Corrigé du problème de Mathématiques générales 2010

Matthieu Romagny, 7 septembre 2014

Partie I.

1.(a) On a $XA = XX^n = X^nX = AX$.

1.(b) Le polynôme $m_A(x^n)$ est annulateur de X donc il est divisible par m_X.

1.(c) Pour $a \in K$ notons $M_a := aE_{1,p} \in M_p(K)$ la matrice dont le seul terme non nul est celui d'indice $(1,p)$ égal à a. Comme K est infini, les matrices M_a sont en nombre infini. Comme $p \geqslant 2$, ces matrices sont nilpotentes d'ordre 2. Enfin comme $n \geqslant 2$, on a $(M_a)^n = 0$. On obtient une infinité de matrices dans S_{0_p}.

1.(d) Si $S_{\lambda I_p} \neq \varnothing$, soit X telle que $X^n = \lambda I_p$. Alors $r := \det(X)$ est une racine de $x^n - \lambda^p$. Réciproquement, supposons que $x^n - \lambda^p$ possède une racine r. Si $\lambda \neq 0$, choisissons un couple de Bézout $(u,v) \in \mathbb{Z}^2$ tel que $up + vn = 1$ et posons $s = r^u\lambda^v$. Si $\lambda = 0$, posons $s = 0$. On vérifie alors que $s^n = \lambda$ dans tous les cas. Ainsi la matrice $X := sI_p$ est dans $S_{\lambda I_p}$.

2.(a) Si $A' = PAP^{-1}$ avec $P \in \mathrm{GL}_p(K)$, on a les équivalences :

$$X \in S_A \iff X^n = A \iff (PXP^{-1})^n = PX^nP^{-1} = A' \iff PXP^{-1} \in S_{A'}.$$

Ceci montre que $S_{A'} = \{PXP^{-1},\ X \in S_A\}$.

2.(b) On a $(PXP^{-1})^n = PAP^{-1}$, donc $PXP^{-1} \in S_A$ si et seulement si $PAP^{-1} = A$ i.e. $P \in C(A)$.

3.(a) L'énoncé est clair pour $r = 1$. Si $P \in K[x]$ est de degré $r \geqslant 2$, en adjoignant à K une racine de P on obtient un corps K' avec $[K' : K] \leqslant r$ tel que l'on peut écrire $P = (x-\alpha)P'$ dans $K'[x]$. Par récurrence, le corps de décomposition K'' de P' sur K' est de degré $\leqslant (r-1)!$. Or le corps de décomposition de P sur K est inclus dans K'', donc son degré sur K est $\leqslant [K'' : K] = [K'' : K']\,[K' : K] \leqslant (r-1)!r = r!$.

Dans la suite, nous utiliserons souvent et sans le répéter le fait que, sur un corps de base *infini*, un polynôme est déterminé par sa fonction polynôme associée (à laquelle on peut donc l'identifier).

3.(b) Une fonction polynôme non nulle en $d = 1$ variable prend une valeur non nulle sur K car celui-ci est infini. Par récurrence, soit $f \in \mathbb{C}[x_1, \ldots, x_d]$ avec $d \geqslant 2$. En privilégiant la variable x_d, on peut écrire f comme une somme de monômes $f_i(x_1, \ldots, x_{d-1})(x_d)^i$. Si la fonction polynôme associée à f est non nulle sur $\mathbb{C}^d$, l'une des fonctions f_i est non nulle sur $\mathbb{C}^{d-1}$. Par hypothèse de récurrence, il existe $(\lambda_1, \ldots, \lambda_{d-1}) \in K^d$ en lequel f_i ne s'annule pas. Alors $f(\lambda_1, \ldots, \lambda_{d-1}, x_d) \in \mathbb{C}[x_d]$ est non nulle sur $\mathbb{C}$ donc sur K.

3.(c) Sur L, le polynôme minimal $m_A = m_{A'}$ devient scindé. D'après le théorème de Jordan, il existe des matrices de Jordan $J, J' \in M_p(L)$ et $P, Q \in \mathrm{GL}_p(L)$ telles que $A = PJP^{-1}$ et $A' = QJ'Q^{-1}$. Comme A et A' sont semblables sur $\mathbb{C}$, l'assertion d'unicité du théorème dit que $J' = MJM^{-1}$ pour une certaine matrice de permutation $M \in \mathrm{GL}_p(\mathbb{Q})$. Finalement $A' = RAR^{-1}$ avec $R = QMP^{-1} \in \mathrm{GL}_p(L)$.

