PROBLEMAS

(parcial 2)

3.1

① Estudiar si los siguientes conjuntos, con las operaciones usuales de suma y producto, tienen estructura de anillo. En caso afirmativo indicar si es conmutativo, con identidad, de división y si es cuerpo.

a) $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ siendo $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\} \neq \emptyset$

$\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ ¿subanillo de $\mathbb{R}$?

- $(a+b\sqrt{2})-(c+d\sqrt{2}) = (a-c)+(b-d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$
- $(a+b\sqrt{2})\cdot(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

→ Es anillo ✓

¿conmutativo? prod. de reales → sí

¿Identidad? $(1,0)$, tiene la identidad de $\mathbb{R}$, anillo padre, eso implica que tenga identidad.

¿Inverso? $\left(\frac{1}{a+b\sqrt{2}}\right) = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$

$\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}$ siempre que $a^2-2b^2 \neq 0$

$\Updownarrow$

$\frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2 \neq 2$

Es de división

Es cuerpo con grado de extensión 2 (no definido todavía)

dimensión de la base que necesitamos para extender un cuerpo desde $\mathbb{Q}$. $\mathbb{Q}$ es el más pequeño, la base, y todos los cuerpos serán una extensión de $\mathbb{Q}$ ($\mathbb{Q}$ es "subcuerpo")

(aquí empieza con apr. Alicia)

c) $(S,+,\cdot)$ siendo $S=\{a+b\sqrt{2}+c\sqrt{3} : a,b,c, \in \mathbb{Z}\}$

¿subanillo de $(\mathbb{R},+,\cdot)$?

1) $S \neq \emptyset$ $(1 \in S)$

2) $\forall x,y \in S$ ¿$x-y \in S$? $\quad x = a+b\sqrt{2}+c\sqrt{3}$, $y = d+e\sqrt{2}+h\sqrt{3}$

$\Rightarrow x-y = (a-d)+(b-e)\sqrt{2}+(c-h)\sqrt{3} \in S$

3) ¿$\forall x,y \in S$, $xy \in S$?

$xy = (ad+2be+3ch)+(ae+bd)\sqrt{2}+(dc+eh)\sqrt{3}+(bh+ce)\sqrt{6}$

$\notin S \Rightarrow$ S no es anillo

d) $(\mathbb{Z}[i],+,\cdot)$ siendo $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}] = \{a+bi : a,b \in \mathbb{Z}\}$

¿es subanillo de $(\mathbb{C},+,\cdot)$?

- $\mathbb{Z}[i] \neq \emptyset$
- $\forall x,y \in \mathbb{Z}[i]$ $\quad x = a+bi$, $y = c+di$

$x-y = (a-c)+(b-d)i$

$xy = (ac-bd)+(ad+bc)i \in \mathbb{Z}[i]$

- Es anillo conmutativo (tiene identidad, no es de división)

No es cuerpo $\rightarrow$ es D.I.

¡ Si existieran $x,y \in \mathbb{Z}[i]$ con $x \neq 0$, $y \neq 0$ y tq $xy = 0$!

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

e) $(\mathbb{Z}_p[i],+_p,\cdot_p)$ siendo $\mathbb{Z}_p[i] = \mathbb{Z}_p[\sqrt{-1}] = \{a+bi : a,b \in \mathbb{Z}_p\}$

Habría que comprobar:

- $(\mathbb{Z}_p[i],+_p)$ es grupo abeliano
- Propiedad asociativa del producto

$([a]_p \cdot_p [b]_p) \cdot_p [c]_p = [a]_p \cdot_p ([b]_p \cdot [c]_p)$

- Propiedad distributiva

$([a]_p +_p [b]_p) \cdot_p [c]_p = ([a]_p \cdot_p [c]_p) +_p ([b]_p \cdot_p [c]_p)$

- Propiedad conmutativa del producto

$[a]_p \cdot_p [b]_p = [b]_p \cdot_p [a]_p$

(por tanto, basta con esta → distributiva)

cont.

cont. → • $1_R = [1]_p$ tiene identidad ✓ ¿cuál?

• Si p es primo y $p \equiv 3 \bmod 4$ ⇒ sí es cuerpo ✓ pq sí será de división

• Si p no es primo o p es primo y $p \equiv 1 \bmod 4$ → no es de división

(*) para saber si es de división (si existe inverso para todo $a \in R$)

PQ SIMÉTRICAS?

② Encontrar todos los valores $k, m \in \mathbb{Z}$ para los cuales $(\mathbb{Z}, \oplus, \odot)$ es un anillo, siendo para todo $x, y \in \mathbb{Z}$, $x \oplus y = x + y - k$ y $x \odot y = x + y - mxy$. Para tales valores, estudias si el anillo correspondiente es conmutativo, tiene identidad, es de división y si es cuerpo.

① $(\mathbb{Z}, \oplus)$ grupo abeliano (→ $(\mathbb{Z}, \oplus, \odot)$ anillo) (→ NO, ESTO SOLO VALE PARA $(G, +)$ abelianos) y $(G, \cdot)$ CREO NO SE!

