

PR 2019

1.

a) Conjunto $S = \left\{ \begin{pmatrix} x & 2y \\ -y & x \end{pmatrix} : x, y \in \mathbb{Z}_4 \right\}$, es un subanillo $(\mathbb{Z}^{2 \times 2}, +, \cdot)$. Estudiar.

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

Si es subanillo

$$\begin{pmatrix} x & 2y \\ -y & x \end{pmatrix} \cdot \begin{pmatrix} x' & 2y' \\ -y' & x' \end{pmatrix} = \begin{pmatrix} xx'-2yy' & 2xy'+2xx' \\ -yx'-xy' & -2yy'+xx' \end{pmatrix} \in S$$

b) Obtener los mínimos, máximos de div. y rest. del anillo $(R, +, \cdot, 0)$ con $R = \{0, 5, 10, 15\}$

$\text{Un}_R = \{5, 15\} \Rightarrow$ unidades

$$\text{div}_R = \{10\} \Rightarrow \text{div. de cero} \Rightarrow \frac{20}{10} = \text{resto cero}$$

$\text{char}(R) = 4 \Rightarrow$ características (orden, mcm)

2.

a) Estudiar si $15\mathbb{Z}/30\mathbb{Z}$ tiene estructura de anillo compatible con la del anillo $(15\mathbb{Z}, +, \cdot)$. Afirmar \Rightarrow Todos los operadores y ax. si es cuerpo.

$$I = 30\mathbb{Z} = \mathbb{Z} \Rightarrow \text{ideal de } 15\mathbb{Z}, \text{ entero.}$$

$15\mathbb{Z}/30\mathbb{Z} = \{[0], [15]\}^4$ tiene una estructura de anillo compatible con la de $(15\mathbb{Z}, +, \cdot)$

Es un ideal maximal y por tanto es cuerpo.

+	[0]	[15]
[0]	[0]	[15]
[15]	[15]	[0]

*	[0]	[15]
[0]	[0]	[0]
[15]	[0]	[15]

b) Obtener los máximos y mínimos de $\mathbb{Z}_4 \times \mathbb{Z}_6$

$$([2]_4) \times [2]_6 \Rightarrow \text{con } \mathbb{Z}_4 \Rightarrow [0]_4 \sqcup [2]_4$$

2×3 sale de que
 $4 = 2^2 \Rightarrow 6 = 2 \cdot 3$

$$\mathbb{Z}_4 \times ([2]_6) \Rightarrow \{ \text{con } \mathbb{Z}_6 \}$$

$$\mathbb{Z}_4 \times ([3]_6) \Rightarrow \{ \text{con } \mathbb{Z}_6 \}$$



Resolutor.

6. Dem. intersección de 2 ideales, de un mismo anillo, es un ideal

Sea $(R, +, \cdot)$ anillo y sean I y J ideales, entonces $a \in I$ y $b \in J$
x tanto $a, b \in I \cap J \Rightarrow I \cap J \neq \emptyset$. & $x, y \in I \cap J \Rightarrow x, y \in I$ y $x, y \in J \Rightarrow x-y \in I$ y $x-y \in J \Rightarrow x-y \in I \cap J$. Si $x \in I \cap J$ y $r \in R \Rightarrow x \in I$ y $x \in J \Rightarrow rx, xr \in I$ y $rx, xr \in J$. Por tanto $I \cap J$ es un ideal.

7. $x^5 - x^2 + 1$ es irreducible en $\mathbb{Q}[x]$?

$$\begin{array}{c|ccccc} 1 & 0 & 0 & -1 & 0 & 1 \\ -1 & & -1 & 1 & -1 & 0 \\ \hline 1 & -1 & 1 & -1 & 0 & -1 \end{array} \left. \begin{array}{l} \text{No tiene raíces} \\ \text{y no divisible por } x^2 + x + 1 \end{array} \right\}$$

$$\begin{array}{c} x^5 \\ -x^5 - x^4 - x^3 \\ \hline -x^4 - x^3 - x^2 \\ \hline -x^2 - x \\ \hline x^2 + x + 1 \\ \hline x^2 - x^2 \\ \hline 1 \end{array}$$

Es irreducible.

8. Dados resultados $F_3 = \mathbb{Q}[x]/(x^2 + x + 2) : (x + 1)x^{-1}$

$$X \quad \begin{array}{c} \text{Gráfico de } F_3 \text{ en } \mathbb{C} \\ \text{B} \in \mathbb{A} \text{ en } x \\ \text{No divisible} \end{array} \quad \begin{array}{c} \text{y la forma canónica base} \\ \text{de } F_3 \text{ es } x^2 + x + 2 \end{array}$$

$$x^{-1} = \begin{cases} x^2 + x + 2 = x(x + 1) + 2 \\ x = (x + 1) \cdot 1 - 2 \end{cases} \quad \begin{array}{c} x^2 + x + 2 \mid x \\ -x - x - 2 - x^2 - x^1 - x^0 \\ \hline 2x - 2 \end{array} \quad (2)$$

$$\therefore -2 = x - (x + 1)$$

$$-2 = x - [(x^2 - x + 2) - x \cdot x] = x + x - 2 = 2x - 2$$

$$\begin{array}{c} x^2 = x + 1 \\ \hline 2x - 2 \end{array}$$

$$\text{en } \mathbb{F}_3 \quad x^2 + x + 2$$

$$\boxed{x^2}$$

$$x^2 = \begin{cases} x^2(x+1) = x^3 + x = 2x + 1 + x = \boxed{2x + 1} \end{cases}$$

y ya sigue.

9. Base de $\mathbb{Q}(\alpha)$ sobre \mathbb{Q} en $\alpha = \sqrt{5} - \sqrt{2}$

$$B = \{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$$

mem

10. Polinomio mínimo $\Rightarrow \alpha = \sqrt{5} - \sqrt{2}$

$$\alpha = \sqrt{5} - \sqrt{2} \Rightarrow \alpha + \sqrt{2} = \sqrt{5} \Rightarrow (\alpha + \sqrt{2})^2 = 5 \Rightarrow$$

$$\Rightarrow \alpha^2 + 2\sqrt{2}\alpha + 2 = 5 \Rightarrow \alpha^2 + 2 - 5 = -2\sqrt{2}\alpha \Rightarrow (\alpha^2 - 3)^2 = (-2\sqrt{2}\alpha)^2 \Rightarrow$$

$$\Rightarrow \alpha^4 - 6\alpha^2 + 9 = 4 \cdot 2 \cdot \alpha^2 \Rightarrow \alpha^4 - 6\alpha^2 + 9 = 8\alpha^2 \Rightarrow \boxed{\alpha^4 - 14\alpha^2 + 9}$$

en x.

5.

a.) Obtener una base de extensión de $\alpha = \sqrt[6]{7}$ sobre \mathbb{Q}

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[6]{7}) \subset \mathbb{Q}(\sqrt[3]{7}) \subset \mathbb{Q}(\sqrt[3]{7}) \subset \mathbb{Q}(\sqrt[3]{7})$$

$$B = \{1, \sqrt[6]{7}, \sqrt[3]{7}, \sqrt[3]{7^2}, \sqrt[3]{7^3}\}$$

$\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q} = 6 \Rightarrow$ no dom. base

b) Sea $h = x^2 + x + 1 \in \mathbb{K}[x]$. Justifica que $\mathbb{K}[x]/(h)$ es un cuerpo e indica sus elementos.

$$x^2 + x + 1 = 0 \Rightarrow x = \frac{-1 \pm \sqrt{1-4}}{2} \Rightarrow \text{Es irreducible (no raíces) en } \mathbb{K}$$

Tiene grado 2.

c.) Obtener en $\mathbb{K}[x]/(h)$ el resultado de la sig. op. $x^3(x^2+1)$

$$\begin{array}{r} x^5 + x^3 \rightarrow x^5 + x^3 \\ -x^5 - x^4 - x^3 \\ \hline x^4 + x^3 + x^2 \\ -x^4 - x^3 - x \\ \hline \end{array} \quad \begin{array}{c} |x^2 + x + 1 \\ \hline x^3 - x^2 + x \end{array}$$

$$x^5 + x^3 = (x^2 + x + 1)(x^3 - x^2 + x) - x$$

i?

