$$S\mathbb{F} = \{ f : S \to \mathbb{F} \mid f \text{ es función} \}$$

Ej. 11

- $\mathbb{F}$ un campo (y ya)
- S finito

Ejemplo $S = \{1,2\}$, $^{\{1,2\}}\mathbb{F} = \{ f : \{1,2\} \to \mathbb{F} \mid f \text{ función} \}$

¿Cómo son los casos que viven aquí?
Desde empezar son funciones
$f : \{1,2\} \to \mathbb{F}$
¿Qué más se puede decir de ellas?

La idea es que f quede determinada por los valores
$f(1)$ y $f(2)$ ($f(1), f(2) \in \mathbb{F}$)
(en ese orden).

Por "quede determinada" nos referimos a que:
Si $g : \{1,2\} \to \mathbb{F}$ también tome los valores $f(1)$ y $f(2)$ en ese orden, es decir,
$$g(1) = f(1)$$
$$g(2) = f(2).$$

De aquí, f y g son dos funciones que tienen el mismo dominio, el mismo contradominio y la misma regla de correspondencia.
Por ello,
$$f = g$$ (es decir, f queda determinada por los valores $f(1)$ y $f(2)$ en ese orden)

La idea del ejercicio es asociar funciones $f : \{1,2\} \to \mathbb{F}$ con vectores $(x_1, x_2) \in \mathbb{F}^2$, mediante la correspondencia

$$f \in {}^{\{1,2\}}\mathbb{F} \xrightarrow{\Phi} (f(1), f(2)) \in \mathbb{F}^2.$$

$$\Phi(f) = (f(1), f(2))$$

Pd. $f, g \in \text{Dom } \Phi$ son tq $\Phi(f) = \Phi(g) \Rightarrow f = g$

Pd Φ es inyectiva:

Si $f, g \in \text{Dom } \Phi$ cumplen $\Phi(f) = \Phi(g)$, entonces

$$(f(1), f(2)) = (g(1), g(2))$$

Esto significa $f(1) = g(1)$ y $f(2) = g(2)$.

Por lo tanto, $f = g$. ——— Δ ———

¿Φ es suprayectiva?

Si $(x_1, x_2) \in \mathbb{F}^2$, ent. la función $h: \{1,2\} \to \mathbb{F}$ dada por

$$h(1) = x_1$$
$$h(2) = x_2$$

cumple que $\Phi(h) = (h(1), h(2)) = (x_1, x_2)$.

∴ Φ es suprayectiva.

¿A qué se refiere con "de tal manera que las operaciones de espacio se corresponden"?

Φ cumple que "sumar antes" o "sumar después"

da lo mismo.

$f, g \in \{1,2\}_{\mathbb{F}}$

① $\Phi(f+g) = \Phi(f) + \Phi(g)$

Análogamente para $\lambda \in \mathbb{F}$ y $f \in \{1,2\}_{\mathbb{F}}$ se cumple

② $\Phi(\lambda \cdot f) = \lambda \cdot \Phi(f)$

¿Cómo demostrar ①?

Si $f, g \in \{1,2\}_{\mathbb{F}}$, entonces $f+g : p \in \{1,2\} \mapsto f(p)+g(p)$,

Desde aquí vemos que $\Phi(f+g) = \big((f+g)(1), (f+g)(2)\big)$

$= \big(f(1)+g(1),\ f(2)+g(2)\big)$

$= \big(f(1), f(2)\big) + \big(g(1), g(2)\big)$

$= \Phi(f) + \Phi(g)$.

Generalización: Si $f : \{1, 2, \dots, n\} \to \mathbb{F}$, entonces f queda determinada por los valores

$f(1), f(2), \dots, f(n)$

en ese orden

Si $g : \{1, \dots, n\} \to \mathbb{F}$ tal que $g(1) = f(1)$, $g(2) = f(2)$, …, $g(n) = f(n)$

$\Rightarrow f = g$

Vectores en $\mathbb{F}^n$

$$\Phi : \{1,2,\dots,n\}_{\mathbb{F}} \to \mathbb{F}^n$$

$$\Phi(f) = (f(1), \dots, f(n)) \in \mathbb{F}^n$$

$$f(i) \in \mathbb{F}$$

$$\mathbb{R}^{\infty} = \underbrace{\mathbb{R} \times \mathbb{R} \times \dots \times \mathbb{R} \times \dots}_{\infty \text{ veces ?}}$$

¿Qué infinito?

$$\infty = \aleph_0 = \#\mathbb{N}$$

$$\mathbb{R}^{\mathbb{N}} = \underbrace{\mathbb{R} \times \mathbb{R} \times \dots \times \mathbb{R} \times \dots}_{\mathbb{N} \text{ veces}}$$

$$^{\mathbb{N}}\mathbb{R} = \{ f : \mathbb{N} \to \mathbb{R} \mid f \text{ función} \}$$

$$\mathbb{R}^{\mathbb{N}_0} = \text{esp. de sucesiones.}$$

6| $\mathbb{F}$ campo con q elementos.

