

P1

(a) Sean $f, g, h \in \mathcal{F}$

* Sabemos que $(f \circ (g \circ h))(x) = f((g \circ h)(x))$
 $= f(g(h(x)))$
 $= (f \circ g)(h(x))$
 $= ((f \circ g) \circ h)(x) \quad \forall x \in \mathbb{R}$

Es decir: $f \circ (g \circ h) = (f \circ g) \circ h$

γ , por lo tanto, $\circ$ asocia en $\mathcal{F}$.

* Además, $\text{id}: \mathbb{R} \rightarrow \mathbb{R}$ def. por $\text{id}(x) = x$, verifica: $\forall x \in \mathbb{R}$

$$(f \circ \text{id})(x) = f(\text{id}(x)) = f(x) = \text{id}(f(x)) = (\text{id} \circ f)(x)$$

γ como $\text{id} \in \mathcal{F}$, id es el neutro en $\mathcal{F}$ para $\circ$.

* Como f es biyectiva, existe f^{-1} (inversa de f),
que verifica: $\forall x \in \mathbb{R}$

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = x = \text{id}(x) = x = f^{-1}(f(x)) = (f^{-1} \circ f)(x)$$

$\therefore (\mathcal{F}, \circ)$ es grupo.

(b) Claramente $\mathcal{L} \subseteq \mathcal{F}$ y $\mathcal{L} \neq \emptyset$ pues $\text{id} \in \mathcal{L}$.

Siguiendo la indicación, sean $f_{a,b}, g_{c,d} \in \mathcal{L}$ definidas

por: $f_{a,b}(x) = ax + b$

$$g_{c,d}(x) = cx + d$$

(elementos genéricos de $\mathcal{L}$!)

Sabemos que la inversa de $g_{c,d}$ está dada por:

$$g_{c,d}^{-1}(x) = \frac{1}{c}x - \frac{d}{c}, \quad \forall x \in \mathbb{R}.$$

Y luego:

$$\begin{aligned} (f_{a,b} \circ g_{c,d}^{-1})(x) &= f(g_{c,d}^{-1}(x)) \\ &= f\left(\frac{1}{c}x - \frac{d}{c}\right) \\ &= a\left(\frac{1}{c}x - \frac{d}{c}\right) + b \\ &= \frac{a}{c}x + \left(b - \frac{ad}{c}\right), \quad \forall x \in \mathbb{R}. \end{aligned}$$

Y notando que: $\frac{a}{c}, \left(b - \frac{ad}{c}\right) \in \mathbb{R}$, tenemos que $\underbrace{f_{a,b} \circ g_{c,d}^{-1}}_{\in L} \in L$.

Es decir:

$$(\forall f_{a,b}, g_{c,d} \in L) \quad (f_{a,b} \circ g_{c,d}^{-1}) \in L.$$

$\Leftrightarrow (L, \circ)$ es subgrupo de $(\mathbb{T}, \circ)$.

P2

(a) ($\Rightarrow$) Debemos mostrar que $(G, *)$ es grupo y que $*$ conmuta en G .

Por enunciado se tiene que $(G, *)$ es grupo.
Luego, basta probar que $*$ conmuta.

Sean $x_0, y_0 \in G$.

Nos gustaría que: $x_0 * y_0 = y_0 * x_0$ ($*$)

Como f es isomorfismo:

$$(\forall x, y \in G) \quad f(x * y) = f(x) * f(y)$$

En particular:

$$f(x_0^{-1} * y_0^{-1}) = f(x_0^{-1}) * f(y_0^{-1}) = (x_0^{-1})^{-1} * (y_0^{-1})^{-1} = x_0 * y_0$$

y por otra parte:

$$f(x_0^{-1} * y_0^{-1}) = (x_0^{-1} * y_0^{-1})^{-1} = (y_0^{-1})^{-1} * (x_0^{-1})^{-1} = y_0 * x_0.$$

Lo que prueba ($*$). Luego $*$ conmuta en G .

Luego $(G, *)$ es grupo abeliano.

($\Leftarrow$) Queremos probar que: (pues f es claramente biyectiva)

$$(\forall x, y \in G) \quad f(x * y) = f(x) * f(y)$$

$$\Leftrightarrow (\forall x, y \in G) \quad (x * y)^{-1} = x^{-1} * y^{-1}$$

$$\Leftrightarrow (\forall x, y \in G) \quad y^{-1} * x^{-1} = x^{-1} * y^{-1}$$

Y esto último se tiene pues suponemos $(G, *)$ grupo abeliano.

Luego, f es isomorfismo.

Con todo esto:

f es isomorfismo $\Leftrightarrow G$ es grupo abeliano.



(b) (i) $\oplus$ ASOCIA en $\mathbb{Z}_2 \times \mathbb{Z}_3$, pues $+_2$ y $+_3$ ASOCIAN en $\mathbb{Z}_2$ y $\mathbb{Z}_3$, respectivamente.

* El neutro en $(\mathbb{Z}_2 \times \mathbb{Z}_3)$ para $\oplus$ está dado por el neutro en $\mathbb{Z}_2$ para $+_2$ y el neutro en $\mathbb{Z}_3$ para $+_3$, es decir; el neutro buscado es:

$$([0]_2, [0]_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$$

* Que todo elemento de $\mathbb{Z}_2 \times \mathbb{Z}_3$ tiene inverso, se deduce de manera similar. Es fácil ver que, dado: $([x]_2, [y]_3)$ en $\mathbb{Z}_2 \times \mathbb{Z}_3$ su inverso será: $([-x]_2, [-y]_3)$, también en $\mathbb{Z}_2 \times \mathbb{Z}_3$.

