

Chapitre 8

Matrices

1 Points importants
2 Plan du cours

3 Questions de cours
4 Exercices types
5 Exercices

6 Exercices corrigés
7 Devoir maison

Et s'il ne fallait retenir que quatre points ?

1. **Opérations sur les matrices.** Savoir additionner et multiplier deux matrices, multiplier une matrice par un réel. Savoir également quand ces opérations sont possibles. Enfin connaître les structures qui découlent de ces opérations : $(\mathcal{M}_{pq}, +, \cdot)$ est un \mathbb{R} -espace vectoriel et $(\mathcal{M}_n, +, \times, \cdot)$ est une \mathbb{R} -algèbre.

2. **Connaître les matrices particulières suivantes et leurs principales propriétés :**
 - *Les matrices inversibles.*
 - Les matrices inversibles sont exactement les matrices carrées A telle qu'il existe une matrice carrée B vérifiant $AB = I$ OU $BA = I$. Dans ce cas $B = A^{-1}$.
 - En particulier les matrices non carrées ne sont jamais inversibles.
 - Si A et B sont inversibles alors AB est aussi inversible et $(AB)^{-1} = B^{-1}.A^{-1}$.
 - *Les matrices diagonales.*
 - $D_n(\mathbb{R})$ est stable par les loi $+$ et \times .
 - Elever une matrice diagonale à puissance n revient à élever chaque coefficient à la puissance n .
 - Une matrice diagonale est inversible si et seulement si elle ne contient aucun réel nul sur la diagonale.
 - *Les matrices symétriques/antisymétriques.*
 - $S_n(\mathbb{R})$ et $A_n(\mathbb{R})$ sont stables par la loi $+$ (mais pas par \times).
 - Les coefficients diagonaux des matrices antisymétriques sont nuls.
 - *Les matrices triangulaires supérieures (resp. inférieures).*
 - Le produit et la somme de deux matrices triangulaires supérieures (resp. inférieures) est une matrice triangulaire supérieure (resp. inférieure).
 - Une matrice triangulaire supérieure (resp. inférieure) est inversible si et seulement si elle ne contient aucun réel nul sur la diagonale.
 - *Les matrices élémentaires.*
 - La matrice $E_{ij} \times E_{kl}$ est nulle si $j \neq k$ et vaut E_{il} si $j = k$.

3. **Avoir quelques idées sur les façons de pouvoir calculer la puissance d'une matrice A .** Voici les principales :
 - a) Si c'est une matrice diagonale, il suffit d'élever les coefficient de la matrice à cette puissance.
 - b) On calcule les premières puissances : A^2, A^3, \dots . On conjecture une formule et on la démontre par récurrence. Attention, la conjecture peut s'avérer difficile.
 - c) On décompose A en $D + N$ avec $DN = ND$ et où D est une matrice diagonale et N une matrice dont les puissances sont vite toutes nulles. On utilise ensuite le binôme de Newton.
 - d) On décompose A sous la forme $P^{-1}DP$ où D est une matrice dont l'élévation à une puissance ne pose pas de problème, typiquement une matrice diagonale. Alors $A^n = P^{-1}D^nP$.
 - e) Si les colonnes de la matrice sont proportionnelles, alors $A^n = tr^{n-1}(A).A$ (Il faut le redémontrer à chaque fois).

4. Eviter les erreurs de débutants :

- a) " $AB = BA$ " est faux en général. Si A et B vérifiant cela, on dit que A et B commutent.
- b) " $AB = 0 \implies (A = 0 \text{ ou } B = 0)$ " est faux en général. Pour pouvoir l'utiliser, il faut vérifier que A ou B est inversible.
- c) " $AB = AC \implies B = C$ " est faux en général. Pour pouvoir l'utiliser, il faut vérifier que A est inversible.
- d) Pour utiliser le binôme de Newton, ne pas oublier de vérifier que les matrices A et B commutent.
- e) N'employer le symbole A^{-1} que si vous êtes sûr que A est inversible.
- f) N'employer le symbole $(AB)^n = A^n B^n$ que si vous A et B commutent.
- g) La fraction $\frac{A}{B}$ de deux matrices n'a aucun sens. Remplacez-la par AB^{-1} ou $B^{-1}A$.

