INTRODUCTION

Ce livre propose les énoncés et les corrigés des épreuves de mathématiques générales de l'agrégation externe de mathématiques des dix dernières années (de 1989 à 1998). A notre connaissance, il vient combler un vide éditorial. Nous avons souhaité en faire le complément du "Problèmes d'analyse pour l'agrégation" publié dans la même collection : un pivot pour organiser son travail en vue du concours. En effet si l'on met de côté la pratique des leçons d'oral, exercices nécessitant une solide préparation spécifique, l'année de l'agrégation présente deux caractéristiques essentielles :

- Ce doit être une année de révision, de mise à plat et de structuration des connaissances qui ont été acquises jusqu'en maîtrise, parfois de façon éparse tout au long de modules universitaires distincts.
- Ce doit être une année d'entraînement et il faut véritablement entendre ce terme dans son acception sportive de pratique régulière et intensive.

Ceci vaut spécialement pour l'épreuve de mathématiques générales qu'il n'est pas facile de définir rigoureusement en quelques mots mais dont on pourrait presque dire qu'elle recouvre tout ce qui n'est pas du ressort exclusif de l'analyse ou des disciplines optionnelles, avec comme évident noyau central l'algèbre et la géométrie. Le corollaire immédiat est qu'elle fait appel à un spectre étendu de culture mathématique, à une vision transversale globale du programme, que l'on n'a pas toujours l'occasion de mettre en pratique lors de sa scolarité universitaire.

Il n'y a pas de meilleur moyen de remplir ces deux objectifs que de chercher à résoudre des problèmes d'agrégation. Ceux-ci, en plus de constituer le meilleur exemple de ce qui attend le futur candidat, sont difficiles (c'est en quelque sorte le summum au niveau de l'enseignement universitaire) et offrent une photographie aussi complète que précise des connaissances et compétences exigibles des candidats, étant minutieusement construits dans ce but. Les commentaires que nous avons placés après chaque corrigé et qui ne se subsituent absolument pas aux rapports des concours qu'il faut consulter, sont justement là pour aider le candidat à s'organiser en lui fournissant un aperçu rapide du problème en question, et le cas échéant une clarification sur un point laissé volontairement dans l'ombre par l'énoncé.

Nous espérons que le profit retiré de cet ouvrage par ses futurs lecteurs, qui déborderont peut-être du cadre strict des candidats au concours comme le laisse supposer l'actuel succès de cette collection, sera proportionnel au plaisir qu'ont pris ensemble ses auteurs en le rédigeant.

Table des matières

Chapitre 1

Session de 1989

1.1 Sujet

1.2 Correction

I. Préliminaires

A. *Dans cette partie, p est un nombre premier impair.*

1.a. On remarque que l'hypothèse w non nul n'est pas nécessaire : il y a dans ce cas une solution triviale. $\mathbb{F}_p^*$ est un groupe. Soient u et v dans $\mathbb{F}_p^*$, ils sont en particulier inversibles. Rappelons le fait classique suivant : l'ensemble $C = \{z^2 | z \in \mathbb{F}_p\}$ possède $\frac{p+1}{2}$ éléments.

En effet : $C = \{z^2 | z \in \mathbb{F}_p^*\} \cup \{0\}$ or l'application k de $\mathbb{F}_p^*$ dans $\mathbb{F}_p^*$ qui à z associe z^2 est un morphisme de groupe dont le noyau est déterminé par $(z \in \mathbb{F}_p^*)$:

$k(z) = 1 \Leftrightarrow (z-1)(z+1) = 0 \Leftrightarrow z = 1$ ou $z = -1$ car $\mathbb{F}_p$ est un anneau intègre.

On en déduit $\ker(k) = \{-1, 1\}$. De plus, $\mathrm{Im}(k)$ est isomorphe à $\mathbb{F}_p^*/\ker(k)$. Comme $\mathrm{Im}(k)$ est par définition $\{z^2 | z \in \mathbb{F}_p^*\}$, on obtient : $|\{z^2 | z \in \mathbb{F}_p^*\}| = \frac{p-1}{2}$ d'où $|C| = \frac{p+1}{2}$.

Considérons la translation à gauche τ_u par u : pour tout z dans $\mathbb{F}_p$, $\tau_u(z) = uz$. On a $\tau_u(C) = \{ux^2 | x \in \mathbb{F}_p\}$. Comme u est inversible dans $\mathbb{F}_p$, τ_u est une bijection donc $|\tau_u(C)| = |C| = \frac{p+1}{2}$.

De même, on considère l'application f de $\mathbb{F}_p$ dans $\mathbb{F}_p$ qui à z associe $f(z) = w - vz$. Comme v est inversible dans $\mathbb{F}_p$, f est une bijection. On a donc $|f(C)| = |C| = \frac{p+1}{2}$. De plus, par définition, $f(C) = \{w - vy^2 | y \in \mathbb{F}_p\}$.

On remarque que $|\tau_u(C)| + |f(C)| = p+1 > |\mathbb{F}_p|$ donc que $\tau_u(C) \cap f(C) \neq \emptyset$. Soit $z \in \tau_u(C) \cap f(C)$, z s'écrit d'une part ux^2 avec $x \in \mathbb{F}_p$ et d'autre part, $w - vy^2$ avec $y \in \mathbb{F}_p$. On a alors $ux^2 + vy^2 = w$.

1.b. On commence par remarquer que, si a et b sont des entiers relatifs : $a^2 + ab + nb^2 + 1 = (a + \frac{b}{2})^2 + (4n-1)(\frac{b}{2})^2 + 1$.

On considère l'équation dans $\mathbb{F}_p$: $x^2 + \overline{(4n-1)}y^2 = \overline{-1}$, où $\bar{h}$ désigne la classe d'un entier h. Comme p ne divise pas $4n-1$, $\overline{(4n-1)} \neq \bar{0}$. On a aussi $\overline{-1} \neq \bar{0}$. D'après la question 1.a, il existe une solution $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ à l'équation précédente. En considérant des représentants de x et y, on a l'existence de r et s dans $\mathbb{Z}$ tels que : $r^2 + (4n-1)s^2 = -1 + mp$, où $m \in \mathbb{Z}$ (et puisque le membre de gauche est positif, nécessairement : $m \geq 1$) . On pose $b = 2s$ et $a = r - s = r - \frac{b}{2}$. a et b sont des entiers et $(a + \frac{b}{2})^2 + (4n-1)(\frac{b}{2})^2 + 1 = mp$. La remarque initiale donne le résultat.

2. On rappelle que $P(t) = t^4 + 1$ est réductible dans $\mathbb{F}_p$ (cf le Cours d'Algèbre de D. Perrin : ch.III.15). Pour exhiber un corps de rupture de P, on peut par exemple considérer $K = \mathbb{F}_p(b)$ où b est une racine de P dans un corps de décomposition de P. Comme $b^4 = -1$, $b \neq 0$ donc inversible (K est un corps).

2.a. On a $x^2 = b^2 - 2 + b^{-2} = b^{-2}(b^4 + 1) - 2 = -2$.

Comme K est une extension de $\mathbb{F}_p$, sa caractéristique est p. Soit $f(z) = z^p$ le Frobenius de K. On a $f(b - b^{-1}) = f(b) - f(b^{-1})$ (on rappelle que ceci se démontre via le binôme de Newton et le fait que p divise C_p^k pour $1 \leq k \leq p-1$). Ainsi :

si $p = 8k+1$: $f(x) = b.(b^8)^k - b^{-1}(b^{-1})^8$ car $b^4 = -1$ donc $f(x) = x$.

si $p = 8k+3$: $f(x) = b^3 - (b^{-1})^3 = -b^{-1} + b$ car $b^4 = -1$ ie $b^3 = -b^{-1}$ donc $f(x) = x$.

D'après le (petit) théorème de Fermat, on a $\mathbb{F}_p \subset \{k \in K | k^p - k = 0\}$. Comme $X^p - X$ a au plus p racines dans le corps K, $\mathbb{F}_p = \{k \in K | k^p - k = 0\}$. D'après le résultat précédent, $x^p - x = 0$ donc $x \in \mathbb{F}_p$.

2.b. On déduit de 2.a que -2 est un carré dans $\mathbb{F}_p$ donc $(-2)^{-1}$ aussi. Il existe x dans $\mathbb{F}_p$ tel que $x^2 = (-2)^{-1}$ donc on a : $2x^2 + 1 = 0$. En "remontant" dans $\mathbb{Z}$ (autrement dit, en choisissant un représentant), il existe a et q dans $\mathbb{N}$ tel que $2a^2 + 1 = qp$. Comme p est impair, q est nécessairement impair donc s'écrit $2m - 1$ avec m dans $\mathbb{N}$.

On considère la matrice :

$$M = \begin{pmatrix} p & a & 0 \\ a & m & 1 \\ 0 & 1 & 2 \end{pmatrix}.$$

On a $\det(M) = p(2m-1) - 2a^2 = 1$ et M est clairement symétrique réelle. Pour montrer que M est définie positive, nous proposons deux méthodes.

La première utilise un résultat classique : il suffit de montrer que les mineurs principaux sont tous strictement positifs. Le premier vaut $p > 0$ et le second : $mp - a^2 = \frac{1}{2}(p+1) > 0$. Le troisième vaut $\det(M) = 1 > 0$. Ainsi M est définie positive.

La seconde méthode est élémentaire et à peine plus calculatoire. Pour tout vecteur (x, y, z) de $\mathbb{R}^3$, on calcule ${}^tXMX$:

$${}^tXMX = (x, y, z) \begin{pmatrix} p & a & 0 \\ a & m & 1 \\ 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = px^2 + 2axy + my^2 + 2yz + 2z^2.$$

La méthode de Gauss donne :

$${}^tXMX = p\big(x + p^{-1}ay\big)^2 + \big(m - p^{-1}a^2\big)\big(y + \frac{p}{mp - a^2}z\big)^2 + \big(2 - \frac{p}{mp - a^2}\big)z^2.$$

où $mp - a^2 = \dfrac{1}{2}(p+1) > 0$ et $2 - \dfrac{p}{mp - a^2} > 0 \Leftrightarrow (2m-1)p - 2a^2 > 0$ or $(2m-1)p - 2a^2 = 1$. Ainsi, M est définie positive.

Résolution du cas $p = 17$. Il y a deux solutions à l'équation $\mathbb{F}_p$: $2x^2 + 1 = 0$ car $r^2 = s^2 \Leftrightarrow r = \pm s$. Ici les solutions modulo 17 sont 5 et -5 (qui est égal à 12 modulo 17). On cherche les solutions sous la forme $a = 5 + 17q$ et $a = 12 + 17q$.

Si $a = 5+17q$ alors $17q^2+10q+2 = m$ donc $(a, m) = (5+17q, 17q^2+10q+2)$ où $q \in \mathbb{Z}$.

