Rodolfo Núñez | Auxiliar 11 | 12/6/2010

Intro al Álgebra (MA1101)

P1. (a) Las tablas corresponden a las operaciones en el anillo $(A, \oplus, \odot)$ para $A = \{a, b, c, d\}$ (con a, b, c, d distintos)

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

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

(i) Llene la tabla justificando cada relleno

HINT: Completar primero $\oplus$ y luego usar distributividad

¿Alguna vez han jugado sudoku? bueno, esto es lo mismo. Usaré la notación $x + y$ (x → fila de la tabla, y → columna de la tabla)

- $b \oplus a = b$ ya que $\oplus$ conmuta y $a \oplus b = b$
- $d \oplus a = d$ por lo mismo
- notar que a es el neutro para la $\oplus$ ya que $(A, \oplus)$ es un grupo conmutativo $\therefore$ debe tener neutro para $\oplus$. Esto no puede ser b ya que $a \oplus b = b \neq a$, no puede ser c, ya que $c \oplus c = a \neq c$ y no puede ser d ya que $a \oplus d = d \neq a$ $\therefore$ solo a puede ser el neutro
- Como a es neutro $\Rightarrow c \oplus a = c$ y $a \oplus c = c$
- Como el inverso de c/elemento existe y es único, a, b, c son sus propios inversos $\therefore d$ lo es también, de lo contrario $d = x^{-1}$ / $x \in \{a, b, c\}$ pero $x = x^{-1} \Rightarrow x = d$ $\Rightarrow\Leftarrow$

$\therefore d \oplus d = a$

•) $b \oplus c = c \oplus b$ (conmut.) debe ser d ya que si no fuera:

si $b \oplus c = b \Rightarrow b \oplus c \oplus b^{-1} = b \oplus b^{-1} \underset{\uparrow \text{conmut.}}{\Rightarrow} c = a$ $\#$

si $b \oplus c = c \Rightarrow b \oplus c \oplus c^{-1} = c \oplus c^{-1} \Rightarrow b = a$ $\#$

si $b \oplus c = a \Rightarrow b = c^{-1} = c \Rightarrow b = c$ ya que el inv. es único $\#$

$\therefore b \oplus c = d$

•) De manera análoga, $d \oplus c = c \oplus d = b$
$d \oplus b = b \oplus d = c$

$\Rightarrow$

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

•) notar que el neutro aditivo es absorvente para $\odot$

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

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

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

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

•) $c \odot d = c \odot (c \oplus b) = (c \odot c) \oplus (c \odot b) = c \oplus b = d$

$\Rightarrow$

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

(ii) Analice si:

1) $(A, \oplus, \odot)$ es anillo conmutativo
2) $(A, \oplus, \odot)$ posee unidad
3) $(A, \oplus, \odot)$ tiene divisores de 0

1) Claramente, no es conmutativo, basta notar que $c \odot b = b \neq b \odot c = a$

2) No tiene unidad, ya que para esto deberíamos tener algún elemento t.q. $\begin{matrix} x \odot e = x \\ e \odot x = x \end{matrix} \quad \forall x \in \{a, b, c, d\}$

es decir, en la tabla debería haber una fila i-ésima con (a, b, c, d) con su columna i-ésima respectiva con (a, b, c, d)

i.e.
$$\begin{array}{r|cccc} & \hat{i} & & \hat{i} & \\ \odot & a & \cdots & & d \\ \hline 1 \to a & & & a & \\ & & & b & \\ i \to i & a & b & c & d \\ d & & & d & \end{array}$$

NOTA: en este dibujo $e = c$ pero se puede usar un i más general cuando tenemos más de 4 elementos.

3) Tiene divisores de 0 (en este caso $0 = a$) y estos son b (ya que $\underset{\neq a}{b} \odot \underset{\neq a}{b} = a$), c $(\underset{\neq a}{c} \odot \underset{\neq a}{b} = a)$ y d $(\underset{\neq a}{d} \odot \underset{\neq a}{b} = a)$

(b) Sea un anillo $(A, +, \cdot)$ t.q. $x \cdot x = x \quad \forall x \in A$

Dato Freak: Estos son los anillos booleanos. Tienen algunas aplicaciones en informática.

