AM

HOJA 8:

PROBLEMA 1: a) Sea $\mathbb{Q}[i] = \{a+ib : a,b \in \mathbb{Q}\}$ con $i^2 = -1$.

Claramente $\mathbb{Q}[i] \subseteq \mathbb{C}$; para $(a+ib), (c+id) \in \mathbb{Q}[i]$

$(a+ib) - (c+id) = (a-c) + (b-d)i \in \mathbb{Q}[i]$

Luego $(\mathbb{Q}[i], +)$ es un subgrupo de $(\mathbb{C}, +)$

Por otro lado $(a+ib)\cdot\left(\frac{a}{a^2+b^2} + \frac{b}{a^2+b^2}i\right) = 1$

con $\frac{a}{a^2+b^2} + \frac{b}{a^2+b^2}i \in \mathbb{Q}[i]$, luego todo elemento de $\mathbb{Q}[i] - \{0\}$ tiene inverso; además es claro que $(a+bi)(c+di) = (ac-bd) + (ad+bc)i \in \mathbb{Q}[i]$.

Luego $(\mathbb{Q}[i]^*, \cdot)$ es un subgrupo de $\mathbb{C}^*$; por tanto $\mathbb{Q}[i]$ es un subanillo de $\mathbb{C}$.

PROBLEMA 2: a) Calculemos los polinomios mónicos de grado 2 de $\mathbb{Z}_5[x]$

$\mathbb{Z}_5^*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Sea $p(x) = x^2 + ax + b \in \mathbb{Z}_5[x]$ mónico de grado 2 e irreducible.

Entonces $b \neq 0$; si p fuese reducible

$p(x) = (x+\beta_1)(x+\beta_2) \Rightarrow \begin{cases} b = \beta_1\cdot\beta_2 \\ a = \beta_1 + \beta_2 \end{cases}$

Discutimos casos.

Si $b_1 = 1 \Rightarrow$
- o $\beta_1 = \beta_2 = 1 \Rightarrow a = 2$
- o $\beta_1 = 2$, $\beta_2 = 3 \Rightarrow a = 0$
- o $\beta_1 = \beta_2 = 4 \Rightarrow a = 3$

Luego $x^2 + x + 1$ y $x^2 + 4x + 1$ son irreducibles

Si $b_2 = 2 \Rightarrow$
- $\beta_1 = 1$ y $\beta_2 = 2 \Rightarrow a = 3$
- $\beta_1 = 3$ y $\beta_2 = 4 \Rightarrow a = 2$

Luego $x^2 + x + 2$, $x^2 + 2$, $x^2 + 4x + 2$ son irreducibles.

AM

Hoja 5:

Problema 2: a) Continuación.

Si $b=3$ $\Rightarrow$ $\begin{cases} \beta_1=1 \text{ y } \beta_2=3 & \Rightarrow a=2 \\ \beta_1=2 \text{ y } \beta_2=4 & \Rightarrow a=1 \end{cases}$

Luego x^2+3

x^2+2x+3

y x^2+3x+3 son irreducibles

Si $b=4$ $\Rightarrow$ $\begin{cases} \beta_1=1 \text{ y } \beta_2=4 & \Rightarrow a=0 \\ \beta_1=\beta_2=2 & \Rightarrow a=2 \\ \beta_1=\beta_2=3 & \Rightarrow a=1 \end{cases}$

Luego x^2+2x+4

y x^2+3x+4 son irreducibles

En total lo polinomios de grado 2 mónicos irreducibles son todos menos los 2 polinomios mónicos de grado 2.

b) $x^4+1 \in \mathbb{Z}_5[x]$ ¿es irreducible? ¿Cómo es su descomposición en factores irreducibles?

como $\phi(5)=4$ (función de Euler) $a^{\phi(5)}=a^4\equiv 1 \bmod 5$ si $a\neq 0$

Luego para $x=0$ $x^4+1\neq 0$

para $x\neq 0$ $x^4+1\equiv 1+1=2 \bmod 5$

Luego x^4+1 no tiene raíces en $\mathbb{Z}_5[x]$.

¿Existe $x^2+ax+b\in\mathbb{Z}_5[x]$ irreducible con $x^2+ax+b \mid x^4+1$?

Podemos razonar con lo polinomios irreducibles encontrados en a); pero hay una forma más sencilla:

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

$-4=1$ (diferencia de cuadrados) $\quad -2\equiv 3 \bmod 5$

Observemos que x^2+3 y x^2+2 están en la lista de irreducibles del Apartado a)

AM

Hoja 8:

Problema 3:

$$f(x) = x^6 - 1 = (x^3)^2 - 1 = (x^3-1)(x^3+1) =$$
$$= (x-1)(x^2+x+1)(x+1)(x^2-x+1)$$

$x^3 - 1 \;|\; x-1$
$x^2 + x \quad\; x^2+x+1$

Dem de x^2+x+1 y x^2-x+1 son irreducibles en $\mathbb{R}$.

