SEMAINE 2

ALGÈBRE LINÉAIRE (Programme de MPSI)

EXERCICE 1 : Idéaux à droite de $\mathcal{L}(E)$ en dimension finie

a. Théorème de factorisation

Soient E, F, G trois espaces vectoriels, soient $w \in \mathcal{L}(E,G)$ et $v \in \mathcal{L}(F,G)$. Montrer l'équivalence

$$\operatorname{Im} w \subset \operatorname{Im} v \iff \exists u \in \mathcal{L}(E,F) \quad w = v \circ u \ .$$

b. Soient $u_1, \cdots, u_k$ et v des endomorphismes d'un espace vectoriel E tels que $\operatorname{Im} v \subset \sum_{i=1}^{k} \operatorname{Im} u_i$.

Montrer qu'il existe des endomorphismes $a_1, \cdots, a_k$ de E tels que $v = \sum_{i=1}^{k} u_i \circ a_i$.

c. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Montrer que les idéaux à droite de l'algèbre $\mathcal{L}(E)$ sont les ensembles de la forme $\mathcal{I}_F = \{u \in \mathcal{L}(E) \mid \operatorname{Im} u \subset F\}$, où F est un sous-espace vectoriel de E.

Solution proposée par François CHARLES, étudiant en MP au Lycée Louis-le-Grand*

- -

a. L'implication dans le sens indirect est immédiate.

Supposons donc $\operatorname{Im} w \subset \operatorname{Im} v$. Soit T un supplémentaire de $\operatorname{Ker} v$ dans F (*on en admet l'existence*). On sait que v induit un isomorphisme (que nous noterons $\overline{v}$) de T sur $\operatorname{Im} v$. Pour tout x de E, on a $w(x) \in \operatorname{Im} v$ d'après l'hypothèse, il est donc loisible de poser $u(x) = \overline{v}^{-1}\big(w(x)\big)$. On définit ainsi une application de E dans F, dont la linéarité est immédiate et on a bien $v\big(u(x)\big) = w(x)$ pour tout x de E.

Autre solution en admettant l'existence d'une base $(e_i)_{i\in I}$ de E : si $\operatorname{Im} w \subset \operatorname{Im} v$ alors, pour tout $i \in I$, il existe un vecteur f_i de F tel que $w(e_i) = v(f_i)$. Si on appelle u l'unique application linéaire de E vers F telle que $u(e_i) = f_i$ pour tout i, on a bien $v \circ u = w$.

b. Considérons l'application linéaire $f : E^k \to E$ définie par $f(x_1, \cdots, x_k) = \sum_{i=1}^{k} u_i(x_i)$. On a clairement $\operatorname{Im} f = \sum_{i=1}^{k} \operatorname{Im} u_i$, donc $\operatorname{Im} v \subset \operatorname{Im} f$ et il existe une application linéaire A de E vers E^k telle que $v = f \circ A$. En posant $A(x) = \big(a_1(x), \cdots, a_k(x)\big)$ pour tout x de E, on a

$$\forall x \in E \qquad v(x) = f\big(A(x)\big) = f\big(a_1(x), \cdots, a_k(x)\big) = \sum_{i=1}^{k} u_i\big(a_i(x)\big) \ ,$$

donc $v = \sum_{i=1}^{k} u_i \circ a_i$.

c. *On appelle idéal à droite de $\mathcal{L}(E)$ toute partie $\mathcal{I}$ qui est un sous-groupe additif de $\mathcal{L}(E)$ et qui vérifie*

$$\forall u \in \mathcal{I} \quad \forall a \in \mathcal{L}(E) \qquad u \circ a \in \mathcal{I}\ .$$

- D'abord, si F est un sous-espace vectoriel de E, l'ensemble $\mathcal{I}_F = \{u \in \mathcal{L}(E) \mid \operatorname{Im} u \subset F\}$ est bien un idéal à droite de $\mathcal{L}(E)$.
- Soit $\mathcal{I}$ un idéal à droite de $\mathcal{L}(E)$.

Alors il est clair que $\mathcal{I}$ est un sous-espace vectoriel de $\mathcal{L}(E)$, soit $(f_1, \cdots, f_k)$ une base de l'espace vectoriel $\mathcal{I}$ (on est en dimension finie), posons $F = \sum_{i=1}^{k} \operatorname{Im} f_i$. On a alors $\mathcal{I} = \mathcal{I}_F$: en effet,

- si $f \in \mathcal{I}$, on a $f = \sum_{i=1}^{k} \lambda_i f_i$ où les λ_i sont des scalaires, donc $\operatorname{Im} f \subset F$ et $f \in \mathcal{I}_F$.

- si $f \in \mathcal{I}_F$, d'après la question **b.**, on peut écrire $f = \sum_{i=1}^{k} f_i \circ a_i$, où les a_i sont des endomorphismes de E, et $f \in \mathcal{I}$ (car les f_i appartiennent à $\mathcal{I}$ et $\mathcal{I}$ est un idéal à droite).

Remarque. Si p est un projecteur sur F, on peut noter que

$$\mathcal{I}_F = p \circ \mathcal{L}(E) = \{p \circ f\ ;\ f \in \mathcal{L}(E)\}\ :$$

$\mathcal{I}_F$ est l'"idéal à droite engendré par p".

Ce qui précède ne se généralise pas dans un espace vectoriel E de dimension infinie ; l'ensemble $\mathcal{I}$ des endomorphismes de E de rang fini est alors un idéal (bilatère) de $\mathcal{L}(E)$ qui n'est pas de la forme $\mathcal{I}_F$.

EXERCICE 2 : Idéaux à gauche de $\mathcal{L}(E)$ en dimension finie

a. Théorème de factorisation

Soient E, F, G trois espaces vectoriels, soient $w \in \mathcal{L}(E, G)$ et $u \in \mathcal{L}(E, F)$. Montrer l'équivalence

$$\operatorname{Ker} u \subset \operatorname{Ker} w \iff \exists v \in \mathcal{L}(F, G) \quad w = v \circ u\ .$$

b. Soient $u_1, \cdots, u_k$ et v des endomorphismes d'un espace vectoriel E tels que $\bigcap_{i=1}^{k} \operatorname{Ker} u_i \subset \operatorname{Ker} v$.