I. Opérations sur les matrices.	2
1/ Définition et premiers exemples.	2
2/ Somme de deux matrices	3
3/ Multiplication d'une matrice par un réel.	3
4/ Produit de deux matrices.	3
5/ Puissance de matrices.	4
II. Matrices particulières.	4
1/ Matrices inversibles.	4
2/ Matrices élémentaires.	4
3/ Matrices triangulaires/diagonales.	4
4/ Matrices symétriques/antisymétriques.	5
5/ Matrices diviseurs de 0.	5
6/ Matrices nilpotentes.	5
III. Calcul avec des matrices.	5
1/ Autour de $AB=0$	5
2/ Pourquoi ne peut-on pas diviser par une matrices ?.	6
3/ Formule de $(AB)^n$	6
4/ Formule de Newton.	6
5/ Polynôme de matrices.	6
IV. Des outils matriciels	6
1/ La transposée.	6
2/ La trace.	7
3/ Déterminants.	7

1. Donner les coefficients du produit de matrice AB en fonction des coefficients de A (I)
et de B .
2. Soit E_{ij} et E_{kl} des matrices élémentaires de $\mathcal{M}_n(\mathbb{R})$. Déterminer le produit $E_{ij} \times E_{kl}$. (II)
Vous montrerez votre résultat.
3. Donner la définition d'une matrice symétrique, anti-symétrique, triangulaire su- (II)
périeure, triangulaire inférieure, matrice diagonale. Les ensembles $S_n(\mathbb{R})$, $A_n(\mathbb{R})$,
 $T_n^+(\mathbb{R})$, $T_n^-(\mathbb{R})$ et $D_n(\mathbb{R})$ sont-ils stables par $+$, \times et combinaisons linéaires?
4. Montrer que les matrices diviseurs de 0 puis que les matrices nilpotentes ne sont (II)
jamais inversibles.
5. Soient A et B des matrices inversibles de $\mathcal{M}_n(\mathbb{R})$, (II-IV)
 1. Montrer que tA est inversible. Que vaut $({}^tA)^{-1}$
 2. Montrer que AB est inversible. Que vaut $(AB)^{-1}$
 3. En déduire que $(GL_n(\mathbb{R}), \times)$ est un groupe non commutatif.
6. Les implications suivantes sont-elles vraies dans $\mathcal{M}_n(\mathbb{R})$: (III)

$$AB = 0 \implies A = 0 \text{ ou } B = 0 \qquad AB = AC \implies B = C$$

Si ce n'est pas le cas, donner une condition suffisante pour qu'elles soient vraies.

Exercice 1 - Puissance d'une matrice - Technique 1 : par intuition.

On note $M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

1. Calculer M^2 , M^3 , M^4 .
2. Conjecturer la valeur des coefficients de M^n , puis montrer votre résultat par récurrence.

Exercice 2 - Puissance d'une matrice - Technique 2 : avec Newton.

On note $M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $N = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

1. Énoncer la formule du binôme de Newton dans $\mathcal{M}_n(\mathbb{R})$.
2. Calculer N^2 et N^3 . En déduire N^n pour tout n de \mathbb{N} .
3. Exprimer M en fonction de N et I . En déduire M^n pour tout n de \mathbb{N} .
4. Calculer $(I + N)(I - N + N^2)$. En déduire M^{-1} .

Exercice 3 - Puissance d'une matrice - Technique 3 : par diagonalisation.

