① Teoría

② ⓐ $x=1$ es raíz de $p(x)$. Dividiendo $p(x)$ entre $x-1$ obtenemos

$$\begin{array}{c|cccccc} & 1 & 0 & 0 & 0 & 0 & -1 \\ 1 & & 1 & 1 & 1 & 1 & 1 \\ \hline & 1 & 1 & 1 & 1 & 1 & \boxed{0} \end{array}$$

$$p(x) = (x-1)\underbrace{(x^4+x^3+x^2+x+1)}_{= q(x)}$$

Veamos que $q(x)$ es irreducible sobre $\mathbb{Q}$.
Vamos a usar el criterio modular con el primo $r=2$.
Sobre $\mathbb{Z}_2$, $q(x)$ es un polinomio sin raíces por lo que no puede factorizar como producto de un polinomio de grado 1 por otro de grado 3.
Por otro lado, el único polinomio irreducible

Luego $q(x)$ no puede factorizar en producto de 2 irreducibles de grado 2 sobre $\mathbb{Z}_2$.

Por tanto $q(x)$ irreducible sobre $\mathbb{Z}_2$.

Por el criterio modular, $q(x)$ irreducible sobre $\mathbb{Q}$.

Por tanto $p(x) = (x-1)(x^4+x^3+x^2+x+1)$ es la factorización en irreducibles de $p(x)$ sobre $\mathbb{Q}$ (el primer factor es irreducible por ser de grado 1).

b) No, la factorización de $p(x)$ sobre $\mathbb{R}$ tiene que tener, al menos, 3 factores irreducibles, ya que los polinomios irreducibles sobre $\mathbb{R}$ sólo pueden ser de grado 1 ó 2.

3º a) 1) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I$ (tomando $b=0$)

2) $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} \in I \Rightarrow$

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b-b' \\ 0 & 0 \end{pmatrix} \in I$$

3) Si $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in A$, $\begin{pmatrix} 0 & b' \\ 0 & c \end{pmatrix} \in I$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ab' \\ 0 & 0 \end{pmatrix} \in I$$

$$\begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & b'c \\ 0 & 0 \end{pmatrix} \in I$$

b) Definimos

$$f : A \longrightarrow \mathbb{R} \times \mathbb{R}$$
$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \longmapsto (a, c)$$

Veamos que f es un homomorfismo

① f respeta la suma:

$$f\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\right) =$$

$$= f\left(\begin{pmatrix} a+a' & b+b' \\ 0 & c+c' \end{pmatrix}\right) = (a+a', c+c') =$$

$$= (a,c) + (a',c') = f\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) + f\left(\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\right)$$

② f respeta el producto:

$$f\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\right) = f\left(\begin{pmatrix} aa' & ab'+bc' \\ 0 & c \cdot c' \end{pmatrix}\right) =$$

$$= (aa', c \cdot c') = (a,c) \cdot (a',c') =$$

$$= f\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) \cdot f\left(\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\right)$$

Veamos que f es suprayectiva:

Dado $(a,c) \in \mathbb{R} \times \mathbb{R}$ $\exists M \in A / f(M) = (a,c)$:

tomamos $M = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$.

Por el 1er tma. de isomorfía, la función

Falta ver que $Ker(f) = I$.

$Ker(f) = \{M \in A / f(M) = (0,0)\} =$

$= \{M \in A / (a,c) = (0,0)\} =$

$= \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} / (a,c) = (0,0),\ b \in \mathbb{R} \right\} = I$

Por tanto $g : A/I \longrightarrow \mathbb{R} \times \mathbb{R}$

$\left[\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right]_I \longmapsto (a,c)$

es isomorfismo de anillos.

(4º) (a) $p(x) = x^2 + 2$ es irreducible sobre $\mathbb{Z}_5[x]$ por ser de grado 2 y no tener raíces en $\mathbb{Z}_5$.

Por teoría sabemos que si $p(x)$ es irreducible $\Rightarrow \mathbb{Z}_5[x]/(p(x))$ es cuerpo.

Veamos que $\forall f(x) \in \mathbb{Z}_5[x]\ \exists r(x) \in \mathbb{Z}_5[x]$

Por el teorema de la división en $K[x]$ (K cuerpo)

$\exists\, q(x), r(x) \in \mathbb{Z}_5[x]$ /

$f(x) = q(x)(x^2+2) + r(x)$ y $gr(r(x)) \leq 1$.

Tomando clases módulo $I = (x^2+2)$,

como $[x^2+2]_I = [0]_I$, tenemos

$[f(x)]_I = [r(x)]_I$

Por tanto hay, a lo sumo, tantas clases como polinomios de grado ≤ 1 sobre $\mathbb{Z}_5$.

Todos esos polinomios son de la forma $ax+b$ con $a, b \in \mathbb{Z}_5$, luego hay 25.

Falta ver que dos polinomios distintos de grado ≤ 1 dan clases distintas.

La resta de dos de estos polinomios es un polinomio de grado ≤ 1 no nulo, por tanto no puede estar en I ya que

(b) $\mathbb{Z}_{25}$ no es cuerpo ya que

$$5 \cdot 5 = 25 = 0 \mod 25$$
$$\begin{matrix} \neq & \neq \\ 0 & 0 \end{matrix}$$

por lo que $\mathbb{Z}_{25}$ ~~nn~~ tiene divisores de cero, esos elementos no son invertibles y por tanto $\mathbb{Z}_{25}$ no es cuerpo.
Como A/I sí lo es, no son isomorfos.

(c) Hallamos una id. de Bezout entre

x^2+2 y $x+4$

$$\begin{array}{rl} x^2+2 & \underline{|\,x+4\,} \\ -(x^2+4x) & x+1 \\ -4x+2 & \\ \shortparallel & \\ x+2 & \\ \underline{-(x+4)} & \\ -2=3 & \end{array}$$

$$3 = x^2+2 - (x+1)(x+4)$$

Tomando clases mod I

$$[1]_I = [-2x-2]_I\,[x+4]_I =$$

$$= [3x+3]_I\,[x+4]_I$$

luego $[x+4]_I^{-1} = [3x+3]_I$

5º a)

I primo $\Rightarrow A/I$ es D.I.

A a.c.c.u.

Veamos que A/I es cuerpo.

Como A tiene $1_A \in A$, $I \neq A$ por ser primo. $\Rightarrow 1_A \notin I$ (si $1_A \in I \Rightarrow I = A$).

Por tanto $[1_A]_I$ es la unidad de A/I.

Veamos que si $[a]_I \neq [0]_I \Rightarrow$

$\Rightarrow [a]_I$ invertible.

$$[a]_I \underset{\uparrow}{=} [a\cdot a]_I = [a]_I[a]_I$$

Luego $[a]_I$ es invertible ya que

$$[a]_I \cdot [a]_I = [1]_I .$$

Por tanto A/I cuerpo. $\Rightarrow$ I maximal.

(b) De hecho, en (a) hemos visto que

si $[a]_I \neq [0]_I$ entonces $[a]_I = [1]_I$

luego $A/I = \{ [0]_I, [1]_I \}$

tiene 2 elementos