Déterminants

Marc SAGE

9 août 2008

Table des matières

Comme dans la feuille sur les matrices, on notera M_n au lieu de $M_n(K)$ lorsque le corps de base ne jouera aucun rôle.

Le déterminant d'une matrice A pourra être noté $|A|$, avec l'avantageuse propriété $|AB| = |A|\,|B|$.

Les trois premiers exercices sont essentiellement destinés à vérifier que la construction et les principales propriétés du déterminant sont maîtrisées.

1 Quid des formes n-linéaires alternées ?

1. *À une matrice A de M_n on associe une application*

$$f_A : \left\{ \begin{array}{ccc} M_n & \longrightarrow & K \\ (C_1 \mid \cdots \mid C_n) & \longmapsto & \sum_{j=1}^{n} \det(C_1 \mid \cdots \mid C_{j-1} \mid AC_j \mid C_{j+1} \mid \cdots \mid C_n) \end{array} \right.$$

où les C_i désignent les colonnes de la matrice $(C_1 \mid \cdots \mid C_n)$. Montrer que

$$f_A = (\operatorname{tr} A) \det .$$

2. **Une application.**

On considère l'équation différentielle $X' = AX$ où I est un intervalle de $\mathbb{R}$, A une application continue[1] *$I \longrightarrow M_n(\mathbb{R})$ et l'inconnue X est une application dérivable $I \longrightarrow \mathbb{R}^n$. Calculer $w_{\overrightarrow{X}} := \det(X_1(t), ..., X_n(t))$ où les X_i sont n solutions de l'équation $X' = AX$. Commenter.*

Solution proposée.

1. Montrons dans un premier temps que f_A et det sont colinéaires, on calculera ensuite le coefficient de colinéarité en évaluant en l'identité. Il s'agit donc de prouver que f_A est une forme n-linéaire alternée (en les colonnes de la variable). Le caractère n-linéaire est évident car A est linéaire et det est n-linéaire. Pour le côté alterné, prenons deux colonnes C_i et C_j égales (avec $i < j$), et regardons

$$f_A(\cdots \mid C_i \mid \cdots \mid C_j \mid \cdots) = \sum_{k=1}^{n} \det(\cdots \mid C_{k-1} \mid AC_k \mid C_{k+1} \mid \cdots).$$

Pour k différent de i et j, la colonne commune apparaît deux fois dans le déterminant de droite, ce qui donne 0 par alternance de det. Il reste donc à calculer la somme des deux termes restants. On utilise pour cela l'antisymétrie de det quand on intervertit les i-ième et j-ième colonnes du second terme :

$$\begin{array}{rl} & \det(\cdots \mid C_{i-1} \mid AC_i \mid C_{i+1} \mid \cdots \mid C_{j-1} \mid C_j \mid C_{j+1} \mid \cdots) \\ & + \det(\cdots \mid C_{i-1} \mid C_i \mid C_{i+1} \mid \cdots \mid C_{j-1} \mid AC_j \mid C_{j+1} \mid \cdots) \\ = & \det(\cdots \mid C_{i-1} \mid AC_i \mid C_{i+1} \mid \cdots \mid C_{j-1} \mid C_j \mid C_{j+1} \mid \cdots) \\ & - \det\left(\cdots \mid C_{i-1} \mid \underbrace{AC_j}_{=AC_i} \mid C_{i+1} \mid \cdots \mid C_{j-1} \mid \underbrace{C_i}_{C_j} \mid C_{j+1} \mid \cdots\right) \\ = & 0. \end{array}$$

On a donc montré que $f_A = \lambda \det$ pour un certain scalaire λ. Il reste à trouver λ en évaluant f_A en une matrice particulière pertinente, par exemple l'identité. En notant E_j et A_j les j-ièmes colonnes de l'identité et de la matrice A, on a clairement $AE_j = A_j$, d'où

$$\det(\cdots \mid E_{j-1} \mid AE_j \mid E_{j+1} \mid \cdots) = \begin{vmatrix} \ddots & & \vdots & & \\ & 1 & a_{j-1,j} & & \\ & & a_{j,j} & & \\ & & a_{j+1,j} & 1 & \\ & & \vdots & & \ddots \end{vmatrix} = a_{j,j}$$

[1] Une fonction de $\mathbb{R}$ dans $M_n(\mathbb{R})$ sera dite *continue* si chacune de ses fonctions coordonnées est continue.

en développant selon la j-ième ligne. Il en résulte

$$\lambda = \lambda \det I_n = f_A(I_n) = \sum_{j=1}^{n} \det(\cdots \mid E_{j-1} \mid AE_j \mid E_{j+1} \mid \cdots) = \sum_{j=1}^{n} a_{j,j} = \operatorname{tr} A,\ CQFD.$$

2. Pour utiliser les données $X_i' = AX_i$, on dérive w. Le déterminant étant multilinéaire, on trouve

$$w' = \sum \det(..., X_{i-1}, X_i', X_{i+1}, ...) = \sum \det(..., X_{i-1}, AX_i, X_{i+1}, ...).$$

La première question permet d'obtenir $w' = (\operatorname{tr} A)\, w$, d'où pour tout $t_0 \in I$

$$w = w(t_0) \exp\left(\int_{t_0}^{\cdot} \operatorname{tr} A\right).$$

En particulier, on voit que ou bien w est nul ou bien w ne s'annule jamais. Ainsi, pour tester la liberté d'une famille de n solutions, il suffit de tester la liberté de la famille évaluée en un point arbitraire.

2 Inverses et polynômes

Soit $P : \mathbb{C} \longrightarrow GL_n(\mathbb{C})$ une application dont toutes les composantes sont polynomiales. Montrer que $z \mapsto P(z)^{-1}$ est aussi polynomiale en chacune de ses composantes.

Le résultat reste-t-il si l'on prive le domaine **C** de départ d'un point ?

Solution proposée.

On connaît une formule pour l'inverse : $A^{-1} = \frac{1}{|A|}\ {}^t\operatorname{com} A$. Les cofacteurs étant des déterminants (donc des polynômes) en les coefficients de A, l'application $z \mapsto {}^t\operatorname{com} P(z)$ est bien polynomiale. Pour se débarasser du déterminant, il suffit de dire que $\det \circ P$ est un polynôme en z qui ne s'annule jamais (P est à image dans GL_n !) sur $\mathbb{C}$ tout entier, c'est donc une constante par D'Alembert-Gauss. Ploum.

Soit a un complexe hors du domaine de départ. L'application $\lambda \mapsto (\lambda - a) I_n$ vérifie alors les hypothèses de l'énoncé mais pas la conclusion, donc on ne peut pas remplacer le domaine de départ par un ensemble plus petit.

3 Formule de Miller pour calculer un déterminant (ou comment illustrer une idée géniale)

1. *Soit A une matrice de $M_n(K)$ telle que $a_{1,1} \neq 0$. Montrer que*

$$\det A = \frac{1}{a_{1,1}^{n-2}} \det\left(\begin{vmatrix} a_{1,1} & a_{1,j} \\ a_{i,1} & a_{i,j} \end{vmatrix}_{i,j=2,\ldots,n}\right).$$

2. *En déduire que le déterminant d'une matrice de taille n à coefficients dans $\{-1, 1\}$ est divisible par 2^{n-1}.*

Solution proposée.

1. Notons $C_j = \left(\begin{vmatrix} a_{1,1} & a_{1,j} \\ a_{i,1} & a_{i,j} \end{vmatrix}\right)_{i=2,\ldots,n}$ la j-ième colonne du terme de droite et A_j la j-ième colonne de A privée de sa première ligne. On remarque que

$$\frac{1}{a_{1,1}} C_j = A_j - \frac{a_{1,j}}{a_{1,1}} A_1 :$$

en effet, il suffit d'écrire $\frac{1}{a_{1,1}}\begin{vmatrix} a_{1,1} & a_{1,j} \\ a_{i,1} & a_{i,j} \end{vmatrix} = a_{i,j} - \frac{a_{1,j}}{a_{1,1}}a_{i,1}$ pour tout $i = 2, ..., n$. On en déduit

$$\frac{1}{a_{1,1}^{n-2}} \det(C_2 \mid \cdots \mid C_n) = a_{1,1} \det\left(\frac{C_2}{a_{1,1}} \mid \cdots \mid \frac{C_n}{a_{1,1}}\right) = a_{1,1} \det\left(A_j - \frac{a_{1,j}}{a_{1,1}}A_1\right)_{j=2,\ldots,n}.$$

Pour calculer ce déterminant, on aimerait bien pouvoir faire des opérations sur les colonnes pour faire sauter le A_1 qui apparaît partout. Mais A_1 n'apparaît pas toute seule... Qu'à cela tienne, on la fait apparaître en incrémentant le taille de la matrice ! (c'est ça, l'idée géniale, merci à Bruno Le Floch) :

$$\begin{aligned} \det\left(A_j - \frac{a_{1,j}}{a_{1,1}}A_1\right)_{j=2,\ldots,n} &= \det\begin{pmatrix} 1 & (0) \\ A_1 & \left(A_j - \frac{a_{1,j}}{a_{1,1}}A_1\right)_{j=2,\ldots,n} \end{pmatrix} = \det\begin{pmatrix} 1 & \left(\frac{a_{1,j}}{a_{1,1}}\right) \\ A_1 & (A_j) \end{pmatrix} \\ &= \frac{1}{a_{1,1}} \det\begin{pmatrix} a_{1,1} & (a_{1,j}) \\ A_1 & (A_j) \end{pmatrix} = \frac{1}{a_{1,1}} \det A, \ \textit{CQFD.} \end{aligned}$$

2. Soit A une matrice à coefficients dans $\{-1, 1\}$. Les petits déterminants $\begin{vmatrix} a_{1,1} & a_{1,j} \\ a_{i,1} & a_{i,j} \end{vmatrix}$ sont donc tous pairs en tant que différences de produits d'impairs. Ainsi, d'après la formule de Miller, $\det A$ vaut (à un coefficient $\frac{1}{a_{1,1}^{n-2}} = \pm 1$ près) le déterminant d'une matrice de taille $(n-1)^2$ dont tous les coefficients sont pairs : factoriser chacune des $n-1$ colonnes par 2 fait sortir un facteur 2^{n-1} devant un déterminant qui reste entier (car à coefficients entiers), ce qui conclut.