Considérons les matrices :

$$A = \begin{pmatrix} 1 & -8 & -11 \\ 0 & -13 & -20 \\ 0 & 12 & 18 \end{pmatrix} \quad P = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 3 & 4 \end{pmatrix} \quad Q = \begin{pmatrix} 1 & 1 & -2 \\ 0 & 4 & -5 \\ 0 & -3 & 4 \end{pmatrix}$$

1. Calculer le produit PQ . En déduire que P est inversible et donner P^{-1} .
2. Montrer que $A = P^{-1}DP$ où D est une matrice diagonale que vous précisez.
3. En déduire A^n

Exercice 4 - Puissance d'une matrice - Technique 4 : le cas des matrices de rang 1

Considérons la matrice :

$$A = \begin{pmatrix} 1 & 2 & 5 \\ 2 & 4 & 10 \\ 3 & 6 & 15 \end{pmatrix}$$

1. Montrer qu'il existe une matrice ligne L et une matrice colonne C tels que $A = CL$
2. Montrer que $LC = \text{tr}(A).I_1$.
3. En déduire que $A^n = (\text{tr}(A))^{n-1}.A$
4. Essayer de deviner sans démonstration les matrices pouvant s'écrire sous la forme CL où C est une matrice colonne et L une matrice ligne.

*Si les miroirs réfléchissaient vraiment,
ils ne reflèteraient pas n'importe qui!*

Vrai - Faux

Exercice 1.

Soient $A = (a_{ij})$, $B = (b_{ij})$ dans $\mathcal{M}_n(\mathbb{R})$. Déterminer si les affirmations suivantes sont vraies ou fausses.

1. $tr(AB) = tr(BA)$.
2. A est diagonale si et seulement si $a_{ii} \neq 0$ pour tout i de $\{1, \dots, n\}$.
3. ${}^t(AB) = {}^tA \cdot {}^tB$
4. $tr(AB) = tr(A) \cdot tr(B)$.
5. $tr(A + B) = tr(A) + tr(B)$.
6. Si A et B sont inversibles, alors $A \cdot B$ est inversible.
7. Si A et B sont inversibles, alors $(A + B)^2 = A^2 + B^2 + 2AB$.
8. Si A et B sont inversibles, alors $A + B$ est inversible.

Rep : 3 vraies / 5 fausses (VFFFVFFF)

Niveau 1

Exercice 2.

Soit $A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}$. Calculer A^2 . En déduire que A est inversible et calculer A^{-1} .

Exercice 3.

Calculer les produits de matrices :

1. $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

2. $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$

3. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

4. $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$

5. $\begin{pmatrix} 3 & 6 \\ -1 & -2 \end{pmatrix} \begin{pmatrix} -2 & 2 \\ 1 & -1 \end{pmatrix}$

6. $\begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix}$

7. $\begin{pmatrix} 1 & -1 \\ -2 & -2 \end{pmatrix} \begin{pmatrix} 7 \\ 2 \end{pmatrix}$

8. $\begin{pmatrix} 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -2 & 2 \end{pmatrix}$

9. $\begin{pmatrix} 1 & -1 & 3 \\ -2 & -2 & 2 \\ -1 & -3 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -2 & 2 \\ -2 & 2 \end{pmatrix}$

10. $\begin{pmatrix} 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 \\ -2 \\ 3 \end{pmatrix}$

11. $\begin{pmatrix} 1 \\ -2 \\ 3 \end{pmatrix} \begin{pmatrix} 3 & 4 & 5 \end{pmatrix}$

12. $\begin{pmatrix} 4 & 5 \\ 6 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Exercice 4.

Soit A et B des matrices carrées de taille n .

1. Simplifier les expressions suivantes :

1/ $(A.B.A^{-1})^3$ 2/ $(A + A^{-1})^2$ 3/ $A^2(A^{-1} + 2I)^2 - I$
4/ $A.A^{-1}.C + A.B.A^{-1} - C - B$ 5/ $(A + B)^2 - A^2 - B^2$

2. En supposant que $A^3 = 0$, simplifier $(A + 2I)^5$.

3. En supposant que $A^2 = 2A$, simplifier $(A + I)^5$.

Exercice 5.

On considère la matrice $M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ Le but de l'exercice est de calculer M^n .