$x^3 + 1 \;|\; x+1$
$-x^2 + x \quad\; x^2-x+1.$

Visto $f(x) = x^6 - 1$ como un polinomio de $\mathbb{C}[x]$.

$$x^6 - 1 = \prod_{k=0}^{5} \left(x - e^{i\frac{2k\pi}{6}}\right).$$

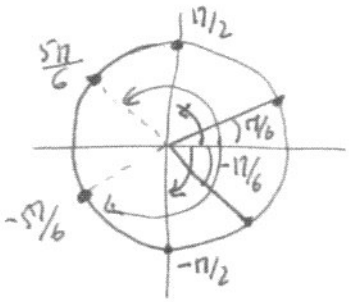
$g(x) = x^6 + 1 \in \mathbb{R}[x]$ no existe $\alpha \in \mathbb{R}$ con $\alpha^6 + 1 = 0$, así si g se descompone en $\mathbb{R}[x]$, la suma de un polinomio de grado 1 o 2 con otro no tiene raíces y otro grado impar con otro grado 2; luego tenemos reales

---

$g(x) = x^6 + 1 \in \mathbb{C}[x]$, luego

$$x^6 + 1 = \prod_{k=0}^{5} x - e^{i\left(\frac{\pi + 2k\pi}{6}\right)} =$$

$$= (x - e^{i\pi/6})(x - e^{-i\pi/6})(x-i)(x+i)\left(x - e^{i\frac{5\pi}{6}}\right)\left(x - e^{-i\frac{5\pi}{6}}\right) =$$



$$= (x^2 - 2(\cos 30^\circ)x + 1)(x^2+1)(x^2 + 2(\cos 30^\circ)x + 1) =$$
$$= (x^2 - 2\sqrt{3}/2\, x + 1)(x^2+1)(x^2 + 2\sqrt{3}/2\, x + 1)$$

$\cos \pi/6 = \cos 30^\circ = \sqrt{3}/2$

$\operatorname{sen} 30^\circ = 1/2$

AM

LISTA 8ª

PROBLEMA 4)

$f(x) = 4x^2 - 4x + 8$ EN $\mathbb{Z}$ NO HAY RAÍCES!

$$4x^2 - 4x + 8 = 0 \iff x = \frac{4 \pm \sqrt{16 - 16 \cdot 8}}{8} = \frac{1 \pm \sqrt{1 - 8}}{2} = \frac{1}{2} \pm i\frac{\sqrt{7}}{2}$$

LUEGO NO ES REDUCIBLE NI EN $\mathbb{Z}[x]$, NI EN $\mathbb{Q}[x]$; PUESTO ELLO SERÍA PRODUCTO DE POLINOMIO LINEALES Y ASÍ f TENDRÍA QUE TENER RAÍCES EN $\mathbb{Z}$ ó $\mathbb{Q}$

× $\mathbb{Z}_{11}$

	1	2	3	4	5	6	7	8	9	10
1	1	(2)	3	4	5	6	7	8	9	10
2	(2)	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	(2)	5	8
4	4	8	1	5	9	(2)	6	10	3	7
5	5	10	4	9	3	8	(2)	7	1	6
6	6	1	7	(2)	8	3	9	4	10	5
7	7	3	10	6	(2)	9	5	1	8	4
8	8	5	(2)	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	(2)
10	10	9	8	7	6	5	4	3	(2)	1

$4x^2 - 4x + 8 =$

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

$= 4(x + a)(x + b)$

↓

EN $\mathbb{Z}_{11}[x]$

POR TANTO:

$ab = 2$

Y $a + b = -1 \equiv 10 \bmod 11$

- ASI $a = 1$ Y $b = 2$

$\Rightarrow a + b = 3$ NO

LUEGO $4(x^2 - x + 2) =$

$= 4(x + 4)(x + 6)$ EN $\mathbb{Z}_{11}[x]$.

- $a = 3$ Y $b = 8$, PERO $8 + 3 \equiv 0 \bmod 11$ NO

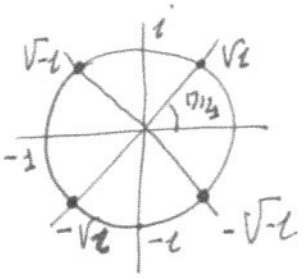
- $a = 4$ $b = 6$ Y ADEMÁS $4 + 6 = 10 \bmod 11$

- $a = 5$ Y $b = 7$, PERO $5 + 7 \equiv 1 \bmod 11$

AM.

HOJA 8:

PROBLEMA 5: $f(x) = x^4 + 1 = (x^2+1)(x^2-1) =$ en $\mathbb{C}$



$= (x-\sqrt{i})(x+\sqrt{i})(x-\sqrt{-i})(x+\sqrt{-i}) =$

$= (x^2 - \frac{2}{\sqrt{2}}x + 1)(x^2 + \frac{2}{\sqrt{2}}x + 1)$ NO CONSIDERADO en $\mathbb{R}[x]$; pero en $\mathbb{Q}[x]$ y $\mathbb{Z}[x]$ x^4+1 es irreducible.

$f(x) = x^4+1 \in \mathbb{Z}_2[x]$ $x=1$ es raíz; además $-1 \equiv 1 \bmod 2$

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

$= (x+1)(x+1)(x+1)(x-1) = (x+1)^4$.

Luego $x=1$ es una raíz cuadrada de x^4+1 en $\mathbb{Z}_2[x]$.

