Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

II. Matrices à coefficients dans un corps.

Soit K un corps commutatif ; pour $m, n \in \mathbb{N}$, soit $\mathbf{M}_{m,n}(K)$ le K-espace vectoriel des matrices à coefficients dans K à m lignes et n colonnes. Pour $m, n, p \in \mathbb{N}$ le produit des matrices définit une application bilinéaire :

$$\mathbf{M}_{m,n}(K) \times \mathbf{M}_{n,p}(K) \longrightarrow \mathbf{M}_{m,p}(K)$$

En particulier, $\mathbf{M}_n(K) = \mathbf{M}_{n,n}(K)$ est un anneau dont le groupe des éléments inversibles est $\mathbf{GL}_n(K)$.
Le groupe $\mathbf{GL}_n(K)$ opère à droite sur l'espace $\mathbf{M}_{m,n}(K)$ et à gauche sur l'espace $\mathbf{M}_{n,m}(K)$ tandis que le groupe $\mathbf{GL}_m(K)$ opère à gauche sur l'espace $\mathbf{M}_{m,n}(K)$.
On *identifie* l'espace K^m à l'espace des matrices-colonnes $\mathbf{M}_{m,1}(K)$ et l'espace dual $(K^n)^\star$ à l'espace $\mathbf{M}_{1,n}(K)$ des matrices-lignes.
Pour $M \in \mathbf{M}_{m,n}(K)$, on désignera par $L_i(M) \in (K^n)^\star$ $(1 \leq i \leq m)$ la $i^{\text{ème}}$ ligne de M et par $C_j(M) \in K^m$ $(1 \leq j \leq n)$ la $j^{\text{ème}}$ colonne de M.
On dispose aussi de la *transposition* :

$$\begin{array}{ccc} \mathbf{M}_{m,n}(K) & \longrightarrow & \mathbf{M}_{n,m}(K) \\ M & \longrightarrow & {}^{\mathrm{t}}M \end{array}$$

1 Opérations sur les lignes et colonnes d'une matrice

1.1 Matrices élémentaires

On considère la base canonique $(E_{i,j})_{1\leq,i,j\leq n}$ de $\mathbf{M}_n(K)$; on a :

$$E_{i,j}.E_{k,l} = \delta_{j,k} E_{i,l}$$

Une matrice *élémentaire* est une matrice carrée de la forme :

$$X_{i,j}^{(n)}(s) = \mathrm{Id} + sE_{i,j} = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & & 1 & \cdots & s & \cdots & \ddots \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & & 0 & \cdots & 1 & \cdots & \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

avec $1 \leq i \neq j \leq n$. Ainsi, les coefficients de la diagonale sont égaux à 1, s est situé à la position (i, j), tous les autres coefficients sont nuls.
Pour $1 \leq i \neq j \leq n$ et $k \neq j$ on a donc :

$$\begin{cases} C_j(M\, X_{i,j}^{(n)}(s)) & = & sC_i(M) + C_j(M) \\ C_k(M\, X_{i,j}^{(n)}(s)) & = & C_k(M) \end{cases}$$

Ainsi, la multiplication de M à droite par une matrice $X_{i,j}^{(n)}(s)$ revient à ajouter à une colonne de M un multiple d'une autre colonne de M : $C_j \rightsquigarrow C_j + sC_i$.

De même pour $1 \leq i \neq j \leq m$ et $k \neq i$:

$$\left\{ \begin{array}{lcl} L_i(X_{i,j}^{(m)}(s)\, M) & = & L_i(M) + sL_j(M) \\ L_k(X_{i,j}^{(m)}(s)\, M) & = & L_k(M) \end{array} \right.$$

Ainsi, la multiplication de M à gauche par une matrice $X_{i,j}^{(m)}(s)$ revient à ajouter à une ligne de M un multiple d'une autre ligne de M : $L_i \rightsquigarrow L_i + sL_j$.