(i) P.D.Q. $x = -x \quad , \forall x \in A$

Sea $x \in A$ cualquiera

$$x \underset{\text{hip}}{=} x \cdot x \underset{\text{prop. vista}}{=} (-x)(-x) \underset{\text{hip.}}{=} (-x) \cdot ((-x) \cdot (-x)) \underset{\text{prop. vista}}{=} (-x) \cdot (x \cdot x) \underset{\text{hip}}{=} (-x) \cdot (x) \overset{\text{otra prop. vista}}{\underset{\text{otra prop. vista}}{=}} -(x \cdot x) \overset{\text{hip.}}{=} -x$$

q.e.d.

(ii) P.D.Q. $(A, +, \cdot)$ es anillo conmutativo

Ya sabemos que $(A, +, \cdot)$ es anillo, veamos que es conmutativo.

Sean $x, y \in A$ P.D.Q. $x \cdot y = y \cdot x$

Cuando no se les ocurra cómo proceder, estudien el caso primero. ¿Cómo sería si cumpliera lo que quieren?

$$x \cdot y = y \cdot x = -(y \cdot x) \quad (\text{por (i)}) \quad / + (y \cdot x)$$
$$\Rightarrow (x \cdot y) + (y \cdot x) = 0$$

$\therefore$ si logramos demostrar que $(x \cdot y) + (y \cdot x) = 0$ estaremos listos (esto solo porque trabajé solamente con equivalencias, si hubiera usado implicancias simples estaría mal, ya que no podemos partir de la hipótesis)

NOTA: Ustedes pueden demostrar cosas partiendo de la conclusión y llegando a la hipótesis solo si usan solamente equivalencias (y su uso es correcto). Sin embargo, se arriesgan a que los corrijan mal si no destacan que usaron SOLO equivalencias (basta una sola implicancia simple para cortarles el camino)

Tomemos $(x+y)\cdot(x+y) = (x+y)$ (por ser anillo booleano)

pero además,

$$(x+y)\cdot(x+y) = (x\cdot x) + (x\cdot y) + (y\cdot x) + (y\cdot y)$$
$$= (x+y) + (x\cdot y) + (y\cdot x) \quad \text{(anillo booleano)}$$

$$\Rightarrow (x+y)\cdot(x+y) = (x+y) = (x+y) + [(x\cdot y) + (y\cdot x)] \;/ -(x+y)$$

$$\Rightarrow 0 = (x\cdot y) + (y\cdot x) \quad \text{que es lo que queríamos}$$

$$\Leftrightarrow (x\cdot y) = (y\cdot x) \quad \text{q.e.d.}$$

(iii) PDQ. $(x\cdot y)\cdot(x+y) = 0 \quad \forall x, y \in A$

Sean $x, y \in A$

$$(x\cdot y)(x+y) = (x\cdot y)\cdot x + (x\cdot y)\cdot y \overset{\text{anillo conmut. (parte (ii))}}{=} \underbrace{(x\cdot x)}_{x}\cdot y + x\cdot\underbrace{(y\cdot y)}_{y}$$

$$\overset{\text{anillo booleano}}{=} x\cdot y + x\cdot y \overset{\text{parte (i)}}{=} x\cdot y - x\cdot y = 0 \quad \text{q.e.d.}$$

P2.) En $\mathbb{R}^2$ consideremos las operaciones

$$(a,b)\oplus(c,d) = (a+c, b+d)$$
$$(a,b)\odot(c,d) = (a\cdot c, b\cdot d)$$

(a) P.D.Q. $(\mathbb{R}^2, \oplus, \odot)$ es anillo conmutativo con unidad

Primero veamos que $(\mathbb{R}^2, \oplus)$ es grupo abeliano

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

•) l.c.i $(a,b)\oplus(c,d) = (a+c, b+d) \in \mathbb{R}^2$ q.e.d.