Si $a = 12+17q$ alors $17q^2+24q+9 = m$ donc $(a, m) = (12+17q, 17q^2+24q+9)$ où $q \in \mathbb{Z}$.

B. *Soit $D \geq 1$ non divisible par le carré d'un nombre premier.*

1. La matrice $\begin{pmatrix} p & a + b\omega_D \\ a + b\overline{\omega_D} & m \end{pmatrix}$ est clairement hermitienne.

Si $D \equiv 3$ [4] : $\frac{D+1}{4} \in \mathbb{N}$ et le A.1.b assure l'existence de a, b, m dans $\mathbb{Z}$ tels que $a^2 + ab + \frac{D+1}{4}b^2 + 1 = mp$ car p ne divise pas $D = 4n - 1$ où $n = \frac{D+1}{4}$.

Si $D \equiv 1$ ou 2 [4] : le A.1.a assure l'existence de a, b, m dans $\mathbb{Z}$ tels que $-1 + mp = a^2 + b^2 D$ car p ne divise pas D (ie $\bar{D} \neq \bar{0}$).

Dans chacun des cas, on remarque que m est nécessairement positif et que $\det(M) = mp - |a + b\omega_{_D}|^2 = 1$. M est hermitienne donc diagonalisable et les valeurs propres sont réelles. Comme $\det(M) = 1$, elles sont de même signe. Comme $Tr(M) = p + m > 0$, elles sont strictement positives. Ainsi, M est définie positive.

2.a. Si E est un ensemble, on désigne par $conv(E)$ l'enveloppe convexe de E. Ω le centre du cercle circonscrit est l'intersection des médiatrices. Notons comme d'habitude A', B', C' les milieux respectifs des segments $[BC], [AC], [AB]$. Les trois médiatrices séparent le triangle T en trois zones : $conv(A, C', \Omega, B')$, $conv(B, C', \Omega, A')$, $conv(C, A', \Omega, B')$. Soit M un point de T, M est dans une de ces trois zones : $conv(A, C', \Omega, B')$ pour fixer les idées. On a $AB \leq 2R$ car A et B appartiennent au disque de centre Ω et de rayon R. Ce disque est convexe donc $AC' \leq R$. De même $AB' \leq R$. Enfin, $A\Omega = R$ par définition. Ainsi, A, C', Ω et B' appartiennent au disque de centre A et de rayon R. Par convexité, ce disque contient $conv(A, C', \Omega, B')$ donc M. On conclut $AM \leq R$. Les cas $M \in conv(B, C', \Omega, A')$ et $M \in conv(C, A', \Omega, B')$ reviennent à considérer respectivement MB et MC.

2.b. On a $u \in \mathbb{Z}[\omega_{_D}] \iff u = \alpha + \beta\omega_{_D}$ où $\alpha, \beta \in \mathbb{Z}$. Pour tout z dans $\mathbb{C}$, on peut écrire $z = x + y\omega_{_D}$ où $x, y \in \mathbb{R}$. On a donc

$$k = \sup\Big\{ \inf_{\alpha,\beta\in\mathbb{Z}} \{|(x-\alpha) + (y-\beta)\omega_{_D}|^2\}; z \in \mathbb{C}, z = x + y\omega_{_D} \text{ avec } x, y \in \mathbb{R}\Big\}.$$

En approximant un réel par un entier relatif, on remarque que si E est un intervalle de longueur $\frac{1}{2}$:

$$k = \sup\Big\{ \inf_{\alpha,\beta\in\mathbb{Z}} \{|(x-\alpha) + (y-\beta)\omega_{_D}|^2\}; z = x + y\omega_{_D} \in \mathbb{C}; y \in [0, \frac{1}{2}]; x \in E\Big\}.$$

Ceci s'écrit encore

$$k = \sup\Big\{\inf\{d(M, N)^2; N \in \text{réseau de points à affixe dans } \mathbb{Z}[\omega_{_D}]\}; M \in \mathcal{E}\Big\}$$

$$\text{où} \quad \mathcal{E} = \big\{M; \text{l'affixe de } M \text{ s'écrit } x + y\omega_{_D} \text{ avec } y \in [0, \frac{1}{2}], x \in E\big\}.$$

Pour $D \equiv 3$ [4], on choisit $E = [\frac{1}{4}, \frac{3}{4}]$ et pour $D \equiv 1$ ou 2 [4], on choisit $E = [0, \frac{1}{2}]$. On remarque que le rectangle $E + i[0, \frac{1}{2}]$ (on identifie les points et leurs affixes) est contenu dans le triangle T. On obtient l'inégalité :

$$k \leq \sup_{M\in T} \inf\{MA^2, MB^2, MC^2\}.$$

Enfin, on remarque qu'approximer par un entier dans la définition de k revient à raisonner modulo 1 sur les parties réelles et imaginaires de z. Ainsi,

$$k = \sup\Big\{\inf\{|(x-\alpha) + (y-\beta)\omega_{_D}|^2 / \alpha, \beta \in \mathbb{Z}\}; z \in \mathbb{C}, z = x + y\omega_{_D}; x, y \in [0, 1]\Big\}$$

le rectangle $[0,1]+i[0,1]$ contient le triangle T donc on a l'inégalité

$$k \geq \sup_{M\in T} \inf\{MA^2, MB^2, MC^2\}.$$

2.c. D'après les questions a et b, on a : $k \leq R^2$ et l'égalité est atteinte pour $M = \Omega$. On a donc : $k = R^2 = A\Omega^2$. Si on note ω l'affixe de Ω, on a $k = |\omega|^2$.

Si $D \equiv 1$ ou 2 $[4]$: Ω est l'intersection des médiatrices et un calcul élémentaire donne $\omega = \frac{\omega_D+1}{2}$ donc $k = \frac{D+1}{4}$.

Si $D \equiv 3$ $[4]$: ω a clairement pour partie réelle $\frac{1}{2}$. Ω est à égale distance de A, B et C donc $|\omega| = |\omega - 1| = |\omega - \omega_D|$. On obtient $\omega = \dfrac{1}{2} + i\dfrac{1-D}{4\sqrt{D}}$ donc $k = \frac{(1+D)^2}{16D}$.

2.d. Soient α et $\beta \neq 0$ dans $\mathbb{Z}[\omega_D]$. On pose $z = \frac{\alpha}{\beta}$. Par définition de k (par compacité, la borne inférieure est un minimum) : il existe γ dans $\mathbb{Z}[\omega_D]$ tel que $|z-\gamma|^2 \leq k$. Ainsi, $|\alpha - \gamma\beta|^2 \leq k|\beta|^2$.

Pour $k < 1$, on en déduit que α s'écrit $\gamma\beta + r$ où r vérifie $|r|^2 = |\alpha - \gamma\beta|^2 \leq k|\beta|^2 < |\beta|^2$. Le raisonnement précédent est valable pour tout α et $\beta \neq 0$ dans $\mathbb{Z}[\omega_D]$ donc $\mathbb{Z}[\omega_D]$ est un anneau euclidien (dont une norme N est le carré du module).

Il suffit de trouver D tel que $k < 1$.

Si $D \equiv 1$ ou 2 $[4]$: $k = \frac{D+1}{4} < 1$ pour $D = 1$ ou 2.

Si $D \equiv 3$ $[4]$: $k = \frac{(1+D)^2}{16D} < 1$ pour $D = 3, 7$ ou 11.

Application : pour $D = 2$, $\omega_2 = i\sqrt{2}$ et $k = \frac{3}{4}$. $\dfrac{\alpha}{\beta} = \dfrac{13}{19} - \dfrac{18i\sqrt{2}}{19}$. On peut écrire $\dfrac{\alpha}{\beta} = 1 - i\sqrt{2} + (\dfrac{-6}{19} + \dfrac{i\sqrt{2}}{19})$ et $|\dfrac{-6}{19} + \dfrac{i\sqrt{2}}{19}| \leq k$. On peut aussi écrire $\dfrac{\alpha}{\beta} = i\sqrt{2} + (\dfrac{13}{19} + \dfrac{i\sqrt{2}}{19})$ et $|\dfrac{13}{19} + \dfrac{i\sqrt{2}}{19}| \leq k$. Il n'y a pas d'autres possibilités et on trouve donc pour γ deux valeurs possibles : $1 - i\sqrt{2}$ et $i\sqrt{2}$.

II. Matrices hermitiennes de la forme B^*B.

1. On note S^* l'ensemble des inversibles de S. Comme A et B sont congruentes, $A = UBU^*$ où $B \in GL(n,S)$. On a $\det(A) = \det(B)|\det(U)|^2$. Comme $U \in GL(n,S)$, il existe V dans $GL(n,S)$ telle que $UV = VU = I$. Donc $\det(U)\det(V) = 1$ et $\det(U) \in S^*$.

On rappelle le résultat classique :

$$(R) \qquad S^* = \{s \in S;\ |s| = 1\}.$$

Effectivement, soit $s \in S^*$, il existe r dans S tel que $rs = 1$. En passant aux modules, on obtient : $|r|^2|s|^2 = 1$ or $|r|^2, |s|^2 \in \mathbb{N}$ donc nécessairement : $|s|^2 = 1$. Inversement, si $|s| = 1$ alors $s\bar{s} = 1$ donc s est inversible dans S (car $\bar{s} \in S$). Ce qui prouve (R).

Ainsi, $|\det(U)| = 1$ et $\det(A) = \det(B)$.

2.a. Soit x dans $S^n \setminus \{0\}$, $xAx^* \in \mathbb{R}^{+*}$ car A est définie positive. D'autre part, $xAx^* \in S$. Comme $\mathbb{R}^{+*} \cap S = \mathbb{N} \setminus \{0\}$, l'ensemble $\{xAx^* | x \in S^n \setminus \{0\}\}$ est une partie non vide de $\mathbb{N} \setminus \{0\}$ donc admet un plus petit élément $m(A)$. Celui-ci est atteint pour un certain $z \in S^n \setminus \{0\}$ vérifiant $zAz^* = m(A)$.

On peut écrire $z = (z_1, \cdots, z_n)$. Soit $u \in S \setminus \{0\}$ tel que u divise z_i pour tout $1 \leq i \leq n$. On a

$$zAz^* = \sum_{i,j=1}^{n} A_{i,j} z_j \bar{z}_i = |u|^2 yAy^*.$$

où on a posé $y = (y_1, \cdots, y_n)$ avec $y_i \in S$ tel que $uy_i = z_i$.

Comme $|u|^2 \geq 1$ (car non nul), $m(A) = zAz^* = |u|^2 yAy^* \geq yAy^* \geq m(A)$. Donc $|u|^2 = 1$ et u est inversible dans S. Les composantes de z sont premières entre elles.