1. Montrer que $M^2 = 5M - 4I$

2. Montrer par récurrence que, pour tout entier naturel n , il existe deux entiers α_n et β_n tels que

$$M^n = \alpha_n.M + \beta_n.I_3$$

En déduire une relation de récurrence des suites $(\alpha_n)_{n \in \mathbb{N}}$ et $(\beta_n)_{n \in \mathbb{N}}$ et les valeurs de α_0 et β_0 .

3. Calculer α_4 et β_4 . En déduire M^4 .

Exercice 6.

Soit $A = \frac{1}{2} \begin{pmatrix} 3 & -1 \\ -1 & 3 \end{pmatrix}$.

1. Déterminer des réels α et β tels que $A^2 = \alpha A + \beta I$.
2. En déduire qu'il existe pour tout entier n des réels α_n et β_n tels que $A^n = \alpha_n A + \beta_n I$

Exercice 7.

Soient $(u_n)_{n \in \mathbb{N}}$, $(v_n)_{n \in \mathbb{N}}$ et $(w_n)_{n \in \mathbb{N}}$ les suites réelles définies par $u_0 = 0$, $v_0 = 1$ et $w_0 = 2$ et pour tout entier n :

$$\begin{cases} u_{n+1} &= u_n + v_n + w_n \\ v_{n+1} &= v_n + w_n \\ w_{n+1} &= w_n \end{cases}$$

On note $C_n = \begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix}$

1. Déterminer une matrice A telle que pour tout entier n , $C_{n+1} = A \cdot C_n$.
2. Soit $B = A - I$. Calculer B^2 , B^3 puis pour tout entier $n \geq 3$: B^n (est-ce valable pour $n = 0, 1, 2$?)
3. En déduire A^n puis u_n , v_n et w_n en fonction de n

Exercice 8.

Soit $A = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 2 & 0 \\ -1 & 1 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & +1 & -1 \\ 0 & 1 & 0 \\ -1 & 1 & 0 \end{pmatrix}$

1. Calculer A^2 en déduire la valeur de A^n pour tout entier n non nul. Est-ce valable pour $n = 0$?
2. Déterminer a et b tels que $B = aA + bI$. En déduire la valeur de B^n en fonction de n . (est-ce valable pour $n = 0$?)

Niveau 2

Exercice 9.

Considérons B et C des matrices carrées de taille n telle que $C^3 = C$ et $B^2 - 3B + 2I = 0$.

1. Montrer que si $C^2 \neq I$ alors C n'est pas inversible.
2. Montrer que B est inversible.
3. Généraliser ce résultat.

Exercice 10.

Soit A et B dans $M_n(K)$ vérifiant $AB = A + B$.

1. Calculer $(I - A)(I - B)$
2. Montrer que $AB = BA$.

Ⓜ Exercice 11.

1. **Partie I.** Considérons les matrices

$$A = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Posons également $N = A - D$.

- a) Calculer N, N^2 . En déduire N^n pour tout n de \mathbb{N}
- b) En déduire les valeurs de A^n pour tout n de \mathbb{N} .

2. **Partie II.** Notons à présent les matrices

$$B = \frac{1}{2} \begin{pmatrix} 5 & 2 & 5 \\ 3 & 0 & 1 \\ -3 & -2 & -3 \end{pmatrix} \quad P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad Q = \begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{pmatrix}$$

- a) Calculer le produit PQ . En déduire que P est inversible et calculer P^{-1} .
- b) Montrer que $B = P^{-1}AP$
- c) En déduire que : $B^n = \frac{1}{2} \begin{pmatrix} 3n+2 & 1 - (-1)^n & 3n+1 - (-1)^n \\ 3n & 1 + (-1)^n & 3n-1 + (-1)^n \\ -3n & -1 + (-1)^n & -3n+1 + (-1)^n \end{pmatrix}$ pour tout n de \mathbb{N} .