$f(x) = x^4+1 \in \mathbb{Z}_3[x]$, para $a=0$, $a=1$ ó $a=2$, $a^4+1 \neq 0$

Luego f no tiene raíces en $\mathbb{Z}_3$.

Si f es reducible, $f(x) = (x^2+ax+b)(x^2+a'x+b')$.

Ambos factores mónicos de 2º grado irreducibles en $\mathbb{Z}_3[x]$.

Por lo visto en el ejercicio 2

x^2+ax+b debe ser x^2+1; x^2+x+2 ó x^2+2x+2.

Dividiendo x^4 entre x^2+x+2 (no. la división x^2+1 como se comprueba fácilmente)

$+1 \;|\; x^2+x+2$

$2x^3+x^2$ — x^2+2x+2

$\frac{x^2+2x}{2x^2+2x+1}$

$2x^2+2x+1 = 2(x^2+x+2)$

Así $x^4+1 = (x^2+x+2)(x^2+2x+2)$

AM

HOJA 8:

PROBLEMA 5: (continuación)

$f(x) = x^4 + 1 \in \mathbb{Z}_7[x]$

$x \in \mathbb{Z}_7^*$	$f(x)$
1	2
2	3
3	$[3^2][3^2]+1 = 5$
4	$[4^2][4^2]+1 = 5$
5	$[5^2][5^2]+1 = 3$
6	$[36][36]+1 = 2$ mod 7

Vemos fácilmente que f no tiene raíces en $\mathbb{Z}_7$; luego si f es reducible

$x^4+1 \overset{(*)}{=} (x^2+ax+b)(x^2+cx+d)$

con x^2+ax+b, y x^2+cx+d irreducibles.

De (*) se sigue que
$$\begin{cases} bd = 1 \\ ad+cb = 0 \\ b+d+ac = 0 \\ c+a = 0 \end{cases}$$

$\mathbb{Z}_7^* \times$	1	2	3	4	5	6
1	(1)	2	3	4	5	6
2	2	4	6	(1)	3	5
3	3	6	(2)	5	(1)	4
4	4	(1)	5	(2)	6	3
5	5	3	(1)	6	4	2
6	6	5	4	3	2	(1)

Como $bd = 1 \Rightarrow$

$b = d = 1$

o bien

$b = 2$ y $d = 4$

o bien

$b = 3$ y $d = 5$

o bien

$b = d = 6$

Si $b = d = 1 \Rightarrow \begin{cases} a+c = 0 \\ 2+ac = 0 \end{cases} \Rightarrow \begin{cases} a = -c \\ 2-c^2 = 0 \end{cases}$ luego $c^2 = 2$

Así $c = 3$ ó $c = 4$

$(-3 = 4$ y $-4 = 3)$

Luego $x^4+1 = (x^2+4x+1)(x^2+3x+1)$. ∎

PROBLEMA 6: $f(p/q) = a_n \frac{p^n}{q^n} + \cdots + a_1 \frac{p}{q} + a_0 = 0 \Rightarrow$

$\Rightarrow a_n p^n + \cdots + a_1 p q^{n-1} + a_0 q^n = 0 \Rightarrow a_0 q^n = p(-a_n p^{n-1} \cdots - a_1 q^{n-1})$

Como $p \nmid q$ por ser p/q irreducible entonces $p \mid a_0$

Por otra lado $a_n p^n = q(-a_{n-1} p^{n-1} - \cdots - a_1 p q^{n-2} + a_0 q^{n-1})$

Así $q \mid a_n p^n$ y como $q \nmid p \Rightarrow q \mid a_n$. ∎

Sea $f(x) = 3x^3 + 4x^2 + 2x - 4 \in \mathbb{Z}[x]$ $-4, -2, -1, 1, 2$ y 4 posibles raíces enteras; o bien en la parte anterior $2/3$; $-2/3$; $-4/3$ ó $-4/3$ posibles raíces racionales; $f(2/3) = \frac{8}{9} + 4\frac{4}{9} + \frac{4}{3} - 4 = \frac{8+16+12}{9} - \frac{36}{9} = 0$

AM

Hoja 8:

PROBLEMA 8: $I = \{ f(x) \in \mathbb{Z}[x] : f(0) \in 3\mathbb{Z} \}$

Si $f \in I \Rightarrow -f(0) \in \mathbb{Z}$.

Si $f, g \in I \quad (f-g)(0) = f(0) - g(0) \in 3\mathbb{Z}$

Además para $f \in I$ y $\forall g \in \mathbb{Z}[x]$

$f \cdot g(0) = f(0) \cdot g(0)$ Si $f(0)$ es múltiplo de 3 entonces $f(0) \cdot g(0)$ también.

Con todo esto podemos ver que I es un ideal.

a) $I = \langle x, 3 \rangle$ veámoslo.

