Ayudantia 10

Profesor: Cristóbal Rivas
Ayudantes: Benajamin Martinez, Javier Pavez

Viernes 30 de Septiembre 2022

Ejercicio 10.1. Sean G, H grupos y $\varphi : G \longrightarrow Aut(H)$ un homomorfismo. Demostrar que $H \rtimes_\varphi G$ es abeliano si y solo si G, H son abelianos y φ es el homomorfismo que envía todo al neutro respectivo.

Demostración. ($\Leftarrow$) 1° Veremos lo que significa que φ envíe todo al neutro. El neutro de $Aut(H)$ es la función identidad de H, por temas de notación diremos que es $id_{Aut(H)} \equiv f : H \longrightarrow H$, $h \mapsto h$. Luego, $\varphi(g) = f \in Aut(H)\ \forall g \in G$, o sea, $\varphi_g := \varphi(g) = f \in Aut(H)\ \forall g \in G$. Así nos queda que $\varphi_g(x) = f(x) = x\ \forall (g,\, x) \in G \times H$.

2° Veremos que significa que nuestros grupos sean abelianos. Por definición tendremos que $gy = yg\ \forall g,\, y \in G$ y $hx = xh\ \forall h,\, x \in H$. Luego, $(hy,\, gx) = (yh,\, xg)\ \forall g,\, y \in G$ y $\forall h,\, x \in H$.

3° Usar 1° y 2°. Sean $x,\, g \in G$ y $y,\, h \in H$. Por definición del producto semidirecto tendremos (1) y (5); por 1° tendremos (2) y (4); y por 2° tendrémos (3).

$$\begin{aligned} (h,g)(x,y) &= (h\varphi_g(x), gy) && (1)\\ &= (hx, gy) && (2)\\ &= (xh, yg) && (3)\\ &= (x\varphi_y(h), yg) && (4)\\ &= (x,y)(h,g) && (5) \end{aligned}$$

Lo anterior se cumple para todo $x,\, h \in H$ y todo $y,\, g \in G$, ya que eran cualquier elemento de sus respectivos grupos. Eso es equivalente a decir que se cumpe para todo $(h,\, g),\, (x,\, y) \in H \rtimes_\varphi G$, lo que demuestra su conmutatividad y concluye la demostración de esta implicancia.

($\Rightarrow$) 4° Veremos lo que significa que nuestro grupo sea abeliano. Por definición tendremos que $(h,g)(x,y) = (x,y)(h,g)$ para todo $(h,\, g),\, (x,\, y) \in H \rtimes_\varphi G$. Por definición de prodructo directo obtenemos (6) y (7).

$$\begin{aligned} (h,g)(x,y) &= (h\varphi_g(x), gy) && (6)\\ (x,y)(h,g) &= (x\varphi_y(h), yg) && (7) \end{aligned}$$

Deduciendo de (6) y (7) que $(h\varphi_g(x), gy) = (x\varphi_y(h), yg)$ para todo $(h,\, g),\, (x,\, y) \in H \rtimes_\varphi G$.

5° Usar la definición de los elementos de nuestro grupo. De lo deducido en 4°, obtenemos que $h\varphi_g(x) = x\varphi_y(h)$ y $gy = yg$ para todo $(h,\, g),\, (x,\, y) \in H \rtimes_\varphi G$; o sea, $h\varphi_g(x) = x\varphi_y(h)$ y $gy = yg$ para todo $h,\, x \in H$ y todo $g,\, y \in G$. La última igualdad nos dice que G es abeliano, por lo que ya demostramos una de las tres cosas pedidas ($\checkmark$).

6° Ir de lo más general a lo más particular. En 5° obtuvimos que $h\varphi_g(x) = x\varphi_y(h)$ para todo $h,\, x \in H$ y todo $g,\, y \in G$. Luego, tendremos que la igualdad se cumplirá para todo $h \in H$, todo $g,\, y \in G$ y $x = id_H$. O sea, $h\varphi_g(id_H) = id_H\varphi_y(h)$ para todo $h, \in H$ y todo $g,\, y \in G$.

