Fiche Algèbre linéaire 2

MATRICE D'UNE APPLICATION LINÉAIRE, RANG, DÉTERMINANT

Notions abordées

- *Matrices, rang d'une matrice.*
- *Matrices équivalentes, changement de bases.*
- *Systèmes linéaires.*
- *Propriétés du déterminant d'une matrice, matrices inversibles, matrices semblables.*

PARTIE 0 : Matrices de passage

Soit $u : E \to F$ une application linéaire entre deux K-espaces vectoriels de dimensions finies et deux bases $\mathcal{B}_E$ et $\mathcal{B}_F$ respectivement de E et F.

On note $A = \mathrm{mat}_{\mathcal{B}_E,\mathcal{B}_F}(u)$ la matrice de u dans les bases $\mathcal{B}_E, \mathcal{B}_F$.

Soit $x \in E$ et $y \in F$. On note $X = \mathrm{mat}_{\mathcal{B}_E}(x)$ la matrice colonne des coordonnées de x dans la base $\mathcal{B}_E$. On note de même $Y = \mathrm{mat}_{\mathcal{B}_F}(y)$.

1 - Compléter : $y = u(x)$ si et seulement si $Y =$

2 - Soit $p = \dim E$ et $(e_1, \ldots, e_p) = \mathcal{B}_E$. Pour $j \in \{1, \ldots, p\}$, la j-ème colonne C_j de A vérifie $C_j = \mathrm{mat}$.

On considère deux autres bases $\mathcal{B}'_E$ et $\mathcal{B}'_F$ respectivement de E et F et on note $A' = \mathrm{mat}_{\mathcal{B}'_E,\mathcal{B}'_F}(u)$, $X' = \mathrm{mat}_{\mathcal{B}'_E}(x)$ et $Y' = \mathrm{mat}_{\mathcal{B}'_F}(y)$.

3 - Compléter : $y = u(x)$ si et seulement si $Y' =$

On note $P = \mathrm{mat}_{\mathcal{B}_E}(\mathcal{B}'_E)$ la matrice de passage de la base $\mathcal{B}_E$ à la base $\mathcal{B}'_E$, et $Q = \mathrm{mat}_{\mathcal{B}_F}(\mathcal{B}'_F)$ la matrice de passage de la base $\mathcal{B}_F$ à la base $\mathcal{B}'_F$.

4 - Soit $(e'_1, \ldots, e'_p) = \mathcal{B}'_E$. Pour $j \in \{1, \ldots, p\}$, la j-ème colonne de P vaut mat .

5 - Compléter : $P = \mathrm{mat}$ (id_E).

6 - On a : $X =$, $X' =$, $Y =$ et $Y' =$.

7 - Enfin, $A =$ et $A' =$.

PARTIE I : Rang d'une matrice

Pour la suite, on fixe un corps commutatif K.

Définition

Soit $A \in \mathcal{M}_{n,p}(K)$ et $C_1, \ldots, C_p$ ses colonnes dans $\mathcal{M}_{n,1}(K)$. On appelle rang de A la dimension du sous-espace vectoriel engendré par $(C_1, \ldots, C_p)$ dans $\mathcal{M}_{n,1}(K)$.

$$\mathbf{rg}\, \boldsymbol{A} = \mathbf{dim}\, \mathbf{Vect}(\boldsymbol{C_1}, \ldots, \boldsymbol{C_p}) \ (= \mathbf{rg}(\boldsymbol{C_1}, \ldots, \boldsymbol{C_p}) \ )$$

1 - (a) Pour une matrice $A \in \mathcal{M}_{n,p}(K)$, on note φ_A l'application linéaire de $\mathcal{M}_{p,1}(K)$ dans $\mathcal{M}_{n,1}(K)$ définie par $\varphi_A(X) = AX$. Vérifier que $\operatorname{rg} A = \operatorname{rg} \varphi_A$.

(b) Montrer que pour tout $A \in \mathcal{M}_{n,p}(K)$, on a $\operatorname{rg} A \leq \min\{n, p\}$.

(c) Montrer que pour tout $A \in \mathcal{M}_{n,p}(K)$ et tout $B \in \mathcal{M}_{p,q}(K)$ on a $\operatorname{rg}(AB) \leq \min\{\operatorname{rg} A, \operatorname{rg} B\}$

2 - Soit $u : E \to F$ une application linéaire entre deux K-espaces vectoriels de dimensions finies et deux bases $\mathcal{B}_E$ et $\mathcal{B}_F$ respectivement de E et F.

