

- Dado un grupo $(G, *)$

1. Elemento neutro único

2. inverso elemento neutro único

3. Cancelativa $(G, *)$ $a, b, c \in G$

$$a * b = a * c \Rightarrow b = c$$

$$4. (a * b)^{-1} = b^{-1} * a^{-1}$$

- Potencias en $(G, *)$

$$g^n = g * g * \dots * g \quad \text{y/o } g^n * g^m = g^{n+m}$$

$$g^0 = e \text{ (elemento neutro)} / (g^n)^m = g^{nm}$$

$$g^{-n} = (g^{-1})^n / \quad g^{-n} \text{ inverso de } g^n$$

2.2 Ejemplos

2.2.1 \mathbb{Z}_n ($n \in \mathbb{N}$)

$$\text{En } \mathbb{Z}_5: [3] + [4] = [2] \\ [3] \cdot [4] = [2]$$

$(\mathbb{Z}_n, +)$ grupo abeliano

(\mathbb{Z}_n^*, \cdot) grupo abeliano si n es primo

$$\mathbb{Z} = \{0, 1, \dots, n-1\}$$

\uparrow

Enteros módulo n = Posibles

restos al dividir entre n

n no primo

(\mathbb{Z}_4^*, \cdot)	[1]	[2]	[3]
[1]	[1]	[2]	[3]
[2]	[2]	[0]	[2]
[3]	[3]	[2]	[1]

0 no pertenece
a \mathbb{Z}_4^*

n primo

(\mathbb{Z}_5^*, \cdot)	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

Elemento neutro en
todas las columnas
(tiene inverso)

1.2-2 Grupo Simétrico (S_n, \circ)

$$N_n = \{1, 2, \dots, n\}$$

- $S_n =$ Función biyectiva

$$f: N_n \rightarrow N_n$$

- $\alpha, \beta \in S_n, \alpha \cdot \beta =$ Composición

Aplicación biyectiva

• Inyección

Dos elementos no tienen la misma imagen

• Sobreyectiva

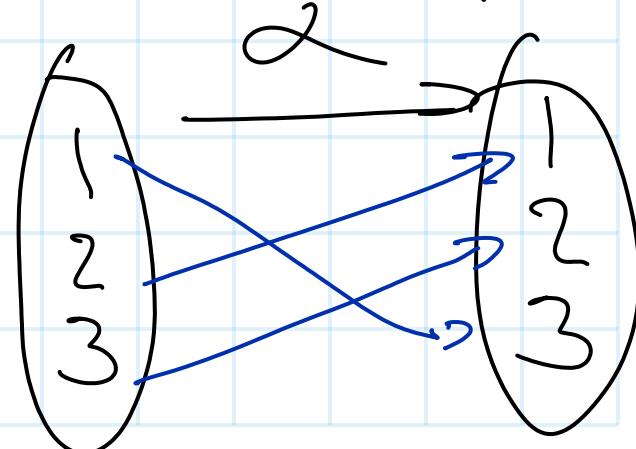
Todos los elementos del conjunto final es imagen de algún

Ejemplo: $n=3, N_3 = \{1, 2, 3\}$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = [3, 1, 2]$$