2.b.

$$S^n \setminus \{0\} = \{(xU)^* | x \in S^n \setminus \{0\}\} \quad \text{car } U \in GL(n, S).$$

donc $m(A) = m(B)$.

2.c. Clairement, $m(A) \leq 2$ car le vecteur $z = (1, 0)$ vérifie $zAz^* = 2$. Cherchons si $zAz^* = 1$ a une solution.

Cette équation s'écrit en posant $z = (x, y)$: $2x^2 + 14xy + 25y^2 = 1$ soit $(2x + 7y)^2 + y^2 = 2$ ce qui est vérifié pour $x = 4$ et $y = -1$. Donc $m(A) = 1$.

A. *Le cas* $n = 2$.

1.a. z s'écrit (x, y) où x et y sont premiers entre eux d'après la question 2.a. Le théorème de Bezout s'applique car S est euclidien donc principal : il existe $u, v \in S$ tels que $ux + vy = 1$.

$$\text{La matrice } U_o = \begin{pmatrix} x & -v \\ y & u \end{pmatrix} \in GL(2, S) \quad \text{car le déterminant vaut 1.}$$

ceci se voit aussi avec la relation :

$$U_o \begin{pmatrix} u & v \\ -y & x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

La matrice $B = U_o^*.A.U_o$ est congruente à A et on a :

$$\begin{aligned} b_{1,1} &= \bar{x}(a_{1,1}x + a_{1,2}y) + \bar{y}(\bar{a}_{1,2}x + a_{2,2}y) \\ &= a_{1,1}|x|^2 + 2Re(\bar{a}_{1,2}y\bar{x}) + a_{2,2}|y|^2 \\ &= zAz^* = m(A). \end{aligned}$$

1.b. D'après le I.B.2.d. dans le cas $S = \mathbb{Z}[\omega_D]$ et d'après l'approximation d'un réel par un entier dans le cas $S = \mathbb{Z}$, il existe s dans S tel que : $|b_{1,1}s + b_{1,2}| \leq \sqrt{k} b_{1,1}$. car $b_{1,1} \geq 1$. On définit la matrice

$$C = \begin{pmatrix} 1 & 0 \\ \bar{s} & 1 \end{pmatrix} B \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} m(A) & m(A)s + b_{1,2} \\ m(A)\bar{s} + \bar{b}_{1,2} & m(A)|s|^2 + +2Re(s\bar{b}_{1,2}) + b_{2,2} \end{pmatrix}.$$

On remarque que la matrice $\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$ est inversible, d'inverse $\begin{pmatrix} 1 & -s \\ 0 & 1 \end{pmatrix}$.

C est hermitienne et congruente à B donc à A. Ainsi, $m(A) = m(C)$. On a $a = c_{1,1} = m(A) = m(C)$. La remarque du début de question donne $(\sqrt{k})^{-1}|b| \leq b_{1,1} = m(A)$.

Enfin, avec $z = (0, 1)$, on a $c \geq m(C) = a$.

1.c. Comme $\det(A) = \det(C)$, $d = ac - |b|^2$. On a $|b|^2 \leq ka^2$ donc $d \geq ac - ka^2 \geq (1-k)a^2$. On obtient : $\sqrt{d}(1-k)^{-\frac{1}{2}} \geq a = m(A)$.

1.d. A une matrice hermitienne définie positive de déterminant d. D'après les questions précédentes, A est congruente à une matrice C vérifiant (i) et (ii) dans 1.b. et d'après 1.c., le nombre de valeurs possibles pour $a = m(A)$ est fini.

$|b|^2 \leq k|a|^2$ donc $|b|^2 \in \mathbb{N}$ ne peut prendre qu'un nombre fini de valeurs. A fortiori, comme $b \in \mathbb{Z}[\omega_D]$, b ne peut prendre qu'un nombre fini de valeurs.

Enfin, $c = \frac{d-|b|^2}{a}$ donc c ne peut prendre qu'un nombre fini de valeurs.

Donc le nombre de classes de congruence est fini.

2.a. Pour chacune des possibilités de S, on constate que $(1-k)^{-\frac{1}{2}} < 2$. On a donc $1 \leq m(A) < 2$. Comme $m(A)$ est un entier, $m(A) = 1$.

Si on considère la matrice C comme dans 1.b., on a : $|b|^2 \leq k < 1$ donc $b = 0$. Enfin, comme $d = 1$, on a $c = 1$. Finalement $C = I_2$. Comme A et I_2 sont congruentes, il existe $B \in GL(2, S)$ telle que $A = B^*B$.

2.b. Soit D tel que p ne divise pas D. D'après la question I.B.1., il existe des entiers relatifs a, b, m tels que

$$A = \begin{pmatrix} p & a + b\omega_D \\ a + b\overline{\omega_D} & m \end{pmatrix} \quad \text{est hermitienne définie positive et } \det(A) = 1.$$

$$A = BB^* \text{ où } \mathcal{B} = \begin{pmatrix} r & s \\ u & v \end{pmatrix} \in GL(2, S).$$

En identifiant le coefficient $(1, 1)$ dans les matrices, on obtient la relation : $p = |r|^2 + |s|^2$, avec $r, s \in S$.

i) Pour $D = 1$, r et s s'écrivent $x + iy$ et $n + im$, où $x, y, n, m \in \mathbb{Z}$. Donc, $p = x^2 + y^2 + n^2 + m^2$.

ii) Si $p = 3$, on remarque que $3 = 1^2 + 1.1 + 1^2$.. Comme $D = 3$ et $p \neq 3$ (p ne divise pas D), il existe $x, y, n, m \in \mathbb{Z}$ tels que $p = x^2 + x.y + y^2 + n^2 + n.m + m^2$.

iii) Si $p = 7$, on remarque que $3 = (-1)^2 + (-1).2 + 2.2^2$. Comme $D = 7$ et $p \neq 7$ (p ne divise pas D), il existe $x, y, n, m \in \mathbb{Z}$ tels que $p = x^2 + x.y + 2y^2 + n^2 + n.m + 2m^2$.

B. *Matrices symétriques à coefficients entiers.*

1.a. On remarque que la surjectivité de f assure l'existence de x. Soit $G_x = \mathbb{Z}x$ le sous-groupe engendré par x. Soit $y \in G_x \cap \ker(f)$, $y = qx$ avec $q \in \mathbb{Z}$ et $q = f(y) = 0$ donc $y = 0$. Ainsi $G_x \cap \ker(f) = \{0\}$. Soit $y \in \mathbb{Z}^n$, $f(y) \in \mathbb{Z}$ et $z = y - f(y)x \in \ker(f)$ donc y s'écrit $z + f(y)x$, avec $z \in \ker(f)$. On a donc $\mathbb{Z}^n = \ker(f) \oplus G_x$.

1.b.

$(i) \Rightarrow (ii)$ on pose $x = b_1$. On peut compléter $\{b_1\}$ en une base $\{b_j\}_j$ de $\mathbb{Z}^n$ d'après l'hypothèse (i). Soit M la matrice des coordonnées des vecteurs b_i dans la base canonique $\{e_j\}$ de $\mathbb{Z}^n$. La première colonne de M est ${}^t x$. De

plus, $M \in GL(n,\mathbb{Z})$ (cf P.Tauvel "mathématiques générales pour l'agrégation" ch.VIII ou S.Lang : "Algebra") car c'est une matrice de changement de base de $\mathbb{Z}$-module (en fait un simple calcul matriciel, formellement le même que pour les espaces vectoriels, le montre : l'inverse de M n'est autre que la matrice des coordonnées des vecteurs e_i dans la base $\{b_j\}$).

$(ii) \Rightarrow (iii)$ $M = \left({}^t x, v_2, \cdots, v_n\right)$ avec v_j vecteur à coordonnées dans $\mathbb{Z}$. M est inversible donc il existe une matrice N telle que $NM = I_n$. Le premier vecteur ligne de N est de la forme : $(a_1, \cdots, a_n)$ avec $a_i \in \mathbb{Z}$. Le calcul du coefficient $(1,1)$ du produit $NM = I_n$ donne : $\displaystyle\sum_{j=1}^{n} x_j a_j = 1$.

$(iii) \Rightarrow (iv)$ on considère le morphisme de groupe :

$$f \ : \ \begin{cases} \mathbb{Z}^n & \longrightarrow & \mathbb{Z} \\ (y_1, \cdots, y_n) & \longmapsto & \displaystyle\sum_{j=1}^{n} a_j y_j \end{cases}$$

on a $f(x) = 1$ par hypothèse donc, pour tout $n \in \mathbb{Z}$, $f(nx) = n$ et f est surjectif.

$(iv) \Rightarrow (i)$ la question 1.a donne : $\mathbb{Z}^n = \ker(f) \oplus \mathbb{Z}x$. Rappelons le fait suivant : tout sous-module de $\mathbb{Z}^n$ est libre de type fini. (voir compléments). Ainsi $\ker(f)$ est libre de type fini donc admet une base $\{b_1, \cdots, b_l\}$. D'où $\{x, b_1, \cdots, b_l\}$ est une base de $\mathbb{Z}^n$ et a posteriori $n = l + 1$.

2. $m(A) = zAz^*$ où $z \in \mathbb{Z}^n \setminus \{0\}$ et les composantes (z_j) de z sont premières entre elles (cf II.2.a.). D'après Bezout, il existe $u_1, \cdots, u_n$ tels que $\displaystyle\sum_{j=1}^{n} u_j z_j = 1$. Le critère (iii) de 1.b. implique l'existence de $M \in GL(n,\mathbb{Z})$ ayant pour premier vecteur colonne ${}^t z$. $B = M^* A M$ est congruente à A et $b_{1,1} = zAz^* = m(A)$.

3.a. Par hypothèse, on a $a_{1,1} y_1 = \displaystyle\sum_{i=1}^{n} a_{1,i} x_i$.

