312 : Exercices illustrant l'utilisation de matrices inversibles

Idée : matrices inversibles est d'usage répandu : calcul de rang, résolution de système linéaire, réduction de matrices (matrices de passage inversibles)

Propriétés équivalentes à l'inversibilité de $A \in \mathcal{M}_n(\mathbb{K})$

1) $\det A \neq 0$
2) 0 n'est pas valeur propre de A
3) $\mathrm{rg}(A) = n$
4) A possède n pivots
5) $\forall b \in \mathcal{M}_{n,1}(\mathbb{K})$, le système linéaire $AX = b$ a exactement une solution
6) L'endomorphisme canoniquement associé à A est bijectif.

Exemple 1 : Cryptage de Hill (Beauville T.S spé p63 ex 105 et TD 22 p130) en 2 dimension, ex 105 p63 et en 3 dimension TD 22. (même)

- Chaque lettre est représentée par un nombre entier $\in [\![0, 25]\!]$.

L'algorithme transforme un bloc $(x_1, \dots, x_n)$ en un bloc $(y_1, \dots y_n)$ avec $\epsilon(y_1, \dots y_n) = A\,\epsilon X$ avec A clé de chiffrement $\in \mathcal{M}_n(\mathbb{Z}/26\mathbb{Z})$

- Soit $A = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 7 & 4 \\ 8 & 6 & 5 \end{pmatrix}$ et le texte CODAGE DE HILL

1) Donner le texte chiffré.

2) Décodage.

a) Mq $H' = \frac{1}{21}\begin{pmatrix} -11 & 8 & 13 \\ 13 & 13 & -23 \\ 2 & -10 & 11 \end{pmatrix}$ est H sont l'inverse l'un de l'autre.

b) Expliquer pourquoi H' n'est pas la matrice de décodage

c) Déterminer D tq $DH = I \pmod{26}$

d) déchiffrer CCYKWO.

Exercice 2 : Système de Cramer (par Vandermonde) Sorosina / L2 Algèbre

Soient $(a,b,c) \in \mathbb{K}^3$, résoudre le système

$$(S) \begin{cases} x + ay + a^2 z = a^3 \\ x + by + b^2 z = b^3 \\ x + cy + c^2 z = c^3 \end{cases}$$ d'inconnues $(x,y,z) \in \mathbb{K}^3$

A appuyer $\det(A) = (c-b)(b-a)(c-a) \neq$

Exercice 3 Topologie matricielle, densité des matrices diagonalisables dans $M_n(\mathbb{C})$

Gourdon p 195 ex 1

a) Mq l'ensemble des matrices diagonalisables de $M_n(\mathbb{C})$ est dense dans $M_n(\mathbb{C})$.

b) Que dire pour $M_n(\mathbb{R})$

Dev

A trigonalisable $\exists P \in GL_n(\mathbb{C})$ $T = P^{-1}AP$

- construction de matrices diag. par perturbation
- image continue d'une limite de suite.

Exercice 4 Étude de suites récurrentes Monier Alg. MP p 104

Soient $(u_n), (v_n), (w_n)$ suites réelles définies par

$u_0 = 0, \quad v_0 = 22, \quad w_0 = 22$

$\forall n \in \mathbb{N}$
$$u_{n+1} = \frac{1}{4}(2u_n + v_n + w_n)$$
$$v_{n+1} = \frac{1}{3}(u_n + v_n + w_n)$$
$$w_{n+1} = \frac{1}{4}(u_n + v_n + 2w_n)$$

$\chi_A(\lambda) = (1-\lambda)\left(\frac{1}{12}-\lambda\right)\left(\frac{1}{4}-\lambda\right)$

Diagonalisable.

$\forall n \in \mathbb{N}$ $X_n = A^n X_0 = P D^n P^{-1} X_0$

cvg toutes vers 14.