Con la propiedad de los homomorfismos de preservar el neutro y la propiedad del neutro de preservar los elementos del grupo deducimos (8) y (9).

$$h\varphi_g(id_H) = h \cdot id_H = h \tag{8}$$

$$id_H\varphi_y(h) = \varphi_y(h) \tag{9}$$

Estas igualdades se siguen cumpliendo para todo $h \in H$ e $y \in G$. Luego, como (8) y (9) son iguales ya que $h\varphi_g(id_H) = id_H\varphi_y(h)$, obtenemos que $\varphi_y(h) = h$ para todo $h \in H$ y todo $y \in G$. Esto significa que $\varphi_y = f$ nuestra función identidad en H para todo $y \in G$. O sea, $\varphi(y) = \varphi_y = f$ para todo $y \in G$, lo que es equivalente a decir que φ envía todo al neutro. Por lo que ya demostramos dos de las tres cosas pedidas (✓).

7° Por 6° tenemos que $\varphi(y) = \varphi_y = f = \varphi_g = \varphi(g)$ para todo $y,\, g \in G$. Remplazando eso en lo obtenido en 5°, llegamos a que $hx = hf(x) = h\varphi_g(x) = x\varphi_y(h) = xf(h) = xh$ para todo $x,\, h \in H$ y todo $y,\, g \in G$. O sea, $hx = xh$ para todo $x,\, h \in H$, lo que demuestra que H es abeliano. Por lo que demostramos tres de las tres cosas que queríamos demostrar. ✓✓ □

Ejercicio 10.2. Demostrar que existen al menos tres grupos no isomorfos entre si, que provienen de un producto semidirecto $H \rtimes \mathbb{Z}/3\mathbb{Z}$, donde H es un grupo de cardinalidad 4.
Hint: $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong D_3$.

Demostración. Como H es un grupo de cardinalidad 4, tenemos dos opciónes, $H = \mathbb{Z}/4\mathbb{Z}$ o $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

($H = \mathbb{Z}/4\mathbb{Z}$) Consideramos el homomorfismo trivial $\varphi : \mathbb{Z}/3\mathbb{Z} \to Aut(H)$, $g \mapsto id_{Aut(H)}$. Obteniendo que $H \rtimes_\varphi \mathbb{Z}/3\mathbb{Z} \cong H \times \mathbb{Z}/3\mathbb{Z}$, usando el problema 10.3. b), deducimos que $H \rtimes_\varphi \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$. O sea, es un grupo cíclico.

($H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) 1° Consideramos de nuevo el homomorfismo trivial $\psi : \mathbb{Z}/3\mathbb{Z} \to Aut(H)$, $g \mapsto id_{Aut(H)}$. Obteniendo que $H \rtimes_\varphi \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, usando el problema 10.3. a), deducimos que $H \rtimes_\varphi \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. O sea un grupo abeliano. Nos percatamos que su cardinalidad es 18, pero $6 \cdot g = (0,\, 0)$ para todo $g \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, por lo que no puede ser un grupo ciclico.

2° Usando el Hint, tendremos un $\psi : D_3 \to Aut(H)$ isomorfismo, no sabemos cual es su regla de asignación pero sabemos que existe.
Definimos $f : \mathbb{Z}/3\mathbb{Z} \to D_3$, $[x] \mapsto r^x$. Notemos que está bien definido porque $ord(r) = 3$ por definición de D_3. Sean $[x],\, [y] \in \mathbb{Z}/3\mathbb{Z}$ tal que $[x] = [y]$, tendremos que $x - y = 3m$ con $m \in \mathbb{Z}$. Luego, $r^{x-y} = r^{3m} = (r^3)^m = id_{D_3}^m = id_{D_3}$, por lo que $r^x = r^y$ y obtenemos que está bien definida ya que $f([x]) = f([y])$. Además es un homomorfismo, ya que $f([x]+[y]) = f([x+y]) = r^{x+y} = r^x r^y = f(x)f(y)$.
Finalmente, definimos nuestra función $\varphi : \mathbb{Z}/3\mathbb{Z} \to Aut(H)$, $x \mapsto (\psi \circ f)(x)$. Notar que es un homomorfismo ya que es la composición de homomorfismos. Debemos notar que esta función no envía todo al neutro, ya que $\varphi([1]) = (\psi \circ f)([1]) = \psi(f([1])) = \psi(r) \neq id_{Aut(H)}$, esta última no-igualdad la tenemos porque ψ es inyectiva por lo que $r \neq id_{D_3}$ implica que $\psi(r) \neq \psi(id_{D_3}) = id_{Aut(H)}$.
Así, como φ no envía todo al cero, por el problema 10.1 $H \rtimes \mathbb{Z}/3\mathbb{Z}$ no es abeliano, lo que termina la demostración.