Montrer qu'il existe des endomorphismes $a_1, \cdots, a_k$ de E tels que $v = \sum_{i=1}^{k} a_i \circ u_i$.

c. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Montrer que les idéaux à gauche de l'algèbre $\mathcal{L}(E)$ sont les ensembles de la forme $\mathcal{J}_F = \{u \in \mathcal{L}(E) \mid F \subset \operatorname{Ker} u\}$, où F est un sous-espace vectoriel de E.

Source : Jacques CHEVALLET, Algèbre MP/PSI, Éditions Vuibert, ISBN 2-7117-2092-6

- -

a. L'implication dans le sens indirect est immédiate.

Supposons donc $\operatorname{Ker} u \subset \operatorname{Ker} w$. Soit S un supplémentaire de $\operatorname{Ker} u$ dans E (*on en admet l'existence*). On sait que u induit un isomorphisme (que nous noterons $\overline{u}$) de S sur $\operatorname{Im} u$.

Soit, par ailleurs, T un supplémentaire de $\operatorname{Im} u$ dans F. Pour tout y dans $\operatorname{Im} u$, posons $v(y) = w\big(\overline{u}^{-1}(y)\big)$ et, pour tout y dans T, posons $v(y) = 0_G$; on a ainsi défini (de façon unique puisque $T \oplus \operatorname{Im} u = F$) une application linéaire v de F vers G.

Si $x \in E$, alors $u(x) \in \operatorname{Im} u$, donc $\overline{u}^{-1}\big(u(x)\big)$ est un élément x' de S, donc de E (pas nécessairement égal à x), tel que $u(x') = u(x)$; puisque $\operatorname{Ker} u \subset \operatorname{Ker} w$ par hypothèse, on a aussi $w(x') = w(x)$, ce qui se traduit par $v\big(u(x)\big) = w(x)$, on a donc $w = v \circ u$.

b. Considérons l'application linéaire $f : E \to E^k$ définie par $f(x) = \big(u_1(x), \cdots, u_k(x)\big)$. On a clairement $\operatorname{Ker} f = \bigcap_{i=1}^{k} \operatorname{Ker} u_i$, donc $\operatorname{Ker} f \subset \operatorname{Ker} v$ et il existe une application linéaire A de E^k vers E telle que $v = A \circ f$. En posant $a_1(x) = A(x, 0, 0, \cdots, 0)$, $a_2(x) = A(0, x, 0, \cdots, 0)$, et ainsi de suite, pour tout x de E, on a

$$\begin{array}{lrcl} \forall x \in E & v(x) & = & A\big(f(x)\big) = A\big(u_1(x), \cdots, u_k(x)\big) \\ & & = & A\big(u_1(x), 0, 0, \cdots, 0\big) + A\big(0, u_2(x), 0, \cdots, 0\big) + \cdots \\ & & = & \displaystyle\sum_{i=1}^{k} a_i\big(u_i(x)\big) \ , \end{array}$$

donc $v = \displaystyle\sum_{i=1}^{k} a_i \circ u_i$.

c. *On appelle idéal à gauche de $\mathcal{L}(E)$ toute partie $\mathcal{J}$ qui est un sous-groupe additif de $\mathcal{L}(E)$ et qui vérifie*

$$\forall u \in \mathcal{J} \quad \forall a \in \mathcal{L}(E) \qquad a \circ u \in \mathcal{J} \ .$$

- D'abord, si F est un sous-espace vectoriel de E, l'ensemble $\mathcal{J}_F = \{u \in \mathcal{L}(E) \mid F \subset \operatorname{Ker} u\}$ est bien un idéal à gauche de $\mathcal{L}(E)$.
- Soit $\mathcal{J}$ un idéal à gauche de $\mathcal{L}(E)$.

Alors il est clair que $\mathcal{I}$ est un sous-espace vectoriel de $\mathcal{L}(E)$, soit $(f_1, \cdots, f_k)$ une base de l'espace vectoriel $\mathcal{I}$ (on est en dimension finie), posons $F = \bigcap_{i=1}^{k} \operatorname{Ker} f_i$. On a alors $\mathcal{I} = \mathcal{J}_F$: en effet,

- si $f \in \mathcal{I}$, on a $f = \displaystyle\sum_{i=1}^{k} \lambda_i f_i$ où les λ_i sont des scalaires, donc $F \subset \operatorname{Ker} f$ et $f \in \mathcal{J}_F$.

- si $f \in \mathcal{J}_F$, d'après la question **b.**, on peut écrire $f = \sum_{i=1}^{k} a_i \circ f_i$, où les a_i sont des endomorphismes de E, et $f \in \mathcal{I}$ (car les f_i appartiennent à $\mathcal{I}$ et $\mathcal{I}$ est un idéal à gauche).

Remarque. Si p est un projecteur de direction F (c'est-à-dire $\operatorname{Ker} p = F$*), on peut noter que*

$$\mathcal{J}_F = \mathcal{L}(E) \circ p = \{f \circ p \,;\ f \in \mathcal{L}(E)\} \ :$$

$\mathcal{J}_F$ est l'"idéal à gauche engendré par p".

Ce qui précède ne se généralise pas dans un espace vectoriel E de dimension infinie ; l'ensemble $\mathcal{J}$ des endomorphismes de E de rang fini est alors un idéal (bilatère) de $\mathcal{L}(E)$ qui n'est pas de la forme $\mathcal{J}_F$.

EXERCICE 3 :

C'est un paysan, l'a $2n+1$ vaches. Quand qu'y met d'côté l'une quelconque d'ses vaches, ben les $2n$ qui restent, y peut les répartir en deux sous-troupeaux de n vaches chacun et ayant le même poids total.

Montrer qu'les vaches, è z'ont toutes le même poids.