D'autre part,

$$\begin{aligned} a_{1,1} x A^t x &= a_{1,1} \sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,j} x_i x_j \\ &= a_{1,1} \sum_{i=2}^{n}\sum_{j=1}^{n} a_{i,j} x_i x_j + a_{1,1} x_1 \sum_{j=1}^{n} a_{1,j} x_j \\ &= a_{1,1} \sum_{i=2}^{n}\sum_{j=1}^{n} a_{i,j} x_i x_j + \big(\sum_{i=1}^{n} a_{1,i} x_i\big)\big(\sum_{j=1}^{n} a_{1,j} x_j\big) \\ &\qquad -\big(\sum_{i=2}^{n} a_{1,i} x_i\big)\big(\sum_{j=1}^{n} a_{1,j} x_j\big) \\ &= \sum_{i=2}^{n}\sum_{j=1}^{n} (a_{i,j} a_{1,1} - a_{1,i} a_{1,j}) x_i x_j + (a_{1,1} y_1)^2. \end{aligned}$$

Comme A est symétrique, on a une simplification pour $j = 1$ donc, compte-tenu de $x_i = z_{i-1}$ pour $i \geq 2$, on obtient :

$$a_{1,1} x A^t x = (a_{1,1} y_1)^2 + \sum_{i=2}^{n}\sum_{j=2}^{n} (a_{i,j} a_{1,1} - a_{1,i} a_{1,j}) z_{i-1} z_{j-1}.$$

Ainsi, $xA^tx = a_{1,1}y_1^2 + a_{1,1}^{-1}zB^tz$ avec $B_{i-1,j-1} = a_{i,j}a_{1,1} - a_{1,i}a_{1,j}$ pour $2 \leq i,j \leq n$. $B \in M_{n-1}(\mathbb{Z})$ est symétrique car A l'est. Comme $U^tx = {}^ty$, on peut écrire

$$U = \begin{pmatrix} 1 & & a_{1,i}.a_{1,1}^{-1} & & \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & & \ddots & & 0 \\ \vdots & & & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

On a la relation :

$${}^tU \begin{pmatrix} a_{1,1} & 0 \\ 0 & a_{1,1}^{-1}B \end{pmatrix} U = \begin{pmatrix} a_{1,1} & a_{1,i} \\ a_{1,i} & \tilde{B} \end{pmatrix}$$

avec $\tilde{B}_{i-1,j-1} = a_{1,i}.a_{1,j}.a_{1,1}^{-1} + a_{1,1}^{-1}B_{i-1,j-1} = a_{i,j}$ pour $2 \leq i,j \leq n$. Donc

$${}^tU \begin{pmatrix} a_{1,1} & 0 \\ 0 & a_{1,1}^{-1}B \end{pmatrix} U = A.$$

Montrons que B est définie positive. Comme U est inversible, on a pour tout vecteur $v = (v_1, \dots, v_n) \in \mathbb{Z}^n$

$$v \begin{pmatrix} a_{1,1} & 0 \\ 0 & a_{1,1}^{-1}B \end{pmatrix} {}^tv = (v^tU^{-1})A^t(v^tU^{-1}) \begin{cases} \geq 0 & \text{si } v \neq 0 \\ = 0 & \text{si } v = 0 \end{cases}$$

car A définie positive. La matrice $\begin{pmatrix} a_{1,1} & 0 \\ 0 & a_{1,1}^{-1}B \end{pmatrix}$ est donc symétrique et définie positive.
Par restriction au sous-espace $\{0\} \times \mathbb{R}^{n-1}$ de $\mathbb{R}^n$, $a_{1,1}^{-1}B$ donc B est définie positive (car $a_{1,1} = m(A) > 0$).

Enfin, $\det(A) = \det(U)^2.a_{1,1}\det(a_{1,1}^{-1}B)$. Or U est inversible et $|\det(U)| = 1$; de plus, B est une matrice d'ordre $n-1$ donc $\det(A) = a_{1,1}^{n-2}\det(B)$.

3.b. Montrons ceci par récurrence sur n. Soient $n \geq 2$ et H_n la proposition : "Pour toute matrice $A \in M_n(\mathbb{Z})$ symétrique et définie positive, on a $m(A) \leq \frac{4}{3}^{\frac{n-1}{2}} \det(A)^{\frac{1}{n}}$".

Pour $n = 2$, il suffit d'appliquer la question A.1.c.

Suppsons H_{n-1} vraie. Soit $z = (x_2, \dots, x_n) \in \mathbb{Z}^{n-1}$ tel que $zB^tz = m(B)$ (cf. II.2.a). On peut considérer un entier x_1 approximant le réel $-\sum_{i=2}^{n} a_{1,i}a_{1,1}^{-1}x_i$ à $\frac{1}{2}$ près donc $|y_1| \leq \frac{1}{2}$. L'inégalité $m(A) \leq xA^tx = a_{1,1}y_1^2 + a_{1,1}^{-1}m(B)$ donne alors $\frac{4}{3}m(A)^2 \leq m(B)$.

Or d'après l'hypothèse H_{n-1}, on a :

$$m(B) \leq \frac{4}{3}^{\frac{n-2}{2}} \det(B)^{\frac{1}{n-1}} \leq \frac{4}{3}^{\frac{n-2}{2}} m(A)^{\frac{n-2}{n-1}} \det(A)^{\frac{1}{n-1}}.$$

Finalement $\frac{4}{3}m(A)^2 \leq \frac{4}{3}^{\frac{n}{2}-1} m(A)^{\frac{n-2}{n-1}} \det(A)^{\frac{1}{n-1}}$ donc $m(A) \leq \frac{4}{3}^{\frac{n-1}{2}} \det(A)^{\frac{1}{n}}$.

Par récurrence, le résultat est vrai pour tout $n \geq 2$.

4.a. Pour $n \leq 5$, on remarque que $1 \leq m(A) < 2$ donc nécessairement $m(A) = 1$. On raisonne ensuite par récurrence sur n. Le cas $n = 2$ a été traité au A.2.

Pour $n \geq 3$, on suppose le résultat vrai pour $n-1$. On peut supposer $a_{1,1} = m(A) = 1$ d'après le 2) donc

$$A = {}^tU \begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix} U$$

et $\det(B) = \det(A) = 1$ donc $m(B) = 1$ (cf remarque initale). D'après l'hypothèse de récurrence, $B = {}^tQQ$ où $Q \in M_{n-1}(\mathbb{Z})$. On obtient

$$A = {}^tU \begin{pmatrix} 1 & 0 \\ 0 & {}^tQQ \end{pmatrix} U = {}^tU^t \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} U$$

et $\quad B = \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} U \quad$ convient pour avoir le résultat au rang n.

4.b. D'après le I.2, il existe a, m tels que la matrice

$$A = \begin{pmatrix} p & a & 0 \\ a & m & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

est définie positive de déterminant 1. La question précédente implique donc $A = {}^tBB$ où le premier vecteur colonne de $B = (r, s, t)$. En identifiant les coefficients $(1, 1)$, on a : $p = r^2 + s^2 + t^2$.

III. Classes d'idéaux et anneaux principaux.

A. On notera π_A le polynôme minimal et χ_A le polynôme caractéristique de A.

On remarque qu'on peut écrire $\mathbb{Z}[\theta] = \mathbb{Z} \oplus \mathbb{Z}.\theta \oplus \cdots \oplus \mathbb{Z}.\theta^{n-1}$ qui est un $\mathbb{Z}$-module libre de rang n.

1. Soit I un idéal non nul de $\mathbb{Z}[\theta]$. I est un groupe abélien et un sous-module de $\mathbb{Z}[\theta]$. Soit $j \in I \setminus \{0\}$, $j.\mathbb{Z}[\theta]$ est un sous-module de I et I est un sous-module $\mathbb{Z}[\theta]$, qui est un $\mathbb{Z}$-module libre de rang n. Donc (on utilise le même résultat qu'à la question II.B.1.b : voir compléments.) I et $j.\mathbb{Z}[\theta]$ sont libres. Le rang de $j.\mathbb{Z}[\theta]$ est nécessairement inférieur à celui de I, qui est inférieur à n (le rang de $\mathbb{Z}[\theta]$).

D'autre part, on a $j.\mathbb{Z}[\theta] = \mathbb{Z}.j \oplus \mathbb{Z}.j\theta \oplus \cdots \oplus \mathbb{Z}.j\theta^n$ car j est non nul et $\mathbb{Z}[\theta]$ est intègre (P est irréductible).

Donc $j.\mathbb{Z}[\theta]$ est de rang n. A fortiori I est de rang n.

2.a. On peut interpréter la question comme : "montrer que θ est valeur propre de A", en faisant attention au sens que l'on peut donner à cette phrase (valeur propre en travaillant dans quel espace vectoriel ou quel module ?).

Comme $P(A) = 0$ (théorème de Cayley-Hamilton), π_A divise P. En effet, on effectue la division euclidienne de P par π_A et on obtient un reste R, polynôme

de degré strictement inférieur à celui de π_A. Comme $P(A) = \pi_A(A) = 0$, on a $R(A) = 0$. Par définition de π_A, R est nécessairement nul.

Comme P est irréductible, comme P et π_A sont unitaires, on a $P = \pi_A$. Donc (le degré de P est n) π_A et χ_A sont de même degré : n. On a donc : $\chi_A = (-1)^n P$.

A est une matrice à coefficients dans $\mathbb{Z}$ donc dans le corps $\mathbb{Q}$. On note $\mathbb{Q}(\theta)$ le corps des fractions de $\mathbb{Z}[\theta]$. Le polynôme caractéristique de A vue comme matrice de $M_n(\mathbb{Q})$ est le même que celui de A vue comme matrice de $M_n(\mathbb{Q}(\theta))$: c'est $\det(A - XI) \in \mathbb{Q}[X]$. Il s'agit donc de $(-1)^n P$ et celui-ci s'annule en $\theta \in \mathbb{Q}(\theta)$ par hypothèse. θ est donc valeur propre de A vue comme matrice de $M_n(\mathbb{Q}(\theta))$. Il existe donc un vecteur non nul $v = (v_1, \ldots, v_n) \in \mathbb{Q}(\theta)^n$ tel que $A^t v = \theta.{}^t v$. En multipliant v par $c \in \mathbb{Z}[\theta]$ non nul adequat, on obtient $x \in \mathbb{Z}[\theta]^n$ non nul tel que $A^t x = \theta.{}^t x$.

2.b. $I = \mathbb{Z}.x_1 + \cdots + \mathbb{Z}.x_n$ est un sous-groupe additif de $\mathbb{Z}[\theta]$. Montrons que I est un idéal de $\mathbb{Z}[\theta]$. Soient $j \in I$ et $R(\theta) \in \mathbb{Z}[\theta]$ ($R \in \mathbb{Z}[X]$), on peut écrire $j = \sum_{k=1}^{n} l_k x_k$ avec $l_k \in \mathbb{Z}$. Comme $A^t x = \theta.{}^t x$, en explicitant la k^{ieme} ligne, on obtient $\theta.x_k \in \mathbb{Z}.x_1 + \cdots + \mathbb{Z}.x_n = I$ pour tout k. Par une récurrence immédiate, on a $R(\theta).x_k \in I$ pour tout k. Enfin, $R(\theta).j = \sum_{k=1}^{n} l_k R(\theta).x_k \in I$.

Remarquons que θ est racine simple de P : sinon P et P' admettent θ comme racine. Comme P est irréductible, P et P' sont premiers entre eux et le théorème de Bezout donne $UP + VP' = 1$ ($U, V \in \mathbb{Q}[X]$). En prenant la valeur en θ, on obtient une contradiction. On conclut alors que θ est racine simple du polynôme caractéristique de A vue comme matrice de $M_n(\mathbb{Q}(\theta))$. θ est donc valeur propre simple et le sous-espace propre associé à θ est de dimension 1 : c'est $\mathbb{Q}(\theta).{}^t x$.

