - A^{-1}b = x + A^{-1}b - A^{-1}b = x.$$

(ii) Sean $T = A + b, S = C + d$ dos transformaciones afines. Concretamente, para cada $x \in \mathbb{R}^n$ es $T(x) = A \cdot x + b$ y $S(x) = C \cdot x + d$. Por un cálculo directo es

$$T \circ S = T(Cx + d) = A(Cx + d) + b = ACx + Ad + b,$$

así que $T \circ S = AC + (Ad + b)$ resulta afín.

■

Ejercicio 2. Sean $H = \{T \in \mathrm{Aff}_n(\mathbb{R}) : \ T \text{ es lineal}\}$ y $K = \{I + b : b \in \mathbb{R}^n\}$ los subgrupos de transformaciones lineales y traslaciones de $\mathrm{Aff}_n(\mathbb{R})$ respectivamente. Probar que:

(i) Existen isomorfismos $H \simeq \mathsf{GL}_n(\mathbb{R})$ y $K \simeq \mathbb{R}^n$.

(ii) El subgrupo K es normal en $\mathrm{Aff}_n(\mathbb{R})$, pero H no.

Demostración. Hacemos cada inciso por separado.

(i) Si $T = A + b \in H$, por linealidad es $b = T(0) = 0$, así que toda tal transformación es de la forma $T(x) = A \cdot x$. La matriz A determina una única transformación afín lineal. Además, si $S(x) = B \cdot x$, entonces $ST(x) = B(Ax) = (BA)x$. Todo esto dice que la asignación $T = A + 0 \in H \mapsto A \in GL_n(\mathbb{R})$ es un isomorfismo de grupos.

Para K, podemos definir $\Gamma : I + b \in K \mapsto b \in \mathbb{R}^n$. Esta función es biyectiva, y es un morfismo pues si $T = I + b$ y $S = I + c$, entonces

$$\Gamma(TS) = \Gamma(I + (b + c)) = b + c = \Gamma(T) + \Gamma(S).$$

(ii) Mostremos primero que K es normal: sean $T = A + b \in \mathrm{Aff}_n(\mathbb{R})$ y $S = I + c \in K$, y veamos que $TST^{-1} \in K$. En efecto, como

$$\begin{aligned} TST^{-1}(x) &= TS(A^{-1}x - A^{-1}b) = T(A^{-1}x - A^{-1}b + c) \\ &= A(A^{-1}x - A^{-1}b + c) + b \\ &= x - b + Ac + b = x + Ac, \end{aligned}$$

debe ser $TST^{-1} = I + Ac \in K$.

Por otro lado H no es normal, ya que por ejemplo si $T = 2I \in H$ y $S = I + e_1 \in \mathrm{Aff}_n(\mathbb{R})$ entonces $S^{-1} = I - e_1$ y

$$STS^{-1}(x) = ST(x - e_1) = S(2x - 2e_1) = 2x - 2e_1 + e_1 = 2x - e_1,$$

por lo que $STS^{-1} = 2I - e_1 \notin H$.

[1] Una forma de deducir la definición de la inversa es la siguiente: si $z = Ax + b$, entonces $z - b = Ax$ y multiplicando por A^{-1} a izquierda, se sigue que $A^{-1}z - A^{-1}b = A^{-1}(z - b) = A^{-1}Ax = x$.

■

Ejercicio 3. ¿Cuántos subgrupos de $D_{7981326}$ que contienen a $H := \langle r^2 \rangle$ hay?

Resolución. La idea del ejercicio es usar la correspondencia entre subgrupos de un cociente y subgrupos que contienen a otro subgrupo dado. Para hacer uso de la misma, debemos ver en primera instancia que H es un subgrupo normal.

Como observamos en la clase, es suficiente para esto probar que sHs, rHr^{-1} y $r^{-1}Hr$ están contenidos en H. Esto último sucede, pues si $r^{2j} \in H$ entonces se tienen las igualdades

$$\begin{aligned} sr^{2j}s &= s^2r^{-2j} = r^{-2j} = (r^{2j})^{-1}, \\ rr^{2j}r^{-1} &= r^{1+2j-1} = r^{2j} \\ r^{-1}r^{2j}r &= r^{-1+2j+1} = r^{2j} \end{aligned}$$

con todos estos elementos de H.

Por lo tanto $D_{7981326}/H$ es un grupo y sus subgrupos están en correspondencia biyectiva con los subgrupos de $D_{7981326}$ que contienen a H. Para conocer esto último, caractericemos al cociente. Como r tiene orden 7981326, sabemos

$$\text{ord}(r^2) = |\langle r^2 \rangle| = \frac{7981326}{2}$$

y por lo tanto, por Lagrange, debe ser

$$|D_{7981326}/H| = \frac{|D_{7981326}|}{|H|} = 4.$$

Sabemos que hay sólo dos grupos de orden 4 salvo isomorfismo, así que o bien $D_{7981326}/H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ o bien $D_{7981326}/H \simeq \mathbb{Z}_4$.