$f(x) = 3 \in \mathbb{Z}[x]$ y $f(0) = 3 \in 3\mathbb{Z}$

$g(x) = x \in \mathbb{Z}[x]$ y $g(0) = 0 \in 3\mathbb{Z}$

Luego $x, 3 \in I$; luego $\langle x, 3 \rangle \subseteq I$ por ser I ideal

Ahora si $h \in I \quad h(x) = \sum_{j=0}^{n} a_j x^j$

$a_j x^j = a_j x^{j-1} x \in \langle x, 3 \rangle$ por ser $\langle x, 3 \rangle$ ideal

$j \geq 1$

$h(0) = a_0 = 3n \in \langle x, 3 \rangle$

Luego $h \in \langle x, 3 \rangle$; así $\langle x, 3 \rangle = I$

$\mathbb{Z}$ no es un cuerpo por tanto $\mathbb{Z}[x]$ no $\mathbb{Z}$ no es un dominio de ideales tiene por que ser un dominio de ideales principales; de hecho, como no hemos visto, no lo es.

b) $\psi \quad \mathbb{Z}[x] \to \mathbb{Z}_3$
$f \to \psi(f) = [f(0)]_3$

$$\begin{cases} [f+g(0)]_3 = [f(0)]_3 + [g(0)]_3 \\ [f \cdot g(0)]_3 = [f(0)]_3 [g(0)]_3 \end{cases}$$

Luego ψ es un homomorfismo de anillos.

$\mathbb{Z}[x]$ y $\mathbb{Z}_3$ son claramente unitarios y $f = 1 \quad \psi(1) = [1]_3$.

$\ker \psi = \{ f \in \mathbb{Z}[x] : \psi(f) = [f(0)]_3 = 0 \} = I \quad [f(0)]_3 = 0 \Leftrightarrow f(0) \in 3\mathbb{Z}$.

Claramente ψ es un epimorfismo y $\operatorname{Im} \psi = \mathbb{Z}_3$

por el teorema de isomorfía $\frac{\mathbb{Z}}{\ker \psi} = \frac{\mathbb{Z}[x]}{I} \cong \mathbb{Z}_3$.

AM

HOJA 8:

PROBLEMA 9:

$f \in \mathbb{Q}[x]$ IRREDUCIBLE Y $a \in \mathbb{C}$ CON $f(a)=0$

a) $eva: \mathbb{Q}[x] \longrightarrow \mathbb{C}$

$h \longrightarrow eva(h) = h(a)$

eva ES CLARAMENTE UN HOMOMORFISMO DE ANILLOS

$\ker(eva) = \{h \in \mathbb{Q}[x] : h(a)=0\} = (f)$? $(\subseteq f)$

IDEAL GENERADO POR f EN $\mathbb{Q}[x]$)

$\langle f \rangle = \{ gf : g \in \mathbb{Q}[x] \}$.

POR TANTO $\forall h \in \langle f \rangle$, $h = gf \Rightarrow h(a) = g(a)f(a) = 0$

LUEGO $h \in \ker eva$

POR SER f IRREDUCIBLE, $\langle f \rangle$ ES UN IDEAL MAXIMAL Y $\langle f \rangle \subseteq \ker eva$ QUE ES OTRO IDEAL LUEGO $\ker eva = \mathbb{Q}[x]$ O CUAL NO ES POSIBLE ASI QUE $\langle f \rangle = \ker eva$

b) SI $g \in \mathbb{Q}[x]$ Y $g(a)=0 \Rightarrow g \in \ker eva = \langle f \rangle$

LUEGO $\exists h \in \mathbb{Q}[x]$ TAL QUE $g = h \cdot f$ Y ASI $f \mid g$ c.q.d.

AM

HOJA 8:

PROBLEMA 11:

$f(x) = 4x^2 - 12 \in \mathbb{Z}[x]$ como $4x^2 - 12 = 0 \iff x^2 = 3$

f es irreducible en $\mathbb{Q}[x]$ y sus raíces en $\mathbb{Z}[x]$.

En cambio $f(x) \in \mathbb{R}[x]$ aquí existen $\pm\sqrt{3} \in \mathbb{R}$

y $f(x) = (x - \sqrt{3})(x + \sqrt{3})$.

$\mathbb{R}[x]/(f)$ es un anillo, pero no es un cuerpo ya que hay divisores de cero:

$[x - \sqrt{3}] \in \mathbb{R}[x]/(f) \setminus \{0\}$ y son no nulos

$[x + \sqrt{3}] \in \mathbb{R}[x]/(f) \setminus \{0\}$

$[x - \sqrt{3}] \cdot [x + \sqrt{3}] = [(x - \sqrt{3})(x + \sqrt{3})] = [x^2 - 3] \equiv 0$.

(concordancias)

Como f es irreducible en $\mathbb{Q}[x]$, $\mathbb{Q}[x]/(f)$ es un cuerpo; además es un espacio vectorial sobre el cuerpo $\mathbb{Q}$ de dimensión 2, con una base $\{1, \alpha\}$ con $\alpha^2 = 3$

Así $\mathbb{Q}[x]/(f) = \{a + b\alpha : a, b \in \mathbb{Q}\}$ con $\alpha^2 = 3$

Así $\dim \mathbb{Q}[x]/(f) = 2$

Como $\mathbb{Q} \hookrightarrow \mathbb{Q}[x]/(f)$ $\operatorname{Char} \mathbb{Q}[x]/(f) = 0$

Por otro lado el cuerpo $\mathbb{Q}[\sqrt{3}] = \{a + \sqrt{3}b : a, b \in \mathbb{Q}\}$ (ejercicio 1), es un cuerpo cualquiera de característica 0 igual (isomorfo) a $\mathbb{Q}[x]/(f)$;

Así $\mathbb{Q} \hookrightarrow \mathbb{Q}[x]/(f) = \mathbb{Q}[\sqrt{3}] \hookrightarrow \mathbb{R}$.