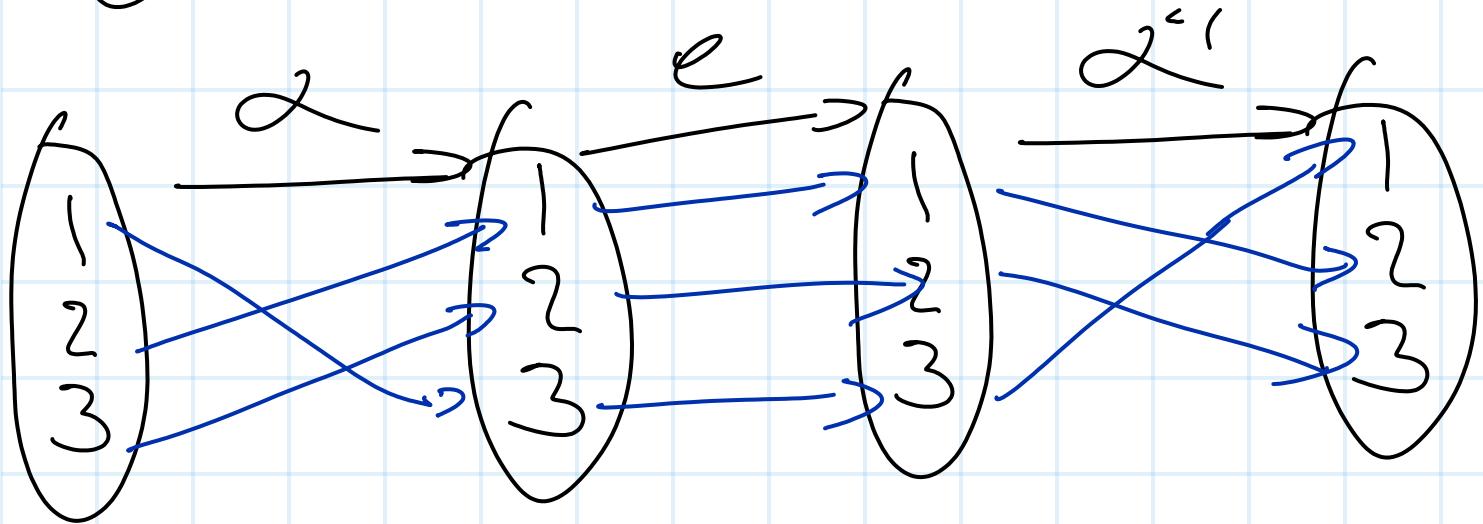
$$\text{Si } \beta = [3, 2, 1]$$

$$\alpha \cdot \beta = [2, 1, 3]$$



- Teorema = (S_n, \circ) es un grupo

- ① La operación es interca
- ② Elementos neutros: Identidad
- ③ Inverso



- Ejercicio:

$$\alpha = [2, 1, 4, 3], \beta = [3, 1, 2, 4]$$

$$\alpha \circ \beta = [4, 2, 1, 3] \quad \alpha^{-1} \beta^{-1} = [1, 4, 2, 3]$$

$$\beta \circ \alpha = [1, 3, 4, 2]$$

$$\beta^{-1} = [2, 3, 1, 4]$$

$$\alpha^{-1} = [2, 1, 4, 3]$$

$$(\beta \circ \alpha)^{-1} = [1, 4, 2, 3]$$

I. 3 Construcción de Grupos

I.3.1 Subgrupos

Pregunte: Tengo $(G, *)$ grupo y tomo los

$H \subseteq G$, ¿es H grupo con $*$?

Ejemplo: $(\mathbb{Z}_6, +)$

a) $H = \{[0], [2], [3]\}$

$$[2] + [3] = [5]$$

$[5] + [0]$ no es cerrada en H

b) $H_2 = \{[2], [4]\}$

$$[2] + [2] = [4]$$

$$[4] + [4] = [8] = [2]$$

$$[4] + [2] = [6]$$

H_2 no tiene elementos extraños

c) $H_3 \setminus \{[0], [2], [4]\}$

Si se cumple:
 - Hay inversos
 - Tiene elementos neutros
 - Cerrado suma
 Es un grupo

$(G, *)$ es abeliano

$H \subseteq G$

$\rightarrow H$ es abeliano} Si $a * b = b * a$

Si G es un grupo y $a \in G$, el menor natural n tal que $a^n = e$ (elemento neutro) se dice **orden de a** = $O(a)$

2) $O(a)$ coincide con el número de elementos de $\langle a \rangle$

b) $a^m = a^r$ donde r es resto de m entre n

■ Si $\langle a \rangle = G$, G grupo cíclico

Ej: (\mathbb{Z}_7^*, \cdot)

$$\langle [2] \rangle = \{[9], [13], [23]\}$$

$$\langle [3] \rangle = \{[3], [2], [6], [4], [5], [13]\} = \mathbb{Z}_7^*$$

$$\mathcal{L} = [3, 4, 2, 1]$$

$$\mathcal{L}^2 = [2, 1, 4, 3]$$

$$\mathcal{L}^3 = [4, 3, 1, 2]$$

$$\mathcal{L}^4 = [1, 2, 3, 4]$$

$$\mathcal{L}^{235} = \underbrace{\mathcal{L}}_{m} + \underbrace{\mathcal{L}^3}_{I}$$