1.2 Matrices diagonales

Pour tout $\lambda = (\lambda_1, \cdots, \lambda_n) \in (K^*)^n$ on désigne par

$$\mathrm{Diag}(\lambda) = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

la matrice diagonale inversible associée à λ. On a alors :

$$C_j(M\mathrm{Diag}(\lambda)) = \lambda_j C_j(M) \text{ pour } 1 \leq j \leq n$$

L'application $\lambda \longrightarrow \mathrm{Diag}(\lambda)$ de $(K^*)^n$ dans $\mathbf{GL}_n(K)$ est un homomorphisme injectif dont l'image est le sous-groupe de $\mathbf{GL}_n(K)$ formé des matrices diagonales.
On posera, pour tout [1] $d \in K^*$:

$$D_j^{(n)}(d) = \mathrm{Diag}(d\, \epsilon_j)$$

De même on a l'homomorphisme injectif $\mu \longrightarrow \mathrm{Diag}(\mu)$ de $(K^*)^m$ dans $\mathbf{GL}_m(K)$ et on a :

$$L_i(\mathrm{Diag}(\mu)M) = \mu_i L_i(M) \text{ pour } 1 \leq i, j \leq m$$

1.3 Matrices de permutation

L'application $\pi : \mathfrak{S}_\mathfrak{n} \longrightarrow \mathbf{GL}_n(K)$ définie par $\pi_\sigma = (\delta_{i,\sigma(j)})_{1 \leq i,j \leq n}$ pour tout $\sigma \in \mathfrak{S}_n$ est un homomorphisme injectif de groupes dont l'image $\mathcal{P}$ est le sous-groupe de $\mathbf{GL}_n(K)$ des matrices de permutation.
Pour une matrice $M \in \mathbf{M}_{m,n}(K)$

$$C_j(M\, \pi_\sigma) = C_{\sigma(j)}(M) \text{ pour } 1 \leq j \leq n$$

de même on a l'homomorphisme $\pi : \mathfrak{S}_\mathfrak{m} \longrightarrow \mathbf{GL}_m(K)$ et :

$$L_i(\pi_\sigma\, M) = L_{\sigma^{-1}(i)}(M) \text{ pour } 1 \leq i \leq n$$

Les matrices élémentaires permettent d'obtenir les *transpositions au signe près* : En particulier, pour $1 \leq i \neq j \leq n$, posons :

$$P_{i,j}^{(n)} = X_{i,j}^{(n)}(1).X_{j,i}^{(n)}(-1).X_{i,j}^{(n)}(1)$$

---

1. $\epsilon_j = \underbrace{(1, \cdots, 1, d, 1, \cdots, 1)}_{d \text{ à la } j^{\text{ème}} \text{ place}}$

de sorte que :

$$\left\{\begin{array}{rcl} C_i(M\,P^{(n)}_{i,j}) & = & -C_j(M) \\ C_j(M\,P^{(n)}_{i,j}) & = & C_i(M) \\ C_k(M\,P^{(n)}_{i,j}) & = & C_k(M) \end{array}\right.$$

On a donc :

$$P^{(n)}_{i,j} = \mathrm{D}_i(-1)\pi_{(i,j)} = \pi_{(i,j)}\mathrm{D}_j(-1)$$

De même on a :

$$\left\{\begin{array}{rcl} L_i(P^{(m)}_{i,j}\,M) & = & L_j(M) \\ L_j(P^{(m)}_{i,j}\,M) & = & -L_i(M) \\ L_k(P^{(m)}_{i,j}\,M) & = & L_k(M) \end{array}\right.$$

avec, pour $1 \leq i \neq j \leq m$ et $k \neq i,j$:

$$P^{(m)}_{i,j} = X^{(m)}_{i,j}(1).X^{(m)}_{j,i}(-1).X^{(m)}_{i,j}(1)$$

Enfin, pour tout $M \in \mathcal{M}_n(K)$ et tout $\sigma \in \mathfrak{S}_n$ on a :

$$(\pi_\sigma^{-1}\,M\,\pi_\sigma)_{i,j} = M_{\sigma(i),\sigma(j)}$$

pour $1 \leq i,j \leq n$.

