Estructuras Algebraicas Segundo examen parcial	1$^{\text{er}}$ Apellido: ________________	24 de mayo de 2016
	2$^{\text{o}}$ Apellido: ________________	Tiempo 2 h.
Departamento Matem. aplic. TIC ETS de Ingenieros Informáticos Universidad Politécnica de Madrid	Nombre: ________________ Número de matrícula:	**Calificación:**

1. (2,5 puntos)

   a) Sea $(R, +, \cdot)$ un anillo y sea $S \subseteq R$. ¿Qué propiedades debe verificar S para ser un subanillo de R?

   b) Demostrar que $T = \{\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} : a \in \mathbb{Q}\}$ es un subanillo de $(\mathbb{Q}^{2\times 2}, +, \cdot)$. ¿Es un ideal?

   c) ¿Es T un subanillo conmutativo? Marca la opción correcta y justifica la respuesta.

   d) ¿Es T un cuerpo? Marca la opción correcta y justifica la respuesta.

   e) Estudiar si T es isomorfo a $(\mathbb{Q}, +, \cdot)$

2. (2,5 puntos) Los siguientes conjuntos, con las operaciones usuales en cada uno de ellos, son anillos conmutativos con identidad:

$$R_1 = \mathbb{Z}_5, \qquad R_2 = \mathbb{Z}_6 \times \mathbb{Z}_4, \qquad R_3 = \mathbb{Z}[x], \qquad R_4 = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Q}\}$$

   a) Dar la identidad de cada uno de los anillos R_1, R_2, R_3, R_4.

   b) Encontrar la característica de cada uno de los anillos R_1, R_2, R_3, R_4.

   c) Describir las unidades de cada uno de los anillos R_1, R_2, R_3, R_4.

   d) Indicar si algunos de los anillos R_1, R_2, R_3, R_4 tienen divisores de cero. En caso afirmativo dar un ejemplo.

   e) ¿Es alguno de ellos dominio de integridad? ¿Es alguno de ellos cuerpo? En caso afirmativo indicar cuáles. Justificar la respuesta

3. (2,5 puntos)

   a) Estudiar si $\mathbb{Q}(\sqrt{2}, \sqrt{6})$ es una extensión simple de $\mathbb{Q}$.

   b) Se considera el polinomio $p = x^4 - 2x^3 + 6x - 10 \in \mathbb{Q}[x]$. Demostrar que es irreducible.

   c) El teorema de Kronecker garantiza la existencia de una raíz α de p. ¿En qué cuerpo asegura el teorema de Kronecker que existe una raíz de p?

   d) En el cuerpo y para la raíz α citados en el apartado anterior, realizar las siguientes operaciones:

      1) $(\alpha^2 - 1)(\alpha^2 - \alpha + 1)$
      2) $(\alpha^2 - 2\alpha + 3)^{-1}$

4. (2,5 puntos)

   a) Calcular el polinomio mínimo de $\beta = \sqrt[3]{2} + \sqrt[3]{4}$ sobre $\mathbb{Q}$.

   b) Calcular una base y el grado de extensión de $\mathbb{Q}(\sqrt{5}, \sqrt[6]{5})$ sobre $\mathbb{Q}$.

   c) Demostrar que $h = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ es irreducible en $\mathbb{Z}_2[x]$.

   d) Estudiar si h es un polinomio primitivo. Justificar la respuesta.

   e) Indicar qué elementos del cuerpo $\mathbb{Z}_2[x]/\langle h \rangle$ tienen raíz cuadrada.