En conclusión, tenemos un grupo cíclico, uno abeliano pero no cíclico y uno no abeliano; por lo que entre si no pueden ser isomorfos y tenemos tres grupos diferentes entre si salvo isomorfismo. □

Ejercicio 10.3. Sean p y q primos distintos en los naturales y m y n números naturales tal que $MCD(m,\, n) = 1$.

a) Demostrar que $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

b) Demostrar que $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Demostración. Como a) es un caso particular de b), porque $MCD(p, q) = 1$ siempre que sean primos distintos, demostraremos solamente b).

Consideremos $\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $x \mapsto ([x], [x])$; notar que la primera cordenada está en $\mathbb{Z}/m\mathbb{Z}$ y la segunda cordenada está en $\mathbb{Z}/n\mathbb{Z}$, queda como ejercicio para el lector demostrar que π es un homomorfismo.

Usaremos el primer teorema de isomorfía para la demostración.
Primeros nos aseguraremos que sea sobreyectiva. Como $MCD(m, n) = 1$, necesariamente existen $t, s \in \mathbb{Z}$ tal que $1 = tm + sn$. Luego, $1 \equiv tm \pmod{n}$ y $1 \equiv sn \pmod{m}$.
Sea $([x], [y]) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, consideramos $z = x(sn) + y(tm)$ y calculamos.

$$\begin{aligned}
\pi(z) &= ([z], [z]) &(10)\\
&= ([x(sn) + y(tm)], [x(sn) + y(tm)]) &(11)\\
&= ([x(sn)] + [y(tm)], [x(sn)] + [y(tm)]) &(12)\\
&= ([x][sn] + [y][tm], [x][sn] + [y][tm]) &(13)\\
&= ([x][1] + [y][0], [x][0] + [y][1]) &(14)\\
&= ([x \cdot 1] + [y \cdot 0], [x \cdot 0] + [y \cdot 1]) &(15)\\
&= ([x] + [0], [0] + [y]) &(16)\\
&= ([x + 0], [0 + y]) &(17)\\
&= ([x], [y]) &(18)
\end{aligned}$$

Dado que $([x], [y])$ es cualquier elemento de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, deducimos que π es sobreyectiva.

Finalmente, calculemos $Ker\varphi$. Lo haremos por doble inclusión.
Sea $z \in \mathbb{Z}$ tal que $\pi(z) = ([0], [0])$ ($z \in Ker\varphi$). Así tendremos que $([z], [z]) = ([0], [0])$, o sea, $z \equiv 0 \pmod{m}$ y $z \equiv 0 \pmod{n}$. Eso último quiere decir que m y n dividen a z. Por lo que necesariamente $MCM(m, n)$ divide z, pero como $MCD(m, n) = 1$, obtenemos que $MCM(m, n) = mn$. Y como mn divide a z entonces $z \in mn\mathbb{Z}$. Deduciendo que $Ker\varphi \subset mn\mathbb{Z}$.
Sea $z \in mn\mathbb{Z}$. Luego, $z = t(mn)$ para algún $t \in \mathbb{Z}$. Por lo que $\varphi(z) = \varphi(t(mn)) = ([t(mn)], [t(mn)]) = ([t]([m][n]), [t]([m][n])) = ([t]([0][n]), [t]([m][0])) = (0, 0)$, teniendo que $z \in Ker\varphi$. Deduciendo que $mn\mathbb{Z} \subset Ker\varphi$.
Y con lo anterior llegamos a que $Ker\varphi = mn\mathbb{Z}$.

