2013-2014

Les cours du Lycée J. Durand

Mathématiques

Terminale S

Enseignement de spécialité

Rédaction :

David Zancanaro

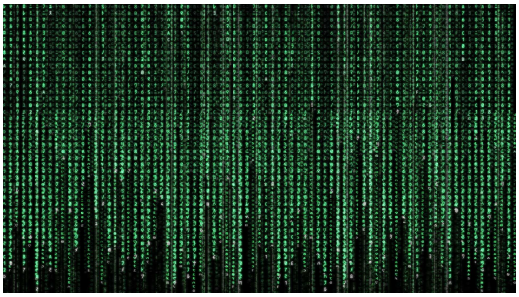
Réalisé à l'aide de :

LaTeX

Table des matières

Leçon 2

Matrice PARTIE 2



I. Inverse d'une matrice carrée

Dans tous le chapitre l'ensemble des matrices carrés de taille n à coefficients réels est noté $\mathscr{M}_n(\mathbb{R})$. En particulier $\mathscr{M}_2(\mathbb{R})$ est l'ensemble des matrices carrés d'ordre 2 à coefficients réels. Par exemple $A = \begin{pmatrix} 1 & 2 \\ 3 & 3 \end{pmatrix} \in \mathscr{M}_2(\mathbb{R})$.

I.1. Matrice unité

Définition 1.

Soit $n \in \mathbb{N}$, la matrice de $\mathscr{M}_n(\mathbb{R})$ comportant des 1 sur la diagonale (principale) et des 0 partout ailleurs est appelée matrice unité de taille n, noté I_n et vérifie pour toute matrice $A \in \mathscr{M}_n(\mathbb{R})$ on a :

$$A \times I_n = I_n \times A = A$$

Il s'agit de l'élément neutre pour la multiplication de matrice.
Par convention, on rappelle que pour toute matrice A de $\mathscr{M}_n(\mathbb{R})$ on a :

$$A^0 = I_n$$

I.2. Inverse d'une matrice - définitions

Si x est un réel non nul, il admet un inverse : c'est un réel $y = 1/x$ tel que $xy = 1$ et par commutativité, $yx = 1$. La multiplication n'étant pas commutative dans $\mathscr{M}_n(\mathbb{R})$, il faut a priori prendre des précautions.

Définition 2.

Soit $A \in \mathscr{M}_n(\mathbb{R})$ une matrice carrée d'ordre n. Une matrice B carrée d'ordre n est appelée inverse à droite de A si $AB = I_n$ et inverse à gauche de A si $BA = I_n$.

Exemple :

Soit les matrices $A = \begin{pmatrix} 10 & -2 \\ -18 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0,5 \\ 4,5 & 2,5 \end{pmatrix}$, on a :

$$A \times B = \begin{pmatrix} 10 & -2 \\ -18 & 4 \end{pmatrix} \times \begin{pmatrix} 1 & 0,5 \\ 4,5 & 2,5 \end{pmatrix} = \begin{pmatrix} 10-9 & 5-5 \\ -18+18 & -9+10 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

B est donc un inverse à droite de A mais calculons $B \times A$:

$$\begin{pmatrix} 1 & 0,5 \\ 4,5 & 2,5 \end{pmatrix} \times \begin{pmatrix} 10 & -2 \\ -18 & 4 \end{pmatrix} = \begin{pmatrix} 10-9 & -2+2 \\ 45-45 & -9+10 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

B vérifie donc $A \times B = B \times A = I_2$, par conséquent B est un inverse à droite et à gauche de A.

Si une matrice A admet un inverse à gauche et un inverse à droite alors il existe deux matrices B et C telles que $AB = CA = I_n$, on a alors :

$$(CA)B = I_nB = B \qquad \text{et} \qquad C(AB) = CI_n = C$$

Puisque $(CA)B = C(AB)$ on en déduit que $B = C$; ainsi si une matrice admet un inverse à gauche B et un inverse à droite C on a $B = C$.

Par ailleurs, si une matrice A admet un inverse à droite et à gauche, cet inverse est unique. Supposons que B et C sont deux inverses à droite et à gauche : $AB = BA = I_n$ et $AC = CA = I_n$. Alors :

$$C = CI_n = C(AB) = (CA)B = I_nB = B$$

Définition 3.

Une matrice carrée est dite inversible si elle admet un inverse à droite et à gauche. Cet inverse est alors unique. On note A^{-1} l'inverse de la matrice inversible A.
Si $A \in \mathscr{M}_n(\mathbb{R})$, on a :

$$AA^{-1} = A^{-1}A = I_n$$

Le théorème suivant est plus compliqué mais il permet en pratique d'oublier la distinction entre inverse à droite et à gauche. Il est admis.

Théorème 1.

Si une matrice carrée admet un inverse à gauche, alors elle admet un inverse à droite. Elle est donc inversible.

Ce théorème implique qu'étant donné une matrice carrée A, si on trouve une matrice de même taille B telle que $AB = I_n$ alors $BA = I_n$ et donc $B = A^{-1}$. Il est donc inutile de calculer le produit BA.

