Corrigé du DS 4

Problème. Pseudo-inversibilité.

Partie A. Matrices pseudo-inversibles.

1. Unicité de la pseudo-inverse.
   (a) On a supposé que B_1 et B_2 vérifiaient toutes les deux les trois propriétés des pseudo-inverses de A. L'associativité du produit matriciel va nous être utile. D'une part,
   $$AB_1AB_2 = (AB_1A)B_2 \underset{(ii)}{=} AB_2.$$
   D'autre part,
   $$AB_1AB_2 = (AB_1)(AB_2) \underset{(i)}{=} (B_1A)(B_2A) = B_1(AB_2A) \underset{(ii)}{=} B_1A \underset{(i)}{=} AB_1.$$
   On a bien obtenu $AB_1 = AB_2$.
   (b) Attention à la tentation de « simplifier par A » : cette matrice n'est pas inversible ! On remarque, en revanche que le point (iii) ne nous a servi à rien pour l'instant...
   La question précédente donne $AB_1 = AB_2$. En multipliant à gauche par B_1, on obtient $B_1AB_1 = B_1AB_2$, soit d'après (iii),
   $$B_1 = B_1AB_2.$$
   D'autre part, par commutation, la question précédente donne aussi $B_1A = B_2A$. En multipliant à droite par B_2, on obtient
   $$B_1AB_2 = B_2AB_2 \underset{(iii)}{=} B_2.$$
   On a prouvé
   $$B_1 = B_1AB_2 = B_2,$$
   il y a bien unicité de la pseudo-inverse.
   La pseudo-inverse de A sera désormais notée A^* lorsqu'elle existe.

2. Pseudo-inversibilité et inversibilité.
   (a) Soit M une matrice inversible de $M_n(\mathbb{R})$.
   On a que $MM^{-1} = I_n = M^{-1}M$ (i). De plus,
   $$MM^{-1}M = I_nM = M \quad (ii).$$
   Enfin,
   $$M^{-1}MM^{-1} = I_nM^{-1} = M^{-1} \quad (iii).$$
   Ceci montre que notre matrice M est pseudo-inversible et que $M^* = M^{-1}$.
   (b) La matrice 0_n étant la matrice nulle de $M_n(\mathbb{K})$, il est facile de vérifier que
   $$\begin{cases} 0_n0_n & = & 0_n0_n & (i) \\ 0_n0_n0_n & = & 0_n & (ii) \text{ et } (iii) \end{cases}$$
   Ceci montre que 0_n est pseudo-inversible et que $0_n^* = 0_n$.

3. Pseudo-inversibilité des matrices diagonales.
   Posons $N = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix}$.
   Calculer avec des matrices diagonales est aisé : il est facile de vérifier que
   $$MN = NM, \qquad MNM = M, \qquad NMN = N.$$
   Ceci montre que M est pseudo-inversible, d'inverse $M^* = N$. Montrer que M est pseudo-inversible et donner M^*.
   Généralisons. Soit $D = \text{Diag}(d_1, \cdots, d_n)$. On définit $D' = \text{Diag}(d'_1, \cdots, d'_n)$, en posant
   $$\forall k \in [\![1, n]\!] \quad d'_k = \begin{cases} d_k^{-1} & \text{si} \quad d_k \neq 0 \\ 0 & \text{si} \quad d_k = 0 \end{cases}$$
   On a
   $$DD'D = \text{Diag}(d_1d'_1d_1, \cdots, d_nd'_nd_n).$$
   Soit $k \in [\![1, n]\!]$.
   — Si $d_k = 0$, alors $d_kd'_kd_k = 0 = d_k$;
   — et si $d_k \neq 0$, alors $d_kd'_kd_k = d_kd_k^{-1}d_k = d_k$.
   Ceci prouve que $DD'D = D$, et montre le point (ii) de la définition de pseudo-nilpotence. On laisse au lecteur le soin de vérifier (i) et (iii). Ceci achèvera de démontrer que D est pseudo-inversible et que $D^* = D'$.

