Pauta Aux 12

P1 a) $[0]$ no es invertible

$\Rightarrow (\mathbb{Z}_5, \cdot_5)$ no es grupo.

b) $(\mathbb{Z}_5 \setminus \{[0]\}, \cdot_5)$ es grupo abeliano.

$\rightarrow$ asocia, conmuta, todos son invertibles, tiene neutro. (conmuta por abeliano).

asocia. Es bien sabido que $[a]_n \cdot [b]_n = [a \cdot b]_n$

$\rightarrow ([a]_5 \cdot_5 [b]_5) \cdot_5 [c]_5 = [a \cdot b]_5 \cdot_5 [c]_5$

$= [(a \cdot b) \cdot c]_5 = [a \cdot (b \cdot c)]_5 = [a]_5 \cdot_5 [b \cdot c]_5$

$= [a]_5 \cdot ([b]_5 \cdot_5 [c]_5)$

conmuta: $[a]_5 \cdot_5 [b]_5 = [a \cdot b]_5 = [b \cdot a]_5 = [b]_5 \cdot_5 [a]_5$

todos los elementos son invertibles:

sí, el de $[1]$ es $[1]$ el de $[2]$ es $[3]$ el de $[3]$ es $[2]$ el de $[4]$ es sí mismo.

tiene neutro: sí, es conocido, el $[1]$

c) Por Lagrange, solo pueden haber subgrupos de orden 1 o 2.
Como el neutro se hereda, sabemos que $\{[1], \cdot_5\}$ es un subgrupo y falta hallar los de orden 2.
Verificamos entonces que tengan al 1 y a sí mismo.

$2 \cdot 2 \equiv 4 \pmod 5$ $\quad 3 \cdot 3 \equiv 4 \pmod 5$ $\quad 4 \cdot 4 \equiv 1 \pmod 5$

Vemos que el único útil es 4. *
Se corrobora (uds. lo hacen) que $\{[1], [4], \cdot_5\}$ es subgrupo de $(\mathbb{Z}_5 \setminus \{[0]\}, \cdot_5)$.

* (por l.c.i.) si el 2 o el 3 estuvieran en el subgrupo, el 4 tb tendría que estar y el 1 igual, pero no hay grupos de orden 3. Esto está garantizado por teo de Lagrange.

P2

a) Basta verificar que:

i) $\odot$ asocia

ii) $\odot$ distribuye respecto a $\oplus$.

i) Sean $(a,b),(c,d),(e,f) \in \mathbb{Z}^2$.

pdq $(a,b)\odot((c,d)\odot(e,f)) = ((a,b)\odot(c,d))\odot(e,f)$

En efecto:

$$(a,b)\odot((c,d)\odot(e,f)) \overset{def}{=} (a,b)\odot(ce,0) \overset{def}{=} (ace,0)$$

$$\overset{def}{=} (ac,0)\odot(e,f) \overset{def}{=} ((a,b)\odot(c,d))\odot(e,f).$$

ii) Sean $(a,b),(c,d),(e,f) \in \mathbb{Z}^2$,

pdq: $(a,b)\odot((c,d)\oplus(e,f)) = [(a,b)\odot(c,d)]\oplus[(a,b)\odot(e,f)]$

Veamos:

$$(a,b)\odot(c+e,d+f) \overset{def}{=} (a(c+e),0)$$

$$= (ac+ae,0) = (ac,0)+(ae,0)$$

$$\overset{def}{=} ((a,b)\odot(c,d))\oplus((a,b)\odot(e,f))$$

$\therefore (\mathbb{Z}^2,\oplus,\odot)$ es anillo. !!

b) ¡la unidad es el neutro para la SEGUNDA operación!

$\Rightarrow (a,b) \odot (u_1, u_2) = (a,b)$

$\Leftrightarrow (au_1, 0) = (a,b)$.

Vemos que si $b \neq 0$ la igualdad no se tiene. Como el neutro debe ser uno para todos (uwu) el neutro no existe.

¿Divisores de cero? (el cero es el neutro de la 1ª op., es fácil ver que corresponde a $(0,0)$)

$(a,b) \odot (c,d) = (0,0)$ tq $(a,b),(c,d) \neq (0,0)$

$\Leftrightarrow (ac, 0) = (0,0)$

esto indica que basta que a o c sean cero, podemos tomar entonces $(0,3)$ y $(2,48)$ y es fácil verificar que al tratarlos con la segunda operación llegamos al cero. (mucho ojo, aquí no teníamos restricciones sobre b o d, así que fue fácil hallar los divs.)

P2 b) <u>Por propiedad</u>, como el anillo tiene divs. de cero NO es cuerpo.