ⓐ $\oplus$ asociativa: $(x \oplus y) \oplus z = (x + y - k) \oplus z = x + y + z - 2k$

$x \oplus (y \oplus z) = x \oplus (y + z - k) = x + y + z - 2k$ ✓

ⓑ $\oplus$ conmutativa: $x \oplus y = x + y - k = y + x - k = y \oplus x$

ⓒ elem. ~~neutro~~ nulo: $0_R = k$ $\quad 0_R \oplus x = k \oplus x = x + k - k = x$

ⓓ opuesto de x: $x' \oplus x = k \iff x' + x - k = k \iff x' = 2k - x$

② $\odot$ Asociativa

$(x \odot y) \odot z = (x + y - mxy) \cdot z = x + y + z - mxy - m(x + y - mxy)z =$

$= x + y + z - mxy + m^2xyz - mxz - myz$

$x \odot (y \odot z) = \ldots = x + y + z - mxy + m^2xyz - mxz - myz$

③ Distributiva:

$(x \oplus y) \odot z = (x + y - k) \odot z = x + y - k + z - mz(x + y - k) =$

$= x + y - k + z - mxz - myz + mkz$

$(x \odot z) = x + z - mxz$

$(y \odot z) = y + z - myz$

$-(x \odot z) + (y \odot z) = x + z - mxz + y + z - myz - k$

(a) (b)

Será distributiva para: $z + mkz = 2z \iff mk = 1$

$m = 1, k = 0$ o $m = 0, k = 1$ entonces será anillo

(Falta ver si es conmut, ident, de división y cuerpo)

Jon ops. Alicia. Ops. Inés:

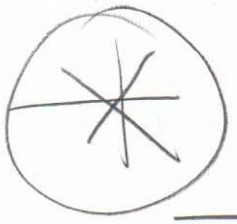
③ Se considera el conjunto $\mathbb{Q}$ con las operaciones de suma y producto definidas del siguiente modo: $\forall x,y \in \mathbb{Q}\ x \oplus y = x+y+7$, $x \odot y = x+y+\frac{xy}{7}$. Estudiar si $(\mathbb{Q}, \oplus, \odot)$ es un anillo y en caso afirmativo indicar si es un anillo conmutativo, si tiene identidad, si es de división y si es cuerpo.

$k=-7$, $m=-1/7$ $\Rightarrow km=1 \Rightarrow$ es un anillo ✓

$e=-7$ conmutativo
$1_R=0$ con identidad

$x+y+\frac{xy}{7}=0 \Leftrightarrow y=\frac{-x}{1+\frac{x}{7}}=\frac{-7x}{7+x}$

$x^{-1}=\frac{-7x}{7+x}$ $\quad x^{-1} \in R\ \forall x \in R-\{e\} \Rightarrow$ es un cuerpo



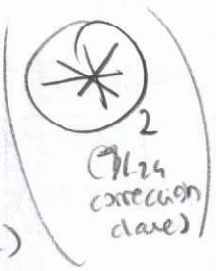
conexión clave ej ③

WATCH IT

④ a) Encontrar todos los subanillos de $\mathbb{Z}_{12}$, $\mathbb{Z}_{18}$, $\mathbb{Z}_{24}$

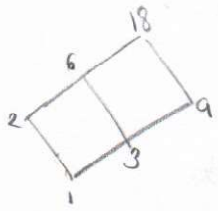
para $\mathbb{Z}_{18}$

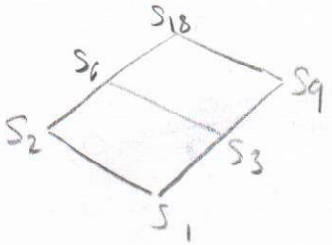
$S_1=\{0\}=(0)$
$S_2=\{0,9\}=(9)$
$S_3=\{0,6,12\}=(6)$
$S_6=\{0,3,6,9,12,15\}=(3)$
$S_9=\{0,2,4,6,8,10,12,14,16\}=(2)$
$S_{18}=\mathbb{Z}_{18}=(1)$



$S_r=(a)$ $p=ah_1$
$\forall p,q \in S_r$ $q=ah_2 \Rightarrow$
$\Rightarrow p \cdot q = a(ah_1h_2) \in (a) = S_r$

b) Construir un diagrama de Hasse del conjunto de subanillos de cada uno de los anillos indicados en el apartado anterior, donde el orden parcial está determinado por la inclusión de conjuntos.





⑤ Sea $S=\{(a,b,c) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z} : a=b+c\}$. Demostrar que S no es subanillo de $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$.

$(a+b,a,b)$, $(c+d,c,d)$ $\Rightarrow (a+b-c-d, a-c, b-d) \in S$

$a+b-c-d=(a-c)+(b-d)$ $\Rightarrow S \leq \mathbb{Z}^3$

2ª condición: $(a,b,c) - (a',b',c) \in S$ ✓

$S \neq \emptyset$! 1ª condición ✓

$((a+b)(c+d), ac, bd) = (ac+bd+ad+bc, ac, bd)$ $\quad ac+bd \neq ac+bd+ad+bc$

ejemplo $(2,1,1) \in S$

$(2,1,1)(3,1,1)=(4,1,1)$ $\quad 4 \neq 1+1$

3ª condición: $(a,b,c) \cdot (a',b',c') \in S$

X este ej. NO cumple la 3ª $\Rightarrow$ No es subanillo

⑥ Estudiar si los siguientes conjuntos son subanillos de $\mathbb{Z}^{2\times 2}$

a) $S = \left\{ \begin{pmatrix} x & x \\ y & y \end{pmatrix} : x, y \in \mathbb{Z} \right\}$

① $S \neq \emptyset$ (contiene la matriz 0)

② $\begin{pmatrix} x & x \\ y & y \end{pmatrix} - \begin{pmatrix} t & t \\ t & t \end{pmatrix} = \begin{pmatrix} x-t & x-t \\ y-t & y-t \end{pmatrix} \in S$

③ $\begin{pmatrix} x & x \\ y & y \end{pmatrix} \begin{pmatrix} z & z \\ t & t \end{pmatrix} = \begin{pmatrix} xz+xt & xz+xt \\ yz+yt & yz+yt \end{pmatrix} \in S$

Sí es subanillo ✓

→ ej ③

Para q sea anillo:

a) $(Q, \oplus)$ grupo abeliano:

1) $a \oplus (b \oplus c) = a \oplus (b+c+7) = a+b+c+14 = (a \oplus b) \oplus c =$
$(a+b+7) \oplus c = a+b+c+14$ ✓