$\therefore (\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$ es un grupo.



(iii) f debe cumplir:

$$f([1]_6) = ([1]_2, [1]_3) \quad (*)$$

y además: $\forall [x]_6, [y]_6 \in \mathbb{Z}_6$

$$f([x]_6 +_6 [y]_6) = f([x]_6) \oplus f([y]_6)$$

Luego:

$$\begin{aligned} f([2]_6) &= f([1]_6 +_6 [1]_6) = ([1]_2, [1]_3) \oplus ([1]_2, [1]_3) \\ &= ([0]_2, [2]_3) \quad (*) \end{aligned}$$

De la misma manera:

$$\begin{aligned} f([3]_6) &= f([2]_6 +_6 [1]_6) = ([0]_2, [2]_3) \oplus ([1]_2, [1]_3) \\ &= ([1]_2, [0]_3) \quad (*) \end{aligned}$$

$$\begin{aligned} \Rightarrow f([4]_6) &= f([2]_6 +_6 [2]_6) = ([0]_2, [2]_3) \oplus ([0]_2, [2]_3) \\ &= ([0]_2, [1]_3) \quad (*) \end{aligned}$$

$$\begin{aligned} \Rightarrow f([5]_6) &= f([4]_6 +_6 [1]_6) = ([0]_2, [1]_3) \oplus ([1]_2, [1]_3) \\ &= ([1]_2, [2]_3) \quad (*) \end{aligned}$$

$$\begin{aligned} \Rightarrow f([0]_6) &= f([3]_6 +_6 [3]_6) = ([1]_2, [0]_3) \oplus ([1]_2, [0]_3) \\ &= ([0]_2, [0]_3) \quad (*) \end{aligned}$$

Luego, $(*_1), (*_2), (*_3), (*_4), (*_5)$ y $(*_6)$ definen la función f que buscamos.

(No es difícil probar que f es biyectiva y que además es morfismo...)

(iii) Razonando por contradicción, supongamos que no es único. Es decir, supongamos que existe g , isomorfismo de $(\mathbb{Z}_6, +_6)$ en $(\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$, tal que $g \neq f$.

Como g es isomorfismo, en particular es morfismo.

Si g es morfismo, a lo menos, g debe cumplir $(*_1), (*_2), (*_3), (*_4), (*_5)$ y $(*_6)$ (reemplazando f por g).

Pero estas 6 igualdades definen completamente g !

Luego: $g = f$ 

Con lo que se prueba que el isomorfismo de (ii) es único.

P3

(a) Sean $x_1, x_2 \in H * K$.

$$\Rightarrow \exists h_1, h_2 \in H, \exists k_1, k_2 \in K; x_1 = h_1 * k_1 \wedge x_2 = h_2 * k_2$$

$$\Rightarrow x_2^{-1} = (h_2 * k_2)^{-1} = k_2^{-1} * h_2^{-1}$$

$$\Rightarrow x_1 * x_2^{-1} = h_1 * k_1 * k_2^{-1} * h_2^{-1}$$

Sabemos que $k_1 * k_2^{-1} \in K$, pues $(K, *)$ es grupo.

Llamando: $k_1 * k_2^{-1} = k_3 \in K$, tenemos:

$$x_1 * x_2^{-1} = h_1 * k_3 * h_2^{-1}$$

Y como $(G, *)$ es grupo abeliano, conmutando:

$$x_1 * x_2^{-1} = h_1 * h_2^{-1} * k_3$$

Luego, llamamos: $h_3 = h_1 * h_2^{-1} \in H$ ($\in H$ pues $(H, *)$ es grupo).

Así $x_1 * x_2^{-1} = h_3 * k_3$, donde: $h_3 \in H$, $k_3 \in K$.

$$\Rightarrow x_1 * x_2^{-1} \in H * K$$

Es decir, hemos probado que:

$$(\forall x_1, x_2 \in H * K) x_1 * x_2^{-1} \in H * K$$

Finalmente, como $H * K$ es claramente subconjunto de G ,

se concluye que: $(H * K, *)$ es subgrupo de $(G, *)$.

(b) Obedientemente, razonemos por contradicción.

Supongamos que $\exists a \in G \setminus \{e\} ; a^3 = e$

$$\Rightarrow a * a * a = e$$

$$\Rightarrow (a * a) * a = a * (a * a) = e$$

$\Rightarrow a^2, a$ son inversos para $*$!

Así, $(\{e, a, a^2\}, *)$ es un subgrupo de G .

Y además: $|\{e, a, a^2\}| = 3$

Es decir, G , de orden 4, tiene un subgrupo de orden 3.



Pero esto contradice el teorema de Lagrange pues 3 no divide a 4. Luego, nuestro supuesto debe ser falso. Es decir:

$$\nexists a \in G \setminus \{e\} ; a^3 = e$$

$$\Leftrightarrow \forall a \in G \setminus \{e\} ; a^3 \neq e.$$

Que es lo que se quería demostrar.

