

3.1 Anillos y libanillos

Un anillo $(R, +, \cdot)$ es un cjo. no vacío R con dos operaciones internas, suma y producto:

$$+, \cdot : R \times R \rightarrow R \quad (R \times R \rightarrow R)$$

Talos que:

- ① • $(R, +)$ es grupo abeliano, cuyo elemento neutro se denomina elemento nulo y se nota por $0_R \in R$, y el inverso de $a \in R$ se denomina opuesto de a y se nota por $-a \in R$.
- ② • Propiedad asociativa del producto: $\forall a, b, c \in R$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
- ③ • Propiedad distributiva: $\forall a, b, c \in R$

$$(a+b) \cdot c = (a \cdot c) + (b \cdot c) \text{ y } a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$



Estudiar si es anillo:

$$G \times G \rightarrow G, \quad \forall a, b \in G, \quad a \cdot b = 0_G$$

Si $(G, +)$ es abeliano $\rightarrow (G, +, \cdot)$ es anillo

Estudiar si es anillo

$$\left(\left\langle \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{K} \right\rangle, +, \cdot \right)$$

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C \rightarrow \text{asociativa} \checkmark$$

$$A \cdot (B+C) = (A \cdot B) + (A \cdot C) \quad] \begin{array}{l} \text{(hay q verificarse q el} \\ \text{es p q el} \\ \text{grupo no} \\ \text{es comunitativo)} \end{array} \rightarrow \text{distributiva} \checkmark$$

$$(A+B) \cdot C = (A \cdot C) + (B \cdot C)$$

Es grupo abeliano

$$(G, +) \checkmark \rightarrow$$

↓
Es un anillo

(No es comunitativo en prod, pero si en suma, por eso $(G, +)$ es comunitativa y por tanto abeliano)

④ > Un anillo $(R, +, \cdot)$ que verifica ④ se dice que es un anillo conmutativo:

⑤ Propiedad conmutativa del producto: Saber se verifica $a \cdot b = b \cdot a$

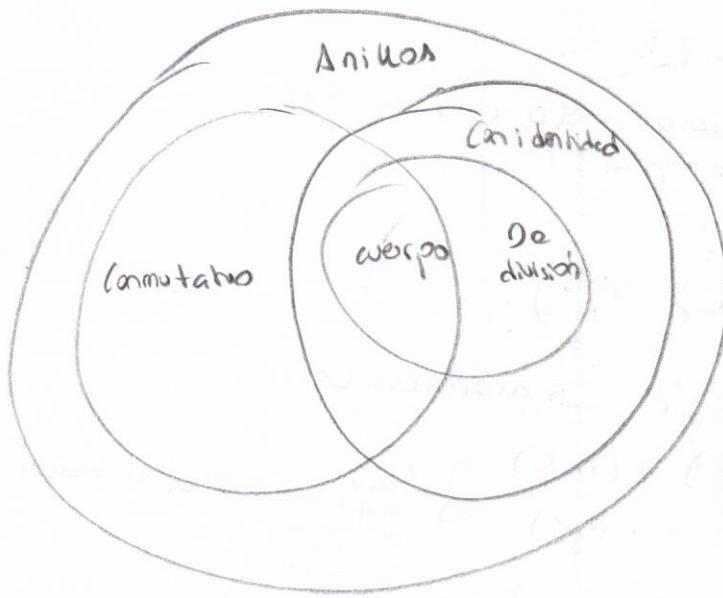
> un anillo $(R, +, \cdot)$ que verifica ⑤ se dice que es un anillo con identidad:

⑥ existe elemento neutro para la operación producto, dicho elemento se denomina identidad del anillo, y se nota por $1_R : 1_R : \exists 1_R \in R \text{ tq } 1_R \neq 0_R \text{ y } 1_R \cdot a = a \cdot 1_R = a \forall a \in R$.

> un anillo con identidad $(R, +, \cdot)$ que verifica ⑥ se denomina anillo de división:

⑦ Existe el inverso, para la op. producto, de todo elemento no nulo del anillo: $\forall a \in R$ con $a \neq 0_R$, existe $a^{-1} \in R$ tq. $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$.

Un anillo, conmutativo y de división que verifica ④ ⑤ y ⑥ se denomina CERDO.



Estudiar si es conmutativo, con identidad, de división y cuerpo

+	0	1	a	b
0	0	1	ab	
1	1	0	ba	
a	a	b	01	
b	b	a	10	

Grupo abeliano ✓

*	0	1	a	b
0	0	0	0	0
1	0	1	ab	
a	0	a	a	0
b	0	b	0b	

Tabla entera respecto de la diagonal

→ Comutativo
Con identidad (El 1 que multiplica)
No es de división
↳ NO ES ANILLO

② al valor q multiplique, no afecta)

■ Estudiar el conmutativo, con identidad, de división y anillo

$$(P(X), \overset{+}{\wedge}, \overset{\times}{\wedge}, \overset{-}{\wedge})$$

tiendo $X = \{1, 2, 3\}$

$$A \Delta B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B) \text{ (diferencia simétrica)}$$

Sabemos q es un grupo abeliano.

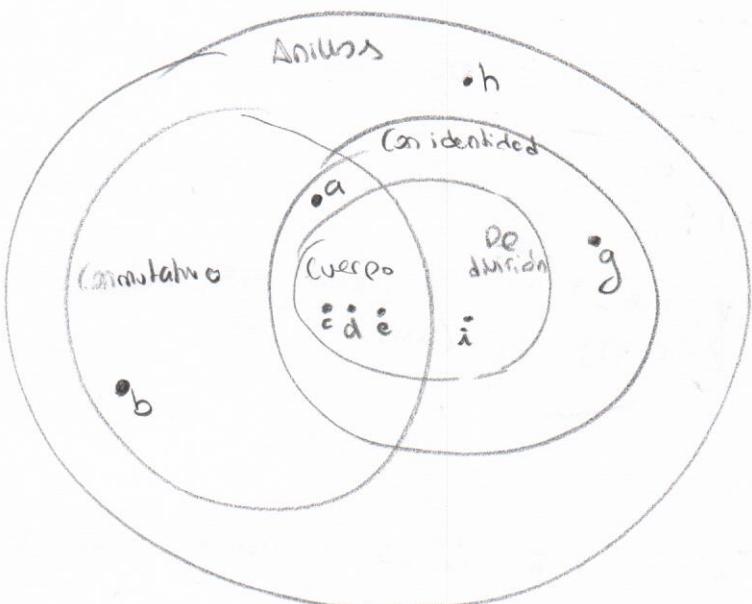
$$\text{(nulo)} \quad e_X^+ = 0_X = \emptyset$$

$$\text{(inverso)} \quad -A = A$$

$$P(X) = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

$$|P(X)| = 8$$

$\left. \begin{array}{l} \text{comuta: Anillo conmutativo (la intersección} \\ \text{de conj. es conmutativa)} \\ \\ \text{identidad: } 1_R \cap A_R = A \quad \forall A \in P(X) \\ \\ \hookrightarrow 1_R = \{e_1 + e_2 + e_3\} = \{1, 2, 3\} \\ \\ \text{inverso: } A \cap B = X = \{1, 2, 3\} = 1_R \\ \hookrightarrow \text{No existe } X \rightarrow \text{No es de división} \end{array} \right\}$



eje $\mathbb{Z}_L - \{0\}$ No es anillo

La la suma no es distributiva respecto del producto

■ Estudiar si los anillos conmutativos, con identidad, de división y anillo.

- a) $(\mathbb{N}, +, \cdot)$
- b) $(2\mathbb{Z}, +, \cdot)$
- c) $(\mathbb{Q}, +, \cdot)$
- d) $(\mathbb{IR}, +, \cdot)$
- e) $(CC, +, \cdot)$
- f) $(\mathbb{Z}_n, +, \cdot)$

residuo de división si n es primo:

si n primo $\forall r \in \{1, \dots, n-1\}$

$$\text{mod}(n, r) = 1 \Rightarrow$$

$$\Rightarrow 1 = nx + ry$$

$$[1]_n = [r]_n \circ [y]_n \Rightarrow$$

$$\Rightarrow [y]_n = [r]_n^{-1}$$

g) $(\{(\frac{a}{c}, \frac{b}{d}) : a, b, c, d \in \mathbb{Z}\}, +, \circ) // (\mathbb{C}, +)$ no tiene inverso

h) $(\{(\frac{a}{c}, \frac{b}{d}) : a, b, c, d \in \mathbb{Z}\}, +, \circ)$

i) $(\{a+bi+cj+dk : a, b, c, d \in \mathbb{R}\}, +, \circ)$ sabiendo que $i^2 = j^2 = k^2 = -1$, $ij = k$,

$$jk = i, ki = j \quad // (a+bi+cj+dk)^{-1} = \frac{1}{a^2+b^2+c^2+d^2} \cdot (a-bi-cj-dk)$$

es de división ✓

→ Propiedades de anillos

sea $(R, +, \circ)$ anillo. $\forall a, b \in R$ se verifican:

$$1. 0_R \cdot a = a \cdot 0_R = 0_R$$

$$2. a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$$

$$3. (-a) \cdot (-b) = a \cdot b$$

distrib.

$$\underline{\text{demo 1}}: 0_R \cdot a = (0_R + 0_R) a \stackrel{d}{=} 0_R \cdot a + 0_R \cdot a \Rightarrow 0_R + (0_R \cdot a) = \\ = (0_R \cdot a) + (0_R \cdot a) \Rightarrow \underline{0_R = 0_R \cdot a}$$

$$\boxed{x+a=y+a \Rightarrow x=y}$$

en todo grupo

demo 2: $\cancel{a} \cdot (-b) \cancel{+} (ab) = 0_R$?