2) $e \oplus a = a \iff e+a+7 = a \iff e = -7$ ✓

3) $a' \oplus a = e \iff a'+a+7 = -7 \iff a' = 14 - a$ ✓

4) $a \oplus b = a+b+7 = b+a+7 = b \oplus a$ ✓

Sí es abeliano

b) $(a \odot b) \odot c = \left(a+b+\frac{ab}{7}\right) \odot c = a+b+c+\frac{ab}{7}+\frac{ac}{7}+\frac{bc}{7}+\frac{abc}{49}$

$a \odot (b \odot c) = a \odot \left(b+c+\frac{bc}{7}\right) = a+b+c+\frac{bc}{7}+\frac{ab}{7}+\frac{ac}{7}+\frac{abc}{49}$ ✓

c) $a \odot b = a+b+\frac{ab}{7} = b+a+\frac{ba}{7} = b \odot a$

d) $a \odot (b \oplus c) = a \odot (b+c+7) = a+b+c+7+\frac{ab}{7}+\frac{ac}{7}+a$

$(a \odot b) \oplus (a \odot c) = \left(a+b+\frac{ab}{7}\right) \oplus \left(a+c+\frac{ac}{7}\right) = a+b+c+7+a+\frac{ab}{7}+\frac{ac}{7}$ ✓

Por tanto sí es anillo

¿Identidad? $I \odot a = a \iff I+a+\frac{Ia}{7} = a \iff I\left(1+\frac{a}{7}\right) = 0$

ó $\begin{cases} 1+\frac{a}{7} = 0 \iff \frac{a}{7} = -1 \iff a = -7 \Rightarrow a = e \\ \boxed{I = 0} \end{cases}$

el 0 es mi identidad

(cont.)

¿Es de división?

cont. $a' \cdot a = 1$

$a' + a + \frac{a'a}{7} = 0$

$a'(1 + \frac{a}{7}) = -a$

$a' = \frac{-a}{1+\frac{a}{7}} = \frac{-7a}{7+a} \Rightarrow \forall a \neq e = -7, \exists a' = \frac{-7e}{a+7} \in \mathbb{Q}$ tq

$a' \odot a = 1$

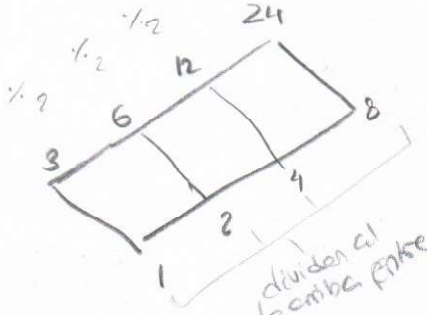
Sí es de división

(Sí es cuerpo)

(*)$_2$ $\mathbb{Z}_{24}$:

(a) ¿Subgrupos de $\mathbb{Z}_{24}$?

Ponemos sus divisores: $24 = 2^3 \cdot 3$



$\Rightarrow$

$H_0 = (1) = \mathbb{Z}_{24}$

$H_1 = (2) = \{2n : n \in \mathbb{Z}_{24}\}$

$H_2 = (3) = \{3n : n \in \mathbb{Z}_{24}\}$

$H_3 = (4) = \{4n : n \in \mathbb{Z}_{24}\}$

$H_4 = (6) = \{6n : n \in \mathbb{Z}_{24}\}$

$H_5 = (12) = \{0, 12\}$

$H_6 = (8) = \{0, 8, 16\}$

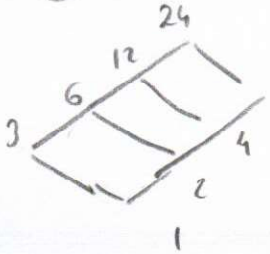
$H_7 = (0) = \{0\}$

Todos estos son subanillos, y para demostrarlo:

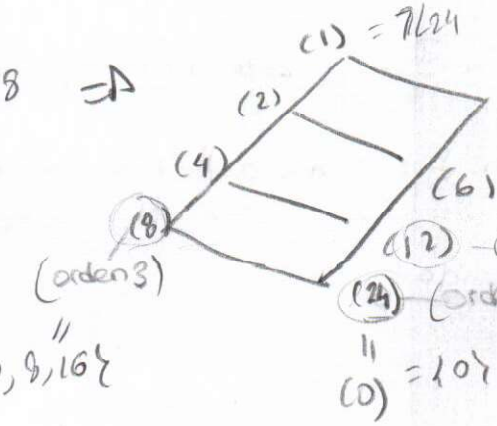
$H = (a) = \{a \cdot n : n \in \mathbb{Z}_{24}\}$

$\forall x, y \in H$ es $x = a \cdot r$, $y = a \cdot s \Rightarrow x \cdot y = a(ars) \in H$ ✓

(b)



$\Rightarrow$



$(x) = \langle x \rangle \Rightarrow x$ generador

⑦ Encontrar un $n \in \mathbb{N}$ tq en $\mathbb{Z}_n$ no ocurra:

a) $\forall a \in \mathbb{Z}_n$ tq $a^2 = a \Rightarrow a = 0$ ó $a = 1$

$a^2 = a \Rightarrow a^2 - a = 0 \Rightarrow a(a-1) = 0$

↑ en todos los anillos

↓ Esto no se verificará en los anillos en los que hay divisores de cero. Ej: $\mathbb{Z}_4$ ó $\mathbb{Z}_6$

en $\mathbb{Z}_6$: $a = 3$ es $a^2 = 9 \equiv 3 \bmod 6$

$a^2 = a$ en $\mathbb{Z}_6$, pero $a = 3 \notin \langle 0, 1 \rangle$ en $\mathbb{Z}_6$

b) $\forall a, b \in \mathbb{Z}_n$ tq $ab = 0 \Rightarrow a = 0$ ó $b = 0$

Esto no se va a verificar en todos los anillos, solo en D.I.