(a) Montrer que $\operatorname{rg}(\operatorname{mat}_{\mathcal{B}_E,\mathcal{B}_F}(u)) = \operatorname{rg} u$.

(b) Montrer qu'il existe des bases $\mathcal{B}'_E$ et $\mathcal{B}'_F$ respectivement de E et F telles que la matrice de u dans ces bases est de la forme suivante où r est le rang de u :

$$\operatorname{mat}_{\mathcal{B}'_E,\mathcal{B}'_F}(u) = \begin{pmatrix} I_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}$$

3 - (a) Rappeler la définition des matrices équivalentes.

Deux matrices A et B de $\mathcal{M}_{n,p}(K)$ sont équivalentes s'il existe telles que

$$B = \quad A$$

(b) Démontrer que deux matrices sont équivalentes si et seulement si elles sont les matrices d'une même application linéaire dans des bases différentes.

(c) Soit $A \in \mathcal{M}_{n,p}(K)$. Montrer que $\operatorname{rg} A = r$ si et seulement si A est équivalente à $\begin{pmatrix} I_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}$.

(d) Montrer que deux matrices A et B de $\mathcal{M}_{n,p}(K)$ sont équivalentes si et seulement si $\operatorname{rg} A = \operatorname{rg} B$.

(e) Montrer que pour tout $A \in \mathcal{M}_{n,p}(K)$, on a $\operatorname{rg}({}^tA) = \operatorname{rg} A$.

4 - On considère le système linéaire d'inconnues $x_1, \ldots, x_p$ dans K et à coefficients dans K suivant :

$$(S) \begin{cases} a_{11}x_1 & + & \ldots & + & a_{1p}x_p & = & b_1 \\ & & \vdots & & & & \vdots \\ a_{n1}x_1 & + & \ldots & + & a_{np}x_p & = & b_n \end{cases}$$

(a) Écrire sous forme matricielle ce système.

(b) Exprimer la dimension du sous-espace vectoriel formé des solutions du système homogène associé en fonction de p et du rang r d'une matrice.

(c) Que peut-on dire sur l'ensemble des solutions de (S) ?

(d) Que peut-on dire de plus si le rang r vaut n ?

PARTIE II : Propriétés du déterminant

1 - Rappeler l'effet des opérations élémentaires sur les colonnes (resp. les lignes) d'une matrice carrée :

— multiplier une colonne par un scalaire, entraîne

— échanger deux colonnes, entraîne

— ajouter à une colonne une combinaison linéaire des **autres** colonnes,

2 - Soit A et B deux matrices de $\mathcal{M}_n(K)$ et $\lambda \in K$. Compléter :

— $\det I_n =$ $\det(\lambda A) =$ $\det(AB) =$ $\det({}^tA) =$

— $\det(A) = 0$ si et seulement si $\mathrm{GL}_n(K)$ si et seulement si $\mathrm{rg}(A)$

— Si $A \in \mathrm{GL}_n(K)$, on a $\det(A^{-1}) =$

3 - (a) Rappeler la définition des matrices semblables.

Deux matrices A et B de $\mathcal{M}_n(K)$ sont semblables s'il existe telle que

$$B = \quad A$$

(b) Montrer que deux matrices semblables ont même déterminant. Est-ce nécessairement le cas pour deux matrices équivalentes de $\mathcal{M}_n(K)$?

(c) Est-ce que deux matrices de $\mathrm{GL}_n(K)$ ayant même déterminant, sont nécessairement semblables ?

(d) Démontrer que deux matrices sont semblables si et seulement si elles sont les matrices d'un même endomorphisme. (On rappellera la définition d'un endomorphisme et d'une matrice d'un endomorphisme dans une base donnée.)

(e) En déduire une définition du déterminant d'un endomorphisme.

PARTIE III : Extrait sujet 1 Capes Externe 2016 - suite

Partie D : déterminant de Vandermonde

On considère la matrice de Vandermonde

$$A = \begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{pmatrix}$$

où n est un entier naturel supérieur ou égal à 2 et $a_1, \dots, a_n$ sont des nombres réels.
On cherche à déterminer par deux méthodes différentes une condition nécessaire et suffisante portant sur les a_k pour que A soit inversible.