Exercice 5 Système différentiel linéaire Ex 8.3.6 Anal MP p 477

Résoudre le système diff linéaire de variable t, d'inconnues x et y à valeurs réelles.
$$\begin{cases} x' = x + y + \sin t \\ y' = -x + 3y \end{cases}$$

A trigonalisable

calcul de P^{-1} nécessaire

Système différentiel
$$\begin{cases} u' = 2u + v + \sin t \\ v' = 2v - \sin t \end{cases}$$

Exercice 6 Dénombrement X Alg T1 Ex 1.12 p 24 / R.B. Monier MPSI p 266

Soit A un ensemble fini de cardinal $m \geq 2$. et $U_1, \dots U_n$ des parties non vides 2 à 2 distinctes de A. On suppose qu'il existe un entier $a \geq 0$ tq si $i \neq j$ $\mathrm{Card}(U_i \cap U_j) = a$.

Mq $n \leq m$

matrice d'incidence

déterminant de Hurwitz

312 compléments

Echanger le développement de l'exercice par la décomposition polaire (avec log)

Soit $A \in \mathcal{M}_n(\mathbb{R})$

1) On suppose A inversible. Mq un unique couple $(O, S) \in O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$ tq $A = OS$

2) Mq $Gl_n(\mathbb{R})$ est dense dans $\mathcal{M}_n(\mathbb{R})$

3) On suppose A non inversible, mq A s'écrit sous la forme $A = OS$ avec O orthogonale et S symétrique positive

Vietnam Dev 6.

312 : <u>Chiffrement de Hill</u> - TD 22 p130 Terracher TS Spé.

1°/ a) $\begin{pmatrix} C \\ O \\ D \end{pmatrix}, \begin{pmatrix} A \\ G \\ E \end{pmatrix}, \begin{pmatrix} D \\ E \\ H \end{pmatrix}, \begin{pmatrix} I \\ L \\ L \end{pmatrix} \rightarrow \begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 6 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 7 \end{pmatrix} \begin{pmatrix} 8 \\ 11 \\ 11 \end{pmatrix}$

Calcul de l'image par f : $\begin{pmatrix} 39 \\ 128 \\ 115 \end{pmatrix} \begin{pmatrix} 24 \\ 58 \\ 56 \end{pmatrix}, \begin{pmatrix} 32 \\ 83 \\ 83 \end{pmatrix}, \begin{pmatrix} 63 \\ 193 \\ 185 \end{pmatrix}$

Utilisation de la division euclidienne par 26 $(\mathbb{Z}/26\mathbb{Z})$

on obtient $\begin{pmatrix} 13 \\ 24 \\ 11 \end{pmatrix}, \begin{pmatrix} 24 \\ 6 \\ 4 \end{pmatrix}, \begin{pmatrix} 6 \\ 5 \\ 5 \end{pmatrix}, \begin{pmatrix} 11 \\ 11 \\ 3 \end{pmatrix}$ soit $\begin{pmatrix} N \\ Y \\ L \end{pmatrix} \begin{pmatrix} Y \\ G \\ E \end{pmatrix} \begin{pmatrix} G \\ F \\ F \end{pmatrix} \begin{pmatrix} L \\ L \\ D \end{pmatrix}$

2°/ a) On vérifie que $HH' = H'H = I$

ou bien, on calcule $H^{-1} = H' = \frac{1}{\det A} {}^t\text{Com} A$.

b) Pour pouvoir appliquer les étapes de codage, les coefficients de la matrice de chiffrement sont nécessairement des entiers naturels.

H' ne peut donc pas être la matrice D recherchée pour le décodage

<u>Rq</u> on dira que deux matrices A et B, à coefficients, sont égales mod 26 si les coefficients de même emplacement sont congrus modulo 26.

