13. Semana 12

P2 **(a)** Si $(A, \circ)$ es grupo debemos demostrar asociatividad, existencia de neutro e inverso.

- Asociatividad: Esto ya se tiene porque la composición de funciones es asociativa.
- Neutro: Es claro que el neutro es la identidad, fijarse que $F \circ id_G = id_g \circ F = F$, falta ver que $id_G \in A$, es decir que sea isomorfismo, en efecto $id_G(x * y) = x * y = id_G(x) * id_G(y)$.
- Inverso: Dado un $F \in A$ es claro que el inverso es F^{-1} sabemos que existe porque es una función biyectiva, falta ver que sea morfismo. En efecto, sea $z = F(x)$ y $w = F(y)$, se tiene que $F^{-1}(z) = x$ y $F^{-1}(w) = y$, luego

$$\begin{aligned} F^{-1}(z * w) &= F^{-1}(F(x) * F(y)) \\ &= F^{-1}(F(x * y)) \qquad \backslash\text{ya que } F \text{ es isomorfismo} \\ &= x * y \\ &= F^{-1}(z) * F^{-1}(w) \end{aligned}$$

Se concluye que, dado un F, el inverso es F^{-1} (la inversa de la función).

Con esto se tiene que $(A, \circ)$ es grupo.

(b) b.1 Demostraremos que F_g es homomorfismo de $(G, *)$ en $(G, *)$, en efecto, sean $x, y, g \in G$

$$\begin{aligned} F_g(x * y) &= g * (x * y) * g^{-1} \\ &= g * (x * e * y) * g^{-1} \qquad \backslash\text{operar con el neutro que no altera la ecuación} \\ &= g * (x * (g^{-1} * g) * y) * g^{-1} \\ &= (g * x * g^{-1}) * (g * y * g^{-1}) \qquad \backslash\text{por asociatividad} \\ &= F_g(x) * F_g(y) \end{aligned}$$

Se concluye que F_g es homomorfismo de $(G, *)$ en $(G, *)$.

b.2 Sean $x, g, h \in G$

$$\begin{aligned} F_{g*h}(x) &= (g * h) * x * (g * h)^{-1} \\ &= (g * h) * x * (h^{-1} * g^{-1}) \qquad \backslash\text{propiedad de los inversos} \\ &= g * (h * x * h^{-1}) * g^{-1} \qquad \backslash\text{por asociatividad} \\ &= g * F_h(x) * g^{-1} \\ &= F_g(F_h(x)) \\ &= F_g \circ F_h(x) \end{aligned}$$

Se concluye que $F_{g*h} = F_g \circ F_h$.

b.3 Recordemos que el inverso de e es él mismo, luego se tiene que $F_e(x) = e * x * e^{-1} = x * e^{-1} = x * e = x$.

Para concluir que F_g es isomorfismo, falta ver que sea biyectiva.

- Inyectiva: $(\forall x_1, x_2 \in G)(F_g(x_1) = F_g(x_2) \Rightarrow x_1 = x_2)$, en efecto

$$\begin{aligned} F_g(x_1) &= F_g(x_2) \\ g * x_1 * g^{-1} &= g * x_2 * g^{-1} \backslash \text{operando con inversa de } g \text{ por la izquierda } g^{-1}* \\ (g^{-1} * g) * x_1 * g^{-1} &= (g^{-1} * g) * x_2 * g^{-1} \qquad \backslash \text{por asociatividad} \\ id_G * x_1 * g^{-1} &= id_G * x_2 * g^{-1} \\ x_1 * g^{-1} &= x_2 * g^{-1} \qquad \backslash \text{operando con } g \text{ por la derecha } g* \\ x_1 * (g^{-1} * g) &= x_2 * (g^{-1} * g) \qquad \backslash \text{por asociatividad} \\ x_1 * id_G &= x_2 * id_G \\ x_1 &= x_2 \end{aligned}$$