4. Pseudo-inversibilité et nilpotence.
   Soit N une matrice nilpotente et pseudo-inversible.
   Notons p le *plus petit* entier k tel que $N^k = 0$. On a donc $p \in \mathbb{N}^*$, $N^p = 0$ et $N^{p-1} = 0$.
   Supposons maintenant que $N \neq 0$. Alors $p \geq 2$.
   En suivant l'indication de l'énoncé, on calcule
   $$N^*N^p = N^*NN^{p-1} = NN^*N^{p-1} = (NN^*N)N^{p-2} = NN^{p-2} = N^{p-1}.$$
   Puisque $N^p = 0$, on obtient $N^{p-1} = 0$, ce qui est en contradiction avec la minimalité de p. On a donc prouvé par l'absurde que $N = 0$.

Partie B. Matrices semblables.

1. • Réflexivité. Soit $A \in M_n(\mathbb{R})$. On a $A = I_n A I_n$ et puisque I_n est inversible et est son propre inverse, on a $A = I_n^{-1} A I_n$, ce qui donne $A \sim A$.
   • Symétrie. Soient $A, B \in M_n(\mathbb{R})$ telles que $A \sim B$. Il existe donc une matrice P de $GL_n(\mathbb{R})$ telle que $A = P^{-1}BP$. En multipliant à gauche par P et à droite par P^{-1}, on obtient
   $$PAP^{-1} = \underbrace{PP^{-1}}_{=I_n} B \underbrace{P^{-1}P}_{=I_n},$$
   ce que l'on réécrit
   $$B = (P^{-1})^{-1} A P^{-1}.$$
   Puisque $P^{-1} \in GL_n(\mathbb{R}$, on a bien que $B \sim A$.
   • Transitivité. Soient $A, B, C \in M_n(\mathbb{R})$ telles que $A \sim B$ et $B \sim C$. Alors,
   $$\exists P \in GL_n(\mathbb{R}) : A = P^{-1}BP \quad \text{et} \quad \exists Q \in GL_n(\mathbb{R}) : B = Q^{-1}CQ.$$
   On a donc
   $$A = P^{-1}BP = P^{-1}(Q^{-1}CQ)P = (P^{-1}Q^{-1})C(QP).$$
   Posons $R = QP$. Cette matrice est inversible comme produit de matrices inversibles, d'inverse $R^{-1} = P^{-1}Q^{-1}$. On a donc $A = R^{-1}CR$, ce qui donne $A \sim C$.
2. La classe d'équivalence de la matrice nulle 0_n est l'ensemble des matrices s'écrivant $P^{-1}0_nP$, avec P inversible : cet ensemble est réduit à la matrice nulle.
   Si A est inversible, sa classe d'équivalence
   $$\left\{P^{-1}AP, \quad P \in GL_n(\mathbb{R})\right\}$$
   ne contient que des matrices inversibles, comme produit de matrices inversibles.
3. Soient A et B deux matrices semblables : $\exists P \in GL_n(\mathbb{R}) \quad A = P^{-1}BP$.
   $$\begin{aligned}\mathrm{Tr}(A) &= \mathrm{Tr}(P^{-1}BP)\\ &= \mathrm{Tr}(BPP^{-1}) \qquad \text{en utilisant } \forall (X,Y) \in M_n(\mathbb{R})\ \mathrm{Tr}(XY) = \mathrm{Tr}(YX)\\ &= \mathrm{Tr}(B).\end{aligned}$$
4. La matrice nulle a la même trace que la matrice $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$.
   Elles ne sauraient être semblables, puisque dans la classe d'équivalence de la matrice nulle, il n'y a que la matrice nulle.

Partie C. Une diagonalisation.