3.(d) D'après (c) on peut choisir $P \in \mathrm{GL}_p(L)$ telle que $A' = PAP^{-1}$, i.e. $A'P = PA$. Soit $e_1, \ldots, e_d$ une K-base de L où $d = [L : K]$, et écrivons $P = P_1e_1 + \cdots + P_de_d$ avec $P_i \in \mathrm{GL}_p(K)$. Comme $\{e_i\}$ est K-libre, l'égalité $A'P = PA$ est équivalente à : $A'P_i = P_iA$ pour tout $i \in \{1 \ldots d\}$. Il s'ensuit que, si $x_1, \ldots, x_d$ sont des indéterminées, on a $A'(P_1x_1 + \cdots + P_dx_d) = (P_1x_1 + \cdots + P_dx_d)A$. Comme la fonction polynomiale $f(x_1, \ldots, x_d) = \det(P_1x_1 + \cdots + P_dx_d)$ ne s'annule pas en $(e_1, \ldots, e_d)$, d'après (b) il existe une valeur $(\lambda_1, \ldots, \lambda_d) \in K^d$ où f ne s'annule pas. Alors on a $A'Q = QA$ avec $Q = \lambda_1P_1 + \cdots + \lambda_dP_d \in \mathrm{GL}_p(K)$, i.e. A et A' sont semblables sur K.

Commentaire : il s'agit d'un truc assez classique, que l'on peut trouver par exemple dans [Gou]*, problème 11 du chap. 3 (c'est le problème 10 dans la première édition du livre). Une variante de la même preuve se trouve dans* [FGN2]*, exercice 2.15. Si K est un corps fini le résutat est encore vrai et se prouve à l'aide de la réduction de Frobenius, pour laquelle on peut consulter par exemple* [MM]*, chap. XI,* [ADG]*, chap. 4.3,* [Sz]*, chap. 11, par. XI.2 ou* [Gou]*, Annexe B, notamment B.3.2.*

4.(a) Soit J une matrice de Jordan. Pour chacune de ses valeurs propres a, notons $k(a)$ la plus grande des tailles k des blocs de Jordan $J_k(a)$ relatifs à a qui apparaissent dans J. Alors le polynôme minimal m_J est le produit des $(x-a)^{k(a)}$, portant sur les valeurs propres distinctes. Ainsi lorsque le polynôme minimal $m = m_J$ est fixé, la matrice J est déterminée par les tailles $k < k(a)$ des blocs $J_k(a)$ des différentes valeurs propres. En particulier il y a un nombre fini de matrices de Jordan $J_1, \dots, J_N$ de polynôme minimal m. Utilisons la notation $O_G(x)$ pour l'orbite d'un point $x \in X$ sous l'action d'un groupe G agissant sur un ensemble X ; ainsi $O_{\mathrm{GL}_p(\mathbb{C})}(J)$ est la classe de similitude complexe d'une matrice J. Par le théorème de Jordan et le raisonnement précédent, dans $M_p(\mathbb{C})$ l'ensemble des matrices de polynôme minimal m fixé est la réunion finie des classes de $\mathbb{C}$-similitude $O_{\mathrm{GL}_p(\mathbb{C})}(J_i)$, $i = 1, \dots, N$. La question 3.(d) montre que la classe de K-similitude d'une matrice $A \in M_p(K)$ est l'intersection avec $M_p(K)$ de la classe de $\mathbb{C}$-similitude de sa forme de Jordan J. Les classes de K-similitude des matrices de $M_p(K)$ de polynôme minimal m sont donc égales à ceux des ensembles $O_{\mathrm{GL}_p(\mathbb{C})}(J_i) \cap M_p(K)$ qui sont non vides ; il y en a un nombre fini.

4.(b) D'après la question 1.(b) les polynômes minimaux des éléments de S_A sont des diviseurs de $m_A(x^n)$; ils sont donc en nombre fini. D'après 4.(a) il y a donc un nombre fini de classes de similitude $O_{\mathrm{GL}_p(K)}(M)$ qui rencontrent S_A. Comme S_A est stable par conjugaison par des éléments de $\mathrm{GL}_p(K)$, il est réunion des ensembles $O_{\mathrm{GL}_p(K)}(M) \cap S_A$, en nombre fini. Or la question 2.(b) montre qu'on a $O_{\mathrm{GL}_p(K)}(M) \cap S_A = O_{C(A)}(M) \cap S_A$, d'où le résultat.

5.(a) L'hypothèse de la question implique que les orbites des éléments de S_A sous $C(A)$ sont des points, donc la question 4.(b) donne le résultat.

5.(b) Nous utiliserons le fait suivant : si une fraction rationnelle $f = r/s \in K(x)$ est non constante, elle prend une infinité de valeurs sur K. Ceci découle du fait que si f prend un nombre fini de valeurs $a_1, \dots, a_n$ alors la fonction associée au polynôme $g = \prod_{i=1}^n (r - a_i s)$ est identiquement nulle, donc $g = 0$ i.e. $f = a_i$ pour un i. Passons à la question proprement dite. Comme $Y^n = A$, on a $C(Y) \subset C(A)$; donc l'hypothèse signifie qu'il existe $P \in C(A) \backslash C(Y)$. Soit x une indéterminée. Le polynôme $d(x) = \det(I_p + xP)$ est non nul puisque $d(0) = 1$, donc $I_p + xP \in \mathrm{GL}_p(K(x))$. La matrice $F(x) = (I_p + xP)Y(I_p + xP)^{-1}$ est non constante (i.e. n'appartient pas à $\mathrm{GL}_p(K)$) puisque $F'(0) = PY - YP \neq 0$. Donc l'une de ses composantes $f = F_{ij} \in K(x)$ est non constante. Par le fait énoncé au début, f prend une infinité de valeurs sur K, donc F prend une infinité de valeurs, qui, comme $P \in C(A)$, sont toutes dans S_A.