AM

HOJA 8:

PROBLEMA 13: b) Sea $f(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$

$f(0) = 1$, $f(1) = 1$; luego f no tiene raíces en $\mathbb{Z}_2$ y por tanto es irreducible (no se puede factorizar como producto de polinomios de grado 1 y 2.).

Por el teorema de Kronecker $\mathbb{Z}_2[x]/f =$

$$= \{ a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Z}_2 \}$$ (es un cuerpo

con $\alpha^3 + \alpha^2 + 1 = 0$; que tiene a $\mathbb{Z}_2$ como subcuerpo

$\text{Char. } \mathbb{Z}_2[x]/f = 2$

$\dim(\mathbb{Z}_2[x]/f, \mathbb{Z}_2) = 3$ y $\text{Card } \mathbb{Z}_2[x]/f = 8$

$$\mathbb{Z}_2[x]/f = \{0, 1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$$

$\alpha^3 = -\alpha^2 - 1 = \alpha^2 + 1$.

$\alpha^4 = \alpha\alpha^3 = \alpha(\alpha^2+1) = \alpha^3 + \alpha = \alpha^2 + \alpha + 1$

TABLAS DE OPERACIONES

+	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
1	1	0	$1+\alpha$	α	$1+\alpha^2$	α^2	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$
α	α	$1+\alpha$	0	1	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	α^2	$1+\alpha^2$
$1+\alpha$	$1+\alpha$	α	1	0	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha^2$	α^2
α^2	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	0	1	α	$1+\alpha$
$1+\alpha^2$	$1+\alpha^2$	α^2	$\alpha+\alpha^2$	$\alpha+\alpha^2$	1	0	$1+\alpha$	α
$\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	α^2	$1+\alpha^2$	α	$1+\alpha$	0	1
$1+\alpha+\alpha^2$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha^2$	α^2	$1+\alpha$	α	1	0

LA MATRIZ ANTISIMÉTRICA ES LA CARACTERÍSTICA DE $\mathbb{Z}_2[x]/f$ ES 2.

X	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0	0	0	0	0	0	0	0	0
1	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
α	0	α	α^2	$\alpha+\alpha^2$	α^2+1	$1+\alpha+\alpha^2$	1	$1+\alpha$
$1+\alpha$	0	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha^2$	1	α	$1+\alpha+\alpha^2$	α^2
α^2	0	α^2	α^2+1	1	$1+\alpha+\alpha^2$	$1+\alpha$	α	$\alpha+\alpha^2$
$1+\alpha^2$	0	$1+\alpha^2$	$1+\alpha+\alpha^2$	α	$1+\alpha$	$\alpha^2+\alpha$	$\alpha+\alpha^2$	1
$\alpha+\alpha^2$	0	$\alpha+\alpha^2$	1	$1+\alpha+\alpha^2$	α	$\alpha+\alpha^2$	$1+\alpha$	α^2
$1+\alpha+\alpha^2$	0	$1+\alpha+\alpha^2$	$1+\alpha$	α^2	$\alpha+\alpha^2$	1	α^2	α

PROBLEMA 14: Sea $\mathbb{Z}_2[x]$, vamos a tomar un polinomio irreducible de $\mathbb{Z}_2[x]$ de grado tres (uno que no tenga raíces en $\mathbb{Z}_2$); sirve $x^3 + x^2 + 1$ (mirar el ejercicio 2)

Luego $\mathbb{Z}_2[x]/(x^3+x^2+1) = \{0, 1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$.

es un cuerpo de $\alpha^3 = \alpha^2 + 1$ extendiendo con característica 2 ya que $\mathbb{Z}_2 \hookrightarrow \mathbb{Z}_2[x]/(x^3+x^2+1)$

AM

MOJA 8:

PROBLEMA 15:

$f(x) = x^3 - x^2 + x - 1 \in \mathbb{Q}[x]$ no es irreducible

ya que $x = 1$ es raíz; así

$$f(x) = (x-1)(x^2+1)$$

$x^3 - x^2 + x - 1 \;\big|\; x-1$ / $x^2 + 1$

$-x^3 + x^2$

$0 \quad x - 1$

luego $[x-1], [x^2+1] \in \mathbb{Q}[x]/_{x^3-x^2+x-1}$

y no son nulos ya que $f \nmid x-1$ y $f \nmid x^2+1$.

sin embargo $[x-1] \cdot [x^2+1] = [(x-1)(x^2+1)] = [f] = 0$

ambos son divisores de cero.

