Mathématiques Générales : corrigé
Agrégation Externe de Mathématiques 2023

J. Le Borgne

Exercice 1.

1. Soit d un diviseur de n. Si $H \subset \mathbf{Z}/n\mathbf{Z}$ est un sous-groupe d'ordre d, et $a \in \mathbf{Z}$ est tel que la classe $\bar{a}$ de k dans $\mathbf{Z}/n\mathbf{Z}$ soit dans H, alors da est divisible par n, donc a est divisible par $m = n/d$. Ainsi, H est contenu dans le sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ engendré par la classe de m. Or ce sous-groupe est d'ordre d : en effet, pour $k \in \mathbf{Z}$, on a :

$$n|km \Leftrightarrow \exists b \in \mathbf{Z} \text{ t.q.} nb = kn/d \Leftrightarrow \exists b \in \mathbf{Z} \text{ t.q.} bd = k \Leftrightarrow d|k.$$

Ainsi, tout sous-groupe d'ordre d est contenu dans le sous-groupe engendré par la classe de $m = n/d$, dont on vient de voir qu'il est d'ordre d : c'est donc le seul tel sous-groupe.

2. a) On a $(2q-1)^2 = 4q^2 - 4q + 1 \equiv 1 \pmod{4q}$. De même, $(2q+1)^2 \equiv 1 \pmod{4q}$. Ces deux éléments sont donc d'ordre 1 ou 2. Le seul cas où l'un de ces éléments est d'ordre 1 est le cas de l'élément $2q-1$ lorsque $q = 1$, dans tous les autres cas on a $2q-1, 2q+1 \neq 1 \pmod{4q}$ (car $1 < 2q-1 < 2q+1 < 4q$).

b) Si $q = 1$, alors G est d'ordre 2, donc cyclique. Si $q \geq 3$, le groupe G n'est pas cyclique. En effet, le sous-groupe engendré par la classe a de $2q-1$ est $\{1, a\}$ et celui engendré par la classe b de $2q+1$ est $\{1, b\}$, qui sont tous les deux d'ordre 2 et distincts car $a \neq b$. La question 1. montre alors que G n'est pas cyclique (tout groupe cyclique étant, par définition, isomorphe à un groupe de la forme $\mathbf{Z}/n\mathbf{Z}$).

Exercice 2.

1. Soit $(x, y) \in (\mathbf{Z}/3\mathbf{Z})^2$ une solution, que l'on suppose différente de la solution triviale $(0, 0)$. On peut supposer $y \neq 0$, on a alors $(x/y)^2 = -1$. Or -1 n'est pas un carré modulo 3 ($0^2 = 0$, $1^2 = 2^2 = 1 \pmod 3$). Ainsi, $(0, 0)$ est l'unique solution de cette équation.

2. Soit $(x, y) \in \mathbf{Z}^2$ une solution. Alors, en notant $\pi : \mathbf{Z} \to \mathbf{Z}/3\mathbf{Z}$ la projection canonique, on obtient $\pi(x)^2 + \pi(y)^2 = 0$ dans $\mathbf{Z}/3\mathbf{Z}$. Par conséquent, $x \equiv y \equiv 0 \pmod 3$ d'après la question 1. Mais alors $x^2 - 5y^2 \equiv 0 \pmod 9$, or 33 n'est pas divisible par 9, donc cette équation n'a pas de solution dans $\mathbf{Z}^2$.

3. Supposons que cette équation ait une solution $(x, y) \in \mathbf{Q}^2$. On peut supposer $x = a/b$, $y = a'/b'$ avec $a, a' \in \mathbf{Z}$, $b, b' \in \mathbf{N}^*$, et les entiers a, b (resp. a', b') premiers entre eux. Fixons parmi ces solutions une solution pour laquelle l'entier b est minimal. En

chassant les dénominateurs, il vient $(ab')^2 - 5(a'b)^2 = 33(bb')^2$. Le même argument qu'à la question 2. montre alors que ab' et $a'b$ sont divisibles par 3. Ainsi, comme 3 est premier, a ou b' est divisible par 3. Les conditions de coprimalité donnent alors l'alternative suivante : ou bien a et a' sont tous les deux divisibles par 3, et b et b' sont tous les deux non divisibles par 3, ou bien b et b' sont tous les deux divisibles par 3, et a et a' sont tous les deux non divisibles par 3. Dans le premier cas, $(ab')^2 - 5(a'b)^2$ est divisible par 9, contrairement à $33(bb')^2$, ce qui est contradictoire. Dans le deuxième cas, en posant $\beta = b/3$ et $\beta' = b'/3$, le couple $(a/\beta, a'/\beta')$ est solution, ce qui contredit la minimalité de b. On en conclut que cette équation n'a pas de solution dans $\mathbf{Q}^2$.

Exercice 3.

1. D'après le théorème de Riesz, l'application $E \to E^*$ définie par $z \mapsto (x \mapsto (z,x)_E)$ est un isomorphisme (il est clair que cette application est bien définie et linéaire, injective car pour $z \neq 0$, $(z,z)_E \neq 0$, et donc surjective par égalité des dimension de E et E^* en dimension finie).
En particulier, l'application $x \mapsto (y, u(x))_F$ étant une forme linéaire sur E, il existe un unique $z \in E$ tel que $(z,x)_E = (y,u(x))_F$.

2. La question 1. montre qu'à tout $y \in F$, on peut associer un unique $z \in E$ tel que pour tout $x \in E$, $(z,x)_E = (y,u(x))_F$. Notons u^* l'application ainsi définie : on a bien $u^* : F \to E$. Soient alors $y, y' \in F$ et $\lambda \in \mathbf{R}$. On a pour tout $x \in E$, $(u^*(\lambda y + y'), x)_E = (\lambda y + y', u(x))_F = \lambda(y, u(x))_F + (y', u(x))_F$ par linéarité à gauche du produit scalaire dans F, et donc $(u^*(\lambda y + y'), x)_E = \lambda(u^*(y), x)_E + (u^*(y'), x)_E = (\lambda u^*(y) + u^*(y'), x)_E$ par linéarité à gauche du produit scalaire dans E. Par unicité, on a donc $u^*(\lambda y + y') = \lambda u^*(y) + u^*(y')$. Cette relation étant valable pour tous $y, y' \in F$ et $\lambda \in \mathbf{R}$, l'application u^* est bien linéaire.

Problème

Partie I.

1. Procédons par double inclusion. Soit $x \in \ker u$, alors $u^*u(x) = 0$, donc $x \in \ker(u^* \circ u)$. Réciproquement, soit $x \in \ker(u^* \circ u)$. Alors $(u(x), u(x))_F = (u^* \circ u(x), x)_E = 0$, donc $u(x) = 0$. On a bien l'égalité attendue. Remarquons que le même argument montre que $\ker(u \circ u^*) = \ker u^*$.

2. Soit $\lambda \in \mathbf{C}$ une valeur propre de u^*u. Comme u^*u est autoadjoint et d'après le théorème spectral, on a $\lambda \in \mathbf{R}$. De plus, si X est un vecteur propre associé :

$$0 \leq (u(x), u(x))_F = (u^*u(x), x)_E = \lambda(x,x)_E,$$

avec $(x,x)_E > 0$ donc $\lambda \in \mathbf{R}_+$. Un argument analogue montre que les valeurs propres (complexes) de uu^* sont positives.

3. Soit λ réel strictement positif. Soit $x \in E_\lambda$ et $y = u(x)$. On a $uu^*(y) = uu^*u(x) = \lambda u(x) = \lambda y$, donc $u(x) \in F_\lambda$. De même, si $x \in F_\lambda$ et $y = u^*(x)$, on a $u(y) = u^*uu^*(x) = \lambda y$, donc $u^*(x) \in E_\lambda$. On a bien montré $u(E_\lambda) \subset F_\lambda$ et $u^*(F_\lambda) \subset u(E_\lambda)$.

4. Il suffit de démontrer que $v_\lambda = u_\lambda/\sqrt{\lambda} : E_\lambda \to F_\lambda$ est une isométrie, car cela montrera que $\dim E_\lambda = \dim F_\lambda$.
Soit $x \in E_\lambda$, on a $(v_\lambda(x), v_\lambda(x))_{F_\lambda} = \lambda^{-1}(u(x), u(x))_F = \lambda^{-1}(u^*u(x), x)_E = (x, x)_E$. Cela montre que v_λ préserve le produit scalaire, et est donc injectif. Il reste à voir que v_λ est surjectif. Soit $y \in F_\lambda$, soit $x = u^*(y)/\sqrt{\lambda}$. Alors $u(x) = \sqrt{\lambda}y$ donc $v_\lambda(x) = y$. Cela montre bien que v_λ est une isométrie et donc que $\dim E_\lambda = \dim F_\lambda$.