Ej: $\mathbb{Z}_4$: $a = 2$ $\quad a \cdot a = 4 = 0$ en $\mathbb{Z}_4$

$a \notin \langle 0 \rangle$

c) $\forall a, b, c \in \mathbb{Z}_n$ tq $ab = ac \Rightarrow a = 0$ ó $b = c$

No se verifica en todos los anillos

$ab - ac = 0 \Rightarrow a(b-c) = 0$ pero el recíproco para: $a = 0$ $b = c$

↑ (esto sí en todos los anillos)

Ej: en $\mathbb{Z}_6$: $a = 3$
$b = 3$
$c = 1$

$3(3-1) = 0$ ✓ $(= 6$ en $\mathbb{Z}_6)$

en cambio $3 \neq 0$
$3 \neq 1$

y $ab = ac$: $3 \cdot 3 = 3 \cdot 1$ ✓
$9 = 3$ en $\mathbb{Z}_6$

⑧ Sea $(S, +_1, \cdot_1)$ y $(T, +_2, \cdot_2)$ anillos y sea $R = S \times T$ el anillo producto. Demostrar que:

a) S y T son conmutativos y entonces R es conmutativo

$\forall (a,b), (c,d) \in R = S \times T$

$(a,b) \cdot (c,d) = (a \cdot_1 c, b \cdot_2 d) = (c \cdot_1 a, d \cdot_2 b) = (c,d) \cdot (a,b)$ ✓

($\cdot_1$ y $\cdot_2$ son conmutativos)

b) Si S y T tienen identidad, R tb

$(1_S, 1_T) \in R = S \times T$ $\quad \forall (a,b) \in R = S \times T$

$(1_S, 1_T) \cdot (a,b) = (1_S \cdot_1 a, 1_T \cdot_2 b) = (a,b)$ luego sí, $(1_S, 1_T)$ es la identidad, 1_R

c) Si S y T son cuerpos, ¿R el cuerpo?

No, porque el producto nunca será de división: (aunq cada uno de ellos (o sea [por separado] pq son cuerpos y por tanto tienen q ser de división)

$(1_S, 0_T) \in R = S \times T$

$(1_S, 0_T) \neq (0_S, 0_T) = 0_R$

$(a,b) \cdot (1_S, 0_T) = (a \cdot_1 1_S, b \cdot_2 0_T) = (a, 0_T) \neq (1_S, 1_T)$

$\forall a, b \in R$

3.2

① Describir todas las unidades de cada uno de los siguientes anillos:

a) $(\mathbb{Z}, +, \cdot)$

Unidades de $\mathbb{Z}$: $\{1, -1\}$ (son los únicos que tienen inverso en $\mathbb{Z}$)

$U_{\mathbb{Z}}$

b) $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$

$U_{\mathbb{Z}\times\mathbb{Z}} = \{(1,1), (1,-1), (-1,1), (-1,-1)\}$ cada componente de cada elemento debe ser unidad de $\mathbb{Z}$ (los primeros) y de $\mathbb{Z}$ (los segundos) → 1 ó -1 únicos posibles componentes

d) $(\mathbb{Q}, +, \cdot)$

$U_{\mathbb{Q}} = \mathbb{Q}^* = \mathbb{Q} - \{0\}$

c) $(\mathbb{Z}_3, +_3, \cdot_3)$

$U_{\mathbb{Z}_3} = \{1, 2\}$ todos estos tienen inverso en $\mathbb{Z}_3$ $\quad (1+2 = [0]_3 \quad 2+1 = [0]_3)$

(y primos con 3, $\text{mcd}(\mathbb{Z}_1, 3) = 1$)

e) $(\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}, +, \cdot)$

$$U_{\mathbb{Z}\times\mathbb{Q}\times\mathbb{Z}} = \{(a,b,c) : a,c \in \{1,-1\},\ b \in \mathbb{Q}^{*} = \mathbb{Q} - \{0\}\}$$

f) $(\mathbb{Z}_4, +_4, \cdot_4)$ ($\mathbb{Z}_4$ no es anillo)

$$U_{\mathbb{Z}_4} = \{r \in \{1,2,3\} : \text{mcd}(r,4) = 1\}$$

$$U_4 = \{1,3\}$$

② Encontrar divisores de cero y unidades de los siguientes anillos:

a) $(\mathbb{Z}_{10}, +_{10}, \cdot_{10})$

$U_{10} = \{1,3,7,9\}$

$C_{10} = \{2,4,5,6,8\}$

b) $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$

$U_{12} = \{1,5,7,11\}$ (tq mcd $(a,12) = 1$) primos con 12

$C_{12} = \{2,3,4,6,8,9,10\}$ [resto]

d) $(P(X), \Delta, \cap)$ donde $A \Delta B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$

$0_A = \phi$

$I_A = X$

Unidades: $A \in P(X)$ tq $A' \cap A = X$ para algún $A' \in P(X)$

↳ la única unidad es la identidad

$$U_{P(X)} = \{X = I_A\}$$

no hay nada que en una intersección con A pre de X (A está contenido en X!)

Divisores de cero:

$$C_{P(X)} = \{A \in P(X) : A \neq \phi \text{ y } A \neq X\}$$

③ Demostrar que todo elemento no nulo de $(\mathbb{Z}_n, +_n, \cdot_n)$ es una unidad o un divisor de cero.

Sea $a \in \mathbb{Z}_n$ que no es unidad ¿a es divisor de cero?

$\Rightarrow d = \text{mcd}(a,n) > 1 \Rightarrow$ ¿a es divisor de cero?