Exemple :

$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}$. Vérifions que $A^{-1} = B$:

$$AB = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix} = \begin{pmatrix} -2+2 & 1-1 \\ -6+6 & 3-2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

On déduit du théorème précédent que $BA = I_2$ et donc que $B = A^{-1}$.

I.3. Inverse d'une matrice - propriétés

Propriété 1.

Soit A une matrice inversible et $\lambda \in \mathbb{R}^*$ alors :

1. A^{-1} est inversible d'inverse A.
2. λA est inversible d'inverse $\frac{1}{\lambda}A^{-1}$.

Preuve

1. $A^{-1} \times A = I_n$ donc A est l'inverse de A^{-1}.
2. $\lambda A \times \frac{1}{\lambda}A^{-1} = \frac{\lambda}{\lambda}AA^{-1} = I_n$ donc λA est inversible d'inverse $\frac{1}{\lambda}A^{-1}$.

Exemple :

Soit $A = \begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix} = 2\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ est inversible d'inverse $\frac{1}{2}\begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}$

Théorème 2.

Soit $A \in \mathscr{M}_n(\mathbb{R})$ et $B \in \mathscr{M}_n(\mathbb{R})$ deux matrices inversibles alors le produit AB est inversible d'inverse $(AB)^{-1} = B^{-1}A^{-1}$

Preuve

$$AB \times B^{-1}A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$$

ce qui montre bien que AB est inversible d'inverse $B^{-1}A^{-1}$

Exemple :

Soit $A=\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}$ et $B=\begin{pmatrix}10 & -2\\ -18 & 4\end{pmatrix}$ sont deux matrices inversibles d'inverse $A^{-1}=\begin{pmatrix}-2 & 1\\ 3/2 & -1/2\end{pmatrix}$ et $B^{-1}=\begin{pmatrix}1 & 0,5\\ 4,5 & 2,5\end{pmatrix}$, le produit AB vaut :

$$AB=\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}\times\begin{pmatrix}10 & -2\\ -18 & 4\end{pmatrix}=\begin{pmatrix}-26 & 6\\ -42 & 10\end{pmatrix}$$

est une matrice inversible d'inverse :

$$B^{-1}A^{-1}=\begin{pmatrix}1 & 0,5\\ 4,5 & 2,5\end{pmatrix}\times\begin{pmatrix}-2 & 1\\ 3/2 & -1/2\end{pmatrix}=\begin{pmatrix}-5/4 & 3/4\\ -21/4 & 13/4\end{pmatrix}$$

I.4. Inverse d'une matrice carrée d'ordre 2

On considère une matrice $A\in\mathscr{M}_2(\mathbb{R})$ s'écrivant :

$$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

Théorème 3.

A est inversible si et seulement si $ad-bc\neq 0$.

Définition 4.

Le nombre $ad-bc$ est appelé déterminant de la matrice A, ainsi A est inversible si et seulement si son déterminant est non nul.

Preuve

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

1. Si $det A \neq 0 \iff ad - bc \neq 0$, considérons la matrice $B = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, puis calculons AB :
$$AB = \frac{1}{ad-bc} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc} \times \begin{pmatrix} ad-bc & -ab+ab \\ cd-cd & -bc+ad \end{pmatrix}$$
c'est-à-dire :
$$AB = \frac{1}{ad-bc} \times \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$
On vient de démontrer que si $det A \neq 0$ alors A était une matrice inversible d'inverse B.
2. Si $\det A = 0 \iff ad - bc = 0 \iff ad = bc$. Raisonnons par l'absurde et supposons que A soit inversible, notons alors A^{-1} son inverse. Observons par exemple le système (S), d'inconnus x et y suivant :
$$A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \iff \begin{pmatrix} x \\ y \end{pmatrix} = A^{-1} \times \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$
Si A est inversible le système (S) admet un unique couple solution. Le système (S) s'écrit encore :
$$\begin{cases} ax + by = 1 \\ cx + dy = 1 \end{cases}$$
Notons $\mathscr{D}$ la droite d'équation $ax + by = 1$ et Δ la droite d'équation $cx + dy = 1$; puisque le système (S) admet une unique solution cela signifie d'un point de vu géométrique que les droites $\mathscr{D}$ et Δ sont sécantes.
Or, le vecteur $\vec{d}(-b;a)$ dirige la droite $\mathscr{D}$ et le vecteur $\delta(-d;c)$ dirige Δ. Ces deux vecteurs sont colinéaires puisque :
$$-b \times c - a \times (-d) = -bc + ad = ad - bc = 0$$
Mais puisque les deux vecteurs directeurs sont colinéaires il vient que les droites sont parallèles (éventuellement confondus) ce qui est absurde puisque elles sont sécantes.
Par conséquent il est impossible que A soit inversible.

Théorème 4.