5. On reprend les notations de l'énoncé. Le théorème spectral appliqué à u^*u assure l'existence d'une base orthonormée formée de vecteurs propres de u^*u. Comme $\ker u^*u = \ker u$, une telle base est aussi formée de vecteurs propres associés aux valeurs propres non nulles de u^*u, et d'éléments du noyau de u. On dispose donc d'une base $(e_1, \dots, e_n)$ de E telle que $e_1, \dots, e_r$ soient associés aux valeurs propres $\lambda_1, \dots, \lambda_r$, et telle que $u(e_{r+1}) = \cdots = u(e_n) = 0$.
Posons alors, pour $1 \leq i \leq r$, $f_i = u(e_i)/\sqrt{\lambda_i}$. Le théorème spectral appliqué à uu^* montre que $(\bigoplus_{i=1}^r F_{\lambda_i}) \oplus \ker(uu^*) = F$, cette somme directe étant orthogonale. La question 4. montre donc que la famille f_i est orthonormée et peut être complétée en une base orthonormée de F (en lui ajoutant une base orthonormée de $\ker u^*$). Finalement, les familles $(e_1, \dots, e_n)$ et $(f_1, \dots, f_m)$ sont des bases orthonormées respectives de E et F, et $u(e_i) = \sqrt{\lambda_i} f_i$ pour tout $1 \leq i \leq r$, et $u(e_i) = 0$ pour $i > r$.

6. a) Soit $u : \mathbf{R}^n \to \mathbf{R}^m$ l'application linéaire canoniquement associée à M (les espaces $\mathbf{R}^n$ et $\mathbf{R}^m$ sont munis de leur structure euclidienne canonique). Notons $\lambda_1 \geq \cdots \geq \lambda_r$ les valeurs propres strictement positives de u^*u (cela est conforme à $r = \mathrm{rg}(u)$ grâce au théorème du rang et à l'égalité $\ker u = \ker u^*u$), et $\sigma_i = \sqrt{\lambda_i}$ pour $1 \leq i \leq r$. D'après la question 5, on dispose de bases orthonormées $(e_1, \dots, e_n)$ de $\mathbf{R}^n$ et $(f_1, \dots, f_m)$ de $\mathbf{R}^m$ telles que $u(e_i) = \sigma_i f_i$ pour $1 \leq i \leq r$, et $u(e_i) = 0$ pour $i > r$. Alors, en notant P^{-1} (resp. Q) la matrice de passage de la base canonique de $\mathbf{R}^m$ à la base $(f_1, \dots, f_m)$ (resp. de la base canonique de $\mathbf{R}^n$ à la base $(e_1, \dots, e_n)$), on a la relation $PMQ = D$ avec D la matrice dont les coefficients $d_{i,j}$ sont donnés par $d_{i,i} = \sigma_i$ pour $1 \leq i \leq r$, et $d_{i,j} = 0$ si $i \neq j$ ou $i > r$. Comme les bases $(e_1, \dots, e_n)$ et $(f_1, \dots, f_m)$ sont orthonormées, on a $P \in O_m(\mathbf{R})$ et $Q \in O_n(\mathbf{R})$. On a donc bien la décomposition attendue pour M.

b) Sous les hypothèses de cette question, M admet une unique décomposition polaire sous la forme $M = OS$ avec $O \in O_n(\mathbf{R})$ et S symétrique (l'unicité résulte du fait que $M \in GL_n(\mathbf{R})$). On a aussi, dans les notations de a), $M = PQ({}^tQDQ)$, et $PQ \in O_n(\mathbf{R})$, ${}^tQDQ$ symétrique. Ainsi, par unicité de la décomposition polaire, $PQ = O$ et ${}^tQDQ = S$. En particulier, le produit PQ ne dépend pas de la factorisation choisie.

Partie II.

7. On a $r = \mathrm{rg}(u) = \dim \mathrm{Im}(u)$. On dispose donc d'une base $(x_1, \dots, x_r)$ de $\mathrm{Im}(u)$. Cette base peut être complétée en une base $(x_1, \dots, x_n)$ de E. L'algorithme de Gram-Schmidt appliqué à cette famille garantit l'existence d'une base orthonormée $(e_1, \dots, e_n)$ de E telle que pour tout $0 \leq i \leq n$, $\mathrm{Vect}(e_1, \dots, e_i) = \mathrm{Vect}(x_1, \dots, x_i)$. En particulier, $\mathrm{Vect}(e_1, \dots, e_r) = \mathrm{Im}(u)$, donc la famille $(e_1, \dots, e_n)$ est une base orthonormée telle que $(e_1, \dots, e_r)$ soit une base de $\mathrm{Im}(u)$.

8. La condition $u^2 = 0$ est clairement équivalente à la condition $\mathrm{Im}(u) \subset \ker u$. On a donc $\dim \ker u \geq r$, et le théorème du rang montre alors que $n = r + \dim \ker u \geq 2r$.

9. a) Soit u l'endomorphisme canoniquement associé à M. La question 6. assure l'existence d'une base orthonormée $(e_1, \ldots, e_n)$ telle que $(e_1, \ldots, e_r)$ soit une base de $\mathrm{Im}(u)$. Alors, comme $u \in \mathcal{E}_n$, dans la base $(e_1, \ldots, e_n)$, la matrice de u est de la forme voulue. En effet, d'une part $\mathrm{Im}(u) \subset \ker u$ donc $u(\mathrm{Vect}(e_1, \ldots, e_r)) = \{0\}$, et d'autre part les vecteurs $u(e_{r+1}), \ldots, u(e_n)$ sont dans $\mathrm{Im}(u) = \mathrm{Vect}(e_1, \ldots, e_r)$. En outre, la matrice de passage P est bien orthogonale car $(e_1, \ldots, e_n)$ est orthonormée.

b) Suivant l'énoncé, on applique le résultat de la question I.6. à la matrice B, qui est de rang r comme la matrice M. On dispose alors de $U \in O_{n-r}(\mathbf{R}), V \in O_r(\mathbf{R})$ et $\sigma_1 \geq \cdots \geq \sigma_r$ tels que $UBV = D$, avec $D = \begin{pmatrix} \sigma_1 & 0 & \cdots & 0 \\ 0 & \ddots & \cdots & 0 \\ 0 & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \sigma_r \\ 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix}$ (comme $r \leq n - r$, la matrice a bien cette forme, avec $n - 2r$ lignes de 0 en bas).

On considère maintenant la matrice par blocs $W = \begin{pmatrix} U & 0 \\ 0 & V^{-1} \end{pmatrix}$, qui est orthogonale car U et V le sont. On a

$$W \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} W^{-1} = \begin{pmatrix} 0 & UB \\ 0 & 0 \end{pmatrix} \begin{pmatrix} U^{-1} & 0 \\ 0 & V \end{pmatrix} = \begin{pmatrix} 0 & D \\ 0 & 0 \end{pmatrix} = K_{r,\sigma}.$$

Ainsi, en posant $Q = WP$, on a bien $Q \in O_n(\mathbf{R})$ et $QMQ^{-1} = K_{r,\sigma}$.

10. La question précédente montre l'existence d'une matrice de la forme $K_{r,\sigma}$ dans chaque orbite de $\mathcal{E}_n$ sous l'action de $O_n(\mathbf{R})$. Montrons maintenant l'unicité. Soient r, σ, r', σ' tels que $K_{r,\sigma}$ et $K_{r',\sigma'}$ soient orthogonalement semblables. D'une part, on sait que $r = \mathrm{rg} K_{r,\sigma}$, donc $r = r'$. D'autre part, les valeurs propres non nulles de ${}^tK_{r,\sigma}K_{r,\sigma}$ sont $\sigma_1^2, \ldots, \sigma_r^2$. Si $K_{r,\sigma'} = PK_{r,\sigma}P^{-1}$ avec P orthogonale, alors ${}^tK_{r,\sigma'}K_{r,\sigma'} = P{}^tK_{r,\sigma}K_{r,\sigma}P^{-1}$, donc $(\sigma_1, \ldots, \sigma_r) = (\sigma'_1, \ldots, \sigma'_r)$ puisque les σ_i, σ'_i sont positifs et rangés par ordre décroissant. Cela montre que $K_{r,\sigma} = K_{r',\sigma'}$.

Partie III.

11. a) Par définition, pour $i \geq h$, on a $u^i(x) = 0$, donc $\langle x \rangle_u = \mathrm{Vect}(x, \ldots, u^{h-1}(x))$. Supposons la famille $x, u(x), \ldots, u^{h-1}(x)$ liée. Une relation de dépendance linéaire entre ces vecteurs fournit un polynôme non nul $P \in K[X]$ de degré $\leq h - 1$ tel que $P(u)(x) = 0$. Soit alors $D = \mathrm{pgcd}(P, X^h)$. On dispose d'une relation de Bezout $D = AP + BX^h$, et on a donc $D(u)(x) = 0$. Comme D est un diviseur de X^h, D est de la forme X^ℓ pour un certain entier ℓ. Comme D est un diviseur de P, on a $\ell = \deg D \leq h - 1$. Ainsi $u^{h-1}(x) = 0$, ce qui contredit la minimalité de h. En conclusion, $(x, u(x), \cdots, u^{h-1}(x))$ est libre, et c'est donc une base de $\langle x \rangle_u$.

b) Soit $y \in \langle x\rangle_u \cap \ker u$. Alors on dispose de $\lambda_0, \dots, \lambda_{h-1} \in K$ tels que $y = \sum_{i=0}^{h-1} \lambda_i u^i(x)$, et $0 = u(y) = \sum_{i=1}^{h-1} \lambda_{i-1} u^i(x)$. Comme la famille $(x, \dots, u^{h-1}(x))$ est libre, on a $\lambda_0 = \cdots = \lambda_{h-2} = 0$, donc $y \in \mathrm{Vect}(u^{h-1}(x))$. Comme il est clair que $0 \neq u^{h-1}(x) \in \langle x\rangle_u \cap \ker u$, on a bien $\langle x\rangle_u \cap \ker u = \mathrm{Vect}(u^{h-1}(x))$ et ce sous-espace est une droite vectorielle.