Remarque. Cette formule a un grand avantage sur le développement selon une ligne ou une colonne. D'une part, sa complexité est moindre : on calcule

$$\sum_{i=1}^{n-1} i^2 = \frac{n(n-1)(2n-1)}{6} \leq \frac{n^3}{3}$$

déterminants d'ordre 2 au lieu de $n!$. D'autre part, calculer un déterminant de la sorte est bien plus agréable à faire et à présenter que d'écrire les n cofacteurs de la ligne/colonne par rapport à laquelle on développe (pour le cas général, bien sûr...).

4 Le déterminant n'est *pas* linéaire

1. *Trouver toutes les matrices A de M_n telles que*

$$\forall M \in M_n, \ \det(A + M) = \det A + \det M.$$

2. *En déduire que si $\det(A + M) = \det(B + M)$ pour toute matrice M, alors $A = B$.*

Solution proposée.

1. En réduisant $A = PJ_rQ$, on paramétrise naturellement M_n par $M = PNQ$ où N décrit M_n, de sorte que notre hypothèse de travail est équivalente à

$$\begin{aligned} &\det[P(J_r + N)Q] = \\ &\det(PJ_rQ) + \det(PNQ) \\ \iff &\det(J_r + N) = \\ &\det J_r + \det N. \end{aligned}$$

On vient donc de réduire le problème[2] aux J_r.

Le problème n'a guère d'intérêt pour $n = 1$: l'égalité ci-dessus est en effet alors toujours vérifiée. On supposera donc $n \geq 2$.

[2] Comme quoi ce procédé à l'apparence sthûssieuse sert vraiment : il faut y penser dans ce genre de problème matriciels très « bidouillatoires ».

En prenant $M = A$, on obtient

$$2^n |A| = 2 |A|,$$

d'où $|A| = 0$. En prenant ensuite $N = I_n$, on obtient

$$2^r = 1,$$

ce qui impose $r = 0$. La seule matrice pouvant convenir est donc $A = 0$.

Ce qui précède utilise implicitement la nullité de la caractéristique, hypothèse dont on peut se débarasser : prendre $N = \mathrm{Diag}(-1, 0, 0, ..., 0)$ donne $0 = \delta_r^n + 0$, d'où $r < n$, puis prendre $N := 1 - J_r$ donne $1 = 0 + \delta_{n-r}^n$, d'où $r = 0$.

2. Pour le corollaire, on pose $M = N - A$, ce qui impose pour toute matrice N

$$\det N = \det(C + N) \text{ avec } C := B - A.$$

Faire $N = 0$ montre que $\det C = 0$, ce qui permet de réécrire nous hypothèse sous la forme

$$\det(C + N) = \det C + \det N$$

de la première question. On en déduit $C = 0$, *i. e.* $A = B$.

5 Des déterminants positifs

Soit A et B deux matrices réelles qui commutent.

1. *Donner une CNS sur* $\det(A + B)$ *pour avoir* $\det(A^p + B^p) \geq 0$ *pour tout entier* $p \geq 1$.
2. *Peut-on modifier garder cette CNS en remplaçant* ≥ 0 *par* > 0 *?*

1. Faire $p = 1$ donne une condition nécessaire simple : $|A + B| \geq 0$.

Pour $p = 2$, on peut factoriser $A^2 + B^2 = (A + iB)(A - iB)$ car A et B commutent, d'où en prenant le déterminant

$$\left|A^2 + B^2\right| = |A + iB| \, |A - iB| \overset{A \text{ et } B \text{ réelles}}{=} |A + iB| \, \overline{|A + iB|} = |\det(A + iB)|^2 \geq 0.$$

Ceci montre d'ailleurs que $|A^p + B^p| \geq 0$ dès que p est pair (remplacer A et B par leurs puissances p-ièmes)

Pour p impair quelconque, on peut factoriser $|A^p + B^p|$ et regarder les déterminants qui sont deux à deux conjugués. En se plaçant dans le corps $\mathbb{R}(X, Y)$, en notant $\omega := e^{\frac{\pi i}{p}}$, on a

$$X^p + Y^p = X^p - (\omega Y)^p = (\omega Y)^p \left(\left(\frac{X}{\omega Y}\right)^p - 1\right) = (\omega Y)^p \prod_{0 \leq k < p} \left(\frac{X}{\omega Y} - \omega^{2k}\right) = \prod_{0 \leq k < p} \left(X - \omega^{2k+1} Y\right),$$

d'où la même factorisation[3] en spécialisant X en A et Y en B. En regroupant les facteurs deux par deux selon

$$\begin{array}{ccccccc} A - \omega B & & A - \omega^3 B & & A - \omega^5 B & \cdots & A - \omega^{p-2} B \\ A - \omega^{2p-1} B & & A - \omega^{2p-3} B & & A - \omega^{2p-5} B & \cdots & A - \omega^{p+2} B \end{array} \quad \underbrace{A - \omega^p B}_{= A + B}$$

puis en observant que A et B sont réelles et que $\overline{\omega} = \omega^{-1}$, on voit que chaque colonne correspond à deux (matrices) complexes conjugées. Il en résulte que $|A^p + B^p|$ est du signe de $|A + B|$, ce qui montre que la condition $|A + B| \geq 0$ est suffisante.

2. Il est faux de dire

$$|A + B| > 0 \implies (\forall p \geq 2, \ |A^p + B^p| > 0).$$

Prenons des matrices A et B diagonales pour simplifier[4]. Pour nier la conclusion, il suffit que l'un des facteurs $a_{i,i} - \omega^{2k+1} b_{i,i}$ soit nul. Pour avoir en outre la prémisse, on peut prendre $A = \begin{pmatrix} \omega & \\ & \overline{\omega} \end{pmatrix}$ et $B = \mathrm{Id}$; il vient alors (pour $p \geq 2$)

$$|A + B| = |1 + \omega|^2 > 0 \text{ et } A^p + B^p = 0.$$

[3] évidemment valable pour tout $p \geq 1$ sans condition de parité

[4] Comme l'on va raisonner uniquement sur les valeurs propres, cela n'a en fait rien de restrictif.

Mais il faut quand même que A soit réelle ; il suffit de la remplacer par une matrice de même polynôme caractéristique[5] $X^2+\omega^2$, par exemple sa matrice compagnon $\begin{pmatrix} 0 & \omega^2 \\ 1 & 0 \end{pmatrix}$.

6 Application du caractère polynomial du déterminant

1. *Soient A et B deux matrices réelles semblables dans $M_n(\mathbb{C})$. Montrer qu'en fait A et B sont semblables dans $M_n(\mathbb{R})$.*
2. *Généraliser le résultat en considérant une extension[6] $\mathbb{R} \hookrightarrow K$ de dimension finie[7] sur $\mathbb{R}$, puis de dimension quelconque.*
3. *Que se passe-t-il si l'on remplace $\mathbb{R}$ par un corps infini ?*

Solution proposée.

1. Soit P une matrice complexe inversible telle que $B = PAP^{-1}$. En décomposant P selon parties réelle et imaginaire, disons $P = R+iS$ avec R et S réelles, on obtient (en identifiant parties réelle et imaginaire)

$$PA = BP \implies RA + iSA = BR + iBS \implies \begin{cases} RA = BR \\ SA = BS \end{cases} \implies \forall t \in \mathbb{R},\ (R+tS)A = B(R+tS).$$

Il s'agit maintenant de trouver un t tel que $R+tS$ soit inversible. Or, l'application $t \mapsto \det(R+tS)$ est polynomiale sur $\mathbb{C}$, non nulle puisque $\det(R+iS) = \det P \neq 0$ (P est inversible !), donc n'admet qu'un nombre fini de racines. N'importe quel réel t en dehors de ces racines fera alors l'affaire.

2. Soit maintenant K une extension de $\mathbb{R}$ de dimension finie $d \geq 1$. Considérons deux matrices réelles A et B semblables dans $M_n(K)$, disons $PA = BP$ avec P inversible. Tout comme l'on avait décomposé une matrice complexe sur la $\mathbb{R}$-base $(1, i)$ de $\mathbb{C}$, décomposons P sur une $\mathbb{R}$-base $(e_1, ..., e_d)$ de K : $P = \sum_{i=1}^{d} e_i P_i$ où les P_i sont réelles. On en déduit comme dans le cas complexe

$$\forall t \in \mathbb{R},\ \left(tP_1 + \sum_{i=2}^{d} e_i P_i\right) A = B \left(tP_1 + \sum_{i=2}^{d} e_i P_i\right).$$

En copiant l'argument déjà évoqué, l'application $t \mapsto \det\left(tP_1 + \sum_{i=2}^{d} e_i P_i\right)$ est polynomiale sur K, non nulle car en $t = e_1$ on obtient $\det P \neq 0$, donc n'admet qu'un nombre fini de racines. En prenant un réel t_1 en dehors de ces racines, on peut recommencer : l'application $t \mapsto \det\left(t_1P_1 + tP_2 + \sum_{i=3}^{d} e_i P_i\right)$ est polynomiale sur K et non nulle pour $t = e_2$, donc on peut choisir un réel t_2 hors de ses racines. Ainsi de suite, on aboutit à une matrice réelle inversible $t_1P_1 + tP_2 + \cdots + t_dP_d$ qui rend A et B semblables.

Si K n'est plus supposé de dimension finie sur $\mathbb{R}$, le résultat reste valable. En effet, si $PA = BP$ dans $M_n(K)$, on regarde le $\mathbb{R}$-espace vectoriel E engendré par les coefficients de P, qui est – par construction – de dimension finie sur $\mathbb{R}$. On procède comme au point précédent en décomposant $P = \sum_{i=1}^{n} e_i P_i$ sur une $\mathbb{R}$-base de E puis en introduisant les applications $t \mapsto \det\left(tP_1 + \sum_{i=2}^{d} e_i P_i\right)$.

