Clase Álgebra II

Franco Rufolo

9 de Septiembre de 2023

Producto directo

Recuerdo: Dados dos grupos H y K, se define su producto directo (externo) $H \times K$ como el producto cartesiano de ellos con la multiplicación coordenada a coordenada. Esta es una manera de conseguir grupos nuevos a partir de otros.

Observaciones:

- Como $H \simeq H \times 1 \leq H \times K$ y $K \simeq 1 \times K \leq H \times K$, se puede identificar H y K como subgrupos del producto de esta manera. Via esta identificación, se tiene que $H, K \trianglelefteq H \times K$. ¿A qué son isomorfos los cocientes?
- Via la identificación, $HK = H \times K$. Es decir, todo elemento de $H \times K$ se escribe como alguien de $H(= H \times 1)$ multiplicado por alguien de $K(= 1 \times K)$.
- Nuevamente, via la identificación de antes, $H \cap K = 1$.

Se tiene el siguiente resultado, que nos da hipótesis suficientes para asegurar que un grupo es un producto directo (externo):

Proposición: Sean G un grupo, $H, K \trianglelefteq G$ dos subgrupos normales de G tales que $G = HK$ y $H \cap K = 1$. Entonces $G = HK \simeq H \times K$.

(Es un ejercicio de la práctica) Esto motiva la siguiente definición:

Definición: Un grupo G en las condiciones de la proposición de recién se dice que es el producto directo interno de H y K.

Observación: Como $H \cap K = 1$, todo elemento de $HK = G$ se escribe de manera única como hk, con $h \in H$ y $k \in K$, pues

$$\begin{aligned} h_1 k_1 &= h_2 k_2 \\ \underbrace{h_2^{-1} h_1}_{\in H} &= \underbrace{k_2 k_1^{-1}}_{\in K} \in H \cap K = 1, \end{aligned}$$

de donde $h_1 = h_2$ y $k_1 = k_2$.

Ejemplo: Sea $n \in \mathbb{N}$ impar. Probemos que $D_{2n} \simeq D_n \times \mathbb{Z}_2$. Consideremos los subgrupos

$$H = \langle s, r^2 \rangle \qquad \text{y} \qquad K = \langle r^n \rangle.$$

Notemos primero que $H \simeq D_n$ y $K \simeq \mathbb{Z}_2$. Veamos ahora que D_{2n} es el producto directo interno de H y K.

- Se tiene que
$$s \in HK \qquad \text{y} \qquad r = (r^2)^{\frac{n+1}{2}} r^n \in HK,$$
de donde $D_{2n} = HK$.
- $[D_{2n} : H] = 2$, por lo que $H \trianglelefteq D_{2n}$.
- $sr^n = r^{-n}s = r^n s$, y $rr^n = r^n r$, es decir que $K \leq Z(D_{2n})$, y en particular, $K \trianglelefteq D_{2n}$.
- Como $H \cap K \leq K = \{1, r^n\}$, veamos que $r^n \notin H$. Si no fuera así, existiría un $m \in \mathbb{N}$ tal que $r^n = (r^2)^m$, pero el término izquierdo tiene orden 2, mientras que el derecho tiene orden divisor de n, que es impar, por lo que no puede ser orden 2. Así, $H \cap K = 1$.

Luego, D_{2n} es el producto directo interno de H y K, y por la proposición concluimos que

$$D_{2n} \simeq H \times K \simeq D_n \times \mathbb{Z}_2,$$

como queríamos ver.

Observación/Ejercicio: $D_{4n} \not\simeq D_{2n} \times \mathbb{Z}_2$.

Producto semidirecto

La idea ahora será, como se hizo con los productos directos, dar una forma de crear nuevos grupos a partir de otros. Esta construcción será una generalización del producto directo, en la que uno de los subgrupos ya no tiene por qué ser normal.

Sean G un grupo, $H \trianglelefteq G$ un subgrupo normal y $K \leq G$ un subgrupo, tales que $G = HK$ y $H \cap K = 1$. En esta situación, sigue siendo cierto que la escritura de los elementos de la forma hk, con $h \in H$ y $k \in K$ es única. Veamos, con esta escritura, cómo escribir su producto:

$$(h_1k_1)(h_2k_2) = h_1k_1h_2(k_1^{-1}k_1)k_2 = \underbrace{h_1(k_1h_2k_1^{-1})}_{\in H}\underbrace{k_1k_2}_{\in K}.$$

Buscamos entonces, hacer como antes: comenzar con dos grupos H y K, y definir un nuevo grupo que contenga copias isomorfas de ellos, de manera que (salvo esta identificación), H sea normal y $H \cap K = 1$. Para esto, hay que entender esta ecuación en términos de H y K, sin asumir que tenemos un grupo que los contiene. Notar en particular, que los productos $h_1(k_1h_2k_1^{-1})$ y k_1k_2 tienen sentido, pero hay que entender cómo escribir $k_1h_2k_1^{-1}$ en términos de H y K.