<u>P3</u> a) Nos iremos por el camino siguiente:

→ $(\mathbb{R}, *)$ es grupo abeliano

→ $(\mathbb{R}\setminus\{0\}, \cdot)$ es grupo abeliano.

→ $\cdot$ dist respecto a $*$.

i) <u>Asocia</u>: sean $x, y, z \in \mathbb{R}$, pdq: $x * (y * z) = (x * y) * z$

Dem

$$x * \left(\sqrt[3]{y} + \sqrt[3]{z}\right)^3 = \left(\sqrt[3]{x} + \sqrt[3]{\left(\sqrt[3]{y} + \sqrt[3]{z}\right)^3}\right)^3$$

$$= \left(\sqrt[3]{x} + \left(\sqrt[3]{y} + \sqrt[3]{z}\right)\right)^3 = \left(\left(\sqrt[3]{x} + \sqrt[3]{y}\right) + \sqrt[3]{z}\right)^3$$

$$= \left(\sqrt[3]{x} + \sqrt[3]{y}\right)^3 * z = (x * y) * z. \quad //$$

<u>Conmutatividad</u>:

$$x * y = \left(\sqrt[3]{x} + \sqrt[3]{y}\right)^3 = \left(\sqrt[3]{y} + \sqrt[3]{x}\right)^3 = y * x.$$

el cero de $\star$ es:

$$x \star cero = \left(\sqrt[3]{x} + \sqrt[3]{cero}\right)^3 = x$$ ← recordar que es el neutro de la 1ª operación.

$$\Leftrightarrow \cancel{\sqrt[3]{x}} + \sqrt[3]{cero} = \cancel{\sqrt[3]{x}}$$

$$\Leftrightarrow \sqrt[3]{cero} = 0$$

$$\Rightarrow cero = 0.$$

O sea que el cero es el cero usual.

<u>Inverso</u>:

$$x \star i = 0 \Leftrightarrow \left(\sqrt[3]{x} + \sqrt[3]{i}\right)^3 = 0$$

$$\Leftrightarrow \sqrt[3]{x} + \sqrt[3]{i} = 0$$

$$\Leftrightarrow \sqrt[3]{x} = -\sqrt[3]{i}$$

$$\Leftrightarrow \sqrt[3]{x} = \sqrt[3]{-i}$$

$$\Leftrightarrow x = -i$$

$$\Leftrightarrow \boxed{i = -x}$$

Los inversos son los mismos elementos con signo cambiado sabemos que existen $\forall x \in \mathbb{R}$.

$\therefore$ $(\mathbb{R}, \star)$ es grupo abeliano.

ii) Es sabido que $(\mathbb{R}\setminus\{0\}, \cdot)$ es grupo abeliano, pues $(\mathbb{R}, +, \cdot)$ es cuerpo.

* ojo que con este cero me refiero al 0 usual. Esto podría no pasar siempre.

iii) Sean $x, y, z \in \mathbb{R}$.

pdq: $x \cdot (y * z) = (x \cdot y) * (x \cdot z)$.

Veamos:

$$x \cdot (y * z) = x \cdot \left(\sqrt[3]{y} + \sqrt[3]{z}\right)^3$$

buscamos como juntarlos.

$$= \left(\sqrt[3]{x}\right)^3 \cdot \left(\sqrt[3]{y} + \sqrt[3]{z}\right)^3$$

chum paentro.

$$= \left(\sqrt[3]{xy} + \sqrt[3]{xz}\right)^3$$

es lo mismo

$$= \left(\left(\sqrt[3]{xy}\right) + \left(\sqrt[3]{xz}\right)\right)^3$$

por def

$$= (xy) * (xz)$$

$\therefore (\mathbb{R}, \star, \cdot)$ es cuerpo.

$(\mathbb{R}, \star, \cdot) \to (\mathbb{R}, +, \cdot)$

b) $\underbrace{\text{morfismo}}_{i}$ y $\underbrace{\text{biyectivo}}_{ii}$.

i) $f(x \star y) = f(x) + f(y)$

$f(x \cdot y) = f(x) \cdot f(y)$

$f(1) = 1$

$\longrightarrow \sqrt[3]{\left(\sqrt[3]{x} + \sqrt[3]{y}\right)^3} = \sqrt[3]{x} + \sqrt[3]{y} = f(x) + f(y)$

$\longrightarrow \sqrt[3]{x \cdot y} = \sqrt[3]{x} \cdot \sqrt[3]{y} = f(x) \cdot f(y)$

$\longrightarrow \sqrt[3]{1} = 1$. ★ ojo con esto, no siempre es tan directo. Va a depender de sus operaciones (como aquí es la misma, tenemos el mismo 1)

<u>Biyección</u>: $f(x) = f(y) \Longleftrightarrow \sqrt[3]{x} = \sqrt[3]{y} \Rightarrow x = y$

$\forall y \, \exists x$ tq $f(x) = y \Longleftrightarrow \sqrt[3]{x} = y \Longleftrightarrow x = y^3$.