Source : Merci à Christophe HÉNOCQ

- -

Soient $p_1, \ldots, p_{2n+1}$ les poids des vaches (nommées $V_1, \ldots, V_{2n+1}$, c'est plus pratique que "Marguerite"). Soit $P = \begin{pmatrix} p_1 \\ \vdots \\ p_{2n+1} \end{pmatrix} \in \mathbb{R}^{2n+1}$.

Traduisons l'hypothèse : pour tout $i \in [\![1, 2n+1]\!]$, les vaches V_j $(j \neq i)$ peuvent être réparties en deux sous-troupeaux de même effectif et de même poids total. Il existe donc des coefficients $a_{i,j}$ (avec $1 \leq j \leq 2n+1$) tels que

- **(1)** $a_{i,i} = 0$ (*la vache V_i part brouter dans son coin*) ;
- **(2)** $a_{i,j} = \pm 1$ si $j \neq i$; (*le signe dépend du sous-troupeau dans lequel on met la vache V_j*)
- **(3)** $\sum_{j=1}^{2n+1} a_{i,j} = 0$ (*les deux sous-troupeaux ont même effectif*)
- **(4)** $\sum_{j=1}^{2n+1} a_{i,j} p_j = 0$ (*les deux sous-troupeaux ont même poids total*).

Autrement dit, il existe une matrice $A = (a_{i,j}) \in \mathcal{M}_{2n+1}(\mathbb{R})$ telle que

- **(1)** : les coefficients diagonaux sont nuls ;
- **(2)** : les autres coefficients valent ± 1 ;

• **(3)** : la somme des éléments de chaque ligne est nulle, ce qui revient à dire que $X_0 = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ appartient au noyau $\mathrm{Ker}\, A$;

• **(4)** : la somme des éléments de chaque ligne, pondérés des coefficients p_j, est nulle, c'est-à-dire $P \in \mathrm{Ker}\, A$.

Nous allons montrer que toute matrice $A \in \mathcal{M}_{2n+1}(\mathbb{R})$ vérifiant les conditions **(1)** et **(2)** est de rang $2n$, ce qui signifie que son noyau est de dimension 1. Les conditions **(3)** et **(4)** entraîneront alors que les vecteurs P et X_0 sont colinéaires, donc que les vaches ont toutes le même poids.

Soit donc une matrice $A \in \mathcal{M}_{2n+1}(\mathbb{R})$ vérifiant les conditions **(1)** et **(2)**. Considérons la matrice extraite $B = (a_{ij})_{1 \leq i,j \leq 2n}$ obtenue en ôtant la dernière ligne et la dernière colonne, et montrons qu'elle est inversible. Son déterminant est

$$D = \det(B) = \sum_{\sigma \in \mathcal{S}_{2n}} \varepsilon(\sigma)\, a_{1,\sigma(1)} \dots a_{2n,\sigma(2n)} \ .$$

Les termes diagonaux étant nuls, les seuls termes non nuls du développement de ce déterminant sont ceux pour lesquels σ est un **dérangement** (permutation sans point fixe) de $[\![1, 2n]\!]$. Par ailleurs, chacun de ces termes non nuls vaut ± 1, donc le déterminant D est un entier relatif de même parité que le nombre de dérangements de l'ensemble $[\![1, 2n]\!]$. Si nous prouvons que ce nombre est impair, la démonstration est achevée.

Soit donc, pour tout k entier naturel non nul, d_k le nombre de dérangements de l'ensemble $[\![1, k]\!]$. Nous allons prouver la relation de récurrence

$$(\mathbf{R}) \ : \qquad d_k = (k-1)(d_{k-1} + d_{k-2}) \qquad\qquad (k \geq 3) \ .$$

Preuve de la relation **(R)** : soit $k \geq 3$, soit σ un dérangement de $[\![1, k]\!]$. Il y a $k-1$ choix possibles pour le nombre $j = \sigma(k) \in [\![1, k-1]\!]$. Deux possibilités s'excluent alors mutuellement :

- si $\sigma(j) = k$, alors la restriction de σ à l'ensemble $[\![1, k]\!] \setminus \{j, k\}$ est un dérangement d'un ensemble à $k-2$ éléments, il y en a d_{k-2} ;

- si $\sigma(j) \neq k$, le dénombrement est un peu moins évident. Introduisons pour cela l'ensemble $\mathcal{E}_j$ des dérangements de $[\![1, k]\!]$ tels que $\sigma(k) = j$ et $\sigma(j) \neq k$, puis l'ensemble $\mathcal{F}$ des dérangements de $[\![1, k-1]\!]$. A tout élément σ de $\mathcal{E}_j$, associons l'élément τ de $\mathcal{F}$ défini par $\begin{cases} \tau\big(\sigma^{-1}(k)\big) = j \\ \tau(p) = p \quad \text{si } p \neq \sigma^{-1}(k) \end{cases}$ (en quelque sorte, on "zappe" l'élément k). On voit facilement que la correspondance $\sigma \mapsto \tau$ est une bijection de $\mathcal{E}_j$ sur $\mathcal{F}$, la bijection réciproque est $\tau \mapsto \sigma$, avec $\begin{cases} \sigma\big(\tau^{-1}(j)\big) = k \\ \sigma(k) = j \\ \sigma(p) = \tau(p) \quad \text{sinon} \end{cases}$. Donc le cardinal de $\mathcal{E}_j$ est d_{k-1}, ce qui achève la démonstration.

Revenons à nos vaches... De la relation **(R)**, il résulte que $d_{2n-1} = (2n-2)(d_{2n-2} + d_{2n-3})$ est toujours un nombre pair, puis on montre par récurrence sur n que d_{2n} est impair :

- pour $n = 1$, $d_2 = 1$;

- si d_{2n-2} est impair (pour $n \geq 2$), alors $d_{2n} = (2n-1)(d_{2n-1} + d_{2n-2})$ avec $2n-1$ impair, d_{2n-1} pair et d_{2n-2} impair, donc d_{2n} est impair, ce qui achève le troupeau.