12. a) Soit $1 \leq i \leq m$. La famille $\{u^k(y_i), k \in \mathbf{N}\}$ engendre $\langle y_i\rangle_u$, et on a pour tout $k \in \mathbf{N}$ $u(u^k(y_i)) \in \langle z_i\rangle_u$, donc $u(\langle y_i\rangle_u) \subset \langle z_i\rangle_u$. Supposons maintenant qu'il existe $(x_1, \dots, x_m) \in \langle y_1\rangle_u \times \cdots \times \langle y_m\rangle_u$ tels que $x_1 + \cdots + x_m = 0$. Alors $u(x_1) + \cdots + u(x_m) = 0$, donc la remarque précédente montre que pour tout $1 \leq i \leq m$, $u(x_i) = 0$ (car les $\langle z_i\rangle_u$ sont en somme directe). Ainsi, pour tout $1 \leq i \leq m$, $x_i \in \langle y_i\rangle_u \cap \ker u = \mathrm{Vect}(u^{h_i-1}(y_i))$ d'après la question 11.b) (où h_i est la longueur de y_i). Comme $h_i \geq 2$ (puisque $u(y_i) = z_i \neq 0$), on a pour tout i, $x_i \in \langle z_i\rangle_u$. Ainsi, la relation $x_1 + \cdots + x_m = 0$ implique que pour tout $1 \leq i \leq m$, $x_i = 0$: les espaces $\langle y_i\rangle_u$ sont donc bien en somme directe.

b) On a clairement $u(F) \subset \mathrm{Im}(u)$. Soit $z \in \mathrm{Im}(u)$, on peut écrire $z = \sum_{i=1}^m P_i(u)(z_i)$ avec $P_i \in K[X]$. Si on pose $y = \sum_{i=1}^m P_i(u)(y_i)$, alors par définition des y_i, on a $u(y) = \sum_{i=1}^m P_i(u)(z_i) = z$, et $y \in F$. Donc $z \in u(F)$, d'où l'inclusion réciproque, et donc $u(F) = \mathrm{Im}(u)$.

c) Par définition de G, on a $\ker u = (F \cap \ker u) \oplus G$. On a donc $F \cap G \cap \ker u = \{0\}$. Comme $G \subset \ker u$, on a $G \cap \ker u = G$. Par associativité de l'intersection, on a alors $F \cap G = \{0\}$, donc F et G sont en somme directe.
Par ailleurs, soit $x \in E$. D'après b), on dispose de $y \in F$ tel que $u(x) = u(y)$, donc $x - y \in \ker u$. On peut donc écrire $x - y = z_F + z_G$, avec $z_F \in F \cap \ker u$ et $z_G \in G$. Mais alors $x = (y + z_F) + z_G$ avec $y + z_F \in F$ et $z_G \in G$. Cela montre que $F \oplus G = E$.

d) Pour $1 \leq i \leq m$, on pose $x_i = y_i$, et pour $m+1 \leq i \leq \ell$, on note $(x_{i+1}, \dots, x_\ell)$ une base de G. Alors $F = \bigoplus_{i=1}^m \langle x_i\rangle_u$, et pour $i \geq m+1$, on a $\langle x_i\rangle_u = \mathrm{Vect}(x_i)$ (d'après 11. par exemple) donc $G = \bigoplus_{i=m+1}^{\ell} \langle x_i\rangle_u$. On en déduit que $E = F \oplus G = \bigoplus_{i=1}^{\ell} \langle x_i\rangle_u$.

13. On démontre ce résultat par récurrence (dite forte) sur la dimension de E. Pour $n \in \mathbf{N}$, on note H_n l'hypothèse de récurrence suivante : « Pour tout K-espace vectoriel E de dimension $\leq n$, et pour tout endomorphisme nilpotent u de E, il existe une famille finie $x_1, \dots, x_\ell$ telle que $E = \bigoplus_{i=1}^{\ell} \langle x_i\rangle_u$. »
Initialisation. L'hypothèse H_0 est vérifiée car si $E = \{0\}$, alors la famille $\emptyset$ convient.
Hérédité. Soit $n \in \mathbf{N}$. Supposons H_n vérifiée, et démontrons que H_{n+1} l'est aussi. Soit E est un K-espace vectoriel de dimension $n+1$, et soit $u \in \mathrm{End}(E)$ nilpotent. Le sous-espace vectoriel $\mathrm{Im}(u)$ est stable par u et l'endomorphisme induit par u sur $\mathrm{Im}(u)$ est nilpotent. En outre, comme $\dim \ker u \geq 1$, le théorème du rang montre que $\dim \mathrm{Im}(u) \leq n$. On peut appliquer l'hypothèse de récurrence à $\mathrm{Im}(u)$ muni de l'endomorphisme $\bar{u}$ induit par u. On dispose donc de $z_1, \dots, z_m \in \mathrm{Im}(u)$ tels que $\mathrm{Im}(u) = \bigoplus_{i=1}^m \langle z_i\rangle_{\bar{u}} = \bigoplus_{i=1}^m \langle z_i\rangle_u$. Cette situation est celle étudiée en 12., et en appliquant le résultat de cette question on en déduit qu'il existe $x_1, \dots, x_\ell \in E$ tels que $E = \bigoplus_{i=1}^{\ell} \langle x_i\rangle_u$. Cela démontre l'hérédité de la propriété, le principe de récurrence conclut.

14. a) La question 11.a) montre que si x est de hauteur h, $\dim\langle x\rangle_u = h$, et $(x, \ldots, u^{h-1}(x))$ est une base de ce sous-espace. La matrice de l'endomorphisme $\langle x\rangle_u$ de induit par u dans cette base est J_h. Ainsi, si u est de type λ, la concaténation des bases correspondant aux $\langle x_i\rangle_u$ fournit une base de E dans laquelle la matrice de u est J_λ. Réciproquement, si la matrice de u dans une base convenable est J_λ, et qu'on note x_i le dernier vecteur de base du i-ème bloc, on obtient immédiatement $E = \bigoplus_i \langle x_i\rangle_u$.

b) Chaque bloc de J_λ contribue pour 1 à la dimension du noyau de u, donc $\dim\ker u^1 - \dim\ker u^0$ est égal au nombre de parts de λ, c'est-à-dire λ'_1. Ensuite, chaque bloc de taille ≥ 2 contribue pour 2 à la dimension de $\ker u^2$, tandis que les blocs de taille 1 y contribuent pour 1, de sorte que $\dim\ker u^2 - \dim\ker u$ est le nombre de blocs de taille au moins 2, c'est-à-dire le nombre de parts ≥ 2 dans λ : par définition, c'est λ'_2. Plus généralement, $\dim\ker u^i - \dim\ker u^{i-1}$ est le nombre de parts $\geq i$ dans λ, c'est-à-dire λ'_i. En effet, les blocs de taille au moins i contribuent pour i dans $\dim\ker u^i$, tandis que les autres blocs contribuent pour une quantité égale à leur dimension, et donc la différence $\dim\ker u^i - \dim\ker u^{i-1}$ calcule précisément le nombre de blocs de taille au moins i.

c) Le point b) montre que la partition conjuguée de λ est entièrement déterminée par les $\dim\ker u^i$ qui ne dépendent d'aucun choix, donc λ aussi. Ainsi, si (E, u) est de type λ et de type μ, alors $\lambda = \mu$.

15. a) L'existence résulte de 13., l'unicité de 14.c).

b) On a $\dim\ker K_{r,\sigma} = n - r$ et $\dim\ker K_{r,\sigma}^2 = n$. D'après la question précédente, la partition conjuguée de λ est $\lambda' = (n-r, r)$. La partition λ est donc (2, …, 2,1,…,1) avec r fois 2 et $n - 2r$ fois 1.

c) Si $M, M' \in \mathcal{M}_n(K)$ sont nilpotentes et telles que $M' = \alpha M$ avec $\alpha \in K^\times$, alors pour tout $i \geq 0$, $\dim\ker M^i = \dim\ker(M')^i$, donc M et M' sont semblables à une même matrice J_λ : elles sont semblables.

Partie IV.

16. a) On considère la matrice diagonale par blocs P dont le i-ème bloc diagonal est $\tilde{P}_{\lambda_i}$. Les relations données dans l'énoncé montrent alors immédiatement que $P^2 = I_n$ et que $PJ_\lambda P^{-1} = {}^tJ_\lambda$.

b) Comme on a supposé que K est algébriquement clos, on dispose d'une racine a du polynôme $2X^2 - 1$, et i une racine de $X^2 + 1$. Posons alors $b = ia$. On a $(aI_n + bP)(aI_n - bP) = (a^2 - b^2)I_n = I_n$, de sorte que l'inverse de $Q = aI_n + bP$ est $aI_n - bP$. On a alors $QJQ^{-1} = (aI_n + bP)J(aI_n - bP) = (aJ + bPJ)(aI_n - bP) = a^2J - abJP + abPJ - b^2PJP$. Or, on a $PJ = JP$, donc $QJQ^{-1} = a^2J - b^{2t}J = a^2(J + {}^tJ)$ est symétrique.