1.3.3. Producto de grupos

$$\mathbb{Z}_2^S = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2}_{\forall x_i \in \mathbb{Z}_2} \left\{ (x_1, x_2, x_3, x_4, x_5) \right\}$$

$$(x_1, x_2, x_3, x_4, x_5) + (y_1, y_2, y_3, y_4, y_5)$$

$$(x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4, x_5 + y_5)$$

$$\begin{matrix} (G, \square) \\ (H, \Delta) \end{matrix}$$

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 \square g_2, h_1 \Delta h_2)$$

$$G \times H \Rightarrow \text{Grupo}$$

1.4 Homomorfismos de grupos

¿Cómo comparar 2 grupos?

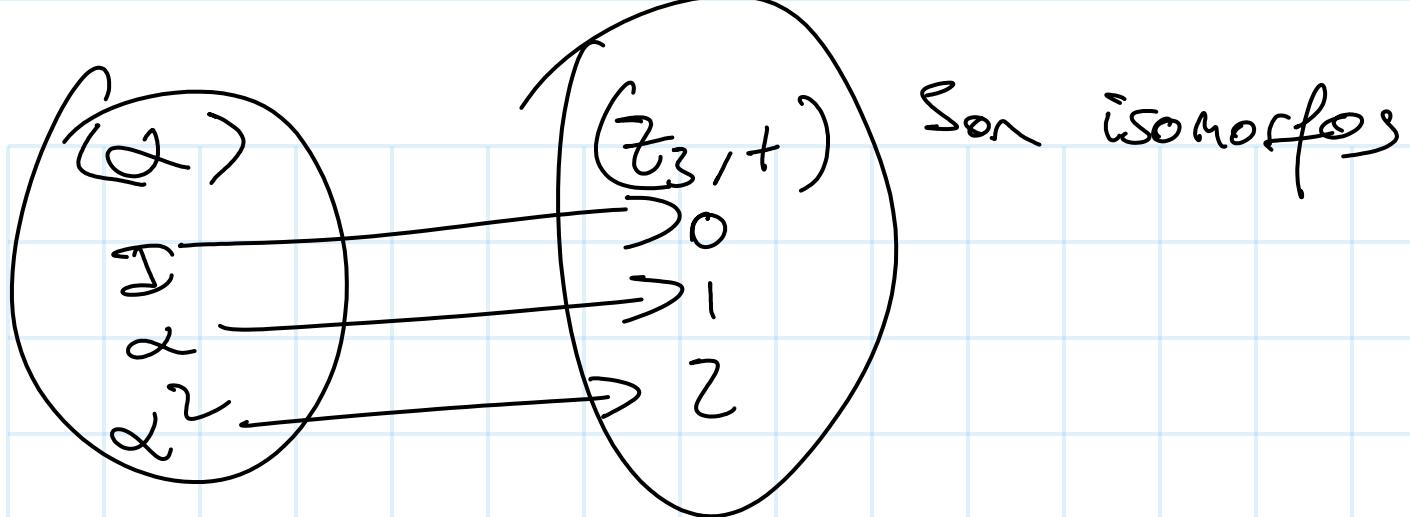
$$(G, *) \text{ y } (H, \oplus)$$

- Ejemplos

c) En S_4 , $\langle \alpha \rangle = \{ \{2, 1, 3, 4\}, \{1, 2, 3, 4\} \}$

$\langle \alpha \rangle, G, (\mathbb{Z}_2, +)$ son isomorfos

d) En S_5 , $\langle \alpha \rangle = \{ \overset{\alpha}{\{2, 3, 1, 4, 5\}}, \{3, 1, 2, 4, 5\}, \{1, 2, 3, 4, 5\} \}$