****

Quelques compléments sur les dérangements, sans plus déranger les vaches qui finiraient par devenir folles...

La relation de récurrence **(R)** permet d'écrire une fonction récursive en MAPLE pour calculer le nombre d_n, not `der(n)` :

```
> der:= proc(n) option remember:
        if n=1  then 0
                elif n=2 then 1
                else (n-1)*(der(n-1)+der(n-2))
          fi
  end:
```

La relation **(R)** peut s'écrire $d_n - nd_{n-1} = -\big[d_{n-1} - (n-1)d_{n-2}\big]$; la suite de terme général $u_n = d_n - nd_{n-1}$ est donc géométrique de raison -1, d'où $u_n = d_n - nd_{n-1} = (-1)^n$ pour $n \geq 2$. On a donc, pour tout $k \geq 2$, la relation $\dfrac{d_k}{k!} - \dfrac{d_{k-1}}{(k-1)!} = \dfrac{(-1)^k}{k!}$. En sommant pour k de 2 à n, on obtient

$$d_n = n! \left(\sum_{k=2}^{n} \frac{(-1)^k}{k!} \right)$$

et, comme conséquence, l'équivalence $d_n \sim \dfrac{n!}{e}$.

EXERCICE 4 :

Soient P et Q deux polynômes de $\mathbb{C}[X]$, de degrés m et n respectivement.

1. Montrer que P et Q ont une racine commune si et seulement si la famille

$$(P, XP, \ldots, X^{n-1}P, Q, XQ, \ldots, X^{m-1}Q)$$

est liée dans $\mathbb{C}[X]$.

2. On pose $P = \sum_{k=0}^{m} a_k X^k$, $Q = \sum_{j=0}^{n} b_j X^j$.

Écrire un déterminant qui s'annule si et seulement si P et Q ont une racine commune.

3. En déduire une condition nécessaire et suffisante pour que le polynôme $P = X^3 + pX + q$ admette une racine double.

4. Un nombre complexe a est dit **algébrique** s'il annule un polynôme (non nul) à coefficients rationnels.

Montrer que la somme de deux nombres algébriques est algébrique.

Ecrire un polynôme non nul de $\mathbb{Q}[X]$, de plus petit degré possible, admettant pour racine $i+j$.

Source : Jean-Pierre ESCOFIER, Théorie de Galois, Éditions Masson, ISBN 2-225-82948-9.

- -

1. Les polynômes P et Q ont une racine commune si et seulement si leur pgcd $P \wedge Q$ est non constant, c'est-à-dire si et seulement si leur ppcm $P \vee Q$ est de degré strictement inférieur à $m+n$ (puisque les polynômes PQ et $(P \wedge Q)(P \vee Q)$ sont associés). Cela équivaut à l'existence d'un multiple commun non nul de degré $< m+n$, ou encore de deux polynômes U et V non tous deux nuls tels que

$$UP - VQ = 0\,, \quad \text{avec} \quad \deg U < n \quad \text{et} \quad \deg V < m\,.$$

Une condition nécessaire et suffisante est donc que la famille de polynômes

$$\mathcal{P} = (P, XP, \ldots, X^{n-1}P, Q, XQ, \ldots, X^{m-1}Q)$$

soit liée.

2. Il suffit de considérer le déterminant (d'ordre $m+n$) de la famille $\mathcal{P}$ dans la base canonique $(1, X, X^2, \ldots, X^{m+n-1})$ de $\mathbb{C}_{m+n-1}[X]$:

$$\mathcal{S}_X(P,Q) = \begin{vmatrix} a_0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & \ldots & 0 \\ a_1 & \ddots & \ddots & \vdots & b_1 & \ddots & \ddots & & \vdots \\ \vert & \ddots & \ddots & 0 & \vert & \ddots & \ddots & \ddots & \vdots \\ \vert & & \ddots & a_0 & \vert & & \ddots & \ddots & 0 \\ \vert & & & a_1 & b_n & & & \ddots & b_0 \\ a_m & & & \vert & 0 & \ddots & & & b_1 \\ 0 & \ddots & & \vert & \vdots & \ddots & \ddots & & \vert \\ \vdots & \ddots & \ddots & \vert & \vdots & & \ddots & \ddots & \vert \\ 0 & \ldots & 0 & a_m & 0 & \ldots & \ldots & 0 & b_n \end{vmatrix}$$

(les n premières colonnes sont constituées des coefficients du polynôme P, que l'on décale et les m colonnes suivantes des coefficients du polynôme Q, que l'on décale). $\mathcal{S}_X(P,Q)$ est le **déterminant de Sylvester** des polynômes P et Q.

3. On cherche une condition pour que le polynôme P et sa dérivée P' aient une racine commune. Or,

$$\mathcal{S}_X(P,P') = \begin{vmatrix} q & 0 & p & 0 & 0 \\ p & q & 0 & p & 0 \\ 0 & p & 3 & 0 & p \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = \begin{vmatrix} 0 & 0 & p & -3q & 0 \\ 0 & q & 0 & -2p & 0 \\ 0 & 0 & 3 & 0 & -2p \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = - \begin{vmatrix} 0 & p & -3q & 0 \\ 0 & 0 & -2p & -3q \\ 0 & 3 & 0 & -2p \\ 1 & 0 & 0 & 3 \end{vmatrix}$$

$$= \begin{vmatrix} p & -3q & 0 \\ 0 & -2p & -3q \\ 3 & 0 & -2p \end{vmatrix} = 4p^3 + 27q^2$$

(*on a effectué d'abord les opérations* $L_1 \leftarrow L_1 - qL_4$, $L_2 \leftarrow L_2 - pL_4$, $L_3 \leftarrow L_3 - pL_5$, *puis un développement par rapport à la première colonne et* $L_2 \leftarrow L_2 - qL_4$). La condition cherchée est donc $4p^3 + 27q^2 = 0$.