Supposons donc avoir un ensemble $J = \mathbb{Z}.x'_1 + \cdots + \mathbb{Z}.x'_n$ où $x' = (x'_1, \ldots, x'_n)$ répond aussi à la question 2.a. Le vecteur x' est vecteur propre de A. On en déduit l'existence de $a, b \in \mathbb{Z}[\theta]$ tels que $ax = bx'$ donc $aI = bJ$. Ainsi, I et J appartiennent à la même classe.

2.c. Soit $Q \in GL(n, \mathbb{Z})$, QAQ^{-1} est une matrice semblable à A donc admet aussi θ comme valeur propre simple. Un vecteur propre associé est $x' = Q^t x$. D'après la question précédente, l'idéal $I_{QAQ^{-1}}$ s'écrit $\mathbb{Z}.x'_1 + \cdots + \mathbb{Z}.x'_n$. Comme $x' = Q^t x$, on a $x'_k \in \mathbb{Z}.x_1 + \cdots + \mathbb{Z}.x_n$ donc $I_{QAQ^{-1}} \subset I_A$. Par symétrie des rôles joués par les deux idéaux, on a aussi $I_A \subset I_{QAQ^{-1}}$ d'où l'égalité.

3. Si $J = 0$, alors tous les y_j sont nuls donc n'importe quelle matrice B telle que $P(B) = 0$ convient (on peut considérer par exemple une matrice compagnon associée à P). On suppose désormais J non nul. D'après 1., J est libre de rang n et $(y_1, \ldots, y_n)$ est $\mathbb{Z}$-libre. Pour tout i, $\theta.y_i \in J$ donc s'écrit $\sum_{j=1}^{n} B_{i,j} y_j$. On définit la matrice $B = \{B_{i,j}\}_{i,j} \in M_n(\mathbb{Z})$ et les relations précédentes s'écrivent : $B^t y = \theta.{}^t y$.

On a alors $P(B)^t y = P(\theta)^t y = 0$. Notons $c_{i,j}$ la matrice $P(B)$, on a pour tout i : $\sum_{j=1}^{n} c_{i,j} y_j = 0$. Comme $(y_1, \ldots, y_n)$ est libre, on obtient pour tout j : $c_{i,j} = 0$. Ainsi $P(B) = 0$.

4. Comme le vecteur x défini par la question 2.a est non nul, pour tout M, I_M n'est pas nul. Il faut donc séparer le cas nul.

On note $\mathcal{K} = \{(QAQ^{-1})_{Q\in GL(n,\mathbb{Z})};\ A \in M_n(\mathbb{Z}),\ P(A) = 0\}$. Considérons l'application ϕ définie par

$$\begin{array}{ccc} \mathcal{K} & \longrightarrow & \{\text{classes d'idéaux non nulles de } \mathbb{Z}[\theta]\} \\ C = (QAQ^{-1})_{Q\in GL(n,\mathbb{Z})} & \longmapsto & I_M \quad \text{où } M \in C \end{array}$$

$\phi(C)$ a un sens d'après 2.b et 2.c et est indépendant du représentant M choisi dans $(QAQ^{-1})_{Q\in GL(n,\mathbb{Z})}$ car I_M ne dépend que de la classe de M. ϕ est surjective d'après le 3.

Montrons que ϕ est injective. Soient C et $C' \in \mathcal{K}$ telles que $\phi(C) = \phi(C')$ (que l'on notera J). Soient M un représentant de C et N un représentant de C'. L'idéal J est non nul et il existe $a, b \in \mathbb{Z}[\theta]$ non nuls tels que $aI_M = bI_N$. Il existe aussi $x, y \in \mathbb{Z}[\theta]^n$ tels que $I_M = \mathbb{Z}.x_1 + \cdots + \mathbb{Z}.x_n$ et $I_N = \mathbb{Z}.y_1 + \cdots + \mathbb{Z}.y_n$ avec $M^t x = \theta.{}^t x$ et $N^t y = \theta.{}^t y$. Comme $aI_M = bI_N$, on a : $ax_i = b\sum_{j=1}^{n} q_{i,j}y_j$ pour tout i, où $q_{i,j} \in \mathbb{Z}$. En notant $Q = (q_{i,j}) \in M_n(\mathbb{Z})$, on a $a^t x = bQ^t y$. De même, il existe $\tilde{Q} \in M_n(\mathbb{Z})$ telle que $b^t y = a\tilde{Q}^t x$. On a alors $ba.Id = ab.Q\tilde{Q}$ (où Id est la matrice identité d'ordre n). ab est non nul donc $Id = Q\tilde{Q}$ et on obtient de même $\tilde{Q}Q = Id$ donc $Q \in GL(n,\mathbb{Z})$.

Enfin, $MQ^t y = \theta Q^t y$ s'écrit aussi $(Q^{-1}MQ)^t y = N^t y$. On conclut comme à la fin de la question 3. (via $(y_1, \cdots, y_n)$ libre) que $Q^{-1}MQ = N$ donc que M et N sont dans la même classe de similitude : $C = C'$. ϕ est injective donc bijective.

5. Il faut encore faire attention au cas de la classe nulle. D'après 4., l'assertion (ii) est équivalente à l'existence d'une unique classe d'idéaux non nuls de $\mathbb{Z}[\theta]$ donc à l'assertion (i') suivante : "Pour tout idéal non nul I de $\mathbb{Z}[\theta]$, il existe a et b dans $\mathbb{Z}[\theta]$, non nuls, tels que $aI = b\mathbb{Z}[\theta]$." Il suffit en effet de remarquer que $\mathbb{Z}[\theta]$ est un idéal de $\mathbb{Z}[\theta]$.

L'implication $(i) \Rightarrow (i')$ est triviale. Quant à la réciproque, pour tout idéal non nul I de $\mathbb{Z}[\theta]$, on considère a et b dans $\mathbb{Z}[\theta]$, non nuls, tels que $aI = b\mathbb{Z}[\theta]$. Comme $1 \in \mathbb{Z}[\theta]$, b s'écrit ar avec $r \in I$ donc $aI = ar\mathbb{Z}[\theta]$ puis la non nullité de a et l'intégrité de $\mathbb{Z}[\theta]$ donnent $I = r\mathbb{Z}[\theta]$ donc I est un idéal principal et $\mathbb{Z}[\theta]$ est un anneau principal.

B. $D \geq 1$

1. $\omega_{_D}$ s'écrit $i\sqrt{D}$ donc $P(\omega_{_D}) = 0$. De plus, P est clairement irréductible. On applique A.5. avec $\theta = \omega_{_D}$ et $n = 2$: $\mathbb{Z}[\omega_{_D}]$ est principal si et seulement s'il existe une unique classe de similitude dans $M_2(\mathbb{Z})$ de matrices A avec $P(A) = 0$.

Soit donc $A \in M_2(\mathbb{Z})$ telle que $P(A) = 0$. Le polynôme caractéristique de A est P car il s'annule en $\omega_{_D}$, appartient à $\mathbb{Q}_2[X]$ et est unitaire. Comme la somme des valeurs propres de A est nulle, A est de trace nulle donc de la forme $A(\alpha, \beta, \gamma)$. Le déterminant de A vaut $-\alpha^2 - \beta\gamma$ et d'autre part , c'est D. Ainsi, $D\alpha^2 = \beta\gamma$

Pour que $\mathbb{Z}[\omega_{_D}]$ soit principal, il faut que $A(1, \beta, \gamma)$ et $A(0, r, s)$ soient semblables pour tous les β, γ, r et s dans $\mathbb{Z}$.

Par exemple, on choisit $r = 1$ et $s = -D$. La condition de similitude s'écrit : il existe $Q \in GL(2,\mathbb{Z})$ telle que $QA(0,1,-D) = A(\alpha,\beta,\gamma)Q$. On pose :

$$Q = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

En explicitant le produit matriciel, on obtient un système (Σ).

Si $D \equiv 1$ [4] *:* on choisit $\alpha = 1$. D s'écrit à la fois $1 + 4k$ et $-1 - \beta\gamma$ donc $2(2k+1) = -\beta\gamma$. On choisit alors $\beta = -2$ et $\gamma = 2k+1$.

$$(\Sigma) \quad \begin{cases} a + 2c - (4k+1)d & = & 0 \\ a + b + 2d & = & 0 \\ (2k+1)a + c + (4k+1)b & = & 0 \\ (2k+1)b - c + d & = & 0 \end{cases}$$

Il y a une solution non triviale à (Σ) : les coefficients de $Q \in GL(2,\mathbb{Z})$ ne peuvent être tous nuls. Ainsi le déterminant de (Σ) est nul or il vaut $2k(4k+1)(2k+1)$. Donc $k = 0$ et $D = 1$.

Si $D \equiv 2$ [4] *:* D s'écrit $2 + 4k$ et $-1 - \beta\gamma$. On choisit alors $\alpha = 0$, $\beta = -2$ et $\gamma = 2k+1$. Le système (Σ) se réduit aux équations : $a = -2d$ et $c = (2k+1)b$. Comme $|\det(Q)| = 1$, on a $2d^2 + (2k+1)b^2 = 1$ (le cas -1 est impossible) donc $|b| = 1$ et $k = d = 0$. Ainsi $D = 2$.

Enfin, on remarque que $\mathbb{Z}[\omega_1]$ et $\mathbb{Z}[\omega_2]$ sont euclidiens (cf I.B.2.d) donc principaux.

2.a. On justifie l'écriture de B par $tr(A) = tr(B) = 1$ (le coefficient de X est -1). On peut toujours supposer que $|a|$ est minimal.

i) Pour $P = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, $PBP^{-1} = \begin{pmatrix} -a+nc & n(2a+1) - n^2c - b \\ c & -nc + a + 1 \end{pmatrix}$

ii) Pour $P = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$, $PBP^{-1} = \begin{pmatrix} -a+nb & -b \\ -n(2a+1) + n^2b + c & -nb + a + 1 \end{pmatrix}$

iii) Pour $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $PBP^{-1} = \begin{pmatrix} a+1 & c \\ -b & -a \end{pmatrix}$

iv) Pour $P = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $PBP^{-1} = \begin{pmatrix} -a & b \\ -c & a+1 \end{pmatrix}$

En regardant le déterminant de B, on obtient l'égalité

$$(det) \qquad -a(a+1) + bc = K = \tfrac{D+1}{4}.$$

Si $a < 0$, $a \leq -1$ ie $a + 1 \leq 0$ donc avec (iii), le coefficient (1,1) est $(a+1)$ avec $-(a+1) \geq 0$. Dans ce cas, on a $|a+1| = -a+1 > -a = |a|$ ce qui contredit que $|a|$ est minimal. Ainsi, on peut supposer a positif.

