tema 1

ARITMÉTICA MODULAR

Toda matriz está formada por un cuerpo K ($\mathbb{R}, \mathbb{Q}, \mathbb{Z}$)

Por ejemplo: $\mathbb{Z}_2 : \{0, 1\}$

En $\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

como da 5 se vuelve al inicio

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

El opuesto es aquel que sumado al inicial, da 0.

$[-2 = 3 \pmod 5]$

El inverso es el que multiplicado por el inicial da 1.

$[2^{-1} = 3 \pmod 5]$

OPERACIONES ELEMENTALES

- $E(p) \cdot \lambda$
- $E(p) + \lambda(q)$
- $E(p,q) \rightarrow$ intercambiar filas

REDUCCIÓN POR FILAS

1. Buscamos el primer elemento no nulo.
2. Lo convertimos a 1.
3. Hacemos ceros debajo del 1.
4. Hacemos lo mismo en la segunda fila.

Teorema fundamental de reducción por filas: Dada una matriz B, si la amplío con la identidad y la reduzco por filas $[B|I] \rightsquigarrow [R|P]$, entonces $P \cdot B = R$.

Si en vez de R, queda una matriz identidad, la matriz es invertible.

$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$

COMANDOS PARA SAGE

`A = matrix(QQ, [[.,.,.],[.,.,.,.]])` H = R[:,3:] extraer ~~filas~~ columnas

`show(A)`

`C = A.augment(I)` o `C = block_matrix([[A, 1]])` (1: identidad)

`R = C.echelon_form()`

`A[2,2]` → nos da la posición (sage cuenta desde 0)

`A.T` traspuesta

Matriz columna: `column_matrix`

`A.subdivide(.,.)` división, para ello hacemos una copia `M = copy(M)`

COMANDOS PARA LATEX

`$\sage{..}$` o `\[ ... \]` para centrar

`\rightarrow` →	`\equiv` ≡
`\cdot` ·	`\alpha` α
`\in` ∈	`X_2` X_2
`\Z` $\mathbb{Z}$	

Escaneado con CamScanner

SISTEMAS DE ECUACIONES

Compatible determinado

$$\left[\begin{array}{cc|c} 1 & 0 & 3 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{array}\right]$$

Compatible indeterminado

$$\begin{array}{c} \left[\begin{array}{ccc|c} 1 & 1 & 0 & 4 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{array}\right] \\ \downarrow \qquad\quad \downarrow \\ \text{pivotes} \end{array}$$

se utilizan parámetros libres en las variables que no son pivote

$x_2 = \lambda$

Incompatible

$$\left[\begin{array}{cc|c} 1 & 0 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{array}\right]$$

columnas : nº incógnitas

filas: nº ecuaciones

tema 2

en este tema en las prácticas usamos el cuerpo 22 para que no salgan decimales o fracciones.

MÁXIMO COMÚN DIVISOR

Dados a, b, existen q, r tales que $\underset{\text{dividendo}}{a} = \overset{\text{divisor}}{b} \cdot q + \overset{\text{resto}}{r} \quad 0 \leq r \leq b$

El m.c.d entre dos números se saca reduciendo la matriz cuyos elementos son dichos números.

Los números serán coprimos si su m.c.d es igual a 1.

$mcd(a, b) = d \quad d = a \cdot v + b \cdot u$

$$\left[\begin{array}{c|cc} 14375 & 1 & 0 \\ 143 & 0 & 1 \end{array}\right] \rightsquigarrow \left[\begin{array}{c|cc} 1 & 82 & -8243 \\ 0 & 143 & -14375 \end{array}\right] \quad \begin{bmatrix} 82 & -8243 \\ 143 & -14375 \end{bmatrix} \cdot \begin{bmatrix} 14375 \\ 143 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\underbrace{14375}_{a} \cdot \underbrace{82}_{v} + \underbrace{(-8243)}_{u} \cdot \underbrace{(143)}_{b} = \underbrace{1}_{d}$$

Además, de esta manera se resuelven las ecuaciones diofánticas, solo que sacamos también la otra ecuación (la que da 0) y la multiplicamos por t para tener una solución más completa.

Una ecuación diofántica de esta forma $(2n\,\cancel{[illegible]})x + (2n\,\cancel{[illegible]})y = \boxed{2n+1}$ no puede tener solución. M debe ser divisible entre d.

FUNCIÓN PHI DE EULER

1) $\varphi(p) = p - 1$ si p es primo.
2) $\varphi(p^t) = p^t - p^{t-1}$ si p es primo y t positivo
3) $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ si m y n son coprimos

Nº de elementos invertibles.