4. Soient a et b deux nombres algébriques, soient P et Q deux polynômes non nuls de $\mathbb{Q}[X]$ tels que $P(a) = 0$ et $Q(b) = 0$. Les polynômes $P(X)$ et $Q(a + b - X)$ ont une racine commune a, donc leur déterminant de Sylvester $\mathcal{S}_X\big(P(X), Q(a + b - X)\big)$ est nul.

Posons $R(Y) = \mathcal{S}_X\big(P(X), Q(Y - X)\big)$: c'est un déterminant dont les coefficients sont des polynômes de $\mathbb{Q}[Y]$, donc $R(Y)$ est un polynôme de $\mathbb{Q}[Y]$ admettant $a + b$ pour racine. Le nombre complexe $a + b$ est donc algébrique.

Avec $a = i$ et $b = j$, on peut choisir $P = X^2 + 1$ et $Q = X^2 + X + 1$ qui sont leurs polynômes minimaux respectifs sur $\mathbb{Q}$ (si $a \in \mathbb{C}$ est algébrique, l'ensemble $\{P \in \mathbb{Q}[X] \mid P(a) = 0\}$ est un idéal non nul de $\mathbb{Q}[X]$ et le générateur normalisé de cet idéal est appelé **polynôme minimal** de a sur $\mathbb{Q}$). Un polynôme de $\mathbb{Q}[X]$ annulateur de $i + j$ est alors

$$\begin{aligned} R(Y) &= \mathcal{S}_X\big(X^2 + 1, (Y - X)^2 + (Y - X) + 1\big) \\ &= \mathcal{S}_X\big(X^2 + 1, X^2 - (2Y + 1)X + (Y^2 + Y + 1)\big) \\ &= \begin{vmatrix} 1 & 0 & Y^2 + Y + 1 & 0 \\ 0 & 1 & -(2Y + 1) & Y^2 + Y + 1 \\ 1 & 0 & 1 & -(2Y + 1) \\ 0 & 1 & 0 & 1 \end{vmatrix} = Y^4 + 2Y^3 + 5Y^2 + 4Y + 1\ . \end{aligned}$$

Montrons le caractère minimal de ce polynôme R. Supposons qu'il existe un polynôme $S \in \mathbb{Q}[Y]$, diviseur strict (normalisé) de R, tel que $S(i + j) = 0$. Un tel polynôme S ne peut être de degré 1 car on aurait alors $i + j \in \mathbb{Q}$; il ne peut être de degré 3 car on aurait alors $R = ST$ avec $T \in \mathbb{Q}[Y]$ de degré un, et le polynôme R aurait une racine rationnelle (ce n'est pas le cas car le polynôme R, par construction, admet pour racines tous les nombres que l'on peut écrire comme somme d'une racine de P et d'une racine de Q, à savoir les quatre nombres irrationnels distincts $\alpha = i + j$, $\beta = -i + j$, $\gamma = i + j^2$, $\delta = -i + j^2$ appelés **conjugués** de $i + j$ sur le corps $\mathbb{Q}$ et ces quatre nombres sont donc ses seules racines). Enfin, si S tait de degré deux, on aurait $S(Y) = (Y - \alpha)(Y - \overline{\alpha}) = \big(Y - (i + j)\big)\big(Y - (-i + j^2)\big) = Y^2 + Y + 2 + \sqrt{3}$ qui n'est pas à coefficients rationnels.

Le polynôme minimal de $\alpha = i + j$ sur $\mathbb{Q}$ est donc $R(Y) = Y^4 + 2Y^3 + 5Y^2 + 4Y + 1$.

****

Quelques compléments sur ce "déterminant de Sylvester" : on note les propriétés suivantes :

- si Q est un polynôme constant ($Q = \lambda$), alors $\mathcal{S}_X(P, Q) = \lambda^{\deg(P)}$;
- on a $\mathcal{S}_X(Q, P) = (-1)^{\deg(P)\cdot\deg(Q)}\mathcal{S}_X(P, Q)$: en effet, en reprenant les notations de la question **1.**, on voit que $\mathcal{S}_X(P, Q)$ est transformé en $\mathcal{S}_X(Q, P)$ si l'on fait opérer sur les colonnes de la

matrice la permutation $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n & n+1 & n+2 & \cdots & n+m \\ m+1 & m+2 & \cdots & m+n & 1 & 2 & \cdots & n \end{pmatrix}$ et cette permutation a pour signature $(-1)^{mn}$, on peut la décomposer en produit de mn transpositions par exemple en échangeant l'élément n successivement avec les m éléments qui le suivent, puis idem pour l'élément $n-1$, et ainsi de suite jusqu'à l'élément 1 ;

• si $m = \deg(P) \geq n = \deg(Q)$ et si R est le reste de la division euclidienne de P par Q, on a

$$\mathcal{S}_X(P,Q) = b_n^{\deg(P)-\deg(R)}\, \mathcal{S}_X(P,R)\ ;$$

en effet, notons R_1 le premier reste partiel dans la division euclidienne de P par Q (*le lecteur est vivement invité à traiter un exemple*), en effectuant sur la matrice présentée à la question **2.** les opérations sur les colonnes $C_j \leftarrow C_j - \dfrac{a_m}{b_n} C_{m+j}$ $(1 \leq j \leq n)$ et en développant par rapport à la dernière ligne $\deg(P) - \deg(R_1)$ fois, on obtient l'égalité $\mathcal{S}_X(P,Q) = b_n^{\deg(P)-\deg(R_1)}\, \mathcal{S}_X(P,R_1)$, il ne reste plus qu'à itérer.

Cela montre que l'on peut calculer le déterminant de Sylvester de deux polynômes de façon récursive (*cf. procédure ci-dessous*) et cela prouve aussi que ce déterminant de Sylvester est la même chose que le **résultant** défini dans l'exercice **5** de la semaine **1**.