- - -

por otro lado $\alpha = [x]$ tiene inverso en $\mathbb{Q}[x]/_{x^3-x^2+x-1}$

ya que $x \nmid f$ así

$$m.c.d.(x, f(x)) = 1$$

luego por el lema de bezout $\exists\, u, v \in \mathbb{Q}[x]$ tal

$$1 = v(x)\, x + u(x)\, f(x)$$

luego $[1] = [v(x)\, x + u(x)\, f(x)] = [v(x)][x] + [u(x) f(x)] =$

$$= [v(x)][x]$$

por tanto $[x]^{-1} = [v(x)]$

de forma precisa, aplicando el algoritmo de

euclides, o también

$$(x^3 - x^2 + x - 1) + 1 = x^3 - x^2 + x = (x^2 - x + 1)\, x$$

luego $(x^2 - x + 1)\, x - (x^3 - x^2 + x - 1) = 1$

así $[x]^{-1} = [x^2 - x + 1]$

PROBLEMA 16: $f(x) = x^2 + x - 1 \in \mathbb{Z}_3[x]$ $\begin{cases} \bar{f}(0) = -1 \\ \bar{f}(1) = 1 \\ \bar{f}(2) = 4 + 2 - 1 = 2 \end{cases}$

como no tiene raíces en $\mathbb{Z}_3$ y es de grado 2 es irreducible; por tanto $\mathbb{Z}_3[x]/_f$ es un cuerpo finito formado únicamente por 9 clases y todos sus elementos tienen inverso

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

$x^4 + x^3 + x^2 + x \;\big|\; x^2 + x - 1$ / $x^2 + 2$

$-x^4 - x^3 + x^2$

$2x^2 + x$

$-2x^2 - 2x + 2$

$-x + 2$

así $[x^4 + x^3 + x^2 + x] = [-x+2] = [2x+2] = 2[x+1]$

podemos usar el lema de bezout

$x^2 + x - 1 + 1 = x^2 + x = x(x+1)$. luego $[x+1]^{-1} = [x]$

y $(2[x+1])^{-1} = 2[x]$ ($2 \cdot 2 = 1$ en $\mathbb{Z}_3$).

AM

Hoja 8ª

PROBLEMA 1ª) Sea la aplicación.

$$\Psi : \mathbb{Z}_n[x]/x^2-x \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_n$$

$$a+b[x] \longrightarrow \Psi(a+b[x]) = (a+b, a)$$

Veamos que Ψ es un isomorfismo de anillos

Como Grad $x^2-x = 2$ $\mathbb{Z}_n[x]/x^2-x$ es un espacio vectorial sobre el cuerpo $\mathbb{Z}_n$ (n primo), de dimensión dos; así

$$\mathbb{Z}_n[x]/x^2-x = \{ a+b[x] : a, b \in \mathbb{Z}_n \}$$

Luego como $a+b \in \mathbb{Z}_n$ y $b \in \mathbb{Z}_n$

$\Psi(a+b[x]) \in \mathbb{Z}_n \times \mathbb{Z}_n$ está bien definida

*) Ψ es un homomorfismo de anillos, ya que:

$$\Psi((a+b[x]) + (c+d[x])) = \Psi((a+c) + (b+d)[x]) =$$

$$= ((a+c)+(b+d), a+c) \underset{\mathbb{Z}_n \times \mathbb{Z}_n}{=} (a+b, a) + (c+d, c) =$$

$$= \Psi(a+b[x]) + \Psi(c+d[x])$$

Además $\Psi((a+b[x])(c+d[x])) = \Psi(ac + (ad+cb)[x] + bd[x]^2) =$

$$= \Psi(ac + (ad+cb+bd)[x]) =$$

$[x^2-x] = [x^2] - [x] \equiv 0$

Luego $[x]^2 = [x]$

$$= (ac + ad + cb + bd, ac) \underset{\mathbb{Z}_n \times \mathbb{Z}_n}{=}$$

$$= (a+b, a) \times (c+d, c) =$$

$$= \Psi(a+b[x]) \cdot \Psi(c+d[x])$$

**) Ψ es inyectiva; ya que si $(a+b, a) = (a'+b', a')$

$\Rightarrow a = a'$ y $a+b = a'+b' \Rightarrow b = b'$.

Ψ es sobreyectiva; ya que si $(r, s) \in \mathbb{Z}_n \times \mathbb{Z}_n$

se tiene que $s + (r-s)[x] \in \mathbb{Z}_n[x]/f$ y

$$\Psi(s + (r-s)[x]) = (r-s+s, s) = (r, s).$$

Luego Ψ es un homomorfismo biyectivo y por tanto es un isomorfismo.

AM

HOJA 8ª

PROBLEMA 19:] LOS SEIS ANILLOS SIGUIENTES

$\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_2[x]/x^2+x+1$, $\mathbb{Z}_2[x]/x^3+x+1$, $\mathbb{Z}_2[x]/x^3+x^2+1$

Y $\mathbb{Z}_2[x]/x^2$ SON DOS A DOS ANILLOS FINITOS.

DE CARDINAL 4 SON

$\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_2[x]/x^2+x+1$ Y $\mathbb{Z}_2[x]/x^2$

LUEGO ENTRE ESTOS PUEDE HABER UN ISOMORFISMO

DE CARDINAL 8 SON

$\mathbb{Z}_2[x]/x^3+x+1$ Y $\mathbb{Z}_2[x]/x^3+x^2+1$.