Why

d.) Obtener en $\mathbb{K}[x]/(h)$ el dominio: $(x+2)^{-1}$

$$h = x^2 + x + 1$$

$$(x+2)^{-1}$$

j?

$$\begin{array}{r} x^2 + x + 1 \quad |x+2 \\ -x^2 - 2x \\ \hline -x + 1 \\ +x + 2 \\ \hline 3 \end{array}$$

$$\begin{aligned} x^2 + x + 1 &= (x+2)(x-1) + 3 \Rightarrow \\ \Rightarrow 3 &= \frac{x^2 + x + 1}{(x+2)(x-1)} \end{aligned}$$

MAL OPERADO

3. Estudiar si aplicación $\varphi: \mathbb{Z}_{40} \rightarrow \mathbb{Z}_{24}$ definida por $\varphi(x) = 9x$ es un homomorfismo de anillos. Si yes \Rightarrow obtener imágenes y el núcleo. Calcular el cociente $\mathbb{Z}_{40}/\text{ker } (\varphi)$ e indicar si $\text{ker } (\varphi)$ es un ideal maximal.

$$\begin{array}{l|l} \text{Si es homomorfismo} & 40 \cdot 9 \equiv 0 \pmod{24} \\ \not\rightarrow \text{anillos} & 9^2 \equiv 9 \pmod{24} \end{array}$$

$$\text{im } (\varphi) = \{0, 3, 6, 9, 12, 15, 18, 21\} = ([3]_{24})$$

$$\text{ker } (\varphi) = \{0, 8, 16, 24, 32\} = ([8]_{40})$$

$\mathbb{Z}_{40}/([8]_{40}) \cong ([3]_{24})$, que no es cuerpo ya que tiene divisores de cero ($[12]_{24} \cdot [12]_{24} = [0]_{24}$), x tanto $\text{ker } (\varphi)$ no es maximal.

4.

a) Polinomio de $\mathbb{Q}[x]$, que es máximo común divisor de los polinomios $f = x^5 + x^4 + x^3 + 2x^2 + 2x + 2 \in \mathbb{Q}[x]$ y $g = x^4 + x^3 - x - 1 \in \mathbb{Q}[x]$. Expressar d como comb. lineal de f y g.

b) Polinomio mínimo de $\alpha = \sqrt[4]{5+\sqrt{5}}$ sobre el cuerpo \mathbb{Q}

$$\begin{aligned} \alpha = \sqrt[4]{5+\sqrt{5}} &\Rightarrow \alpha^4 = 5 + \sqrt{5} \Rightarrow \alpha^4 - 5 = \sqrt{5} \Rightarrow \\ &\Rightarrow (\alpha^4 - 5)^2 = 5 \Rightarrow \alpha^8 - 10\alpha^4 + 25 = 5 \Rightarrow \\ &\Rightarrow \alpha^8 - 10\alpha^4 + 20 = 0 \Rightarrow \text{Polinomio mínimo } | x^8 - 10x^4 + 20 = 0 \end{aligned}$$

x ej: p=5 (primo) IRREDUCIBLE x EISENSTEIN

$$(511, 510, 510, 510, 51-10, 510, 510, 510, 5120) \wedge (5^2 \nmid 20)$$



	A	ME	3E
Obj	200	1000	0
Arte	0	400	250

$$\left\{ \begin{array}{l} \text{Objetivo 1500 €} \\ \text{Arte 2000 €} \\ \\ \left\{ \begin{array}{l} A 1000 \text{ art} \\ ME 1200 \text{ art} \\ 3E 800 \text{ art} \end{array} \right. \end{array} \right.$$

a)

$$x_1 = \text{nº conc. objetivo}$$

$$x_2 = \text{nº de esp. arte}$$

$$\min z = p_1(\Delta_1^+) + p_2(\Delta_2^-) + p_3(3\Delta_3^- + \Delta_4^-)$$

s.a.

$$15x_1 + 30x_2 + \Delta_1^- - \Delta_1^+ = 150 \quad (\text{Disp. presup.})$$

$$200x_1 + \Delta_2^- - \Delta_2^+ = 1000 \quad (\text{Art. A})$$

$$1000x_1 + 400x_2 + \Delta_3^- - \Delta_3^+ = 1200 \quad (\text{Art. ME})$$

$$250x_2 + \Delta_4^- - \Delta_4^+ = 800 \quad (\text{Art. 3E})$$

$$x_1, \Delta_1^-, \Delta_1^+, \Delta_2^-, \Delta_2^+, \Delta_3^-, \Delta_3^+, \Delta_4^-, \Delta_4^+ \geq 0 \text{ y enteros}$$

b.1) Introducción (2)

$$1. \min z_1 = \Delta_1^+$$

s.a.

$$15x_1 + 30x_2 + \Delta_1^- - \Delta_1^+ = 150$$

$$x_1, x_2, \Delta_1^-, \Delta_1^+, \Delta_2^-, \Delta_2^+, \Delta_3^-, \Delta_3^+, \Delta_4^-, \Delta_4^+ \geq 0 \text{ y enteros}$$

→ Valor óptimo de la función objetivo es $\Delta_1^+ = 0$

$$\text{con } x_1^* = x_2^* = 0 \text{ y } \Delta_1^- = 150 \quad (\text{una de las sol. óptimas alternativas})$$

$$2. \min z_2 = \Delta_2^-$$

s.a.

$$200x_1 + \Delta_2^- - \Delta_2^+ = 1000$$

$$\Delta_2^+ = 0$$

$$x_1, x_2, \Delta_1^-, \Delta_1^+, \Delta_2^-, \Delta_2^+, \Delta_3^-, \Delta_3^+, \Delta_4^-, \Delta_4^+ \geq 0 \text{ y enteros}$$

$$3. h = x^4 - x^3 - 3x^2 + x + 1 \in \mathbb{Q}[x]$$

a) h irreducible en $\mathbb{Q}[x]$

$$f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}[x] \text{ irreducible en } \mathbb{Z}[x] \Rightarrow h \text{ irreducible}$$

y no es divisible entre $x^2 + x + 1$

b) El cuerpo finito extensión de \mathbb{Q} tiene raíz alpha

base sobre \mathbb{Q} es operación $\alpha^3 - 2\alpha^2 + 1$.

$$\mathbb{K} = \mathbb{Q}(\alpha)$$

$$\mathbb{K} = \{1, \alpha, \alpha^2, \alpha^3\}$$

$$\begin{array}{r} x^4 \\ -x^3 \\ +x^4 + 3x^3 - x^2 - x \\ \hline x^4 + 3x^3 - 3x^2 - x \\ -x^4 + x^3 + 3x^2 - x + 1 \\ \hline 4x^3 - 2x + 1 \end{array}$$

c.) Express el elemento $(\alpha^3 - 2\alpha^2 + 1)^{-1}$ como producto $\{1, \alpha, \alpha^2, \alpha^3\}$

?.

$$04. \text{ Pol. min } \sqrt{3+\sqrt{3}} \Rightarrow \mathbb{Q}(\beta) \cup \mathbb{Q}(\sqrt{3+\sqrt{3}})$$

$$\beta = \sqrt{3+\sqrt{3}} \Rightarrow \beta^2 - 3 = \sqrt{3} \Rightarrow \beta^4 - 6\beta^2 + 9 - 3 = 0 \Rightarrow \beta^4 - 6\beta^2 + 6 = 0 \text{ con } \alpha \text{ de } x.$$

$$\begin{aligned} &[\mathbb{Q}(\beta):\mathbb{Q}] = 2 \quad \text{NO.} \\ &[\mathbb{Q}(\sqrt{3+\sqrt{3}}):\mathbb{Q}] = 4 \quad \text{NO.} \end{aligned}$$

$$b.1 \text{ En } \mathbb{Z}_2[x]/(x^2+x+2) \text{ se res. } (2x+1)^2(x+1)$$

$$(2x+1)(x+2) = 2x^2 + x + 4x + 2 = 2x^2 + 5x + 2$$

$$\begin{array}{r} 2x^2 + 5x + 2 \\ -2x^2 - 2x - 4 \\ \hline 3x - 2 \end{array}$$

?.

