

PAUTA AYUDANTÍA 1 ESTRUCTURAS ALGEBRAICAS

14 DE MARZO DE 2023

Problema 1. Demuestre que todos los subgrupos de \mathbb{Z} son de la forma $n\mathbb{Z}$ para algún $n \in \mathbb{Z}$. Si $m, n \in \mathbb{Z}$ son enteros distintos, determine bajo qué condiciones sobre m y n se verifica que $n\mathbb{Z}$ es subgrupo de $m\mathbb{Z}$.

Demostración. Es claro que los subconjuntos de la forma $n\mathbb{Z}$ son subgrupos, así que la demostración consiste en probar que todo subgrupo es de esta forma. Sea entonces $H \subseteq \mathbb{Z}$ subgrupo y consideremos $n = \min(H \cap \mathbb{Z}_+)$, el cual existe pues estamos tomando el mínimo de un subconjunto de números naturales (principio del buen orden). Probaremos que $H = n\mathbb{Z}$. Por un lado es directo que $n\mathbb{Z} \subseteq H$ pues H es subgrupo. Sea $x \in H$, y gracias al lema de división euclidea existen $q, r \in \mathbb{Z}$ tales que $x = nq + r$ con $0 \leq r < n$. Como $nq \in n\mathbb{Z} \subseteq H$, como H es subgrupo tenemos que $r = x - nq \in H$, y por minimalidad de n tenemos que $r = 0$. Notemos que la condición $n\mathbb{Z} \subseteq m\mathbb{Z}$ se cumple si y sólo si $m|n$, puesto que si suponemos $n\mathbb{Z} \subseteq m\mathbb{Z}$ entonces $np \in m\mathbb{Z}$ para todo $p \in \mathbb{Z}$, y tomando $p = 1$ encontramos que existe $q \in \mathbb{Z}$ tal que $n = mq$, y por otro lado si $m|n$ entonces $n = mq$ y $np = mqp \in m\mathbb{Z}$ para todo $p \in \mathbb{Z}$. \square

Problema 2. Sean $(G, \cdot_G), (H, \cdot_H)$ grupos. Definimos el *producto directo* de G, H como el grupo cuyo conjunto subyacente es

$$G \times H = \{(g, h) | g \in G, h \in H\}$$

junto con la ley de composición

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2) \quad \forall g_1, g_2 \in G, \forall h_1, h_2 \in H$$

1. Demuestre que $G \times H$ es un grupo.
2. Muestre que $G \times H$ es abeliano si y solo si G y H son ambos abelianos.
3. Sean $g \in G, h \in H$ elementos de orden finito. Pruebe que el orden de (g, h) es el mínimo común múltiplo entre $|g|$ y $|h|$.
4. Suponga que G, H son grupos finitos cíclicos. Muestre que $G \times H$ es cíclico si y sólo si $\text{mcd}(|G|, |H|) = 1$.
5. Dé un ejemplo de un producto directo $G \times H$ el cual contenga un subgrupo que no sea de la forma $K \times L$ con K, L subgrupos de G, H respectivamente.

Demostración.

1. Notar que el elemento neutro en $G \times H$ corresponde a (e_G, e_H) y el elemento inverso de un elemento arbitrario $(g, h) \in G \times H$ está dado por (g^{-1}, h^{-1}) . El hecho que estos elementos son efectivamente neutro e inverso, y que la ley de grupo definida es asociativa se deja como ejercicio para el lector.
2. Si G, H son abelianos esto es directo. En efecto, si $(g_1, h_1), (g_2, h_2) \in G \times H$ entonces

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2) = (g_2 \cdot_G g_1, h_2 \cdot_H h_1) = (g_2, h_2) \cdot (g_1, h_1)$$

Ahora suponemos que $G \times H$ es abeliano. Sean $g_1, g_2 \in G, h_1, h_2 \in H$. Entonces como el producto es abeliano

$$(g_1 \cdot_G g_2, h_1 \cdot_H h_2) = (g_1, h_1) \cdot (g_2, h_2) = (g_2, h_2) \cdot (g_1, h_1) = (g_2 \cdot_G g_1, h_2 \cdot_H h_1)$$

y así vemos que $g_1 \cdot_G g_2 = g_2 \cdot_G g_1$ y $h_1 \cdot_H h_2 = h_2 \cdot_H h_1$, deduciendo que G, H son ambos abelianos.