porque $+$ es l.c.i en $\mathbb{R}$ ($a+c \in \mathbb{R}$, $b+d \in \mathbb{R}$)

•) asociativa $\underbrace{((a,b) \oplus (c,d))}$ $\oplus (e,f)$

$= (a+c, b+d) \oplus (e,f) = ((a+c)+e, (b+d)+f)$

$= (a+(c+e), b+(d+f)) = (a,b) \oplus (c+e, d+f)$

asociativ. de $(\mathbb{R},+)$ $= (a+b) \oplus ((c,d) \oplus (e,f))$ q.e.d.

•) Neutro Basta tomar $(0,0)$ NOTA: Si no se les ocurre, supongan que existe y vean cómo debe ser en caso de existir, y luego vean que efectivamente es el neutro ya que podrían llegar a un candidato a neutro que no está en el conjunto, como a mi se me ocurrió, solo haré la 2da parte)

$(0,0) \oplus (a,b) = (0+a, 0+b) = (a,b)$

$(a,b) \oplus (0,0) = (a,b)$ (análogo) q.e.d.

•) Conmutatividad

$(a,b) \oplus (c,d) = (a+c, b+d) \overset{\text{conmut. de } (\mathbb{R},+)}{=} (c+a, d+b) = (c,d) \oplus (a,b)$

•) Inverso Veamos que $(-a,-b) = (a,b)^{-1}$

$(-a,-b) \oplus (a,b) = (-a+a, -b+b) = (0,0)$

y como $(\mathbb{R}^2, \oplus)$ es conmutativa, $(a,b) \oplus (-a,-b) = 0$

$\Longrightarrow (-a,-b) = (a,b)^{-1}$ q.e.d.

NOTA: a veces puede ser útil demostrar conmut. antes de neutro e inverso para escribir menos y hacer un solo caso. En este caso era simple de todos maneras

$\Longrightarrow (\mathbb{R}^2, \oplus)$ es grupo abeliano

Vamos ahora que en $(\mathbb{R}^2, \oplus, \odot)$, $\odot$ distribuye s/r a $\oplus$, y asocia, tiene neutro para $\odot$ y conmuta.

•) Conmutatividad

$$(a,b)\odot(c,d) = (a\cdot c,\ b\cdot d) \overset{\text{conmut. de } (\mathbb{R},\cdot)}{=} (c\cdot a,\ d\cdot b) = (c,d)\odot(a,b)$$

q.e.d.

•) Neutro. El neutro es $(1,1)$, verifiquémoslo

$$(a,b)\odot(1,1) = (a\cdot 1,\ b\cdot 1) \overset{1 \text{ neutro en } (\mathbb{R},\cdot)}{=} (a,b)$$ y como además conmuta,

$(1,1)\odot(a,b) = (a,b) \Longrightarrow (1,1)$ es neutro

q.e.d.

•) Distributividad $\big((a,b)\oplus(c,d)\big)\odot(e,f)$

$= (a+c,\ b+d)\odot(e,f) = \big((a+c)\cdot e,\ (b+d)\cdot f\big)$

$= (a\cdot e + c\cdot e,\ b\cdot f + d\cdot f) = (ae,\ bf)\oplus(ce,\ df)$

$= \big((a,b)\odot(e,f)\big)\oplus\big((c,d)\odot(e,f)\big)$ y como $\odot$ conmuta, se tiene hacia el otro lado

$\Longrightarrow (\mathbb{R}^2, \odot)$ conmuta $\Longrightarrow (\mathbb{R}^2, \oplus, \odot)$ es Anillo conmutativo con unidad.

q.e.d.

(b) P.D.Q. $(\mathbb{R}^2, \oplus, \odot)$ posee divisores de 0

NOTA: al igual que antes, siempre que no se les ocurra la respuesta, estudien el caso para obtener candidatos

En efecto, sí tiene divisores de 0, basta tomar

$$\underset{\neq (0,0)}{(1,0)}\odot\underset{\neq (0,0)}{(0,1)} = (0,0)$$ (de hecho, sirve cualquier $(a,0)\odot(0,b)$ / $a,b\in\mathbb{R}\setminus\{0\}$) q.e.d.