3. Si l'on dispose d'une extension $k \hookrightarrow K$ quelconque où k est un corps infini, tout marche pareil, le caractère infini de k permettant de choisir un scalaire hors des racines de nos polynômes déterminants.

Remarque. Si l'on remplace $\mathbb{R}$ par un corps fini, le résultat reste valable, mais il semble difficile d'en donner une preuve directe sans utiliser les invariants de similitude (qui trivialisent l'exercice quel que soit le corps de base, *cf.* cours sur la réduction de Frobenius).

[5] $X^2+\omega^2$ étant scindé simple dans $\mathbb{C}$, la nouvelle matrice A sera alors diagonalisable et les calculs précédents maintenus.

[6] Une *extension* d'un corps K est la donnée d'un morphisme de corps $K \hookrightarrow L$. Un tel morphisme est toujours injectif, ce qui permet de voir K comme un sous-corps de L. Une extension de K doit donc être vue comme un sur-corps de K.

[7] Une extension $K \hookrightarrow L$ est automatiquement munie d'une structure de K-ev. Si ce dernier est de dimension finie n, on dit que L est une extension *finie* sur K de degré n. Par exemple, $\mathbb{R} \hookrightarrow \mathbb{C}$ est une extension finie de degré 2.

7 Déterminants par blocs : deux idées à retenir

Soit A, B, C, D quatre matrices carrées.

1. *Montrer que, si A ou D est inversible et commute avec C, on peut écrire*

$$\begin{vmatrix} A & B \\ C & D \end{vmatrix} = \det(AD - BC).$$

On cherchera à multiplier la grosse matrice pour obtenir une matrice triangulaire par blocs.

2. *La formule reste-elle valable si A et D ne sont plus supposées inversibles ?*
3. *Et si C ne veut plus commuter avec personne ?*

Solution proposée

1. Une idée est de faire apparaître $AD - BC$ sur la diagonale, ce qui peut se faire en écrivant

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} D & ? \\ -C & ? \end{pmatrix} = \begin{pmatrix} AD - BC & ? \\ CD - DC & ? \end{pmatrix} \text{ (parfait si } C \text{ et } D \text{ commutent).}$$

Pour que le détérminant $\begin{vmatrix} D & ? \\ -C & ? \end{vmatrix}$ soit aisé à calculer, on peut compléter sur la diagonale avec D^{-1} (tiens, une hypothèse non utilisée) et un 0 ailleurs :

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} D & \\ -C & D^{-1} \end{pmatrix} = \begin{pmatrix} AD - BC & ? \\ & I \end{pmatrix}.$$

Il reste à prendre les déterminants pour conclure.

Si c'est A qui commute avec C et qui est inversible, on s'y prend presque pareil :

$$\begin{pmatrix} A^{-1} & \\ C & -A \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} I & ? \\ & BC - AD \end{pmatrix}.$$

2. Il y a une bonne idée qui permet de rendre n'importe quelle matrice (carrée) inversible. On remplace tous ses coefficients par des inderminées $X_{i,j}$; le déterminant alors obtenu est un polynôme non nul[8], donc un scalaire non nul du corps $K(X_{i,j})$, donc notre matrice est inversible dans $M_n(K(X_{i,j}))$, donc notre formule est valide dans le corps $K(X_{i,j})$. Il reste ensuite à remplacer les indéterminées par les valeurs de notre matrice de départ.
3. Sans l'hypothèse de commutativité, la formule tombe. En cherchant un exemple avec beaucoup de 0, on peut trouver (entres autres...) la matrice $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. Son déterminant est nul à cause de la ligne de 0 en bas, mais pourtant on a

$$\det\left[\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right] = \det\left[\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right] = -1.$$

Remarque. La règle de Sarrus se généralise aisément à une matrice de matrices qui commutent toutes deux à deux.

???? À rédiger : pour montrer la formule, vérifier qu'elle est blinéaire alternée en (A, C) et (B, D) ????

[8] il prend en effet un valeur non nulle en l'identité

8 Déterminant de Smith : une idée à connaître

En notant $d_{i,j}$ le nombre de diviseurs communs à i et j et $\delta_{i,j}$ le pgcd de i et j, calculer les déterminants des matrices $(d_{i,j})_{i,j=1,...,n}$ et $(\delta_{i,j})_{i,j=1,...,n}$.

Solution proposée.

L'idée est d'écrire la matrice concernée comme un produit de deux matrices dont le déterminant est plus ou moins trivial à calculer.

On peut toujours écrire

$$d_{i,j} = \sum_{\substack{k|i\\k|j}} 1 = \sum_{k=1}^{n} a_{i,k}a_{j,k} = \sum_{k=1}^{n} [A]_{i,k} \left[{}^tA\right]_{k,j} = \left[A\ {}^tA\right]_{i,j} \text{ où } a_{p,q} = \begin{cases} 1 \text{ si } q \mid p \\ 0 \text{ sinon} \end{cases}.$$

La matrice A étant triangulaire, son déterminant est le produit de ses coefficients diagonaux, d'où $\det A = 1$, qui est du coup la valeur du déterminant cherché.

De même, en se souvenant miraculeusement de l'identité $n = \sum_{d|n} \varphi(d)$, on écrit

$$\delta_{i,j} = i \wedge j = \sum_{k|i\wedge j} \varphi(k) = \sum_{\substack{k|i\\k|j}} \varphi(k) = \sum_{k=1}^{n} [\Phi]_{i,k} \left[{}^tA\right]_{k,j} = \left[\Phi\ {}^tA\right]_{i,j} \text{ où } [\Phi]_{p,q} = \begin{cases} \varphi(q) \text{ si } q \mid p \\ 0 \text{ sinon} \end{cases}.$$

La matrice Φ étant triangulaire, le déterminant cherché vaut $\prod_{k=1}^{n} \varphi(k)$.

Remarque. Recourir à l'identité $n = \sum_{d|n} \varphi(d)$ n'est pas si astucieux que ça. En effet, ce qui compte était d'exprimer $i \wedge j$ comme une somme sur plusieurs conditions (dans notre cas $k \mid i$ et $k \mid j$) et d'introduire les matrices correspondantes à ces conditions en priant pour qu'elles soient « gentilles ». En ce sens, l'indicatrice d'Euler ne joue aucun rôle particulier.

9 Déterminant d'Hurwitz : une autre idée à retenir

Soit $a, b, x_1, ..., x_{n\geq 1}$ des scalaires sur un corps K. On veut évaluer

$$D_{a,b} = \begin{vmatrix} x_1 & a & \cdots & \cdots & a \\ b & x_2 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & x_{n-1} & a \\ b & \cdots & \cdots & b & x_n \end{vmatrix}.$$

On posera $P := \prod_{i=1}^{n} (x_i - X)$.

1. *On suppose dans un premier temps $a \neq b$. En rajoutant un x à chaque coordonnée, considérer D comme un polynôme en x de degré 1 et montrer que*

$$D_{a\neq b} = \frac{bP(a) - aP(b)}{b-a}.$$

2. *Dans le cas $a = b$, remplacer b par une indéterminée X et appliquer le premier cas en se plaçant dans le corps $K(X)$ pour obtenir*

$$\begin{aligned} D_{a,a} &= P(a) - aP'(a) \\ &= \prod_{i=1}^{n} (x_i - a) + a \sum_{i=1}^{n} \prod_{j\neq i} (x_j - a) \\ &= P(a) \left(1 - \sum \frac{a}{x_i - a}\right) \text{ (si } x_i \neq a\ \forall i). \end{aligned}$$

Solution proposée.

1. En rajoutant un x à chaque coefficient, on voit, par multilinéarité et alternance, ou en développant selon la première ligne L_1 après avoir effectué les opérations $L_i \longleftarrow L_i - L_1$, que $D(x)$ est un polynôme $\alpha x + \beta$ de degré au plus 1. On veut la valeur de $D(0) = \beta$. Or, on connaît

$$\begin{cases} -\alpha a + \beta = D(-a) = \prod_{i=1}^{n} (x_i - a) \\ -b\alpha + \beta = D(-b) = \prod_{i=1}^{n} (x_i - b) \end{cases} \quad \text{(matrices triangulaires)},$$

d'où $b\beta - a\beta = b\prod_{i=1}^{n}(x_i - a) - a\prod_{i=1}^{n}(x_i - b)$, et en introduisant le polynôme on trouve

$$D = \frac{bP(a) - aP(b)}{b - a}.$$

2. Remplaçons à présent b par X. Puisque $a \neq X$ dans $K(X)$, ce qui précède s'applique :

$$D(X) = \frac{XP(a) - aP(X)}{X - a} = P(a) + P(X) - \frac{XP(X) - aP(a)}{X - a}.$$

Or, la formule de Taylor appliquée au polynôme XP au point a montre que

$$\left[\frac{XP(X) - aP(a)}{X - a}\right](a) = (XP)'(a) = P(a) + aP'(a).$$

On en déduit la valeur de D dans le cas $a = b$:

$$D = 2P(a) - (P(a) + aP'(a)) = P(a) - aP'(a).$$

10 Combinatoire et matrice d'incidence

Soit $A_1, ..., A_p$ des parties distinctes de $\{1, ..., n\}$ telles que l'intersection de deux quelconques distinctes d'entres elles soit de cardinal $c \geq 1$ fixé. Montrer que $p \leq n$.

On pourra introduire la matrice d'incidence A définie par $a_{i,j} = \begin{cases} 1 \text{ si } i \in A_j \\ 0 \text{ si } i \notin A_j \end{cases}$ et s'intéresser à la matrice carrée ${}^tAA$.

Solution proposée.