$\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) =$

$2 \cdot 20 = 40$

$23^{40} \pmod{100} = 1$

TEOREMA CHINO DE LOS RESTOS

Se utiliza para cuando nos dan un sistema de congruencias:

$n \equiv a_1 \pmod{m_1} \longrightarrow n = a_1 + m_1 \cdot x$

$n \equiv a_2 \pmod{m_2} \longrightarrow n = a_2 + m_2 \cdot y$

ahora igualamos $\longrightarrow a_1 + m_1 x = a_2 + m_2 y$

$m_1 x - m_2 y = a_2 - a_1$

La forma que nos queda es la misma que la de una ecuación diofántica, por lo que se resuelve de una manera muy similar.

① $\left.\begin{array}{l} n \equiv 9 \pmod{27} \\ n \equiv 1 \pmod{13} \end{array}\right\} \quad \left.\begin{array}{l} n = 9 + 27x \\ n = 1 + 13y \end{array}\right\} \quad 9 + 27x = 1 + 13y$

lo que nos dan

$27x - 13y = -8$ * ②

③

$$\left[\begin{array}{c|cc} 27 & 1 & 0 \\ -13 & 0 & 1 \end{array}\right] \rightsquigarrow \left[\begin{array}{c|cc} 1 & 1 & 2 \\ 0 & 13 & 27 \end{array}\right]$$

B — R — P

El teorema fundamental de la reducción por filas nos dice que: ④

$$P \cdot B = R \longrightarrow \begin{bmatrix} 1 & 2 \\ 13 & 27 \end{bmatrix} \cdot \begin{bmatrix} 27 \\ -13 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

sacamos las ecuaciones

⑤

$1 \cdot 27 + (2) \cdot (-13) = 1 \xrightarrow{\text{multiplicamos por } -8\,*} \boxed{-8} \cdot 27 + \boxed{-16}(-13) = 8$

$13 \cdot 27 + 27 \cdot (-13) = 0 \xrightarrow{\text{multiplicamos por } t} \boxed{13t} \cdot 27 + \boxed{27t} \cdot (-13) = 0$

las x's — las y's

$x = -8 + 13t$

$y = -16 + 27t$

sustituimos en una ecuación

el número que va con la t indica el módulo

$$n = 9 + 27(-8 + 13t) = 9 - 216 + 351t = -207 + 351t$$

$$n \equiv -207 \pmod{351} \longrightarrow n \equiv 144 \pmod{351}$$

!! especial atención

Puede aparecer con 3 ecuaciones en vez de 2, en ese caso lo hacemos con las dos primeras y luego con la resultante y la tercera.

Si aparecen de esta manera:

$5n \equiv 2 \pmod 7$, para quitar el 5 multiplicamos por su inverso en ese cuerpo. En este caso $5 \cdot 3 = 15$, $15 - 7 - 7 = 1$, por lo que 3 es su inverso. Quedaría así:

$$3 \cdot 5n \equiv 3 \cdot 2 \pmod 7 \to n \equiv 6 \pmod 7.$$

EXPONENCIACIÓN MODULAR

$a^e \pmod n$

- Si $\text{mcd}(a,n) = 1$, se reduce a $a^{\varphi(n)} \equiv 1 \pmod n$.
- Si $\text{mcd}(a,n) \neq 1$, reducimos el problema a exponentes más pequeños.
  - Si e es impar entonces:

    $a^e = a^{1+2f} = a \cdot (a^2)^f$
  - Si e es par

    $a^e = a^{2f} = (a^2)^f$

$10^{159} \pmod{39}$ $\quad \text{mcd}(10,39) = 1$

$10^{\varphi(39)} \equiv 1 \pmod{39}$

$\varphi(39) = 2 \cdot 12 = 24$, entonces

$10^{24} \equiv 1 \pmod{39}$

$159/24 = 6 \cdot 24 + 15$, luego

$10^{159} = \underbrace{(10^{24})^6}_{1} \cdot 10^{15} \equiv 10^{15} \pmod{39}$

$10^{15} = 10 \cdot 10^{14} = 10 \cdot (10^2)^7$

...

(ejemplo incompleto)

tema 3

En este tema llamaremos a las matrices horizontales, de tipo A : [≡]

y a las verticales, de tipo B : [|||]

ESPACIOS VECTORIALES

Sea K^m = $M_{m\times n}(K)$: $\left\{ \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \dots \right\}$

Un espacio vectorial se representa con una matriz cuyas columnas son vectores. Si U y V son espacios vectoriales de K^m, entonces su intersección y su suma también lo son.