$$a(-b) \cancel{+} (ab) = a(-b+b) = a \cdot 0_R = 0_R$$

↑
distrib.

$$(-a)b \cancel{+} (ab) \stackrel{d}{=} (-a+c)b = 0_R \cdot b = 0_R$$

$$\underline{\text{demo 3}}: \text{(deducción [KIND of])} \quad \text{en un grupo } (a^{-1})^{-1} = a$$

$$(-a)(-b) = -(a(-b)) = -(-ab) \stackrel{d}{=} ab$$

→ Producto directo de anillos

Dados dos anillos $(R_1, +_1, \circ_1)$ y $(R_2, +_2, \circ_2)$ se llama producto directo al anillo: $(R_1 \times R_2, +, \circ)$ // $(R_1 \times R_2, +)$ el grupo abeliano

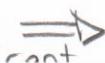
con las operaciones definidas considerando a coordinate:

$$\forall (a_1, a_2), (b_1, b_2) \in R_1 \times R_2$$

$$(a_1, a_2) + (b_1, b_2) = (a_1 +_1 b_1, a_2 +_2 b_2) \in R_1 \times R_2$$

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \circ_1 b_1, a_2 \circ_2 b_2) \in R_1 \times R_2$$

$$(R_1 \times R_2, \circ) \text{ es asociativa}$$



cont

cont.

$$\begin{aligned}(a_1, a_2) \cdot ((c_1, c_2) + (d_1, d_2)) &= (a_1, a_2) \cdot (a_1+d_1, c_2+d_2) = \\&= (a_1(c_1+d_1), a_2(c_2+d_2)) = (a_1c_1+a_1d_1, a_2c_2+a_2d_2) = \\&= (a_1c_1, a_2c_2) + (a_1d_1, a_2d_2) = [(a_1, a_2) \cdot (c_1, c_2)] + [(a_1, a_2) \cdot (d_1, d_2)]\end{aligned}$$

// faltaria demostrar hacia el otro lado, pero es distributiva
 $(a_1, a_2) \cdot ((c_1, c_2) + (d_1, d_2)) = (a_1, a_2)$

Definición de subanillo

Sea $(R, +, \cdot)$ un anillo. Un subconjunto $S \subseteq R$ tq $(S, +, \cdot)$ es anillo, se dice que es subanillo de $(R, +, \cdot)$.

Caracterización de subanillo

Sea $(R, +, \cdot)$ un anillo. Un subconjunto no vacío $\emptyset = S \subseteq R$ es subanillo de $(R, +, \cdot)$ si y solo si:

- ① $\forall a, b \in S$ se cumple que $a - b \in S$
- ② $\forall a, b \in S$ se cumple que $a \cdot b \in S$

demos 1 y 2:

" \Rightarrow " Si $(S, +, \cdot)$ es subanillo de $(R, +, \cdot)$ $\Rightarrow (S, +)$ es subgrupo de $(R, +)$
 $\Rightarrow \forall a, b \in S$, $a - b \in S$ y $S \neq \emptyset$ // caracteriz. de subgrupos
y como $(S, +, \cdot)$ es subanillo de $(R, +, \cdot)$ $\Rightarrow (S, +, \cdot)$ es anillo \Rightarrow
 \Rightarrow el producto es operación binaria
interna $\forall a, b \in S \Rightarrow a \cdot b \in S$

" \Leftarrow " Si $S \neq \emptyset$ y $\forall a, b \in S$ $a - b \in S$ $\Rightarrow (S, +)$ es subgrupo de $(R, +)$

$\Rightarrow (S, +)$ es grupo abeliano

$\cdot (R, +) \Rightarrow (S, +)$ es grupo abeliano

$\cdot \forall a, b, c \in S \Rightarrow a, b, c \in R \Rightarrow a \cdot (b + c) = (a \cdot b) + c$ porque $(R, +, \cdot)$ es anillo

$\cdot \forall a, b, c \in S \Rightarrow a, b, c \in R \Rightarrow a \cdot (b + c) = a \cdot b + a \cdot c$ $\left. \begin{array}{l} \text{por ser} \\ (b+c) \cdot a = b \cdot a + c \cdot a \end{array} \right\} (R, +, \cdot)$ anillo

Estudiar si el es subanillo

- De $(R, +, \cdot)$

$(Q[\sqrt{3}], +, \cdot)$

Mundo $Q[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in Q\}$

cont. \Rightarrow

cont.

$$\textcircled{1} \cdot (a+b\sqrt{3}) - (c+d\sqrt{3}) = (a-c) + (b-d)\sqrt{3} = x+y\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$$

$$a, b, c, d \in \mathbb{Q} \Rightarrow a-c = x \in \mathbb{Q}, b-d = y \in \mathbb{Q}$$

$$\cdot (a+b\sqrt{3})(c+d\sqrt{3}) = (ac+3bd) + \sqrt{3}(ad+bc) = z+\sqrt{3}t \in \mathbb{Q}[\sqrt{3}]$$

$$a, b, c, d \in \mathbb{Q} \Rightarrow ac+3bd = z \in \mathbb{Q}, ad+bc = t \in \mathbb{Q}$$

\textcircled{2} d tiene identidad?

$$1_2 = 1 + 0\sqrt{3} = 1 \in \mathbb{Q}$$

Es comunitativo

d es de división?

$$a+b\sqrt{3} \in \mathbb{Q}[\sqrt{3}] \text{ tq } a+b\sqrt{3} \neq 0 \in \mathbb{Q}$$

$$(a+b\sqrt{3})^{-1} = \frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{a^2-3b^2} = \frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3} = c+d\sqrt{3} \quad c, d \in \mathbb{Q}$$

porque

$$a^2-3b^2 \neq 0$$

\Updownarrow

Es de división

$$\frac{a^2}{b^2} + 3 \quad (\text{3 es primo})$$

$$3 + \left(\frac{a}{b}\right)^2$$

Es correcto ✓

\textcircled{3} Estudiar si es subanillo

De $(\mathbb{C}, +, \cdot)$

$(\mathbb{Z}[i], +, \cdot)$

$$\text{Miendo } \mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\} \quad \mathbb{Z}[i] \neq \emptyset$$

$$\cdot (a+bi) - (c+di) = (a-c) + (b-d)i = x+yi \in \mathbb{Z}[i]$$

$$x = a-c \in \mathbb{Z}$$

$$y = b-d \in \mathbb{Z}$$

$$\cdot (a+bi)(c+di) = (ac-bd) + (ad+bc)i = z+ti \in \mathbb{Z}[i]$$

$$ac-bd = z \in \mathbb{Z}$$

$$ad+bc = t \in \mathbb{Z}$$

Es cierto ✓

Es comunitativo

Tiene identidad (el 1)

No es de división (\textcircled{4})

$$(a+bi)^{-1} = \frac{1}{a+bi} =$$

$$= \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i =$$

$$= x+yi$$

$$x = \frac{a}{a^2+b^2}$$

No se multiplican entre sí
entre sí no se multiplican

$y = \frac{b}{a^2+b^2}$

□ Estudiar si es subanillo

De $(\mathbb{C}, +, \cdot)$

módulo \mathfrak{p}

$(\mathbb{Z}_p[i], +_p, \cdot_p)$

$$\text{tiendo } \mathbb{Z}_p[i] = \{a+bi : a, b \in \mathbb{Z}_p\} \neq \emptyset$$

$$\cdot (a+bi) - (c+di) = (a-c) + (b-d)i \in \mathbb{Z}_p[i]$$

$$a-c = x \in \mathbb{Z}_p$$

$$b-d = y \in \mathbb{Z}_p$$

$$\cdot (a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i \in \mathbb{Z}_p[i]$$

$$\frac{1}{a+bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i = ([a]_p \cdot [a^2+b^2]_p^{-1}) - ([b]_p \cdot [a^2+b^2]_p^{-1})i$$

si $p \rightarrow \exists i' \in \{1, 2, \dots, p-1\}$

ej: $p=5$ $(1+2i)^{-1}$ al calcular el inverso me quedé de denominador el 0 \rightarrow No hay inverso

□ Estudiar si es subanillo

De $R = \mathbb{R}^{2 \times 2}$

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}; a \in \mathbb{R} \right\} \neq \emptyset$$

En caso afirmativo estudiar si tiene identidad e inverso el elemento identidad de R y S .

$$\cdot \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ 0 & 0 \end{pmatrix} \text{ es}$$

$$\cdot \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \text{ es}$$

es anillo ✓

¿Identidad? $I_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (de R)

$I_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ (de S)

— esto no pasaba en grupos pq: $(a, *)$ q, $\forall a \in S \exists a^{-1} \in S$: $a^{-1}a = e$

pero en anillos, el elemento identidad no está relacionado con todos los inversos del anillo (de hecho en S no está relacionado con ninguno)

■ Estudiar si el subanillo

$$\text{DO } \mathbb{N} = \mathbb{Z} \times \mathbb{Z}$$

$$S = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : 2 | (a+b)\} \neq \emptyset$$

$$\textcircled{1} (a,b) - (c,d) = (a-c, b-d) \in S$$

$$2 | a-b \quad 2 | c-d \Rightarrow a = b + 2q \quad c = d + 2h \Rightarrow a-c = b-d + 2(q-h) \Rightarrow \\ \Rightarrow 2 | ((a-c) - (b-d)) \in S$$

$$\textcircled{2} (a,b) \cdot (c,d) = (ac, bd)$$

$$ac - bd = (b+2q)(2+2h) - bd = bd - b2h - d2q + 4hq - bd = \\ = 2(-bh - dq + 2hq)$$

(empezó con ap Alicia:)

3.2 Dominios de Integridad

> Divisores de cero y unidades: sea $(R, +, \cdot)$ un anillo y sea $R^* = R - \{0_R\}$:

• divisor de cero del anillo: $\exists r \in R^* \text{ tq } \exists s \in R^* \text{ tq } r \cdot s = 0_R$

• unidad del anillo: $a \in R^*$, si existe $a' \in R^*$ tq $a \cdot a' = a' \cdot a = 1_R$ (los únicos elementos que tienen inverso en el propio anillo)

$(R, +, \cdot)$ el anillo con identidad 1_R (y por tanto $1_R \in R^* \neq \emptyset$)

Un anillo comunitativo, con identidad y sin divisores de cero se llama dominio de integridad.