12P 2016

1.

b) Dem $T = \{ \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} | a \in \mathbb{Q} \}$ es subanillo de $(\mathbb{Q}^{2x2}, +, \cdot)$ si es un IDEAL?

$$T \neq \emptyset \Rightarrow \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in T$$

$$\forall \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} \left\{ \begin{array}{l} a, b \in \mathbb{Q} \\ a, b \neq 0 \end{array} \right. \begin{cases} \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ -(a-b) & 0 \end{pmatrix} \in T \\ \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ -ab & 0 \end{pmatrix} \in T \end{cases}$$

T subanillo $\Rightarrow \mathbb{Q}^{2x2}$

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin T \Rightarrow T \text{ NO IDEAL } \Rightarrow \mathbb{Q}^{2x2}$$

$\mathbb{Q}^{2x2}, \mathbb{C}_T$

c) T subanillo comunitativo?

$$\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ -ab & 0 \end{pmatrix} = \begin{pmatrix} ba & 0 \\ -ba & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}$$

d) T cuerpo?

- Comunitativo \Rightarrow Sí \uparrow
- Anillo con inverso $\Rightarrow \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}$
- Anillo \Rightarrow $a \neq 0$
- inverso $\Rightarrow \forall \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \in T$ et no nulo $\Rightarrow \frac{1}{a} \in Q \Rightarrow \begin{pmatrix} \frac{1}{a} & 0 \\ -\frac{1}{a} & 0 \end{pmatrix}$

$$\hookrightarrow \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{a} & 0 \\ -\frac{1}{a} & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}$$

e) Estudia T (anillo a $(\mathbb{Q}, +, \cdot)$)

$$\varphi: T \rightarrow \mathbb{Q} \text{ tal que } \varphi \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} = a$$

$$1. \varphi \text{ biyectiva } \varphi \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} = \varphi \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} \Leftrightarrow a = b \Leftrightarrow \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix}$$

$$\forall a \in \mathbb{Q} \exists \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \in T \Leftrightarrow \varphi \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} = a$$

2. φ homomorfismo \Rightarrow anillo

$$\forall \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} \in T$$

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

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

$$2. R_1 = \mathbb{F}_5 \quad R_2 = \mathbb{F}_6 \times \mathbb{F}_6 \quad R_3 = \mathbb{F}[x] \quad R_4 = \mathbb{F} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

- a) Identizar anillos
b) Caracterist. anillos

c) Unidades
d) Div. de cero + ejemplo
e) UST. cuerpos?

	\mathbb{F}_5	$\mathbb{F}_6 \times \mathbb{F}_6$	$\mathbb{F}[x]$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$
IDENTIDAD	$[1]_5$	$12 = \text{MCM}$	1	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$
CARACTER.	5	$[1]_6 [1]_6$	0	0
UNIDADES	$1, [1]_5, [2]_5, [3]_5, [4]_5$	$([1]_6 [1]_6), ([1]_6 [3]_6)$ $([2]_6, [1]_6), ([5]_6, [3]_6)$	$1, -1$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$
Div. de 0	✗	$x \nmid ([3]_6 [2]_6)$	✗	$x \nmid \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$

DJ \Rightarrow com., unid. y sin. div. $\Rightarrow R_1 \cup R_3$

Cuerpo \Rightarrow com., i.e., div. ($\forall u \neq 0 \in R_1$) $\Rightarrow R_1$
caract. cuia div.

3.

a) $\mathbb{Q}(\sqrt{2}, \sqrt{6})$ extensión simple $\cong \mathbb{Q}$

$$\alpha = \sqrt{2} + \sqrt{6} \Rightarrow \sqrt{2} + \sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$\hookrightarrow \mathbb{Q}(\sqrt{2} + \sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

b) $P = x^4 - 2x^3 + 6x - 10 \in \mathbb{Q}[x]$ Dem. irreducible. EISENSTEIN

$$P = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

$$\begin{matrix} \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & -2 & 0 & 6 & -10 \end{matrix}$$

Coeficientes en P constan $\begin{pmatrix} 0/2 \rightarrow \\ 0/5 \rightarrow \\ 1/5 \rightarrow \end{pmatrix}$

y p divide los

a/b

$$\hookrightarrow \frac{b}{a} = 10 \text{ ratio}$$

Es irreducible.

c) Th Kronecker \exists raiz α de P en cuerpo algebraico?

$$\mathbb{Q}[x]/\langle P \rangle \cong \mathbb{Q}(\alpha)$$

d) Cuerpo y raiz α

$$1. (\alpha^2 - 1)(\alpha^2 - \alpha + 1)$$

$$\hookrightarrow x^3 - 5x + 9$$

$$2. (\alpha^2 - 2\alpha + 5)^{-1}$$

$$\hookrightarrow x^2 - 3$$

4.

a) Polinomio minimo $\Rightarrow \beta = \sqrt[3]{2} + \sqrt[3]{4}$ sobre \mathbb{Q}

$$\mathbb{B} \cap \mathbb{Q}(\beta) = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$$

$$11 \quad g(1) = 0 + \cancel{\sqrt[3]{2}} + \cancel{\sqrt[3]{4}}$$

$$22 \quad g(\sqrt[3]{2}) = 0 + \cancel{\sqrt[3]{4}} + 1$$

$$33 \quad g(\sqrt[3]{4}) = 0 + \cancel{1} + \cancel{1} \sqrt[3]{2}$$

$$\alpha = \sqrt[3]{2} + \sqrt[3]{4} \Rightarrow \alpha^2 = (\sqrt[3]{2} + \sqrt[3]{4})^2 \Rightarrow$$

$$\Rightarrow \alpha^2 = \sqrt[3]{4} + 2\sqrt[3]{2} + 4 \Rightarrow$$

$$\Rightarrow 2 + 2\sqrt[3]{4} + 4\sqrt[3]{2} + 2\sqrt[3]{2} + 4 + 4\sqrt[3]{4} =$$

$$= 6 + 6\sqrt[3]{2} + 6\sqrt[3]{4} = 1 + \sqrt[3]{2} + \sqrt[3]{4}$$

$$\hookrightarrow \begin{pmatrix} 0 & 2 & \cancel{2} \\ \cancel{2} & 0 & 1 \\ \cancel{1} & \cancel{1} & 0 \end{pmatrix} \xrightarrow{\sqrt[3]{2}} \begin{pmatrix} -1 & 2 & 2 \\ 1 & -1 & 2 \\ 1 & 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 2 \\ 0 & -1 & 2 \\ 0 & 1 & -1 \end{pmatrix} =$$

$\cancel{g(1)} \quad \cancel{g(\sqrt[3]{4})}$

$\begin{matrix} g(1) \\ g(\sqrt[3]{4}) \\ x_3 \text{ es el primero} \end{matrix}$

$$= -1 [(-1^2 + 2)(-1 + 2) - (2 \cdot 2)(1 + 1)] =$$

$$= -1 [(-1^2 - 2 \cdot 2 + 2 \cdot 2) \cdot 4 - 2 \cdot 2 - 2 \cdot 2 - 2 - 2] =$$

$$= -1 [(-1^3 - 6 \cdot 2 - 6) \cancel{+ 12}] =$$

$$X^3 - 6X - 6 \text{ es min}$$

b) Base y grado extension $\mathbb{Q}(\sqrt[3]{5}, \sqrt[9]{5})$ sobre \mathbb{Q}

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{5}, \sqrt[9]{5}) \quad \text{min com} = 6 \quad \text{Grado extensión}$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[9]{5}) \approx (\alpha + b\sqrt[9]{5})(\alpha + b'\sqrt[9]{5})(\sqrt[9]{5}) + (\alpha'' + b''\sqrt[9]{5})\sqrt[9]{5}$$

$$\hookrightarrow \mathbb{B} = \{1, \sqrt[3]{5}, \sqrt[3]{5}^2, \sqrt[3]{5}^3, \sqrt[3]{5}^4, \sqrt[3]{5}^5, \sqrt[3]{5}^6\}$$

c) Dem $\nexists h = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ irreducible en $\mathbb{Z}_2[x]$ ↓
polinomio minimo

grado extensión = 3

→ deb $\cong 1^2 \times 1$

$$\nexists x - \alpha \mid p = 1 \Rightarrow 111, 111, 111 \quad 1^2 \mid 1 \quad \text{No cumple.}$$