3. En primer lugar, notar que para todo $(g, h) \in G \times H$ tenemos que $(g, h)^n = (g^n, h^n)$ para todo $n \in \mathbb{Z}$ (directo utilizando inducción). Denotemos $n := |g|, m := |h|, k = |(g, h)|$ entonces notamos que $(g, h)^r = (e_G, e_H)$ si y sólo si $g^r = e_G$ y $h^r = e_H$, y esto a su vez equivale a decir que $n|r$ y $m|r$, que es equivalente a afirmar que $\text{mcm}(n, m)|r$. Así, por un lado tenemos que $\text{mcm}(n, m)|k$, mientras que por otro tenemos que $(g, h)^{\text{mcm}(n, m)} = 0$, de donde $\text{mcm}(n, m) = k$.

4. (\Rightarrow) Suponer que $G \times H$ es cíclico y sea $(g, h) \in G \times H$ un generador. Notar ahora que el orden del producto directo corresponde a $|G \times H| = |G||H| = nm$ donde denotamos $n := |G|, m := |H|$. Además, por el punto anterior tenemos que $|(g, h)| = \text{mcm}(|g|, |h|)$. Veamos que g es un generador de G . Sea $g' \in G$. Dado que (g, h) genera $G \times H$ tenemos que existe $k \in \mathbb{N}$ tal que

$$(g, h)^k = (g^k, h^k) = (g', e_H) \Rightarrow g^k = g'$$

De manera similar podemos probar que h es un generador de H . De esta manera, como el orden de un grupo cíclico es igual al orden de su generador tenemos que

$$\text{mcm}(n, m) = \text{mcm}(|g|, |h|) = |(g, h)| = |G \times H| = nm$$

La conclusión se sigue notando que el mínimo común múltiplo es igual al producto solo en caso que $\text{mcd}(n, m)^1$. (\Leftarrow) Suponer que $\text{mcd}(|G|, |H|) = 1$. Sean $g \in G, h \in H$ tales que $\langle g \rangle = G, \langle h \rangle = H$ y denotemos nuevamente $n := |G|, m := |H|$. Probaremos que $(g, h) \in G \times H$ tiene orden nm lo cual permitirá concluir. Sea $k := |(g, h)|$. Entonces

$$\begin{aligned} (g, h)^k = (g^k, h^k) = e_{G \times H} &\Rightarrow g^k = e_G \quad \wedge \quad h^k = e_H \\ &\Rightarrow n|k \quad \wedge \quad m|k \\ &\Rightarrow \text{mcm}(n, m)|k \\ &\Rightarrow nm|k \end{aligned}$$

donde la última línea se debe a que n, m son coprimos. Sin embargo,

$$(g, h)^{nm} = ((g^n)^m, (h^m)^n) = e_{G \times H}$$

así que $|(g, h)| = nm$.

5. Considere el grupo $\mathbb{Z} \times \mathbb{Z}$ y el subgrupo diagonal $\Delta := \{(n, n) | n \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$. Note que si existieran K, L subgrupos de \mathbb{Z} tales que $\Delta = K \times L$ entonces $K = \mathbb{Z}$ pues Δ recorre todo \mathbb{Z} , pero es evidente que $\Delta \subsetneq \mathbb{Z} \times \mathbb{Z}$.

□

Problema 3. Sea G un grupo y $\{H_i\}_{i \in I}$ colección arbitraria de subgrupos de G .