■ Ejemplo: Divisores de cero y unidades ($\mathbb{Z}_{18}, +_{18}, \cdot_{18}$)

En este caso, todos los divisores de 18 son divisores de 0 (C_{18})

$$C_{18} = \{2, 4, 6, 8, 10, 12, 14, 16, 3, 9, 15\} \text{ wtj? } (\vdash \text{mcd}\{18, a_{18}\} \neq 1, \underline{\text{creo}}) \stackrel{\text{TOPQ}}{a_{18} \cdot x = [0]_{18}} \stackrel{\text{ej: }}{12 \cdot 3 = 36 = [0]_{18}}$$

$$\text{unidades: } U_{18} = \{1, 5, 7, 11, 13, 17\} \quad C = \text{mcd}\{18, u_{18}\} = 1, \underline{\text{creo}}$$

* En los anillos de división no hay divisores de cero: si $(R, +, \cdot)$ es un anillo de división y $a, b \in R$ tq $a \cdot b = 0_R \Rightarrow a = 0_R \text{ o } b = 0_R$

> Anillo de unidades de un anillo con identidad

sea $(R, +, \cdot)$ un anillo con identidad y sea $U_R = \{a \in R : a \text{ unidad de } R\}$
se verifica que (U_R, \cdot) es un grupo, y ademas no vacío, $\neq \emptyset$, porque
 $1_R \in R, \in U_R$.

Exercicio: obtener el grupo de unidades del anillo $(R^{2 \times 2}, +, \cdot)$

$$R^{2 \times 2} = \left\{ \begin{pmatrix} ab \\ cd \end{pmatrix} : a, b, c, d \in R \right\}$$

$$U_{R^{2 \times 2}} = GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} ab \\ cd \end{pmatrix} \in R^{2 \times 2} : ad - bc \neq 0 \right\}$$

> Caracterización de dominios de integridad: Propiedad cancelativa

sea $(R, +, \cdot)$ un anillo conmutativo y con identidad. Entonces $(R, +, \cdot)$ es dominio de integridad \Leftrightarrow para todos $a, b, c \in R$ tq $a \neq 0_R$ y $a \cdot b = a \cdot c$
se verifica $b = c$

demonstración: Alicia

Ej: estudiar si $(\mathbb{Z}_{24}, +_{24}, \cdot_{24})$ es dominio de integridad

No porque por ej. 2 es divisor de 0.

$$\begin{aligned} 2 \cdot 12 &= 24 = [0]_{24} \\ 2 \in \mathbb{Z}_{24} \\ 12 \in \mathbb{Z}_{24} \end{aligned}$$

$$\langle Q \times \emptyset, +, \cdot \rangle$$

$$\begin{matrix} (1, 0) \cdot (0, 1) &= (0, 0) \\ \times & \times \\ (0, 0) & \end{matrix} \quad \text{por tanto } (1, 0) \text{ y } (0, 1) \text{ div. 0}$$

$(\mathbb{Z}_7, +_7, \cdot_7)$ si es dominio de integridad ya que no tiene divisores de 0.

> Relación entre dominios de integridad y cuerpos:

1. Todo cuerpo es un dominio de integridad.

2. Todo dominio de integridad finito es cuerpo.

]- demo: Alicia

> Operaciones sucesivas en anillos

sea $(R, +, \cdot)$ un anillo. Para todo $a \in R$ y para todo $r \in \mathbb{N}$ se escribe

$$ra = \underbrace{a + \dots + a}_r$$

$$1. (rs)a = r(sa)$$

$$2. r(a+b) = (ra) + (rb)$$

> Definición de característica de un anillo

sea $(R, +, \cdot)$ un anillo y sea $C = \{n \in \mathbb{N} : na = 0_R \text{ para todo } a \in R\}$

si $C \neq \emptyset$ se llama característica de R al valor $c(R) = \min(C)$

si $C = \emptyset$, el anillo tiene característica cero $c(R) = 0$

Ejercicio: calcular la característica de $(\mathbb{Z}_{24}, +_{24}, \cdot_{24})$

$$C = \{n \in \mathbb{N} : na = 0 \text{ para todo } a \in \mathbb{Z}_{24}\} = \{24h : h \in \mathbb{N}\}$$

$$c(\mathbb{Z}_{24}) = 24$$

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

$C = \emptyset$ porque $n(1, 0) \neq (0, 0) \forall n \in \mathbb{N}$

↳

$$c(\mathbb{Q} \times \mathbb{Q}) = 0$$

> Característica de anillos con identidad

sea $(R, +, \cdot)$ un anillo con identidad $1_R \in R$

1. si el orden de $1_R \in R$ en el grupo aditivo $(R, +)$ es finito entonces $c(R) = |1_R|$ [demostración]
2. si el orden de $1_R \in R$ en el grupo aditivo $(R, +)$ es infinito entonces $c(R) = 0$. [Altura]

> Característica de un dominio de integridad

La característica de un dominio de integ. es cero o un nº primo

demo. Alicia

> Característica de un cuerpo

cero o un nº primo (ya que todo cuerpo es un D. I.)

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

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

$(\mathbb{Z}[\sqrt{2}], +, \cdot)$ es subanillo de $(\mathbb{R}, +, \cdot)$

0) $\mathbb{Z}[\sqrt{2}] \neq 0$ pq $0 \in \mathbb{Z}[\sqrt{2}]$

1) $x, y \in \mathbb{Z}[\sqrt{2}] \quad \& x-y \in \mathbb{Z}[\sqrt{2}] ?$

$$\begin{cases} x = a + b\sqrt{2} \\ y = c + d\sqrt{2} \end{cases} \Rightarrow x - y = (a - c) + (b - d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

→ cont.

cont.

2) $\forall x, y \in \mathbb{Z}[\sqrt{2}]$ d $x, y \in \mathbb{Z}[\sqrt{2}]?$

$$\begin{array}{l} x = a + b\sqrt{2} \\ y = c + d\sqrt{2} \end{array} \Rightarrow xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

$\Rightarrow (\mathbb{Z}[\sqrt{2}], +, \cdot)$ es anillo ✓

Es comunitativo ✓ pq $(R, +, \cdot)$ lo es

Tiene identidad ✓ : $1 \in \mathbb{Z}[\sqrt{2}]$: $1 = 1 + 0\sqrt{2}$

No es de división ✗ : $1 + \sqrt{2}$ no tiene inverso en $\mathbb{Z}[\sqrt{2}]$

3.3 IDEALES Y ANILLOS COUENTES

> sea $(R, +, \cdot)$ un anillo y sea $I \subseteq R$ un subconjunto de $(R, +, \cdot)$.

Se dice que I es ideal si para todos $r \in R$ y $a \in I$ se verifica:

$$r \cdot a \in I \text{ y } a \cdot r \in I$$

- $I_0 = \{0_R\}$ se dice que es el ideal trivial de $(R, +, \cdot)$

- Un ideal $I \subseteq R$ de $(R, +, \cdot)$ se dice que es propio si $I \neq R$

- El mínimo ideal que contiene a $a_1, \dots, a_n \in R$ se denomina ideal generado por $\{a_1, \dots, a_n\}$, se nota $(a_1, \dots, a_n)_I$, o, si no hay lugar a confusión (a_1, \dots, a_n) y es la intersección de todos los ideales que contienen a $\{a_1, \dots, a_n\} \subseteq R$.

- Un ideal $I \subseteq R$ de $(R, +, \cdot)$ se dice que es principal si existe $a \in R$ tal que $I = (a)$.

> Caracterización de ideal

Sea $(R, +, \cdot)$ un anillo. Un subconjunto no vacío $\phi \neq I \subseteq R$ es ideal de $(R, +, \cdot)$ si y solo si:

1. Para todos $a, b \in I$ se verifica que $a - b \in I$

2. Para todos $a \in I$, $r \in R$ se verifica que $ar \in I$ y $ra \in I$

Propiedades:

① Sea $(R, +, \cdot)$ anillo comunitativo con identidad $\Rightarrow (a_1, \dots, a_n) = \{r_1 a_1 + \dots + r_n a_n : r_i \in R\}$

② Sea $(R, +, \cdot)$ anillo con identidad e $I \subseteq R$ un ideal q contiene a $I \cap R \neq \emptyset \Rightarrow I = R$