Notons que A est de taille $n \times p$. Calculons les coefficients de $B := {}^tAA$, qui est de taille $p \times p$:

$$b_{i,j} = \sum_{k=1}^{n} a_{k,i}a_{k,j} = \sum_{k=1}^{n} \begin{cases} 1 \text{ si } k \in A_i \cap A_j \\ 0 \text{ si } k \notin A_i \cap A_j \end{cases} = |A_i \cap A_j|.$$

B a donc la tête suivante, en notant $a_i = |A_i|$:

$$B = \begin{pmatrix} a_1 & c & \cdots & \cdots & c \\ c & a_2 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & a_{p-1} & c \\ c & \cdots & \cdots & c & a_p \end{pmatrix}.$$

Il est clair que $a_i \geq c$ pour tout i, mais il ne peut y avoir égalité que pour au plus un i : en effet, un cas d'égalité $|A_i| = a_i = c = |A_i \cap A_j|$ entraînerait $A_i \subset A_j$ pour tout j ; si l'on avait deux telles égalités, disons $a_i = c = a_j$, on aurait alors la double-inclusion $\begin{cases} A_j \subset A_i \\ A_i \subset A_j \end{cases}$, d'où l'égalité $A_i = A_j$ et $i = j$.

Ceci étant dit, l'exercice précédent montre que

$$\det C = \prod_{i=1}^{n}(a_i - c) + c\sum_{i=1}^{n}\prod_{j\neq i}(a_j - c) \geq 0 + c\prod_{j\neq k}(a_j - c) > 0$$

où k est l'éventuel indice tel que $a_k = c$. B est donc inversible, donc de rang p. Mais alors

$$p = \operatorname{rg} B = \operatorname{rg}\left({}^tAA\right) \leq \operatorname{rg} A \leq \min\{n, p\},$$

ce qui prouve $p \leq n$ comme voulu.

11 Un caractérisation du déterminant

On appellera *caractère* (sous-entendu *multiplicatif*) d'une K-algèbre $\mathcal{A}$ toute application $f : \mathcal{A} \longrightarrow K$ vérifiant

$$\forall a, b \in \mathcal{A},\ f(ab) = f(a) f(b).$$

Par exemple, le déterminant est un caractère de $M_n(K)$. Si l'on compose avec un caractère de K, mettons φ, on obtient encore un caractère $\varphi \circ \det$ de $M_n(K)$.

Cet exercice montre que cette description est exhaustive.

Montrer que le déterminant est l'unique caractère de $M_n(K)$ modulo les caractères de K.

On pourra déterminer l'image des J_r pour $r < n$ puis montrer que les transvections s'écrivent comme des commutateurs[9] *– attention à la caractéristique du corps...*

Solution proposée.

Soit f un caractère de $M_n(K)$. L'application nulle étant trivialement un caractère, on écartera le cas $f = 0$ par la suite. Puisque $f = f(I_n \cdot) = f(I_n) f$, on doit avoir $f(I_n) = 1$. Ainsi, pour toute matrice A inversible, on aura

$$1 = f(I_n) = f\left(AA^{-1}\right) = f(A) f\left(A^{-1}\right),$$

d'où $f\left(A^{-1}\right) = \frac{1}{f(A)}$. On en déduit que f est constante sur chaque classe de similitude[10] :

$$f\left(PAP^{-1}\right) = f(P) f(A) f\left(P^{-1}\right) = f(P) f(A) \frac{1}{f(P)} = f(A).$$

Regardons comme le suggèe l'énoncé l'image des J_r. En faisant un changement de base cyclique, on décale les 1 du J_r un cran plus haut (ceci est possible pour $r < n$), ce qui donne une matrice T triangulaire supérieure stricte, donc nilpotente. Par ce qui précède, J_r étant semblable à T, elle ont même image par f. On en déduit

$$f(J_r) = f(J_r^n) = f(J_r)^n = f(T)^n = f(T^n) = f(0) = 0.$$

Ainsi, en écrivant toute matrice A sous la forme PJ_rQ où $r = \operatorname{rg} A$, on voit que f est nulle sur les matrices non inversibles.

Soit maitenant A inversible, que l'on décompose sous la forme d'un produit de transvections multiplié par la dilatation $\begin{pmatrix} I_{n-1} & \\ & \det A \end{pmatrix}$. Ademettons un moment que les transvections soient toutes de la forme $MNM^{-1}N^{-1}$; elles sont alors toutes envoyées sur 1, donc l'image de A ne dépend que de son déterminant : $f(A) = f\begin{pmatrix} I_{n-1} & \\ & \det A \end{pmatrix}$. On peut alors écrire

$$f = \varphi \circ \det$$

où $\varphi : \begin{cases} K & \longrightarrow & K \\ \Delta & \longmapsto & f\begin{pmatrix} I_{n-1} & \\ & \Delta \end{pmatrix} \end{cases}$ est un caractère de K. Noter que le cas $f = 0$ exclu tout au début rentre dans cette description (prendre $\varphi = 0$). Réciproquement, la donnée d'un caractère φ de K définit un caractère f de $M_n(K)$ via la formule $f = \varphi \circ \det$.

Il nous reste donc à monter que les transvections sont des commutateurs. Déjà, modulo un bon changement de base, on peut supposer les transvections sous la forme $\begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & I_{n-2} \end{pmatrix}$. On va chercher à écrire $T = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ comme un commutateur, puis il suffira de complèter avec I_{n-2} pour avoir le résultat pour $n \geq 2$.

On reamarque que $T^2 = \begin{pmatrix} 1 & 2 \\ & 1 \end{pmatrix}$ est une transvection, donc semblable à T, ce qui s'écrit $T^2 = PTP^{-1}$, ou encore $T = PTP^{-1}T^{-1}$, *CFQD*. Joli, non ? Mais cette démonstration possède une faille : si $2 = 0$, $T^2 = I_n$ n'est plus une transvection. On s'en sort autrement : $f(T)^2 = f(I_n) = 1$, donc $f(T) = \pm 1 = 1$, ce qui montre que les transvections sont encore envoyées sur 1, et la suite de la preuve s'applique.

[9] Dans un groupe G, le *commutateur* de deux éléments a et b est défini par

$$[a, b] := aba^{-1}b^{-1}.$$

Puisque $ab = [a, b]\, ba$, les éléments a et b commutent ssi leur commutateur vaut le neutre de G.

[10] Une idée à retenir : si l'on commute à l'arrivée, penser à prendre l'image pour tuer les défauts de commutativité.

12 Sur le groupe spécial linéaire complexe

On se place dans $M_n(\mathbb{C})$. On identifie comme d'habitude $\mathbb{C}$ aux matrice scalaires complexes.

Soit G un sous-groupe de $SL_n(\mathbb{C})$ tel que $\begin{cases} G \cap \mathbb{C} = \{1\} \\ SL_n(\mathbb{C}) = \mathbb{C}G \end{cases}$.

1. *Montrer qu'il y un morphisme surjectif $f : G \twoheadrightarrow {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$.*
2. *Montrer que f s'annule sur les transvections.*
3. *Conclure $n = 1$.*

Solution proposée.
S'inpirant des supplémentaires dans les espaces vectoriels, on montre que les deux conditions signifient

$$\forall S \in SL_n(\mathbb{C}),\ \exists!\,(\lambda, g) \in \mathbb{C} \times G,\ S = \lambda g.$$

L'existence est tautologique, l'unicité s'obtient en remarquant que C commute avec tous les éléments de G.

1. Pour $S = \lambda G$ dans SL_n, il vient en prenant le déterminant $1 = |S| = \lambda^n |G| = \lambda^n$, ce qui montre que l'application $\lambda G \mapsto \lambda$ est à valeurs dans $\mathbb{U}_n \simeq {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. C'est un morphisme de groupes car tout commute, et surjectif car vaut l'identité[11] sur $\mathbb{U}_n$.
2. D'après l'exercice précédent, toute transvection s'écrit comme un commutateur. Or, le groupe d'arrivée ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ est commutatif, donc f annule tous les commutateurs, en particulier les transvections.
3. SL_n est engendré par les transvections, donc notre morphisme f est trivial. Sa surjectivité impose $n = 1$.

Remarque. On a montré que $SL_n(\mathbb{C})$ ne peut pas être isomorphe au produit de $\mathbb{C}$ par l'un de ses sous-groupes (sauf dans le cas trivial $n = 1$).

13 Un peu d'analyse

1. *Soient $n \geq 1$ et $f_1, ..., f_n$ des applications de $\mathbb{R}$ dans $\mathbb{C}$. Montrer qu'elles sont libres ssi il y a n réels $a_1, ..., a_n$ tel que la matrice $(f_i(a_j))$ soit inversible.*
2. *Soit F un sous-espace vectoriel de dimension finie des applications bornées de $\mathbb{R}$ dans $\mathbb{C}$. Montrer qu'une suite de F converge simplement ssi elle converge uniformément.*

Solution proposée.

1. Montrons le premier sens par récurrence sur n.

   Pour $n = 1$, (f_1) est libre ssi f_1 n'est pas identiquement nulle, ce qui revient à dire qu'il y a un a tel que $f_1(a) \neq 0$, d'où le résultat.

   Soient maintenant $f_1, ..., f_{n+1}$ libres et $a_1, ..., a_n$ comme dans l'énoncé pour $f_1, ..., f_n$ (pour un $n \geq 1$). On cherche un réel x tel que

$$\delta(x) := \begin{vmatrix} f_1(a_1) & \cdots & f_1(a_n) & f_1(x) \\ \vdots & & \vdots & \vdots \\ f_n(a_1) & \cdots & f_n(a_n) & f_n(x) \\ f_{n+1}(a_1) & \cdots & f_{n+1}(a_n) & f_{n+1}(x) \end{vmatrix} \text{ soit non nul.}$$

   Or, en développant selon la dernière colonne, on obtient une relation $\delta(x) = \sum_{i=1}^{n+1} \lambda_i f_i(x)$ avec $\lambda_{n+1} = \det\left(f_i(a_j)_{i,j=1,...,n}\right)$ non nul par hypothèse de récurrence. Par liberté de la famille $(f_1, ..., f_{n+1})$, δ ne peut être identiquement nul, d'où un réel a_{n+1} tel que $\delta(a_{n+1}) \neq 0$, *CFQD*.