con aplicaciones $f: G \rightarrow H$ que reflejan las operaciones

$$f(a * b) = f(a) \oplus f(b)$$

Homomorfismos de Grupo

Si f es inyectiva y sobrejetiva
(biyectiva) $\Rightarrow f$ es un isomorfismo

1.5 Clases Ceterales

$$(H_2, +), H_2 = \{03, 43, 83\}$$

$$\cdot \{[1] + h | h \in H\} = \{[13], [53], [23]\}$$

$$\{[5] + h | h \in H\} = \{[53], [13], [33]\}$$

$$\{[2] + h | h \in H\} = \{[23], [63], [103]\}$$

$$\{[3] + h \mid h \in H\} = \{[3], [7], [1]\}$$

$$\{[0] + h \mid h \in H\} = \{[0], [4], [8]\}$$

CLASES LATERALES A IZQUIERDA DE H

c) $[0] + H = +$

b) Si $[b] \in [a] + H \Rightarrow [b] + H = [a] + H$

c) Las clases laterales son iguales o disjuntas

d) Todas las clases laterales tienen el mismo número de elementos que H

e) G es igual a G unión de las clases laterales

f) N° clases laterales \times N° elementos de H = N° elementos de G

-Teorema de Lagrange

El número de elementos de un subgrupo H de un Grupo G divide al número de elementos G.

- Ejemplos

Es $\{[0], [1], [2], [3], [4]\}$ Subgrupo de \mathbb{Z}_{12}

$$\text{Nº Nº elementos} = S \quad 12/S \neq 0$$

Ejercicio 3

$$(u,v) \circ (x,y) = \left(ux, \frac{y}{v} + xv\right)$$

Asociativa

$$[(u,v) \circ (x,y)] \circ (c,d) =$$

$$\left(ux, \frac{y}{v} + xv\right) \circ (c,d) =$$

$$\left(uxc, \frac{d}{ux} + c\left(\frac{y}{v} + xv\right)\right)$$

$$\left(uxc, \frac{d}{ux} + \frac{yc}{v} + xv^2\right)$$

*TEORÍA ALGEBRAICA DE ALGORITMOS

- Mensajes que queremos enviar

$W \subseteq \mathbb{Z}_2^m$

$$\mathbb{Z}_2^m = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2$$

- Codificación: Añadir dígitos de control al msg

$C \subseteq \mathbb{Z}_2^n$

$$(n > m)$$

- Función de codificación

$$E: W \longrightarrow C \quad E(w) = c$$

$$w \longmapsto c$$

- Recibimos el mensaje: $T(c)$

-Corregir $T(c) \rightarrow c$

-Decodificar c : $D(c) = w$

$(W, C, E) \quad (n, m)$ - código
 \hookrightarrow código

Ejemplo: $(9,8)$ - código

$$E: \mathbb{Z}_2^8 \rightarrow \mathbb{Z}_2^9$$

$$E(x_1, x_2, x_3, \dots, x_8) = x_1 x_2 x_3 \dots x_8 (x_1 + x_2 + x_3 + \dots + x_8)$$

Ejemplo: $G: \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^3$ $(5,2)$ - código

$$E(x_1, x_2) = x_1 x_2 x_1 x_2 (x_1 + x_2)$$

$$C = \{ E(00), E(01), E(01), E(11) \}$$

$$= 0000, 1010, 0100, 11110$$

a) Recibimos $w = 1010 \Rightarrow D(w) = 10$

" " $w = 10100 \Rightarrow D(w) = 10$

\hookrightarrow correcta = 1010 $\Rightarrow D(w) = 10$

" " $w = 11100$

\hookrightarrow correcta = 1110 $\Rightarrow D(w) = 11$

¿Cómo buscamos la palabra más cercana?

a) Comparamos

b) Menor número de diferencias

. 11100 · № de 1 \Rightarrow Peso

$$\begin{array}{r} 00000 : 11100 \\ \hline 00001 : 01001 \\ \hline 01001 : 10111 \\ \hline 11100 : 00010 \end{array} \quad \begin{array}{r} 3 \\ 2 \\ 4 \\ 1 \end{array}$$

¿Cuando el algoritmo de decodificación funciona?

$$k = \min \{ d(c_1, c_2) \mid c_1, c_2 \in C \}$$

Menor distancia entre palabras del código

① El código a) Si recibo w con $k-1$ errores
detectar $k-1$ errores

$$d(c, w) = k-1$$

b) Hay 1 más cercano a w si w tienen
 $\frac{k-1}{2}$ errores \Rightarrow Corrige $\frac{k-1}{2}$ errores

