

## Fiche 1 – Algorithme de Gauss et théorème du rang

On fixe un corps commutatif  $\mathbf{K}$ . Soit  $p \in \mathbf{N} - \{0\}$ . On désigne par  $I_p$  la matrice identité d'ordre  $p$  et par  $E_{i,j}^{(p)}$  la matrice  $p \times p$  dont le coefficient d'indice  $(i, j)$  vaut 1 et les autres 0. Étant donné une permutation  $\sigma \in \mathfrak{S}_p$ , on désigne par  $W_\sigma$  la matrice (dans la base canonique) de l'application linéaire  $\mathbf{K}^p \rightarrow \mathbf{K}^p$  définie par  $e_i \mapsto e_{\sigma(i)}$ . On considère par ailleurs les matrices  $p \times p$  suivantes (D pour *dilatation* et T pour *transvection*) :

$$\begin{aligned}
 & 1 \leq i \leq p, \quad \alpha \in \mathbf{K}, \quad \alpha \neq 0 \quad D_{i,\alpha}^{(p)} = \begin{pmatrix} I_{i-1} & & \\ & \alpha & \\ & & I_{p-i} \end{pmatrix}, \\
 & 1 \leq i \neq j \leq p, \quad \beta \in \mathbf{K} \quad T_{i,j;\beta}^{(p)} = I_p + \beta E_{i,j}^{(p)} = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \beta & \\ & & & \ddots \\ & & & & 1 \end{pmatrix} \quad (\beta \text{ en position } (i, j))
 \end{aligned}$$

**Exercice 1** (Mise en route) —

1. Pour toute permutation  $\sigma \in \mathfrak{S}_p$ , expliciter la matrice  $W_\sigma$ .
2. Décrire géométriquement l'effet d'une dilatation et d'une transvection (on pourra se borner à  $p \in \{2, 3\}$  et faire des dessins).

**Exercice 2** (Opérations élémentaires) — Soit  $A$  une matrice de taille  $m \times n$  à coefficients dans  $\mathbf{K}$ . On désigne par  $L_i$  (resp.  $C_j$ ) la  $i$ -ème ligne (resp. la  $j$ -ème colonne) de  $A$ . En calculant le produit  $D_{i,\alpha}^{(m)} A$ , vérifier qu'il s'agit de la matrice obtenue en remplaçant  $L_i$  par  $\alpha L_i$ , ce que l'on notera :  $L_i \leftarrow \alpha L_i$ . Ceci donne la première colonne du tableau suivant, que l'on vérifiera :

opération	$D_{i,\alpha}^{(m)} A$	$T_{i,j;\beta}^{(m)} A$	$W_{(i,j)} A$	$A D_{i,\alpha}^{(n)}$	$A T_{i,j;\beta}^{(n)}$	$A W_{(i,j)}$
résultat	$L_i \leftarrow \alpha L_i$	$L_i \leftarrow L_i + \beta L_j$	$L_i \leftrightarrow L_j$	$C_i \leftarrow \alpha C_i$	$C_j \leftarrow C_j + \beta C_i$	$C_i \leftrightarrow C_j$

*Question subsidiaire* : pour toutes permutations  $\sigma \in \mathfrak{S}_m$  et  $\tau \in \mathfrak{S}_n$ , décrire les matrices  $W_\sigma A$  et  $A W_\tau$ .

**Exercice 3** (Preuve effective du théorème du rang) — Soit  $A$  une matrice dans  $M_{m,n}(\mathbf{K})$ . Rappelons que le rang de  $A$  est par définition la dimension du sous-espace de  $\mathbf{K}^m$  engendré par ses colonnes.

1. Vérifier que le rang de la matrice  $A$  est le rang de l'application linéaire  $\varphi_A : \mathbf{K}^n \rightarrow \mathbf{K}^m, X \mapsto AX$ .
2. Prouver que le rang d'une matrice est invariant par les opérations élémentaires de l'exercice précédent.
3. En utilisant l'algorithme de Gauss, démontrer que toute matrice  $m \times n$  est équivalente à une matrice de la forme

$$I_{m,n;r} = \left( \begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array} \right), \quad \text{où } r \in \{0, \dots, \min\{m, n\}\}.$$

4. Démontrer que l'entier  $r$  dans la question précédente est le rang de  $A$ . En déduire le théorème du rang :  $\dim \ker A + \text{rg } A = n$ .
5. Démontrer que les rangs d'une matrice et de sa transposée sont égaux.