[11] Lorsque l'on dispose dans un groupe G d'un morphisme f de G sur un sous-groupe H qui vaut l'identité sur H, on dit que f est une *rétraction* (de G sur H).

Montrons l'autre sens par contraposée. Soient $f_1, ..., f_n$ liées, par exemple $f_1 \in \text{Vect}(f_2, ..., f_n)$. Alors, pour tous réels $a_1, ..., a_n$, le déterminant $\begin{vmatrix} f_1(a_1) & \cdots & f_1(a_n) \\ \vdots & & \vdots \\ f_n(a_1) & \cdots & f_n(a_n) \end{vmatrix}$ est nul : remplacer f_1 par la combinaison linéaire correspondante et utiliser la linéarité du déterminant par rapport à la première ligne.

2. Montrons que la convergence simple implique la convergence uniforme, la réciproque étant plus ou moins tautologique.

Soit $f_1, ..., f_n$ une base de F. D'après le premier point, il y a n réels $a_1, ..., a_n$ tels que la matrice $(f_i(a_j))$ soit inversible.

Soit maintenant $u^k = \sum_{i=1}^n \lambda_i^k f_i$ une suite de fonctions de F qui converge simplement. En évaluant en les a_i, il vient

$$\begin{pmatrix} u^k(a_1) \\ \vdots \\ u^k(a_n) \end{pmatrix} = \begin{pmatrix} f_1(a_1) & \cdots & f_n(a_1) \\ \vdots & & \vdots \\ f_1(a_n) & \cdots & f_n(a_n) \end{pmatrix} \begin{pmatrix} \lambda_1^k \\ \vdots \\ \lambda_n^k \end{pmatrix},$$

d'où en inversant

$$\begin{pmatrix} \lambda_1^k \\ \vdots \\ \lambda_n^k \end{pmatrix} = \begin{pmatrix} f_1(a_1) & \cdots & f_n(a_1) \\ \vdots & & \vdots \\ f_1(a_n) & \cdots & f_n(a_n) \end{pmatrix}^{-1} \begin{pmatrix} u^k(a_1) \\ \vdots \\ u^k(a_n) \end{pmatrix}$$

qui converge simplement vers un vecteur $(\lambda_1, ..., \lambda_n)$. On en déduit que u^k converge simplement vers $u := \sum_{i=1}^n \lambda_i f_i$. Ainsi,

$$\left|u^k(x) - u(x)\right| = \left|\sum_{i=1}^n \lambda_i^k f_i(x) - \sum_{i=1}^n \lambda_i f_i(x)\right| \leq \sum_{i=1}^n \left|\lambda_i^k - \lambda_i\right| |f_i(x)| \leq \sum_{i=1}^n \|f_i\|_\infty \underbrace{\left|\lambda_i^k - \lambda_i\right|}_{\longrightarrow 0} \xrightarrow{k\infty} 0,$$

d'où la convergence uniforme.

Remarque. Ce lemme s'applique par exemple à $K_n[X]$: pour qu'une suite de polynômes de degré borné converge dans $K_n[X]$, il suffit qu'elle converge pour la norme infinie, *i. e.* uniformément, donc il suffit qu'elle converge simplement.

14 Un lemme inutile illustrant une idée géniale

Pour une matrice $A \in M_n$ et I une partie de $\{1, ..., n\}$, on notera A_I la matrice extraite $(a_{i,j})_{i,j \in I}$.

Montrer que la quantité $\sum_{|I|=k} \det A_I$ est invariante par conjugaison.

Solution proposée.

On se rappelle que GL_n est engendré par les transvections et les dilatations. Il suffit donc de vérifier que $\sum_{|I|=k} \det A_I$ est invariant par l'action sur A (par conjugaison) d'une transvection ou une dilatation.

Or, lorsque l'on dilate la i-ième ligne/colonne de A par un scalaire λ, l'opération se répercute de la même manière sur A_I si $i \in I$, ce qui fait sortir un λ quand on prend le déterminant. Mais on conjugue, donc il sort aussi un scalaire $\frac{1}{\lambda}$ qui vient tuer le premier. Dans le cas où $i \notin I$, les dilatations ne touchent pas à A_I, donc le déterminant est inchangé dans tous les cas.

Le même raisonnement tient (presque) pour les transvections. Lorsque l'on fait agir une transvection $I_n + \alpha E_{i,j}$ sur A, on fait une opération sur les lignes/colonnes de A, laquelle opération se répercute sur les lignes/colonnes de A_I (évidemment, si i et j sont hors de I, A_I est inchangée) ; en particulier, la nouvelle matrice extraite A_I est obtenue à partir de l'ancienne par une opération de transvection si i et j sont tous deux dans I, ce qui ne change pas son déterminant. Évidemment, la conjugaison étant deux multiplications successives, conjuguer par une transvection ne change pas nos $\det A_I$.

Il reste à voir le cas où exactement l'un des indices i, j est dans I : en effet, lorsque l'on extrait A_I, on emporte avec soi la ligne/colonne dont on aimerait disposer pour faire opérer la transvection en sens inverse.

Qu'à cela ne tienne, on va la rajouter pour pouvoir faire ce qu'on veut (c'est cela l'idée géniale !). Détaillons cela.

Notons A' la conjuguée de A par la transvection $I+\alpha E_{i,j}$: on applique à A les opérations $\left\{ \begin{array}{l} L_i \longleftarrow L_i + \alpha L_j \\ C_j \longleftarrow C_j - \alpha C_i \end{array} \right.$.
Considérons à présent une partie I de cardinal k contenant i mais pas j. On a clairement une partie « duale » I^* où l'on a remplacé i par j. Montrons que $\det A_I + \det A_{I^*}$ est inchangé par la conjugaison considérée. Les autres déterminants extraits mettant restant inchangés d'après les remarques préliminaires, on aura gagné.

Explicitons les indices de I :

$$I = \{i_1 < i_2 < \cdots < i_\nu < \cdots < i_k\} \text{ où } \nu \text{ est la place de } i = i_\nu.$$

On calcule $\det A'_I$ en rajoutant la ligne manquante (L_j indexée par I) en incrémentant la taille de la matrice :

$$\begin{aligned} \det A'_I &= \begin{vmatrix} a_{i_1,i_1} & \cdots & a_{i_1,i_k} \\ \vdots & & \vdots \\ a_{i_\nu,i_1} + \alpha a_{j,i_1} & \cdots & a_{i_\nu,i_k} + \alpha a_{j,i_k} \\ \vdots & & \vdots \\ a_{i_k,i_1} & \cdots & a_{i_k,i_k} \end{vmatrix} = \begin{vmatrix} 1 & a_{j,i_1} & \cdots & a_{j,i_k} \\ 0 & & & \\ \vdots & & A'_I & \\ 0 & & & \end{vmatrix} = \begin{vmatrix} 1 & a_{j,i_1} & \cdots & a_{j,i_k} \\ 0 & & & \\ \vdots & & & \\ -\alpha & & A_I & \\ \vdots & & & \\ 0 & & & \end{vmatrix} \\ &= \det A_I - (-1)^\nu \, \alpha \det \begin{pmatrix} l_j \\ l_{i_1} \\ \vdots \\ l_{i_k} \end{pmatrix} \text{ où il manque la } \nu\text{-ième ligne } l_i \text{ de } A_I \\ &= \det A_I + \alpha \det \begin{pmatrix} l_{i_1} \\ \vdots \\ l_{i_k} \end{pmatrix} \text{ où la ligne } l_i \text{ est remplacée par la ligne } l_j. \end{aligned}$$

Le même calcul tient pour $\det A_{I^*}$: on tranpose la matrice pour avoir exactement la même situation, à une transposition (i,j) et à un signe devant le α près :

$$\det A_{I^*} = \det A_I - \alpha \det (c_{i_1}, ..., c_{i_k}) \text{ où la colonne } c_j \text{ est remplacée par } c_i.$$

Il reste à remarquer que les deux matrices perturbatrices qui apparaissent sont en fait les mêmes : on extrait de A les colonnes d'indice $\in I$ et les lignes d'indice $\in I^*$.

Remarque. Une solution beaucoup plus courte consiste à dire que la quantité recherchée est le coeffcient en $(-X)^k$ du polynôme caractéristique, lequel est bien sûr invariant par conjugaison – voir exercice suivant.

15 DL du déterminant

Avec les notations de l'exercice précédent, montrer la formule suivante :

$$\det (A + tI_n) = \sum_{k=0}^{n} \left(\sum_{|I|=n-k} \det A_I \right) t^k.$$

Solution proposée.
À ce niveau (sans outils de réduction), un calcul direct semble être la seule possibilité. Il s'agit juste de développer le terme de gauche et de regrouper les même puissances en t : somme toute, c'est de la combinatoire.