Cumple las siguientes condiciones:

- Si $u, v \in K$, entonces $u + v \in V$ → espacio vectorial
- Si $c \in K$ y $v \in K$, entonces $c \cdot v \in V$

CUALQUIER CONJUNTO DE K^m QUE NO CONTENGA EL "0" NO PUEDE SER ESPACIO VECTORIAL

Combinación lineal
- → Forma vectorial $x_1 v_1 + x_2 v_2 + \dots x_n v_n$
- → Forma matricial $\begin{bmatrix} \vdots & \vdots & & \vdots \\ v_1 & v_2 & \dots & v_n \\ \vdots & \vdots & & \vdots \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$

PARAMÉTRICAS

Si un conjunto de vectores (v_i) son las columnas de una matriz M, se dice que el espacio generado por las columnas de M es C(M).

$$M : \begin{bmatrix} 1 & 2 \\ 3 & 1 \\ 4 & 1 \\ 1 & 1 \end{bmatrix} \rightarrow x_1 \underbrace{\begin{bmatrix} 1 \\ 3 \\ 4 \\ 1 \end{bmatrix}}_{\text{vector}} + x_2 \begin{bmatrix} 2 \\ 1 \\ 1 \\ 1 \end{bmatrix} \rightarrow \begin{aligned} y_1 &= x_1 + 2x_2 \\ y_2 &= 3x_1 + x_2 \\ y_3 &= 4x_1 + x_2 \\ y_4 &= x_1 + x_2 \end{aligned}$$

para $x_1, x_2 \in \mathbb{Z}_5$

TIPO B

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} : \begin{bmatrix} 1 & 2 \\ 3 & 1 \\ 4 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

En esta representación usamos parámetros libres

IMPLÍCITAS

Otra forma de dar un espacio vectorial es con un sistema de ecuaciones homogéneo. El vector nulo debe ser solución de dicho sistema.

Sea una matriz $A \in M_{m \cdot n}(k)$. Llamaremos espacio anulador por la derecha de A → $\boxed{N(A)}$, al conjunto

$$N(A) : \{x \in K^n \mid Ax = 0\}$$

TIPO A

IMPLÍCITAS A PARAMÉTRICAS

Nos dan una matriz de tipo A (horizontal).

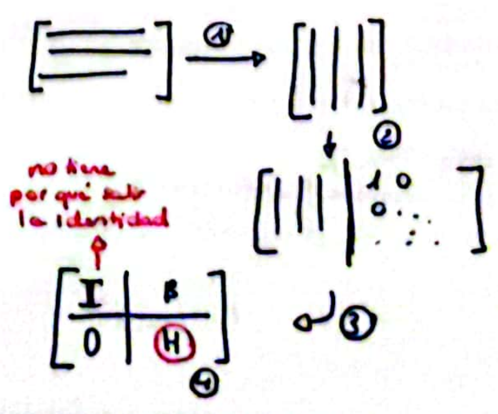
Pasos:

① Hacemos la traspuesta.

② Ampliamos la con la matriz identidad.

③ Reducimos por Gauss

④ Cogemos la matriz a la derecha de los ceros y trasponemos.



Escaneado con CamScanner

PARAMÉTRICAS A IMPLÍCITAS

Nos dan una matriz de tipo B.

Pasos:

① Ampliar con la identidad.

② Reducir por Gauss.

③ Coger la matriz a la derecha de los 0's.

$$[\,|||\,] \to [\,|||\,|\,\mathbb{I}\,] \to \left[\begin{array}{c|c} \mathbb{I} & A \\ \hline 0 & H \end{array}\right]$$

no tiene porque salir la identidad

INVERSAS E INVERSAS LATERALES

El proceso es similar al del paso de paramétricas a implícitas y viceversa, pero tiene algunos matices.

- En el caso de matrices cuadradas (nº filas = nº columnas)

  Utilizamos el teorema fundamental de la reducción por filas: $[B|I] \rightsquigarrow [R|P]$, donde, para que B tenga inversa, R debe ser la matriz identidad. Así:

  $$P \cdot B = \mathbb{I} \qquad P = B^{-1}$$, siendo P la inversa de B.

  (Ampliamos con la identidad y reducimos por Gauss)

  Como es una matriz cuadrada, su inversa lo será tanto por la derecha como por la izquierda.

- En el caso de las matrices tipo B (verticales, nº filas > nº columnas)

  Ampliamos con la identidad y reducimos, y debe de quedar lo siguiente.

$$[B\,|\,\mathbb{I}] \rightsquigarrow \left[\begin{array}{c|c} \mathbb{I} & A \\ \hline 0 & H \end{array}\right]$$

esta sería la matriz inversa (una de ellas)

matriz de ceros

OBLIGATORIO QUE QUEDE LA IDENTIDAD

SAGE:

```
B: matrix......
C: block_matrix([[B, 1]])
R: C.echelon_form()    R: copy(R)
R.subdivide(.,.) hacer la división
A: R.subdivision(0,1)
H: R.subdivision(1,1)
```

Además, como la fórmula general es:

$A + CH$

debemos sacar también la matriz H

colocar en forma de la fórmula general, donde C se deja como una letra c.