Usando el primer teorema de isomofía concluimos que $\mathbb{Z}/mn\mathbb{Z} = \mathbb{Z}/Ker\varphi \cong Im(\varphi) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. □

Problemas propuestos por estudiantes.

Ejercicio 1 Guía 3. Sea G un grupo abeliano y $Tor(G) = \{g \in G \mid ord(g) < \infty\}$, el conjunto de elementos de orden finito de G. Demuestre que $Tor(G)$ es un subgrupo de G.

Demostración. 1° Demostrar que es distinto de vacío.
Dado que $id_G^1 = id_G$, tenemos que $ord(id_G) = 1$. Luego, $id_G \in Tor(G)$, por lo que $Tor(G) \neq \emptyset$. ✓

2° Demostrar que es cerrado bajo multiplicación.
Sean $x, y \in Tor(G)$. Por definición existen $m, n \in \mathbb{N}$ tal que $x^m = id_G = y^n$. Luego, como el grupo es abeliano podemos decir que $(xy)^{mn} = x^{mn}y^{mn}$, y con propiedades de potencias llegamos a que $x^{mn}y^{mn} = (x^m)^n(y^n)^m = id_G^n id_G^m = id_G$. Deduciendo que $ord(xy) \leq mn$, por ende $xy \in Tor(G)$, por lo que $Tor(G)$ es cerrado bajo multiplicación. ✓

3° Demostrar que es cerrado bajo inversos.
Sea $x \in Tor(G)$. Por definición existe $m \in \mathbb{N}$ tal que $x^m = id_G$. Luego, $(x^{-1})^m = (x^m)^{-1} = id_G^{-1} = id_G$. Deduciendo que $ord(x^{-1}) \leq m$, por ende $x^{-1} \in Tor(G)$, por lo que $Tor(G)$ es cerrado bajo inversos. ✓ □

Comentario: En el siguiente ejercicio tuve un error de comprensión lectora durante la ayudantantía. Dejaré lo que entendí inicialmente para que el lector pueda descubrir cual fue el error. Además la solución real del problema.
El error en mi comprensión se reduce a que entendí que lo que había que demostrar era: "Para algún H tal que tenga índice finito, entonces existe N tal que..."

Ejercicio 4 Guía 3. Suponga que G contiene un subgrupo H de índice finito. Demuestre que G contiene un subgrupo normal N tal que N tiene índice finito y $N \subset H$.
Ayuda: Considere la acción por multiplicación a izquierda de G en G/H.

Demostración. Siguiendo la ayuda y considerando esa acción, por la proposición 1.77. de los apuntes de la clase existe un homomorfismo $\varphi : G \longrightarrow Sym(G/H)$. Como $|G/H| = [G : H] < \infty$, tendremos que $|Sym(G/H)| < \infty$, algo que usaremos más adelante.

Dado que $Ker\varphi \lhd G$, diremos que $N = Ker\varphi$ y demostraremos lo faltante.

Demostraremos primero la contención.
Sea $z \in Ker\varphi$, tendremos que $\varphi(z) = (1) \in Sym(G/H)$. Luego, $z(xH) = xH$ para todo $xH \in G/H$. En particular, $zH = (zid_G)H = z(id_G H) = id_G H$. Deducimos que $z \in H$ y por ende $Ker\varphi \subset H$, o sea, $N \subset H$. ✓

Finalmente demostraremos el que tenga índice finito.
Usando el primer teorema de isomorfía, tendremos (19).

$$G/N = G/Ker\varphi \cong Im(\varphi) \leq Sym(G/H) \tag{19}$$

Como djimos, $|Sym(G/H)| < \infty$, añadiendo eso a (19), tenemos que $[G : N] = |G/N| = |Im(\varphi)| \leq |Sym(G/H)| < \infty$. Lo que verfifica lo último sobrante, que el índice de N sea finito. ✓

En conclusión, para todo subgrupo H de G que tenga índice finito, existe un subgrupo normal N ($Ker\varphi$) de G tal que también tiene índice finito y $N \subset H$. □