Para motivarnos, volvamos al caso del grupo G. Como $H \trianglelefteq G$, K actúa en H por conjugación:

$$k \cdot h = khk^{-1},$$

y esta acción da un morfismo $\varphi : K \to \mathrm{Aut}(H)$. De esta manera, el producto se puede escribir como

$$(h_1k_1)(h_2k_2) = (h_1(k_1h_2k_1^{-1}))(k_1k_2) = (h_1k_1 \cdot h_2)(k_1k_2) = (h_1\varphi(k_1)(h_2))(k_1k_2),$$

donde esta expresión depende únicamente de H, K y el morfismo φ, que está definido en términos de H y K. Se tiene el siguiente resultado:

Teorema: Sean H, K grupos y $\varphi : K \to \mathrm{Aut}(H)$ un morfismo. Entonces, $H \times K$ tiene una estructura de grupo dada por

$$(h_1, k_1)(h_2, k_2) = (h_1\varphi(k_1)(h_2), k_1k_2),$$

la cual satisface que $H \times 1$ y $1 \times K$ son subgrupos isomorfos a H y K respectivamente, y que bajo esta identificación,

- $H \trianglelefteq H \times K$.
- $H \cap K = 1$.
- Para todos $h \in H$ y $k \in K$, $khk^{-1} = \varphi(k)(h)$.

Veamos cómo sale lo último, lo demás queda de ejercicio para amigarse con la definición. Deshaciendo la identificación, tenemos

$$\begin{aligned}(1, k)(h, 1)(1, k)^{-1} &= ((1, k)(h, 1))(1, k^{-1}) = (\varphi(k)(h), k)(1, k^{-1}) \\ &= (\varphi(k)(h)\varphi(k)(1), kk^{-1}) = (\varphi(k)(h), 1),\end{aligned}$$

así que, pasando por la identificación, queda lo que queríamos.

Definición: Sean H, K grupos y $\varphi : K \to \mathrm{Aut}(H)$ un morfismo. El producto semidirecto (externo) de H por K con respecto a φ es el grupo recién definido, y se denota por $H \rtimes_\varphi K$.

Ejemplo: Sean H un grupo abeliano y $K = \langle x \rangle$ un grupo cíclico de orden 2 (ambos escritos en notación multiplicativa). Sea $\varphi : K \to \mathrm{Aut}(H)$ definido por $\varphi(x)(h) = h^{-1}$ (invertir es morfismo ya que H es abeliano). Entonces, $H \trianglelefteq H \rtimes_\varphi K$ porque tiene índice 2, y además, por el teorema,

$$\begin{aligned}xhx^{-1} &= h^{-1} \\ xh &= h^{-1}x.\end{aligned}$$

Esto se parece mucho a lo que sucede en el grupo diedral, y de hecho, cuando H es cíclico, se tiene que: si $H \simeq \mathbb{Z}_n$, $H \rtimes_\varphi K \simeq D_n$, y si $H \simeq \mathbb{Z}$, $H \rtimes_\varphi K$ se suele llamar el grupo diedral infinito, denotado por D_∞.

Se tiene el siguiente resultado, que como antes, nos da hipótesis suficientes para asegurar que un grupo es un producto semidirecto (externo):

Proposición: Sean G grupo, $H \trianglelefteq G$, $K \leq G$ tales que $G = HK$ y $H \cap K = 1$, y $\varphi : K \to \mathrm{Aut}(H)$ definido por $\varphi(k)(h) = khk^{-1}$. Entonces $G \simeq H \rtimes_\varphi K$.

Demostración: La función $f : G \to H \rtimes_\varphi K$, $f(hk) = (h, k)$ es una biyección. El hecho de que es un morfismo es la cuenta que hicimos antes para motivar la definición del producto:

$$\begin{aligned}f(h_1k_1h_2k_2) = f((h_1k_1h_2k_1^{-1})(k_1k_2)) &= (h_1k_1h_2k_1^{-1}, k_1k_2) \\ &= (h_1\varphi(k_1)(h_2), k_1k_2) = (h_1, k_1)(h_2, k_2) = f(h_1k_1)f(h_2k_2),\end{aligned}$$

por lo que es un isomorfismo. ■

Como antes, esto motiva definir:

Definición: Se dice que un grupo G es el producto semidirecto (interno) de dos subgrupos H y K si $G = HK$, $H \trianglelefteq G$ y $H \cap K = 1$.

Con este lenguaje y la proposición, concluímos que, como pasaba con el producto directo, la distinción entre la construcción externa e interna termina siendo puramente notacional.

Mencionemos un resultado más, y pasemos a ver una aplicación de esto.

Proposición: Sean H, K grupos y $\varphi : K \to \mathrm{Aut}(H)$ un morfismo. Entonces, las siguientes condiciones son equivalentes:

(a) La identidad entre $H \rtimes_\varphi K$ y $H \times K$ es un morfismo de grupos (y por ende un isomorfismo).

(b) φ es el morfismo trivial (es decir, $\varphi(k) = \mathrm{id}_H$ para todo $k \in K$).

(c) $K \trianglelefteq H \rtimes_\varphi K$.