Proposition 1 *Pour $K \neq \mathbb{F}_2$ on a $\mathrm{N}_{\boldsymbol{GL}_n(K)}(\mathcal{H}) = \mathcal{H} \rtimes \mathcal{P}$ où $\mathcal{M} = \mathcal{H} \rtimes \mathcal{P}$ est le sous-groupe de $\boldsymbol{GL}_n(K)$ des matrices monomiales (ayant un unique coefficient non nul dans chaque ligne et chaque colonne).*

$\triangledown$ Pour tout $\mathrm{Diag}(\lambda) \in \mathcal{H}$ on a

$$(\pi_\sigma^{-1}\,\mathrm{Diag}(\lambda)\,\pi_\sigma) = \mathrm{Diag}(\sigma.\lambda)$$

où $\sigma.\lambda = (\lambda_{\sigma(1)}, \cdots, \lambda_{\sigma(n)})$ de sorte que $\mathcal{P}$ *normalise* $\mathcal{H}$.
$\mathcal{H}$ est un sous-groupe distingué de $\mathcal{P}$ et l'on a $\mathcal{H} \cap \mathcal{P} = \{\mathrm{id}\}$ de sorte que $\mathcal{M} = \mathcal{H}.\mathcal{P}$ est un sous-groupe de $\mathbf{GL}_n(K)$, que le produit $\mathcal{H}.\mathcal{P}$ est *semi-direct* et que $\mathcal{M} \subset \mathrm{N}_{\mathbf{GL}_n(K)}(\mathcal{H})$.
Réciproquement soit $M \in \mathrm{N}_{\mathbf{GL}_n(K)}(\mathcal{H})$; pour tout $\lambda \in (K^*)^n$ on a $M\mathrm{Diag}(\lambda)M^{-1} \in \mathcal{H}$ de sorte qu'il existe $\lambda' \in (K^*)^n$ tel que $M\mathrm{Diag}(\lambda) = \mathrm{Diag}(\lambda')M$. On a donc pour $1 \leq i,j \leq n$:

$$\lambda'_i M_{i,j} = \lambda_j M_{i,j}$$

Supposons qu'il existe une ligne de M ayant deux coefficients non nuls : il existe donc des indices i, j_1, j_2 avec $j_1 \neq j_2$ tels que $M_{i,j_1} \neq 0$ et $M_{i,j_2} \neq 0$; il suffit de choisir $\lambda \in (K^*)^n$ avec $\lambda_{j_1} \neq \lambda_{j_2}$ pour obtenir une contradiction. On remarque enfin que ${}^{\mathrm{t}}M \in \mathrm{N}_{\mathbf{GL}_n(K)}(\mathcal{H})$ pour conclure. $\triangle$

2 Matrices échelonnées

2.1 Matrices échelonnées en colonnes

On définit la fonction *hauteur* $\mathrm{ht} : K^m \longrightarrow [0, \cdots, m]$ en désignant, pour tout élément[2] $x = (a_1, \cdots, a_m)$ de K^m, par $\mathrm{ht}(x)$ le plus petit entier $h \in [0, \cdots, m]$ tel que $a_i = 0$ pour $1 \leq i \leq m-h$ (on a ainsi $h = 0$ si et seulement si la vecteur x est nul ; sinon on a $a_{m-h+1} \neq 0$).

Considérons une matrice $H \in \mathbf{M}_{m,n}(K)$; la matrice H est *échelonnée (en colonnes)* si l'on a :

$$\mathrm{ht}(C_1(H)) > \cdots > \mathrm{ht}(C_r(H)) > \mathrm{ht}(C_{r+1}(H)) = \cdots = 0$$

où $r \leq n$; on a posé $C_j(H) = 0 \in K^m$ pour $j > n$.
Pour chaque colonne non nulle $C_j(H)$ $(1 \leq j \leq r)$ de H, on pose $s(j) = m - \mathrm{ht}(C_j(H)) + 1$ et on appelle le coefficient $C_j(H)_{s(j)}$ un *pivot* de la matrice H.
De plus la matrice échelonnée (en colonnes) H est dite *réduite* si on a[3]

$$L_{s(j)}(H) = L_j(\mathrm{I}_n) \text{ pour } 1 \leq j \leq r$$

2. rappelons que les éléments de $x \in K^m$ sont vus comme des *vecteurs-colonnes*
3. *ie.* tous les pivots de H sont égaux à 1, et les autres coefficients de la ligne de chaque pivot sont nuls.