6.(a) Soit $q \in \mathbb{Q}[x]$ le développement limité de $(1+x)^{1/n}$ à l'ordre $p-1$, i.e. $(1+x)^{1/n} = q(x) + x^p r(x)$. En élevant à la puissance n on trouve $1 + x = q(x)^n + x^p r'(x)$. En évaluant cette égalité en la matrice N_p de puissance p-ème nulle, on obtient $I_p + N_p = q(N_p)^n$.

6.(b) On recherche une matrice B telle que $B^n = A$. Comme A est semblable à une matrice de Jordan J, en travaillant bloc par bloc il suffit de traiter le cas où $A = J_p(a)$ pour un $a \in \mathbb{C}$. Comme A est inversible, on a $a \neq 0$. En choisissant une racine n-ème complexe b de a, ce qui est possible car $\mathbb{C}$ est algébriquement clos, et en remplaçant A par $b^{-1}A$, on peut même supposer que $a = 1$. Dans ce cas, le résultat est donné par 6.(a).

Partie II.

1. Soit $|\cdot|$ une norme sur $\mathbb{C}^n$, par exemple la norme du sup ou la norme hermitienne standard. Toute matrice $B \in M_p(\mathbb{C})$ définit une application linéaire de $\mathbb{C}^p$ qui est continue (dimension finie) donc atteint son sup sur la boule unité de $\mathbb{C}^p$. On peut poser $N(B) = \sup_{|x|=1} |Bx|$. On vérifie immédiatement que $N(BC) \leqslant N(B)N(C)$.

2.(a) Comme X_0 commute avec A, la sous-$\mathbb{C}$-algèbre $B := \mathbb{C}[A, X_0]$ de $M_p(\mathbb{C})$ est commutative. Il est clair que tous les X_k appartiennent à B. De plus, comme tout sous-espace vectoriel en dimension finie, B est fermée dans $M_p(\mathbb{C})$ pour la topologie standard de $\mathbb{C}$-espace vectoriel. Il s'ensuit que $Y = \lim X_k$ est aussi dans B. Finalement $X_k, X_{k'}, Y, A$ sont toutes dans l'algèbre commutative B donc commutent deux à deux.

2.(b) Par continuité de la fonction $F(X) = (1 + 1/n)X - (1/n)BX^{n+1}$, la limite Y vérifie $Y = (1 + 1/n)Y - (1/n)BY^{n+1}$. Comme Y est supposée inversible, on en déduit que $Y^n = B^{-1} = A$.

2.(c) Substituons $X_k = (U_k + I_p)Y$ (pour tout k) dans la relation qui définit X_{k+1}. On trouve :

$$(U_{k+1} + I_p)Y = (1 + 1/n)(U_k + I_p)Y - (1/n)B((U_k + I_p)Y)^{n+1}.$$

Comme $U_k + I_p$ et Y commutent on peut distribuer la puissance $n+1$-ème. Utilisant de plus le fait que $BY^n = I_p$ et multipliant par nY^{-1}, la relation ci-dessus devient :

$$n(U_{k+1} + I_p) = (n+1)(U_k + I_p) - (U_k + I_p)^{n+1}$$

Compte tenu de la formule du binôme de Newton pour $(U_k + I_p)^{n+1}$, c'est la relation demandée.

3.(a) L'idée naturelle est d'utiliser une étude de fonction. Puisqu'on cherche une solution parmi les $r > 0$, on peut diviser par r l'égalité de l'énoncé, ce qui rendra la dérivée plus simple. Posons donc $f(x) = -n + \sum_{j=2}^{n+1} \binom{n+1}{j} x^{j-1}$. Alors $f'(x) = \sum_{j=2}^{n+1} (j-1)\binom{n+1}{j} x^{j-2}$ qui est > 0 pour $x > 0$. Ainsi f est strictement croissante sur $[0, +\infty[$, avec $f(0) = -n$ et de limite $+\infty$ en l'infini. Donc f possède un unique zéro $r > 0$. (Si on n'avait pas divisé par r il faudrait aller jusqu'à f'' pour l'étude de signe.)

3.(b) La fonction définie par $g(x) = (1/n)\sum_{j=2}^{n+1} \binom{n+1}{j} x^j$ a sa dérivée nulle en $x = 0$ et > 0 pour $x > 0$. Donc g est strictement croissante sur $[0, +\infty[$. De plus d'après la question 3.(a) les seuls points de rencontre sur $[0, +\infty[$ entre la courbe de g et la diagonale sont $x = 0$ et $x = r$. Comme $g'(0) = 0$, on en déduit que la courbe de g est tout entière située sous la diagonale. (DESSIN.) On déduit que g stabilise l'intervalle compact $[0, r]$, la suite récurrente définie par $x_0 \in [0, r]$ et $x_{k+1} = g(x_k)$ est décroissante, bornée, donc convergente. Sa limite est solution de $g(r) = r$, donc c'est 0 puisque $x_0 < r$.