I. Calculer le déterminant de A lorsque $n = 2$ et $n = 3$.

II. Première méthode.

1. Montrer que A est la matrice de l'application linéaire F définie dans la question A.II. dans des bases bien choisies.

2. En déduire que si les a_k sont deux à deux distincts A est inversible.

3. Qu'en est-il si deux des a_k sont égaux ?

4. Conclure.

III. Seconde méthode. On considère le polynôme

$$P(X) = (X - a_1) \dots (X - a_{n-1}).$$

1. Montrer qu'il existe des nombres réels $\lambda_0, \dots, \lambda_{n-2}$ tels que

$$P(X) = X^{n-1} + \lambda_{n-2} X^{n-2} + \dots + \lambda_1 X + \lambda_0.$$

2. On note $C_1, \dots, C_n$ les colonnes de A. Montrer que

$$C_n + \lambda_{n-2} C_{n-1} + \dots + \lambda_0 C_1 = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ P(a_n) \end{pmatrix}.$$

3. En déduire que

$$\det(A) = P(a_n) \begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-2} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & \dots & a_{n-1}^{n-2} \end{vmatrix}.$$

4. Montrer que

$$\det(A) = \prod_{1 \leqslant k < l \leqslant n} (a_l - a_k).$$

5. Conclure.

Partie E : application à la recherche de paraboles

On fixe trois points distincts A_1, A_2, A_3 du plan affine euclidien. On recherche toutes les paraboles de ce plan passant par A_1, A_2 et A_3.

I. Dans cette question, on impose en plus aux paraboles recherchées d'avoir un axe parallèle à une droite D donnée. On choisit un repère orthonormé du plan tel que D ait pour équation $x = 0$. Par définition, les paraboles d'axe parallèle à D sont les courbes d'équation

$$y = \alpha x^2 + \beta x + \gamma,$$

avec $(\alpha, \beta, \gamma) \in \mathbb{R}^3$, $\alpha \neq 0$. Les coordonnées du point A_i dans ce repère sont notées (a_i, b_i) pour $1 \leqslant i \leqslant 3$.

1. Montrer que la recherche des paraboles d'axe parallèle à D et passant par les points A_1, A_2 et A_3 est équivalente à la recherche des solutions (γ, β, α), avec $\alpha \neq 0$, du système :

$$(S) : \begin{cases} \gamma + a_1\beta + a_1^2\alpha &= b_1, \\ \gamma + a_2\beta + a_2^2\alpha &= b_2, \\ \gamma + a_3\beta + a_3^2\alpha &= b_3. \end{cases}$$

2. Montrer que si deux des points A_i ont la même abscisse (S) n'a aucune solution.

3. On suppose que les abscisses des points A_i sont deux à deux distinctes.

a. Montrer que le système (S) possède une unique solution (γ, β, α).

b. Exprimer α sous forme d'un quotient de déterminants.

c. Montrer que les conditions suivantes sont équivalentes :

i) $\alpha = 0$.

ii) $\begin{vmatrix} a_2 - a_1 & b_2 - b_1 \\ a_3 - a_1 & b_3 - b_1 \end{vmatrix} = 0$.

iii) A_1, A_2 et A_3 sont alignés.

4. Montrer que le problème admet une solution si et seulement si A_1, A_2, A_3 ne sont pas alignés et aucune des droites (A_1A_2), (A_2A_3) et (A_1A_3) n'est parallèle à D.

II. **1.** On suppose A_1, A_2 et A_3 alignés. En utilisant les résultats précédents, montrer qu'il n'existe aucune parabole passant par A_1, A_2 et A_3.

2. On suppose que A_1, A_2 et A_3 ne sont pas alignés. Montrer qu'il existe une infinité de paraboles passant par A_1, A_2 et A_3 et préciser les directions de leurs axes.

Extraits du rapport de jury 2016 :

Le jury a été particulièrement attentif aux questions suivantes :

[...]

Question D.III.3. du premier problème

Il s'agissait ici d'exploiter les propriétés du déterminant. Environ 19 % des candidats ont répondu correctement à cette question ; 12 % n'ont pas répondu correctement ou de manière incomplète ; 61 % n'ont pas abordé cette question. Environ 69 % des candidats ayant abordé cette question y ont répondu correctement.[...]