(c) P.D.Q. $(\mathbb{R}^2, \oplus, \odot) \ncong (\mathbb{C}, +, \cdot)$

NOTA: Recuerden usar las partes anteriores

supongamos que $(\mathbb{R}^2, \oplus, \odot) \cong (\mathbb{C}, +, \cdot)$

Por (b), sabemos que $(\mathbb{R}^2, \oplus, \odot)$ tiene divisores de 0

$\therefore (\mathbb{C}, +, \cdot)$ también tendrá divisores de 0, pero de ser así, $\exists\, a, b, c, d \in \mathbb{R} \,/\, (a \neq 0 \vee b \neq 0) \wedge (c \neq 0 \vee d \neq 0)$ t.q.

$(a + ib)\cdot(c + id) = a\cdot c - b d + i(ac + bd) = 0$

i.e. $a\cdot c = b d \wedge ac = -bd$ $\Rightarrow\Leftarrow$

al final está el detalle de que $(\mathbb{R}^2, \oplus, \odot)$ tiene div. de cero y $(\mathbb{R}^2, \oplus, \odot) \cong (\mathbb{C}, +, \cdot) \Rightarrow \left\{\begin{matrix}(\mathbb{C},+,\cdot) \text{ tiene} \\ \text{div. de cero}\end{matrix}\right)$

$\therefore$ Como $(\mathbb{C}, +, \cdot)$ no puede tener divisores de 0

$\Longrightarrow (\mathbb{R}^2, \oplus, \odot) \ncong (\mathbb{C}, +, \cdot)$ q.e.d.

P3. Sea $z \in \mathbb{C} \,/\, |z| = |z+1| = 1$

P.D.Q. z es raíz cúbica de la unidad
(i.e. $z^3 = 1$) NOTA: Recordar que $\overline{(a+ib)} = (a - ib)$

De $|z| = 1$ deducimos (tomando $z = a + ib \,/\, a, b \in \mathbb{R}$)

$\Rightarrow |z|^2 = 1^2 \Rightarrow (a + ib)(a - ib) = 1 \Rightarrow a^2 + b^2 = 1$

De $|z+1| = 1 \Rightarrow |z+1|^2 = 1^2$

$\Rightarrow (a + ib + 1)(a - ib + 1) = [(a+1) + ib]\cdot[(a+1) - ib]$

$= (a+1)^2 + b^2 = 1 \Rightarrow a^2 + b^2 + 2a + 1 = 1$

$\Rightarrow a^2 + b^2 = -2a$

juntando ambas partes $\Rightarrow |z+1| = |z| = 1$

$\Rightarrow a^2 + b^2 = -2a = 1 \Rightarrow \boxed{a = \frac{-1}{2}}$

Reemplazando a en $a^2 + b^2 = 1$

$\Rightarrow \frac{1}{4} + b^2 = 1 \Rightarrow \boxed{b = \pm\frac{\sqrt{3}}{2}}$

Ahora calculemos z^3 (sin módulo)

$z^3 = (a+ib)^3 = (a^2 + 2abi - b^2)(a+ib)$

$= a^3 + 2a^2bi - ab^2 + a^2bi - 2ab^2 - b^3i$

$= a^3 + 3a^2bi - 3ab^2 - b^3i \xrightarrow{\text{con } b = \frac{\sqrt{3}}{2}} = \frac{-1}{8} + 3\underbrace{\left(\frac{-1}{2}\right)^2}_{\frac{1}{4}} \cdot \frac{\sqrt{3}}{2}i - 3\left(\frac{-1}{2}\right) \cdot \frac{3}{4} - \frac{3\sqrt{3}i}{8}$

$= \frac{-1}{8} + \frac{3 \cdot 3}{8} = \frac{8}{8} = 1 \Rightarrow z^3 = 1$ suma $= 0$

(El procedimiento con $b = -\frac{\sqrt{3}}{2}$ es análogo, basta analizar los signos)

q.e.d.