Allons-y, en regroupant les permutations selon leur support :

$$\begin{aligned}
\det(A+t\,\mathrm{Id}) &= \sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\prod_{i=1}^{n}[A+t\,\mathrm{Id}]_{i,\sigma(i)}\\
&= \sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\prod_{i\notin\mathrm{Supp}\,\sigma}(a_{i,i}+t)\prod_{i\in\mathrm{Supp}\,\sigma}a_{i,\sigma(i)}\\
&= \sum_{I}\sum_{\mathrm{Supp}\,\sigma=I}\varepsilon(\sigma)\prod_{i\notin I}(a_{i,i}+t)\prod_{i\in I}a_{i,\sigma(i)}\\
&= \sum_{I}\prod_{i\notin I}(a_{i,i}+t)\sum_{\mathrm{Supp}\,\sigma=I}\varepsilon(\sigma)\prod_{i\in I}a_{i,\sigma(i)}.
\end{aligned}$$

Pour développer le produit $\prod_{i\notin I}(a_{i,i}+t)$ (rappelons que l'on souhaite obtenir les coefficients de ce polynôme en t), il s'agit de choisir j indices hors de I, de piocher $a_{i,i}$ pour ces indices et t pour les $(n-|I|)-j$ indices restants, ce qui donne $\sum_{J\cap I=\emptyset}\left(\prod_{j\in J}a_{j,j}\right)t^{n-|I|-|J|}$. Poursuivons le calcul, en introduisant $K:=I\cup J$:

$$\begin{aligned}
&= \sum_{I}\left(\sum_{J\cap I=\emptyset}\prod_{j\in J}a_{j,j}t^{n-|I|-|J|}\right)\sum_{\mathrm{Supp}\,\sigma=I}\varepsilon(\sigma)\prod_{i\in I}a_{i,\sigma(i)}\\
&= \sum_{I}\sum_{J\cap I=\emptyset}t^{n-|I|-|J|}\sum_{\mathrm{Supp}\,\sigma=I}\varepsilon(\sigma)\prod_{k\in I\cup J}a_{k,\sigma(k)}\\
&= \sum_{K}t^{n-|K|}\sum_{I\subset K}\sum_{\mathrm{Supp}\,\sigma=I}\varepsilon(\sigma)\prod_{k\in K}a_{k,\sigma(k)}\\
&= \sum_{K}t^{n-|K|}\sum_{\mathrm{Supp}\,\sigma\subset K}\varepsilon(\sigma)\prod_{k\in K}a_{k,\sigma(k)}.
\end{aligned}$$

Il reste à voir pourquoi le truc après $t^{n-|K|}$ vaut exactement $\det A_K$. Mais la condition $\mathrm{Supp}\,\sigma\subset K$ signifie que σ induit une permutation de K tout en fixant les autres points dont on n'a que faire pour calculer le produit $\prod_{k\in K}a_{k,\sigma(k)}$. Ceci montre que

$$\sum_{\mathrm{Supp}\,\sigma\subset K}\varepsilon(\sigma)\prod_{k\in K}a_{k,\sigma(k)}=\sum_{\sigma\in\mathfrak{S}_K}\varepsilon(\sigma)\prod_{k\in K}a_{k,\sigma(k)}=\det A_K,\ \textit{CQFD.}$$

Remarque. Si le lecteur a bien suivi le calcul ci-dessus, il devrait pouvoir généraliser sans mal :

$$\det(A+\mathrm{Diag}(t_1,...,t_n))=\sum_{I}\det A_I\prod_{i\notin I}t_i.$$

L'idéal serait de sentir cette formule de manière purement combinatoire. Regardons les termes $\prod a_{i,\sigma(i)}$ de la formule de Sarrus qui contribuent à $\prod_{i\notin I}t_i$: pour en former un, il faut piocher dans la matrice A les termes diagonaux d'indices $\notin I$ et piocher du coup les autres facteurs dans la matrice A_I, et ce de toutes les façons possibles, ce qui donne bien (en mettant les signes) le facteur $\det A_I$. Tout le calcul ci-dessus n'est que la formalisation des trois lignes qui précèdent.

Moralité : il faut savoir naviguer entre ces deux extrêmes, à savoir le monde aveugle du calcul réflexe et celui de l'intuition combinatoire obscure.

Pour ceux qui n'ont pas digéré le calcul ci-dessus, quelques connaissances élémentaires de réduction, combinées au lemme inutile de l'exercice précédent, permettent d'obtenir une solution bien plus élégante (*cf.* feuille 1 sur la réduction).

16 Sur la connexité de matrices à rang préfixé

Une fonction de $\mathbb{R}$ dans $M_n(\mathbb{R})$ sera dite *continue* si chacune de ses fonctions coordonnées est continue.

Une partie C de $M_n(\mathbb{R})$ sera dite *connexe par arcs* si l'on peut relier deux éléments quelconques de C par un arc continu qui reste dans C, *i. e.* si $\forall a,b\in C$ il y a une application continue $\gamma:[0,1]\longrightarrow C$ telle

que $\left\{ \begin{array}{l} \gamma(0) = a \\ \gamma(1) = b \end{array} \right.$ (on notera alors $a \rightsquigarrow b$). On se convaincra que $\rightsquigarrow$ est une relation d'équivalence. On appelle *composante connexe* d'une partie de $M_n(\mathbb{R})$ une classe d'équivalence pour la relation $\rightsquigarrow$.

On pourra admettre que le déterminant $\det : M_n(\mathbb{R}) \longrightarrow \mathbb{R}$ est une application continue.

Soit R un ensemble de rangs dans $\{0, ..., n\}$ et $\mathcal{M}^R = \{A \in M_n(\mathbb{R}) \ ; \operatorname{rg} A \in R\}$ l'ensemble des matrices réelles dont le rang est dans R. On cherche une condition nécessaire et suffisante pour que $\mathcal{M}^R$ soit connexe par arcs.

On pourra traiter successivement les cas :
- $R = \{n\}$,
- $R = \{r\}$ où $r < n$,
- $R = \{r, n\}$ avec $r < n$,
- $R = \{r, r'\}$ avec $r, r' < n$.

Solution proposée.

Suivons les indications de l'énoncé.

On regarde d'abord le cas $R = \{n\}$, *i. e.* $\mathcal{M}^R = GL_n(\mathbb{R})$. On cherche donc à relier deux matrices inversibles A et B par un chemin de matrices inversibles.

On sait que A et B s'écrivent toutes deux comme un produit de transvections mulitplié par une matrice de dilatation $Dil_\Delta := \begin{pmatrix} \Delta & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$ où Δ est le déterminant de A ou B (remarquer que le déterminant d'une matrice de transvection vaut 1).

On commence par se débarasser des matrices de transvections $I_n + \alpha E_{i,j}$ en étouffant continûment le coefficient α en dehors de la diagonale à l'aide de

$$\gamma : \left\{ \begin{array}{ccc} [0,1] & \longrightarrow & GL_n(\mathbb{R}) \\ \lambda & \longmapsto & I_n + \lambda\alpha E_{i,j} \end{array} \right.$$

(γ est bien continue car toutes ses applications coordonées sont constantes sauf une qui est linéaire). En étouffant successivement les coefficients des matrices de transvection, on montre (par transitivité de $\rightsquigarrow$) que $A \rightsquigarrow Dil_{\det A}$, et de même $B \rightsquigarrow Dil_{\det B}$. On cherche maintenant à relier

$$\begin{pmatrix} \det A & & \\ & I_{n-1} & \end{pmatrix} \rightsquigarrow \begin{pmatrix} \det B & & \\ & I_{n-1} & \end{pmatrix}.$$

On y parviendra si l'on arrive à relier deux réels non nuls par un chemin ne pasant pas par 0 (on veut rester dans $GL_n(\mathbb{R})$!), et il facile de voir qu'il n'y a que deux alternatives : ou bien $\det A$ et $\det B$ ont même signe, auquel cas on relie $Dil_{\det A}$ et $Dil_{\det B}$ par le chemin « segment »

$$\gamma : \left\{ \begin{array}{ccc} [0,1] & \longrightarrow & GL_n(\mathbb{R}) \\ \lambda & \longmapsto & \begin{pmatrix} \lambda \det B + (1-\lambda) \det A & & \\ & I_{n-1} & \end{pmatrix} \end{array} \right. ,$$

ou bien $\det A \det B < 0$ et alors il n'est pas possible de relier A et B en restant dans $GL_n(\mathbb{R})$: en effet, si γ est un chemin dans $GL_n(\mathbb{R})$ reliant A et B, alors $f = \det \circ \gamma$ est une application continue de $\mathbb{R}$ dans $\mathbb{R}$ telle que $f(0) f(1) < 0$, donc doit s'annuler par le théorème des valeurs intermédiaires, ce qui est impossible si l'on veut rester dans $GL_n(\mathbb{R})$.

Regardons à présent le cas $R = \{r\}$ où $r < n$. Le cas des matrices inversibles étant traité, on va s'y ramener en écrivant toute matrice A comme PJ_rQ où P et Q sont inversibles et $r = \operatorname{rg} A$.

Le problème revient à présent à relier deux matrices du type PJ_rQ et $P'J_rQ'$ en restant de rang r. On a envie de ne pas toucher aux J_r, afin de s'assurer que le rang reste constammenent égal à r. On va donc chercher à relier $P \rightsquigarrow P'$ et $Q \rightsquigarrow Q'$. Si $\det P \det P' > 0$, on a vu que cela ne pose pas de problème. En revanche, dans le cas contraire...

Pour s'en sortir, on utilise le fait que J_r a au moins une ligne de zéros tout en bas (on est dans le cas $r < n$!) pour modifier P sans toucher au produit PJ_r :

$$PJ_r = \begin{pmatrix} * & * & a_1 \\ * & * & \vdots \\ * & * & a_n \end{pmatrix} \begin{pmatrix} * & * & \\ * & * & \\ 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} * & * & -a_1 \\ * & * & \vdots \\ * & * & -a_n \end{pmatrix} \begin{pmatrix} * & * & \\ * & * & \\ & & 0 \end{pmatrix} = \widetilde{P} J_r$$

avec $\det \widetilde{P} = -\det P$ par linéarité du déterminant. On modifierait de même la dernière ligne de Q en mettant des signes $-$ si besoin.

On a donc montré que $\mathcal{M}^R$ est connexe par arcs si $\mathcal{M}^R = \{r\}$ avec $r < n$.

Supposons maintenant que R contienne exactement deux élements $r < n$. Pour relier deux matrices de même rang r, on utilise la méthode décrite précédemment. Pour relier une matrice $A = PJ_rQ$ de rang r à une matrice inversible B, on commence par changer les signes de $\det P$ et $\det Q$ pour relier $P \rightsquigarrow B$ et $Q \rightsquigarrow I_n$, puis on relie $J_r \rightsquigarrow I_n$ à l'aide du chemin

$$\lambda \in [0,1] \longmapsto \begin{pmatrix} I_r & \\ & \lambda I_{n-r} \end{pmatrix}.$$

Enfin, pour relier deux matrices inversibles, on passe par une matrice de rang r – par exemple J_r.