3. **Partie III.** Définissons les suites $(u_n)_{n \in \mathbb{N}}$, $(v_n)_{n \in \mathbb{N}}$ et $(w_n)_{n \in \mathbb{N}}$ par :

$$\begin{cases} u_{n+1} = 5u_n + 2v_n + 5w_n \\ v_{n+1} = 3u_n + w_n \\ w_{n+1} = -3u_n - 2v_n - 3w_n \end{cases} \quad \text{Posons également } C_n = \begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix}$$

Les valeurs initiales sont données par $u_0 = w_0 = 1$ et $v_0 = -1$.

- a) Trouver une matrice D telle que $C_{n+1} = DC_n$
- b) En déduire les expressions de u_n, v_n et w_n en fonction de u_0, v_0, w_0 et n .

Exercice 12.

On note $E_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $E_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $E_3 = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 3 \\ 0 & 0 & 3 \end{pmatrix}$, $A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$.

1. Calculer : $A.E_1, A.E_2, A.E_3, E_1.A, E_2.A, E_3.A$.
2. Trouver les matrices de $M_3(\mathbb{R})$ qui commutent avec E_1, E_2, E_3 .

Exercice 13.

Soit A dans $M_n(k)$ vérifiant $\text{tr}(AM) = 0$ pour toute matrice M de $M_n(k)$. Montrer que $A = 0$. On pourra essayer de remplacer M par les matrices élémentaires.

Niveau 3

Exercice 14.

Le but de l'exercice est de chercher l'ensemble des matrices de $M_n(\mathbb{R})$ qui commutent avec toutes les autres. Cet ensemble est appelé le centre de $M_n(\mathbb{R})$. Considérons une matrices A dont les coefficients sont notés par les réels (a_{ij}) . De plus pour tout i et j de $\{1, \dots, n\}$, on note par E_{ij} la matrice élémentaire contenant des 0 partout sauf à la ligne i et la colonne j où elle contient un 1.

1. Calculer $E_{11}.A$ et $A.E_{11}$. En conclure des conditions sur les coefficients de A pour que cette matrice commute.
2. Soit i et j quelconques. Calculer $E_{ij}.A$ et $A.E_{ij}$. En conclure des conditions sur les coefficients de A pour que cette matrice commute.
3. En déduire les matrices que commutent avec toutes les autres matrices.

Exercice 15.

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice quelconque de $M_2(\mathbb{R})$. Le déterminant de A est défini comme étant : $\det(A) = ad - bc$

1. Montrer que : $A^2 - \text{tr}(A).A + \det(A).I = 0$ (Cayley-Halmilton en taille 2).
2. Nous allons montrer que A est inversible si et seulement si $\det(A) \neq 0$.
 - a) Montrer que si $\det(A)$ est non nul alors A est inversible.
 - b) Montrer par l'absurde que si A est inversible alors $\det(A) \neq 0$.
3. Nous allons montrer qu'il n'existe pas de matrice A de taille (2,2) telle que $A^2 \neq 0$ et $A^3 = 0$. Pour cela raisonnons par l'absurde en supposant que A soit une matrice telle que $A^2 \neq 0$ et $A^3 = 0$.
 - a) Montrer que A ne peut pas être inversible.
 - b) Montrer que $A^2 = 0$. Conclure.

Application à d'autres disciplines.

Exercice 16 - Cryptographie - Chiffrement de Hill.

Partie I. L'anneau $\mathbb{Z}/p\mathbb{Z}$.

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble $\{0, 1, 2, \dots, p-1\}$ sur lequel on a mis les opérations $+$ et \times . Pour effectuer une somme ou un produit, on effectue l'opération dans \mathbb{Z} , puis on retranche p suffisamment de fois pour que le résultat soit dans $\{0, 1, 2, \dots, p-1\}$. Par exemple, dans $\mathbb{Z}/5\mathbb{Z}$, on a : $3 + 4 = 2$ et $3 \times 4 = 2$. Déterminer les tables d'addition et de multiplication de $\mathbb{Z}/7\mathbb{Z}$.