17. a) Pour tout $1 \leq i \leq n$, on dispose de $\beta_i \in K$ tels que $\beta_i^2 = \alpha_i$, car K est algébriquement clos. Soit f le polynôme d'interpolation de Lagrange qui envoie α_i sur β_i : si on note $\alpha_1, \ldots, \alpha_k$ les valeurs propres deux à deux distinctes de D (ce qu'on peut suppposer quitte à réordonner), il s'agit du polynôme $\sum_{i=1}^k \beta_i \prod_{j\neq i} \frac{X-\alpha_j}{\alpha_i-\alpha_j}$, qui vérifie bien $f(\alpha_i)^2 = \alpha_i$ pour tout $1 \leq i \leq n$. Si $D = PD_0P^{-1}$ avec D_0

diagonale et $P \in GL_n(K)$, les coefficients diagonaux de D_0 sont les α_i et donc $f(D_0)^2 = D_0$. On en déduit immédiatement que $f(D)^2 = D$.

b) Modulo X^n, on a :

$$\Phi(X)^2 = 1 - 4\sum_{k=0}^{n-2} C_k X^{k+1} + 4X^2 \sum_{k=0}^{n-3} \left(\sum_{i=0}^{k} C_i C_{k-i} \right) X^k = 1 - 4C_0 X.$$

On a donc $\Phi(X)^2 \equiv 1 - 4X \pmod{X^n}$.

c) Soit $g(X) = \Phi(-X/4)$ (qui est bien défini car K est supposé de caractéristique différente de 2). On a alors $g(X)^2 \equiv 1 + X \pmod{X^n}$. Soit $N \in \mathcal{M}_n(K)$ nilpotente, alors comme $N^n = 0$, on a $g(N)^2 = I_n + N$.

18. a) Le sous-espace vectoriel $F = \ker D$ de K^n est stable par N car D et N commutent. L'endomorphisme N_F induit par N sur F est nilpotent ; si $F \neq \{0\}$, $\ker N_F \neq \{0\}$, on dispose donc de $x \in \ker N_F$ non nul. Mais alors $Nx = Dx = 0$, donc $Px = 0 : x \in \ker P$ est non nul, ce qui est absurde. Donc $\ker D = \{0\}$ et D est inversible.

Dans ce cas, le coefficient constant du polynôme caractéristique χ_D est non nul (c'est $\pm \det D$), on peut écrire $Xp(X) \equiv 1 \pmod{\chi_D}$ avec $p = \chi_D(0)^{-1}(\chi_D - \chi_D(0))/X$, et en vertu du théorème de Cayley-Hamilton on a $Dp(D) = I_n$. Comme $D = h(P)$, on a $Dp(h(P)) = I_n$, onc $D^{-1} = k(P)$ avec $j = p \circ h$.

b) On peut écrire $P = D(I + D^{-1}N)$, avec D diagonalisable inversible, et $D^{-1}N$ nilpotente car D et N commutent et D^{-1} est un polynôme en D. Soit alors g tel que $g(I + D^{-1}N)^2 = D^{-1}N$, h tel que $h(D)^2 = D$, on a alors $R = h(D)g(I + D^{-1}N) \in K[P]$ (car D, D^{-1} et N sont des polynômes en P), et $h(D)$ et $g(I + D^{-1}N)$ commutent pour la même raison. Donc $R^2 = h(D)^2 g(I + D^{-1}N)^2 = D(I + D^{-1}N) = P$.

c) Soit $M = {}^tPP$. Comme $P \in GL_n(K)$, $M \in GL_n(K)$. On dispose donc de $S \in GL_n(K)$ telle que $S^2 = M$ et telle que S soit un polynôme en M. Comme M est symétrique et que S est un polynôme en M, S est symétrique. Soit alors $Q = PS^{-1}$, on a ${}^tQQ = (S^{-1}){}^tPPS^{-1}$ (car S^{-1} est symétrique par symétrie de S). Ainsi, ${}^tQQ = S^{-1}S^2S^{-1} = I_n$, donc $Q \in \mathbf{O}_n(K)$. Dans cette construction, S est bien un polynôme en ${}^tPP$.

19. Soient $A, B \in \mathcal{M}_n(K)$ symétriques semblables. On dispose de $P \in GL_n(K)$ telle que $PAP^{-1} = B$. D'après la question 18, on dispose de $Q \in \mathbf{O}_n(K)$, $S \in \mathcal{M}_n(K)$ symétrique, telles que $P = QS$, et telle que S soit un polynôme en ${}^tPP$. Or, comme A et B sont symétriques, on a $({}^tPP)A({}^tPP)^{-1} = {}^tPB({}^tP)^{-1} = A$, donc A commute avec ${}^tPP$. En particulier, A commute avec S, donc $B = PAP^{-1} = QSAS^{-1}Q^{-1} = QAQ^{-1}$. Cela montre le résultat voulu.

20. Soit $P \in \mathbf{O}_n(K)$ et $M \in \mathcal{N}_n^{\mathrm{sym}}(K)$. Comme $GL_n(K)$ agit sur $\mathcal{N}_n(K)$ par conjugaison, PMP^{-1} est nilpotente. De plus, comme P orthogonale, on a de plus ${}^t(PMP^{-1}) = P({}^tM)P^{-1} = PMP^{-1}$ car M est symétrique. Donc $P \cdot M \in \mathcal{N}_n^{\mathrm{sym}}(K)$.

21. Notons Ω l'ensemble des $GL_n(K)$-orbites de $\mathcal{N}_n(K)$, et Ω^{sym} l'ensemble des $\mathbf{O}_n(K)$-orbites de $\mathcal{N}_n^{\mathrm{sym}}(K)$. Soit $\mathcal{O} \in \Omega$. Alors d'après 15.a), il existe une partition λ de n telle que $\mathcal{O}$ soit l'orbite de J_λ. D'après 16.b), il existe $Q \in \mathbf{O}_n(K)$ telle que $QJ_\lambda Q^{-1}$ soit symétrique, donc $\mathcal{O} \cap \mathcal{N}_n^{\mathrm{sym}}(K)$ est non vide. Ce sous-ensemble de $\mathrm{sym}_n(K)$ est

évidemment stable par conjugaison par un élément de $\mathbf{O}_n(K)$. Enfin, d'après 19., si $A, B \in \mathcal{O} \cap \mathcal{N}_n^{\mathrm{sym}}(K)$, alors A et B étant nilpotentes, symétriques et semblables, elles sont conjuguées par un élément de $\mathbf{O}_n(K)$. Donc $\mathcal{O} \cap \mathcal{N}_n^{\mathrm{sym}}(K) \in \Omega^{\mathrm{sym}}$. L'opération $\mathcal{O} \mapsto \mathcal{O} \cap \mathcal{N}_n^{\mathrm{sym}}(K)$ définit donc bien une application $\Omega \to \Omega^{\mathrm{sym}}$.
Cette application est injective : si deux éléments de Ω ont la même intersection avec $\mathcal{N}_n^{\mathrm{sym}}(K)$ (nécessairement non vide, comme on l'a vu grâce à 16.b), alors elles ont une intersection non vide et donc elles sont égales. Cette application est surjective : soit $\mathcal{O}^{\mathrm{sym}} \in \Omega^{\mathrm{sym}}$ et soit $N \in \mathcal{O}^{\mathrm{sym}}$, alors l'orbite $\mathcal{O}$ de N sous l'action de $GL_n(K)$ vérifie $N \in \mathcal{O} \cap \mathcal{N}_n^{\mathrm{sym}}(K)$, donc $\mathcal{O} \cap \mathcal{N}_n^{\mathrm{sym}}(K) = \mathcal{O}^{\mathrm{sym}}$.

22. a) On constate immédiatement que ces deux matrices vérifient $\dim\ker M = 1$, $\dim\ker M^2 = 2$, $\dim\ker M^3 = 3$. Elles sont donc toutes deux semblables à $J_{(3)}$.

b) Soit $P = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Si on note M_1, M_2 les deux matrices de la question précédente, on a $M_1 P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ et $P M_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Comme $\det P = 1$ on a $P^{-1} M_1 P = M_2$. Maintenant, si $Q \in GL_3(K)$ est telle que $M_1 Q = M_2 Q$, alors QP^{-1} commute avec M_1. Comme M_1 est semblable à $J_{(3)}$ qui est la matrice d'un endomorphisme cyclique, un résultat classique montre que QP^{-1} est de la forme $aI_3 + bM_1 + cM_1^2 = \begin{pmatrix} a+c & b & c \\ b & a & b \\ c & b & a+c \end{pmatrix}$, avec $a, b, c \in K$.
Ainsi, les matrices Q telles que $M_1 Q = Q M_2$ sont les matrices de la forme $\begin{pmatrix} a+b+c & b & b+c \\ a+b & a & a+b \\ b+c & b & a+b+c \end{pmatrix}$.
Parmi les matrices de cette forme, celles qui sont dans $\mathbf{O}_n(K)$ doivent avoir des colonnes qui forment une famille orthonormale pour la forme quadratique $q(x, y, z) = x^2 + y^2 + z^2$. Cela implique notamment $a^2 = 1$ (en considérant la deuxième colonne) et $a^2 = 0$ (en considérant les deux premières colonnes). Ces deux conditions étant incompatibles, il n'existe pas de matrice $Q \in \mathbf{O}_n(K)$ telle que $Q^{-1} M_1 Q = M_2$. Le résultat de la question 19. n'est donc pas valable lorsque K est de caractéristique 2, y compris si K est algébriquement clos.