4. Notons que Y est inversible, puisque $Y^n = A$ et A est supposée inversible dans toute la partie II. Considérons $\alpha = r/N(Y^{-1})$. Dès que $N(X_0 - Y) < \alpha$, on a $N(U_0) \leqslant N(X_0 - Y)N(Y^{-1}) < r$ et on a une suite récurrente (x_k) bien définie comme dans 3.(b) avec $x_0 = N(U_0) < r$. Montrons par récurrence que $N(U_k) \leqslant x_k$ pour tout k. Le cas $k = 0$ est clair, puis pour $k \geqslant 1$, d'après 2.(c) :

$$N(U_{k+1}) = \frac{1}{n} N\left(\sum_{j=2}^{n+1} \binom{n+1}{j} U_k^j\right) \leqslant \frac{1}{n} \sum_{j=2}^{n+1} \binom{n+1}{j} x_k^j = x_{k+1}.$$

On en déduit que $N(U_k)$ converge vers 0, donc X_k converge vers Y.

Partie III.

Commentaire : un vecteur $v \in K^p$ tel que $(A^j v)_{0 \leqslant j < p}$ soit une base de K^p est appelé un vecteur cyclique, *et un endomorphisme qui possède un vecteur cyclique est appelé un endomorphisme* cyclique. *La théorie de base de ces endomorphismes est décrite par exemple dans* [MM], *chap. VI ou dans* [Gou], *Annexe B. Voir aussi* [FGN2], *exercice 2.38 et les références mentionnées plus haut au sujet de la réduction de Frobenius.*

1.(a) Comme $\mathscr{B} := (A^j v)_{0 \leqslant j \leqslant p-1}$ est une base, il existe p scalaires h_i tels que $Xv = \sum_{j=0}^{p-1} h_j A^j v$. Posons $h(x) = \sum_{j=0}^{p-1} h_j x^j$. Pour tout $k \in \{0, \ldots, p-1\}$ on a $XA^k v = A^k Xv = A^k \sum_{j=0}^{p-1} h_j A^j v = h(A)A^k v$. On en déduit que $X = h(A)$ puisque c'est vrai sur tous les éléments de la base $\mathscr{B}$.

1.(b) Considérons le morphisme de K-algèbres $u : K[x] \to M_p(K)$ défini par $u(h) = h(A)$. Le noyau est par définition l'idéal engendré par m_A, donc u induit un morphisme injectif $u' : K[x]/(m_A) \hookrightarrow M_p(K)$ qui envoie $\overline{x}$ sur A. D'après (a) les éléments de S_A sont dans l'image de u', et ils correspondent aux $z \in K[x]/(m_A)$ tels que $z^n = \overline{x}$.

1.(c) Posons $K' := K[x]/(m_A)$. Si m_A est irréductible, alors K' est un corps. Donc l'équation $Z^n = \overline{x}$ possède au plus n racines dans ce corps, i.e. $\mathrm{card}(S_A) \leqslant n$. Supposons m_A produit de s polynômes irréductibles distincts $m_1, \ldots, m_s$. Comme les m_i sont premiers entre eux deux à deux, d'après le théorème des restes chinois on a un isomorphisme de K-algèbres $v : K' \xrightarrow{\sim} K[x]/(m_1) \times \cdots \times K[x]/(m_s)$. Comme les m_i sont irréductibles, chaque facteur $K_i := K[x]/(m_i)$ est un corps. Les $z \in K'$ tels que $z^n = \overline{x}$ correspondent par v aux uplets $(z_1, \ldots, z_s)$ avec $z_i \in K_i$ tels que $z_i^n = \mathrm{cl}_i(x)$, où $\mathrm{cl}_i(x)$ désigne la classe de x modulo m_i. Il y a n^s tels uplets, d'où le résultat.

Commentaire : un endomorphisme dont le polynôme minimal est sans facteur carré i.e. est produit de polynômes irréductibles distincts est appelé un endomorphisme semi-simple. *La théorie de base de ces endomorphismes est décrite par exemple Gourdon* [Gou]*, problème 19 du chap. 4. Dans le cas où le polynôme caractéristique est scindé, voir aussi* [FGN2]*, exercice 2.37.*

1.(d) Soit $z \in K[x]/(m_A)$ tel que $z^n = \overline{x}$. Soit $f \in K[x]$ un représentant de z modulo $m_A = x^p$, donc il existe $g \in K[x]$ tel que $f^n = x + x^p g$. Cette égalité implique que x divise f, et alors x^n divise f^n, ce qui contredit $f^n = x + x^p g$ si $n \geqslant 2$. Donc S_A est vide.