- Epiyectiva: $(\forall y \in G)(\exists x \in G)(F_g(x) = y)$, en efecto, basta tomar $x = g^{-1} * y * g$, con esto se tiene que

$$\begin{aligned} F_g(x) &= g * x * g^{-1} \\ &= g * (g^{-1} * y * g) * g^{-1} \\ &= (g * g^{-1}) * y * (g * g^{-1}) \qquad \backslash \text{por asociatividad} \\ &= id_G * y * id_G \\ &= y \end{aligned}$$

Se concluye que F_g es un isomorfismo, además usando las propiedad (b.2) y (b.3) se tiene que $F_g \circ F_{g^{-1}} = F_{g^{-1}} \circ F_g = F_{g*g^{-1}} = F_{g^{-1}*g} = F_e = id_G$, con esto se concluye que el inverso de F_g llamado $(F_g)^{-1}$ es $F_{g^{-1}}$.

(c) Basta ocupar la propiedad compacta, es decir demostrar que $(\forall F_g, F_h \in B)\ F_g \circ (F_h)^{-1} \in B$, en efecto, sean $F_g, F_h \in B$, utilizando la parte (b) se tiene que $F_g \circ (F_h)^{-1} = F_g \circ F_{h^{-1}} = F_{g*h^{-1}}$, claramente $g*h^{-1} \in G$ por ser grupo y obedecer la ley de composición interna, luego $F_{g*h^{-1}} \in B$, se concluye que $(B, \circ)$ es subgrupo de $(A, \circ)$.

P1 (a)

$\oplus$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\odot$	a	b	c	d
a	a	a	a	a
b	a	a	a	a
c	a	b	c	d
d	a	b	c	d

1.1) Recordemos que $(A, \oplus)$ es grupo abeliano, con esto tenemos $a \oplus b = b \oplus a = b$ y $a \oplus d = d \oplus a = d$, tenemos que a es neutro, ya que ni b ni d pueden serlo ($a \oplus b \neq a$ y $a \oplus d \neq a$), c tampoco puede serlo ya que $c \oplus c \neq c$, por lo tanto, $a \oplus c = c \oplus a = c$, notemos que los inversos de b y c son ellos mismos, ahora veamos que $c \oplus b = b \oplus c = d$, $b \oplus d = d \oplus b = c$ y $d \oplus c = c \oplus d = b$.

Supongamos que $c \oplus b = b \oplus c \neq d$, esto entonces nos lleva a tres casos posibles:

- $c \oplus b = b \oplus c = a \Rightarrow$ el inverso de c es b, lo cual es una contradicción porque el inverso es único.
- $c \oplus b = b \oplus c = c \Rightarrow b$ es elemento neutro, lo cual es imposible porque el neutro es único.
- $c \oplus b = b \oplus c = b \Rightarrow c$ es elemento neutro, lo cual es imposible porque el neutro es único.

Se concluye que $c \oplus b = b \oplus c = d$.

Supongamos que $b \oplus d = d \oplus b \neq c$, esto entonces nos lleva a tres casos posibles:

- $b \oplus d = d \oplus b = a \Rightarrow$ el inverso de b es d, lo cual es una contradicción porque el inverso es único.
- $b \oplus d = d \oplus b = d \Rightarrow b$ es elemento neutro, lo cual es imposible porque el neutro es único.
- $b \oplus d = d \oplus b = b \Rightarrow d$ es elemento neutro, lo cual es imposible porque el neutro es único.

Se concluye que $b \oplus d = d \oplus b = c$.

Supongamos que $d \oplus c = c \oplus d \neq b$, esto entonces nos lleva a tres casos posibles:

- $d \oplus c = c \oplus d = a \Rightarrow$ el inverso de c es d, lo cual es una contradicción porque el inverso es único.
- $d \oplus c = c \oplus d = d \Rightarrow c$ es elemento neutro, lo cual es imposible porque el neutro es único.
- $d \oplus c = c \oplus d = c \Rightarrow d$ es elemento neutro, lo cual es imposible porque el neutro es único.