Proposition 2 (réduction à la forme échelonnée réduite)
Soit $M \in \boldsymbol{M}_{m,n}(K)$, il existe une matrice échelonnée $H \in \boldsymbol{M}_{m,n}(K)$ et une matrice $V \in \boldsymbol{GL}_n(K)$ telle que $H = M.V$.

Cette forme échelonnée réduite s'obtient par opérations élémentaires sur les colonnes. Plus précisément on a l'algorithme suivant :

1. *entrée :* $M \in \mathbf{M}_{m,n}(K)$
2. *initialisations :* $H := M$, V matrice unité d'ordre n, $j := 1$
3. *boucle principale :* pour i variant de 1 à m :
   (a) *recherche d'un pivot :*
   si : $H_{i,j} = 0$
   s'il existe $s \geq j+1$ *tel que* $H_{i,s} \neq 0$
   {
      i. $X = P_{j,s}^{(n)}$
      ii. $V := V.X$
      iii. $H := H.X$

   sinon passer à l'étape suivant de la boucle
   }
   (b) *mettre le pivot à 1 :*
      i. $X = D_j^{(n)}(\frac{1}{H_{i,j}})$
      ii. $V := V.X$
      iii. $H := H.X$
   (c) *réduire et échelonner : mettre à 0 les autres coefficients de la ligne du pivot :*
   pour s *variant de* 1 *à* $j-1$ *puis de* $j+1$ *à* n *boucle* : {
      i. $X := X_{j,s}^{(n)}(-H_{i,s})$
      ii. $H := H.X$
      iii. $V := V.X$

   }
   (d) $j := j+1$
   (e) *sortir quand* $j = n$

   fin de boucle principale
4. *sortie* H échelonnée et $V \in \mathrm{GL}_n(K)$ telles que $H = M.V$

$\triangledown$ Les boucles étant *énumérées* sont nécessairement finies (*terminaison*)
Soient H_j et V_j les matrices calculées à la $j^{\text{ème}}$ étape d'échelonnement ; on a $H_0 = M$ et $V_0 = \mathrm{I}$. Par hypothèse de récurrence on suppose que $V_j \in \mathbf{GL}_n(K)$, la sous-matrice de H_j formée des j premières colonnes est échelonnée réduite et $H_j = M.V_j$. A l'étape suivante on introduit une matrice X, produit d'une matrice de permutation (a) , diagonale (b) et élémentaire (c) et on pose $H_{j+1} = H_j.X$ et $V_{j+1} = V_j.X$ de sorte que $V_{j+1} \in \mathbf{GL}_n(K)$, la sous-matrice de H_{j+1} formée des $j+1$ premières colonnes est échelonnée réduite et $H_{j+1} = M.V_{j+1}$ (*correction*)
Pour évaluer le nombre d'opérations effectuées dans le corps K, il faut évidemment remplacer les produits de matrices par les opérations élémentaires qu'ils réalisent. Ceci fait la boucle principale comporte m étapes. Pour chacune de ces étapes la partie (b) comporte au plus $2n$ opérations et la partie (c) $4n$ opérations de sorte que la *complexité* est de d'ordre $\mathrm{O}(mn^2)$. $\triangle$

Proposition 3
Soit $M \in \boldsymbol{M}_{m,n}(K)$; on considère une décomposition $H = M.V$ avec H échelonnée réduite (en colonnes) et $V \in \boldsymbol{GL}_n(K)$; l'ensemble $\mathcal{E} = \{C_j(H)/1 \leq j \leq r\}$ des colonnes non nulles de H est une base de l'image $\mathrm{Im}(M)$ de M tandis que $\mathcal{K} = \{C_j(V)/r+1 \leq j \leq n\}$ est une base du noyau $\mathrm{Ker}(M)$ de M.