Partie V.

23. a) Soit $i \geq 1$. On note u_i (resp. $u_{i,F}$) l'application induite par u sur $u^{i-1}(E)$ (resp. sur $u^{i-1}(F)$). On a $u^{i-1}(F) \subset u^{i-1}(E)$, donc $\ker u_{i,F}$ est un sous-espace vectoriel de $\ker u_i$, et $\dim\ker u_{i,F} \leq \dim\ker u_i$. D'autre part, $\mathrm{Im}(u_i) = u^i(E)$ et $\mathrm{Im}(u_{i,F}) = u^i(F)$, donc d'après le théorème du rang,

$$\dim u^{i-1}(E) - \dim u^i(E) = \dim\ker u_i \geq \dim\ker u_{i,F} = \dim u^{i-1}(F) - \dim u^i(F).$$

En appliquant à nouveau le théorème du rang avec $u^i, u^{i-1}, u^i_{|F}$ et $u^{i-1}_{|F}$, on obtient

$$\dim\ker u^i - \dim\ker u^{i-1} \geq \dim\ker u^i_{|F} - \dim\ker u^{i-1}_{|F}.$$

Cela montre que $\mu' \subset \lambda'$, et donc que $\mu \subset \lambda$.

b) On considère comme précédemment pour $i \geq 1$ les applications linéaires $u_i : u^{i-1}(E) \to u^i(E)$ et $u_{E/F,i} : u^{i-1}_{E/F}(E/F) \to u^i_{E/F}(E/F)$ induites respectivement par u et $u_{E/F}$, qui sont surjectives par définition. On a aussi immédiatement pour tout $i \geq 0$, $u^i(E)/F = u^i_{E/F}(E/F)$.
Notons que si $f : V \to V'$ est une application linéaire, et $W \subset V'$ est un sous-espace vectoriel, on a $\dim f^{-1}(W) = \dim \ker f + \dim(W \cap \mathrm{Im}(f))$. En effet, f induit une application linéaire $f^{-1}(W) \to W$, dont l'image est $W \cap \mathrm{Im}(f)$ et dont le noyau est $\ker f \subset f^{-1}(W)$. Le théorème du rang donne alors l'égalité annoncée.
Appliquons ce résultat à $u_i : u^{i-1}(E) \to u^i(E)$ et au sous-espace vectoriel $F \cap u^i(E)$. On a alors $\dim u_i^{-1}(F) = \dim \ker u_i + \dim(F \cap u^i(E))$. D'après la discussion précédente, on a $\dim \ker u_{i,E/F} = \dim u_i^{-1}(F) - \dim F = \dim \ker u_i + \dim(F \cap u^i(E)) - \dim F \leq \dim \ker u_i$. On en déduit que :

$$\dim \ker u^i_{E/F} - \dim \ker u^{i-1}_{E/F} \leq \dim \ker u^i - \dim \ker u^{i-1}.$$

Cela montre que $\nu' \subset \lambda'$ et donc que $\nu \subset \lambda$.

24. On note $F_1 = \mathrm{Vect}(e_1, e_2, e_3)$ et $F_2 = \mathrm{Vect}(e_4, e_5)$. Soit F un sous-espace de K^5, stable par $J_{(3,2)}$, et tel que (F, u_F) soit de type $(2, 1)$. Comme $\dim \ker u = \dim \ker u_F = 2$, on a $\ker u \subset F$. Le sous-espace F est donc entièrement déterminé par la donnée d'un $x \in F$ tel que $u(x) \neq 0$; un tel x vérifie nécessairement $u(x) \in \ker u$, donc x est de la forme $\alpha_1 e_1 + \alpha_2 e_2 + \alpha_4 e_4 + \alpha_5 e_5$, avec $(\alpha_2, \alpha_5) \neq (0, 0)$. L'endomorphisme quotient $u_{E/F}$ est de type (2) si et seulement si $u_{E/F} \neq 0$, c'est-à-dire si et seulement si $\mathrm{Im}(u) \not\subset F$. Comme une base de $\mathrm{Im}(u)$ est e_1, e_2, e_4, et qu'une base de F est e_1, e_4, x, cette condition équivaut à $\alpha_5 \neq 0$.
Ainsi, les sous-espaces F recherchés sont de la forme $F = \mathrm{Vect}(e_1, e_4, e_5 + \alpha e_2)$, avec $\alpha \in \mathbf{F}_q$. Réciproquement, un sous-espace de cette forme vérifie bien (F, u_F) de type $(2, 1)$ et $(E/F, u_{E/F})$ de type (2). Le nombre de tels sous-espaces est q, car si F est de cette forme, il admet une unique base de la forme $(e_1, e_4, e_5 + \alpha e_2)$.

25. a) Si $\lambda = (n)$ avec $n \geq 2$ alors $\mathrm{Im}(J_\lambda) = \mathrm{Vect}(e_1, \ldots, e_{n-1})$ et l'endomorphisme induit a pour partition associée $(n-1)$. Si $\lambda = (1)$, l'endomorphisme induit sur l'image a encore pour partition associée (1). Il en découle que dans le cas général, $(\mathrm{Im}(u), u)$ a pour partition $(\lambda_1 - 1, \ldots, \lambda_k - 1, 1, \ldots, 1)$ où $k = \max\{j \geq 1 \text{ tels que } \lambda_j \geq 2\}$ (ce maximum existe dès que cet ensemble est non vide, ce qu'on peut supposer car sinon $u = 0$ et le résultat est clair).

b) On a $u_{E/F} = 0$ si et seulement si $u(E) \subset F$. D'après 23.a), on a $\lambda_{\mathrm{Im}(u)} \subset \mu \subset \lambda$, donc pour tout $i \geq 0$, $\lambda_i - \mu_i \in \{0, 1\}$, c'est-à-dire que le diagramme de Ferrers de (F, u_F) s'obtient à partir de celui de u en supprimant au plus une boîte par ligne.

c) Soit $i \geq 1$. On considère l'application $f = u^i : u(E) \to u^{i+1}(E)$, qui est surjective par définition. Son noyau est $\{x \in u(E) \text{ tels que } u^i(x) = 0\} = \mathrm{Im}(u) \cap \ker u^i$. Le premier théorème d'isomorphisme montre alors que f induit un isomorphisme $\mathrm{Im}(u)/(\mathrm{Im}(u) \cap \ker u^i) \to \mathrm{Im}(u^{i+1})$. Le second théorème d'isomorphisme assure que $\mathrm{Im}(u)/(\mathrm{Im}(u) \cap \ker u^i) \simeq (\mathrm{Im}(u) + \ker u^i)/\ker u^i$, d'où $\mathrm{rg}(u^{i+1}) = \mathrm{rg}(f) = \dim(\mathrm{Im}(u) + \ker u^i)/\ker u^i) = \dim((\mathrm{Im}(u) + \ker u^i)/\mathrm{Im}(u)) +$

$\mathrm{rg}(u) - \dim\ker u^i$, d'où $\dim\left(\mathrm{Im}(u) + \ker u^i\right)/\mathrm{Im}(u)) = \mathrm{rg}(u^{i+1}) - \mathrm{rg}(u) + \dim\ker u^i$. Par ailleurs, on sait que $\lambda'_1 - \lambda'_{i+1} = \dim\ker u - (\dim\ker u^{i+1} - \dim\ker u^i) = \mathrm{rg}(u^{i+1}) - \mathrm{rg}(u) + \dim\ker u^i$ d'après le théorème du rang. On en déduit que $\lambda'_1 - \lambda'_{i+1} = \dim\left((\mathrm{Im}(u) + \ker u^i)/\mathrm{Im}(u)\right)$.

d) Notons pour $i \geq 0$, $d_i = \dim F \cap (\mathrm{Im}(u) + \ker u^i)$. On a supposé que $u_{E/F} = 0$, c'est-à-dire que $\mathrm{Im}(u) \subset F$. On a donc pour tout $i \geq 0$, $(\ker u^i + \mathrm{Im}(u)) + F = \ker u^i + F$. En appliquant aux deux membres la relation de Grassmann, on trouve d'une part :

$$\dim\ker(u^i + F) + d_i = \lambda'_1 - \lambda'_{i+1} + \mathrm{rg}(u) + \dim F,$$

et d'autre part :

$$\dim(\ker u^i + F) + \dim(\ker u^i \cap F) = \dim\ker u^i + \dim F.$$

Comme $\ker u^i \cap F = \ker u^i_F$, on en déduit que :

$$\dim\ker u^i_F = d_i + \dim\ker u^i + \lambda'_{i+1} - \lambda'_1 + \mathrm{rg}(u).$$