Si $det A \neq 0$, A est inversible et :
$$A^{-1} = \frac{1}{ab-bc} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

II. Applications

II.1. Application au système linéaire

Soit le système linéaire (S) d'inconnues x et y :

$$\begin{cases} 10x+4y=3 \\ 6x+2y=-5 \end{cases}$$

On pose $A=\begin{pmatrix}10 & 4\\ 6 & 2\end{pmatrix}$, $U=\begin{pmatrix}x\\ y\end{pmatrix}$ et $V=\begin{pmatrix}3\\ -5\end{pmatrix}$. Le système (S) s'écrit encore :

$$AU=V$$

Ici $detA=10\times 2-6\times 4=20-24\neq 0$ donc A est inversible, par conséquent :

$$AU=V \Longleftrightarrow A^{-1}AU=A^{-1}V \Longleftrightarrow U=A^{-1}V$$

Or, $A^{-1}=-\frac{1}{4}\begin{pmatrix}2 & -4\\ -6 & 10\end{pmatrix}=\begin{pmatrix}-0,5 & 1\\ 3/2 & -2,5\end{pmatrix}$, par conséquent :

$$\begin{pmatrix}x\\ y\end{pmatrix}=\begin{pmatrix}-0,5 & 1\\ 3/2 & -2,5\end{pmatrix}\times\begin{pmatrix}3\\ -5\end{pmatrix}=\begin{pmatrix}-1,5-5\\ 4,5+12,5\end{pmatrix}=\begin{pmatrix}-6,5\\ 17\end{pmatrix}$$

Théorème 5.

Soit A = UV l'écriture matricielle d'un système linéaire.
Si la matrice A est inversible alors le système admet une unique solution égale à la matrice colonne $A^{-1}V$.
Si la matrice A n'est pas inversible alors le système linéaire admet soit une infinité de solution, soit aucune solution.

Exercice 1. Résoudre le système linéaire (S) à l'aide du calcul matriciel suivant :

$$\begin{cases} -3x+2y=2 \\ 5x-7y=-1 \end{cases}$$

II.2. Chiffrement de Hill

Le principe :

On choisit quatre entiers a, b, c et d constituant la **clé** du chiffrement. Les lettres de l'alphabet sont codées de 0 à 25 grâce au tableau suivant : A chaque lettre de l'alphabet, on associe, grâce au tableau ci-dessous, un nombre entier m compris entre 0 et 25.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

A un bloc de deux lettres correspondent un couple $(x;y)$ d'entiers compris entre 0 et 25. On calcule les codes du message chiffré en associant au couple $(x;y)$ le couple $(x';y')$ tel que :

$$\begin{cases} x' \equiv ax+by \quad (26) \\ y' \equiv cx+dy \quad (26) \end{cases}$$

On souhaite chiffrer le mot DREAM.

On partage le mot en blocs de 2 lettres : DR- EA - MA (le dernier bloc est complété au hasard).

Choisissons $a=5$, $b=7$, $c=2$ et $d=3$, le système de chiffrement est donc :

$$\begin{cases} x' \equiv 7x+3y \quad (26) \\ y' \equiv 5x+8y \quad (26) \end{cases}$$

1. Chiffrer le mot DREAM.
2. On considère la matrice $\mathrm{A}=\begin{pmatrix}7 & 3\\ 5 & 8\end{pmatrix}$.
   (a) Montrer que la matrice A est inversible puis déterminer B telle que $\mathrm{A}^{-1}=\dfrac{1}{41}\mathrm{B}$.
   (b) Montrer qu'il existe un unique entier m compris entre 0 et 25 tel que $41m \equiv 1[26]$. Déterminer m.
   (c) Montrer que la matrice mB est une matrice vérifiant :
   $$m\mathrm{B}\times\begin{pmatrix}x'\\ y'\end{pmatrix}\equiv\begin{pmatrix}x\\ y\end{pmatrix}[26]$$
   (*Cette congruence sur les matrices colonnes signifie la congruence des coefficients de chaque ligne.)*
   (d) Déterminer alors quatre entiers A, B, C et D compris entre 0 et 25 tels que :
   $$\begin{pmatrix}\mathrm{A} & \mathrm{B}\\ \mathrm{C} & \mathrm{D}\end{pmatrix}\times\begin{pmatrix}x'\\ y'\end{pmatrix}\equiv\begin{pmatrix}x\\ y\end{pmatrix}[26]$$
   (e) En déduire un algorithme de décodage de ce chiffrement de Hill et déchiffrer le message :

« XZEQGCXWCO »

3. Dans le chiffrement précédent, quelle condition particulière sur 41 et 26 permet de répondre à la question 2.(b)
4. On souhaite adopter le chiffrement de Hill donné par le procédé :

$$\begin{cases} x' & \equiv & 6x+2y \quad (26) \\ y' & \equiv & 7x+3y \quad (26) \end{cases}$$

   Soit A la matrice associé à ce chiffrement. Calculer le PGCD de detA et de 26.
5. Comparer les produits $\begin{pmatrix} 6 & 2 \\ 7 & 3 \end{pmatrix} \times \begin{pmatrix} x+13 \\ y+13 \end{pmatrix}$ avec $\begin{pmatrix} 6 & 2 \\ 7 & 3 \end{pmatrix} \times \begin{pmatrix} x \\ y \end{pmatrix}$. Le procédé de codage est-il satisfaisant ? Justifier.