↓
deben ser 1×1 No cumple

No tiene raíces

d) Del ejercicio

$$\left. \begin{array}{l} x^0 = 1 \\ x = x \\ x^2 = x^2 \\ x^3 = x^2 + 1 \end{array} \quad \begin{array}{l} x^4 = \frac{x^3 + x}{x(x^2 + 1)} = x^2 + x + 1 \\ x^5 = x + 1 \\ x^6 = x^2 + 1 \\ x^7 = 1 \end{array} \right\} \mathbb{Z}_2[x]$$

e) Dem $\mathbb{Z}_2[x]/(h)$ no es cuadrado.

$$\left. \begin{array}{lll} x^0 = 1 & x^4 = 1 & \mathbb{Z}_3[x] \\ x = x & x^5 = 2x \\ x^2 = x + 1 & x^6 = x^2 \\ x^3 = 2x + 1 & x^7 = x + 2 & x \neq 1 \end{array} \right\}$$

2017 2P

1.

a) $(V_1, +_1, \cdot_1) \times (V_2, +_2, \cdot_2) \Rightarrow$ Anillo producto de $V_1 \times V_2 \Rightarrow$ anillo

• Commutativos $(a, b)(c, d) = (ac, bd) = (c, d)(a, b)$

• A. Identidad $1_{V_1 \times V_2} = (1_{V_1}, 1_{V_2})$

• A. \Rightarrow adición inversa $(a, b)^{-1} = (a^{-1}, b^{-1}) = (a \cdot a^{-1}, b \cdot b^{-1}) = 1_{\mathbb{Q}}$

b) $\mathbb{F}[x] \oplus \mathbb{Q}$ igual a $\mathbb{Q}[x]$

$$\boxed{F} \Rightarrow x \in \left\{ \begin{array}{l} x+1 \in \mathbb{F}[x] \\ \text{multp. } \\ 1/2 \in \mathbb{Q}[x] \end{array} \right\} \left\{ \begin{array}{l} \frac{1}{2}x + \frac{1}{2} \notin \mathbb{F}[x] \end{array} \right\}$$

c) Aplicación $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ s.t. $\varphi(x) = x''$, numero de dígitos

$$\varphi(x) = x''$$

$$\vdash \varphi(xy) = \varphi(x)y'' = x'' \cdot y'' = \varphi(x)\varphi(y)$$

$$\vdash \varphi(x+y) = \varphi(x) + \varphi(y)$$

$$\varphi(x+y)'' = x'' + y'' \text{ mod } 11$$

d) $x^2 + 1$ irreducible en $\mathbb{R}[x]$

$$x^2 + 1 = (x - 4)(x - 13) \in \mathbb{R}[x]$$

$\sqrt{17}x^2 + 17x + 1$ es irreducible.

\sqrt{x}

e) $\mathbb{Q}[x]/(x^2 - 1) \Rightarrow$ anillo

¿?

g) $\sqrt[3]{2} \in \mathbb{Q}[\sqrt[3]{2}]$

$B_{\mathbb{Q}[\sqrt[3]{2}]} = \{1, 2^{1/3}, 2^{2/3}, 2^{4/3}, 2^{5/3}, 2^{7/3}, 2^{8/3}, 2^{10/3}\}$

L. $\sqrt[3]{2}$ no se puede expresar como comb. lineal \Rightarrow $\mathbb{Q}[\sqrt[3]{2}]$ es gen. de $\mathbb{Q}[\sqrt[3]{2}]$.

$$2. R = \{a\mathbb{I} + bM : a, b \in \mathbb{K}\} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

a) Dado $(R, +, \cdot)$ anillo (vectores)

R subanillo $\Rightarrow \mathbb{K}^{2 \times 2} : I \in R \Rightarrow IR \neq \emptyset$ y tiene identidad

$$\hookrightarrow X = \{a\mathbb{I} + bM\}, \quad Y = a\mathbb{I} + bM$$

$$\hookrightarrow X - Y = (a - c)\mathbb{I} + (b - d)M$$

$$XY = (ac\mathbb{I}) + (a\mathbb{I} + bc)M + (b\mathbb{I} + dM)^2 \quad | \quad M^2 = 2M$$

$$\hookrightarrow XY = ac\mathbb{I} + (a\mathbb{I} + bc + 2bd)M$$

b) Si R es anillo comunitativo y se ha de ser.

$$XY = ac\mathbb{I} + (a\mathbb{I} + bc + 2bd)M = YX$$

$$R \text{ no es divisor } (2\mathbb{I} - M) \cdot M = 0$$

c) Unidades: $2\mathbb{I}, \mathbb{I} - M$

$2\mathbb{I}$ no es unidad en R .

$\mathbb{I} - M$ si es unidad en R : $(\mathbb{I} - M)^2 = \mathbb{I}$

d) Dado $J = \{3a\mathbb{I} + 3bM : a, b \in \mathbb{K}\}$ es un ideal de R

$$J \neq \emptyset \quad x \in J \subseteq R$$

e) DW. de los anillos cocientes R/J : $\mathbb{C}(2\mathbb{I} - M)J, \mathbb{C}M^2J$

$$\hookrightarrow M^2(2\mathbb{I} - M) = 2M(2\mathbb{I} - M) = 0$$

f) J maximal $\Leftrightarrow R/J$

R/J tiene fin. de car.

$$\begin{array}{r} x^4 - x^3 - 3x^2 + x + 1 \quad | \quad x^3 - x^2 - 3x + 2 \\ - x^4 + x^3 \quad 3x^2 - 2x \quad x \\ \hline x^5 - x^4 + 3x^3 + 2x^2 - x + 1 \\ - x^5 + x^4 \quad - x^2 \\ \hline - x + 1 \quad | \quad - 3x + 2 \end{array}$$

$$3. h = x^4 - x^3 - 3x^2 + x + 1 \in \mathbb{Q}[x]$$

a) Dado irreducible en $\mathbb{Q}[x]$

Por divisiones, No tiene raiz y no es $(x^2 + x + 1)^2$

$$x^3 - 2$$

$$\downarrow$$

$$\mathbb{Q}[x^5 - 2x^2]$$

b) K min extensión de la raiz real de h . Debe ser \mathbb{Q} sobre \mathbb{Q} a base.

$$K = \mathbb{Q}(\alpha), \quad \alpha^5 = 11, \quad \alpha, \alpha^2, \alpha^3, \alpha^4$$

$$\alpha^5 - 2\alpha^2 \Rightarrow \alpha(\alpha^3 - 2) \Rightarrow 4\alpha^3 - 2\alpha - 1$$

base para otra ext.

$$c) (\alpha^3 - \alpha^2 - 3\alpha + 2)^{-1} \cdot Q.$$

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

4. Pod min $\alpha = \sqrt{3+\sqrt{3}}$. Relación de minimos $\mathbb{Q}(\sqrt{3}) \cup \mathbb{Q}(\sqrt{3+\sqrt{3}})$

$$\text{L. } \alpha^2 = 3 + \sqrt{3} \Rightarrow \alpha^2 - 3 = \sqrt{3} \Rightarrow (\alpha^2 - 3)^2 = 3 \Rightarrow$$
$$\Rightarrow \alpha^4 - 6\alpha^2 + 9 - 3 = 0 \Rightarrow \alpha^4 - 6\alpha^2 + 6 = 0$$
$$x^4 - 6x^2 + 6 = 0 \in \mathbb{Q}[x]$$

$$[\mathbb{Q}(\sqrt{3}); \mathbb{Q}] = 2 \quad (\alpha = \sqrt{3}; \alpha^2 = 3 \Rightarrow \alpha^2 - 3 = 0)$$
$$[\mathbb{Q}(\sqrt{3+\sqrt{3}}); \mathbb{Q}] = 4 \quad \text{NO clásico}$$

b.) $\mathbb{F}_3[x]/(x^2+x+2)$ resultante $\underbrace{(2x+1)^2(x+2)}$

$$(4x^3 + 4x^2 + x + 2)(x+2) = 4x^3 + 4x^2 + x + 8x^2 + 8x + 2 = 4x^3 + (2x^2 + 9x + 2)$$

$$\left. \begin{array}{l} x^0 = 1 \\ x = x \\ x^2 = x+1 \\ x^3 = 2x+1 \end{array} \right\} \begin{aligned} & 4(2x+1) + 2(x+1) + 9x + 2 = \\ & = 8x + 4 + 12x + 12 + 9x + 2 = \\ & = 2x + 1 + \cancel{24} + 2 = 2x + 1 \end{aligned}$$