1. En échelonnant : P est inversible et $P^{-1} = \frac{1}{2}\begin{pmatrix}1 & 0 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}$.
2. On calcule PA puis PAP^{-1} et on obtient $PAP^{-1} = \begin{pmatrix}0 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 4\end{pmatrix}$.
   Notons D la matrice diagonale obtenue. On a $A = P^{-1}DP$: A est semblable à D.
3. On va proposer un candidat pour la pseudo-inverse.
   Posons $B = P^{-1}D^*P$. On a par exemple
   $$ABA = (P^{-1}DP)(P^{-1}D^*P)(P^{-1}DP) = P^{-1}(DD^*D)P = P^{-1}DP = A.$$
   On vient de vérifier le point (ii) de la définition de pseudo-inversibilité. On laisse au lecteur le soin de vérifier les points (i) et (iii). Ceci prouve que A est pseudo-inversible, et que $B = P^{-1}D^*P$.

Partie D. (***) Pseudo-inversibles... dans un anneau quelconque !

1. • Si a s'écrit pu avec p et u comme il faut, il est facile de vérifier que a est pseudo-inversible, de pseudo-inverse pu^{-1}.
   • Réciproquement, supposons a pseudo-inversible, de pseudo-inverse b.
   Posons $p = ab$. On a $p^2 = (aba)b = ab = p$. Ceci implique notamment $p(1-p) = 0$.
   On a aussi $pa = aba = a$, d'où $(1-p)a = a(1-p) = 0$.
   De même et $pb = abb = bab = b$ d'où $(1-p)b = b(1-p) = 0$.
   Posons $u = a + 1 - p$ et $u' = b + 1 - p$.
   On a $uu' = ab + a(1-p) + b(1-a) + (1-p)^2 = ab + 0 + 0 + 1 - 2p + p^2 = p + 1 - 2p + p = 1$.
   On montre de même que $u'u = 1$. Ceci prouve que $u \in U(A)$. De plus,
   $$pu = ab(a + 1 - p) = aba + 0 = a \quad \text{et } up = (a + 1 - p)ab = aba + 0 = a.$$
2. • Sq a pseudo-inversible. $\exists (p, u) \in A^2 : p^2 = p,\ u \in U(A)\ pu = up,$ et $a = pu$.
   Posons
   $$G = \{pv \mid v \in U(A) \text{ et } pv = vp\}.$$
   On vérifie que G est un groupe, c'est-à-dire un magma associatif et unifère (de neutre p) dans lequel tout élément pv est symétrisable (de symétrique pv^{-1}).
   • Sq a est élément d'un groupe pour le produit, dont on note e le neutre.
   Soit b le symétrique de a dans ce groupe. L'élément a est pseudo-inversible d'inverse b car
   $$ab = e = ba, \qquad aba = ea = a \qquad bab = be = b.$$

Exercice 1 Groupe où tous les éléments sont d'ordre 2.

1. Soient g et g' deux éléments de G.
   L'élément $g \star g'$ est d'ordre 2 par hypothèse, donc $(g \star g')^2 = e$.
   Ceci se récrit (pas de parenthèses car $\star$ est associative).

$$g \star g' \star g \star g' = e.$$

   Composons à gauche par g et à droite par g'. On obtient

$$g^2 \star g' \star g \star (g')^2 = g \star g' \quad \text{donc} \quad e \star g' \star g \star e = g \star g' \quad \text{soit} \quad \boxed{g \star g' = g' \star g}.$$

2. (a) Utilisons la caractérisation des sous-groupes.
   - Le neutre e appartient à $H \cup gH$ puisqu'il appartient à H (qui est un sous-groupe).
   - Soient x et x' dans $H \cup gH$. Montrons que $x \star x' \in H \cup gH$. Quatre cas :
     — Cas où x et x' appartiennent à H.
     Alors $x \star x' \in H$ puisque H est un sous-groupe de G.
     — Cas où $x \in H$ et $x' \in gH$.
     Il existe alors $(h, h') \in H^2$ tel que $x = h$ et $x' = g \star h$. Alors

$$x \star x' = h \star (g \star h') = g \star (h \star h'),$$

     (on a utilisé l'associativité et le fait que G est abélien, comme prouvé en question 1). Puisque $h \star h' \in H$ (H étant un sous-groupe), on a $x \star x' \in gH$.
     — Cas où $x \in gH$ et $x' \in H$.
     On se ramène au cas précédent puisque x et x' commutent.
     — Cas où $x \in gH$ et $x' \in gH$. Il existe alors $(h, h') \in H^2$ tel que $x = g \star h$ et $x' = g \star h$. Alors

$$x \star x' = (g \star h) \star (g \star h') = g^2 \star (h \star h') = h \star h'.$$