③ Un cuerpo no tiene ideales propios ni triviales

Características ideales

$$\textcircled{1} \text{ En } (\mathbb{Z}_4, +_4, \cdot_4), S_4 = \langle [2]_4, [2]_4 \rangle$$

$$\begin{aligned} a-b &\in S_4 \quad \forall a, b \in S_4 \\ a+r &= 2n \quad \forall a \in S_4 \quad \underline{\text{es ideal}} \\ &\in S_4 \quad r \in \mathbb{Z}_4 \end{aligned}$$

$$\textcircled{2} \text{ En } (\mathbb{R}[x], +, \cdot), A = \{q \in \mathbb{R}[x] : q(0) = 0\}$$

$$R(x) = \{a_0 + a_1 x + \dots + a_n x^n : n \in \mathbb{N} \cup \{0\} = \{a_0, a_i \in \mathbb{R}\}$$

$$A = \underbrace{\{a_1 x + \dots + a_n x^n : n \in \mathbb{N}_0, a_i \in \mathbb{R}\}}_{x(a_1, \dots, a_n)}$$

$$h \in A \Leftrightarrow h = x \cdot g \quad \forall h \in A, \forall g \in \mathbb{R}[x] \quad h \cdot g = x \cdot g = \underline{x(gg)} \in A$$

$$(hg)(0) = h(0)g(0) = 0 \quad g(0) = 0 \Rightarrow \underline{hg \in A}$$

$$\textcircled{3} \text{ } (\mathbb{Z} \times \mathbb{Z}_3, +, \cdot), S_5 = \{(a, b) : a \equiv b \pmod{3}\}$$

$$a \equiv b \pmod{3}$$

$$c \equiv d \pmod{3}$$

No es ideal, pero sí es subanillo

$$a-c \equiv b-d \pmod{3} \Rightarrow (a-c, b-d) \in S_5$$

$$(a, b) - (c, d) = (a-c, bd)$$

$$(ac, bd) \quad ac \equiv bd \pmod{3}$$

$$(1, 2) \in \mathbb{Z}, (2, 2) \in S_5$$

$$\textcircled{4} \text{ } (\mathbb{Z}_6 \times \mathbb{Z}_6, +_6, \cdot_6), S_6 = \{([0]_6, [0]_6), ([1]_6, [1]_6)\}$$

No es ideal, pero sí subanillo.

> Todo ideal de $(\mathbb{Z}, +, \cdot)$ es principal

↑
el anillo de los enteros

> Anillo cociente

Sea $(R, +, \cdot)$ un anillo y $I \subseteq R$ subanillo de R . En el conjunto cociente $R/I = \{[r]_I = r+I : r \in R\}$ se definen las operaciones suma y producto módulo I : $[r]_I +_I [s]_I = [r+s]_I$. $(R/I, +_I, \cdot_I)$ es un anillo, que se denomina anillo cociente $\Leftrightarrow I$ es un ideal de $(R, +, \cdot)$.

(> Ideal generados:)

$$\langle a \rangle = \{ah : h \in R\}$$

$(R, +, \circ)$ anillo comutativo con identidad $\Rightarrow \langle a_1, \dots, a_n \rangle = \{r_1a_1 + \dots + r_na_n : r_k \in R\}$

① $M = \{r_1a_1 + \dots + r_na_n : r_k \in R\}$ es un ideal

② Todo ideal que contenga a a_1, \dots, a_n , necesariamente debe contener a M .

(> Teorema:)

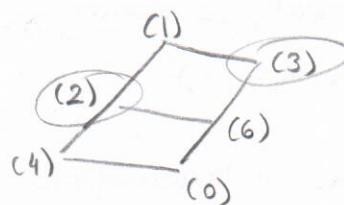
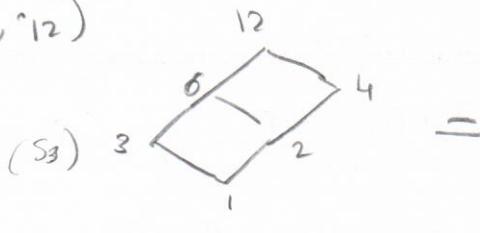
Un cuerpo no tiene ideales propios ni triviales.

$(K, +, \cdot)$ es cuerpo $I \subset K$ ideal $I \neq \{0_K\} \exists a \in I$ con $a \neq 0_K \exists a' \in K$
 $\Rightarrow a'a = 1_K \in I \Rightarrow \underline{\underline{I=K}}$

> Ideales Maximales

Un ideal propio $M \subset R$ de un anillo comutativo $(R, +, \circ)$ se dice que es ideal maximal si para todo ideal I tal que $M \subset I \subset R$ se verifica que $M = I$ o $I = R$.

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



¡siempre generados por primos!

Estos son maximales porque no tienen nada por encima (más que el total)

Todo cuerpo tiene 2 ideales,

el 0 y el resto del cuerpo

Ideal maximal \rightarrow el ideal más grande $\rightarrow M \subseteq I \subseteq R \text{ tq } M > I \text{ o } I = R$

Ej:

① En $(\mathbb{Z}, +, \cdot)$, $A = \{2\}$ es maximal (el siguiente sea $A = \{1\}$ que es = a total)

② En $(\mathbb{Z}, +, \cdot)$, $A = \{q\}$ no es maximal

$$\{qh : h \in \mathbb{Z}\} \neq \{q : q \in \mathbb{Z}\} \neq \mathbb{Z}$$

> Caracterización de ideales maximales en $(\mathbb{Z}, +, \cdot)$

sea $p \in \mathbb{Z}^+$. En $(\mathbb{Z}, +, \cdot)$ el ideal $(p) = p\mathbb{Z}$ es maximal $\Rightarrow p$ primo.

> Ideales maximales y cuerpos

sea $(R, +, \cdot)$ un anillo comutativo con identidad y sea M un ideal de R , entonces M es maximal en R si y solo si $(R/M, +_M, \cdot_M)$ es cuerpo.

* Si un ideal contiene la identidad, entonces es el total (denotado claramente)

3.4) Homomorfismo de anillos

Si $(R, +_1, \cdot_1)$ y $(S, +_2, \cdot_2)$ son anillos, un homomorfismo de anillos es una aplicación $\varphi: R \rightarrow S$ tq para todos $a, b \in R$ se verifica:

$$\varphi(a+_1 b) = \varphi(a) +_2 \varphi(b) \quad y \quad \varphi(a \cdot_1 b) = \varphi(a) \cdot_2 \varphi(b).$$

Núcleo de φ : $\text{Ker}(\varphi) = \{r \in R : \varphi(r) = 0_S\}$

Imagen de φ : $\varphi(R) = \{\varphi(r) : r \in R\}$

Un homomorfismo biyectivo es un isomorfismo

> Propiedades de homomorfismos de anillos

$\varphi: R \rightarrow S$ un homomorfismo entre $(R, +_1, \cdot_1)$ y $(S, +_2, \cdot_2)$:

$$\textcircled{1} \quad \varphi(0_R) = 0_S$$

$$\textcircled{2} \quad \varphi(-a) = -\varphi(a)$$

> El núcleo es ideal, la imagen es subanillo, (φ es un homomorfismo de anillos de $(R, +_1, \cdot_1)$ de $(S, +_2, \cdot_2)$)

> Caracterización de los homomorfismos de $(\mathbb{Z}_n, +_n, \cdot_n)$ en $(\mathbb{Z}_m, +_m, \cdot_m)$

Sea $\varphi: \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ una aplicación de $(\mathbb{Z}_n, +_n, \cdot_n)$ en $(\mathbb{Z}_m, +_m, \cdot_m)$

φ es un homomorfismo de anillos $\Leftrightarrow \varphi([1]_n) = [1]_m$ siendo

$$nK \equiv 0 \pmod{m}$$

$$K^2 \equiv 1 \pmod{m}$$

■ Probar si el homomorfismo

$$\phi: \mathbb{C} \rightarrow \mathbb{R}^{2 \times 2} \text{ definido por: } \phi(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

$a, b \in \mathbb{C}$

$$-\phi((a+bi)+(c+di)) = \phi((a+c)+(b+d)i) = \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \phi(a+bi) + \phi(c+di)$$

$$-\phi((a+bi)(c+di)) = \phi((ac-bd) + (ad+bc)i) =$$

$$= \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \phi(a+bi) \cdot \phi(c+di) \quad \checkmark$$

$$\text{además: } \text{Ker } \phi = \{a+bi \in \mathbb{C} : \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\}$$

Ejemplos: (caracteriz.)

$\phi: \mathbb{Z}_4 \rightarrow \mathbb{Z}_6$ definido por $\phi([a]_4) = [2a]_6$. No es homomorfismo de grupos.

$\phi: \mathbb{Z}_6 \rightarrow \mathbb{Z}_{18} : \phi([a]_6) = [3a]_{18}$ sabemos $3^2 \equiv 1 \pmod{6}$

$$3^2 \equiv 3 \pmod{18} \text{ ¡NO!}$$

↑ por tanto

Es homomorfismo de grupos,
pero no es homomorfismo de anillos.

> Homomorfismos destacables

① Si $C[a,b] = \{f: [a,b] \rightarrow \mathbb{R}\}$ es continua } en el cto. de funciones continuas en un intervalo $[a,b]$,

para todo $\alpha \in [a,b]$, la app. $\psi_\alpha: C[a,b] \rightarrow \mathbb{R}$ definida por $\psi_\alpha(f) = f(\alpha)$ es un homomorfismo de anillos que recibe el nombre de homomorfismo de evaluación en α .

② Si I un ideal del anillo $(R, +, \cdot)$, la app. $\Psi: R \rightarrow R/I$ definida por $\Psi(x) = [x]_I = x + I$ es un homomorfismo de anillos, llamado homomorfismo canónico y su núcleo es $\text{Ker}(\Psi) = I$.

③ Si $(R, +, \cdot)$ es un anillo con identidad $1_R \in R$, entonces la aplicación $\phi: \mathbb{Z} \rightarrow R$ definida por $\phi(n) = n \cdot 1_R$ es un homomorfismo de anillos.

> 1º teorema de isomorfía de anillos

Sea $\varphi: R \rightarrow S$ un homomorfismo del anillo $(R, +, \cdot)$ en el anillo $(S, +_2, \cdot_2)$. Entonces la aplicación $\eta: R/\text{ker}(\varphi) \rightarrow \varphi(R)$ definida por $\eta([a]_{\text{ker}(\varphi)}) = \varphi(a)$ es un isomorfismo de anillos.