Usemos todo esto para clasificar una famlia de grupos. Antes, un recuerdo de la guía, y una observación.

Recuerdo:

- Sean G un grupo finito y $H, K \leq G$. Entonces
$$|HK| = \frac{|H||K|}{|H \cap K|}.$$
- Sean G un grupo finito y $H \leq G$ un subgrupo de índice p, con p el menor primo que divide al orden de G. Entonces, $H \trianglelefteq G$.

Observación/Ejercicio: Dado $n \in \mathbb{N}$, sea
$$\begin{aligned}\mathcal{U}_n = \mathcal{U}(\mathbb{Z}_n) &= \{k \in \mathbb{Z}_n : \text{ existe } l \in \mathbb{Z}_n \text{ con } kl = 1\} \\ &= \{k \in \mathbb{Z}_n : (k : n) = 1\},\end{aligned}$$
que se trata de un grupo bajo la multiplicación. Notemos que si $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$, existe $m \in \mathbb{N}$ coprimo con n tal que $\alpha(1) = m$. Se considera la función
$$\begin{aligned} f : \mathrm{Aut}(\mathbb{Z}_n) &\longrightarrow \mathcal{U}_n \\ \alpha &\longmapsto m,\end{aligned}$$
donde $\alpha(1) = m$. Entonces, f es un isomorfismo de grupos. Además, si n es primo, $\mathcal{U}_n$ es cíclico (este último hecho es bastante más difícil de ver a esta altura).

Ejercicio: Clasificar todos los grupos de orden pq, con $p, q \in \mathbb{N}$ primos.

Sea G un grupo de orden pq. Un primer caso que se puede descartar fácil siempre es si existe un elemento de orden pq. En este caso, G es cíclico, y así $G \simeq \mathbb{Z}_{pq}$.

Si no existe dicho elemento, por un lado separemos el caso $p = q$. En este caso, ya sabemos que los grupos de orden p^2 tienen centro no trivial. Luego, $G/Z(G)$ tiene orden 1 o p, y por lo tanto

es cíclico. En particular, (por un ejercicio de la guía), G es abeliano. Sea $x \in G$. Como no hay elementos de orden p^2, por Lagrange, $\text{ord}(x) = p$. Sea $y \in G \setminus \langle x \rangle$ (este conjunto es no vacío porque tiene orden p). Así, como $|\langle x, y \rangle| > |\langle x \rangle| = p$, se tiene $G = \langle x, y \rangle = \langle x \rangle \langle y \rangle$. Ambos subgrupos son normales por abelianidad, y tienen intersección trivial (por Lagrange). Luego, $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

Si ahora $p \neq q$, asumamos sin pérdida de generalidad que $p > q$. Por el Teorema de Cauchy sabemos que existe un elemento $x \in G$ de orden p. Así, $P = \langle x \rangle$ es un subgrupo de G de orden p. En particular, tiene índice q, que es el menor primo que divide al orden de G. Por el ejercicio antes mencionado de la guía, es normal en G. Nuevamente por el Teorema de Cauchy, existe un elemento $y \in G$ de orden q. Sea $Q = \langle y \rangle$. Como $p \neq q$, $P \cap Q = 1$ (por Lagrange). Así,

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = |G|,$$

de donde $G = PQ$. Luego, sabemos que si $\varphi : Q \to \text{Aut}(P)$ es el morfismo definido por

$$\varphi(q)(p) = qpq^{-1},$$

obtenemos $G \simeq P \rtimes_\varphi Q$. Analicemos qué posibilidades tiene φ. Por un lado, notemos que $\ker\varphi \leq Q$, de donde φ es trivial o monomorfismo (por Lagrange). Como P es cíclico de orden p, por la observación de antes, $\text{Aut}(P) \simeq \text{Aut}(\mathbb{Z}_p) \simeq \mathcal{U}_p$, y en particular, tiene $p - 1$ elementos. Por el Primer Teorema de Isomorfismo aplicado a φ, sabemos que

$$Q/\ker\varphi \simeq \text{Im}\varphi \leq \mathcal{U}_p,$$

de donde $|Q/\ker\varphi| = (q/|\ker\varphi|)|p - 1$. Tenemos entonces dos casos:

Si $q \nmid p - 1$, φ es el morfismo trivial, y entonces $G \simeq P \times Q \simeq \mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq}$, cosa absurda, porque asumimos que no teníamos elementos de orden pq.

Si $q|p - 1$, como P es cíclico de orden primo, $\text{Aut}(P)$ es cíclico. Luego, contiene un único subgrupo de orden q, digamos, de la forma $\langle a \rangle$ (recordar que todo subgrupo de un grupo cíclico es cíclico). Así, los posibles morfismos estarán dados por $\varphi_n(y) = a^n$ para algún $0 \leq n \leq q - 1$. φ_0 es el morfismo trivial, y la afirmación ahora, que queda para la clase que viene, es que para todos $1 \leq n, m \leq q - 1$, $P \rtimes_{\varphi_n} Q \simeq P \rtimes_{\varphi_m} Q$.