QUE EVENTUALMENTE PODRÍAN SER ISOMORFOS

*) VEAMOS SI ESTOS ÚLTIMOS SON ISOMORFOS.

TANTO x^3+x+1 COMO x^3+x^2+1 SON IRREDUCIBLES EN $\mathbb{Z}_2$ PUES QUE TIENE GRADO TRES Y $x=0$ ó 1 NO SON RAÍCES.

POR TANTO $\mathbb{Z}_2[x]/x^3+x+1$ Y $\mathbb{Z}_2[x]/x^3+x^2+1$ SON CUERPOS DEL MISMO CARDINAL FINITO; POR TANTO SON ISOMORFOS; VER TEORÍA.

**) EN CUANTO A LOS ANILLOS DE 4 ELEMENTOS

- $\mathbb{Z}_4 \neq \mathbb{Z}_2 \times \mathbb{Z}_2$ YA QUE $\mathbb{Z}_4$ ES UN GRUPO CÍCLICO CON LA SUMA Y $\mathbb{Z}_2 \times \mathbb{Z}_2$ NO LO ES (VER TEORÍA DE GRUPOS) ADEMÁS TANTO $\mathbb{Z}_4$ COMO $\mathbb{Z}_2 \times \mathbb{Z}_2$ NO SON CUERPOS!
- $x^2+x+1 \in \mathbb{Z}_2[x]$; POR SER DE GRADO DOS Y NO TENER RAÍCES EN $\mathbb{Z}_2$, ES IRREDUCIBLE POR TANTO $\mathbb{Z}_2[x]/x^2+x+1$ ES UN CUERPO
- ASÍ $\mathbb{Z}_2[x]/x^2+x+1$ NO ES ISOMORFO NI A $\mathbb{Z}_4$, NI A $\mathbb{Z}_2 \times \mathbb{Z}_2$ NI A $\mathbb{Z}_2[x]/x^2$ YA QUE NINGUNO DE ESTOS TRES ES UN CUERPO ($x^2+\mathbb{Z}_2[x]$ NO ES IRREDUCIBLE)
- $(\mathbb{Z}_2[x]/x^2+)$ ES UN GRUPO CONMUTATIVO DE 4 ELEMENTOS LUEGO POR LA CLASIFICACIÓN DE GRUPOS CONMUTATIVOS $(\mathbb{Z}_2[x]/x^2+) \simeq (\mathbb{Z}_4+)$ Ó BIEN $(\mathbb{Z}_2[x]/x^2+) \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2+)$

AM

HOJA 8:

PROBLEMA 19: (continuación)

VEAMOS LAS OPERACIONES EN $\mathbb{Z}_2[x]/x^2 = \{0, 1, x, 1+x\}$.

CON $x^2 = 0$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	1+x	x
x	x	1+x	0	1
x+1	x+1	x	1	0

·	0	1	x	x+1
0				
1		1	x	x+1
x		x	0	x
x+1		x+1	1	1

$(\mathbb{Z}_2[x]/x^2, +) \not\cong (\mathbb{Z}_2, +)$ YA QUE EL PRIMERO NO ES CÍCLICO; $\forall a \in \mathbb{Z}_2[x]/x^2$ SE TIENE QUE $a+a=0$

POR TANTO $(\mathbb{Z}_2[x]/x^2, +) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

EN $(\mathbb{Z}_2[x]/x^2, \cdot)$ HAY DIVISORES DE CERO ($x \cdot x = 0$) Y ES MÁS x ES NILPOTENTE

EN $(\mathbb{Z}_2 \times \mathbb{Z}_2, \cdot)$ NO HAY ELEMENTOS NILPOTENTES

(SI $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ CON $a \neq 0$ Y $b \neq 0 \Rightarrow$
$(a,b) \cdot (a,b) = (a^2, b^2)$ Y ADEMÁS Y $a^2 \neq 0$ Y $b^2 \neq 0$)

LUEGO $\mathbb{Z}_2[x]/x^2 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$ COMO ANILLOS.

AM

HOJA 8:

PROBLEMA 20] BUSCAMOS $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Z}_7[x]$

DE MODO QUE $f(1) = 0$, $f(3) = 1$, $f(4) = 2$ Y $f(6) = 0$

DOS FORMAS DE ENCONTRAR f

1:] PLANTEANDO UN SISTEMA LINEAL DE 4 ECUACIONES CON 4 INCÓGNITAS

$$f(1)=0 \iff 0 = a + b + c + d.$$
$$f(3)=1 \iff 1 = a3^3 + b3^2 + c3 + d$$
$$f(4)=2 \iff 2 = a4^3 + b4^2 + c4 + d \quad (*)$$
$$f(6)=0 \iff 0 = a6^3 + b6^2 + c6 + d$$

$$\iff \begin{pmatrix} 0 \\ 1 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 3^3 & 3^2 & 3^1 & 3^0 \\ 4^3 & 4^2 & 4 & 4^0 \\ 6^3 & 6^3 & 6 & 6^0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

SISTEMA PLANTEADO EN EL CUERPO VECTORIAL $\mathbb{Z}_7$

SOBRE EL CUERPO $\mathbb{Z}_7$, Y EL DETERMINANTE

DE VANDERMONDE $\begin{vmatrix} 1 & 1 & 1 & 1 \\ 3^3 & 3^2 & 3 & 1 \\ 4^3 & 4^2 & 4 & 1 \\ 6^3 & 6^2 & 6 & 1 \end{vmatrix} \neq 0$ YA QUE 1, 3, 4 Y 6 SON DISTINTOS ENTRE SÍ

POR TANTO EL SISTEMA TIENE SOLUCIÓN ÚNICA

(SOLO NECESITAMOS PARA ELLO TENER 4 ECUACIONES DE f EN 4 PUNTOS DISTINTOS).