Avec i, ii et la minimalité de a, $|a-nc|$ et $|a-nb| \geq a$ donc $b \leq 0$ ou $b \geq 2na$. De même, $c \leq 0$ ou $c \geq 2na$. Avec (det) et $a(a+1) \geq 0$, on a : $bc \geq 1$ donc b et c sont non nuls et de même signe. Grâce à (iv), on peut toujours supposer b et c positifs. A fortiori, $b \geq 2na$ et $c \geq 2na$. En prenant $n = 2$, on obtient b et $c \geq 2a + 1$.

Enfin, $K = -a^2 - a + bc \geq 3a^2 + 3a + 1$.

2.b. Soient $(x, y) \in \mathbb{Z}^2 \setminus \{0\}$. On remarque que

$$\beta x^2 + (\gamma - 1)y^2 + (2\alpha + 1)xy = \beta(x + \frac{(2\alpha + 1)}{2\beta}y)^2 + (\gamma - 1 - \frac{4\alpha^2 + 4\alpha + 1}{4\beta})y^2.$$

Or compte-tenu de la relation $\beta\gamma = K + \alpha^2 + \alpha$,

$$(I) \qquad \gamma - 1 - \tfrac{4\alpha^2+4\alpha+1}{4\beta} > 0 \Leftrightarrow 4\beta\gamma - 4\beta > 4\alpha^2 + 4\alpha + 1 \Leftrightarrow 4(K - \beta) > 1.$$

Montrons que $K > \beta$. Supposons $K \leq \beta\gamma$; alors comme $\alpha \leq K - 2$

$$\beta\gamma = K + \alpha^2 + \alpha \leq K^2 - 2K + 2 = (K - 1)^2 + 1 \leq (\beta - 1)(\gamma - 1) + 1.$$

On en déduit que $\beta + \gamma \leq 2$ or $\gamma \geq \beta > 1$. On obtient une contradiction et $K > \beta$ donc d'après (I), $\gamma - 1 - \frac{4\alpha^2+4\alpha+1}{4\beta} > 0$. Comme de plus $\beta > 1$, la remarque du début donne :

$$\beta x^2+(\gamma-1)y^2+(2\alpha+1)xy \geq 0 \quad \text{et est nul ssi} \quad (x+\frac{(2\alpha+1)}{2\beta}y) = 0 \quad \text{et} \quad y = 0.$$

Ainsi, l'hypothèse "x et y non nuls" donne le résultat.

Si A et M sont semblables, il existe une matrice Q telle que $QA = MQ$. Ecrivons

$$Q = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \quad \text{avec } ru - st = 1.$$

On obtient le système

$$\begin{cases} s = -\alpha r - \gamma t \\ s - rK = -\alpha s - \gamma u \\ u = r\beta + t(\alpha + 1) \\ u - tK = s\beta + u(\alpha + 1) \end{cases}$$

En multipliant la première ligne par t et la troisième par r, on obtient :

$$1 = ru - st = u = r^2\beta + \gamma t^2 + rt(2\alpha + 1) > t^2$$

car $\{r, t\} \neq \{0, 0\}$ (cf première partie de la question). Nécessairement $t = 0$ donc $1 = r^2\beta$ et $\beta = 1$ ce qui est contraire à l'énoncé.

2.c. D'après A.5, $\mathbb{Z}[\omega_D]$ est principal si et seulement si il existe une unique classe de similitude de matrices $A \in M_2(\mathbb{Z})$ telles que $P(A) = 0$. Il suffit en effet de vérifier que P est irréductible sur $\mathbb{Q}$ et pour cela, que P n'a aucune racine dans $\mathbb{Q}$. Les racines de P sont $\frac{\pm i\sqrt{-1+4K}}{2} \notin \mathbb{Q}$.

Soit $\mathbb{Z}[\omega_D]$ principal : le cas $K = 1$ a déjà été traité : $D = 3$ et $\mathbb{Z}[\omega_D]$ est euclidien (I.B.2.d). Supposons donc que $K > 1$ et qu'il existe $a \in \{0, \ldots, K-1\}$ tel que $K + a^2 + a$ ne soit pas premier donc s'écrive $\beta\gamma$ avec $1 < \beta \leq \gamma$. D'après 2.b avec $\alpha = a$, les matrices A et M ne sont pas semblables. Or on remarque que $\pi_A(X) = \pi_M(X) = P(X)$ et le théorème de Cayley-Hamilton donne $P(A) = P(M) = 0$. Donc il existe au moins deux classes de similitude de matrices $A \in M_2(\mathbb{Z})$ telles que $P(A) = 0$ et $\mathbb{Z}[\omega_D]$ n'est pas principal.

2.d. Le cas $K = 1$ est clair. Pour $K > 1$, supposons $K + a^2 + a$ premier pour tout $a \geq 0$ tel que $3(a^2 + a) + 1 \leq K$. Soit $A \in M_2(\mathbb{Z})$ telle que $P(A) = 0$. On peut écrire ($Tr(A) = 1$)

$$A = \begin{pmatrix} -\alpha & -b \\ c & \alpha + 1 \end{pmatrix}.$$

On peut toujours supposer que $|\alpha|$ est minimal (car l'ensemble des valeurs possibles $|\alpha|$ est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément) et donc que (cf III.B.2.a)

$$\alpha \geq 0 \quad c \geq 2\alpha + 1 \quad b \geq 2\alpha + 1 \quad 3(\alpha^2 + \alpha) + 1 \leq K.$$

Par hypothèse, $K + \alpha^2 + \alpha$ est premier. On a $K = \det(A) = -\alpha^2 - \alpha + bc$ donc $K + \alpha^2 + \alpha = bc$ et nécessairement $b = 1$ ou $c = 1$. Comme $c \geq 2\alpha + 1$ et $b \geq 2\alpha + 1$, on obtient $\alpha = 0$ et $\det(A) = K = bc = b$ ou c. Ainsi, on a

$$A = \begin{pmatrix} 0 & -K \\ 1 & 1 \end{pmatrix} \quad \text{ou} \quad A = \begin{pmatrix} 0 & -1 \\ K & 1 \end{pmatrix}.$$

Il suffit de vérifier que ces deux matrices sont semblables. On remarque que

$$\begin{pmatrix} 0 & -K \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ K & 1 \end{pmatrix}.$$

Il y a donc une unique classe de similitude et $\mathbb{Z}[\omega_D]$ est principal.

2.e. Le cas $K = 1$ soit $D = 3$, a déjà été traité. Suppsons donc $D \leq 200$ et $D \equiv 3$ [4], on a alors $1 < K \leq 50$. On veut que $K + a^2 + a$ soit premier pour tout $a \leq K - 1$ ou tout a tel que $3(a^2 + a) + 1 \leq K$. Ainsi, K est premier donc il reste $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$. Excepté pour $K = 2$, il faut aussi $K + 2$ premier donc il reste $2, 3, 5, 7, 11, 17, 29, 41$. On remarque que si $a \geq 2$, $3(a^2 + a) + 1 \geq 19$ donc pour $K < 19$, le test est déjà suffisant : les cas $K = 2, 3, 5, 11, 17$ conviennent.

Il reste donc à tester $K = 29$ et $K = 41$. On remarque que $3(a^2 + a) + 1 > 41$ dès que $a \geq 4$. Pour $a = 2$, $K + 6$ doit être premier et pour $a = 3$, $K + 12$ doit être premier : il reste $K = 41$.

Finalement, on obtient : $K = 1, 2, 3, 5, 11, 17, 41$ soit $D = 4K - 1$ donc $D = 3, 7, 11, 19, 43, 67, 163$.

2.f. On remarque que $D \leq 10^6$ si et seulement si $K \leq 2,5.10^5 =: N$.

- On fait varier K de 0 à N.
- On initialise une variable $T[K]$ à "true".
- On fait varier a de 0 à la partie entière de $\frac{3+\sqrt{3(4K-1)}}{6}$.
  - On effectue une procédure de test de primalité de $K + a^2 + a$.
  - $T[K]$ passe à "false" si $K + a^2 + a$ n'est pas premier et on passe à la valeur suivante de K. Sinon $T[K]$ reste "true" et on passe à la valeur suivante de a.

C.

1. Déterminons les inversibles de $S = \mathbb{Z}[\omega_D]$ avec $D \equiv 3$ [4]. Soit $r \in S$ inversible, r s'écrit $x + y\omega_D$. On rappelle que r est inversible si et seulement si

$|r|^2 = 1$ soit, ici, $x^2 + xy + \frac{D+1}{4}y^2 = 1$. Comme $\frac{D+1}{4}y^2 > 1$, on a nécessairement $y = 0$ et $x = \pm 1$. Donc l'ensemble des inversibles de S est $\{-1, 1\}$.

Soit $b \in S$, on effectue une division euclidienne (S est supposé euclidien) de b par a. On a $b = aq + r$ avec $q, r \in S$ et $N(r) < N(a)$ ou $r = 0$. D'après l'hypothèse de minimalité sur a, si r est non nul, r est inversible. Ainsi, d'après la remarque initiale $r = 0$, c'est à dire $b \in aS$, ou $r \in \{-1, 1\}$. On a donc

$$S/aS = \{\overline{-1}, \bar{0}, \bar{1}\}.$$

Selon la nature de a, on peut avoir (ou pas) $\bar{1} = \overline{-1}$. Dans tous les cas $\bar{1}$ et $\overline{-1}$ sont distincts de $\bar{0}$ car $\bar{1} = \bar{0}$ signifie $aS = 1 + aS$ ie $ax = 1 + ay \Leftrightarrow 1 = a(x - y)$ donc a serait inversible dans S ce qui est contraire à l'hypothèse.

On conclut donc que S/aS est isomorphe à $\mathbb{F}_2$ (si $\bar{1} = \overline{-1}$) ou $\mathbb{F}_3$ (sinon).

2. On suppose donc ici que $K \geq 5$. Avec $P(X) = X^2 - X + K$, on a $P(\omega_{_D}) = 0$. En passant aux classes déquivalence dans S/aS, on obtient :

$$\overline{\omega_{_D}}^2 - \overline{\omega_{_D}} + K\bar{1} = \bar{0}.$$

Or $P(\bar{0}) = P(\bar{1}) = K\bar{1} \neq \bar{0}$ et $P(\overline{-1}) = K\bar{1} + \bar{2}$. De plus S/aS est isomorphe à $\mathbb{F}_2$ ou $\mathbb{F}_3$ et ni $\bar{K}$ ni $\overline{K+2}$ ne sont nulles pour $K = 5, 11, 17, 41$. Il y a donc une contradiction.