- Ejemplo: $E: \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^6$ $E(x_1 x_2) = x_1 x_2 x_1 x_2 x_1 x_2$

$$C = \{0000000, 100000, 010101, 111111\}$$

k elementos neutros

	000000	100000	010101	111111
000000	000000	101010	010001	111111
101010	101010	000000	111111	010101
010001	010101	111111	000000	101010
111111	111111	010101	101010	000000

Si es subgrado
Los códigos de grupo

$k=3 \left\{ \begin{array}{l} \text{Detecta 2 fallos} \\ \text{Corrige } \frac{k-1}{2} = 1 \text{ fallo} \end{array} \right.$

- Rectificamos 000000

- Más cercana: 000000 $\rightarrow \mathcal{O}(w) = 00$

- Rectificamos 100000

$$(000000 \Rightarrow \mathcal{O}(w) = 00)$$

$$000000 \ 100101$$

$$000000 \ 001111$$

$$000000 \ 110000$$

$$111111 \ 011010$$

Clase lateral de 100101
 $100101 + C$

- Código de grupo: Si C es subgrupo
 $K = \min_{\text{peso}} \{N(c) \mid c \in C \text{ no nulo}\}$

- Proceso de codificación (Tabla de decodificación)

000000 101010 010101 111111 $\rightarrow C$

100000 000000 001010 110101 011111 $\rightarrow 10000000$

010000 010000 111010 000101 101111 $\rightarrow 010000 + C$

- Recibimos 011111

Corrección 111111 $\Rightarrow 0 = 1$

- Buscamos códigos de grupo

$$E = \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^m$$

$$C := E(\mathbb{Z}_2^m) = \begin{array}{l} \text{Imagen de } E \\ \text{Recomiendo de } E \end{array}$$

$\bar{e} = \text{homomorfismo de grupo}$



Multiplicar por una matriz

$$E: \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^6 \quad G$$

$$(x_1, x_2, x_3) \begin{pmatrix} (0 & 0 & 1 & 1 & 0) \\ (0 & 1 & 0 & 0 & 1) \\ (0 & 0 & 1 & 0 & 1) \end{pmatrix}$$

$$= (y_1, y_2, y_3, y_4, y_5, y_6)$$

• Proceso de codificación

$$H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{Ej: } w = 001101 \quad \text{Recibo } w \in \mathbb{Z}_2^6$$

$w = 001101 \quad \text{a)} \quad wt(w) = 0 \Rightarrow w \in C$

$b) \quad wt(w) = 1 \Leftrightarrow w_1, w_4$
están en la misma
clase lateral

- Ejemplo 7
 $k=3 \left\{ \begin{array}{l} \text{Detected 2 errors} \\ \text{Corrects 1 error} \end{array} \right.$

- Recibimos 011 001

↳ No están en $C \rightarrow$ Errors

· Ultimo filte $\rightarrow 010100 \rightarrow$

001101

$$0110001 + (000001) = 111000$$

3. ANILLOS

- Definición: Un anillo es un conjunto abeliano ($A, +$) con otra operación \circ que cumple

- Asociativa $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Distributiva $a \cdot (b + c) = ab + ac$
 $(b + c) \cdot a = ba + ca$

Ejemplos

- a) $(\mathbb{Z}, +, \cdot) \Rightarrow \text{CU}$
- c) $(M_n(\mathbb{R}), +, \cdot) \Rightarrow \text{CU}$
- d) $(P[x], +, \cdot) \Rightarrow \text{CU}$
- e) $(\mathbb{Z}/n, +, \cdot) \Rightarrow \text{CU}$

• Tipos de anillos

- a) Comunitativo: Si \circ es comunitativa
- b) Con unidad: Si \circ tiene elemento neutro
- c) Cuerpo: Si \circ es comunitativo, el neutro y tiene inverso

• Cuerpos

- a) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- b) $(\mathbb{Z}/n, +, \cdot)$
 con n primo

3.3 SUBANILLOS

Si $(R, +, \cdot)$ es un anillo y $S \subseteq R$, es un subconjunto,
¿es S un anillo?