Procédure de calcul récursive :

```
> result:= proc(P,Q,X):
           if (P=0) or (Q=0) then 0
               elif degree(Q,X)=0 then lcoeff(Q,X)^degree(P,X)
               else (-1)^degree(P,X)*degree(Q,X))*
                      lcoeff(Q,X)^(degree(P,X)-degree(rem(P,Q,X),X)) *
                      factor(result(Q,rem(P,Q,X),X))
           fi
   end;
```

EXERCICE 5 :

Pour toute matrice $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$, on appelle **permanent** de A le réel

$$\mathrm{per}(A) = \sum_{\sigma \in \mathcal{S}_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n}\ .$$

1. Dégager les propriétés élémentaires du permanent.

2. Théorème de Frobenius et König

Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice à coefficients positifs ou nuls. Montrer que son permanent est nul si et seulement si on peut extraire de A une matrice nulle de format $s \times (n+1-s)$, où s est un entier appartenant à $[\![1, n]\!]$.

3. Lemme des mariages :

Soient F et G deux ensembles finis, soit $\Phi : G \to \mathcal{P}(F)$ une application.

Démontrer l'équivalence des assertions **(1)** et **(2)** :

(1) : il existe une injection $\varphi : G \to F$ telle que $\forall g \in G \quad \varphi(g) \in \Phi(g)$.

(2) : $\forall\, G' \in \mathcal{P}(G) \quad \left|\bigcup_{g\in G'} \Phi(g)\right| \geq |G'|$.

Source : Jean-Marie MONIER, Algèbre Tome 2, Éditions Dunod, ISBN 2-10-000006-3

- -

1. Le permanent est une forme n-linéaire symétrique des n lignes (ou des n colonnes) de la matrice, il est donc invariant par toute permutation de lignes ou de colonnes.

On peut développer le permanent par rapport à une ligne ou une colonne : si on note A_{ij} la matrice carrée d'ordre $n-1$ obtenue en supprimant de A la i-ième ligne et la j-ième colonne, on a

$$\operatorname{per}(A) = \sum_{j=1}^{n} a_{ij} \operatorname{per}(A_{ij}) \qquad \text{pour tout} \quad i \in [\![1,n]\!] \,;$$

$$\operatorname{per}(A) = \sum_{i=1}^{n} a_{ij} \operatorname{per}(A_{ij}) \qquad \text{pour tout} \quad j \in [\![1,n]\!] \,.$$

On peut calculer des permanents par blocs : $\operatorname{per}\begin{pmatrix} A & 0 \\ C & D \end{pmatrix} = \operatorname{per}(A) \times \operatorname{per}(D)$.

Enfin, on a $\operatorname{per}({}^tA) = \operatorname{per}(A)$.

Les propriétés qui précèdent se démontrent de façon analogue aux propriétés correspondantes pour les déterminants.

Par contre, si A et B sont deux matrices carrées d'ordre n, alors $\operatorname{per}(AB) \neq \operatorname{per}(A) \times \operatorname{per}(B)$ en général, et on a même $\operatorname{per}(AB) \neq \operatorname{per}(BA)$ en général, essayer avec $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$.

2. Notons $\mathcal{M}_n^+$ l'ensemble des matrices carrées d'ordre n à coefficients positifs ou nuls.

- Soit $A \in \mathcal{M}_n^+$, supposons que l'on puisse extraire de A une matrice nulle de format $s \times (n+1-s)$ pour $s \in [\![1,n]\!]$ donné. Par des permutations de lignes et de colonnes (qui ne modifient pas le permanent), on peut transformer A en une matrice $A' = \begin{pmatrix} A_1 & 0_{s,n-s} \\ A_2 & A_3 \end{pmatrix}$, avec A_1 carrée d'ordre s ayant sa dernière colonne nulle (on en déduit le format des autres matrices) ; en développant par rapport à cette dernière colonne, on a $\operatorname{per}(A_1) = 0$, puis $\operatorname{per}(A) = \operatorname{per}(A') = \operatorname{per}(A_1) \times \operatorname{per}(A_3) = 0$.

- Pour l'implication réciproque, montrons par récurrence forte sur $n \in \mathbb{N}^*$ l'assertion

  $(\mathcal{A}_n)$: $\quad \forall A \in \mathcal{M}_n^+ \qquad \operatorname{per}(A) = 0 \implies \exists s \in [\![1,n]\!] \quad 0_{s,n+1-s}$ est extraite de A .

  ▷ pour $n = 1$, la propriété est immédiate.

▷ Soit $n \in \mathbb{N}^*$, supposons l'assertion vérifiée pour les entiers 1, 2, $\cdots$, n et soit $A \in \mathcal{M}_{n+1}^+$ telle que $\text{per}(A) = 0$ et $A \neq 0$.
Soit a_{ij} un coefficient non nul (donc strictement positif) de la matrice A, on a alors $\text{per}(A_{ij}) = 0$: en effet, en développant par rapport à la i-ième ligne, on a $0 = \text{per}(A) = \sum_{k=1}^{n} a_{ik}\,\text{per}(A_{ik})$ et, tous les termes de cette somme étant positifs, ils sont donc tous nuls.
D'après l'hypothèse de récurrence, on peut extraire de la matrice A_{ij} (donc de A) une matrice nulle de format $s \times (n+1-s)$ avec $1 \leq s \leq n$ et des permutations sur les lignes et les colonnes permettent de transformer A en une matrice $A' = \begin{pmatrix} A_1 & 0_{s,n+1-s} \\ A_2 & A_3 \end{pmatrix}$, où A_1 et A_3 sont carrées d'ordres s et $n+1-s$ respectivement, et à coefficients positifs ou nuls . On a

$$0 = \text{per}(A) = \text{per}(A') = \text{per}(A_1) \times \text{per}(A_3)\ ,$$

donc $\text{per}(A_1) = 0$ ou $\text{per}(A_3) = 0$.