L'existence de solutions d'un système linéaire a mis de nombreux candidats en difficulté. Les énoncés suivants ont rencontré un grand succès :

- *« Tout système de trois équations à trois inconnues possède une unique solution. »*
- *« Tout système de deux équations à trois inconnues ne possède aucune solution. »*
- *« Si le déterminant d'un système de trois équations à trois inconnues est nul, alors le système ne possède aucune solution. »*

PARTIE IV : Extrait sujet 2 Capes Externe 2015

Partie B. – Chiffrement de Hill

L'objectif de cette partie est de retrouver quelques résultats sur les matrices carrées d'ordre 2 à coefficients réels, puis de les appliquer au chiffrement de Hill.

La matrice nulle d'ordre 2 est notée O_2 et la matrice unité d'ordre 2 est notée I_2.

Pour tout entier naturel n non nul, si P et Q sont deux matrices carrées d'ordre 2 dont les coefficients respectifs $p_{i,j}$ et $q_{i,j}$ appartiennent à $\mathbb{Z}$, on dit qu'elles sont congrues modulo n et on note $P \equiv Q \pmod{n}$ lorsque

$$\forall (i,j) \in \{1,2\}, \quad p_{i,j} \equiv q_{i,j} \pmod{n}.$$

De même, on dit que les vecteurs colonnes à coefficients dans $\mathbb{Z}$

$$X = \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{et} \quad X' = \begin{pmatrix} x' \\ y' \end{pmatrix}$$

sont congrus modulo n et on note $X \equiv X' \pmod{n}$ lorsque $x \equiv x' \pmod{n}$ et $y \equiv y' \pmod{n}$.

Dans toute cette partie, la matrice A est définie par

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

où a, b, c et d désignent quatre réels.

I. Questions de cours

1. Donner la définition d'une matrice inversible et démontrer l'unicité de son inverse.
2. Établir que $A^2 - (a+d)A + (ad-bc)I_2 = O_2$.
3. Démontrer que la matrice A est inversible si et seulement si $ad - bc \neq 0$.

II. Dans cette question, on suppose que a, b, c et d sont des entiers relatifs.

1. Donner un exemple de matrice inversible à coefficients dans $\mathbb{Z}$, mais dont l'inverse n'a pas tous ses coefficients dans $\mathbb{Z}$.
2. Énoncer une condition suffisante pour que la matrice A soit inversible et que son inverse A^{-1} soit à coefficients dans $\mathbb{Z}$.
3. Quelle notion mathématique (qui ne figure pas dans les programmes de lycée) permet de prouver que cette condition est nécessaire ? Proposer une démonstration du résultat.

III. La méthode étudiée ci-après utilise un chiffrement par blocs de 2 lettres pour coder un mot comportant un nombre pair de lettres :

- On choisit quatre entiers naturels non nuls a, b, c et d.
- On note x le rang de la première lettre du bloc et y le rang de la deuxième lettre du bloc.

- On définit les entiers x' et y' de la manière suivante :

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

- Le rang de la première lettre du bloc codé est le reste modulo 26 de x' ; le rang de la deuxième lettre du bloc codé est le reste modulo 26 de y'.

Un tel chiffrement est dit digraphique.

1. Traduire le système (S) par une relation matricielle à l'aide de la matrice A qui est appelée **matrice de codage**.
2. On donne : $a = 4$, $b = 3$, $c = 5$ et $d = 4$.
   a. Coder le mot BEZOUT.
   b. En détaillant les étapes, décoder le mot suivant :

   S F X M O J
3. On donne à présent $a = 3$, $b = 2$, $c = 1$ et $d = 3$. On souhaite décoder le mot suivant :

   A K X O U E V H D L
   a. Démontrer qu'il existe un unique entier u compris entre 0 et 25 tel que

   $$7u \equiv 1 \pmod{26}.$$

   b. On note A la matrice de codage associée aux entiers a, b, c et d. Déterminer une matrice B, à coefficients entiers relatifs, telle que $uBA \equiv I_2 \pmod{26}$.
   c. Décoder le mot en détaillant la démarche pour le premier bloc de deux lettres.
4. À quelle condition sur a, b, c et d peut-on décoder tout mot comportant un nombre pair de lettres ?

Rappel du préambule du sujet pour le codage des lettres :

Préambule

Ce problème a pour objet l'étude de deux méthodes de chiffrement.

À chaque lettre de l'alphabet est associé un unique entier compris entre 0 et 25 de la façon suivante : à la lettre A est associé 0, à la lettre B est associé 1, ..., à la lettre Z est associé 25. Cet entier est appelé **rang de la lettre**.