Par différence des égalités correspondant aux indices i et $i-1$ pour $i \geq 1$, il vient :

$$\mu'_i = d_i - d_{i-1} + \lambda'_i + \lambda'_{i+1} - \lambda'_i = d_i - d_{i-1} + \lambda'_{i+1}.$$

26. a) Soit $i \geq 1$. On sait que le sous-espace E_{i-1} de E_i est de codimension 1. L'inclusion canonique $F \cap E_i \to E_i$ induit une application linéaire $F \cap E_i \to E_i/E_{i-1}$, dont le noyau est clairement $F \cap E_{i-1}$. On dispose donc d'une application linéaire injective $(F \cap E_i)/(F \cap E_{i-1}) \to E_i/E_{i-1}$, donc $\dim((F \cap E_i)/(F \cap E_{i-1})) \in \{0, 1\}$.

b) Soit $I \subset \{1, \ldots, n\}$ et soit $F \in \mathcal{C}_I$. Soit $i \in I$, alors par hypothèse on dispose d'une droite vectorielle $D \subset E_i$ telle que $E_i \cap F = E_{i-1} \cap F \oplus D$. En particulier $v_i^*(D) \neq 0$, donc on dispose d'un unique $w = w_i \in D$ tel que $v_i^*(w) = 1$. Cela détermine une famille de vecteurs $(w_i)_{i\in I}$ qui est par construction I-échelonnée réduite, c'est donc une base de F car elle est de cardinal $|I|$ (et libre car I-échelonnée).
Une telle base est unique : supposons que F possède une autre base I-échelonnée réduite $(w'_i)_{i\in I}$, et fixons $i \geq 1$. On peut écrire $w'_i = \sum_{j=1}^{|I|} \lambda_j w_j$. En appliquant v_k^* pour $k \in I$, il vient $0 = \sum_{j=1}^{|I|} \lambda_j v_k^*(w_j) = \lambda_k$ pour $k \neq i$, et $1 = \lambda_i$. On a donc $w'_i = w_i$ pour tout $i \in I$, ce qui montre bien l'unicité.

c) Considérons l'application $W : \mathcal{C}_I \to \{\text{Familles } I - \text{échelonnées réduites}\}$ définie par $F \mapsto (w_i)$ où w_i est l'unique base I-échelonnée réduite de F. D'après la question précédente, cette application est bien définie, et elle est injective car F est clairement le sous-espace vectoriel engendré par $(w_i) = W(F)$.
Enfin, si $(w_i)_{i\in I}$ est une famille I-échelonnée réduite, elle est libre car I-échelonnée, et elle engendre donc un sous-espace vectoriel F de E de dimension $|I|$. En outre, si on note $I = \{i_1 < \cdots < i_{|I|}\}$, et comme $v_j^*(w_i) = 0$ pour $j > i$, on a $F \cap E_{i_k} \supset \mathrm{Vect}(w_1, \ldots, w_k)$. De plus, comme $v_{i_k}^*(w_k) = 1$, on a $w_k \in F \cap E_{i_k}$ et $w_k \notin F \cap E_{i_k - 1}$, donc $F \cap E_{i_k} \neq F \cap E_{i_k - 1}$. Comme $\dim F = |I|$, il en résulte que $F \in \mathcal{C}_I$, et on a alors $W(F) = (w_i)$. Cela montre la surjectivité et conclut.

d) Soit I de cardinal d. La famille (w_i) est I-échelonnée réduite si et seulement si, pour tout $1 \leq i \leq d$, $w_i = v_i + \sum_{j \notin I, j<i} \lambda_j v_j$ (cela résulte directement des hypothèses sur les $v_j^*(w_i)$). Si $I = \{i_1 < \cdots < i_d\}$, il y a donc $q^{i_1-1}q^{i_2-2}\cdots q^{i_d-d} = q^{i_1+\cdots+i_d-\frac{d(d-1)}{2}}$ choix possibles pour l'ensemble des coefficients λ_j. Le nombre d'éléments de $\mathcal{C}_I$ est donc $q^{i_1+\cdots+i_d-\frac{d(d+1)}{2}}$ d'après c).

27. a) Soit G le sous-groupe de $GL(E)$ qui stabilise la suite de sous-espaces $E_0 \subset \cdots \subset E_r$. Alors G agit sur les sous-espaces vectoriels F de E, et la stabilité des E_i assure que pour tout $g \in G$ et $i \geq 0$, on a $g(F \cap E_i) = g(F) \cap E_i$. Ainsi, l'action de G sur les sous-espaces vectoriels de E préserve les dimensions des quotients $(F \cap E_i)/(F \cap E_{i-1})$ pour $i \geq 1$.

Soit $f = (f_1, \ldots, f_r)$, notons $\mathcal{G}_f$ l'ensemble des sous-espaces vectoriels F de E tels que pour tout $i \geq 1$, $\dim(F \cap E_i)/(F \cap E_{i-1}) = f_i$. En particulier, les éléments de $\mathcal{G}_f$ sont tous de dimension $f_1 + \cdots + f_r$. Montrons par récurrence sur r que l'action de G sur $\mathcal{G}_f$ est transitive. Le cas $r = 1$ est une conséquence directe du théorème de la base adaptée. Supposons le résultat acquis pour un $r \geq 1$ et montrons-le pour $r+1$. Soient $F, F' \in \mathcal{G}_f$. Par hypothèse de récurrence, on dispose d'un $g \in G(E_r)$ tel que $g(E_i) = E_i$ pour tout $1 \leq i \leq r$ et tel que $g(F \cap E_r) = F' \cap E_r$. On peut écrire $E = (F \cap E_r) \oplus G_r \oplus H_r$, où G_r est un supplémentaire de $F \cap E_r$ dans F et H_r est un supplémentaire de F dans $E = E_{r+1}$, et en écrivant de même $E = (F' \cap E_r) \oplus G'_r \oplus H'_r$, et on a par hypothèse $\dim G_r = \dim G'_r$, $\dim H_r = \dim H'_r$. On peut donc (toujours par le théorème de la base adaptée) prolonger g en un élément de E tel que $g(F) = F'$.

En conclusion, le groupe G opère transitivement sur $\mathcal{G}_f$, donc le cardinal de $\mathcal{G}_f$ est $|G|/|S|$ où $S \subset G$ est le cardinal du stabilisateur d'un élément de G. On peut calculer $|G|$ et $|S|$ en prenant $E = K^n$ muni de sa base canonique $x_1, \ldots, x_n$, $E_i = \mathrm{Vect}(x_1, \ldots, x_{e_i})$ et $F = \mathrm{Vect}(x_1, \ldots, x_{e_1-f_1}, x_{e_2}, \ldots, x_{e_2-f_2}, \ldots, x_{e_r-f_r})$. Le groupe G est alors le sous-groupe de $GL_n(K)$ formé des matrices triangulaires supérieures par blocs, avec des blocs diagonaux de tailles $e_1, \ldots, e_r$, et le stabilisateur de F est le sous-groupe formé des éléments de G dont les blocs diagonaux sont de la forme $\begin{pmatrix} g_{i,1} & a \\ 0 & g_{i,2} \end{pmatrix}$ avec $g_{i,1} \in GL_{e_i-f_i}(K), g_{i,2} \in GL_{f_i}(K)$ et $a \in \mathcal{M}_{e_i-f_i,f_i}(K)$, et dont les blocs sur-diagonaux sont de la forme $\begin{pmatrix} m_{1,1} & m_{1,2} \\ 0 & m_{2,2} \end{pmatrix}$ avec $m_{1,1} \in \mathcal{M}_{(e_i-f_i)(e_j-f_j)}$, $m_{1,2} \in \mathcal{M}_{(e_i-f_i)f_j}$, $m_{2,2} \in \mathcal{M}_{f_if_j}$ (la présence de blocs de 0, de tailles $f_i \times (e_j - f_j)$ pour $j \leq i$, correspond au fait que $F \cap E_i$ doit être envoyé dans $F \cap E_i$ par stabilité). Lorsque $K = \mathbf{F}_q$, l'ensemble quotient $\mathcal{G}_f$ est alors de cardinal :

$$\prod_{i=1}^{r} q^{f_i(e_1-f_1+\cdots+e_{i-1}-f_{i-1})} \frac{|GL_{e_i}(\mathbf{F}_q)|}{|GL_{e_i-f_i}(\mathbf{F}_q)||GL_{e_i}(\mathbf{F}_q)|q^{f_i(e_i-f_i)}}.$$

Comme on a $|GL_d(\mathbf{F}_q)| = q^{\frac{d(d-1)}{2}}(q^d-1)\cdots(q-1)$ pour tout $d \geq 1$, on en déduit après simplification que

$$|\mathcal{G}_f| = \prod_{i=1}^{r} q^{f_i(e_1-f_1+\cdots+e_{i-1}-f_{i-1}+e_i-f_i)} \frac{(q^{e_i}-1)\cdots(q^{e_i-f_i+1}-1)}{(q^{f_i}-1)\cdots(q-1)}.$$