**Exercice 4** (Générateurs du groupe linéaire) —

1. Démontrer que les dilatations, les transvections et les matrices de permutation du préambule engendrent le groupe linéaire  $GL_p(\mathbf{K})$  (reprendre la question 3 de l'exercice précédent).
2. Exprimer la matrice  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  à l'aide des matrices  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  et  $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$  (et de leurs inverses).  
En déduire que l'on peut éliminer les matrices de permutation dans la question précédente.
3. Démontrer que les transvections engendrent le groupe spécial linéaire  $SL_p(\mathbf{K})$  (appliquer l'algorithme de Gauss sans dilatations, puis observer que dans  $GL_2(\mathbf{K})$ , les matrices  $\text{diag}(d_1, d_2)$  et  $\text{diag}(1, d_1 d_2)$  se déduisent l'une de l'autre par multiplication par des transvections).

**Exercice 5** (Décomposition de Bruhat) — On désigne par  $B(\mathbf{K})$  le sous-groupe de  $GL_p(\mathbf{K})$  formé des matrices triangulaires supérieures (*sous-groupe de Borel*) et par  $U(\mathbf{K})$  le sous-groupe de  $B(\mathbf{K})$  formé des matrices dont tous les coefficients diagonaux sont égaux à 1 (*sous-groupe unipotent standard*). L'objectif de cet exercice est de démontrer que l'on a une partition :

$$GL_p(\mathbf{K}) = \bigsqcup_{\sigma \in \mathfrak{S}_p} U(\mathbf{K})W_\sigma B(\mathbf{K}).$$

Pour cela, on va appliquer l'algorithme de Gauss en choisissant dans chaque colonne le pivot en position la plus *basse* possible.

1. Soit  $A \in GL_p(\mathbf{K})$  et soit  $i_1 \in \{1, \dots, p\}$  le plus grand entier  $i$  tel que  $a_{i,1} \neq 0$ . Démontrer qu'il existe une matrice  $U_1 \in U(\mathbf{K})$  et une matrice  $B_1 \in B(\mathbf{K})$  telles que la matrice  $U_1 A B_1$  soit de la forme

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

le 1 étant en  $i_1$ -ème position dans la première colonne.

2. En itérant l'algorithme, démontrer l'existence pour toute matrice  $A \in GL_p(\mathbf{K})$  d'une permutation  $\sigma$  et de matrices  $U \in U(\mathbf{K}), B \in B(\mathbf{K})$  telles que

$$A = UW_\sigma B.$$

3. Considérons deux permutations  $\sigma, \sigma' \in \mathfrak{S}_p$  et deux matrices  $B, B' \in B(\mathbf{K})$  telles que  $BW_\sigma = W_{\sigma'} B'$ . En calculant explicitement les coefficients de ces deux dernières matrices, démontrer que la permutation  $\omega = \sigma'^{-1} \circ \sigma$  est telle que  $\omega(j) \leq j$  pour tout  $j$ , puis conclure que  $\sigma = \sigma'$ .
4. En déduire que la permutation  $\sigma$  obtenue à la question 2 est uniquement déterminée par la matrice  $A$ . Comment peut-on décrire l'ensemble des matrices pour lesquelles  $\sigma$  est le produit des  $\lfloor \frac{p}{2} \rfloor$  transpositions  $(i, j)$  telles que  $1 \leq i < j \leq p$  et  $i + j = p + 1$ ?

**Exercice 6\*** (Complexité de l'algorithme de Gauss) — Évaluer le nombre d'opérations (additions/soustractions et multiplications/divisions) que l'on effectue en résolvant un système linéaire à  $n$  équations et  $n$  inconnues générique (ayant une unique solution) avec l'algorithme de Gauss. (*Réponse* : le nombre d'opérations est équivalent à  $n^3/3$ ).