$a \cdot \frac{n}{d} = \frac{a}{d} \cdot n \equiv 0 \bmod n \Rightarrow a \cdot b = 0$, $b = \frac{n}{d} \neq 0$ $\Rightarrow$ a es divisor de cero

$\frac{n}{d} \in \mathbb{Z}_n$ ($a/d \in \mathbb{Z}$ (pq des divisor de a))

$d = \text{mcd}(a,n) = 1 \Rightarrow$ ¿a es unidad? Según Th. Bezout:

$\exists x, y \in \mathbb{Z}_n$ tq $ax + ny = 1 \Rightarrow ax = 1 \bmod n \Rightarrow$

$\Rightarrow [a]_n \cdot [x]_n = [1]_n \Rightarrow$ a es unidad

④ Encontrar un elemento no nulo (ninguno sería el 0 en $\mathbb{Z}_n$) de un anillo que no sea ni divisor de cero ni unidad. (Por lo demostrado en ③, no sirve ningún $\mathbb{Z}_n$)

$(\mathbb{Z}, +, \cdot)$ es anillo, $a = 2 \in \mathbb{Z}$
no es div. de cero
no es unidad

⑤ Encontrar dos elementos $a, b \in R$ en un anillo $(R, +, \cdot)$ que ambos sean divisores de cero pero que $a+b$ no sea cero ni divisor de cero.

Ej: 3, 2 son div de cero, pero 5 no lo es, en $\mathbb{Z}_6$.

⑥ ¿Cuales de los siguientes anillos son D.I? ¿Cuales son cuerpo?

a) $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$

No. El producto de dos cuerpos nunca es D.I

b) $(\mathcal{P}(\{a\}), \Delta, \cap)$, donde $A \Delta B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$

$X = \{a\}$
$\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$ Los únicos elem. q hay son el vacío y el total. No tiene div. de cero.

Sí es D.I y sí cuerpo, pero solo porque el q/to q tratamos tiene solo 1 elemento, uno no (o sería.

c) $(\{a+bi : a,b \in \mathbb{Q}\}, +, \cdot)$

$\{a+bi : a,b \in \mathbb{Q}\} \subset \mathbb{C}$

$\mathbb{C}$ es cuerpo

y no tiene divisores de cero

$\Rightarrow$ el conjunto $\mathbb{K}$ es un D.I.

Inverso: (para saber si es cuerpo, ya es un D.I es anillo conmut., con identidad, y sin div. de cero pero no asegura el inverso)

$$\frac{1}{a+bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i \in \{x+y : x,y \in \mathbb{Q}\}$$

↑ siempre que: $a+bi \neq 0$

↑ es de división

$\mathbb{K}$ es cuerpo

d) No

e) $(\{[0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}, +_{10}, \cdot_{10})$

¿Es D.I? Es subcjto. de $\mathbb{Z}_{10}$ pero aunq $\mathbb{Z}_{10}$ no sea D.I, este podría serlo, lo comprobamos:

$\cdot_{10}$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

Este anillo tiene un propio idempotente, el 6. Es D.I.

En la tabla no aparece ningún 0 → es de división

$\mathbb{K}$ es cuerpo

(*) Ze div de cero y unidades en $(\mathbb{Z}_2^{2\times 2}, +, \cdot)$

$\mathbb{Z}_2^{2\times 2} = \{ \underset{a}{\begin{pmatrix}0&0\\0&0\end{pmatrix}}, \underset{b}{\begin{pmatrix}1&0\\0&0\end{pmatrix}}, \underset{c}{\begin{pmatrix}0&1\\0&0\end{pmatrix}}, \underset{d}{\begin{pmatrix}0&0\\1&0\end{pmatrix}}, \underset{e}{\begin{pmatrix}0&0\\0&1\end{pmatrix}}$

elementos: $\underset{f}{\begin{pmatrix}1&1\\0&0\end{pmatrix}}, \underset{g}{\begin{pmatrix}0&0\\1&1\end{pmatrix}}, \underset{h}{\begin{pmatrix}1&0\\1&0\end{pmatrix}}, \underset{i}{\begin{pmatrix}0&1\\0&1\end{pmatrix}}, \underset{j}{\begin{pmatrix}1&0\\0&1\end{pmatrix}}, \underset{k}{\begin{pmatrix}0&1\\1&0\end{pmatrix}}$

$\underset{l}{\begin{pmatrix}0&1\\1&1\end{pmatrix}}, \underset{m}{\begin{pmatrix}1&0\\1&1\end{pmatrix}}, \underset{n}{\begin{pmatrix}1&1\\0&1\end{pmatrix}}, \underset{o}{\begin{pmatrix}1&1\\1&0\end{pmatrix}}, \underset{p}{\begin{pmatrix}1&1\\1&1\end{pmatrix}} \}$

$C = \overset{\text{e.neutro}}{a}, b, c, d, e, f, g, h, i, p$

$U = j, k, l, m, n, o$

Como son matrices, si el determinante es 0, son div. de cero, pero no tendrán

(7) Dar un ejemplo de anillo conmutativo con divisores de cero que no sea dominio de integridad.

D.I. Anillo conmutativo con identidad y sin div. de cero

$2\mathbb{Z}, 3\mathbb{Z}$ .... ejs. de anillos conmutativos c/ identidad.

(8) Si un anillo $(R, +, \cdot)$, un elemento $a \in R$ se dice idempotente si $a^2 = a$, se dice nilpotente si existe un n tq $a^n = 0_R$. Encontrar todas las unidades, todos los div. de cero, los elementos nilpotentes e idempotentes del anillo $\mathbb{Z}_3 \times \mathbb{Z}_6$.

$U_{\mathbb{Z}_3 \times \mathbb{Z}_6} = \{(1,1), (1,5), (2,1), (2,5)\}$

$C_{\mathbb{Z}_3 \times \mathbb{Z}_6} = \{(1,a) : \text{tq } a \in \{2,3,4\}\} \cup \{(0,a) : a \in \{1,2,3,4,5\}\} \cup$

$\{(2,a) : \text{tq } a \in \{0,3,4\}\}$

nilpotentes $(a,b)^n = (0,0)$ No hay ninguno en este anillo.