Supposons $\text{per}(A_1) = 0$. En utilisant l'hypothèse de récurrence, il existe un entier t $(1 \leq t \leq s)$ tel que l'on puisse extraire de A_1 une matrice nulle de format $t \times (s+1-t)$. En effectuant des permutations de lignes et de colonnes, on place cette matrice nulle dans "le coin en haut à droite" de la matrice A_1 et, en revenant à la forme diagonale par blocs $A' = \begin{pmatrix} A_1 & 0_{s,n+1-s} \\ A_2 & A_3 \end{pmatrix}$, on voit que l'on peut extraire de A un bloc nul de format $t \times ((s+1-t)+(n+1-s))$, c'est-à-dire $t \times (n+2-t)$, c'est bien ce qu'on voulait obtenir (*raisonnement analogue si* $\text{per}(A_3) = 0$).

3. Pour interpréter la question posée, notons

$G = \{g_1, \ldots, g_m\}$ ("ensemble des garçons")

$F = \{f_1, \ldots, f_n\}$ ("ensemble des filles"}

Φ : à chaque garçon $g \in G$, on associe un ensemble de filles $\Phi(g)$;

(1) : chaque garçon $g \in G$ peut choisir une fille $\varphi(g)$ dans l'ensemble $\Phi(g)$, de telle sorte que deux garçons différents ne choisissent jamais la même fille ;

(2) : si un sous-ensemble de garçons a k éléments, la réunion des ensembles de filles dans lesquels ils peuvent choisir a au moins k éléments.

Allons-y :

- **(1)** $\Longrightarrow$ **(2)** est immédiat : si φ est une injection, on a $|\varphi(G')| = |G'|$ pour toute partie G' de G. Or, $\varphi(G') \subset \bigcup_{g \in G'} \Phi(g)$, donc $|G'| = |\varphi(G')| \leq \left| \bigcup_{g \in G'} \Phi(g) \right|$.
- **(2)** $\Longrightarrow$ **(1)** : c'est un peu plus long...

  Avec $G' = G$, on voit que $\left| \bigcup_{g \in G} \Phi(g) \right| \geq |G|$ donc, *a fortiori*, $|F| \geq |G|$ ou $n \geq m$ (il y a au

moins autant de filles que de garçons).

Construisons une matrice $A \in \mathcal{M}_n^+$ de la façon suivante :

* sur les m premières lignes, le coefficient a_{ij} $(1 \leq i \leq m,\ 1 \leq j \leq n)$ vaut 1 si le i-ième garçon peut choisir la j-ième fille, c'est-à-dire si $f_j \in \Phi(g_i)$, et vaut 0 sinon ;

* les coefficients des $n-m$ dernières lignes valent tous 1.

Le permanent de la matrice A est non nul ; en effet, si on avait $\mathrm{per}(A) = 0$, on pourrait extraire de A une matrice nulle de format $s \times (n+1-s)$ et cette matrice serait nécessairement extraite des m premières lignes (donc $s \leq m$), notons $i_1 < i_2 < \ldots < i_s$ les indices de lignes et $j_1 < j_2 < \ldots < j_{n+1-s}$ les indices de colonnes de cette matrice nulle extraite ; on aurait alors

$$\bigcup_{k=1}^{s} \Phi(g_{i_k}) \subset F \setminus \{f_{j_1}, \ldots, f_{j_{n+1-s}}\} ,$$

donc $\left|\bigcup_{k=1}^{s} \Phi(g_{i_k})\right| \leq n - (n+1-s) = s - 1 < s$, ce qui contredit l'assertion **(2)** avec $G' = \{g_{i_1}, \ldots, g_{i_s}\}$.

Donc $\mathrm{per}(A) = \sum_{\sigma \in \mathcal{S}_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n} \neq 0$, donc il existe au moins une permutation σ telle que $a_{\sigma(i),i} \neq 0$ pour tout $i \in [\![1, n]\!]$. Ainsi, pour tout $i \in [\![1, m]\!]$, on a $a_{i,\sigma^{-1}(i)} \neq 0$ et $f_{\sigma^{-1}(i)} \in \Phi(g_i)$. L'application $\varphi : G \to F$, $g_i \mapsto f_{\sigma^{-1}(i)}$ $(1 \leq i \leq m)$ vérifie les conditions de l'assertion **(1)**.

EXERCICE 6 :

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geq 1$.

Un élément τ de $\mathcal{L}(E)$ est une **transvection** s'il existe un hyperplan H tel que

$$\tau\big|_H = \mathrm{id}_H \qquad \text{et} \qquad \mathrm{Im}(\tau - \mathrm{id}_E) \subset H ,$$

c'est-à-dire $\mathrm{Im}(\tau - \mathrm{id}_E) \subset H \subset \mathrm{Ker}(\tau - \mathrm{id}_E)$.

On note $\mathrm{SL}(E) = \{u \in \mathrm{GL}(E) \mid \det u = 1\}$ le **groupe spécial linéaire** de E.

1. Montrer que $\tau \in \mathcal{L}(E)$ est une transvection si et seulement si

$$\exists \varphi \in E^* \quad \exists a \in \mathrm{Ker}\,\varphi \quad \forall x \in E \qquad \tau(x) = x + \varphi(x)\, a .$$

2. Dans cette question, on suppose $\dim E \geq 2$. Soient x et y deux vecteurs non nuls de E. Montrer qu'il existe τ, transvection ou produit de deux transvections, tel que $\tau(x) = y$.

3. Soit x un vecteur non nul de E, soient H_1 et H_2 deux hyperplans distincts tels que $x \notin H_1 \cup H_2$. Montrer qu'il existe une transvection τ telle que

$$\tau(x) = x \qquad \text{et} \qquad \tau(H_1) = H_2 .$$

4. En déduire que le groupe $\mathrm{SL}(E)$ est engendré par les transvections.

Source : Daniel PERRIN, Cours d'Algèbre, Éditions Ellipses, ISBN 2-7298-5552-1

- -

1. Soit τ une transvection.

- Si $\tau = \mathrm{id}_E$, on peut choisir $\varphi = 0$ et $a \in E$ quelconque.
- Si $\tau \neq \mathrm{id}_E$, alors $\mathrm{Ker}(\tau - \mathrm{id}_E)$ est un hyperplan H, et $\mathrm{Im}(\tau - \mathrm{id}_E)$ est une droite vectorielle D contenue dans H, soit a un vecteur directeur de D. Pour tout x de E, notons $\varphi(x)$ l'unique scalaire tel que $\tau(x) - x = \varphi(x)a$. L'application $\varphi : E \to \mathbb{K}$ est une forme linéaire de noyau H, donc $a \in \mathrm{Ker}\,\varphi$.