On note alors $A \equiv B \ (26)$

On admet que D, à coefficients naturels, permet de décoder un message si $D.H = I \ (26)$

c) Donc on cherche $D \in \mathcal{M}(\mathbb{N})$ tel que $D = H^{-1}$.

en utilisant la formule de la comatrice

$$D = H^{-1} = \frac{1}{\det H} {}^t\text{Com} H$$

$$\text{d'où } H^{-1} \ (26) = \frac{1}{\det H} {}^t\text{Com} H \ (26)$$

Donc il faut que $\det H$ soit inversible modulo 26

On cherche u tel que $u \times \det H \equiv 1 \ (26)$

Par l'algorithme de Bezout, on obtient u.

Ici $\det H = 21$, on cherche $u \in \mathbb{Z}$ tel que $u \times 21 \equiv 1 \ (26)$

Soit $21u - 26n = 1$

$$\left.\begin{array}{l} 26 = 1 \times 21 + 5 \\ 21 = 4 \times 5 + 1 \end{array}\right\} \quad \begin{array}{l} 1 = 21 - 4 \times 5 \\ 1 = 21 - 4(26 - 1 \times 21) \\ 1 = 21 - 4 \times 26 + 4 \times 21 \\ 1 = -4 \times 26 + 5 \times 21 \end{array}$$

d'où $u = 5$.

On calcule alors $H^{-1} = 5 \begin{pmatrix} -11 & -8 & 13 \\ 13 & 15 & -23 \\ 2 & -10 & 4 \end{pmatrix} \ (26)$

$$D = H^{-1} = \begin{pmatrix} 23 & 12 & 13 \\ 13 & 17 & 15 \\ 10 & 2 & 3 \end{pmatrix} \ (26)$$

d) Pour le décoder $\begin{pmatrix} C \\ C \\ Y \end{pmatrix} \begin{pmatrix} K \\ U \\ 0 \end{pmatrix} \to \begin{pmatrix} 2 \\ 2 \\ 24 \end{pmatrix}, \begin{pmatrix} 10 \\ 22 \\ 15 \end{pmatrix}$

On calcule $D \times \begin{pmatrix} 382 \\ 420 \\ 96 \end{pmatrix}, \begin{pmatrix} 676 \\ 715 \\ 186 \end{pmatrix}$ puis calcul modulo 26

$\to \begin{pmatrix} 18 \\ 5 \\ 18 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ 12 \\ 4 \end{pmatrix} \to$ SESAME

Exercice recasable dans 312, 313, 314

Ref Sarrasina ex ~~5.19 p 325~~ 2.12

Soient $(a,b,c) \in \mathbb{K}^3$, résoudre le système

$$(S) \quad \begin{cases} x + ay + a^2 z = a^3 \\ x + by + b^2 z = b^3 \\ x + cy + c^2 z = c^3 \end{cases} \qquad (a,b,c) \in \mathbb{K}^3$$

Solution La matrice A du système $\begin{pmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{pmatrix}$ est une matrice de Vandermonde, de déterminant égal à $\det A = (c-b)(b-a)(c-a)$

Discussion - a, b, c trois nbs distincts 2 à 2.

$\det A \neq 0$, (S) est de Cramer, donc (S) admet une unique solution (x,y,z) définie à l'aide des formules de Cramer

$$x = \frac{1}{\det A} \begin{vmatrix} a^3 & a & a^2 \\ b^3 & b & b^2 \\ c^3 & c & c^2 \end{vmatrix} = \frac{abc}{\det A} \begin{vmatrix} a^2 & 1 & a \\ b^2 & 1 & b \\ c^2 & 1 & c \end{vmatrix} = abc$$

$$y = \frac{1}{\det A} \begin{vmatrix} 1 & a^3 & a^2 \\ 1 & b^3 & b^2 \\ 1 & c^3 & c^2 \end{vmatrix} = \frac{1}{\det A} \begin{vmatrix} 1 & a^3 & a^2 \\ 0 & b^3-a^3 & b^2-a^2 \\ 0 & c^3-a^3 & c^2-a^2 \end{vmatrix}$$