Como para todo real, él mismo al cubo existe (y es real), se corrobora la biyección

$\therefore f(x) = \sqrt[3]{x}$ es isomorfismo//

P4] Por la propiedad compacta, esto sale facilito !!

<u>Prop compacta:</u>

Sea G un grupo, $H \subseteq G$ cumple lo siguiente:

$$\forall x, y \in H \quad x * y^{-1} \in H$$

ssi $(H, *)$ es subgrupo de $(G, *)$.

Veamos que esto pasa:

pdq: $(H * K, *)$ es subgrupo de $(G, *)$

$$\Longleftrightarrow \forall x, y \in H * K : x * y^{-1} \in H * K$$

Si $x, y \in H * K$, entonces tienen la forma:

$x = h_1 * k_1$ con $h_1, h_2 \in H$ y $k_1, k_2 \in K$.

$y = h_2 * k_2$ (esto es mucho muy importante)

Luego
$$x * y^{-1} = (h_1 * k_1) * (h_2 * k_2)^{-1}$$
$$= (h_1 * k_1) * (k_2^{-1} * h_2^{-1})$$

Como $(G, *)$ es grupo, $*$ asocia, luego.

$= h_1 * (k_1 * k_2^{-1}) * h_2^{-1}$

Como es abeliano:

$$= (k_1 * k_2^{-1}) * (h_1 * h_2^{-1})$$

$$= \underbrace{(h_1 * h_2^{-1})}_{\in H} * \underbrace{(k_1 * k_2^{-1})}_{\in K}$$

La razón de que ellos pertenezcan a H y K es que justamente H y K son subgrupos de G. Luego, por propiedad compacta, $h_1 * h_2^{-1} \in H$ y $k_1 * k_2^{-1} \in K$

Luego, como $x * y^{-1}$ se escribe como alguien que pertenece a H operado con alguien que pertenece a K, $x * y^{-1} \in H * K$.

Que es justo lo que queriamos probar.

$\therefore (H * K, *)$ es subgrupo de $(G, *)$.

b) Vean que $(\{e, a, a^{-1}\}, *)$ es subgrupo de G. Contradicción (porque 3 no divide a 4).

P5 a) $f(0_K) = f(0_K + 0_K) = f(0_K) \oplus f(0_K)$

Sumando a ambos lados $-f(0_K)$ (el inverso según $\oplus$ de $f(0_K)$), se tiene el resultado.

$0_A = f(0_K)$

b) <u>Truquito</u>: $f(0_K) = f(x - x)$ $\forall x \in K$.

$$\Rightarrow \underset{\substack{\parallel \\ 0_A}}{f(0_K)} = f(x + (-x)) = f(x) \oplus f(-x)$$

$$\Rightarrow -f(x) = f(-x)$$

c) $\forall x, y \in f(K)$, $x \oplus -y \in f(K)$

Usando las dos props anteriores:

$\exists k_1$ y $k_2 \in K$, tq $f(k_1) = x$, $f(k_2) = y$.

y $f(k_1 - k_2) = f(k_1) \oplus f(-k_2) = f(k_1) \oplus -f(k_2)$
$= x \oplus -y$

basta ver que:

$k_1 - k_2 \in K$, pero k_1 y $k_2 \in K$, luego,

luego, como $+$ es l.c.i.

k_1 y $-k_2 \in K$,

esto se tiene pq $(K, +)$ es grupo abeliano

$k_1 - k_2 \in K$.

$\therefore$ $(f(K), \oplus)$ es subgrupo de $(A, \oplus)$.

d) $\underline{\Leftarrow}$ directo

$\underline{\Rightarrow}$ Supongamos que hubiera un $x \neq 0_K$ tq $f(x) = 0_A$

$$f(x \cdot x^{-1}) = f(x) \odot f(x^{-1}) = 0_A \odot f(x^{-1}) = 0_A$$

$$\begin{array}{c} \| \\ f(1_K) = 1_A \end{array}$$

pero $0_A \neq 1_A$ ✗. Luego, no puede existir tal x. (x^{-1} existe porque $x \neq 0_K$ y $(K \setminus \{0_K\}, \cdot)$ es grupo abeliano por ser $(K, +, \cdot)$ cuerpo).

Luego, $f(x) = 0_A \Leftrightarrow \cancel{x} = 0_K$.

e) $f(x) = f(y) \Rightarrow f(x) - f(y) = 0_A$

$\Rightarrow f(x) \oplus f(-y) = 0_A \Rightarrow f(x-y) = 0_A$

$\Leftrightarrow x - y = 0_K \Rightarrow x = y$

Luego, f es monomorfismo ✓