Dans le cas où R est réduit à deux indices $r < r'$ distincts de n, on a déjà vu que relier deux matrices de même rang r ou r' était possible. Pour relier $PJ_rQ \rightsquigarrow P'J_{r'}Q'$, on modifie les déterminants pour envoyer les matrices inversibles comme l'on veut, puis on relie $J_r \rightsquigarrow J_{r'}$ par le chemin

$$\lambda \longmapsto \begin{pmatrix} I_r & & \\ & \lambda I_{r'-r} & \\ & & 0 \end{pmatrix}.$$

Conclusion. Deux matrices de rang r et r' peuvent toujours être reliées dans $\mathcal{M}^{\{r,r'\}}$ sauf si $r = r' = n$, auquel cas on passe par une matrice intermédiaire de rang $< n$ (et on peut le faire ssi $R \neq \{n\}$).

Finalement, $\mathcal{M}^R$ est connexe par arcs ssi $R \neq \{n\}$. Dans ce dernier cas, $\mathcal{M}^R = GL_n(\mathbb{R})$ a deux composantes connexes selon le signe du déterminant.

17 Déterminant de Cauchy

Soient $\overrightarrow{a}$ et $\overrightarrow{b}$ une famille de $2n$ scalaires tels que $a_i + b_j$ n'est jamais nul. Calculer le déterminant dit de Cauchy

$$C\left(\overrightarrow{a}, \overrightarrow{b}\right) := \det\left(\left(\frac{1}{a_i + b_j}\right)_{i,j=1,\ldots,n}\right).$$

Solution proposée.

On se rappelle de l'identité classique

$$\frac{1}{n} - \frac{1}{n+1} = \frac{1}{n(n+1)},$$

ce qui incite à faire des opérations élémentaires sur les lignes et colonnes pour tuer les numérateurs.

Soustrayons la n-ième ligne à toutes les autres : le coefficient $\frac{1}{a_i+b_j}$ devient

$$\frac{1}{a_i + b_j} - \frac{1}{a_n + b_j} = \frac{a_n - a_i}{(a_i + b_j)(a_n + b_j)}.$$

On voit que le facteur $a_n - a_i$ apparaît sur la nouvelle i-ième ligne (pour $i < n$), et que $\frac{1}{a_n+b_j}$ est commum à la j-ième nouvelle colonne (pour $j = 1, ..., n$), de sorte qu'on peut factoriser

$$C\left(\overrightarrow{a}, \overrightarrow{b}\right) = \frac{\prod_{i<n}(a_n - a_i)}{\prod_{j=1}^{n}(a_n + b_j)} \begin{vmatrix} \frac{1}{a_1+b_1} & \cdots & \cdots & \frac{1}{a_1+b_n} \\ \vdots & & & \vdots \\ \frac{1}{a_{n-1}+b_1} & \cdots & \cdots & \frac{1}{a_{n-1}+b_n} \\ 1 & \cdots & \cdots & 1 \end{vmatrix}.$$

On recommence en soustrayant la n-ième colonne aux autres, ce qui transforme le coefficient (i,j) en

$$\frac{1}{a_i+b_j}-\frac{1}{a_i+b_n}=\frac{b_n-b_j}{(a_i+b_j)(a_i+b_n)}.$$

On peut sortir les b_n-b_j et les $\frac{1}{a_i+b_n}$, d'où

$$\begin{aligned} C\left(\overrightarrow{a},\overrightarrow{b}\right) &= \frac{\prod_{i<n}(a_n-a_i)}{\prod_{j=1}^{n}(a_n+b_j)}\frac{\prod_{j<n}(b_n-b_j)}{\prod_{i=1}^{n-1}(a_i+b_n)}\begin{vmatrix} \frac{1}{a_1+b_1} & \cdots & \frac{1}{a_1+b_{n-1}} & 1 \\ \vdots & & \vdots & \vdots \\ \frac{1}{a_{n-1}+b_1} & \cdots & \frac{1}{a_{n-1}+b_{n-1}} & 1 \\ 0 & \cdots & 0 & 1 \end{vmatrix} \\ &= \frac{\prod_{i<n}(a_n-a_i)}{\prod_{j=1}^{n}(a_n+b_j)}\frac{\prod_{j<n}(b_n-b_j)}{\prod_{i=1}^{n-1}(a_i+b_n)}C(a_1,...,a_{n-1},b_1,...,b_{n-1}) \end{aligned}$$

en développant selon la dernière ligne.

Par une récurrence immédiate, il vient

$$C\left(\overrightarrow{a},\overrightarrow{b}\right)=\frac{\prod_{i<j}(a_j-a_i)(b_j-b_i)}{\prod_{i,j}(a_i+b_j)}.$$

Autre méthode : ? ? ? ? ? à rédiger ? ? ? ? on remplace a_n par X, on a un fraction de deg ≤ -1, de poles les b_i, donc $=\frac{P(X)}{\prod(X+b_j)}$ avec P nul en les $-a_i$, d'où det = cste $\frac{\prod_1^{n-1}(X-a_i)}{\prod_1^n(X+b_i)}$.

Le théorème qui suit nécessite pour sa démonstration la connaissance des déterminants de Cauchy et ceux de Gram[12].

18 Théorème de Müntz

On se place sur le $\mathbb{R}$-espace vectoriel E des fonctions réelles continues sur $[0,1]$ muni du produit scalaire $\langle f \mid g\rangle = \int_0^1 fg$. Rappelons qu'il en découle une norme canoniquement associée $\|f\| = \sqrt{\langle f \mid f\rangle}$. On notera abusivement x^α la fonction puissance $x \mapsto x^\alpha$, qui est un élément de E.

On se donne une suite croissante (α_n) de réels > 0. On cherche à quelle condition sur les α_n peut-on approximer les fonctions de E par des combinaisons linéaires des x^{α_n}. Plus précisément, étant donnée une fonction $u \in E$ et un $\varepsilon > 0$, peut-on trouver un entier n et des scalaires $\lambda_1,...,\lambda_n$ tels que $\|u - \sum_{i=1}^n \lambda_i x^{\alpha_i}\| < \varepsilon$? On dira alors que u est *adhérent* aux x^{α_i} (pour la norme euclidienne). Si tout u de E est adhérent aux x^{α_i}, on dit que les x^{α_i} sont *denses* dans E.

1. *En notant* $E_n = \mathrm{Vect}\,(x^{\alpha_1},...,x^{\alpha_n})$, *montrer qu'un* u *de* E *est adhérent aux* x^{α_i} *ssi la distance de* u *à* E_n, *définie par*
$$d(u,E_n)=\inf_{e_n\in E_n}\|u-e_n\|,$$
tend vers 0 *quand* $n \longrightarrow \infty$.
2. *Pour un réel* $\beta > 0$, *montrer que*
$$d\left(x^\beta,E_n\right)=\frac{1}{\sqrt{2\beta+1}}\prod_{i=1}^{n}\left|\frac{\alpha_i-\beta}{\alpha_i+\beta+1}\right|$$
3. *En déduire que les* x^{α_i} *sont denses dans* E *ssi la série* $\sum \frac{1}{\alpha_n}$ *diverge. On pourra admettre pour la réciproque qu'il suffit de prouver que les* x^n *pour* $n \in \mathbb{N}$ *sont adhérents aux* x^{α_i} – cf. *le théorème de Stone-Wieirstrass.*

[12] *cf.* feuille sur les espaces préhilbertiens

Solution proposée.

1. Supposons que u est adhérent aux x^{α_i}. Soit $\varepsilon > 0$. On dispose donc d'un entier $N \geq 1$ et de scalaires $\lambda_1, ..., \lambda_N$ tels que $\left\| u - \sum_{i=1}^{N} \lambda_i x^{\alpha_i} \right\| < \varepsilon$. Il en résulte, pour $n > N$:

$$d(u, E_n) \leq d(u, E_N) \leq \left\| u - \sum_{i=1}^{N} \lambda_i x^{\alpha_i} \right\| < \varepsilon.$$

On a donc montré que $d(u, E_n) \overset{n\infty}{\longrightarrow} 0$.

Réciproquement, supposons que $d(u, E_n) \overset{n\infty}{\longrightarrow} 0$. Soit $\varepsilon > 0$: il y un n tel que $d(u, E_n) < \varepsilon$. Or, E_n est de dimension finie, donc $d(u, E_n)$ est atteinte en un point de E_n, le projeté orthogonal de u sur E_n. En écrivant ce dernier sous la forme $p = \sum_{i=1}^{n} \lambda_i x^{\alpha_i}$, il vient $\|u - \sum_{i=1}^{n} \lambda_i x^{\alpha_i}\| = d(u, E_n) < \varepsilon$, de sorte que u est bien adhérent aux x^{α_i}.