Pourquoi est-il raisonnable de négliger les comparaisons (pour trouver le plus grand pivot dans chaque colonne) et les permutations de lignes (pour placer le pivot à la bonne place) ?

**Exercice 7\*** (Équations de l'ensemble des matrices de rang donné) — Soit  $E$  un  $\mathbf{K}$ -espace vectoriel (que l'on pourra supposer de dimension finie pour se rassurer...). Pour tout entier  $p \geq 1$ , on désigne par  $\Lambda^p E$  le  $\mathbf{K}$ -espace vectoriel engendré par les symboles  $x_1 \wedge \dots \wedge x_p$ , avec  $x_1, \dots, x_p \in E$ , soumis aux relations suivantes :

- (i) chaque expression  $x_1 \wedge \dots \wedge x_p$  est  $p$ -linéaire, i.e. linéaire en chacun des  $x_i$  ;
- (ii)  $x_1 \wedge \dots \wedge x_p = 0$  si deux vecteurs consécutifs  $x_i, x_{i+1}$  sont égaux.

1. Pour tous vecteurs  $x_1, \dots, x_p \in E$  et toute permutation  $\sigma \in \mathfrak{S}_p$ , démontrer que l'on a

$$x_{\sigma(1)} \wedge \dots \wedge x_{\sigma(p)} = \varepsilon(\sigma) x_1 \wedge \dots \wedge x_p.$$

(Indication : réduction au cas où  $\sigma$  est une transposition de la forme  $(i, i+1)$ , puis calcul en remplaçant  $x_i$  et  $x_{i+1}$  par  $x_i + x_{i+1}$ ).

2. Démontrer que  $\Lambda^p E = 0$  pour tout  $p > \dim E$ .
3. Soit  $\varphi$  une forme linéaire sur  $\Lambda^p E$ . Démontrer que l'application  $\tilde{\varphi} : E^p \rightarrow \mathbf{K}$  définie par  $\tilde{\varphi}(x_1, \dots, x_p) = \varphi(x_1 \wedge \dots \wedge x_p)$  est  $p$ -linéaire et alternée<sup>1</sup>, puis que la correspondance  $\varphi \mapsto \tilde{\varphi}$  réalise un isomorphisme entre le dual de  $\Lambda^p E$  et l'espace vectoriel des formes  $p$ -linéaires alternées sur  $E$ .
4. Soit  $(e_\alpha)_{\alpha \in A}$  une base de  $E$ . On munit l'ensemble  $A$  d'un ordre total. Pour toute partie  $I \subset A$  à  $p$  éléments, on écrit  $I = \{a_1, \dots, a_p\}$  avec  $a_1 < \dots < a_p$  et on pose  $e_I = e_{a_1} \wedge \dots \wedge e_{a_p}$ . Lorsque  $I$  parcourt l'ensemble des parties à  $p$  éléments de  $A$ , démontrer que les vecteurs  $e_I$  forment une base de  $\Lambda^p E$ . (Indication : il est facile de voir que cette famille est génératrice. Pour prouver qu'elle est libre, construire des formes linéaires  $\varphi_I$  sur  $\Lambda^p E$  telles que  $\varphi_I(e_J) = \delta_{IJ}$  en utilisant la question précédente)
5. Pour toute application  $\mathbf{K}$ -linéaire  $u : E \rightarrow F$ , démontrer qu'il existe une unique application  $\mathbf{K}$ -linéaire  $\Lambda^p u : \Lambda^p E \rightarrow \Lambda^p F$  telle que

$$(\Lambda^p u)(x_1 \wedge \dots \wedge x_p) = u(x_1) \wedge \dots \wedge u(x_p)$$

pour tous vecteurs  $x_1, \dots, x_p \in E$ . Vérifier également que l'on a  $\Lambda^p (v \circ u) = (\Lambda^p v) \circ (\Lambda^p u)$  pour toutes applications linéaires composables  $u, v$ .