2018 2P

1. Anillo? Cuerpo? $S = \{a+b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Z}\}$

$$(a+b\sqrt{2}+c\sqrt{3}) - (d+e\sqrt{2}+f\sqrt{3}) = \underbrace{a-d}_{\in \mathbb{Z}} + \underbrace{(b-e)\sqrt{2}}_{\in \mathbb{Z}} + \underbrace{(c-f)\sqrt{3}}_{\in \mathbb{Z}}$$

$$(a+b\sqrt{2}+c\sqrt{3})(d+e\sqrt{2}+f\sqrt{3}) = \dots$$

$$= ad + ae\sqrt{2} + af\sqrt{3} + bd\sqrt{2} + 2be + bf\sqrt{3} + cd\sqrt{3} + ce\sqrt{6} + cf\sqrt{3} =$$

$$= (ad + 2be + 3cf) + (ae + bd)\sqrt{2} + (af + cd)\sqrt{3} + (bf + ce)\sqrt{6} \notin \mathbb{Z}$$

No es anillo

A no es anillo no es cuerpo.

2. Unidad y los divisores de los anillos ($\mathbb{Z} \times \mathbb{Q} \times \mathbb{N}, +, \cdot$)

Unidades: $U = \{(a, b, c) \in \mathbb{Z} \times \mathbb{Q} \times \mathbb{N} : abc = 1, -1\}$, $b \in \mathbb{Q}^\times\}$

Divisores de cero: $(a, b, c) \neq 0 \Rightarrow abc = 0$

3. Estructura concreta de anillo ($\{0, 2, 4, 6, 8, +, 10, \cdot, 0\}$)

$\cdot 10$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

Anillo identidad y la división
CUERPO

4. Construcción de anillo ($\mathbb{Z}_6 \times \mathbb{Z}_{15}, +, \cdot$)

$$\begin{array}{c|c}
6/2 & 15/3 \\
3/3 & 5/5 \\
1/1 & 1/1
\end{array} \quad 2 \cdot 3 \cdot 5 = 30$$

$$\hookrightarrow \mathbb{C}(\mathbb{Z}_6 \times \mathbb{Z}_{15}) = 30$$

5. $(\mathbb{Z}, +, \cdot)$ anillo. Dem $\mathcal{U}(\mathbb{Z}) = \{x \in \mathbb{Z} : x \neq 0\}$ subanillo y obtención ideal

$$xa - ya = (x-y)a = 0 \Leftrightarrow x-y \in \text{N}(a)$$

$$xy(a) = x(ya) = x0 = 0 \Leftrightarrow xy \in \text{N}(a)$$

$$(xr)x = (rx)x = r(xx) = r0 = 0$$

$$\mathcal{U}(\mathbb{Z}) = \{(ab)^{-1} : (ab) \in (\mathbb{Z})\} = \{ab^{-1} : (ab) \in (\mathbb{Z})\}$$

6. Den intersección 2 cocientes, onto

7. $x^5 - x^2 + 1$ irreducible en $\mathbb{Q}[x]$

1x1 = 1 no divisible.

Como no es divisible $x^4 + x^2 + 1 \Rightarrow$ no tiene raíces, onto^2 .

8. $F_9 = \mathbb{F}_3[x] / (x^2 + x + 2) : (x+1)x^{-1}$

$$x^{-1} = \left\{ \begin{array}{l} x^2 + x + 2 = x \cdot x + (x+2) \\ x = (x+2) \cdot 1 + 2 \end{array} \right.$$

$$\begin{array}{r} x^2 + x + 2 \cancel{+ x} \\ - x^2 \\ \hline x \cancel{(x+2)} \\ - x + 2 \end{array}$$

$$-2 = x - (x+2) \cdot 1$$

$$-1 = x - (x^2 + x + 2 - x \cdot x) = -(x^2 + x + 2) + (x^2 \cdot x) = -2x + 2 = 4x + 2$$

$$x^2 \Rightarrow x^2(x+1) = x^3 + 1 = 2x + 1 + 1 = \boxed{x+2}$$

$$x^3 = 2x + 1$$

9. $\alpha = \sqrt{5} - \sqrt{2}$ base

$$\alpha^2 = (\sqrt{5} - \sqrt{2})^2 \quad B = \{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$$

(10) pol min \downarrow

$$g(1) = 0 + \sqrt{2} + \sqrt{5} + \sqrt{10}$$

$$g(\sqrt{2}) = 0 + 2 + \sqrt{10} + 2\sqrt{5}$$

$$g(\sqrt{5}) = 0 + \sqrt{10} + 5 + 2\sqrt{2}$$

$$g(\sqrt{10}) = 0 + 2\sqrt{5} + 5\sqrt{2} + 10$$

0	1
1	0
1	1
1	2

IDEALES Y ANILLOS COCIENTES

Caracterización

Sea $I \subseteq R$, I ideal $\Leftrightarrow \begin{cases} \forall a, b \in S \Rightarrow a - b \in I \\ \forall c \in S, \forall r \in R \Rightarrow ar, rc \in I \end{cases}$

$I \neq \emptyset$ propio si $I \neq R$

$I = 1 + I$ es trivial $\Leftrightarrow R$

I es ppal si $\exists a \in R : I = (a)$

$\text{En } (\mathbb{Z}, +, \cdot)$ todos los ideales son ppales.

$\text{En } (\mathbb{Z}, +, \cdot)$ los ntos son subanillos sencillos
 $\text{En } (\mathbb{A}, +, \cdot)$ el ideal $(p) = p\mathbb{A}$ es maximal ($\Leftrightarrow p$ es primo)

ANILLO COCIENTE

$R/I = \{[r]_I : r \in R\}$ $\left\{ \begin{array}{l} I \text{ es ideal de } R \Leftrightarrow (R/I, +, \cdot) \text{ es anillo} \\ R/I = 1 + I : \text{rel.} \end{array} \right.$

IDEALES MAXIMALES: I es maximal $\Leftrightarrow (R/I, +, \cdot)$ cuerpo $\Leftrightarrow I \subseteq J \subseteq R$

IDEAL GENERADOR: Es el nro $\leq (a, b) = N$ (suma)

IDEAL MINIMO: Es el producto $a \cdot b = M$ (producto)

HOMOMORFISMOS DE ANILLOS

COMPROBACIÓN $\left\{ \begin{array}{l} \text{SUMA: } \varphi(a+b) = \varphi(a) + \varphi(b) \\ \text{PRODUCTO: } \varphi(ab) = \varphi(a)\varphi(b) \end{array} \right.$

COMP. ISOMORFISMO $\left\{ \begin{array}{l} 1. \text{ Sea biyectiva tiene que ser inversa} \\ \text{Ker } \varphi = 1 + I \\ 2. \text{ Suprayectiva } \forall b \in R, \exists a \in A \text{ ta q } \varphi(a) = b \end{array} \right.$

NÚCLEO $\Rightarrow \text{Ker } \varphi = \{r \in R : \varphi(r) = 0\} \Leftrightarrow \text{IDEAL } \trianglelefteq R$ $\left\{ \begin{array}{l} R : R \rightarrow S \\ 0 : R \rightarrow S \end{array} \right.$

IMAGEN $\Rightarrow \varphi(R) = \{\varphi(r) : r \in R\} \Leftrightarrow \text{SUBANILLO } \trianglelefteq S$

$(\mathbb{Z}_n, +, \cdot, 0)$ — $(\mathbb{Z}_m, +, \cdot, 0)$

Homomorfismo $\varphi([1]_n) = [k]_m$

$\left\{ \begin{array}{l} 1. \text{ De grupos} \Leftrightarrow n \cdot k \equiv 0 \pmod m \\ 2. \text{ De anillos} \Leftrightarrow k^2 \equiv 1 \pmod m \end{array} \right.$

biject. $\varphi(1) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \varphi(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix})$
 homom $\varphi((1)+(1)) = \dots \varphi(1)+\varphi(1)$
 $\varphi((1)(1)) = \dots \varphi(1) \cdot \varphi(1)$
 ISOMORFO