- En el caso de la matriz tipo A (horizontales, nº columnas > nº filas)

  Hacemos exactamente lo mismo pero trasponiendo A al inicio y luego al obtener B y H, transponerlas para expresar la solución.

$$[A^T\,|\,\mathbb{I}] \rightsquigarrow \left[\begin{array}{c|c} \mathbb{I} & B^T \\ \hline 0 & H^T \end{array}\right]$$

formula general

$B + H \cdot C$

LINEALMENTE INDEPENDIENTES, CONJUNTOS GENERADORES Y BASE

Para obtener el resultado tan solo hay que reducir la matriz que nos dan. NO AMPLIAR.

- Si nº columnas = nº pivotes → vectores linealmente independientes

Típicamente son de tipo B ↳ verticales

Es lo mismo que el espacio generador de las columnas de M, $B = C(M)$

- Si nº filas = nº pivotes → conjunto generador.

Típicamente son de tipo A ↳ horizontales

- Si cumple ambas condiciones, es una matriz base. Estas son obligatoriamente CUADRADAS, y al reducirla obtenemos la matriz identidad.

Tema 4

APLICACIONES LINEALES

Una aplicación $f: K^n \to K^m$ es lineal si:

① $f(u+v) = f(u) + f(v)$ para todo $u, v \in K^n$

② $f(\lambda u) = \lambda f(u)$ para todo $u \in K^n$ y para todo $\lambda \in K$

Ejemplos:
- La aplicación identidad
- La aplicación nula
- Cualquier operación elemental por filas

Las aplicaciones lineales se representan con matrices.

$M(f)$ → matriz asociada

Ejercicios típicos:

① Te piden calcular $f: K^3 \to K^4$, dándote esto:

$$f\left(\begin{bmatrix}1\\ v_1\\ 1\end{bmatrix}\right) = \begin{bmatrix}1\\ n_1\\ 1\end{bmatrix} \quad f\left(\begin{bmatrix}1\\ v_2\\ 1\end{bmatrix}\right) = \begin{bmatrix}1\\ n_2\\ 1\end{bmatrix} \ \ldots$$

Hay que crear dos matrices, por ejemplo V y N. V con los vectores (K^3) y N con K^4.

Para que sea más fácil creamos matrices por columna → V = column_matrix(QQ,[[v1],[v2]...

Luego planteamos la siguiente ecuación:

$$F \cdot V = N \text{ (siguiendo el enunciado)}$$

Despejamos F y nos queda esto:

$$F = N \cdot V^{-1}$$

Con la matriz N y la inversa de V sacamos F (la aplicación lineal).

② Te preguntan si la ~~matriz o~~ aplicación asociada a una matriz es inyectiva, sobreyectiva o biyectiva. (Literalmente lo mismo del tema 3 pero con otras palabras).

El único paso es reducir por Gauss la matriz

Será
- inyectiva cuando → nº pivotes = nº columnas (vectores independientes)
- sobreyectiva cuando → nº pivotes = nº filas (generadora)
- biyectiva cuando → inyectiva y sobreyectiva a la vez (base)

③

Núcleo de f:

Llamamos núcleo de f al espacio vectorial

$$Ker(f) = \{u \in K^n : f(u) = 0\} = N(M(f)).$$

Nos dan una matriz y nos preguntan que vectores de ella están en el núcleo la aplicación.

Para calcular los vectores del núcleo, aplicamos f a todos los vectores de la matriz A (es decir multiplicamos las dos matrices que nos dan).

$FA = F \cdot A$

De la matriz resultante, las columnas que son enteramente ceros, son las columnas que representan a los vectores que están en el núcleo. (columna 1, columna 2 ... etc)

④

Imagen de F

Llamamos imagen de f al espacio vectorial

$$Im(f) = \{v \in K^m : \exists u \in K^n \text{ tal que } f(u) = v\} = C(M(f))$$

Para calcular los vectores que se encuentran en la imagen hacemos la ampliada de las dos matrices que nos dan: $M(f)$ y A

HA = block_matrix ([[M,A]])

Luego reducimos, y tenemos que determinar que columnas hacen que exista un sistema compatible (esos vectores estarán en la imagen de f)

Por ejemplo:

$$\left[\begin{array}{cccc|cccccc} 1 & 3 & 0 & 1 & 0 & 11 & 2 & 5 & 0 & 8 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & 0 & 8 & 4 \end{array}\right]$$

si hay número al otro lado es incompatible

las dos únicas columnas compatibles.

Condiciones equivalentes

① f es inyectiva
② $Ker(f) = 0$
③ Las columnas son linealmente independientes
④ Existe una aplicación tal que $g: K^m \to K^n$ tal que $g \circ f = id_{K^n}$.

① f es sobreyectiva
② $Im(f) = K^m$
③ Las columnas son generadoras
④ Existe una aplicación tal que $f \circ g = id_{K^m}$