     (on a utilisé l'associativité, le fait que G est abélien et $g^2 = e$). On a donc $x \star x' \in gH$.
   Dans les quatre cas $x \star x' \in H \cup gH$.
   - Soient $x \in H \cup gH$. Deux cas :
     — Cas où $x \in H$.
     Alors $x^{-1} \in H$ puisque H est un sous-groupe.
     — Cas où $x \in gH$.
     Alors il existe $h \in H$ tel que $x = g \star h$. On a donc

$$x^{-1} = (g \star h)^{-1} = h^{-1} \star g^{-1} \underset{G \text{ abélien}}{=} g^{-1} \star h^{-1} \underset{g=g^{-1}}{=} g \star h^{-1}.$$

     (on a utilisé à la dernière égalité que g est d'ordre 2). Puisque $h \star h' \in H$, on a $x^{-1} \in gH$.
   Dans les deux cas $x^{-1} \in H \cup gH$.

   Par caractérisation, $\boxed{H \cup gH \text{ est un sous-groupe de } G}$.

(b) • On va d'abord prouver que la réunion est disjointe. Supposons qu'il existe un élément x dans $H \cap (gH)$. Alors, il existe $(h, h') \in H^2$ tel que $x = h$ et $x = g \star h$. On a donc

$$h = g \star h' \quad \text{donc} \quad g = h \star (h')^{-1}.$$

Puisque h et h' appartiennent à H, sous-groupe de G, on obtient $g \in H$, ce qui est en contradiction avec l'hypothèse faite sur cet élément.
Puisque l'union est disjointe, on a

$$|H \cup gH| = |H| + |gH|.$$

• On va maintenant prouver que $|gH| = |H|$.
Il suffit pour cela d'exhiber une bijection entre ces deux ensembles Posons

$$\varphi : \left\{ \begin{array}{ccc} H & \to & gH \\ h & \mapsto & g \star h \end{array} \right. \quad \text{et} \quad \psi : \left\{ \begin{array}{ccc} gH & \to & H \\ x & \mapsto & g^{-1} \star x \end{array} \right. .$$

(on écrit g^{-1} plutôt que g pour plus de clarté mais ces deux éléments sont égaux). On a $\psi \circ \varphi = \mathrm{id}_H$ et $\varphi \circ \psi = \mathrm{id}_{gH}$, ce qui prouve la bijectivité de φ.
On peut désormais conclure que $\boxed{|H \cup gH| = 2 \times |H|}$.

3. Supposons que G est fini.
   Soit H un sous-groupe dont le cardinal est une puissance de 2 de valeur maximale. Cela existe car il existe au moins un sous-groupe dont le cardinal est une puissance de 2 : c'est le sous-groupe trivial $\{e\}$. De plus, le cardinal de H est majoré par celui de G, qui est fini.
   Supposons que $H \neq G$. Alors, on peut considérer un élément g dans $G \setminus H$. La question 3 donne alors que $H \cup gH$ est un sous-groupe de G de cardinal $2 \times |H|$: son cardinal est donc aussi une puissance de 2, ce qui est en contradiction avec la maximalité supposée pour le cardinal de H.
   Par l'absurde, nous avons établi que $H = G$ et donc que

$$\boxed{\text{le cardinal de } G \text{ est une puissance de 2.}}$$

Exercice 2.

1. $\{2,4,7\} \in \mathcal{Q}_3(E_8)$ et $\{2,4,5\} \in \mathcal{P}_3(E_8) \setminus \mathcal{Q}_3(E_8)$.