Una vez más usando lo visto en clase, un sistema de generadores para el cociente se obtiene de proyectar un sistema de generadores para el diedral. Concretamente, sabemos que $S = \{[r], [s]\}$ genera $D_{7981326}/H$. Ambos elementos tienen orden dos, pues

$$[r]^2 = [r^2] = [1] \text{ y } [s]^2 = [s^2] = [1]$$

al ser $r^2 \in H$ y $s^2 = 1$. En $\mathbb{Z}_4$, no existen un par de elementos de orden dos que generen al grupo, así que esto nos dice que $D_{7981326}/H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Finalmente, vemos que nuestro problema se reduce a contar los subgrupos de $\mathbb{Z}_2 \times \mathbb{Z}_2$. Contemos primero los subgrupos propios no triviales, que por Lagrange deben tener orden 2. En general, un subgrupo de un grupo G de orden dos es de la forma $K = \{1, g\}$. Como $g^2 \in K$ y no puede ser $g^2 = g$ pues $g \neq 1$, se tiene que $g^2 = 1$. Recíprocamente, si $g \in G$ tiene orden dos, entonces por definición $\langle g \rangle$ es un subgrupo de G de orden dos. Este argumento muestra que la cantidad de subgrupos de orden dos de un grupo es exactamente la cantidad de *elementos* de orden dos.

En $\mathbb{Z}_2 \times \mathbb{Z}_2$ hay 3 elementos de orden dos, todos excepto el neutro. Por lo tanto en este grupo hay 3 subgrupos de orden dos, y junto con todo el grupo y el grupo trivial, en total hay 5 subgrupos. En definitiva,

Respuesta: hay exactamente 5 subgrupos de $D_{7981326}$ que contienen a $\langle r^2 \rangle$.

■

Ejercicio 4. Un grupo G se dice **simple** si $G \neq \{1\}$ y sus únicos subgrupos normales son $\{1\}$ y G.

(i) Sea H un subgrupo normal en un grupo G. Probar que G/H es simple si y sólo si el único subgrupo normal que contiene propiamente a H es G.

(ii) Probar que un grupo abeliano finito G es simple si y sólo si $G \simeq \mathbb{Z}_p$ con p primo. Concluir que en todo grupo abeliano finito $G \neq \{1\}$ existe un subgrupo H tal que $G/H \simeq \mathbb{Z}_p$.

Resolución. Para resolver **(i)** apelamos de vuelta a la correspondencia entre subgrupos de G/H y subgrupos de G que contienen a H. Esta vez usaremos aún más que subgrupos normales se corresponden subgrupos normales.

Observemos también que un grupo es simple, equivalentemente, si tiene exactamente dos subgrupos normales. Esto excluye el caso del grupo trivial, y para todo otro grupo G los subgrupos normales en cuestión deben ser $\{1\}$ y G.

En estos términos, el cociente G/H tiene exactamente dos subgrupos normales si y sólo si hay exactamente dos subgrupos normales que contienen a H, y estos necesariamente deben ser H y G. Por lo tanto, es equivalente que G/H sea simple a que el único subgrupo normal que contiene propiamente a H sea G.

Ahora veamos **(ii)**. Si $G = \mathbb{Z}_p$, por Lagrange sabemos que sus únicos subgrupos tienen orden 1 y p, así que no tiene subgrupos propios no triviales. En consecuencia, es simple.

Recíprocamente, si G es simple, entonces no es el grupo trivial y podemos tomar $x \in G$ distinto de 1. El subgrupo $\langle x \rangle \leq G$ es normal ya que G es abeliano, y como además este último es simple debe ser $\langle x \rangle = G$. Concluimos así que G es cíclico y $G \simeq \mathbb{Z}_n$ con $n = \text{ord}(x) \in \mathbb{N}$. Pero más aún, como $\mathbb{Z}_n$ debe ser simple, necesariamente n debe ser primo. De lo contrario, tendríamos un divisor propio $d|n$ y entonces $\langle d \rangle$ sería un subgrupo propio no trivial de $\mathbb{Z}_n$.

Para terminar, veamos que en un grupo abeliano $G \neq \{1\}$ existe un subgrupo H tal que $G/H \simeq \mathbb{Z}_p$ para algún primo p. Como G no es el grupo trivial, contiene algún subgrupo propio. En particular, como G es finito, podemos considerar H un subgrupo propio de cardinal maximal. Esto en particular nos asegura que no existirán subgrupos $K \supset H$ distintos de G.

Por el ítem **(i)** la observación anterior dice que G/H es simple. Por otro lado, el cociente de un grupo abeliano finito sigue siendo abeliano y finito, así que $G/H \simeq \mathbb{Z}_p$ para algún primo p, como buscábamos. ■