> Todo anillo con identidad contiene un subanillo isomorfo a \mathbb{Z} o a \mathbb{Z}_n

Sea $(R, +, \cdot)$ un anillo con identidad.

a) Si $c(R) = n > 0$ entonces R contiene un subanillo isomorfo a \mathbb{Z}_n

b) Si $c(R) = 0$ entonces R contiene un subanillo isomorfo a \mathbb{Z}

18.5 | Anillos de Polinomios

> Polinomios sobre un anillo:

Sea $(R, +, \cdot)$ un anillo. Un polinomio sobre R es una sucesión infinita de elementos de R , indexados con enteros no negativos, tales que existe un entero $n \geq 0$ tal que $a_i = 0$ para todo $i > n$,

$$(a_0, a_1, a_2, \dots, a_n, 0_R, 0_R, \dots) = a_0 + a_1x + \dots + a_n x^n = \sum_{i=0}^n a_i x^i$$

NOTACIÓN

• Polinomios sobre $\mathbb{Z}[x]$

$$(0, 0, 0, 0, \dots) = 0 \in \mathbb{Z}[x] \quad (\text{polinom. nulo})$$

$$(1, 0, 0, 0, \dots) = 1 \in \mathbb{Z}[x]$$

$$(0, x, 0, 0, \dots) = x \in \mathbb{Z}[x]$$

> Coeficientes, grado y polinomio nulo e identidad

Sea $(R, +, \cdot)$ anillo.

los coeffs. son los

$\neq q \in R$

• Si $f = \sum_{k=0}^n a_k x^k \in R[x]$, los valores $a_0, a_1, \dots, a_n \in R$ se denominan coeficientes y se dice que f es un polinomio con coeficientes en R .

de llama polinomio nulo al polinomio cuyos coeficientes son todos iguales a $0_R \in R$.

tipos x / → Anillo de polinomios

sea

• Si f es un polinomio no nulo, se llama grado de f al mayor entero no negativo $n \in \mathbb{N} \cup \{0\}$ para el cual $a_n \neq 0_R$ y se escribe $gr(f) = n$. El grado del polinomio nulo es $-\infty$. Si $gr(f) \leq 0$ se dice que f es un polinomio constante.

• Si $gr(f) = n > 0$, al coeficiente a_n se le llama coeficiente principal (término de mayor grado) y se escribe $cp(f) = a_n$.

En un anillo con identidad $1_R \in R$, un polinomio no nulo $f \in R[x] - \{0_R\}$ se dice que es un polinomio monico si su coeficiente principal es $cp(f) = 1_R$.

> Anillo de polinomios

Sea $(R, +, \cdot)$ anillo conmutativo con identidad.

Para todos $f = \sum_{k=0}^r a_k x^k, g = \sum_{k=0}^s b_k x^k \in R[X]$ se define:

$$f+g = \sum_{k=0}^{\max\{r,s\}} (a_k + b_k) x^k, f \cdot g = \sum_{k=0}^{r+s} \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

Si $(R, +, \cdot)$ es anillo conmutativo con identidad entonces $(R[X], +, \cdot)$ es anillo conmutativo con identidad $1_{R[X]} = (1_R, 0_R, \dots) \in R[X]$. Su cero es el polinomio nulo: $0_{R[X]} = (0_R, 0_R, \dots) \in R[X]$. $(R[X], +, \cdot)$ contiene un subanillo isomorfo a $(R, +, \cdot)$.

> Función polinomial:

Sea $(R, +, \cdot)$ anillo. Para cada polinomio $f = \sum_{k=0}^r a_k x^k \in R[X]$, se llama función polinomial f a la aplicación $f: R \rightarrow R$, definida para $r \in R$ por $f(r) = \sum_{k=0}^r a_k r^k \in R$. Se dice que $\alpha \in R$ es una raíz de $f \in R[X]$ si verifica que $f(\alpha) = 0_R \in R$.

> Polinomios sobre un dominio de integridad

Si $(D, +, \cdot)$ es un dominio de integridad $\Rightarrow \forall f, g \in D[X]$ se verifica:

$$\text{gr}(f \cdot g) = \text{gr}(f) + \text{gr}(g)$$

Por tanto $(D[X], +, \cdot)$ es un dominio de integridad

~~D~~ Si $(R, +, \cdot) = (\mathbb{Z}_4, +_4, \cdot_4)$ \rightarrow este no es D.I.

~~(2x+1)(2x+1) = 4x^2 + 4x + 1 (= 1)~~ \rightarrow Muy? No serían 1 y 2? \boxed{D}

grado 0	grado 1
---------	---------

Recuerda: en $(\mathbb{Z}, +, \cdot)$: todos sus ideales son principales
los ideales maximales están generados por primos

> Los ideales de $(K[x], +, \cdot)$ son principales

Si $(K, +, \cdot)$ es cuerpo \rightarrow todo ideal en $(K[x], +, \cdot)$ es principal

> Polinomios irreducibles en $D[X]$

$(D, +, \cdot)$ dom. de integridad

$f \in D[X]$ con $\text{gr}(f) \geq 0$ es irreducible en $D[X]$ si:

- f no es unidad en $D[X]$

- $f = g \cdot h$ con $g, h \in D[X] \Rightarrow g \circ h$ es unidad de $D[X]$

> Polinomios irreducibles en $K[x]$

$(K, +, \cdot)$ cuerpo

$f \in K[x]$ con $\text{gr}(f) = n > 0$ es irreducible en $K[x]$ si:

• si $f = g \cdot h$ con $g, h \in K[x] \Rightarrow \text{gr}(gh) = \text{gr}(g) + \text{gr}(h) = \text{gr}(f)$

> Ideales maximales en $K[x]$

Lean ~~BKR~~ $(K, +, \cdot)$ cuerpo y $f \in K[x]$

f es maximal en $K[x] \Leftrightarrow f$ es irreducible en $K[x]$

[> Teorema del resto

$(K, +, \cdot)$ cuerpo, $f \in K[x]$ con $\text{gr}(f) = n > 0$.

$\alpha \in K$, $f(\alpha)$ es el resto obtenido al dividir f entre $x - \alpha$

[> Teorema del factor

$(K, +, \cdot)$ cuerpo, $f \in K[x]$ con $\text{gr}(f) = n > 0$

$\alpha \in K$ es raíz de $f \Leftrightarrow (x - \alpha)$ divide a f en $K[x]$

> Polinomios irreducibles en $C[x]$

$f \in C[x]$ es irreducible en $C[x] \Leftrightarrow \text{gr}(f) = 1$

> Polinomios irreducibles en $R[x]$

$f \in R[x]$ es irreducible en $R[x] \Leftrightarrow \text{gr}(f) = 1$ o bien es:

$$f = a_0 + a_1 x + a_2 x^2 \text{ con } a_1^2 - 4a_2 a_0 < 0$$

En $Q[x]$ > Lema de Gauss

Lean $f \in Z[x]$ y $\alpha, \beta \in Q[x]$ tales que $f = \alpha \cdot \beta$ con $\text{gr}(\alpha), \text{gr}(\beta) < \text{gr}(f)$

\Rightarrow existen polinomios $a, b \in Z[x]$ tales que $f = a \cdot b$ y

$$\text{gr}(a) = \text{gr}(\alpha) \quad y \quad \text{gr}(b) = \text{gr}(\beta)$$

en $Q[x]$ > criterio de raíces racionales

Lean $\frac{r}{s} \in Q$ raíz de $f = a_0 + a_1 x + \dots + a_n x^n \in Z[x]$ con $\text{med}(r, s) = 1$

$$\text{gr}(f) = n \geq 1 \quad y \quad a_0 \neq 0 \Rightarrow$$

$$r | a_0 \quad y \quad s | a_n$$

II) Estudiar si es irreducible en $\mathbb{Q}[x]$

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

Tendrá 3, pq un polinomio f de grado n , en \mathbb{C} , tiene n raíces

Potenciales raíces: (racionales!, complejas tb tendrá p.ej):

$$+1, -1, \pm 2, -2, \pm \frac{1}{3}, -\frac{1}{3}, \pm \frac{2}{3}, -\frac{2}{3} \quad \text{En } \mathbb{Q}: \text{ las raíces deben ser:}$$

Comprobamos si alguna de ellas lo es:

$$3\left(\frac{2}{3}\right)^3 - 2\left(\frac{2}{3}\right) + 3\left(\frac{2}{3}\right) - 2 = 0 \quad \checkmark \quad \frac{2}{3} \text{ es raíz}$$

$$\begin{array}{c|cc} f & r_2 & s_3 \\ \hline a_0 & & a_3 \\ & \ddots & \ddots \\ & & a_n \end{array}$$

de lo reducible

En $\mathbb{Q}[x]$ > Criterio de Eisenstein

Dado $f = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{Z}[x]$ con $\text{mcd}(a_0, \dots, a_n) = 1$,

existe $p \in \mathbb{N}$ primo, verificando que:

① $p \mid a_i \quad \forall i \in \{1, \dots, n-1\}$

② $p \nmid a_0$

③ $p^2 \nmid a_0$

$\Rightarrow f$ es irreducible en $\mathbb{Q}[x]$

II) Estudiar si es irreducible en $\mathbb{Q}[x]$

$$x^{10} + 4x^7 - 18x - 14$$

$$\exists p=2 \text{ (primo)} \quad \begin{aligned} p &\mid 14 & p &\nmid 1 & p &\nmid 4 \end{aligned} \Rightarrow \text{Irreducible}$$

$$px_1 \quad p^2x_{14}$$

II) Estudiar si es irreducible en $\mathbb{Q}[x]$

$$x^4 + 3x + 6$$

$$p=3$$

$$p \mid 6 \quad p \mid 3$$

\Rightarrow Irreducible

$$px_1 \quad p^2 \nmid 6$$

$$x^{24} - 12$$

$$p=2$$

$$3 \mid 12 \quad 3 \nmid 1 \quad 3^2 \nmid 12 \quad \Rightarrow \text{Irreducible}$$

$$3 \mid 0$$

Lemma de la
 $n=1$ a $n=2^3$

$\mathbb{Q}[x]$ > Criterio de reducibilidad módulo primo

Sea $f = a_0 + \dots + a_n x^n \in \mathbb{Z}[x]$ con $\text{gr}(f) = n \geq 2$ y $\exists p \in \mathbb{N}$

- primo :
- ① $[f]_p = [a_0]_p + \dots + [a_n]_p x^n \in \mathbb{Z}_p[x]$ es irreducible en $\mathbb{Z}_p[x]$
 - ② $[a_n]_p \neq [0]_p$

entonces f es irreducible en $\mathbb{Q}[x]$

④ Estudiar si es irreducible en $\mathbb{Q}[x]$

$$x^4 + x^3 + 2x - 1 \quad (\overset{x^2=0 \text{ en } \mathbb{Z}_2}{f \in \mathbb{Z}_2})$$

$$\text{en } \mathbb{Z}_2[x] : f \rightarrow [f]_2 = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$$

¿Es irreducible en $\mathbb{Z}_2[x]$?

- ①: $x^4 + x^3 + 1$ no tiene raíces en $\mathbb{Z}_2[x]$ (las únicas posibles serían 0 y 1, y sustituyéndolas en nuestro $f \rightarrow \neq 0$, por tanto no tiene raíces)
- ②: Considerar los polinomios de grado 2 posibles en $\mathbb{Z}_2[x]$

$$x^2 \rightsquigarrow x \cdot x$$

$$x^2 + 1 \rightsquigarrow (x+1)(x-1)$$

$$x^2 + x \rightsquigarrow x(x+1)$$

$x^2 + x + 1 \rightsquigarrow$ es irreducible (lo puedes demostrar además pq. tiene grado 2 y no tiene raíces)

Entonces veo: $x^4 + x^3 + 1 = (x^2 + x + 1)(x^2 + 1) + x$

Lo que se aprecia que mi polinomio es irreducible en $\mathbb{Z}_2[x]$

↓
irreducible en $\mathbb{Q}[x]$

4.1 Cuerpos Finitos

reminder $\mathbb{K}[x]/(h)$ es cuerpo \Leftrightarrow (h) es maximal $\Leftrightarrow h$ es irreducible

ideal (generado por h)

> Cuerpo de orden p^m :

Sean $p \in \mathbb{N}$ primo y $h \in \mathbb{Z}_p[x]$ polinomio irreducible de $\mathbb{Z}_p[x]$.
 $\text{d}e \text{gr}(h) = m \Rightarrow \mathbb{Z}_p[x]/(h)$ es un cuerpo con p^m elementos.

> Cuerpos de Galois

Para todos $p \in \mathbb{N}$ primo y $m \in \mathbb{N}$ se denomina cuerpo de Galois de orden p^m al cuerpo:

$$\mathbb{F}_{p^m} \approx \mathbb{Z}_p[x]/(h) = \{a_0 + a_1 x + \dots + a_{m-1} x^{m-1} : a_i \in \mathbb{Z}_p\}$$

donde $h \in \mathbb{Z}_p[x]$ un polinomio irreducible en $\mathbb{Z}_p[x]$, de grado m .

■ Construir un cuerpo de Galois de 4 elementos:

$4 = 2^2 \rightarrow$ tenemos q construir nuestro cuerpo como

$$\mathbb{Z}_2[x]/(h)$$

donde $\text{gr}(h) = 2$

probamos $h = x^2 + 1$, pero no es irreducible (raíz para (h))

$h = x^2 + x + 1 \in \mathbb{Z}_2[x]$ si es irreducible :

$$\mathbb{Z}_2[x]/(h) = \{a_0 + a_1 x : a_0, a_1 \in \mathbb{Z}_2\} = \{[a_0 + a_1 x] : a_0, a_1 \in \mathbb{Z}_2\}_{x^2 + x + 1}$$

junto en recto!

como h tiene
grado m , mis elementos
tienen grado $m-1$

Elementos del cuerpo:

$+2$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

→ cont.

cont.

$$\begin{array}{c|cccc} & 1 & x & 1+x \\ \hline 1 & 1 & x & 1+x \\ x & x & 1+x & 1 \\ 1+x & 1+x & 1 & x \end{array}$$

$\frac{x^2}{h}$ (q no tengo x^2
en mi cuerpo
como elemento
valido)

$$f: [x^2+x+1]_{(h)} = [0]_{(h)} \Rightarrow$$

$$\Rightarrow [x^2]_{(h)} = [-x-1]_{(h)} \Rightarrow [x-1]_{(h)}$$

$(-1=1$
 $\text{en } \mathbb{Z}_2)$

■ Realizar la siguiente operación en $\mathbb{F}_4 = \mathbb{F}_{2^2} \rightarrow \mathbb{Z}_2[x]$ ②
 $(h) \text{ con grado } = 2$

$$\begin{array}{r} x^3(x+1) \\ \hline x^6 + x^3 \quad | x^2 + x + 1 \\ x^4 - x^3 - x^2 \quad x^2 + 1 \\ \hline x^2 \\ x^2 - x + 1 \\ \hline x+1 \end{array}$$

cojo un (h)
irreducible (ideal)
con grado 2

(1^a forma)
el producto
tene grado
 $4 \rightarrow \notin \mathbb{F}_4$ ③
dividido por el
 (h) !
notas:
- no habla
- grado - 1
- divisores
 (m_1, m_2, \dots, m_n)

(2^a forma) sabemos que
 $h = x^2+x+1 = 0$

$$\begin{aligned} x^3(x-1) &= x^2 \cdot x(x-1) = (x-1) \cdot x \cdot (x-1) = \\ &= x(x^2+1) \text{ etc.} \end{aligned}$$

■ Estudiar si un polinomio h tiene una raíz en \mathbb{F}_4

tiendo: $\mathbb{F}_4 \cong \mathbb{Z}_2[x]/(x^2+x+1)$

$$\text{y } h = x^2+x+1 \in \mathbb{F}_4[x].$$

$$\mathbb{F}_4 = \{0, 1, x, x^2\} \cong \mathbb{Z}_2$$

entonces contiene 1 en \mathbb{F}_4

■ En el nuevo cuerpo que he construido, \mathbb{F}_4 , el polinomio irreducible, h , siempre tiene una raíz⁴

$$x^2+x+1 = x+1 + x+1 \rightsquigarrow \text{un fermín}$$

① Comprobar que $h = x^3 + x + 1$ es irreducible en $\mathbb{Z}_2[x]$
 y obtener el resultado de la div. operación $\mathbb{F}_8 \cong \frac{\mathbb{Z}_2[x]}{(h)}$

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

¿Tiene h alguna raíz en \mathbb{F}_8 ?

$h = x^3 + x + 1 \in \mathbb{Z}_2[x]$ es irreducible

$$\mathbb{Z}_2[x] = \left\{ a_0 + a_1x + a_2x^2 : a_0, a_1, a_2 \in \mathbb{Z}_2 \right\};$$

$$x^3 = x + 1 \quad (x^3/h)$$

$$(x^3 + x^2)(x^2 + x + 1) = (x^2 + x + 1)^2 = x^4 + x^2 + 1 = x(x+1) + x^2 + 1 = \\ = x^2 + x + x^2 + 1 = \underline{\underline{x+1}}$$

del polinomio h
 da raíz es la x , siempre.

② Obtener el resultado de las siguientes operaciones

$$\textcircled{1} \text{ En } \mathbb{F}_4 \cong \mathbb{Z}_2[x]/(x^2 + x + 1) \quad (x+1)^{-1}$$

$$\textcircled{2} \text{ En } \mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3 + x + 1) \quad (x^2 + 1)^{-1}$$

$$\textcircled{1} \quad x^2 + x + 1 = 0 \Rightarrow x(x+1) + 1 = 0 \Rightarrow x(x+1) = 1 \Rightarrow (x+1 = \frac{1}{x}) \Rightarrow (x+1)^{-1} = x$$

$$\textcircled{2} \quad x^3 + x + 1 = 0 \Rightarrow x(x^2 + 1) + 1 = 0 \Rightarrow x(x^2 + 1) = 1 \Rightarrow (x^2 + 1 = \frac{1}{x}) \Rightarrow \\ \Rightarrow (x^2 + 1)^{-1} = x$$

(Método no fiable siempre)

Otro método: si tenemos dos polinomios tg en mod el otro polinomio d podemos calcular el inverso de cualquiera de los dos



Algoritmo para
 expresar $\text{mcd}(f, g) = \lambda f + \mu g$
 (EASA)