6. Soit  $u : E \rightarrow F$  une application  $\mathbf{K}$ -linéaire. Fixons des bases  $(e_\alpha)_{\alpha \in A}$  et  $(f_\beta)_{\beta \in B}$  de  $E$  et  $F$  respectivement, et notons  $M = (m_{\beta, \alpha})$  la matrice de  $u$  relativement à ces bases. On munit les ensembles  $A$  et  $B$  d'un ordre total. Pour toutes parties  $J \subset A$  et  $I \subset B$  de cardinal  $p$ , on pose

$$\Delta_{IJ}(M) = \det (m_{\beta, \alpha})_{\substack{\beta \in I \\ \alpha \in J}}.$$

Démontrer l'identité

$$\Lambda^p u(e_J) = \sum_I \Delta_{IJ}(M) e_I$$

où la somme porte sur l'ensemble des parties à  $p$  éléments de  $B$ .

Considérons maintenant des matrices  $A \in M_{\ell, m}(\mathbf{K})$  et  $B \in M_{m, n}(\mathbf{K})$ . Fixons un entier  $0 < p \leq \min \{\ell, m, n\}$  et des parties  $I \subset \{1, \dots, \ell\}, J \subset \{1, \dots, n\}$  à  $p$  éléments. En principe, on a fait tout ce qu'il fallait pour que la formule suivante devienne à peu près évidente :

$$\Delta_{IJ}(AB) = \sum_L \Delta_{IL}(A) \Delta_{LJ}(B)$$

où  $L$  parcourt l'ensemble des parties à  $p$  éléments de  $\{1, \dots, m\}$ . Êtes-vous d'accord ?

7. Soit  $A \in M_{m, n}(\mathbf{K})$  et soit  $\varphi_A : \mathbf{K}^n \rightarrow \mathbf{K}^m$  l'application linéaire qui lui correspond canoniquement. Démontrer que les trois conditions suivantes sont équivalentes :
- (i)  $\text{rg } A \leq r$  ;
  - (ii)  $\Lambda^r \varphi_A = 0$  ;
  - (iii) tous les mineurs d'ordre  $r+1$  de  $A$  sont nuls.
8. En déduire que le sous-ensemble  $O_r(\mathbf{K})$  de  $M_{m, n}(\mathbf{K})$  formé des matrices de rang  $r$  est défini par les équations polynomiales suivantes :

$$\forall (I \subset \{1, \dots, m\}, J \subset \{1, \dots, n\}, |I| = |J| = r+1), \quad \Delta_{IJ}(A) = 0$$

et

$$\exists (I \subset \{1, \dots, m\}, J \subset \{1, \dots, n\}, |I| = |J| = r), \quad \Delta_{IJ}(A) \neq 0.$$

---

1. On rappelle qu'une application  $p$ -linéaire  $a : E^p \rightarrow \mathbf{K}$  est *alternée* si  $a(x_1, \dots, x_p) = 0$  dès que deux vecteurs consécutifs  $x_i, x_{i+1}$  sont égaux.

**Exercice 8\*** (Algorithme de Gauss sur  $\mathbf{Z}$ ) — L'objectif est d'adapter l'algorithme de Gauss aux matrices à coefficients entiers.

1. Soit  $p \in \mathbf{N} - \{0\}$ . Justifier qu'une matrice  $A \in M_p(\mathbf{Z})$  est inversible si et seulement si  $\det M = \pm 1$ . Comment cet énoncé se généralise-t-il si l'on remplace  $\mathbf{Z}$  par un anneau commutatif unitaire quelconque ?

On adapte les notations du préambule en posant  $T_{i,j;a}^{(p)} = I_p + aE_{ij}^{(p)}$  pour tous  $i, j$  distincts dans  $\{1, \dots, p\}$  et tout  $a \in \mathbf{Z}$ ; ce sont des éléments de  $SL_p(\mathbf{Z})$  (*matrices de transvections*). On désigne par  $D_i^{(p)}$  la matrice  $\text{diag}(1, \dots, 1, -1, 1, \dots, 1) \in GL_p(\mathbf{Z})$ , où  $-1$  est en  $i$ -ème position (*matrice de dilatation*).