Partie II. Inversibilité d'une matrice dans $\mathbb{Z}/26\mathbb{Z}$. Considérons les matrices suivantes à coefficients dans $\mathbb{Z}/26\mathbb{Z}$:

$$A = \begin{pmatrix} 1 & 3 & 5 \\ 0 & 1 & 7 \\ 1 & 4 & 13 \end{pmatrix} \qquad B = \begin{pmatrix} 11 & 7 & 16 \\ 7 & 8 & 19 \\ 25 & 25 & 1 \end{pmatrix}$$

Montrer que ces matrices sont inverses l'une de l'autre.

Partie III. Chiffrement de Hill. Pour effectuer un chiffrement de Hill, on procède comme suit :

1. On choisit un entier n de \mathbb{N}^* et une matrice A inversible de $\mathcal{M}_n(\mathbb{Z}/26\mathbb{Z})$
2. On prend le texte et on enlève la ponctuation, les espaces et les accents et les minuscules sont transformées en majuscule. A présent le texte ne contient que les lettres de A à Z.
3. A chaque lettre, on associe sa position dans l'alphabet : 'A' \rightarrow 0, 'B' \rightarrow 1, 'C' \rightarrow 2, ... On obtient donc une liste de $\mathbb{Z}/26\mathbb{Z}$ que l'on découpe en groupe de n éléments. Le dernier groupe, si nécessaire, est complété par des éléments de $\mathbb{Z}/26\mathbb{Z}$ aléatoires.
4. On considère chaque groupe de n éléments comme une matrice colonne C , puis on effectue le produit $A.C$.
5. Les matrices colonnes obtenues sont ensuite remise sous forme de liste, puis sous forme de lettre. Le texte est codé.

Montrer que le texte 'Salut à toi grand mathématicien!' est codé à l'aide de la matrice A par :

VZFFZTSXSXFRWEJZOQLOMABWZHRL

Partie IV. Déchiffrement de Hill. Pour déchiffrer un texte de Hill, il suffit de suivre les étapes du chiffrement mais en utilisant la matrice A^{-1} à la place. Sachant que le texte suivant a été codé avec la matrice A , décoder-le :

ARRVCZXVLTKHTCV

Partie V. Cryptanalyse. Le chiffrement de Hill est très fragile si on connaît des mots qui sont susceptibles d'être présent dans le texte. Par exemple, vous interceptez le message suivant :

ZBNCHAGBNCXTTMTHQDALIZNNGLE

Vous savez de plus que le texte suivant a été codé par une matrice de Hill de taille 3 que nous noterons A et que la lettre devrait commencer par 'Mon chaton'. Montrer que :

$$\begin{pmatrix} 25 & 2 & 32 \\ 27 & 7 & 27 \\ 13 & 0 & 13 \end{pmatrix} = A \times \begin{pmatrix} 12 & 2 & 19 \\ 14 & 7 & 14 \\ 13 & 0 & 15 \end{pmatrix}$$

Il reste à inverser la matrice située à droite de A (si c'est possible) pour trouver A .

Ⓡ **Exercice 11.**

1. **Partie I.** Considérons les matrices

$$A = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Posons également $N = A - D$.

- Calculer N , N^2 . En déduire N^n pour tout n de \mathbb{N}
- En déduire les valeurs de A^n pour tout n de \mathbb{N} .

2. **Partie II.** Notons à présent les matrices

$$B = \frac{1}{2} \begin{pmatrix} 5 & 2 & 5 \\ 3 & 0 & 1 \\ -3 & -2 & -3 \end{pmatrix} \quad P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad Q = \begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{pmatrix}$$

- Calculer le produit PQ . En déduire que P est inversible et calculer P^{-1} .
- Montrer que $B = P^{-1}AP$
- En déduire que : $B^n = \frac{1}{2} \begin{pmatrix} 3n+2 & 1 - (-1)^n & 3n+1 - (-1)^n \\ 3n & 1 + (-1)^n & 3n-1 + (-1)^n \\ -3n & -1 + (-1)^n & -3n+1 + (-1)^n \end{pmatrix}$ pour tout n de \mathbb{N} .