Il suffit donc de montrer que pour $1 \leq a \leq b$ entiers, l'expression $\frac{(q^b-1)\cdots(q^{b-a+1}-1)}{(q^b-1)\cdots(q-1)}$ est polynomiale en q. Si on note $P_q(a,b)$ cette expression, on a en factorisant par $\frac{q^b-1}{q^{b-a}-1}$ la relation $P_q(a,b) = \frac{q^b-1}{q^{b-a}-1}P_q(a,b-1)$ lorsque $b > a$. En écrivant $\frac{q^b-1}{q^{b-a}-1} = q^{b-a}\frac{q^a-1}{q^{b-a}-1} + 1$, on en déduit que $P_q(a,b) = P_q(a,b-1) + q^{b-a}P_q(a-1,b-1)$. Une récurrence double, d'abord sur b puis sur a à b fixé, montre alors que $P_q(a,b)$ est un polynôme en q à coefficients positifs, car $P_q(1,b) = 1 + q + \cdots + q^{b-1}$.
Cela montre bien que $|\mathcal{G}_f| = \mathcal{A}_{e,f}$ où $\mathcal{A}_{e,f}$ s'exprime comme un polynôme en q.

b) En utilisant le calcul de la question précédente, on obtient le degré de $\mathcal{A}_{e,f}$: les facteurs qui sont des puissances de q contribuent pour $\sum_{i=1}^{r} f_i(e_1 - f_1 + \cdots + e_{i-1} - f_{i-1})$ et comme $P_q(a,b)$ est de degré $a\frac{b+(b-a+1)}{2} - \frac{a(a+1)}{2} = a(b-a)$, on en déduit que :

$$\deg \mathcal{A}_{e,f} = \sum_{i=1}^{r} f_i(e_1 - f_1 + \cdots + e_i - f_i) = \sum_{1\leq i\leq j\leq r} (e_i - f_i)f_j.$$

28. a) On suppose que κ est de longueur 1. La suite de sous-espaces considérée est alors de la forme (E,F), avec F un sous-espace stable par u et de dimension $n - \kappa_1$. Posons $E_0 = \{0\}$ et pour tout $i \geq 1$, $E_i = \mathrm{im}(u) + \ker u^{i-1}$. La suite de sous-espaces $(E_i)_{i\geq 0}$ est croissante. Soit $r-1$ l'indice de nilpotence de u, alors $E_r = E$. Par hypothèse, $u_{E/F} = 0$. D'après la question 25.c), on a pour tout $i \geq 1$, $\lambda'_1 - \lambda'_i = \dim E_i - \mathrm{rg}(u)$, et d'après la question 25.d), pour $i \geq 2$, $\mu'_{i-1} = \dim(F \cap E_i)/(F \cap E_{i-1}) + \lambda'_i$. Ainsi, en posant $e_1 = f_1 = n - \lambda'_1$, et pour tout $i \geq 2$, $e_i = \lambda'_{i-1} - \lambda'_i = \dim E_i/E_{i-1}$ et $f_i = \mu'_{i-1} - \lambda'_i$, on en déduit que la famille de sous-espaces à dénombrer est exactement celle étudiée dans la question 27. On a donc $B^{\lambda}_{\mu,\kappa} = \mathcal{A}_{e,f}(q)$.

b) Supposons maintenant $\ell \geq 2$. On note $\kappa^* = (\kappa_1, \ldots, \kappa_{\ell-1})$. Par définition, $(F_0, \ldots, F_\ell) \in \mathcal{B}^{\lambda}_{\mu,\kappa}$ si et seulement s'il existe une partition μ^* de $|\mu| + \kappa_\ell$ telle que de $(F_0, \ldots, F_{\ell-1}) \in \mathcal{B}^{\lambda}_{\mu^*,\kappa^*}$ et telle que $(F_{\ell-1}, F_\ell) \in \mathcal{B}^{\mu^*}_{\mu,(\kappa_\ell)}$ (en identifiant $\mathcal{B}^{\mu^*}_{\mu,(\kappa_\ell)}$ et l'ensemble des suites de sous-espaces correspondantes dans $F_{\ell-1}$). On a donc :

$$B^{\lambda}_{\mu,\kappa}(q) = \sum_{\mu^* \in \mathcal{P}_{|\mu|+\kappa_\ell}} B^{\lambda}_{\mu^*,\kappa^*}(q) B^{\mu^*}_{\mu,(\kappa_\ell)}(q).$$

Une récurrence sur $|\kappa|$ montre alors immédiatement que $B^{\lambda}_{\mu,\kappa}(q)$ est un polynôme en q, à coefficients entiers positifs, l'initialisation de la récurrence provenant de la question a).

c) Soit $(F_0, \ldots, F_\ell) \in B^{\lambda}_{\mu,\kappa}$. Montrons par récurrence sur $i \geq 1$ que si pour tout $j \leq i$, $\kappa_j \geq \dim\ker(u^{j-1}) - \dim\ker(u^j)$, alors $F_j = \mathrm{Im}(u^j)$. Par hypothèse, $F_0 = E$ et $F_1 \subset u(F_0)$ donc $F_1 \subset \mathrm{Im}(u)$. Comme on a supposé $\kappa_1 \geq \mathrm{rg}(u)$, on a égalité et $F_1 \subset \mathrm{Im}(u)$. L'hérédité se démontre de la même façon en utilisant l'hypothèse $\kappa_i \geq \dim\ker u^i - \dim\ker u^{i-1} = \dim F_{i-1} - \mathrm{rg}(u^i) \geq \dim F_{i-1} - \dim F_i = \kappa_i$, d'où l'égalité $F_i = \mathrm{Im}(u^i)$.
Dans le cas où $\mu = \emptyset$, on a $|\kappa| = |\lambda| = n$. Lorsque $\nu = \kappa'$, la suite définie par $F_i = \mathrm{Im}\ u^i$ convient et la discussion précédente montre que c'est la seule.

Lorsque $\kappa' \not\leq \nu$, la discussion précédente montre qu'il ne peut exister de telle suite : en effet, comme $|\kappa| = |\nu|$, on peut les comparer, et en prenant i minimal tel que $\kappa_1 + \cdots + \kappa_i > \nu'_1 + \cdots + \nu'_i$, une telle suite vérifierait nécessairement $F_j = \operatorname{Im} u^j$ pour $j < i$, et $\dim F_i > \operatorname{rg}(u^i)$, ce qui est impossible car $u(F_i) \subset F_{i-1}$. On a donc les résultats attendus.

d) Lorsque $\kappa = \kappa_1$ et $B^\lambda_{\mu,\kappa} \neq 0$, on a d'après a) :

$$\deg B^\lambda_{\mu,\kappa} = \sum_{1\leq i\leq j\leq r} (e_i - f_i)f_j = \sum_{2\leq i\leq j\leq r+1} (\lambda'_{i-1} - \mu'_{i-1})(\mu'_{j-1} - \lambda'_j) = \sum_{1\leq i\leq j\leq r} (\lambda'_i - \mu'_i)(\mu'_j - \lambda'_{j+1}).$$

En récrivant $\mu'_j - \lambda'_{j+1} = \mu'_j - \lambda'_j + \lambda'_j - \lambda'_{j+1}$, il vient :

$$\deg B^\lambda_{\mu,\kappa} = \sum_{i=1}^r (\lambda'_i - \mu'_i) \sum_{j=i}^r (\lambda'_j - \lambda'_{j+1}) - \sum_{1\leq i\leq j\leq r} (\lambda'_i - \mu'_i)(\lambda'_j - \mu'_j).$$

Le premier terme vaut $\sum_{i=1}^r \lambda'^2_i - \sum_{i=1}^r \lambda'_i\mu'_i$. Comme $\kappa_1 = \sum_{i=1}^r (\lambda'_i - \mu'_i)$, le deuxième terme vaut :

$$\frac{1}{2}\left[\left(\sum_{i=1}^r (\lambda'_i - \mu'_i)\right)^2 + \sum_{i=1}^r (\lambda'_i - \mu'_i)^2\right] = \frac{1}{2}\left(\kappa_1^2 + \sum_{i=1}^r \lambda'^2_i + \sum_{i=1}^r \mu'^2_i - 2\sum_{i=1}^2 \lambda'_i\mu'_i\right).$$

La différence des deux vaut donc :

$$\deg B^\lambda_{\mu,\kappa} = \frac{1}{2}\left(\sum_{i=1}^r \lambda'^2_i - \sum_{i=1}^r \mu'^2_i - \kappa_1^2\right) = d(\lambda) - d(\mu) - d(\kappa').$$

On peut maintenant traiter le cas général. Montrons par récurrence sur la longueur ℓ de $\kappa|$ que pour tous λ, κ, μ tels que $B^\lambda_{\mu,\kappa} \neq 0$, on a $\deg B^\lambda_{\mu,\kappa} = d(\lambda) - d(\mu) - d(\kappa')$. Le résultat est vrai pour $\ell = 1$ d'après ce qui précède. Supposons-le vrai pour un $\ell \geq 1$, alors d'après la formule du b), on a

$$B^\lambda_{\mu,\kappa} = \sum_{\mu^* \in \mathcal{P}_{|\mu|+\kappa_\ell}} B^\lambda_{\mu^*,\kappa^*} B^{\mu^*}_{\mu,(\kappa_\ell)}.$$

Lorsque cette somme est vide, on a $B^\lambda_{\mu,\kappa} = 0$. Si cette somme est non vide, alors comme ces polynômes sont à coefficients positifs, on a : $\deg B^\lambda_{\mu,\kappa} = \max_{\mu^* \in \mathcal{P}_{|\mu|+\kappa_\ell}} \deg B^\lambda_{\mu^*,\kappa^*} B^{\mu^*}_{\mu,(\kappa_\ell)}$. Par hypothèse de récurrence, $\deg B^\lambda_{\mu^*,\kappa^*} B^{\mu^*}_{\mu,(\kappa_\ell)}$ vaut $d(\lambda) - d(\mu^*) - d((\kappa^*)') + d(\mu^*) - d(\mu) - d((\kappa_\ell)')$, c'est-à-dire :

$$\deg B^\lambda_{\mu^*,\kappa^*} B^{\mu^*}_{\mu,(\kappa_\ell)} = d(\lambda) - d(\mu) - \frac{1}{2}\sum_{i=1}^\ell \kappa_i(\kappa_i - 1) = d(\lambda) - d(\mu) - d(\kappa').$$

Cela démontre bien le résultat attendu.