1.(e) On cherche y_2 sous la forme $y_2 = y_1 + f^r q$, ce qui assure la congruence $y_2 \equiv y_1 \mod f^r$. Comme $y_1^n \equiv g \mod f^r$, il existe α tel que $y_1^n = g + f^r\alpha$. On a alors $y_2^n = (y_1 + f^r q)^n = y_1^n + n y_1^{n-1} f^r q + f^{2r}\beta = g + (\alpha + n y_1^{n-1} q) f^r + f^{2r}\beta$ pour un certain β. Pour assurer la congruence $y_2^n \equiv g \mod f^{r+1}$, il faut et il suffit de trouver q tel que f divise $\alpha + n y_1^{n-1} q$. Ceci signifie que $\overline{\alpha} + n\overline{y}_1^{n-1}\overline{q} = 0$ dans $K' := K[x]/(f)$. Or comme f et g sont premiers entre eux, l'élément $\overline{g} \in K'$ est inversible. Comme $\overline{y}_1^n = \overline{g}$, il en va de même de $\overline{y}_1$. Il est donc légitime de poser $\overline{q} := -(1/n)\overline{\alpha}(1/\overline{y}_1)^{n-1}$. Ce choix de q est unique modulo f et détermine un y_2 solution, unique modulo f^{r+1}.

1.(f) Soit $m_A = (m_1)^{d_1} \dots (m_s)^{d_s}$ la décomposition de m_A en irréductibles dans $K[x]$. Posons $A' = K[x]/(m_A)$, $A_i = K[x]/(m_i^{d_i})$ et $K_i = K[x]/(m_i)$ qui est un corps, quotient de A_i. Comme les $m_i^{d_i}$ sont premiers entre eux deux à deux, on a l'isomorphisme du théorème des restes chinois $v : A' \xrightarrow{\sim} A_1 \times \dots \times A_s$. Les $z \in A'$ tels que $z^n = \overline{x}$ correspondent par v aux uplets $(z_1, \dots, z_s)$ avec $z_i \in A_i$ tels que $z_i^n = \mathrm{cl}_i(x)$. D'après la question 1.(e), pour chaque i fixé l'application $A_i \to K_i$ de réduction modulo m_i établit une bijection entre les $z_i \in A_i$ tels que $z_i^n = \mathrm{cl}_i(x)$ (classe mod $m_i^{d_i}$) et les $z_i' \in K_i$ tels que $(z_i')^n = \mathrm{cl}_i'(x)$ (classe mod m_i). Comme le nombre des z_i' est $\leqslant n$ d'après 1.(b), finalement la bijection $z \mapsto (z_1', \dots, z_s')$ montre que le nombre de z tels que $z^n = \overline{x}$, c'est-à-dire le cardinal de S_A, est au plus n^s.

2. L'analyse faite dans la question 1.(f) est encore valable. Par hypothèse, les facteurs de la décomposition $m_A = (m_1)^{d_1} \dots (m_s)^{d_s}$ en irréductibles dans $\mathbb{R}[x]$ sont tous de degré 2. Les corps résiduels K_i sont donc tous isomorphes à $\mathbb{C}$. Alors, l'extraction de racines n-èmes $z_i' \in K_i$ est toujours possible (le nombre de ces racines est 0 ou n selon que $\mathrm{cl}_i'(x)$ est nul ou pas). On peut donc fabriquer une solution z, donc un élément de S_A.

3.(a) Avec la formule trigonométrique de duplication on trouve $a_{n+1} = 2(2\cos^2(2^n r\pi) - 1) = a_n^2 - 2$. Utilisant ceci et le fait que $a_0 = 2s \in \mathbb{Q}$, on voit par récurrence que $a_n \in \mathbb{Q}$ pour tout $n \geqslant 0$. Pour montrer la périodicité, mettons r sous la forme $r = a/(2^m b)$ avec $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ impair non nul, et $m \geqslant 0$. Comme 2 est premier avec b, le petit théorème de Fermat donne $2^{\varphi(b)} \equiv 1 \mod b$. Posons $T := \varphi(b)$, et fixons $k \in \mathbb{Z}$ tel que $2^T - 1 = kb$. Pour tout $n \geqslant 1$, on a : $(2^T - 1)2^{n+m} r\pi = 2^n ak\pi \in 2\pi\mathbb{Z}$. Il s'ensuit que $2^{n+T+m} r\pi \equiv 2^{n+m} r\pi \mod 2\pi\mathbb{Z}$ donc $\cos(2^{n+T+m} r\pi) = \cos(2^{n+m} r\pi)$, c'est-à-dire que $a_{n+m+T} = a_{n+m}$ pour tout $n \geqslant 1$. Ceci exprime que (a_n) est périodique de période T à partir du rang $m + 1$.