(Un ejemplo sería el 2 en $\mathbb{Z}_4$ → nilpotente)

idempotentes $a^2 = a \Leftrightarrow a(a-1) = 0$

cont. (*)

cont. (10)

$\mathbb{Z}_6$: $I_{\mathbb{Z}_6} = \{3,4,1,0\}$

en $\mathbb{Z}_6$:
- $3 \cdot 2 = 0$
- $4 \cdot 3 = 0$
- $1 \cdot 0 = 0$
- $(0 \cdot 0 = 0)$

en $\mathbb{Z}_3$: $I_{\mathbb{Z}_3} = \{0,1\}$
- $1 \cdot 0 = 0$
- $(0 \cdot 0 = 0)$

Idempotentes $\mathbb{Z}_3 \times \mathbb{Z}_6$: $\{(1,3),(1,4),(1,1),(0,0),(0,1),(0,3),(0,4),(1,0)\}$

(9) Si $a \in R$ es nilpotente en un anillo con identidad $(R,+,\cdot)$ tq $a^n = 0_R$.

① Calcular

$$(1_R - a)\sum_{k=0}^{n-1} a^k = \sum_{k=0}^{n-1} a^k - \sum_{k=1}^{n} a^k = a^0 - a^n = 1$$

($a^n = 0$)

② Probar que $1_n - a$ es unidad

$1_R - a$ es unidad: (ya lo demostré arriba)

$$(1_n - a)\sum_{k=0}^{n-1} a^k = 1 \Rightarrow (1-a)b = 1 \Rightarrow (1-a) \text{ es unidad}$$

(10) Encontrar la característica de los sig. anillos

b) $(\mathbb{Z} \times \mathbb{Z})$

$c(\mathbb{Z} \times \mathbb{Z}) = 0$ No hay ningún número $\neq$ sumado n veces sea $= 0$.

c) $(\mathbb{Z}_3 \times 3\mathbb{Z}, +, \cdot)$

$c(\mathbb{Z}_3 \times 3\mathbb{Z}) = (0, 3)$

d) $(\mathbb{Z}_3 \times \mathbb{Z}_3, +, \cdot)$

$c(\mathbb{Z}_3 \times \mathbb{Z}_3) = |(1,1)|_+ = 3$

"La característica de un anillo conmutativo es el orden del $(1,1)$, $|(1,1)|$" (con la suma)

e) $(\mathbb{Z}_3 \times \mathbb{Z}_4, +, \cdot)$

$c(\mathbb{Z}_3 \times \mathbb{Z}_4) = |(1,1)|_+ = 12$

f) $(\mathbb{Z}_6 \times \mathbb{Z}_{15}, +, \cdot)$

$c(\mathbb{Z}_6 \times \mathbb{Z}_{15}) = |(1,1)|_+ = 30$

g) $(\mathbb{Z}_m \times \mathbb{Z}_n, +, \cdot)$

$c(\mathbb{Z}_m \times \mathbb{Z}_n) = |(1,1)| = \text{mcm}(n,m)$] CASO GENERAL

h) $(\{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}, +_{12}, \cdot_{12}\})$

$|2|_+ = 6$
$|4|_+ = 3$
$|6|_+ = 2$
$|8|_+ = 3$
$|10|_+ = 6$

$\Rightarrow \underline{c(R) = 6_{(\text{mcm})}}$

3.3 SACADOS DE LOS APUNTES DE INÉS Y PINDO: pag (75)

④ En el cuerpo de $(\mathbb{Q}, +, \cdot)$ determinar el subanillo que contiene a $\frac{1}{2}$ y el menor subanillo que contiene a $\frac{2}{3}$. ¿Es alguno de ellos ideal?

para $\frac{1}{2}$: S subanillo, $\frac{1}{2} \in S \Rightarrow \frac{1}{2^n} \in S$; (por ser subanillo entonces) $\frac{1}{2} + \frac{1}{2} = 1 \in S \Rightarrow n \in \mathbb{N}$

$$\forall n \in \mathbb{Z} \Rightarrow n + \frac{1}{2^r} = \frac{2^r \cdot n + 1}{2^r} \Rightarrow \frac{m}{2^r} \in S$$

Vamos a comprobar si es subanillo para ver si hemos deducido bien: $S = \left\{ \frac{m}{2^r} : m, r \in \mathbb{N} \right\}$

- $S \neq \emptyset$ ya que $0 \in S$
- $\frac{m}{2^r} - \frac{n}{2^s} = \frac{2^s m - 2^r n}{2^{r+s}} \in S$
- $\frac{m}{2^r} \cdot \frac{n}{2^s} = \frac{m \cdot n}{2^{r+s}} \in S$

} es subanillo ✓

Si I es ideal y $\frac{1}{2} \in I$: $2 \cdot \frac{1}{2} \in I \Rightarrow 1 \in I$

$q \cdot 1 = q \in I \quad \forall q \in \mathbb{Q}$

① En el anillo $(\mathbb{Z}, +, \cdot)$ estudiar si los siguientes ideales son ideales y en caso afirmativo encontrar un solo generador $a \in \mathbb{N}$ para cada uno de ellos.

a) $\{2n + 3m : n, m \in \mathbb{Z}\}$

$2n_1 + 3m_1 \in M$
$2n_2 + 3m_2 \in M$ $\quad n_1, m_1, n_2, m_2 \in \mathbb{Z}$

$(2n_1 + 3m_1) - (2n_2 + 3m_2) = 2\underbrace{(n_1 - n_2)}_{\in \mathbb{Z}} + 3\underbrace{(m_1 - m_2)}_{\in \mathbb{Z}} \Rightarrow 2(n_1 - n_2) + 3(m_1 - m_2) \in M$

$r \cdot (2n_1 + 3m_1) = 2(\underbrace{r n_1}_{\in \mathbb{Z}}, \underbrace{m_1}_{\in \mathbb{Z}}) \in M$

$M = \{2n + 3m : n, m \in \mathbb{Z}\} \Rightarrow 1 \in M$; $1 = 2(-1) + 3(1) \in M$