29. Supposons dans un premier temps qu'on a bien l'égalité :

$$B^\lambda_{\mu,\kappa}(q) = \sum_{\nu\in\mathcal{P}} |\mathcal{G}^\lambda_{\mu,\nu}(\mathbf{F}_q)| B^\nu_{\emptyset,\kappa}(q).$$

Montrons par récurrence forte sur κ' que $|\mathcal{G}^\lambda_{\mu,\kappa}(\mathbf{F}_q)|$ est une fonction polynomiale de q de degré $\leq d(\lambda) - d(\mu) - d(\kappa)$. Cela est légitime, car l'ordre défini sur $\mathcal{P}$ est bien fondé, et ses éléments minimaux sont les partitions de la forme $(1, \ldots, 1)$ (il est clair qu'il ne peut y avoir d'élément strictement plus petit qu'un élément de cette forme, et un tel élément de longueur n est plus petit que toutes les autres partitions de n).
Montrons d'abord le résultat lorsque κ' est minimal (auquel cas $\kappa = (\kappa_1)$ est maximal). La somme dans la relation précédente comporte alors un seul terme non nul d'après 28.c), et ce terme correspond à $\nu = \kappa'$. On a donc $B^\lambda_{\mu,(\kappa_1)}(q) = |\mathcal{G}^\lambda_{\mu,(\kappa_1)'}(\mathbf{F}_q)| B^{(\kappa_1)'}_{\emptyset,(\kappa_1)}(q) = |\mathcal{G}^\lambda_{\mu,(\kappa_1)'}(\mathbf{F}_q)|$. Cela montre que $|\mathcal{G}^\lambda_{\mu,(\kappa_1)'}(\mathbf{F}_q)|$ est bien un polynôme en q, de degré $d(\lambda) - d(\mu) - d(\kappa)$.
Pour l'hérédité, supposons le résultat acquis pour toutes les partitions ν telles que $\nu < \kappa'$. Les seuls termes non nuls de la somme précédente correspondent à $\kappa \leq \nu'$, c'est-à-dire $\nu \leq \kappa'$ (le fait que l'opération $\nu \mapsto \nu'$ soit décroissante s'observe immédiatement sur les diagrammes de Ferrers), et on a alors :

$$|\mathcal{G}^\lambda_{\mu,\kappa}(\mathbf{F}_q)| = B^\lambda_{\mu,\kappa}(q) - \sum_{\nu<\kappa'} |\mathcal{G}^\lambda_{\mu,\nu}(\mathbf{F}_q)| B^\nu_{\emptyset,\kappa}(q),$$

qui est bien une fonction polynomiale de q par hypothèse de récurrence. En outre, cette formule, la question 28.d) et l'hypothèse de récurrence montrent que $|\mathcal{G}^\lambda_{\mu,\kappa}(\mathbf{F}_q)|$ est de degré $\leq d(\lambda) - d(\mu) - d(\kappa)$.
Il nous reste donc à démontrer la relation :

$$B^\lambda_{\mu,\kappa}(q) = \sum_{\nu\in\mathcal{P}} |\mathcal{G}^\lambda_{\mu,\nu}(\mathbf{F}_q)| B^\nu_{\emptyset,\kappa}(q).$$

Pour chaque $\mathbf{F}_q$-espace vectoriel G de dimension finie muni d'un endomorphisme nilpotent v tel que (G, v) soit de type μ, on fixe une base de G comme à la question 13., de sorte que la matrice de v dans cette base soit J_μ. Ce choix de base fournit un isomorphisme $\varphi_G : G \to \mathbf{F}_q^{|\mu|}$ tel que $u \circ \varphi_G = \varphi_G \circ v$. Pour ce qui suit, il nous suffit en fait de faire ces choix de bases pour les sous-espaces vectoriels quotients de E, ce qui épargne l'utilisation de l'axiome du choix.
Soit $(F_0, \ldots, F_\ell) \in \mathcal{B}^\lambda_{\mu,\kappa}(\mathbf{F}_q)$. On peut associer à cette suite de sous-espaces le couple $(F_\ell, (E/F_\ell, \ldots, \{0\}))$. Soit ν le type de $(E/F_\ell, u_{E/F_\ell})$, alors par hypothèse, $F_\ell \in \mathcal{G}^\lambda_{\mu,\nu}(\mathbf{F}_q)$, et $(\varphi_{E/F_\ell}(E/F_\ell), \ldots, \{0\}) \in \mathcal{B}^\nu_{\emptyset,\kappa}(\mathbf{F}_q)$.
On a donc défini une application :

$$\mathcal{B}^\lambda_{\mu,\kappa}(\mathbf{F}_q) \to \bigsqcup_{\nu\in\mathcal{P}} \mathcal{G}^\lambda_{\mu,\nu}(\mathbf{F}_q) \times \mathcal{B}^\nu_{\emptyset,\kappa}(\mathbf{F}_q).$$

Il suffit de montrer que cette application est une bijection.
Pour la surjectivité, soit $(F, (G_0, \ldots, G_\ell = \{0\})) \in \mathcal{G}^\lambda_{\mu,\nu}(\mathbf{F}_q) \times \mathcal{B}^\nu_{\emptyset,\kappa}(\mathbf{F}_q)$. Pour $1 \leq i \leq \ell$, posons $G'_i = \varphi^{-1}_{E/F}(G_i)$: les G'_i sont des sous-espaces vectoriels de E/F stables par $u_{E/F}$. Soit π la projection canonique $E \to E/F$ (qui commute avec u), alors en posant $F_i = \pi^{-1}(G_i)$ on obtient une suite $(F_0, \ldots, F_\ell)$ de sous-espaces de E stables par u, telle que $F_0 = E$, $F_\ell = F$, et on a donc $(F_0, \ldots, F_\ell) \in \mathcal{B}^\lambda_{\mu,\kappa}(\mathbf{F}_q)$ car π^{-1} préserve les codimensions. De plus, par construction, l'image de cette famille par l'application définie précédemment est $(F, (G_0, \ldots, G_\ell))$.
Pour l'injectivité, si $(F_0, \ldots, F_\ell)$ et $(F'_0, \ldots, F'_\ell)$ ont la même image $(F, (G_0, \ldots, G_\ell))$

par cette application, alors $F_\ell = F'_\ell$, et donc $\varphi_{E/F_\ell} = \varphi_{E/F'_\ell}$, ce qui montre aussi que $F_i/F_\ell = \varphi^{-1}_{E/F_\ell}(F_i) = F'_i/F_\ell$ et donc que $\pi(F_i) = \pi(F'_i)$. Comme F_i, F'_i contiennent F_ℓ, on a bien $(F_0, \ldots, F_\ell) = (F'_0, \ldots, F'_\ell)$. On a donc établi l'existence d'une bijection :

$$\mathcal{B}^\lambda_{\mu,\kappa}(\mathbf{F}_q) \to \bigsqcup_{\nu\in\mathcal{P}} \mathcal{G}^\lambda_{\mu,\nu}(\mathbf{F}_q) \times \mathcal{B}^\nu_{\emptyset,\kappa}(\mathbf{F}_q),$$

l'égalité des cardinaux :

$$B^\lambda_{\mu,\kappa}(q) = \sum_{\nu\in\mathcal{P}} |\mathcal{G}^\lambda_{\mu,\nu}(\mathbf{F}_q)| B^\nu_{\emptyset,\kappa}(q)$$

en découle immédiatement.

30. On a démontré cette majoration du degré par récurrence sur ν dans la première partie de la question précédente.

31. Le produit $h_0 \cdots h_{n-1}$ est somme d'au plus $n!$ produits décroissants, où les facteurs de chaque produit forment une famille alphabétique dont le plus petit facteur est $\geq \min\{h_j \mid 0 \leq j \leq n-1\}$. En effet :

$$\begin{aligned} h_0h_1h_2h_3 &= (h_0,h_1)h_2h_3 + h_1(h_0,h_2)h_3 + h_1h_2(h_0,h_3) + h_1h_2h_3h_0 \\ &= ((h_0,h_1),h_2)h_3 + h_2((h_0,h_1)h_3) + h_2h_3(h_0,h_1) + \cdots \end{aligned}$$