$\bar{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}^n$

$q = 3$, $\mathbb{F} = \{0,1,2\}$

$q \cdot q \cdots q = q^n$

x_1	x_2	x_3
0	0	0
1	1	1
2	2	2
⋮	⋮	⋮

b) Si $\alpha_1, \dots, \alpha_n \in \mathbb{F}$, ¿cuántas soluciones tiene la ecuación

$$\sum_{i=1}^{n} \alpha_i x_i = 0$$

$\bar{x} = (x_1, \dots, x_n)$

Op1| Si $\forall i \ \alpha_i = 0 \Rightarrow$ la ecuación $\sum_{i=1}^{n} 0 x_i = 0$

En este caso, hay q^n soluciones

Op2| Si $\exists i \in \{1, \dots, n\}$ tq $\alpha_i \neq 0$, entl. podemos sup sp.dg que $i = n$

Así buscamos las soluciones $\bar{x} = (x_1, \dots, x_n)$

$$0 = \sum_{i=1}^{n} \alpha_i x_i = \alpha_1 x_1 + \dots + \alpha_n x_n = 0$$

$$\Leftrightarrow \alpha_n x_n = -(\alpha_1 x_1 + \dots + \alpha_{n-1} x_{n-1})$$

$$\Leftrightarrow x_n = \frac{1}{\alpha_n}\left[-\left(\alpha_1 x_1 + \dots + \alpha_{n-1} x_{n-1}\right)\right]$$

restricción

1 2 3 ... n−1

grados de libertad

$ax + by + cz = 0$ en $\mathbb{R}^3$ libres

$\Leftrightarrow z = \frac{-1}{c}(ax + by)$

sup $c \neq 0$

2 grados de libertad

$x_1, x_2, \dots, x_{n-1}$

$q \cdot q \cdots q = q^{n-1}$

Soluciones

Sup $i=n$ da $\alpha_n \neq 0$ ✓

Si además $i=n-1$ da $\alpha_{n-1} \neq 0$, ¿qué hago?

$$0 = \sum_{i=1}^{n} \alpha_i x_i = \alpha_1 x_1 + \dots + \alpha_{n-1} x_{n-1} + \alpha_n x_n$$

$$\Leftrightarrow \quad \alpha_{n-1} x_{n-1} = -\left(\sum_{i \neq n-1} \alpha_i x_i \right)$$

$$\Leftrightarrow \quad x_{n-1} = \frac{-1}{\alpha_{n-1}} \left(\sum_{i \neq n-1} \alpha_i x_i \right)$$

$a \neq 0, \ b \neq 0$

$$ax + by + cz = 0 \iff y = \frac{-1}{b}(ax + cz) \quad \text{vs} \quad z = \frac{-1}{c}(ax + by)$$

¿Qué es un campo finito?

Pues un campo $\mathbb{F}$ que tiene una cantidad finita de elementos

Los "canónicos" son los $\mathbb{Z}_p$. (p primo)

$$\mathbb{Z}_p = \mathbb{Z} / \sim_p \; = \mathbb{Z} / p\mathbb{Z}$$

$$= \{ [k]_p \mid k \in \mathbb{Z} \}$$

donde $\sim_p$ está dada por

$$a \sim_p b \iff p \mid a - b$$

$\mathbb{Z}_p$ es un cto con 2 operaciones

$$+ : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$$

$$[a] + [b] = [a+b]$$

$$\cdot : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$$

$$[a] \cdot [b] = [ab].$$

$(\mathbb{Z}_p, +, [0])$ es grupo abeliano

$(\mathbb{Z}_p \setminus \{[0]\}, \cdot, [1])$ es grupo abeliano

(p primo)

$(\mathbb{Z}_p, +, \cdot, [0], [1])$ es un cuerpo

Paso a fuerza → darle sentido con números

$P \longrightarrow$ un número

$0 \longrightarrow$ " "

$SI \longrightarrow$ " "

$0 \longrightarrow$ " "

Hay un cuerpo finito $\mathbb{F}_{256} = \mathbb{F}_{2^8}$

$\mathbb{F}_{2^8} = (\mathbb{F}_2)^8$

$\mathbb{F}_2 = \mathbb{Z}_2$

Símbolos del código ASCII

Quiero un código de longitud $n = 140$

Un código es $\bar{v} \in \mathbb{F}_{256}^{\,n} = (\mathbb{F}_{256})^{140}$

Ejemplo: $\mathbb{Z}_{12}$

6 (am) ← tomar med

(+8 horas)

2 (pm) ← 2ª dosis

$\mathbb{Z}_{24}$: 6h, 14h, 22h (cada 8 horas)

6h

$6h + 24h = 6h$

$24 = 0$

En $\mathbb{Z}_{24}$, $3 \cdot 8 = 24 = 0$

$a, b \in \mathbb{R}$ t.q. $a \cdot b = 0$

$\Rightarrow a = 0 \vee b = 0$

$i = \sqrt{-1}$ se pega a $\mathbb{R}$ y nos da $\mathbb{C}$.

i es solución a x^2+1

ξ se pega $\mathbb{Z}_2$ y nos da $\mathbb{Z}_2(\xi)$

ξ es solución al polinomio x^2+x+1

$x=0$ ⇝ $0^2+0+1=1$

$x=1$ ⇝ $1^2+1+1=1$ (0)

$\mathbb{Z}_2(\xi) = \mathbb{F} = \{0, 1, \xi, \xi^2\}$ ⇒ 4 elementos

imagen

← matriz con 0 y 1

⇝ $A \in \mathbb{M}_{768 \times 1260}(\mathbb{Z}_2)$