Sea $(R, +, \cdot)$ anillo de enteros. $\left\{ \begin{array}{l} C(R) = \{x \in R : x \text{ contiene subanillo } \trianglelefteq a \neq 1\} \\ C(R) = 0 \Rightarrow R \text{ contiene subanillo } \trianglelefteq a \neq 1 \end{array} \right.$

$R/\text{Ker } \varphi \cong \varphi(R)$ TH DE HOMOMORFIA

	\mathbb{Z}_5	$\mathbb{Z}_6 \times \mathbb{Z}_4$	$\mathbb{Z}[x]$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$
IDENT	$[1]_{\mathbb{Z}_5}$	$([1]_6, [1]_4)$	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
CARACT	5	12 (mcml)	0	0
UNIDAD	$([1]_5, [2]_5)$ $([3]_5, [4]_5)$	$([1]_6, [1]_4), ([1]_6, [3]_4)$ $([5]_6, [1]_4), ([5]_6, [3]_4)$	11, -14	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$
DIVISIÓN	\mathbb{Z}	$x \mid ([3]_6, [2]_4)$	\mathbb{Z}	$x \mid \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$

DS

DS

cuerpo

$\text{U}I = \begin{cases} \text{com.} \\ \text{unit.} \\ \text{div.} \end{cases}$

$\text{Cuerpo} = \begin{cases} \text{car} \\ \text{caract} = n \\ \text{div. div.} \\ \text{unit. izq} \end{cases}$

ANILLOS U SISTABILLOS

$$(R, +, \cdot) \left\{ \begin{array}{l} +: R \times R \rightarrow R \\ \cdot: R \times R \rightarrow R \end{array} \right.$$

$$\begin{aligned} 0_R \cdot a &= a \\ a \cdot (-b) &= - (ab) \\ (-a) \cdot (-b) &= ab \end{aligned}$$

ANILLO

- Elemento nulo (cero): $a + 0_R = a$
- Elemento opuesto (doble): $a + (-a) = 0_R$
- Asociativa del producto: $a(b(c)) = (abc)c$
- Distributivas: $a(b+c) = ab+ac$

ejemplos

A. <u>Comunitativo</u> $\Rightarrow a \cdot b = b \cdot a$
A. <u>con identidad</u> $\Rightarrow a \cdot 1_R = a$, $1_R \in R$, $1_R \neq 0_R$ (Tiene elem. neutro)
A. <u>de división (inverso)</u> $\Rightarrow a \cdot a^{-1} = 1_R$ (Tiene inverso)

SUBANILLO

$$\text{SER} \quad \left\{ \begin{array}{l} a-b \in S \\ a \cdot b \in S \end{array} \right.$$

PROPIEDAD $\left\{ \begin{array}{l} (a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \\ (a_1, a_2)(b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2) \end{array} \right.$

DOMINIO DE INTEGRIDAD

Divisor de cero $\Rightarrow r \cdot s = 0_R$

Unidad del anillo $\Rightarrow a \cdot a^{-1} = a^{-1} \cdot a = 1_R$

Dominio de integridad $\left\{ \begin{array}{l} \text{comunitativo } ab = ba \\ \text{con identidad } a \cdot 1_R = a \\ \text{sin divisores de cero } r \cdot s = 0_R \end{array} \right.$

Grupo de unidades $\left\{ \begin{array}{l} (R, +, \cdot) \text{ anillo con identidad} \\ 1_R = \exists a \in R : a \text{ es unidad} \Leftrightarrow \exists b \end{array} \right.$

Propiedad cancelativa $\left\{ \begin{array}{l} (R, +, \cdot) \text{ anillo comunitativo y con identidad} \\ (R, +, \cdot) \text{ DI} \Leftrightarrow a \neq 0_R \text{ y } a \cdot b = a \cdot c \Rightarrow b = c \end{array} \right.$

Relación dominio de integridad y cuerpo $\left\{ \begin{array}{l} 1. \text{ Cuerpo} \Rightarrow \text{DI} \\ 2. \text{ DI} \text{ sin ito es campo.} \end{array} \right.$

Opr. sucesivas en anillos $\left\{ \begin{array}{l} 1. (rs)a = r(sa) \\ (R, +, \cdot) \quad ra = \underbrace{a + \dots + a}_r \quad 2. r(ab) = (ra)b \end{array} \right.$

Caract. Anillo $\left\{ \begin{array}{l} C = \{a \in R : ra = 0_R \forall a \in R\} \\ C \neq \emptyset \Rightarrow \text{CARACTERRÍSTICA} \Delta R, \text{char}(R) = \min(C) \\ C = \emptyset \Rightarrow \text{CARACTERRÍSTICA cero}, \text{char}(R) = 0 \end{array} \right.$

Caract. A. con identidad $\left\{ \begin{array}{l} \text{orden } 1_R \in R \text{ (R,+)} \text{ finito} \Rightarrow \text{char}(R) = 1_R \\ \text{orden } 1_R \in R \text{ (R,+)} \text{ infinito} \Rightarrow \text{char}(R) = 0 \end{array} \right.$

Caract. Dom. INTG. \Rightarrow cero o un pto primo

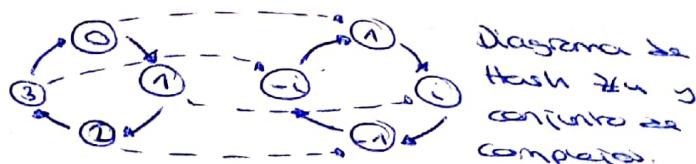
carácteristica de todo anillo ↑

ISOMORFISMO EN GRUPOS

$(G, *)$, $(G', *)'$ isomorfos

$$G \cong G' \Rightarrow \phi(x * y) = \phi(x) *' \phi(y)$$

ϕ isomorf. de grupos



ISOMORFISMOS DE GRUPOS CICLICOS

1. Grupo cíclico $(G, *)$ de orden finito, es isomorfo a $(\mathbb{Z}_n, +)$

2. Grupo cíclico $(G, *)$ de orden n , es isomorfo a $(\mathbb{Z}_n, +_n)$

CONDICIONES NECESARIAS DE ISOMORFISMO.

1. 2 grupos isomorfos tienen el mismo n° de elementos.

2. " " , o ambos abelianos o ninguno de los.

3. " " , o ambos cíclicos, o ninguno de los.

4. " " , mismo n° de elem con la orden determinada.

PRODUCO DE GRUPOS ABELIANOS

El grupo $(\mathbb{Z}_m \times \mathbb{Z}_n, +_m \times +_n)$ es isomorfo a $(\mathbb{Z}_{mn}, +_{mn})$ si $\gcd(m, n) = 1$

DEF DE PRODUCO DIRECCO INTERNO

Sea $(G, *)$ un grupo y sean $H \leq G$ y $K \leq G$.

Se dice que el grupo G es producto directo interno de los subgrupos H y K si verifica que:

$$1. H \cap K = \{e\}$$

$$2. G = HK = \{u * v : u \in H, v \in K\}$$

$$3. \text{Los elementos de } H \text{ y } K \text{ se} \text{comutan}: \forall u \in H, v \in K \text{ es } u * v = v * u$$

RELACION ENTRE PRODUCTO DIRECCO INTERNO Y PRODUCTO DIRECTO

Si $(G, *)$ es producto directo interno de los subgrupos H y K entonces $G \cong H \times K$

TH DE CAUCHY

Todos grupos de orden n son isomorfos a un grupo de permutaciones.

GRUPOS DE PERMUTACIONES

G. SIMÉTRICO (S_n, \circ) aplicaciones biyectivas en X .

G. PERMUTACIONES $X = \{1, 2, \dots, n\} \Rightarrow (S_n, \circ)$

Todo elemento $\geq (1n, \circ)$ es una permutación

$G \subseteq S_n$, G es un ciclo \Rightarrow longitud $\leq n$ si $\exists a_0, \dots, a_{r-1} \in \{1, \dots, n\}$ tal que

$$G(a_0) = a_1, \dots, G(a_{r-2}) = a_{r-1}, G(a_{r-1}) = a_0 \Rightarrow \begin{cases} G(k) = k \\ G = (a_0, a_1, \dots, a_{r-1}) \end{cases}$$

Dos ciclos son distintos si ninguno de los elem. del conjunto $\{1, \dots, n\}$ aparece en las rotaciones de ambos.