Réciproquement, soit τ un endomorphisme de E tel que $\tau(x) = x + \varphi(x)a$, avec φ forme linéaire sur E et $a \in \mathrm{Ker}\,\varphi$.

- si $a = 0$ ou $\varphi = 0$, alors $\tau = \mathrm{id}_E$: c'est une transvection ;
- sinon, $H = \mathrm{Ker}\,\varphi$ est un hyperplan, on a bien $\forall x \in H \quad \tau(x) = x$ et

$$\forall x \in E \qquad \tau(x) - x = \varphi(x)a \in H \ ,$$

donc τ est une transvection "d'hyperplan H".

2. Supposons d'abord x et y non colinéaires, soit $a = y - x$ ($a \neq 0$), soit H un hyperplan vectoriel contenant a mais pas x. Soit φ **la** forme linéaire sur E nulle sur H et telle que $\varphi(x) = 1$. La transvection $\tau : v \mapsto v + \varphi(v)a$ envoie x sur y.

Si x et y sont colinéaires, puisque $\dim E \geq 2$, il suffit de "transiter" par un vecteur z non colinéaire à x et y pour trouver un produit de deux transvections qui envoie x sur y.

3. Le sous-espace $F = H_1 \cap H_2$ est de dimension $n-2$, considérons l'hyperplan $H = F \oplus \mathbb{K}x$. Soient D_1 et D_2 des droites telles que $H_1 = F \oplus D_1$ et $H_2 = F \oplus D_2$. On peut choisir des vecteurs directeurs x_1 et x_2 de D_1 et D_2 respectivement, de façon que $x_1 - x_2 \in H$: en effet, $(D_1 \oplus D_2) \cap H \neq \{0\}$ pour des raisons de dimensions.

Soit enfin τ l'unique endomorphisme de E tel que $\tau\big|_H = \mathrm{id}_H$ et $\tau(x_1) = x_2$ (on a $x_1 \notin H$ car, sinon, on aurait aussi $x_2 \in H$, puis $H_1 \subset H$, $H_2 \subset H$ et finalement $H_1 = H_2 = H$ absurde). On vérifie immédiatement que $\mathrm{Im}(\tau - \mathrm{id}_E) \subset H$, donc τ est bien une transvection "d'hyperplan H". Enfin, $\tau(x) = x$ puisque $x \in H$ et, comme $\tau\big|_F = \mathrm{id}_F$ et $\tau(x_1) = x_2$, on a $\tau(H_1) = H_2$.

Il existe donc une transvection laissant stable x et envoyant H_1 sur H_2.

4. Vérifions d'abord que les transvections appatiennent à $\mathrm{SL}(E)$: pour $\tau = \mathrm{id}_E$, c'est immédiat, sinon si $\tau : x \mapsto x + \varphi(x)a$ avec $a \in H = \mathrm{Ker}\,\varphi$, construisons une base $\mathcal{B} = (e_1, \cdots, e_{n-1}, e_n)$ de E avec $e_{n-1} = a$, $(e_1, \cdots, e_{n-1})$ base de H et $\varphi(e_n) = 1$, alors $M_{\mathcal{B}}(\tau) = I_n + E_{n-1,n}$ a pour déterminant 1.

Démontrons le lemme suivant :

Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \geq 2$, soit $u \in \mathrm{SL}(E)$. Soit H un hyperplan de E, soit $x \in E \setminus H$. Alors il existe un élément v de $\mathrm{SL}(E)$ vérifiant $v(H) = H$ et $v(x) = x$ et tel que $u = \sigma v$ où σ est composé d'un nombre fini de transvections.

Preuve du lemme : D'après la question **2.**, il existe τ (transvection, ou produit de deux transvections) tel que $\tau(x) = u(x)$, c'est-à-dire $\tau^{-1}u(x) = x$.

Soit l'hyperplan $H' = \tau^{-1}u(H)$:

▷ si $H' = H$, on prend $v = \tau^{-1}u$;

▷ si $H' \neq H$, on a $x \notin H \cup H'$, il existe donc (question **3.**) une transvection μ telle que $\mu(x) = x$ et $\mu(H) = H'$ et $v = \mu^{-1}\tau^{-1}u$ répond à la question (*fin de la preuve du lemme*).

On montre alors que les transvections engendrent le groupe $\mathrm{SL}(E)$ par récurrence sur $n = \dim(E)$:

- pour $n = 1$, c'est clair puisque la seule transvection est id_E et $\mathrm{SL}(E) = \{\mathrm{id}_E\}$;
- soit $n \geq 2$, supposons l'assertion vraie au rang $n-1$, soit E de dimension n, soit $u \in \mathrm{SL}(E)$. Soit H un hyperplan de E, soit $x \in E \setminus H$ (alors $E = H \oplus (\mathbb{K}x)$), on écrit $u = \sigma_0 v$, où σ_0 est un produit de transvections de E, et $v \in \mathrm{SL}(E)$ laisse stables H et x (*lemme*). On vérifie alors que $v\big|_H \in \mathrm{SL}(H)$ (*écrire la matrice de v dans une base adaptée à la décomposition $E = H \oplus (\mathbb{K}x)$*), l'hypothèse de récurrence permet d'écrire $v\big|_H = \tau_1 \cdots \tau_k$, où les τ_i $(1 \leq i \leq k)$ sont des transvections de H ; on a alors $v = \sigma_1 \cdots \sigma_k$, où chaque σ_i est l'endomorphisme de E défini par $\sigma_i\big|_H = \tau_i$ et $\sigma_i(x) = x$ (on vérifie facilement que σ_i est une transvection de E). Finalement, $u = \sigma_0\sigma_1 \cdots \sigma_k$ est un produit de transvections.