ASÍ $(*) \iff$ EN $\mathbb{Z}_7$

$$0 = a + b + c + d$$
$$1 = 6a + 2b + 3c + d$$
$$2 = a + 2b + 4c + d$$
$$0 = 6a + b + 6c + d.$$

$\iff$ GAUSS

$$0 = a + b + c + d$$
$$1 = 5a + b + 2c$$
$$2 = b + 3c$$
$$0 = 5a + 5c$$

$\iff$ GAUSS

$$0 = a + b + c + d.$$
$$1 = 5a + b + 2c$$
$$2 = b + 3c$$
$$6 = 6b + 3c$$

$\iff$

$$0 = a + b + c + d$$
$$1 = 5a + b + 2c$$
$$2 = b + 3c$$
$$1 = 6c$$

$\iff$

$c = 6$

LUEGO $b = 2 - 18 = 5$

$5a = 1 - 5 - 12 = -16 = 5 \mod 7$

$a = 1$

$d = -1 - 5 - 6 \equiv 2 \mod 7$

LUEGO EL POLINOMIO BUSCADO ES

$$\boxed{x^3 + 5x^2 + 6x + 2}$$

36 | 6 | 216 LT | 06 30

$\mathbb{Z}_7^*$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

AM

HOJA 8:

PROBLEMA 20: (CONTINUACIÓN)

2c) OTRA FORMA DE HACER ESTE PROBLEMA ES USANDO LA FÓRMULA DE INTERPOLACIÓN DE LAGRANGE (VER TEORÍA SOBRE POLINOMIOS)

SEAN $(1,0)$ $(3,1)$ $(4,2)$ Y $(6,0)$

(a_0,b_0) (a_1,b_1) (a_2,b_2) Y (a_3,b_3)

ESTA $p(x) = b_0 \times p_0 + b_1 p_1 + b_2 p_2 + b_3 p_3 =$

$= 0 \times p_0 + p_1 + 2p_2 + 0\, p_3 =$

↓ EN NUESTRO EJEMPLO

$= p_1 + 2p_2$

DONDE $p_i = \dfrac{\prod_{\substack{j=1 \\ j\neq i}}^{n} (x - a_j)}{\prod_{\substack{j=1 \\ j\neq i}}^{n} (a_i - a_j)}$ $i = 1, 2, \dots, n.$ (EN NUESTRO CASO $n=3$)

OBSERVACIÓN $\left(p_i(a_j) = \begin{cases} 0 & \text{SI } i \neq j \\ 1 & \text{SI } i = j \end{cases} \right)$

EN NUESTRO CASO

$$p_1 = \frac{(x-1)(x-4)(x-6)}{(3-1)(3-4)(3-6)} = \frac{(x^2-5x+4)(x-6)}{6}$$

$$p_2 = \frac{(x-1)(x-3)(x-6)}{(4-1)(4-3)(4-6)} = \frac{(x^2-4x+3)(x-6)}{-2}$$

ASÍ $p = \frac{1}{6}(x^3 - 5x^2 + 4x - 6x^2 + 30x - 36) + 2(x^3 - 4x^2 + 3x - 6x^2 + 24x - 24)$

$= 6(x^3 - 4x^2 + 6x - 3) + 2(x^3 - 3x^2 + 6x - 4) =$

$= 6x^3 - 3x^2 + x - 4 + 2x^3 - 6x^2 + 5x - 1 =$

$= x^3 + 5x^2 + 6x + 2$

TOMAS LAS OPERACIONES EN $\mathbb{Z}_7$

PROBLEMA 22: b) $\mathbb{F}_{25} = \mathbb{Z}_5[x]/x^2+2x+2$; $(\mathbb{F}_{25}^* \times)$ ES UN GRUPO CÍCLICO DE ORDEN 24 (VER TEORÍA); LUEGO $\forall a \in \mathbb{F}_{25}^*$ $a^{24} = 1$

ASÍ $[x] \in \mathbb{Z}_5[x]/x^2+2x+2$; $1300 = 24 \times 54 + 12$

LUEGO $[x]^{1300} = [x]^{24\times 54}[x]^{12} = [x]^{12} = [x^2]^6 = [-2x-2]^6 = [3x+1]^6 = [9x^2+6x+1]^3 =$

$= [4x^2+x+1]^3 = [-8x-16+x-1]^3 = [3x+3]^3 =$ ... ele

($x^2+2x+2=0$ ↓ $\mathbb{Z}_5$; ↓ $\mathbb{Z}_5$)