3. **Partie III.** Définissons les suites $(u_n)_{n \in \mathbb{N}}$, $(v_n)_{n \in \mathbb{N}}$ et $(w_n)_{n \in \mathbb{N}}$ par :

$$\begin{cases} u_{n+1} = 5u_n + 2v_n + 5w_n \\ v_{n+1} = 3u_n + w_n \\ w_{n+1} = -3u_n - 2v_n - 3w_n \end{cases} \quad \text{Posons également } C_n = \begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix}$$

Les valeurs initiales sont données par $u_0 = w_0 = 1$ et $v_0 = -1$.

- Trouver une matrice D telle que $C_{n+1} = DC_n$
- En déduire les expressions de u_n , v_n et w_n en fonction de u_0 , v_0 , w_0 et n .

1.a. $N = \begin{pmatrix} 0 & 3 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ et $N^2 = 0$. Ainsi $N^n = \begin{cases} I_3 & \text{si } n = 0 \\ N & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$

1.b. Comme N et D commutent (calcul rapide), on peut appliquer le binôme de Newton, ce qui donne :

$$A^n = (D + N)^n = \sum_{k=0}^n C_n^k N^k D^{n-k} = C_n^0 N^0 D^n + C_n^1 N^1 D^{n-1} = D^n + n.N.D^{n-1}$$

Comme $D^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (-1)^n \end{pmatrix}$, on trouve : $n.N.D^{n-1} = n.N = \begin{pmatrix} 0 & 3n & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

Ainsi

$$A^n = \begin{pmatrix} 1 & 3n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (-1)^n \end{pmatrix}$$

2.a. Après calcul, on trouve $PQ = 2I$ c'est-à-dire $P(\frac{1}{2}Q) = I$. Ainsi P est inversible et $P^{-1} = \frac{1}{2}Q$.

2.b. Une simple multiplication de matrices.

2.c. $B^n = (P^{-1}AP)(P^{-1}AP) \dots (P^{-1}AP) = P^{-1}A^n P$. Ainsi :

$$P^{-1}A^n = \frac{1}{2} \begin{pmatrix} 1 & 3n+1 & -(-1)^n \\ 1 & 3n-1 & (-1)^n \\ -1 & -3n+1 & (-1)^n \end{pmatrix} \quad B^n = \frac{1}{2} \begin{pmatrix} 3n+2 & 1 - (-1)^n & 3n+1 - (-1)^n \\ 3n & 1 + (-1)^n & 3n-1 + (-1)^n \\ -3n & -1 + (-1)^n & -3n+1 + (-1)^n \end{pmatrix}$$

3.a. La matrice D est la matrice $2.B$.

3.b. Comme $C_n = DC_{n-1}$ la suite C_n est géométrique et $C_n = D^n C_0 = \frac{1}{2^n} B^n C_0$. Ainsi

On trouve :

$$\begin{cases} 2^{n+1}.u_n &= (3n+2) - (1 - (-1)^n) + (3n+1 - (-1)^n) &= 6n+2 \\ 2^{n+1}.v_n &= (3n) - (1 + (-1)^n) + (3n-1 + (-1)^n) &= 6n-2 \\ 2^{n+1}.w_n &= (-3n) - (-1 + (-1)^n) + (-3n+1 + (-1)^n) &= -6n+2 \end{cases}$$

Problème - Calcul de la puissance d'une matrice

Considérons la matrice

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

Le but de l'exercice est de trouver la valeur de A^n .

1. Méthode 1

a) Calculer A^2 , A^3 et A^4 .

b) Conjecturer la valeur de A^n (on pourra remarquer si nécessaire que $32 = 2^3 \times 4$) puis démontrer votre résultat par récurrence.

2. Méthode 2. On pose $D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ et $N = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

a) Calculer N^2 . En déduire la valeur de N^n pour tout n de \mathbb{N} .

b) Déterminer la valeur de D^n , pour tout n de \mathbb{N} .

c) En remarquant $A = D + N$, en déduire la valeur de A^n .