1. Pruebe que la intersección $\bigcap_{i \in I} H_i$ sigue siendo un subgrupo de G .
2. Si H_1, H_2 son subgrupos de G , demuestre que $H_1 \cup H_2$ es subgrupo si y solo si $H_1 \subseteq H_2$ o bien $H_1 \supseteq H_2$.
3. Si $H_1 \subseteq H_2 \subseteq \dots$ una cadena ascendente de subgrupos de G , demuestre que $\bigcup_{n \in \mathbb{N}_{\geq 1}} H_n$ es subgrupo de G .

Demostración. 1. Basta con notar que la intersección es cerrada bajo la ley de grupo, puesto que las propiedades de grupo vienen dadas naturalmente por G . Para ello notamos que

$$g, h \in \bigcap_{i \in I} H_i \Rightarrow g, h \in H_i \quad \forall i \in I \Rightarrow gh \in H_i \quad \forall i \in I \Rightarrow gh \in \bigcap_{i \in I} H_i$$

y similar para los inversos, puesto que si $g \in \bigcap_{i \in I} H_i$ entonces $g^{-1} \in H_i$ para todo $i \in I$ y luego está en la intersección.

2. Notemos que la dirección (\Leftarrow) es directa. Supongamos entonces que $H_1 \cup H_2$ es subgrupo de G y además que $H_1 \subsetneq H_2$ y $H_2 \subsetneq H_1$. Podemos entonces encontrar $g_1 \in H_1 \setminus H_2$ y $g_2 \in H_2 \setminus H_1$ y como $H_1 \cup H_2$ es subgrupo tenemos que $g_1 g_2 \in H_1 \cup H_2$, lo cual significa que $g_1 g_2 \in H_1$ o bien $g_1 g_2 \in H_2$. Sin pérdida de generalidad suponemos que $g_1 g_2 \in H_1$. Entonces multiplicando por g_1 y usando que H_1 es subgrupo tenemos que $g_2 = g_1^{-1}(g_1 g_2) \in H_1$ lo cual supone una contradicción con el hecho que $g_2 \notin H_1$.

¹En general se tiene que $\text{mcm}(m, n) \text{mcd}(m, n) = mn$.

3. Sean $g, h \in \bigcup_{n \in \mathbb{N}^{\geq 1}} H_i$. Entonces por definición existen $i, j \in \mathbb{N}^{\geq 1}$ tales que $g \in H_i, h \in H_j$. Dado que los grupos forman una cadena ascendente de subgrupos de G entonces tenemos que $g, h \in H_k$ donde $k := \max\{i, j\}$, y como H_k es subgrupo entonces $gh \in H_k$. Directamente tenemos entonces que $gh \in \bigcup_{n \in \mathbb{N}^{\geq 1}} H_i$. De manera similar se chequea que $\bigcup_{n \in \mathbb{N}^{\geq 1}} H_i$ es cerrado bajo inverso, pues basta con notar que si $g \in \bigcup_{n \in \mathbb{N}^{\geq 1}} H_i$ entonces existe $i \in \mathbb{N}^{\geq 1}$ tal que $g \in H_i$ y entonces $g^{-1} \in H_i$, deduciendo $g^{-1} \in \bigcup_{n \in \mathbb{N}^{\geq 1}} H_i$. \square

Problema 4. Muestre que no existe un morfismo de grupos sobreyectivo $f : (\mathbb{Q}, +) \rightarrow (\mathbb{Q}^{>0}, \times)$.

Demostración. Supongamos que existe $f : (\mathbb{Q}, +) \rightarrow (\mathbb{Q}^{>0}, \times)$ morfismo sobreyectivo. Luego por definición existe $x \in \mathbb{Q}$ tal que $f(x) = 2$. Entonces como f es morfismo se tiene que

$$f(x) = f\left(\frac{x}{2} + \frac{x}{2}\right) = f\left(\frac{x}{2}\right)^2 \implies f\left(\frac{x}{2}\right) \notin \mathbb{Q}$$

lo cual es una contradicción. Se concluye que dicho morfismo no existe. \square

Definición. Sea G un grupo. Definimos el grupo de automorfismos de G , denotado por $\text{Aut}(G)$ como el conjunto

$$\text{Aut}(G) = \{f : G \rightarrow G \mid f \text{ es automorfismo}\}$$

junto con la composición de funciones como ley de grupo.