L'anneau $\mathbb{Z}[\omega_{_D}]$ est donc principal mais non euclidien.

1.3 Commentaires

Ce problème s'intéresse à la détermination des anneaux euclidiens et principaux parmi les anneaux d'entiers des corps quadratiques imaginaires de discriminant inférieur à 200. On utilise principalement les techniques de réseaux (ce qui généralise notamment les méthodes très classiques sur l'anneau des entiers de Gauss) et les matrices hermitiennes à coefficients dans l'anneau d'entiers. On trouve donc dans ce problème quelques techniques classiques de manipulation de $\mathbb{Z}/p\mathbb{Z}$ et de résolution d'équations diophantiennes. Au passage, ceci permet d'obtenir le théorème de Lagrange sur les sommes de quatre carrés.

Nous avons utilisé plusieurs fois dans ce problème le résultat suivant : tout sous-module de $\mathbb{Z}^n$ est libre de type fini. Nous allons montrer que tout sous-module N d'un module libre M de type fini sur un anneau principal, est libre de type fini. Pour plus de clarté et pour "coller au problème", nous considérerons le cas de l'anneau $\mathbb{Z}$ mais la rédaction est la même avec n'importe quel anneau principal.

Le module M est libre de type fini : il existe une base $(e_1, \ldots, e_n)$. Soit $N_r = N \cap (\mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_r)$ et montrons par récurrence que N_r est libre de dimension inférieure à $r \leq n$.

Pour $r = 1$, $N_1 = \{0\}$ ou $N_r = \mathbb{Z}\alpha.e_1$ avec $\alpha \neq 0$. Le résultat annoncé est donc vrai.

Supposons que N_r soit libre de dimension inférieure à $r < n$ et considérons l'ensemble

$$A = \{a \in \mathbb{Z} |\ \exists \alpha_i \in \mathbb{Z},\ \sum_{i=1}^{r} \alpha_i e_i + a e_{r+1} \in N\}.$$

Comme N est un sous-module de M, on vérifie aisément que A est un idéal de $\mathbb{Z}$ qui est principal donc A est de la forme $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{Z}$.

Si $\alpha = 0$ alors $N_{r+1} = N_r$ donc le résultat annoncé est vrai au rang $r+1$.

Sinon, il existe $c \in N$ et des $\alpha_i \in \mathbb{Z}$ tels que $c = \sum_{i=1}^{r} \alpha_i e_i + \alpha e_{r+1}$. On a alors $N_{r+1} = N_r \oplus \mathbb{Z}c$ et N_{r+1} est libre de dimension inférieure à $r+1$.

Par récurrence, le résultat annoncé est vrai pour tout $r \leq n$.

Pour obtenir le résultat final, il suffit de prendre $r = n$.

Chapitre 2

Session de 1990

2.1 Sujet

2.2 Correction

I. Questions utiles pour la suite du problème

A. *Décomposition d'un élément de* $\mathcal{S}(E)$

1.a. Pour tout vecteur $u \in E$, l'endomorphisme $f_u : x \mapsto (u|x)u$ est symétrique positif car pour tout $x, y \in E, (f_u(x)|y) = (u|x)(u|y) = (x|f_u(y))$ et pour tout $x \in E, (f_u(x)|x) = (u|x)^2 \geq 0$.

1.b. Lorsque $u = 0$, l'application f_u est l'endomorphisme nul de E. Si $u \neq 0$ alors $\mathrm{rg}(f_u) = 1$ puisque $\mathrm{im} f_u \subset \mathbb{R}u$ et $f_u(u) = \|u\|^2 u \neq 0$.

1.c. Si $\|u\| = 1$ alors $f_u(u) = u$. Pour tout $y \in (\mathbb{R}u)^\perp$, on a $f_u(y) = 0$ donc f_u est le projecteur orthogonal sur $\mathbb{R}u$ parallèlement à $(\mathbb{R}u)^\perp$.

1.d. Soit $B = (b_1, ..., b_n)$ une base orthonormale de E et U la matrice de u dans cette base B. On a alors pour tout $1 \leq i \leq n$, $U_i = (u|b_i)$. Le coefficient de la matrice de f_u en $i^{ème}$ ligne et $j^{ème}$ colonne dans la base B est donné par : $(f_u(b_j)|b_i) = (u|b_j)(u|b_i)$ et coïncide avec celui de $UU^\star$. Ceci justifie que dans la suite du problème, on notera $uu^\star$ l'application f_u.

2. Si $uu^\star = vv^\star$: il est clair que $u = 0 \Leftrightarrow v = 0$. Sinon u est colinéaire à v et il existe $\lambda \in \mathbb{R}$ tel que $v = \lambda u$ et comme $uu^\star(u) = vv^\star(u)$ alors $(1-\lambda^2)(u|u)u = 0$. On a donc $\lambda = 1$ ou $\lambda = -1$. Réciproquement si $u = v$ ou $u = -v$ alors $uu^\star = vv^\star$.

3. Soit $f \in \mathcal{S}(E)$. f est donc diagonalisable dans une base orthonormale de vecteurs propres. Notons $(e_1, ..., e_n)$ cette base de vecteurs propres et $(\lambda_1, ..., \lambda_n)$ les valeurs propres associées. Pour tout $x \in E$, on a $f(x) = \sum_{i=1}^n \lambda_i (x|e_i) e_i$ ce qui veut justement dire que $f = \sum_{i=1}^n \lambda_i e_i e_i^\star$. Réciproquement, si f admet une décomposition de la forme $\sum_{i=1}^n \lambda_i e_i e_i^\star$ avec $(e_1, \ldots, e_n)$ base orthonormale de E, alors, pour tout $k \in \{1, \ldots, n\}$, $f(e_k) = \lambda_k e_k$ donc e_k est vecteur propre de f associé à la valeur propre λ_k.

f est dans $\mathcal{S}^+(E)$ si et seulement si pour tout $x \in E$, $(x|f(x)) \geq 0$. Si f est dans $\mathcal{S}^+(E)$ alors pour tout $i = 1, ..., n$, $(f(e_i)|e_i) = \lambda_i \geq 0$ et réciproquement, si toutes les valeurs propres de f sont positives alors $(x|f(x)) = \sum_{i=1}^n \lambda_i (x|e_i)^2 \geq 0$ pour tout $x \in E$.

4. Soit $f \in \mathcal{S}(E)$ tel que $\forall x \in E, (x|f(x)) = 0$ alors pour tout $x, y \in E, (x+y|f(x+y)) = 0$. En développant cette expression et en utilisant le fait que $f \in \mathcal{S}(E)$, on en déduit que $\forall x, y \in E, (f(x)|y) = 0$ c'est à dire que pour tout $x \in E$, $f(x) \in E^\perp$, donc $f = 0$.

5. Soit $f \in \mathcal{S}^+(E)$ et $x \in E$. On sait alors que pour tout $y \in E$, pour tout $\lambda \in \mathbb{R}$, $(\lambda x + y|f(\lambda x + y)) \geq 0$. Si $(x|f(x)) = 0$, on obtient que $2(f(x)|y)\lambda + (y|f(y)) \geq 0$, pour tout $\lambda \in \mathbb{R}$, $y \in E$, ce qui n'est vrai que lorsque $f(x) \in E^\perp$. Ceci implique que $f(x) = 0$.

6. Par le I.A.3 on a déjà vu que si $f \in \mathcal{S}^+(E)$ alors ses valeurs propres sont positives et $f = \sum_{i=1}^n \lambda_i e_i e_i^\star$ où les e_i sont des vecteurs propres de f. En posant $u_i = \sqrt{\lambda_i} e_i$, on a bien $f = \sum_{i=1}^n u_i u_i^\star$. Maintenant, si f admet une décomposition de la forme $f = \sum_{i=1}^n u_i u_i^\star$ alors :

- f est une somme d'endomorphismes symétriques donc $f \in \mathcal{S}(E)$.
- Pour tout $x \in E, (f(x)|x) = \sum_{i=1}^{n}(x|u_i)^2 \geq 0$ donc $\forall x \in E, (f(x)|x) \geq 0$.

B. *Caractérisation des éléments de $\mathcal{B}(E)$ et de $\mathcal{C}(E)$*

1.a. $\forall x \in E$, $\|f(x)\|^2 = (f(x)|f(x)) = (x|f^\star f(x))$, par définition de l'adjoint de f. D'après l'inégalité de Cauchy-Schwarz, on en déduit que $\|f(x)\|^2 \leq \|x\|\|f^\star f(x)\|$.

Comme $\|f^\star f(x)\| \leq \|f^\star\|\|f(x)\|$ alors pour tout $x \in E, \|f(x)\| \leq \|f^\star\|\|x\|$.

1.b. D'après l'inégalité précédente, on obtient $\|f\| \leq \|f^\star\|$, pour tout $f \in \mathcal{L}(E)$. En appliquant cette dernière inégalité à $f^\star$, comme $f^{\star\star} = f$, on a aussi $\|f^\star\| \leq \|f\|$. On a bien pour tout $f \in \mathcal{L}(E)$, $\|f\| = \|f^\star\|$.

2.a. $f^\star f$ est un endomorphisme symétrique car $(f^\star f)^\star = f^\star f^{\star\star} = f^\star f$. De plus $\forall x \in E, (f^\star f(x)|x) = (f(x)|f(x)) \geq 0$ donc $f^\star f \in \mathcal{S}^+(E)$.

2.b. L'endomorphisme $\mathrm{id} - f^\star f$ est évidemment symétrique donc il est élément de $\mathcal{S}^+(E)$ si et seulement si pour tout $x \in E, (x|x - f^\star f(x)) = \|x\|^2 - \|f(x)\|^2 \geq 0$. Cette condition caractérise le fait que $\|f\| \leq 1$ ou encore que $f \in \mathcal{B}(E)$.

3.a. En dimension finie, la sphère unité de E est compacte et comme f est continu ainsi que l'application $x \mapsto \|x\|$ alors $\sup_{\|x\|=1}\|f(x)\|$ est atteint en un point de la sphère unité. On en déduit que si $\|f\| = 1$ alors $E_f \neq \{0\}$. La réciproque est évidente pour $f \in \mathcal{B}(E)$.

3.b. D'après I.B.2.b. $f \in \mathcal{B}(E) \Leftrightarrow \mathrm{id} - f^\star f \in \mathcal{S}^+(E)$, et par le I.A.5., on sait que pour $x \in E, (\mathrm{id} - f^\star f)(x) = 0$ si et seulement si $(x|x - f^\star f(x)) = 0$. On en conclut que $\ker(\mathrm{id} - f^\star f) = E_f$.