2. Vérifier que, pour tous  $i, j$  distincts dans  $\{1, \dots, p\}$ , la matrice

$$W'_{(i,j)} = \begin{pmatrix} I_{i-1} & & & \\ & 0 & \dots & 1 \\ & & I_{j-i-1} & \\ & -1 & \dots & 0 \\ & & & & I_{p-j} \end{pmatrix}.$$

est un produit de matrices de transvections et appartient à  $SL_p(\mathbf{Z})$ .

Étant donné  $A \in M_{m,n}(\mathbf{Z})$ , on vérifie immédiatement que multiplier  $A$  à gauche (resp. à droite) par les matrices introduites ci-dessus s'interprète en termes d'opérations élémentaires sur les lignes (resp. les colonnes), exactement comme dans l'exercice 1. On se propose maintenant de démontrer l'analogie suivant du théorème du rang pour les matrices à coefficients entiers :

Soit  $A$  une matrice de taille  $m \times n$  à coefficients dans  $\mathbf{Z}$ . Il existe des matrices  $P \in GL_m(\mathbf{Z})$  et  $Q \in GL_n(\mathbf{Z})$ , produits de matrices de transvection et de dilatations, telles que

$$PAQ^{-1} = \begin{pmatrix} \text{diag}(d_1, \dots, d_r) & 0 \\ & 0 \end{pmatrix}, \quad \text{avec } r \in \mathbf{N}, d_i > 0 \text{ et } d_1|d_2, d_2|d_3, \dots, d_{r-1}|d_r.$$

3. Posons  $\|A\| = \max\{|a_{ij}|\}$  et supposons  $A \neq 0$ . En raisonnant par récurrence sur  $\|A\|$ , démontrer que des opérations élémentaires sur les lignes et les colonnes permettent de se ramener au cas où  $a_{11} > 0$  et  $a_{11} = \min\{|a_{ij}| \mid a_{ij} \neq 0\}$ , puis au cas où

$$A = \begin{pmatrix} a_{11} & 0 \\ 0 & B \end{pmatrix}$$

avec  $B \in M_{m-1,n-1}(\mathbf{Z})$ . (*Indication* : l'observation-clef est que les opérations élémentaires permettent d'effectuer la *division euclidienne* de  $a_{i1}$  et  $a_{1i}$  par  $a_{11}$ )

4. Si  $B$  possède un coefficient  $b$  non divisible par  $a_{11}$ , démontrer que des opérations élémentaires permettent de faire décroître strictement  $\|A\|$ . (*Indication* : ajouter la colonne contenant  $b$  à la première colonne de  $A$  et faire une division euclidienne)
5. Achever la démonstration.

On va maintenant préciser le théorème ci-dessus en établissant l'*unicité des entiers*  $r$  et  $d_1, \dots, d_r$ .

6. Justifier l'unicité de  $r$  en utilisant l'inclusion  $M_{m,n}(\mathbf{Z}) \subset M_{m,n}(\mathbf{Q})$ .
7. Si  $A \neq 0$ , démontrer que  $d_1$  est le pgcd des coefficients de  $A$ .
8. Plus généralement, pour tout  $s \in \{1, \dots, r\}$ , démontrer que le produit  $d_1 \cdots d_s$  est le pgcd des mineurs d'ordre  $s$  de  $A$ . (*Indication* : utiliser la formule principale de l'exercice 7)

*Trois questions subsidiaires*

9. Si  $A \in SL_p(\mathbf{Z})$ , adapter la démonstration ci-dessus pour obtenir  $P, Q \in SL_p(\mathbf{Z})$  produits de transvections uniquement. (*Indication* : observer que  $D_i D_j = W_{(i,j)}^2$  pour tout  $i, j$  distincts dans  $\{1, \dots, p\}$ )
10. En déduire que le groupe  $SL_p(\mathbf{Z})$  est engendré par les  $2(p^2 - p)$  matrices  $T_{i,j} = I_p \pm E_{i,j}$ .
11. Généraliser tout ce qui précède au cas d'un anneau euclidien quelconque (par exemple,  $\mathbf{K}[T] \dots$ ) !