1. *a*) (i) $T \neq \emptyset$, porque $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in T$ y (ii) Para todos $\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} \in T$ es $a-b \in \mathbb{Q}$ y $a \cdot b \in \mathbb{Q}$, $\Rightarrow$ $\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ -(a-b) & 0 \end{pmatrix} \in T$ y $\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ -ab & 0 \end{pmatrix} \in T$ $\Rightarrow$ T es un subanillo de $\mathbb{Q}^{2\times 2}$

$\begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix} \in \mathbb{Q}^{2\times 2}$, y $\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} \in T$, pero $\begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix} \notin T$ $\Rightarrow$ T no es un ideal de $\mathbb{Q}^{2\times 2}$

b) T es un subanillo conmutativo: $\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ -ab & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}$

c) T es un cuerpo: Es conmutativo, tiene identidad: $\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}$ y es de división: $\forall$ $\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \in T$ no nulo, es $a \neq 0 \Rightarrow \frac{1}{a} \in \mathbb{Q} \Rightarrow \begin{pmatrix} \frac{1}{a} & 0 \\ -\frac{1}{a} & 0 \end{pmatrix} \in T$ y es $\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}\begin{pmatrix} \frac{1}{a} & 0 \\ -\frac{1}{a} & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}$

d) T es isomorfo a $(\mathbb{Q}, +, \cdot)$: $\varphi : T \to \mathbb{Q}$ tal que $\varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}) = a$

(i) φ es biyectiva: $\varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}) = \varphi(\begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix}) \Leftrightarrow a = b \Leftrightarrow \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix}$ y $\forall a \in \mathbb{Q}$ existe $\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \in T$ tal que $\varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}) = a$

(i) φ es homomorfismo de anillos: $\forall$ $\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} \in T$ es

$\varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix}) = \varphi(\begin{pmatrix} a+b & 0 \\ -a-b & 0 \end{pmatrix}) = a+b = \varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}) + \varphi(\begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix})$,

y $\varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix}) = \varphi(\begin{pmatrix} ab & 0 \\ -ab & 0 \end{pmatrix}) = ab = \varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}) \cdot \varphi(\begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix})$

2.

Identidad de R_1	Identidad de R_2	Identidad de R_3	Identidad de R_4
$[1]_5$	$([1]_6, [1]_4)$	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Característica de R_1	Característica de R_2	Característica de R_3	Característica de R_4
5	12	0	0

Unidades de R_1	Unidades de R_2	Unidades de R_3	Unidades de R_4
$\{[1]_5, [2]_5, [3]_5, [4]_5\}$	$\{([1]_6, [1]_4), ([1]_6, [3]_4), ([5]_6, [1]_4), ([5]_6, [3]_4)\}$	$\{1, -1\}$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ $\forall a, b \in \mathbb{Q}^*$

Divisor de cero en R_1	Divisor de cero en R_2	Divisor de cero en R_3	Divisor de cero en R_4
No tiene	Sí tiene por ejemplo: $([3]_6, [2]_4)$	No tiene	Sí tiene por ejemplo: $\begin{pmatrix} 7 & 0 \\ 0 & 0 \end{pmatrix}$

Son dominios de integridad los anillos: R_1 y R_3. El único cuerpo es: R_1

3. *a*) Sí es simple: $\mathbb{Q}(\sqrt{2}+\sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{6})$.
   b) Por el criterio de Eisenstein: $p = 2 \in \mathbb{N}$
   c) $\mathbb{Q}[x]/\langle p\rangle \approx \mathbb{Q}(\alpha)$
   d) 1) $\alpha^3 - 5\alpha + 9$
      2) $\alpha^2 - 3$

4. *a*) $x^3 - 6x - 6$
   b) $B = \{1, 5^{\frac{1}{6}}, 5^{\frac{1}{3}}, 5^{\frac{1}{2}}, 5^{\frac{2}{3}}, 5^{\frac{5}{6}}\}$, $\qquad [\mathbb{Q}(\sqrt{5}, \sqrt[6]{5}) : \mathbb{Q}] = 6$
   c) Es un polinomio de grado 3 y no tiene raíces en $\mathbb{Z}_2$
   d) $\langle x\rangle = \{1,\ x,\ x^2,\ x^3 = x^2+1,\ x^4 = x^2+x+1,\ x^5 = x+1,\ x^6 = x^2+x\} = (\mathbb{Z}_2[x]/\langle h\rangle)^*$
   e) x^2, $\qquad x^2+1 = x^{10} = (x+1)^2$, $\qquad x^2+x = x^6 = (x^2+1)^2$, $\qquad x^2+x+1 = x^4$.