2. Notons $\alpha_0 = \beta$ pour harmoniser les notations. On va calculer la distance $d\left(x^{\beta}, E_n\right)$ à l'aide de déterminants de Gram. On calcule déjà

$$\langle x^{\alpha_i} \mid x^{\alpha_j} \rangle = \int_0^1 x^{\alpha_i + \alpha_j} = \frac{1}{\alpha_i + \alpha_j + 1} = \frac{1}{\left(\alpha_i + \frac{1}{2}\right) + \left(\alpha_j + \frac{1}{2}\right)},$$

d'où (en utilisant la formule des déterminants de Cauchy) :

$$g(x^{\alpha_0}, x^{\alpha_1}, ..., x^{\alpha_n}) = \frac{\prod_{0 \leq i < j \leq n} (\alpha_j - \alpha_i)^2}{\prod_{i,j=0}^{n} (\alpha_i + \alpha_j + 1)} = \frac{\prod_{i=1}^{n} (\alpha_i - \beta)^2}{(2\beta + 1) \prod_{i=1}^{n} (\alpha_i + \beta + 1)^2} \underbrace{\frac{\prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2}{\prod_{i,j=1}^{n} (\alpha_i + \alpha_j + 1)}}_{= g(x^{\alpha_0}, x^{\alpha_1}, ..., x^{\alpha_n})}.$$

Il en résulte

$$d\left(x^{\beta}, E_n\right) = \sqrt{\frac{g(x^{\alpha_0}, x^{\alpha_1}, ..., x^{\alpha_n})}{g(x^{\alpha_1}, ..., x^{\alpha_n})}} = \frac{1}{\sqrt{2\beta + 1}} \prod_{i=1}^{n} \left| \frac{\alpha_i - \beta}{\alpha_i + \beta + 1} \right|.$$

3. Supposons les x^{α_i} denses dans E. En particulier, si $\beta > 0$ est un réel distinct de tous les α_i, la fonction x^{β} est adhérente aux x^{α_i}, donc $d\left(x^{\beta}, E_n\right) \overset{n\infty}{\longrightarrow} 0$, ce qui s'écrit aussi (en prenant le logarithme)

$$\sum_{i=1}^{n} \ln \left| 1 - \frac{2\beta + 1}{\alpha_i + \beta + 1} \right| \overset{n\infty}{\longrightarrow} -\infty.$$

Si la suite (α_i) est bornée, il est clair que $\sum \frac{1}{\alpha_i}$ diverge ; sinon, $\alpha_i \longrightarrow \infty$ et l'on dispose de l'équivalent (pour $\alpha_i > \beta$)

$$\ln \left| 1 - \frac{2\beta + 1}{\alpha_i + \beta + 1} \right| = \ln \left(1 - \frac{2\beta + 1}{\alpha_i + \beta + 1} \right) \sim -\frac{2\beta + 1}{\alpha_i + \beta + 1} \sim -\frac{2\beta + 1}{\alpha_i}.$$

Comme on raisonne sur des séries à signe constant, la série $\sum -\frac{2\beta+1}{\alpha_i}$ est de même nature que $\sum \ln \left| 1 - \frac{2\beta+1}{\alpha_i+\beta+1} \right|$, donc doit diverger, *CFQD*.

Supposons réciproquement que $\sum \frac{1}{\alpha_i}$ diverge. Suivons l'énoncé et montrons que pour tout $m \in \mathbb{N}$ le monôme x^m est adhérent aux x^{α_i}, *i. e.* que $d(x^m, E_n) \overset{n\infty}{\longrightarrow} 0$. On veut donc

$$\prod_{i=1}^{n} \frac{\alpha_i - m}{\alpha_i + m + 1} \overset{n\infty}{\longrightarrow} 0.$$

Si les α_i divergent vers ∞, l'équivalent du paragraphe précédent montre que $\sum \ln \left| 1 - \frac{2m+1}{\alpha_i+m+1} \right|$ diverge, d'où la limite voulue.

Dans le cas contraire, on a directement

$$\prod_{i=1}^{n} \frac{|\alpha_i - m|}{\alpha_i + m + 1} \leq \prod_{i=1}^{n} \frac{\alpha_i + m}{\alpha_i + m + 1} = \prod_{i=1}^{n} \left(1 - \frac{1}{\alpha_i + m + 1} \right) \leq \left(1 - \frac{1}{\sup \alpha_i + m + 1} \right)^n \longrightarrow 0.$$

Remarque. On peut montrer que le théorème de Müntz reste valable en remplaçant la norme L^2 (celle issue du produit scalaire) par la norme L^∞ définie par

$$\|f\|_\infty = \max_{[0,1]} |f| .$$

La norme L^∞ est également appelée *norme de la convergence uniforme*, car une suite (f_n) converge uniformément vers f ssi elle converge pour la norme L^∞.

19 Théorème de Frobenius-Zolotarev

Soit $p \geq 3$ premier et $K = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ le corps fini à p éléments. On rappelle au besoin que K^* est cyclique.

Soit A une matrice de $GL_n(K)$. A définit un isomorphisme de K^n, donc une bijection, *i. e.* une permutation. On peut donc voir $GL_n(K)$ comme une partie de $\mathfrak{S}(K^n)$.

1. *Montrer que A est dans le groupe alterné $\mathfrak{A}(K^n)$ ssi son déterminant est un carré dans K.*
2. *Que dire en remplaçant K par un corps fini quelconque ? Détailler le cas $p = 2$.*

Solution proposée.

1. Il s'agit de calculer $\varepsilon(A)$. Puisque la signature est un morphisme, on se ramène à des générateurs de $GL_n(K)$, de préférence dont l'action en tant que permutation sera facile à étudier. On prend naturellement les transvections, qui se mettent toutes dans une bonne base sous la forme $\begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & I_{n-2} \end{pmatrix}$, et les dilatations, semblables à des $\begin{pmatrix} \Delta & \\ & I_{n-1} \end{pmatrix}$ où Δ est un scalaire.

   Remarquons tout de suite que la signature est un invariant de similitude :

$$\varepsilon\left(PAP^{-1}\right) = \varepsilon(P)\,\varepsilon(A)\,\varepsilon\left(P^{-1}\right) = \varepsilon(P)\,\varepsilon(A)\,\varepsilon(P)^{-1} = \varepsilon(A) .$$

   Ainsi, en écrivant A sous la forme $D\prod T_i$ où D est une dilatation et les T_i des transvections, on peut supposer D et T_i sous la forme simplifiée du paragraphe précédent.

   Regardons tout d'abord pour $n \geq 2$ l'action de la transvection[13] $T := \begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & I_{n-2} \end{pmatrix}$. En remarquant que[14] T est le carré de $\begin{pmatrix} 1 & \frac{1}{2} & \\ & 1 & \\ & & I_{n-2} \end{pmatrix}$, on voit immédiatement que $\varepsilon(T) = 1$. Noter que l'on a le droit de diviser par 2 car $\operatorname{car} K = p > 2$.

   Toute l'information de $\varepsilon(A)$ réside donc dans la dilatation $D := \begin{pmatrix} \Delta & \\ & I_{n-1} \end{pmatrix}$. Cela n'est guère étonnant au vu du résultat à démontrer, puisque le déterminant de A est précisément Δ et n'apparaît pas dans les transvections.

   Observer de suite que, lorsque Δ est un carré, la diliation D l'est aussi, donc son image aussi, d'où $\varepsilon(D) = 1$. Il ne reste donc plus qu'à montrer la réciproque.

   Commençons par le cas $n = 1$. L'action de D sur un vecteur $x \in K$ est trivialement donnée par $D^k(x) = \Delta^k x$. Ainsi, en notant ω l'ordre de Δ dans K^*, toutes les orbites sont du type

$$\Omega_x = \left\{x, \Delta x, \Delta^2 x, ..., \Delta^{\omega-1} x\right\}$$

   et donc de longueur ω (exceptée l'orbite de 0, qui est toujours réduite à un point indépendemment de ω). Si N compte le nombre d'orbites sauf Ω_0 (celle de 0), on doit avoir $N\omega = \#(K^*) = p - 1$, d'où la signature

$$\varepsilon(D) = \left((-1)^{\omega-1}\right)^N = (-1)^{\omega N - N} = (-1)^{p-1}(-1)^N = (-1)^N \text{ car } p-1 \text{ est pair.}$$

[13] On notera que les transvections n'interviennent pas si $n = 1$.

[14] Il faut savoir en général que la puissance d'une transvection se calcule aisément par $(I_n + \alpha E_{i,j})^k = I_n + k\alpha E_{i,j}$.

Le paramètre crucial est finalement N.

En utilisant la cyclicité de K^*, on peut écrire $\Delta = g^\alpha$ (où g engendre K^*), d'où $g^{\omega\alpha} = \Delta^\omega = 1$ et $N\omega = p-1 \mid \omega\alpha$, ce qui impose $N \mid \alpha$. Ainsi, la parité de N force celle de α, de sorte que Δ est un carré, d'où la réciproque cherchée.

Dans le cas général $n \geq 2$, les orbites d'un vecteur $\binom{x}{\overrightarrow{y}}$ sont toutes de la forme

$$\Omega_{\binom{x}{\overrightarrow{y}}} = \left\{ \binom{x}{\overrightarrow{y}},\ \binom{\Delta x}{\overrightarrow{y}},\ \binom{\Delta^2 x}{\overrightarrow{y}}, \dots, \binom{\Delta^{\omega-1} x}{\overrightarrow{y}} \right\},$$

et on peut refaire le même raisonnement. Il faut juste remarquer qu'en faisant varier $\overrightarrow{y}$ on peut regrouper les orbites par paquets de p^{n-1} qui est impair, ce qui ne change pas la signature.

2. Si l'on se place sur un corps fini K en général, son cardinal est de la forme $q = p^\alpha$ où p est premier et $\alpha \geq 1$ un entier.

Si p est impair, on peut reprendre point par point la démonstration ci-dessus.

Dans le cas contraire, *i. e.* si $p = 2$, le facteur q^{n-1} apparaîssant dans le calcul de $\varepsilon(D)$ pour $n \geq 2$ est pair, donc on aura toujours $\varepsilon(D) = 1$. Pour $n = 1$, avec les mêmes notations que ci-dessus, on a $N\omega = \#K^* = 2^\alpha - 1$, donc ω est impair et toutes les orbites sont de longueur impaire, d'où $\varepsilon(D) = 1$ encore une fois. On notera qu'en fait tous les éléments x de K sont des carrés, puisqu'on peut écrire $x = x^{2^\alpha} = \left(x^{2^{\alpha-1}}\right)^2$. Le résultat reste donc valable pour $p = 2$.

Remarque. Il est coutume, dans ces histoires de carrés modulo un premier, d'introduire le *symbole de Legendre* : pour $a \in \mathbb{F}_p^*$, on définit $\left(\frac{a}{p}\right)$ comme 1 si a est un carré modulo p et -1 sinon. Le théorème de Frobenius-Zotolarev s'énonce alors sous la forme plus concise :

$$\varepsilon(A) = \left(\frac{\det A}{p}\right).$$