$\Rightarrow M = \mathbb{Z}$

b) $\{3n+6m : n,m \in \mathbb{Z}\}$

$M = \{3n+6m : n,m \in \mathbb{Z}\}$

$3 \in M$ es el menor entero positivo en $M \Rightarrow M = (3)$

c) $\{an+bm : n,m \in \mathbb{Z}\}$

$m = (mcd(a,b))$

d) $\{5n+10m+15s : n,m,s \in \mathbb{Z}\}$

$m = (5)$

e) $\{3 \cdot 9m : m \in \mathbb{Z}\}$

$m = \{27m : m \in \mathbb{Z}\} = (27) = 27\mathbb{Z}$

2) Sea $(R,+,\cdot)$ un anillo conmutativo. Para cada $a \in R$ se define $N(a) = \{r \in R : r \cdot a = 0_R\}$. Demostrar que $N(a)$ es un ideal de R.

$N(a) = \{r \in R : r \cdot a = 0_R\}$ $\quad a \in R$

- $r_1, r_2 \in N(a)$ ¿$r_1 - r_2 \in N(a)$?

$(r_1 - r_2) \cdot a = r_1 \cdot a - r_2 \cdot a = 0_R - 0_R = 0_R$

($r_1 \in N(a)$, $r_2 \in N(a)$)

$\Rightarrow r_1 - r_2 \in N(a)$

- Sea $b \in R$, $r \in N(a)$ ¿$b \cdot r \in N(a)$?

$(b \cdot r) \cdot a = b \cdot (r \cdot a) = b \cdot 0_R = 0_R$

($r \in N(a)$)

$\Rightarrow b \cdot r \in N(a)$

- $0_R \in N(a) \Rightarrow N(a) \neq \emptyset$

3) Demostrar que $S = \{a+2bi : a,b \in \mathbb{Z}, i^2 = -1\}$ es un subanillo de $\mathbb{Z}[i]$ pero no es ideal.

(cont.)

$\Rightarrow$ (cont.) $(a+2bi),\ (c+2di) \in S$

① $(a+2bi) - (c+2di) = \underbrace{(a-c)}_{\in \mathbb{Z}} + 2\underbrace{(b-d)}_{\in \mathbb{Z}}i \quad \in S$

② $0 \in S \Rightarrow S \neq \phi$

③ $(a+2bi)(c+2di) = \underbrace{(ac-4bd)}_{\in \mathbb{Z}} + 2\underbrace{(ad+bc)}_{\in \mathbb{Z}}i \quad \in S$ Se cumple

④ $e+fi \in \mathbb{Z}[i],\ e, f \in \mathbb{Z}$

$(a+2bi)(e+fi) = (ae-2bf) + (af+2be)i$

$(1+2i)(1+i) = -1+3i \notin S$

$\Rightarrow \lambda$ no es ideal

⑤ Sean $(R, +_1, \cdot_1)$ y $(S, +_2, \cdot_2)$ anillos con identidad. Sabiendo que los ideales del anillo $(R \times S, +, \cdot)$ son de la forma $A \times B$ donde A ideal de R y B ideal de S, hallar todos los ideales de:

a) $\mathbb{Z}_2 \times \mathbb{Z}_2$

En $\mathbb{Z}_2$ ideales: $\begin{cases} I_0 = \langle 0 \rangle \\ I_1 = \mathbb{Z}_2 = \langle 1 \rangle \end{cases}$

$\mathbb{Z}_2 \times \mathbb{Z}_2$ ideales:

$I_0 \times I_0 = \langle (0,0) \rangle$

$I_0 \times I_1 = \{(0,0), (0,1)\}$

$I_1 \times I_0 = \{(0,0), (1,0)\}$

$I_1 \times I_1 = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0)\}$

b) $\mathbb{Z} \times \mathbb{Z}_4$

En $\mathbb{Z}$ ideales: $n\mathbb{Z} = (n) = \{n \cdot a : a \in \mathbb{Z}\}$

En $\mathbb{Z}_4$ ideales: $I_0 = (0) = \langle 0 \rangle$

$I_1 = (1) = \mathbb{Z}_4 = \{0,1,2,3\}$

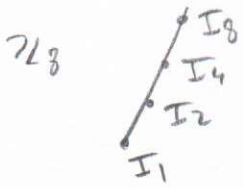
$I_2 = (2) = \langle 0,2 \rangle$

$\mathbb{Z} \times \mathbb{Z}_4$ ideales:

$\mathbb{Z} \times I_K \quad K \in \{0,1,2\}$

$n\mathbb{Z} \times I_K$

① Obtener todos los ideales maximales del anillo $\mathbb{Z}_8 \times \mathbb{Z}_{30}$ con las operaciones usuales componente a componente. Para cada ideal M calculado indicar el número de elementos del anillo cociente $(R/M, +_M, \cdot_M)$ ¿Se puede concluir que hay cuerpos con un número de elementos que sea un número primo? (no)

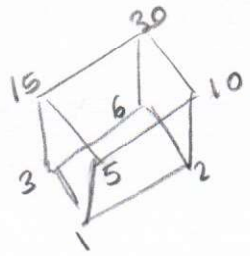


$\rightarrow M = (2)$

$J_1 = (5)$

$J_2 = (3)$

$J_3 = (2)$



$M \times J_1$ no es maximal

$M \times \mathbb{Z}_{30} \rightarrow 2$

$\mathbb{Z}_8 \times J_1 \rightarrow 5$

$\mathbb{Z}_8 \times J_2 \rightarrow 3$

$\mathbb{Z}_8 \times J_3 \rightarrow 2$

(3.5 creo q 144 -divisores)