Problema 5. Considere el grupo de enteros módulo n , denotado por $\mathbb{Z}/n\mathbb{Z}$. Demuestre que $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Indicación: Muestre en primer lugar que el orden de un elemento $x \in \mathbb{Z}/n\mathbb{Z}$ es $n/\text{mcd}(x, n)$.

Demostración. Comenzamos probando la indicación. Para ello notemos que si $x \in \mathbb{Z}/n\mathbb{Z}$ entonces

$$x \cdot (n/\text{mcd}(x, n)) = n \cdot (x/\text{mcd}(x, n)) = 0$$

Sea $m \geq 1$ tal que $mx = 0$ en $\mathbb{Z}/n\mathbb{Z}$. Para concluir debemos probar entonces que $n/\text{mcd}(x, n) \leq m$. Como $mx = 0$ en $\mathbb{Z}/n\mathbb{Z}$ esto se traduce en que $n \mid mx$ así que $(n/\text{mcd}(x, n)) \mid (x/\text{mcd}(x, n))m$, y como $n/\text{mcd}(x, n)$ y $x/\text{mcd}(x, n)$ son coprimos necesariamente tenemos que $(n/\text{mcd}(x, n)) \mid m$, de donde se tiene la conclusión.

Dado que $\mathbb{Z}/n\mathbb{Z}$ es un grupo cíclico con generador 1, es claro que un morfismo de grupos $f \in \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ queda determinado por $m = f(1)$. En efecto, por definición de morfismo de grupos $f(x) = f(1 + \dots + 1) = f(1) + \dots + f(1) = mx$ así que todos sus valores quedan fijados. Además es claro que la imagen de f viene dada por el subgrupo generado por m , es decir, $\text{Im}(f) = \langle m \rangle \subseteq \mathbb{Z}/n\mathbb{Z}$. Ahora, si $f \in \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ en particular es sobreyectivo y entonces $\langle m \rangle = \mathbb{Z}/n\mathbb{Z}$, y por la indicación debemos entonces tener que $\text{mcd}(m, n) = 1$ (pues el orden de m es $n/\text{mcd}(m, n)$ y se debe tener que este orden sea justamente n para la sobreyectividad. Esto sucede entonces si y sólo si $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ ³, y en este caso tenemos que $f(x) = mx$ con inversa $f^{-1}(x) = m^{-1}x$.

Tenemos entonces una biyección

$$\varphi : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(\mathbb{Z}/n\mathbb{Z}), m \mapsto \varphi_m \quad \text{donde} \quad \varphi_m : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, x \mapsto mx$$

Más aún, esta biyección es un morfismo de grupos puesto que

$$\varphi_m \circ \varphi_k(x) = \varphi_m(\varphi_k(x)) = \varphi_m(kx) = mkx = \varphi_{mk}(x) \quad x \in \mathbb{Z}/n\mathbb{Z}$$

lo cual se traduce en

$$\varphi(m) \circ \varphi(k) = \varphi_m \circ \varphi_k = \varphi_{mk} = \varphi(mk)$$

Como último comentario, note que el morfismo inverso de φ corresponde a:

$$\psi : \text{Aut}(\mathbb{Z}/n\mathbb{Z}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times, f \mapsto f(1)$$

el cual es un morfismo por teoría general. \square

²Note que al introducir $n = 0$ obtenemos que $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}^\times = \{\pm 1\}$, i.e. los únicos automorfismos de \mathbb{Z} son $\pm \text{id}$.

³ m es invertible en $\mathbb{Z}/n\mathbb{Z}$ si y sólo si existe $k \in \mathbb{Z}$ tal que $mk \cong 1$ (mód n) si y sólo si existe $b \in \mathbb{Z}$ tal que $mk + bn = 1$ si y sólo si m, n son coprimos, donde la última equivalencia es gracias al lema de Bézout.