3.(b) L'entier b_n est caractérisé par l'écriture $a_n = c_n/b_n$ avec $b_n > 0$ et c_n inversible modulo b_n. Alors $a_{n+1} = (c_n^2 - 2b_n^2)/b_n^2$ où $b_n^2 > 0$ et $c_n^2 - 2b_n^2 \equiv c_n^2 \mod b_n$ est encore inversible modulo b_n. Ceci montre que b_n^2 est le dénominateur > 0 de la forme irréductible de a_{n+1}^2.

3.(c) De la question précédente on déduit que $b_n = (b_0)^{2^n}$ pour tout $n \geqslant 0$. Comme a_n est périodique à partir de $n = m + 1$, alors b_n l'est aussi. En particulier b_n est bornée, donc $b_0 = 1$. De plus, on sait que $2s = a_0 = c_0/b_0 = c_0 \in \mathbb{Z}$. Comme $|s| = |\cos(r\pi)| \leqslant 1$ on a finalement $|s| \in \{0, 1/2, 1\}$.

4.(a) Pour $K = \mathbb{R}$ on peut identifier l'espace $E = K^2$ à $\mathbb{C}$ muni de sa $\mathbb{R}$-base $\{1, i\}$, et l'endomorphisme A agissant sur E à la multiplication par i. Soient les matrices de multiplication par les racines n-èmes de i :

$$M_k = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix}, \qquad \theta_k = (4k+1)\frac{\pi}{2n}, \qquad k = 0, \dots, n-1.$$

On a $M_0, \dots, M_{n-1} \in S_A$, or $\mathrm{card}(S_A) \leqslant n$ d'après 1.(c), donc $S_A = \{M_0, \dots, M_{n-1}\}$.

4.(b) Notons $S_A(L)$ l'ensemble des racines n-èmes de A dans une extension L/K. On a donc $S_A(\mathbb{Q}) = S_A(\mathbb{R}) \cap M_2(\mathbb{Q})$. Soit $X \in S_A(\mathbb{R})$ l'une des matrices décrites dans 4.(a). Compte tenu de 3.(c), pour que $X \in M_2(\mathbb{Q})$ on doit avoir $|\cos(\theta_k)| \in \{0, 1/2, 1\}$. Discutons les cas.

i) $|\cos(\theta_k)| = 0$. Alors $\theta_k = (2u+1)\pi/2$, $u \in \mathbb{Z}$. Comme $0 \leqslant k \leqslant n-1$, on doit avoir $u = 0$ ou $u = 1$.
- $u = 0$: $n \equiv 1\,(4)$, $k = (n-1)/4$, $\theta_k = \pi/2$, $X = A$.
- $u = 1$: $n \equiv 3\,(4)$, $k = (3n-1)/4$, $\theta_k = 3\pi/2$, $X = -A$.

ii) $|\cos(\theta_k)| = 1/2$. Dans ce cas on a $\sin(\theta_k) \notin \mathbb{Q}$, donc $X \notin M_2(\mathbb{Q})$.

iii) $|\cos(\theta_k)| = 1$. Alors $\theta_k = u\pi$, $u \in \mathbb{Z}$. On en déduit $4k+1 = 2nu$, ce qui est impossible par parité.

En conclusion $S_A = \{A\}$ si $n \equiv 1\,(4)$, $S_A = \{-A\}$ si $n \equiv 3\,(4)$, et $S_A = \varnothing$ sinon.

4.(c) Commençons par diagonaliser A : on a $m_A = x^2+1$ et $P^{-1}AP = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ avec $P = \frac{1}{2}\left(\begin{smallmatrix} 1 & 1 \\ -i & i \end{smallmatrix}\right)$. Comme m_X divise $m_A(x^n) = x^{2n}+1$, il est à racines simples donc X est diagonalisable. Comme X commute avec A, elle est codiagonalisable avec A. La restriction de X à $\ker(A - iI_2)$ peut être n'importe quelle homothétie de rapport une racine n-ème de i, i.e. $e^{i\theta_k}$ avec $0 \leqslant k \leqslant n-1$. La restriction de X à $\ker(A + iI_2)$ peut être n'importe quelle homothétie de rapport une racine n-ème de $-i$, i.e. $e^{i(\theta_l - \pi/n)}$ avec $0 \leqslant l \leqslant n-1$. Finalement S_A est composé des n^2 matrices $P\left(\begin{smallmatrix} \exp(i\theta_k) & 0 \\ 0 & \exp(i(\theta_l - \pi/n)) \end{smallmatrix}\right)P^{-1}$, $0 \leqslant k, l \leqslant n-1$.

Partie IV.

1.(a) On a $X^{nk} = A^k = 0$ donc X est nilpotente. Si r est son indice de nilpotence, on a donc $m_X = x^r$. Comme $X^{nk} = 0$, on a $r \leqslant nk$ et comme $X^{(k-1)n} = A^{k-1} \neq 0$, on a $(k-1)n < r$.

1.(b) Par Cayley-Hamilton, on a $r \leqslant p$. Donc par ce qui précède, si $S_A \neq \varnothing$ on a $(k-1)n < p$.