3.6

① Estudiar si la siguiente igualdad es verdadera o falsa en $\mathbb{Z}_{15}[x]$

$$(x+1)(x+14) = (x+4)(x+11)$$

$$x^2 + 14x + x + 14 = x^2 + 11x + 4x + 44$$

$$[x^2+14]_{15} \quad \text{sí} \quad [x^2+44]_{15} = [x^2+14]_{15}$$

② ~~Sea $(R, +, \cdot)$~~ En $(\mathbb{Z}[x], +, \cdot)$ sea $I = \{p \in \mathbb{Z}[x] : p(0) = 0\}$. Demostrar que I no es un ideal maximal

$$I = \{p \in \mathbb{Z}[x] : p(0) = 0\} = \{a_1 x + a_2 x^2 + \dots + a_n x^n : a_i \in \mathbb{Z}\}$$

$$I \subsetneq J \subsetneq \mathbb{Z}[x]$$

$$\{a_0 + a_1 x + \dots + a_n x^n : a_i \in \mathbb{Z}\}$$

(8) Determinar el número de elementos que hay en cada uno de los siguientes anillos cocientes. Obtener característica:

a) $\mathbb{Z}[i]/(3+i)$

$I = (3+i)$ $\qquad (3-i)\underbrace{(3+i)}_{\in I} \in I \Rightarrow 10 \in I$ $\qquad \underbrace{(3-i)}_{\in \mathbb{Z}[i]}$

- $10 \in I$
- ¿10 es el menor entero positivo que está en I?

$(3+i)(a+bi) = (3a-b) + (3b+a)i \in \mathbb{Z} \Leftrightarrow 3b+a=0$

$\Leftrightarrow a = -3b \Leftrightarrow (3+i)(a+bi) = (3(-3b)-b) = -10b \in I$

- $a+bi \in \mathbb{Z}[i]$

$a+bi = (3+i)b + (a-3b) =$

$= \underbrace{(3+i)b + 10q}_{\in I} + r$

$a-3b = q\cdot 10 + r$

$0 \le r < 10$

$[a+bi]_{(3+i)} = [r]_{(3+i)}$

$\mathbb{Z}[i]/_{(3+i)} = \{[0], [1], \dots, [9]\}$

b) $\mathbb{Z}[i]/(2+i)$

$(2+i)(2-i)\cdot 5 \in I = (2+i) \Rightarrow 5$ es el menor entero positivo

$(2+i)(a+bi) = (2a-b) + i(2b+a) \in \mathbb{Z} \Leftrightarrow a = -2b \Leftrightarrow$

$(2+i)(a+bi) = -4b - b = -5b \in 5$

$a+bi = (2+i)b + (a-2b)$

$= \underbrace{(2+i)b + 5q}_{\in (2+i) = I} + r$

$a-2b = 5q + r$

$0 \le r < 5$

$[a+bi] = [r]$

⑥ Estudiar si el conjunto cociente $2\mathbb{Z}/8\mathbb{Z}$ tiene estructura de anillo. En caso afirmativo dar las tablas de las operaciones y determinar si es un anillo conmutativo, con identidad, de división y si es cuerpo.

$2\mathbb{Z}/8\mathbb{Z}$ es anillo $\Leftrightarrow$ $8\mathbb{Z}$ es ideal de $2\mathbb{Z}$

$8u_1, 8u_2 \in 8\mathbb{Z} \Rightarrow 8u_1 - 8u_2 = 8(u_1 - u_2) \in 8\mathbb{Z}$

$\underbrace{8u}_{\in 8\mathbb{Z}} \cdot \underbrace{2k}_{\in 2\mathbb{Z}} = 8(\underbrace{2uk}_{\in \mathbb{Z}}) \in 8\mathbb{Z}$

$\Rightarrow$

$\Rightarrow$ $8\mathbb{Z}$ es ideal de $2\mathbb{Z}$

¿ $2\mathbb{Z}/8\mathbb{Z}$?

$[0] = \{8h : h \in \mathbb{Z}\} = 8\mathbb{Z}$

$[2] = \{2 + 8h : h \in \mathbb{Z}\}$

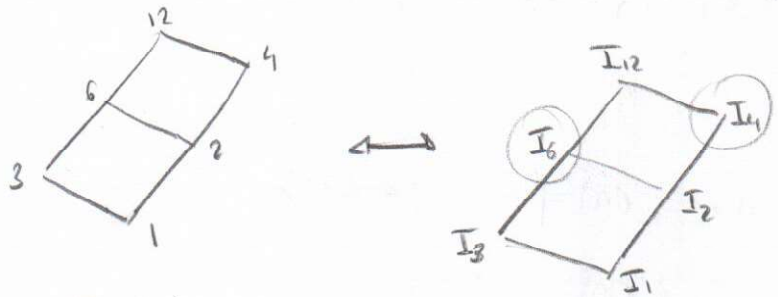
$[4] = \{4 + 8h : h \in \mathbb{Z}\}$

$[6] = \{6 + 8h : h \in \mathbb{Z}\}$

conmutativo
con identidad
NO es de división
NO es cuerpo

·	2	4	6
2	4	0	4
4	0	0	0
6	4	0	4

⑦ Encontrar todos los ideales I de $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$ y estudiar para cada uno de ellos si el anillo cociente $(\mathbb{Z}_{12}/I, +_{12}, \cdot_{12})$ es cuerpo.



$I_1 = (0)$

$I_2 = (6)$

$I_3 = (4)$

$I_4 = (3)$

$I_6 = (2)$

$I_{12} = (1)$

$\mathbb{Z}_{12}/(2)$

$\mathbb{Z}_{12}/(3)$

son cuerpos

③ Encontrar el resto que resulta al dividir $f = x^{100} + x^{90} + x^{80} + x^{50} + 1$ entre $g = x + 1$ en $\mathbb{Z}_2[x]$

$$f = q(x-1) + r \qquad \text{grado}(r) \leq 0$$

$$f(1) = q(1)(1-1) + r(1) \Rightarrow r(1) = 5 = r = f(1)$$

$$\Rightarrow f = q(x-1) + 5$$

(seguir en diap. 184)