(b) Sean $z_1, z_2 \in \mathbb{C}$

P.D.Q. $|1 - z_2\overline{z_1}|^2 - |z_1 - z_2|^2 = (1 - |z_1|^2)(1 - |z_2|^2)$

$|1 - z_2\overline{z_1}|^2 - |z_1 - z_2|^2 = (1 - z_2\overline{z_1})\overline{(1 - z_2\overline{z_1})} - (z_1 - z_2)\overline{(z_1 - z_2)}$

prop. vista

$= (1 - z_2\overline{z_1})(1 - \overline{z_2}z_1) - (z_1 - z_2)(\overline{z_1} - \overline{z_2})$

Recuerda: $\overline{\overline{z}} = z$

$$= 1 - \cancel{z_2\bar{z}_1} - \cancel{\bar{z}_2 z_1} + z_2\bar{z}_1\bar{z}_2 z_1 - z_1\bar{z}_1 + \cancel{z_1\bar{z}_2} + \cancel{z_2\bar{z}_1} - z_2\bar{z}_2$$

$$= 1 + z_2\bar{z}_1\bar{z}_2 z_1 - z_1\bar{z}_1 - z_2\bar{z}_2$$

$$= (1 - z_1\bar{z}_1)(1 - z_2\bar{z}_2) = (1 - |z_1|)(1 - |z_2|)$$ q.e.d.

(c) Usando lo anterior y si $|z_1| < 1$, $|z_2| < 1$

P.D.Q. $\dfrac{|z_1 - z_2|}{|1 - z_2\bar{z}_1|} < 1$

Por (b) sabemos que

$(1 - |z_1|^2)(1 - |z_2|^2) = |1 - z_2\bar{z}_1|^2 - |z_1 - z_2|^2$ lo que se parece mucho a lo que debemos usar, pero está con unos cuadrados "de más"

Como $|z_1| < 1 \Rightarrow |z_1|^2 < 1 \Rightarrow (1 - |z_1|^2) > 0$

$|z_2| < 1 \Rightarrow |z_2|^2 < 1 \Rightarrow (1 - |z_2|^2) > 0$

$\Rightarrow (1 - |z_2|^2)(1 - |z_1|^2) > 0$

$\Rightarrow |1 - z_2\bar{z}_1|^2 - |z_1 - z_2|^2 > 0 \Rightarrow |1 - z_2\bar{z}_1|^2 > |z_1 - z_2|^2$

$\therefore |1 - z_2\bar{z}_1| > |z_1 - z_2|$ NOTA: Estos valores serán positivos, no tendrán un "$\pm$" ya que son módulos

solo falta ver si podemos dividir por $|1 - z_2\bar{z}_1|$

(i.e. $|1 - z_2\bar{z}_1| \neq 0$) si fuera así $(\Leftrightarrow)$ $z_2\bar{z}_1 = 1 \Rightarrow |z_2||z_1| = 1$

Pero como $|z_2| < 1$ y $|z_1| < 1 \Rightarrow |z_2||z_1| < 1 \Rightarrow\Leftarrow$

$\therefore |1 - z_2\bar{z}_1| \neq 0 \Rightarrow \dfrac{|z_1 - z_2|}{|1 - z_2\bar{z}_1|} < 1$ q.e.d.

P4. sea $z \in \mathbb{C}$ / $|z| \neq 1$ y sea $n \in \mathbb{N}$ / $n \geq 1$

PDQ. $\dfrac{1}{1+z^n} + \dfrac{1}{1+\bar{z}^n} \in \mathbb{R}$

(si $w \in \mathbb{C} \wedge w = \bar{w} \iff w \in \mathbb{R}$) $\therefore$ demostraremos que

$$\overline{\left(\frac{1}{1+z^n} + \frac{1}{1+\bar{z}^n}\right)} = \left(\frac{1}{1+z^n} + \frac{1}{1+\bar{z}^n}\right)$$