2.(a) Si $n \geqslant p$, on a $X^n = 0$ donc $\mathrm{Mat}_{\mathcal{B}}(X^n) = 0$. Si $n < p$, $\mathrm{Mat}_{\mathcal{B}}(X^n) = \sum_{i=n+1}^{p} E_{i,i-n}$ où $E_{i,j}$ désigne la matrice élémentaire dont le seul coefficient non nul est celui d'indice (i,j).

2.(b) Si $n \geqslant p$, il n'y a rien à dire. Si $n < p$, on note $p = nq + r$, avec $0 \leqslant r < n$, la division euclidienne de p par n. Pour jordaniser X^n il suffit de trouver la partition de $(X^j v)_{0 \leqslant j < p}$ en itérés de l'endomorphisme X^n. (On aimerait parler d'*orbites* sous X^n mais celui-ci n'étant pas inversible n'engendre pas un sous-groupe de $\mathrm{GL}_p(K)$.) Les r premiers vecteurs $X^j v$ avec $0 \leqslant j \leqslant r-1$ ont des « orbites » de cardinal $q+1$:

$$A_j = \{X^j v, X^{n+j} v, X^{2n+j} v, \ldots, X^{(q-1)n+j} v, X^{qn+j} v\}.$$

Les $n-r$ vecteurs suivants, qui sont $X^j v$ avec $r \leqslant j \leqslant n-1$, ont des « orbites » de cardinal q :

$$A'_j = \{X^j v, X^{n+j} v, X^{2n+j} v, \ldots, X^{(q-1)n+j} v\}.$$

Dans la base $\mathcal{B}' = A'_r \cup \cdots \cup A'_{n-1} \cup A_0 \cup \cdots \cup A_{r-1}$, la matrice de X^n est en forme de Jordan avec pour blocs de Jordan $n-r$ fois N_q et r fois N_{q+1}. En dessin : $X^n \sim \mathrm{diag}(\underbrace{N_q, \ldots, N_q}_{n-r}, \underbrace{N_{q+1}, \ldots, N_{q+1}}_{r})$.

2.(c) Ici $p = 4$ et $m_A = x^2$, donc $k = 2$. Soit $X \in S_A$. D'après 1.(b), $S_A = \varnothing$ si $n \geqslant 4$. Si $n = 1$, $S_A = \{A\}$ est non vide. Si $n = 2$, on voit que $A = (P^{-1}N_4P)^2$ où P est la matrice de la transposition $(2,3)$, donc $S_A \neq \varnothing$. Si $n = 3$, si $X \in S_A$ on a $A = X^3 \neq 0$, et un vecteur v tel que $X^3 v \neq 0$ engendre une base $\{v, Xv, X^2v, X^3v\}$ dans laquelle la matrice de X est N_4. Alors X^3 est de rang 1, ce qui n'est pas le cas de A, donc $S_A = \varnothing$. L'ensemble demandé est donc $\{1, 2\}$.

3.(a) Le calcul direct montre que $\dim\ker(N_k^i) = \min(i,k)$. On déduit que $\dim\ker(A^i) = \sum_{j=1}^{r} \min(i, k_j)$ puis $d_i = \sum_{j=1}^{r} \min(i,k_j) - \min(i-1, k_j)$. Étant donné que $\min(i,e) - \min(i-1,e)$ vaut 1 si $i \leqslant e$ et 0 si $i \geqslant 0$, on obtient $d_i = \mathrm{card}\{j \leqslant r \text{ t.q. } i \leqslant k_j\}$.

3.(b) Soit $X \in S_A$. Nous allons comparer les d_i aux sauts de dimension analogues $\delta_i := \dim\ker X^i - \dim\ker X^{i-1}$. Notons que d'après 3.(a), la suite (d_i) est décroissante, et de même pour la suite (δ_i). On a :

$$d_i = \dim\ker X^{ni} - \dim\ker X^{n(i-1)} = \delta_{ni} + \delta_{ni-1} + \cdots + \delta_{n(i-1)+1}.$$

Par décroissance, on trouve $n\delta_{ni} \leqslant d_i \leqslant n\delta_{n(i-1)+1}$. S'il existe $s \geqslant 0$ tel que $ns < d_{i+1} \leqslant d_i < n(s+1)$, alors on trouve $ns < d_{i+1} \leqslant n\delta_{ni+1} \leqslant n\delta_{ni} \leqslant d_i < n(s+1)$. En particulier $s < \delta_{ni} < s+1$, ce qui est impossible. Par contraposée, pour tout $s \geqslant 0$ il existe au plus un i tel que $d_i \in]ns, n(s+1)[$. Notons que cette condition implique en particulier que si deux d_i d'indices distincts sont égaux, alors cette valeur commune d est multiple de n.