a) S cerrado para las operaciones

$$\left. \begin{array}{l} S_1, S_2 \in S \\ \end{array} \right\} \begin{array}{l} S_1 + S_2 \in S \\ S_1 \cdot S_2 \in S \end{array}$$

b) contiene 0

c) $\forall s \in S \Rightarrow -s \in S$

S es un subanillo de R

- Ejemplo = $(\mathbb{Z}, +, \cdot)$

$S = \text{Múltiplos de } 5$

a.1) ✓ a.2) ✓ b) ✓ c) ✓

$$\mathbb{Z}(S + \mathbb{Z}_2 \cdot S) = (\mathbb{Z}_1 + \mathbb{Z}_2) \cdot S$$

$$0 = 0 \cdot S \in S$$

$$\mathbb{Z}_1 \cdot S + \mathbb{Z}_2 \cdot S = \mathbb{Z}_1 \cdot \mathbb{Z}_2 \cdot S$$

$$- \mathbb{Z}_1 \cdot S = (-\mathbb{Z}_1) \cdot S$$



$$\mathbb{Z}_2 \cdot (\mathbb{Z}_1 \cdot S) \in S'$$

Es un ideal

Un ideal es un subanillo S en el que la propiedad
a.2) es más fuerte

$$\left. \begin{array}{l} r \in R \\ s \in S \end{array} \right\} rs \in S'$$

3.4 HOMOMORFISMOS DE ANILLOS

$$f: R \longrightarrow S \begin{cases} (R, +, \cdot) \\ (S, \oplus, *) \end{cases}$$

$$f(r_1 + r_2) = f(r_1) \oplus f(r_2)$$

$$f(r_1 \cdot r_2) = f(r_1) * f(r_2)$$

$$f: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_5$$

$$f([x]_6) = ([x]_2 [x]_5)$$

$$f([z]_6) = ([z]_2, [z]_5)$$

$$f([x]_6 + [y]_6) = f(x) + f(y)$$

#

$$f([x+y]_6) = ([x]_2 [x]_5) + ([y]_2 [y]_5)$$

||

$$([x+y]_2, [x+y]_5)$$

$$f([x_3 \cdot y_3]_0) = f([x_3]) \cdot f([y_3])$$

$$f([x \cdot y]_0) \quad ([x_3_2, x_3_5] - [y_3_2, y_3_5])$$

~~\rightarrow~~

$$([x \cdot y]_2, [x \cdot y]_5)$$

b) Isomorphism	
$0 \rightarrow (0, 0)$	injective Bijective
$1 \rightarrow (1, 1)$	$5 \rightarrow (1, 0)$
$2 \rightarrow (0, 2)$	$6 \rightarrow (0, 1)$
$3 \rightarrow (1, 3)$	$7 \rightarrow (1, 2)$
$4 \rightarrow (0, 4)$	$8 \rightarrow (0, 3)$
	$9 \rightarrow (1, 4)$

(17)

$(2, 5)$ -código $E: \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^5$ de grupo

$$(x_1, x_2) \begin{pmatrix} 1 & 0 & \stackrel{a}{\sim} & \stackrel{b}{\sim} & c \\ 0 & 1 & \text{de } f \end{pmatrix} = (y_1, y_2, y_3, y_4, y_5)$$

$$C = \{00000, 10101, 11010,$$

$$(0,0) \cdot G = 00000$$

 $\begin{matrix} a & b & c \\ 1 & 0 & 1 \end{matrix}$

$$(1,0) \cdot G = 10abc = 10101$$

$$(1,1) \cdot G = 11(a+d)(b+e)(c+f) = 11010$$

$$1+d=0 \quad d=1 \quad \left| \begin{array}{l} \\ \end{array} \right. C = \{00000, 10101, 11010, 01111\}$$

$$0+e=0 \quad e=1$$

$$1+f=0 \quad f=1$$

$$k=3 \quad \left. \begin{array}{l} \text{Detect } 2 \\ \text{Corrige } 1 \end{array} \right.$$

$$H = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

3.4 HOMOMORFISMO DE ANILLOS

$$(\mathbb{Q}, +, \cdot) \rightarrow \text{Anillo}$$

¿Es dominio de integridad?

$$(\mathbb{Z}, +, \cdot); a, b \in \mathbb{Z} \Rightarrow a \cdot b \neq 0$$

$$(M_n(\mathbb{R}), +, \cdot); A, B \neq 0 \Rightarrow A \cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Notice que los divisores de 0
(dominio de integridad)

$$A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A \cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