$\Leftrightarrow f, g \in \mathbb{K}[X]$ con $\text{gr}(f) \geq \text{gr}(g) \Rightarrow f = g \cdot q + r$ con $\text{gr}(r) < \text{gr}(g)$
 $\text{mcd}(f, g) = \text{mcd}(g, r)$

f		(1, 0)	$1 \cdot f - 0 \cdot g = f$
g		(0, 1)	$0 \cdot f + 1 \cdot g = g$
r_1	q_1	$(a_1, b_1) = (1, 0) - q_1(0, 1)$	$a_1 \cdot f + b_1 \cdot g = r_1$
r_2	q_2	$(a_2, b_2) = (0, 1) - q_2(a_1, b_1)$	$a_2 \cdot f + b_2 \cdot g = r_2$
r_3	q_3	$(a_3, b_3) = (a_1, b_1) - q_3(a_2, b_2)$	$a_3 \cdot f + b_3 \cdot g = r_3$
		⋮ ⋮ ⋮	
0	q_{n+1}		

$$\Leftrightarrow \text{mcd}(f, g) = d = \frac{r_n}{\text{cp}(r_n)} = \frac{a_n}{\text{cp}(r_n)} \cdot f +$$

$$\rightarrow \frac{b_n}{\text{cp}(r_n)} \cdot g$$

$$\lambda = \frac{a_n}{\text{cp}(r_n)}$$

$$\mu = \frac{b_n}{\text{cp}(r_n)}$$

resto	cociente	(1, 0)	
x^2+x+1	x	(0, 1)	
1	$x+1$	$(1, -x-1) = (1, x+1)$	$(x^2+x+1) \cdot 1 + x \cdot (x+1) = 1$

Llego a 1 \rightarrow fin : ¿Cuál sería el inverso de x ?

$$\mu = (x+1) \quad \text{ya que:}$$

$$[1] = \underbrace{[x^2+x+1]}_{x^2+x+1} \cdot [1]_{x^2+x+1} + [x]_{x^2+x+1} \cdot [x+1]_{x^2+x+1}$$

$$[1] = [x]_{x^2+x+1} \cdot [x+1]_{x^2+x+1}$$

Calcular el inverso de g

$$\text{En } \mathbb{F}_3 \cong \mathbb{Z}_2[x] / (x^3 + x + 1)$$

$$g = x^2 + x + 1$$

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

coc.

retos	cocientes	
$x^3 + x + 1$		$(1, 0)$
$x^2 + x + 1$		$(0, 1)$
x	$x + 1$	$(0) - (0, 1) \cdot (x + 1)$ $(1, x+1)$ <small>el $x + 1$ es 0 en \mathbb{Z}_2!</small>
1	$x + 1$	$(0, 1) - ((1, x+1) \cdot (x+1))$ $(-x-1), 1 - (x^2 + 2x + 1) \stackrel{\text{simplificar}}{=} (x+1)x^2$

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

coc.

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

$$\underline{(x^2 + x + 1)^{-1} = x^2}$$

Calcular inverso de g

$$\text{En } \mathbb{Z}_3 / (x^3 + x^2 + x + 2) \cong \mathbb{F}_{3^3}$$

$$g = x^2 + 1$$

$x^3 + x^2 + x + 2$		$(1, 0)$
$x^2 + 1$		$(0, 1)$
1	$x + 1$	$(1, -x-1) \stackrel{\text{simplificar}}{=} (1, 2x+2)$ $-1 = 2 \text{ en } \mathbb{Z}_3$

$$\Rightarrow (x^3 + x^2 + x + 2) \cdot 1 + (x^2 + 1) \cdot (2x + 2) = 1$$

$$\underline{(x^2 + 1)^{-1} = 2x + 2}$$

¿dónde?

$$\begin{array}{r} x^3 + x^2 + x + 2 \\ x^3 + x \\ \hline x^2 + 2 \\ \downarrow \end{array}$$

Coeficientes

> Estructura del grupo aditivo de un cuerpo finito

$(\mathbb{K}, +, \circ)$ cuerpo finito de característica $p \in \mathbb{N}$ primo \Rightarrow el grupo aditivo $(\mathbb{K}, +)$ es isomorfo a un producto directo de grupos cíclicos de orden q :

$$\mathbb{K} \cong \mathbb{Z}_p \times \dots \times \mathbb{Z}_p$$

El orden de \mathbb{K} es p^m para algún $m \in \mathbb{N}$

> Estructura del grupo de unidades de un cuerpo finito

$(\mathbb{K}, +, \circ)$ cuerpo finito de característica $p \in \mathbb{N}$ primo \Rightarrow

el grupo de unidades (\mathbb{K}^*, \circ) acíclico:

$$\mathbb{K}^* \cong \mathbb{Z}_{p^{m-1}}$$

> Polinomio primitivo

Un polinomio $h \in \mathbb{Z}_p[x]$ es irreducible, es un polinomio primitivo si el polinomio x es un generador del grupo unidades (\mathbb{K}^*, \circ) extendido

$$\mathbb{K} = \mathbb{Z}_p[x]/(h)$$

4.2

Obtener el mñ. cuerpo que contiene al anillo indicado

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

$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\} \right\} \quad (a, b) \in \mathbb{Z} \times \mathbb{Z}^*$$

$(a, b) \sim (c, d) \iff ad = bc$

$$[(a, b)] = \frac{a}{b}$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}; \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \Rightarrow (\mathbb{Q}, +, \cdot) \text{ es cuerpo}$$

y además

$$\mathbb{Z} \subset \mathbb{Q}, \forall n \in \mathbb{Z}: n = \frac{n}{1}$$

Mq. que existe \mathbb{K} : $\mathbb{Z} \subset \mathbb{K} \subset \mathbb{Q}$ mdo
 $(\mathbb{K}, +, \cdot)$ cuerpo

además $(\mathbb{Q}, +, \cdot)$ es el cuerpo más pequeño que contiene a $(\mathbb{Z}, +, \cdot)$

¿ $\mathbb{Q} \subset \mathbb{K} \Rightarrow \mathbb{K} = \mathbb{Q}$?

$$\text{sea } \frac{a}{b} \in \mathbb{K} \Rightarrow a, b \in \mathbb{Z} \text{ y } b \neq 0 \Rightarrow a, b \in \mathbb{K} \text{ y } b \neq 0 \Rightarrow$$

$\mathbb{Z} \subset \mathbb{K}$

$$\underset{\mathbb{K} \text{ es cuerpo}}{\Rightarrow} a, b^{-1} \in \mathbb{K} \Rightarrow a \cdot b^{-1} \in \mathbb{K} \Rightarrow \frac{a}{b} = ab^{-1} \Rightarrow \frac{a}{b} \in \mathbb{K}$$

$$\mathbb{K} = \mathbb{Q}$$

por tanto \mathbb{Q} es el cuerpo más pequeño que contiene al anillo de los enteros $(\mathbb{Z}, +, \cdot)$

> Cuerpos mínimos

- Todos cuerpos de característica cero contiene un cuerpo isomorfo a $(\mathbb{Q}, +, \cdot)$

- Todos cuerpos de característica $p \in \mathbb{N}$ primo, contiene un cuerpo isomorfo a $(\mathbb{Z}_p, +_p, \cdot_p)$

Los cuerpos $(\mathbb{Z}_p, +_p, \cdot_p)$ para $p \in \mathbb{N}$ primo, y $(\mathbb{Q}, +, \cdot)$ se denominan cuerpos mínimos o primos.

> Subcuerpos y extensiones de cuerpos

Sean $(K, +, \cdot)$ y $(F, +, \cdot)$ dos cuerpos tales que:

- $K \subseteq F$
- Las operaciones de $(F, +, \cdot)$ restringidas a K coinciden con las operaciones de $(K, +, \cdot)$

Entonces se dice que:

F es un cuerpo de extensión de K

K es subcuerpo de F

$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

> Mínimo subanillo que contiene a un cuerpo y un elemento α

$(F, +, \cdot)$ extensión de K y $\alpha \in F \Rightarrow$

el mínimo subanillo de $(F, +, \cdot)$ que contiene a K y

a α es: $K[\alpha] = \{h(\alpha) : h \in K[x]\} \subseteq F$

> Cuerpo de fracciones

$(D, +, \cdot)$ dominio de integridad, $D^{\times} = D - \{0\}$

en $D \times D^{\times} = \{(a,b) : a, b \in D, b \neq 0\}$, la relación:

$(a,b) \sim (c,d) \Leftrightarrow ad = bc$ es de equivalencia

$F[(a,b)] \in D \times D^{\times} / \sim$ $[c,d] = \frac{a}{b} = \{(a,d) \in D \times D^{\times} : (a,b) \sim (c,d)\}$

en $G(D) = (D \times D^{\times}) / \sim = \left\{ \frac{a}{b} : a, b \in D, \text{ con } b \neq 0 \right\}$

se definen:

$$\frac{a}{b} + \frac{c}{d} = [(a,b)] + [(c,d)] = [(ad+bc, bd)] = \frac{ad+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = [(a,b)] \cdot [(c,d)] = [(ac, bd)] = \frac{ac}{bd}$$

$(G(D), +, \cdot)$ es el mínimo cuerpo que contiene un anillo isomorfo a D , q se denuncia Cuerpo de Fracciones de $(D, +, \cdot)$

> Mínimo cuerpo que contiene un elemento de extensión

$(\mathbb{F}, +, \cdot)$ extensión de \mathbb{K} y $\alpha \in \mathbb{F} \rightarrow$

$$\mathbb{K}(\alpha) = \{g(\mathbb{K}[\alpha]) = \left\{ \frac{g(\alpha)}{h(\alpha)} : g, h \in \mathbb{K}[x], h(\alpha) \neq 0_K \right\} \subseteq \mathbb{F}$$