$\triangledown$ En effet H étant échelonnée, $\mathcal{E}$ est une partie libre de K^m donc une base de l'image $\mathrm{Im}(H)$ de H. Comme $H = M.V$ et que V est inversible on a $\mathrm{Im}(M) = \mathrm{Im}(H)$.
On a $C_j(H) = MC_j(V)$ pour $1 \leq j \leq n$ de sorte que $C_j(V) \in \mathrm{Ker}(M)$ pour $r+1 \leq j \leq n$ et comme V est inversible, les colonnes de V sont linéairement idépendantes.
Considérons alors $y \in \mathrm{Ker}(M)$; comme V est inversible on a $y = Vx$ de sorte que $x \in \mathrm{Ker}(H)$. On a donc $\sum\limits_{j=1}^{n} x_j C_j(H) = \sum\limits_{j=1}^{r} x_j C_j(H) = 0$ et comme H est échelonnée on a $x_j = 0$ pour $1 \leq j \leq r$ de sorte que $y = \sum\limits_{j=r+1}^{n} x_j C_j(V)$ et ainsi $\mathcal{K}$ est une base de $\mathrm{Ker}(M)$. $\triangle$

2.2 Action à droite de $\mathbf{GL}_n(K)$ sur $\mathbf{M}_{m,n}(K)$

Proposition 4
Soient $M, M' \in \boldsymbol{M}_{m,n}(K)$ on a $\mathrm{Im}(M') = \mathrm{Im}(M)$ si et seulement s'il existe $V \in \boldsymbol{GL}_n(K)$ tel que $M' = M.V$

$\triangledown$ Si $M' = MV$ avec $V \in \mathbf{GL}_n(K)$; on a $\mathrm{Im}(M') = \mathrm{Im}(M)$.
Réciproquement supposons que $\mathrm{Im}(M') = \mathrm{Im}(M)$. On a :

$$K^n = \mathrm{Ker}(M) \oplus F \qquad K^n = \mathrm{Ker}(M') \oplus F'$$

Alors M induit un isomorphisme de F sur $\mathrm{Im}(M)$ tandis que M' induit un isomorphisme de F' sur $\mathrm{Im}(M')$ d'où un isomorphisme $x \to V_1 x$ de F' dans F tel que $M'x = M.V_1 x$ pour tout $x \in F'$.
D'autre part il existe un isomorphisme[4] $y \to V_2 y$ de $\mathrm{Ker}(M')$ sur $\mathrm{Ker}(M)$. on pose alors, pour tout $z = y + x \in K^n = \mathrm{Ker}(M') \oplus F'$, $Vz = V_2 y + V_1 x$; on a $V \in \mathbf{GL}_n(K)$ et $M' = MV$. $\triangle$

Proposition 5
L'orbite d'une matrice $M \in \boldsymbol{M}_{m,n}(K)$ pour l'action à droite de $\boldsymbol{GL}_n(K)$ contient une unique matrice échelonnée réduite (en colonnes)

$\triangledown$ Il faut donc montrer que si $H, H' \in \mathbf{M}_{m,n}(K)$ sont deux matrices échelonnées réduites (en colonnes) telles qu'il existe $V \in \mathbf{GL}_n(K)$ avec $H' = HV$ on a $H' = H$. On remarque que H et H' ont le même rang r et on va montrer par récurrence sur r que l'on a :

$$V = \begin{pmatrix} \mathrm{I}_r & 0 \\ X & Y \end{pmatrix}$$

avec $X \in \mathbf{M}_{n-r,r}(K)$ et $Y \in \mathbf{M}_{n-r,n-r}(K)$.
Lorsque V est de cette forme, puisque $H = \begin{pmatrix} \widetilde{H} & 0 \end{pmatrix}$ où $\widetilde{H} \in \mathbf{M}_{m,r}(K)$ est formé des r premières colonnes de H, on a :

$$H' = HV = \begin{pmatrix} \widetilde{H} & 0 \end{pmatrix} \begin{pmatrix} \mathrm{I}_r & 0 \\ X & Y \end{pmatrix} = \begin{pmatrix} H'\mathrm{I}_r & 0 \end{pmatrix} = H$$