Ciclos de longitud 2 \Rightarrow TRANSPOSICIONES

LA DESCOMPOSICIÓN NO ES ÚNICA

Por inducción de r , τ_1, \dots, τ_r

a) Si $r=1 \Rightarrow G_1 = \tau_1$

b) Si cierto para todo producto de $r-1$ transposiciones

c) Sea $\tau_1, \dots, \tau_{r-1}, \tau_r$ con $\tau_r = (a_1 b_1)$

a) Si $\tau_{r-1} = (c_1 d_1)$ con $\{c_1, d_1\} \cap \{a_1, b_1\} = \emptyset$

$$\Rightarrow \tau_{r-1} \tau_r = \tau_r \tau_{r-1} \Rightarrow \tau_1 \dots \tau_{r-2} \tau_r (\text{prop. de inversión})$$

b) Si $\tau_{r-1} = (a_1 c_1)$ con $c \notin \{a_1, b_1\}$

$$(\tau_{r-1} \tau_r = (a_1 c_1)(a_1 b_1) = (abc)) = (ab) (bc) \Rightarrow \text{núm. a } \tau_1 \dots \tau_{r-2} \tau_r$$

c) Si $\tau_{r-1} = (b_1 c_1)$ con $c \notin \{a_1, b_1\}$

$$\tau_{r-1} \tau_r = (b_1 c_1)(a_1 b_1) = (a_1 c_1) = (a_1, c_1)(c_1, b_1) \Rightarrow \text{núm. a } \tau_1 \dots \tau_{r-2} = (ac)$$

d) Si $\tau_{r-1} = (a_1 b_1) = \tau_r \Rightarrow \text{núm. a } \tau_1 \dots \tau_{r-2}$

PROPIEDADES

1. Sean $\begin{cases} G = (a_0, \dots, a_{r-1}) \in S_n = \{a_0, \dots, a_{r-1}, b_0, \dots, b_{s-1}, \dots, c_0, \dots, c_{t-1}\} \\ \tau = (b_0, \dots, b_{s-1}) \end{cases}$

$$G \tau(a_i) = G(\tau(a_i)) = G(a_i) = a_{i+1} \text{ mod } r$$

$$\tau G(b_i) = \tau(G(b_i)) = \tau(b_i) = b_{i+1} \text{ mod } r$$

$$G \tau(b_i) = G(b_{i+1} \text{ mod } s) = b_{i+1} \text{ mod } s$$

$$\tau G(a_i) = \tau(G(a_i)) = \tau(a_i) = b_{i+1} \text{ mod } s$$

$$G \tau(a_i) = G(c_{i+1}) = c_i = \tau(c_i) = \tau G(a_i)$$

2. Sean $\begin{cases} G \in S_n \\ x_1 = 1, G(1), \dots, G^n(1), \dots, n \in \{1, \dots, n\} \end{cases}$

Supg que el 1º zero que se repite es $G^k(1)$:

$$G^k(1) = G^l(1), 0 \leq k < n \Rightarrow G^{n-k}(1) = 1 \quad 0 \leq n-k < l \Rightarrow n-k = l \Rightarrow \\ \Rightarrow k=0 \Rightarrow G^k(1) = 1 \rightarrow (1, G(1), \dots, G^{n-1}(1))$$

GENERADORES. GRUPOS CICLICOS, DIÉFRICOS Y QUATERNICOS

SISTEMA DE GENERADORES

$(G, *)$ un grupo, sea $A \subseteq G$ subconjunto no vacío de G . El menor subgrupo de $(G, *)$ que contiene a $A \Rightarrow$ SUBGRUPO DE G GENERADO POR A .

$$\langle A \rangle = \{a_1^{r_1} * \dots * a_n^{r_n} : a_i \in A, r_i \in \mathbb{Z} \text{ y } n \in \mathbb{N}\}$$

• Un conjunto $A \subseteq G$ es un SISTEMA DE GENERADORES de $(G, *)$ si verifica que $G = \langle A \rangle$

• Grupo $(G, *)$ es cíclico si tiene sist. gen. con un único elemento:
 $\exists g \in G \text{ tal que } G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$

ORDEN DE UN ELEMENTO

No todos operan al elemento hasta obtener el elem. neutro

$$\text{Ej: } (\mathbb{Z}_8, +_8) \rightarrow |[1] \cdot 1| = 8 ; \quad a^r = e \Rightarrow |a| = r$$

LO QUE ORDEN DEL SUBGRUPO QUE GENERA

$$|a|_+ = |\langle a \rangle|$$

ORDEN DE ELEMENTOS DE UN GRUPO CICLICO

Grupo cíclico \Rightarrow orden n $(G, *) \setminus 1. g^k = e \Leftrightarrow n$ divide a k
 $g \in G$ generador de G 2. $|g^n| = \frac{n}{\text{m.c.m}(n)}$

PROPIEDADES GR CICL.

1. Todo grupo cíclico es abeliano
2. Todo subgrupo de un grupo cíclico es cíclico

GRUPO QUATERNICOS

$$\langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle \quad \{Q_8 = \langle a, b : |a| = 4, b^2 = a^2, ba = a^{-1}b \}$$

$$\text{GRUPO DIÉFRICO} \quad \left\{ \begin{array}{l} a \text{ orden } 2 \\ b \text{ orden } 2 \\ ab \text{ orden } 2 \\ a^2 = e \end{array} \right. \quad \left\{ \begin{array}{l} a \text{ orden } 2 \\ b \text{ orden } 2 \\ ab \text{ orden } 2 \\ a^2 = e \end{array} \right. \quad \left\{ \begin{array}{l} a \text{ orden } 2 \\ b \text{ orden } 2 \\ ab \text{ orden } 2 \\ a^2 = e \end{array} \right.$$

L. GRUPO DE KLEIN $n=2$

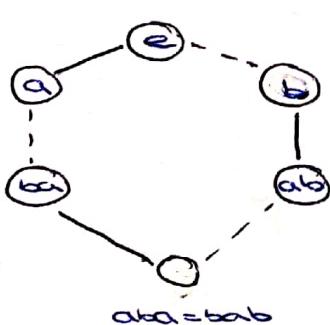
DIAGRAMA DE CAYLEY DE UN GRUPO

$$(Sea b \in H \text{ otro elem} \Rightarrow b = a^m \ (m = r \cdot q + s) \Rightarrow b = (a^r)^q \cdot a^s \Rightarrow b^s = (a^r)^{-q} \cdot b \in H, \text{ si } s = 0, a^r = e \Rightarrow b = (a^r)^q \Rightarrow b \in \langle a^r \rangle)$$

Diagrama de Cayley de C_n



Ej:



*	e	a	b	ab	ba	aba
e	e	a	b	ab	ba	aba
a	a	e	ab	b	aba	ba
b	b	ba	e	bab	a	ab
ab	ab	ba	a	ba	b	e
ba	ba	b	bab	e	ab	a
bab	bab	ab	ba	a	b	e

No es grupo abeliano (\neq dom)
 $|b| = |a| = 2$
 $|ab| = |ba| = 3$
 $|bab| = 2$

$$(ab)(ab) = aba \quad (ab)(aba) = ab \quad aba = ab \\ b(ab) = ab? \\ babab = a \quad ababa = b \quad babab = a$$

GRUPO $\xrightarrow{\text{Prop. asociativa } (a * b) * c = a * (b * c)}$

por $(G, *)$ | El elem. neutro $e * a = a$
 $\downarrow \downarrow$ | El inverso a' de a s.t. $a * a' = e$

conj. neutro // oper. int

G. ABELIANO \Rightarrow As., neu., op. y (comutativa $a * b = b * a$)

ORDEN \Rightarrow cardinal conjunto $|G|$ \rightarrow TABLA DE COMBINACIONES

1. Si es aditiva, asumimos como sumando
2. El elem. neutro $a * e = a \Rightarrow a = e$

INVERSO Y NEUTRO PARA LA OPERACION

$(G, +)$ con $\left\{ \begin{array}{l} a + a' = e \rightarrow a + a' = e \\ \text{elem neutro } a + e = a \end{array} \right.$ para grupos
 cancelativos