Como $\overline{zw} = \bar{z} \cdot \bar{w} \Rightarrow \overline{z^2} = \overline{z \cdot z} = \bar{z} \cdot \bar{z} = \bar{z}^2$

y por inducción se tiene que $\overline{z^n} = \bar{z}^n$

además tenemos que $\overline{(z+w)} = \bar{z} + \bar{w}$

$$\therefore \overline{\left(\frac{1}{1+z^n} + \frac{1}{1+\bar{z}^n}\right)} = \overline{\frac{1}{1+z^n}} + \overline{\frac{1}{1+\bar{z}^n}} \overset{\text{prop. vista}}{=} \frac{\bar{1}}{\overline{1+z^n}} + \frac{\bar{1}}{\overline{1+\bar{z}^n}}$$

$$= \frac{1}{1+\overline{z^n}} + \frac{1}{1+\overline{\bar{z}^n}} = \frac{1}{1+\bar{z}^n} + \frac{1}{1+\bar{\bar{z}}^n} = \frac{1}{1+\bar{z}^n} + \frac{1}{1+z^n}$$

q.e.d.

P2 (c) anexo: Detalle con morfismo

$(\mathbb{R}^2, \oplus, \odot) \cong (\mathbb{C}, +, \cdot)$ (i.e. $\exists\, \varphi$ morfismo biyectivo entre $(\mathbb{R}^2, \oplus, \odot)$ y $(\mathbb{C}, +, \cdot)$)

y además,

$(\mathbb{R}^2, \oplus, \odot)$ tiene div. de cero, basta tomar $(0, a)$ y $(b, 0)$ con $a, b \in \mathbb{R} \setminus \{0\}$

sabemos que $(0, \overset{0}{\underset{}{\neq}}\!a) \odot (\overset{0}{\neq}\!b, 0) = (0, 0)$ y tenemos un morfismo... ocupémoslo (siempre ocupen todas las hipótesis)

$(0,a)\odot(b,0)=(0,0)$ $/\varphi(\cdot)$ $\longrightarrow$ ya que φ es biyect.

$\varphi\big((0,a)\odot(b,0)\big)=\varphi\big((0,0)\big)=0$ (en particular es sobreyec.) $\therefore$ φ (neutro para $\oplus$ en $\mathbb{R}^2$) $=$ neutro para $+$ en $\mathbb{C}$

visto en clases

$\underbrace{\Rightarrow}_{\text{morfismo}}\varphi\big((0,a)\big)\cdot\varphi\big((b,0)\big)=0$

pero como $\varphi\big((0,a)\big)\neq 0$ y $\varphi\big((b,0)\big)\neq 0$ (ojo, estos están en $\mathbb{C}$, no en $\mathbb{R}^2$)

tenemos divisores de cero ... ¿no me creen? pues supongan que alguno es 0, como φ es biyectiva, $\exists\,\varphi^{-1}$ y esta es biyectiva (en particular sobreyectiva).

así que si $\varphi\big((0,a)\big)=0$ (caso $\varphi\big((b,0)\big)=0$ es totalmente análogo)

$\Rightarrow \varphi\big((0,a)\big)=0$ $/\varphi^{-1}(\cdot)$

$\underbrace{\varphi^{-1}\circ\varphi\big((0,a)\big)}_{id_{\mathbb{C}}(0,a)=(0,0)}=\varphi^{-1}(0)=(0,0)$ $\longrightarrow$ ya que φ^{-1} es morf. sobreyect. $\therefore$ lleva al neutro para $(\mathbb{R}^2,\oplus)$ en $(\mathbb{C},+)$

$\Rightarrow (0,a)=(0,0) \Rightarrow a=0$ pero supusimos al comienzo $a\neq 0$ $\therefore$ $\Rightarrow\!\Leftarrow$

$\Rightarrow (\mathbb{C},+,\cdot)$ tendría divisores de cero si fueran isomorfos

q.e.d.

Mucho Exito

Dudas a:

RODO.NUNEZ.V@GMAIL.COM

Rodolfo Núñez