$\mathbb{K}(\alpha)$ mínimo cuerpo que contiene a \mathbb{K} y a α

$\mathbb{K}(\alpha)$ mínimo anillo que contiene a \mathbb{K} y a α

④ Cuarto cuerpo que contiene a \mathbb{Q} y a α

$$\alpha = \sqrt{2}$$

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{h(\sqrt{2})}{g(\sqrt{2})} : h, g \in \mathbb{Q}[x], g(\sqrt{2}) \neq 0 \right\}$$

$$\begin{aligned} \mathbb{Q}(\sqrt{2}) &= \{h(\sqrt{2}) : h \in \mathbb{Q}[x]\} = \{a_0 + a_1\sqrt{2} + a_2(\sqrt{2})^2 + a_3(\sqrt{2})^3 \dots\} = \\ &= \{a_0 + a_1\sqrt{2} : a_0, a_1 \in \mathbb{Q}\} \end{aligned}$$

$$\frac{1}{a_0 + a_1\sqrt{2}} = \frac{a_0 - a_1\sqrt{2}}{a_0^2 - 2a_1^2} = \frac{a_0}{a_0^2 - 2a_1^2} + \frac{-a_1}{a_0^2 - 2a_1^2} \sqrt{2} = \underline{\underline{b_0 + b_1\sqrt{2}}} \in \mathbb{Q}(\sqrt{2})$$

⑤ Obtener el mínimo cuerpo que contiene a \mathbb{Z} y a α

$$\alpha = \sqrt{6}$$

~~$$\mathbb{Z}(\sqrt{6}) = \left\{ \frac{h(\sqrt{6})}{g(\sqrt{6})} : h, g \in \mathbb{Z}[x], g(\sqrt{6}) \neq 0 \right\}$$~~

~~$$\begin{aligned} \mathbb{Z}(\sqrt{6}) &= \{h(\sqrt{6}) : h \in \mathbb{Z}[x]\} = \{a_0 + a_1\sqrt{6} + a_2(\sqrt{6})^2 \dots\} = \\ &= \{a_0 + a_1\sqrt{6} : a_0, a_1 \in \mathbb{Z}\} \end{aligned}$$~~

El mínimo anillo q contiene a $\sqrt{6}$ si sea un anillo

es (\mathbb{Q})

$$\mathbb{Q}(\sqrt{6}) = \left\{ \frac{a_0 + a_1\sqrt{6}}{b_0 + b_1\sqrt{6}} : a_0, a_1, b_0, b_1 \in \mathbb{Q}, b_0^2 + b_1^2 \neq 0 \right\} =$$

$$= \left\{ (a_0 + a_1\sqrt{6}) \cdot \frac{1}{b_0 + b_1\sqrt{6}} : a_0, a_1, b_0, b_1 \in \mathbb{Q}, b_0^2 + b_1^2 \neq 0 \right\} =$$

$\underline{\underline{= (\mathbb{Q}[\sqrt{6}])}}$

$$\text{west. } \frac{1}{b_0 + b_1 \sqrt{6}} = c_0 + c_1 \sqrt{6}$$

① Encontrar una extensión de \mathbb{R} en la que f tenga una raíz

$$f = x^2 + 1 \in \mathbb{R}[x]$$

$$\textcircled{i} \quad \exists i \in \mathbb{C} \text{ tal que } i^2 + 1 = 0$$

↓ $\mathbb{R}(i)$?

$$\mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\}$$

$$\mathbb{R}(i) = \left\{ \frac{a+bi}{c+di} : a, b, c, d \in \mathbb{R}, c^2 + d^2 \neq 0 \right\} = \mathbb{R}(i)$$

$$\frac{1}{c+di} = \frac{c-di}{c^2+d^2} = \frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}i = a' + b'i \in \mathbb{R}(i)$$

$$\textcircled{ii} \quad x^2 + 1 \in \mathbb{R}[x] \text{ es irreducible en } \mathbb{R}[x] \Rightarrow$$

$$\Rightarrow \mathbb{R}[x]/(x^2 + 1) \text{ es un cuerpo, } \mathbb{C} = \frac{\mathbb{R}[x]}{(x^2 + 1)}$$

en \mathbb{C} hay una raíz de $x^2 + 1 \quad \{a_0 + a_1 x : a_0, a_1 \in \mathbb{R}\}$

$$\begin{matrix} [x^2 + 1] \\ (h) \end{matrix} = \begin{matrix} [0] \\ (h) \end{matrix}$$

\downarrow
 $h = x^2 + 1$

> Teorema de Kronecker

(\mathbb{K}, \circ) cuerpo, $h \in \mathbb{K}[x]$ polinomio irreducible en $\mathbb{K}[x]$ con $\text{gr}(h) > 1$.

- ① Existe \mathbb{F} , cuerpo de extensión de \mathbb{K} , en el cual h tiene una raíz
- ② si $\alpha \in \mathbb{F}$ es raíz de $h \Rightarrow \mathbb{K}(\alpha) \cong \mathbb{K}[x]/(h) \cong \mathbb{K}[\alpha]$

③ Comprobar que el polinomio es irreducible en $\mathbb{Q}[x]$

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

y obtener el mínimo cuerpo, extensión de \mathbb{Q} , en el cual h tiene una raíz.

cont. →

cont.

Es un polinomio de grado 3 \Rightarrow es irreducible \Leftrightarrow no tiene raíces

Potenciales raíces en \mathbb{Q} : $\{\pm 1, \pm 2\} \rightarrow$ No tiene raíces en \mathbb{Q}
es irreducible

ii) α es raíz $x^3 - 4x + 2$

$$\begin{array}{l} \text{mín cuadrado} \\ \text{que contiene } \alpha \in \mathbb{R} \\ \text{y a } \alpha \end{array} \quad \left. \begin{array}{l} \mathbb{Q}(x) \\ (\overbrace{x^3 - 4x + 2}) \\ \parallel \end{array} \right\} \approx \mathbb{Q}[\alpha]$$

$$\left\{ a_0 + a_1 \alpha + a_2 \alpha^2 : a_0, a_1, a_2 \in \mathbb{Q} \right\}$$

dado α es la raíz

$$\text{sabemos que: } \alpha^3 - 4\alpha + 2 = 0 \Rightarrow \boxed{\alpha^3 = 4\alpha - 2}$$

4.3

④ y es algebraico sobre \mathbb{K} , si existe un polinomio con coefs. en \mathbb{K} , del cual él es raíz⁴.

> Elementos algebraicos trascendentales

\mathbb{F} cuerpo de extensión del cuerpo $(\mathbb{K}, +, \cdot)$, $\alpha \in \mathbb{F}$.

α es algebraico sobre \mathbb{K} si existe $f \in \mathbb{K}[x]$ con $g(f) \geq 0$ y

$$f(\alpha) = 0.$$

"Un polinomio es algebraico si verifica que existe un polinomio con coefs. racionales del cual él es raíz"⁴ ④

> Polinomio mínimo

li) $\alpha \in \mathbb{F}$ es algebraico sobre \mathbb{K} , se denomina polinomio mínimo de α sobre \mathbb{K} al polinomio nómico $f \in \mathbb{K}[x]$, generador del ideal $\{f \in \mathbb{K}[x] : f(\alpha) = 0\}$

> li) $\alpha \in \mathbb{F}$ no es algebraico sobre \mathbb{K} se dice que α es trascendente sobre \mathbb{K}

> le dice que \mathbb{F} es una extensión algebraica sobre \mathbb{K} si todo $\alpha \in \mathbb{F}$ es algebraico sobre \mathbb{K} .

> Algunos elementos trascendentales: π , e son trascendentales sobre \mathbb{Q}

> Generación de elementos trascendentales

① Si $\alpha \in \mathbb{R}$ es trascendente sobre \mathbb{Q} y $f \in \mathbb{Q}[x] \Rightarrow f(\alpha)$ es trascendente sobre \mathbb{Q}

② Para todos $\beta, \alpha \in \mathbb{R}$ algebraicos sobre \mathbb{Q} con $\alpha \notin \{\beta, 0, 1\}$ y $\beta \notin \mathbb{Q}$ se verifica que:
 α^β es trascendente sobre \mathbb{Q}

> Caracterización de elementos algebraicos
y trascendentales:

Sea \mathbb{F} un cuerpo extendido del cuerpo \mathbb{K} y sea $\alpha \in \mathbb{F}$ entonces:

① α es algebraico sobre $\mathbb{K} \Leftrightarrow \mathbb{K}[\alpha] = \mathbb{K}(\alpha)$

② α es trascendente sobre $\mathbb{K} \Leftrightarrow \mathbb{K}[\alpha] \cong \mathbb{K}(x)$

• Estudiar si α es algebraico

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

y en caso afirmativo obtener el polinomio minimo

$$\text{se que } \alpha^2 = 4 + \sqrt{2} \rightarrow (\alpha^2 - 4)^2 = 2 \Rightarrow \alpha^4 - 8\alpha^2 + 16 = 2 \Rightarrow \alpha^4 - 8\alpha^2 + 14 = 0$$

$f = \alpha^4 - 8\alpha^2 + 14 \in \mathbb{Q}[x]$ que esic un polinomio minimo solo si es irreducible;

$$\begin{array}{c} 2 | 14 \\ 2 | 8 \\ 2 | 4 \\ \hline 14 \end{array}$$

✓ irreducible

es el polinomio minimo

cont.

→
cont. El minimo cuadro dnd tiene una raiz:

$$\frac{Q[x]}{(f)} \approx Q(\alpha) \approx Q[\alpha]$$

↑
Th. Knack.

④ Estudiar si es algebraico

$$\alpha = \frac{1+\sqrt{5}}{2}$$

en caso afirmativo obtener su polinomio minimo

$$(2\alpha - 1)^2 = 5 \Rightarrow 4\alpha^2 - 4\alpha - 4 = 0$$

$\Rightarrow \alpha$ es raiz de $g = 4x^2 - 4x - 4$

$\Rightarrow \alpha$ es raiz de $h = x^2 - x - 1$