UNICIDAD DEL NEUTRO E INVERSO

1. $(G, +)$ el elemento neutro neutro es unico
2. $(G, *)$ el inverso de cada elemento $a \in G$ es unico

• POTENCIA $-1 \in \mathbb{Z}$ DEL ELEMENTO $a \in G$ $\left\{ \begin{array}{l} a^{-1} = a' \text{ INVERSO (GENERAL)} \\ -a = a' \text{ OPUESTO (ABELIANO)} \end{array} \right.$

PROP. CANCELATIVAS (DCHA E IZDA)

- $(G, +) \Rightarrow$ si $x + a = x + b$ entonces $a = b$
- $(G, *) \Rightarrow$ si $a * x = b * x$ entonces $a = b$

GRUPOS DE CONSERVACIONES NIVELLO n

$[a]_n = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$

Relación de equivalencia congruencia $\Leftrightarrow a \equiv b \pmod{n} \Leftrightarrow (b-a) \in n\mathbb{Z}$

1. $[a]_n +_n [b]_n = [a+b]_n \Rightarrow (\mathbb{Z}_n, +_n)$ es grupo abeliano

2. $(n = 1 \text{ Fr})_n \in \mathbb{Z}_n : \text{mcg}(r, n) = 1 \Leftrightarrow [a]_n \cdot_n [b]_n = [ab]_n \Rightarrow (\mathbb{Z}_n, \cdot_n)$ $\left\{ \begin{array}{l} \text{grado} \\ \text{abacino} \end{array} \right.$

$(\mathbb{Q}, +)$ suma $\Rightarrow \frac{a}{n} + \frac{b}{m} = \frac{ma+nb}{m \cdot n} \Rightarrow$ es grupo abeliano $(\mathbb{Q}, +)$

(\mathbb{Q}^*, \cdot) $\mathbb{Q}^* = \mathbb{Q} - \{0\} \Rightarrow \frac{a}{n} \cdot \frac{b}{m} = \frac{a \cdot b}{n \cdot m} \Rightarrow$ es grupo abeliano (\mathbb{Q}^*, \cdot)

SUBGRUPO $(G, *) \Rightarrow H \subseteq G$, H subgr. de G sii $(H, *)$ grupo. $H \leq G$

SUBG. PROPIO $H \leq G$ si $H \subset G$ y $H \neq G \Rightarrow H \subset G$

SUBG. TRIVIAL es elem neutro $\Rightarrow H^0 = \{e_G\} \leq G$

GRUPO \Rightarrow asociat $(a+b)+c = a+(b+c)$
 E. neutro $e = (0)$
 E. opuesto $(a)^{-1}$

ABELIANO \Rightarrow commutativo $a \cdot b = b \cdot a$

$$\alpha = (143)(56)$$

\hookrightarrow Elementos $K = \{ e = (1), \alpha_1 = (143)(56), \alpha_2 = (134), \alpha_3 = (56), \alpha_4 = (143) \}$

ORDEN mat $(\)^n$ y $(\)^{n+1}$ se require = $(\)^n$ in orden

Homomorfismos mat.
 $\begin{cases} \Phi(n+m) = \Phi(n)\Phi(m) \\ \text{Ker } (\Phi) = \emptyset \\ \text{Im } (\Phi) = G \end{cases} \quad \parallel \quad g(x)g(y) = g(xy)$

$$[G:H] \quad (001)H = \{(001)(12)(20)(32)\}$$

$$\begin{aligned} (01)H &= \\ (02)H &= \boxed{?} \\ (03)H &= \end{aligned}$$

$$1^{\text{er}} \text{ th teor} \quad G/\text{Ker}(g) \cong D_2 \Rightarrow |\text{Ker}(g)| = 2 \Rightarrow |\text{Ker}(g)| = 4$$

K_1 cuerpo | $K_1 \times K_2$ NO cuerpo
 K_2 cuerpo

IDEAL númer que este bien en los dos casos

Homomorfismos | $\begin{cases} g(x+y) = g(x)g(y) \\ g(x+y) = g(x) + g(y) \end{cases}$

SUBANILLOS } - $\in S$
} . $\in S$

$$x^2 + 2x + 2y \cdot 2x = 4x^2 + 4x + 2y = 4x^2 + 2y \in \mathbb{Z}[x]$$

ANILLO $\mathbb{F}a + \mathbb{F}b + \mathbb{F}c \Rightarrow$ NO $x \in \mathbb{F} \notin \mathbb{F}$

UNIDADES prod. entre s.

DIV 0 $\Rightarrow \frac{\mathbb{F}_n}{(n)}$ resto 0.

CHAR = $\text{MCZ}(n, m)$

$(\mathbb{Z}_n \times \mathbb{Z}_m)$

$15\mathbb{Z} / 30\mathbb{Z}$ comp. $(15\mathbb{Z}, +, \cdot)$

$$\left\{ \begin{array}{l} I = 30\mathbb{Z} = 30 \text{ ideal } 15\mathbb{Z} \\ 15\mathbb{Z} / 30\mathbb{Z} = \{[0], [15]\} \text{ ideal max.} \\ \text{Table } \begin{array}{|c|c|} \hline & 0 & 15 \\ \hline 0 & 0 & 15 \\ 15 & 15 & 0 \\ \hline \end{array} \end{array} \right.$$

max ideales $\sim \mathbb{Z}_n \times \mathbb{Z}_m$

$$\left\{ \begin{array}{l} ([2]_n) \times \mathbb{Z}_m \\ \mathbb{Z}_n \times ([2]_m) \\ \mathbb{Z}_n \times ([3]_m) \end{array} \right.$$

$$\text{MCN}(n, m) = 2 \begin{smallmatrix} 0 \\ 3 \end{smallmatrix}$$

$h \in \mathbb{Q}[x]$ irreducible

↳ NO RAICES

DIVISIBLE $x^2 + x + 1$ (NO)

$$\rightarrow \alpha = \sqrt[6]{2} \text{ base } \{1, \sqrt[6]{2}, \dots, \sqrt[6]{72}\}$$

$$x^4 - \dots \text{ base } \{1, \alpha, \alpha^2, \alpha^3\} = B_k$$

$$\text{resto } \alpha^5 \rightarrow \alpha^5 \text{ (x^4 -)}$$

$$\alpha = \sqrt[6]{2} - \sqrt[6]{2} \Rightarrow \text{base } \{1, \sqrt[6]{2}, \sqrt[6]{3}, \sqrt[6]{6}\}$$

PERMINING

↳ irreducibles
EISENSTEIN

$$(P^a \mathbb{X}^b, P^{1/n-1}, \dots, P^{1/n}) \wedge (P^c \mathbb{X}^d)$$

$$\begin{aligned} &[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \\ &[\mathbb{Q}(\sqrt[3]{2+\sqrt[3]{2}}) : \mathbb{Q}] = 4 \end{aligned}$$

EISENSTEIN plan, plan₋₁, ..., plan y P¹K₀₁

Lo cumple irreducible

Si no lo cumple

Lo es irreducible pero menor que no tenga raíces de.

BASE $x^n \Rightarrow \{1, \alpha, \dots, \alpha^{n-1}\}$

EXTENSIÓN n (grado)

Polinomio mínimo | ...
| ó con () matices

$$\begin{array}{ll} \mathbb{Z}_2[x] & \begin{array}{ll} x^0 = 1 & x^4 = x^2 + x + 1 \\ x^1 = x & x^5 = x + 1 \\ x^2 = x^2 & x^6 = x^2 + 1 \\ x^3 = x^2 + 1 & x^7 = 1 \end{array} \end{array}$$

$$\begin{array}{ll} \mathbb{Z}_3[x] & \begin{array}{ll} x^0 = 1 & x^4 = 2 \\ x^1 = x & x^5 = 2x \\ x^2 = x + 1 & x^6 = 2x + 2 \\ x^3 = 2x + 1 & x^7 = x + 2 \quad x^8 = 1 \end{array} \end{array}$$