Se concluye que $d \oplus c = c \oplus d = b$.

Finalmente como d tiene que poseer inverso y no pueden ser ni a, b o c ya que el inverso es único, solamente queda que d sea inverso de sí mismo, es decir $d \oplus d = a$.

Para la otra tabla usaremos la propiedad distributiva es así como tenemos lo siguiente:

- $b \odot c = (c \oplus d) \odot c = (c \odot c) \oplus (d \odot c) = c \oplus c = a$
- $b \odot b = b \odot (d \oplus c) = (b \odot d) \oplus (b \odot c) = a \oplus a = a$
- $c \odot b = (b \oplus d) \odot b = (b \odot b) \oplus (d \odot b) = a \oplus b = b$
- $c \odot d = c \odot (b \oplus c) = (c \odot b) \oplus (c \odot c) = b \oplus c = d$
- $d \odot d = d \odot (b \oplus c) = (d \odot b) \oplus (d \odot c) = b \oplus c = d$

1.2) No es conmutativo, basta ver que $b \odot c \neq c \odot b$, tampoco tiene neutro, ya que de existir debería cumplir que $x \odot e = x \ \forall x \in \{a, b, c, d\}$, ilustrativamente debería haber una tabla del estilo

$\odot$	a	b	c	d
a			a	
b			b	
c	a	b	c	d
d			d	

es decir que se repitan los elementos en la fila y columna i-ésima, siendo el elemento i-ésimo el elemento neutro (en el ejemplo es c), como esto no ocurre, el anillo no posee neutro para $\odot$. Finalmente sí posee divisores de cero ya que el neutro para $\oplus$ es a y $b \odot c = b \odot b = b \odot d = a$, con $b, c, d \neq a$.

(b) c.1) Sea $x \in A$

$$\begin{aligned} x &= x \cdot x && \text{\hipótesis} \\ &= (-x) \cdot (-x) && \text{\propiedad de los anillos} \\ &= (-x) \cdot [(-x) \cdot (-x)] && \text{\hipótesis} \\ &= (-x) \cdot (x \cdot x) && \text{\propiedad de los anillos} \\ &= (-x) \cdot x && \text{\hipótesis} \\ &= -(x \cdot x) && \text{\propiedad de los anillos} \\ &= -(x) && \text{\hipótesis} \\ &= -x \end{aligned}$$

c.2) Sean $x, y \in A$

$$\begin{aligned} (x+y) &= (x+y) \cdot (x+y) && \text{\hipótesis} \\ (x+y) &= (x+y) \cdot x + (x+y) \cdot y && \text{\distributividad} \\ (x+y) &= x \cdot x + y \cdot x + x \cdot y + y \cdot y \\ (x+y) &= x + y \cdot x + x \cdot y + y && \text{\hipótesis} \\ (x+y) &= (x+y) + y \cdot x + x \cdot y && \text{\sumando con } -(x+y) \\ (x+y) - (x+y) &= (x+y) - (x+y) + y \cdot x + x \cdot y \\ 0 &= y \cdot x + x \cdot y && \text{\sumando con } -(x \cdot y) \\ 0 - (x \cdot y) &= y \cdot x + x \cdot y - (x \cdot y) \\ -(x \cdot y) &= y \cdot x \\ x \cdot y &= y \cdot x && \text{\propiedad c.1} \end{aligned}$$

c.3) Sean $x, y \in A$

$$\begin{aligned} (x \cdot y) \cdot (x+y) &= (x \cdot y) \cdot x + (x \cdot y) \cdot y && \text{\distributividad} \\ &= (x \cdot x) \cdot y + x \cdot (y \cdot y) && \text{\conmutatividad y asociatividad de } \cdot \\ &= x \cdot y + x \cdot y && \text{\hipótesis} \\ &= x \cdot y - (x \cdot y) && \text{\propiedad c.1} \\ &= 0 \end{aligned}$$