3.(c) Posons $A = J$. Ici $d_1 = d_2 = 3$, $d_3 = 1$ et $d_i = 0$ si $i \geqslant 4$. D'après 3.(b), si $S_J \neq \varnothing$ il y a au plus un d_i dans chacun des intervalles $]ns, n(s+1)[$. En particulier, en regardant $s = 0$ on voit que $n \leqslant 3$ et en regardant $s = 1$ on voit que $n \neq 2$. Pour $n = 1$, $S_J = \{J\}$ est non vide. Il ne reste que le cas $n = 3$. Utilisant 2.(b) pour $X = N_p$ avec $n = 3$, $r = 1$, $q = 2$ on voit que la réduction de Jordan de $(N_7)^3$ est égale à J. Donc $S_J \neq \varnothing$. L'ensemble demandé est l'ensemble des entiers $\neq 0, 1, 3$.

3.(d) En utilisant I.2.(a), on peut se ramener au cas où A est en forme de Jordan. On fait une récurrence sur le nombre r de blocs. Si $r < n$, on a $d_1 = r < n$, donc $d_2 < d_1$ (voir l'observation finale de 3.(b)), et ainsi $d_2 = 0$ encore d'après 3.(b). Ceci implique que tous les blocs sont de taille 1, i.e. $A = 0$ donc $S_A \neq \varnothing$.

Supposons maintenant $r \geqslant n$. On suppose les blocs ordonnés par taille croissante. Soit $\kappa = \sup k_i$ la plus grande taille des blocs de Jordan.

Si $d_\kappa \geqslant n$, les n derniers blocs (en bas à droite) sont de taille κ et forment une matrice qui est la puissance n-ème de $N_{n\kappa}$, d'après 2.(b). Pour la matrice formée par les $r-n$ blocs en haut à gauche, on a $d'_i = d_i - n$ donc l'hypothèse (d'existence pour tout $s \geqslant 0$ d'au plus un indice tel que...) est conservée ; ainsi on conclut par l'hypothèse de récurrence.

Si $d_\kappa < n$, l'hypothèse implique que $d_{\kappa-1} \geqslant n$. Alors les d_κ blocs de taille κ ainsi que les $n - d_\kappa$ derniers blocs de taille $\kappa - 1$ forment une matrice qui est la puissance n-ème de $N_{n(\kappa-1)+d_\kappa}$, d'après 2.(b). Pour la matrice formée par les blocs restants en haut à gauche, on a ici encore $d'_i = d_i - n$ donc l'hypothèse est conservée et on conclut par l'hypothèse de récurrence.

4. Soit k la multiplicité de x dans m_A, i.e. $m_A = x^k f$ avec $\operatorname{pgcd}(x, f) = 1$. D'après le lemme des noyaux, on a une somme directe de l'espace $E = E_1 \oplus E_2$ avec $E_1 = \ker A^k$ et $E_2 = \ker f(A)$. Sur E_1, la restriction de A est nilpotente d'indice k. Sur E_2, la restriction de A a pour polynôme minimal f, en particulier 0 n'est pas valeur propre et A y est inversible. Si P est la matrice de passage de la base canonique vers une base adaptée à la décomposition $E = E_1 \oplus E_2$, on obtient que $P^{-1}AP$ est une matrice diagonale par blocs $\operatorname{diag}(B, C)$ avec $B^k = 0 = B^p$ et C inversible.

Par ailleurs, tout élément X de S_A commute avec A, donc laisse stables E_1 et E_2, et les restrictions X_1, X_2 de $P^{-1}XP$ à E_1, E_2 sont des racines n-èmes de B et C, respectivement. Réciproquement, si X_1 et X_2 sont des racines n-èmes de B et C, alors la matrice $P\operatorname{diag}(X_1, X_2)P^{-1}$ est dans S_A. On obtient ainsi une bijection $S_A \xrightarrow{\sim} S_B \times S_C$.

Commentaire : cette décomposition s'appelle la décomposition de Fitting *de A. Voir* [MM]*, exercice 5.2 du chap. IV, ou* [FGN1]*, exercice 6.14.*

5. En utilisant I.2.(a) et la question 4, on peut se ramener au cas où A est diagonale par blocs $\operatorname{diag}(B, C)$ avec B nilpotente et C inversible. D'après I.6.(b) on a $S_C \neq \varnothing$ et il ne reste qu'à montrer que $S_B \neq \varnothing$. Or les sauts d_i de A sont égaux aux d'_i de B, donc l'hypothèse sur les d_i vaut pour les d'_i et d'après 3.(d), il s'ensuit que $S_B \neq \varnothing$.

Références

[ADG] G. Auliac, J. Delcourt, R. Goblot, *Algèbre et géométrie Licence 3*, Ediscience, Dunod, 2005.

[FGN1] S. Francinou, H. Gianella, S. Nicolas, *Oraux X-ENS*, tome 1, Cassini, 2001.

[FGN2] S. Francinou, H. Gianella, S. Nicolas, *Oraux X-ENS*, tome 2, Cassini, 2006.

[Gou] X. Gourdon, *Algèbre*, 2ème édition, Ellipses, 2009.

[MM] R. Mansuy, R. Mneimné, *Algèbre linéaire, réduction des endomorphismes*, Vuibert, 2012.

[Sz] A. Szpirglas, *Algèbre L3*, Pearson, 2009.