2. On a $y_1 = x_1 + 1 - 1 = x_1 \geq 1$. On a bien $1 \leq y_1$.
Soit $i \in [\![1, p-1]\!]$. On a
$$y_{i+1} - y_i = (x_{i+1} + 1 - (i+1)) - (x_i + 1 - i) = x_{i+1} - x_i - 1.$$
Or, puisque $x_{i+1} - x_i > 0$ et que $x_{i+1} - x_i \neq 1$ (puisque les entiers x_i et x_{i+1} ne sont pas consécutifs), on a $x_{i+1} - x_i \geq 2$, puis
$$y_{i+1} - y_i \geq 1.$$
On a bien $y_i < y_{i+1}$. De plus, $y_p = x_p + 1 - p$, et puisque $x_p \leq n$, on a $y_p \leq n + 1 - p$.
On a bien démontré
$$1 \leq y_1 < y_2 < \cdots y_p \leq n + 1 - p.$$

3. Lorsque $2p > n+1$, le cardinal de $Q_p(E_n)$ vaut 0 car cet ensemble est vide.
En effet, si $Q_p(E_n)$ est non vide et contient une p-combinaison $\{x_1, \ldots, x_p\}$, la question précédente montre que l'ensemble E_{n+1-p} contient les p entiers deux à deux distincts $y_1, \ldots, y_p$. Ceci amène
$$p \leq n + 1 - p \quad \text{soit} \quad 2p \leq n + 1.$$

4. Posons
$$F : \left\{ \begin{array}{ccc} \mathcal{Q}_p(E_n) & \to & \mathcal{P}_p(E_{n+1-p}) \\ \{x_1, \ldots, x_p\} & \mapsto & \{y_1, \ldots, y_p\} \end{array} \right.$$
où les deux p-combinaisons utilisées pour décrire la fonction sont écrites *dans l'ordre*, et où les y_i ont été définis comme dans la question 2.

   On va justifier que F est une bijection.
   Soit $\{y_1, \ldots, y_p\} \in \mathcal{P}_p(E_{n+1-p})$.
   • Supposons qu'il existe $\{x_1, \ldots, x_p\}$ (écrit dans l'ordre) un antécédent par F de $\{y_1, \ldots, y_p\}$. Alors, par définition de F, on a
   $$\forall i \in [\![1, p]\!] \quad y_i = x_i + 1 - i \quad \text{soit} \quad x_i = y_i + i - 1.$$
   Ceci donne l'unicité de l'antécédent $\{x_1, \ldots, x_p\}$: F est injective.
   • Pour $i \in [\![1, p]\!]$, on pose $x_i = y_i + i - 1$. On vérifie que $\{x_1, \ldots, x_p\} \in \mathcal{Q}_p(E_n)$.
   Tout d'abord, remarquons que
   $$\forall i \in [\![1, p-1]\!] \quad x_{i+1} - x_i = (y_{i+1} + i + 1 - 1) - (y_i + i - 1) = y_{i+1} - y_i + 1.$$
   Or, puisque les y_i sont des entiers deux à deux distincts, on a
   $$\forall i \in [\![1, p-1]\!] \quad x_{i+1} - x_i \geq 2.$$
   Les éléments de $\{x_1, \ldots, x_p\}$ sont donc écrits dans l'ordre et l'ensemble ne contient pas de paire d'entiers consécutifs. On a bien vérifié que $\{x_1, \ldots, x_p\} \in \mathcal{Q}_p(E_n)$ et c'est pas construction un antécédent de $\{y_1, \ldots, y_p\}$: F est surjective.

5. Puisqu'il existe une bijection entre les ensembles $\mathcal{Q}_p(E_n)$ et $\mathcal{P}_p(E_{n+1-p})$, ils ont même cardinal. Ainsi,
$$|\mathcal{Q}_p(E_n)| = |\mathcal{P}_p(E_{n+1-p})| = \binom{n+1-p}{p}.$$

6. Il s'agit de calculer le cardinal de $\mathcal{Q}_5(E_{49+1-5})$. D'après la question précédente,
$$|\mathcal{Q}_5(E_{45})| = \binom{45}{5}.$$

7. On calcule
$$|\mathcal{Q}_5(E_{45})| = \frac{45 \times 44 \times 43 \times 42 \times 41}{5 \times 4 \times 3 \times 2 \times 1} = 3^2 \times 7 \times 11 \times 41 \times 43.$$