$$= \frac{1}{\det A} \left((b^3-a^3)(c^2-a^2) - (c^3-a^3)(b^2-a^2) \right)$$

$$= \frac{1}{(c-b)(b-a)(c-a)} \Big((b-a)(b^2+ab+c^2)(c+a)(c-a) - (c-a)(c^2+ac+a^2)(b-a)(b+a) \Big)$$

$$= \frac{1}{c-b} \left((b^2+ab+a^2)(c+a) - (c^2+ac+a^2)(b+a) \right)$$

$$= \frac{1}{c-b} \left(b^2c + ab^2 - bc^2 - ac^2 \right)$$

On vérifie que $(c-\beta)(a\beta + ac + bc) = a\beta c + ac^2 + bc^2 - a\beta^2 - a\beta c - \beta^2 c$

$= ac^2 + \beta c^2 - a\beta^2 - \beta^2 c$

donc $\gamma = -(ab + bc + ac)$

$$\beta = \frac{1}{\det A}\begin{vmatrix} 1 & a & a^3 \\ 1 & \beta & \beta^3 \\ 1 & c & c^3 \end{vmatrix} = \frac{1}{\det A}\begin{vmatrix} 1 & a & a^3 \\ 0 & \beta - a & \beta^3 - a^3 \\ 0 & c-a & c^3 - a^3 \end{vmatrix}$$

$$= \frac{1}{\det A}\left((\beta - a)(c^3 - a^3) - (c-a)(\beta^3 - a^3)\right)$$

$$= \frac{1}{\det A}\left((\beta - a)(c-a)(c^2 + ac + a^2) - (c-a)(\beta - a)(\beta^2 + a\beta + a^2)\right)$$

$$= \frac{1}{c-\beta}\left(c^2 + ac + a^2 - \beta^2 - a\beta - a^2\right)$$

$$= \frac{1}{c-\beta}\left(c^2 - \beta^2 + ac - a\beta\right)$$

et $(c-\beta)(a+\beta+c) = ac + \beta c + c^2 - a\beta - \beta^2 - \beta c$

$= c^2 - \beta^2 + ac - a\beta$

$= (a+\beta+c)$

<u>Deuxième cas :</u> $a = \beta \neq c$, le système (S) est réduit au système (S')

$$(S') \quad \begin{cases} x + a\gamma = a^3 - a^2\beta \\ x + c\gamma = c^3 - c^2\beta \end{cases}$$ de déterminant $(c-a) \neq 0$ par hyp.

(S') est un système de Cramer dont l'unique solution est donnée par

$$x = \frac{1}{c-a}\begin{vmatrix} a^3 - a^2\beta & a \\ c^3 - c^2\beta & c \end{vmatrix} = \frac{1}{c-a}\left(a^3 c - a^2 c\beta - ac^3 + ac^2\beta\right)$$

$$= \frac{1}{c-a}\left(ac(a^2 - c^2) + ac\beta(c-a)\right)$$

$$= \frac{1}{c-a}\left(ac(a-c)(a+c) + ac\beta(c-a)\right)$$

$$= ac\beta - ac(a+c)$$

$$y = \frac{1}{c-a}\begin{vmatrix} 1 & a^3 - a^2 z \\ 1 & c^3 - c^2 z \end{vmatrix} = \frac{1}{c-a}\left(c^3 - c^2 z - a^3 + a^2 z\right)$$

$$= \frac{1}{c-a}\left((c-a)(c^2 + ac + a^2) - z(c^2 - c^2)\right)$$

$$= c^2 + ac + a^2 - z(a+c)$$

Par permutation circulaire, on obtient $a = c \neq b$ et $c = b \neq a$

Troisième cas : $a = b = c$, on obtient une seule équation

$$x + ay + a^2 z = a^3$$

dont les solutions sont $(a^3 - a^2 z - ay, y, z)$ $(y, z) \in \mathbb{R}^2$