4. puisque $\dim(\mathrm{Ker}(M)) = \dim(\mathrm{Ker}(M'))$

Tout d'abord le cas $r = 1$ [5]. Les matrices H et H' sont de la forme :

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \star & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \star & 0 & \cdots & 0 \end{pmatrix}$$

La première ligne non nulle de H (*resp.* de H' étant la ligne $s(1)$ (*resp.* $s'(1)$). Comme l'on a $H\,V = H'$ on a $L_i(H)\,V = L_i(H')$ pour $1 \le i \le m$ et puisque V est inversible on a $s(1) = s'(1)$. On a alors [6] $e_1^\star V = e_1^\star$ de sorte que :

$$V = \begin{pmatrix} 1 & 0 \\ X & Y \end{pmatrix}$$

avec $X \in \mathbf{M}_{n-1,1}(K)$ et $Y \in \mathbf{M}_{n-1,n-1}(K)$.
Supposons $r \ge 2$; on a $L_{s(r)}(H) = e_r^\star$.
Soient $\overline{H}$ et $\overline{H'}$ les matrices obtenues en prenant les $s(r) - 1$ premières lignes de H et de H' de sorte que l'on a $\overline{H'} = \overline{H}V$. Ces matrices étant échelonnées réduites de rang $r - 1$ on a :

$$V = \begin{pmatrix} \mathrm{I}_{r-1} & 0 \\ X' & Y' \end{pmatrix}$$

avec $X' \in \mathbf{M}_{n-r+1,r}(K)$ et $Y' \in \mathbf{M}_{n-r+1,n-r}(K)$. de sorte que $\overline{H} = \overline{K}$.
Ensuite on a :

$$L_{s(r)}(H') = L_{s(r)}(H)V = L_r(\mathrm{I}_n)V = e_r^\star V = L_r(V)$$

Si on sait que $L_{s(r)}(H')$ est une *ligne de pivot* de H' *ie.* $L_{s(r)}(H') = e_r^\star$ et l'on a :

$$L_r(V) = L_r(\mathrm{I}_n) = e_r^\star$$

donc $V = \begin{pmatrix} \mathrm{I}_r & 0 \\ X & Y \end{pmatrix}$ avec $X \in \mathbf{M}_{n-r,r}(K)$ et $Y \in \mathbf{M}_{n-r,n-r}(K)$ et $H' = H$
Si $L_{s(r)}(H')$ n'était pas une ligne de pivot de H' on aurait $V_{r,j} = H'_{s(r),j} = 0$ pour $j \ge r$ d'où [7] :

$$\begin{aligned} L_r(V) &= \begin{pmatrix} V_{r,1} & \cdots & V_{r,r-1} & 0 & \cdots & 0 \end{pmatrix} \\ &= V_{r,1}e_1^\star + \cdots + V_{r,r-1}e_{r-1}^\star \\ &= V_{r,1}e_1^\star V + \cdots + V_{r,r-1}e_{r-1}^\star V \\ &= e_r^\star V \end{aligned}$$

Il en résulte que :

$$(V_{r,1}e_1^\star + \cdots + V_{r,r-1}e_{r-1}^\star - e_r^\star)V = 0$$

Comme V est inversible on a :

$$V_{r,1}e_1^\star + \cdots + V_{r,r-1}e_{r-1}^\star - e_r^\star = 0$$

ce qui n'est pas possible puisque les $e_i^\star$ pour $1 \le i \le n$ sont linéairement indépendants. $\triangle$

---

5. Pour $r = 0$ H et H' sont égales à la matrice nulle et V est quelconque
6. $(e_i^\star)_{1 \le i \le n}$ désigne la base canonique de $(K^n)^\star$
7. puisque $e_i^\star V = e_i^\star$ pour $1 \le i \le r - 1$