Comme $\|f\| = \|f^\star\|$ alors $f \in \mathcal{B}(E) \Leftrightarrow f^\star \in \mathcal{B}(E)$ donc on a de la même manière $E_{f^\star} = \ker(\mathrm{id} - ff^\star)$. En particulier E_f et $E_{f^\star}$ sont des sous-espaces vectoriels de E.

3.c. Si $x \in E_{f^\star}$ alors on vient de voir que $x = f(f^\star(x))$. Comme $(\mathrm{id} - f^\star f)(f^\star(x)) = f^\star(x - ff^\star(x)) = 0$ alors $f^\star(x) \in \ker(\mathrm{id} - f^\star f)$. Ainsi $f^\star(x) \in E_f$ et comme $x = f(f^\star(x))$ alors $x \in f(E_f)$. Réciproquement, si $x \in f(E_f)$ alors $x = f(y)$ avec $y = f^\star f(y)$. On a $x - ff^\star(x) = f(y - f^\star f(y)) = 0$ donc $x \in E_{f^\star}$. Il est établi que $f(E_f) = E_{f^\star}$ et comme $f^{\star\star} = f$ alors $f^\star(E_{f^\star}) = E_f$. De la première égalité, on déduit que f transforme une base de E_f en une famille génératrice de $E_{f^\star}$ donc $\dim E_f \geq \dim E_{f^\star}$. De même de la seconde égalité on tire $\dim E_f \leq \dim E_{f^\star}$.

4. Par le I.B.1.b. on sait que pour tout $f \in \mathcal{L}(E), \|f\| = \|f^\star\|$. Par le théorème du rang, on sait que $\mathrm{rg}(\mathrm{id} - f^\star f) = n - \dim\ker(\mathrm{id} - f^\star f)$. Pour $f \in B(E)$, on sait que $\dim E_f = \dim E_{f^\star}$ donc $\mathrm{rg}(\mathrm{id} - f^\star f) = \mathrm{rg}(\mathrm{id} - ff^\star)$. On a bien $f \in \mathcal{C}(E) \Leftrightarrow f^\star \in \mathcal{C}(E)$.

Comme $(f^\star)^k = (f^k)^\star$ alors $\|f^k\| = \|(f^\star)^k\|$. Par définition et le résultat rappelé par l'énoncé, $f \in \mathcal{C}_0(E)$ si et seulement si $f \in \mathcal{C}(E)$ et $\exists k \in \mathbb{N}$ tel que $\|f^k\| < 1$. Il est alors clair que $f \in \mathcal{C}_0(E) \Leftrightarrow f^\star \in \mathcal{C}_0(E)$.

5. Soit $f \in \mathcal{L}(E)$.

Il est évident que $(ii) \Rightarrow (i)$ car on sait par le I.B.2.b que $f \in \mathcal{B}(E) \Leftrightarrow \mathrm{id} - f^\star f \in \mathcal{S}^+(E)$ et par le I.1.b. que $\mathrm{rg}(uu^\star) \leq 1$. On a facilement $(ii) \Rightarrow (iii)$. Il ne reste qu'à prouver que $(i) \Rightarrow (ii)$ et $(iii) \Rightarrow (ii)$.

$(i) \Rightarrow (ii)$: si $f \in \mathcal{C}(E)$ alors $f \in \mathcal{B}(E)$ et $\mathrm{rg}(\mathrm{id} - f^\star f) \leq 1$. On en déduit que $\mathrm{id} - f^\star f \in \mathcal{S}^+(E)$. Cet endomorphisme est donc diagonalisable dans une base orthonormale de vecteurs propres et toutes ses valeurs propres sont positives. Comme son rang est inférieur à 1, il existe $\lambda \geq 0$ et $v \in E$ tels que $\mathrm{id} - f^\star f = \lambda v v^\star$ car tous les autres vecteurs propres sont asociés à la valeur propre 0. On pose $u = \sqrt{\lambda} v$ et (ii) est vérifiée.

$(iii) \Rightarrow (ii)$: (iii) s'écrit aussi : il existe $u \in E$ tel que pour tout $x \in E, ((\mathrm{id} - f^\star f - uu^\star)(x)|x) = 0$. Comme $\mathrm{id} - f^\star f - uu^\star$ est un élément de $\mathcal{S}(E)$, alors par le I.A.4. on en conclut que (ii) est vrai.

C. *Propriétés des matrices compagnons*

Montrons par récurrence sur n que pour tout polynôme unitaire P de degré n, le polynôme caractéristique de sa matrice compagnon est P.

Si $n = 1$ et $P = X - a_0$ alors $C = [a_0]$ et $\det(X\mathrm{I} - C) = X - a_0$ ce qui démontre la propriété au rang 1.

Supposons la propriété vraie au rang $n-1$. Soit $P = X^n - a_{n-1}X^{n-1} - ... - a_1 X - a_0$ et C sa matrice compagnon. En notant $Q = X^{n-1} - a_{n-1}X^{n-2} - ... - a_1$ et D sa matrice compagnon, alors en développant $\det(X\mathrm{I} - C)$ par rapport à la première ligne, on a

$$\det(X\mathrm{I}_n - C) = X \det(X\mathrm{I}_{n-1} - D) + (-1)^{1+n}(-a_0) \det E$$

où E est une matrice triangulaire supérieure de taille $n-1$ n'ayant que des -1 sur la diagonale. On a $\det E = (-1)^{n-1}$ et d'après l'hypothèse de récurrence $\det(X\mathrm{I}_{n-1} - D) = Q$. Donc $\det(X\mathrm{I}_n - C) = XQ - a_0 = P$.

Pour tout $i \in \{0, ..., n-1\}$, on a $C^i(E_1) = E_{i+1}$ donc la famille $(C^i(E_1))_{0 \leq i \leq n-1}$ est libre dans $\mathbb{R}^n$ et nécessairement la famillle $(C^i)_{0 \leq i \leq n-1}$ est libre dans $\mathcal{M}_n(\mathbb{R})$. Le degré du polynôme minimal de C est donc plus grand que n. Par ailleurs ce polynôme est unitaire et divise P d'après le théorème de Cayley-Hamilton : c'est nécessairement P.

II. Le but de cette partie est de déterminer les matrices triangulaires inférieures qui sont dans $\mathcal{C}(\mathbb{R}^n)$ et, si A est une de ces matrices, de trouver $U \in \mathbb{R}^n$ tel que $\mathrm{I}_n - A^\star A = UU^\star$

1. $A = \begin{pmatrix} \lambda & 0 \\ \nu & \mu \end{pmatrix}$ alors $\mathrm{I}_2 - A^\star A = \begin{pmatrix} 1 - (\lambda^2 + \nu^2) & -\nu\mu \\ -\nu\mu & 1 - \mu^2 \end{pmatrix}$. On sait que $A \in \mathcal{C}(\mathbb{R}^2) \Leftrightarrow (A \in \mathcal{B}(\mathbb{R}^2)$ et $\mathrm{rg}(\mathrm{I}_2 - A^\star A) \leq 1)$.

En dimension 2, $\mathrm{rg}(\mathrm{I}_2 - A^\star A) \leq 1 \Leftrightarrow \det(\mathrm{I}_2 - A^\star A) = 0$, ce qui donne $\nu^2 = (1 - \lambda^2)(1 - \mu^2)$.

Dans ce cas, les valeurs propres de $\mathrm{I}_2 - A^\star A$ sont 0 et $\mathrm{tr}(\mathrm{I}_2 - A^\star A) = 1 - \lambda^2\mu^2$. Par le I.A.3., on sait que $A \in \mathcal{B}(\mathbb{R}^2) \Leftrightarrow \mathrm{I}_2 - A^\star A \in \mathcal{S}^+(\mathbb{R}^2)$ ce qui permet de conclure que

$$A \in \mathcal{C}(\mathbb{R}^2) \Leftrightarrow (\nu^2 = (1 - \lambda^2)(1 - \mu^2) \text{ et } \lambda^2\mu^2 \leq 1). (\star)$$

Si $A \in \mathcal{C}(\mathbb{R}^2)$, on obtient facilement $\lambda^2 \leq 1$ et $\mu^2 \leq 1$ donc on peut trouver deux réels α et β tels que $\lambda = \cos\alpha$ et $\mu = \cos\beta$. On a aussi $\nu^2 = \sin^2\alpha\sin^2\beta$ donc quitte à changer α en $-\alpha$, $\nu = -\sin\alpha\sin\beta$.

Réciproquement si $A = \begin{pmatrix} \cos\alpha & 0 \\ -\sin\alpha\sin\beta & \cos\beta \end{pmatrix}$ alors la condition $(\star)$ est satisfaite et donc $A \in \mathcal{C}(\mathbb{R}^2)$.

De plus, si l'on pose $U = \begin{pmatrix} \sin\alpha\cos\beta \\ \sin\beta \end{pmatrix}$ alors U est une solution de $\mathrm{I}_2 - A^\star A = UU^\star$.

2. On écrit $A = \begin{pmatrix} B & 0 \\ C^\star & a_{nn} \end{pmatrix}$ et $U = \begin{pmatrix} W \\ b_n \end{pmatrix}$ où $B \in \mathcal{M}_{n-1}(\mathbb{R})$, $C, W \in \mathbb{R}^{n-1}$. On a alors : $\mathrm{I}_n - A^\star A = \begin{pmatrix} \mathrm{I}_{n-1} - B^\star B - CC^\star & -a_{nn}C \\ -a_{nn}C^\star & 1 - a_{nn}^2 \end{pmatrix}$ et $UU^\star = \begin{pmatrix} WW^\star & b_nW \\ b_nW^\star & b_n^2 \end{pmatrix}$.

Si $\mathrm{I}_n - A^\star A = UU^\star$ alors on a $1 - a_{nn}^2 = b_n^2$ donc il existe $\theta_n \in \mathbb{R}$ tel que $a_{nn} = \cos(\theta_n)$ et $b_n = \sin(\theta_n)$. De plus, $b_nW = -a_{nn}C$ et on sait que $(a_{nn}, b_n) \neq (0,0)$ donc il existe $V \in \mathbb{R}^{n-1}$ tel que $W = a_{nn}V$ et $C = -b_nV$. On vérifie facilement qu'on a bien $\mathrm{I}_{n-1} - B^\star B = WW^\star + CC^\star = VV^\star$.

La réciproque est évidemment vraie.

3. Soit $(\lambda_1, \ldots, \lambda_n)$ la liste des valeurs propres imposées. Pour tout $k \in \{1, \ldots, n\}, |\lambda_k| \leq 1$ donc il existe $\theta_k \in \mathbb{R}$ tel que $\lambda_k = \cos\theta_k$. Construisons par récurrence finie sur k une famille de matrices $A_k \in \mathcal{M}_k(\mathbb{R})$ et de vecteurs colonnes $U_k \in \mathbb{R}^k$ en posant :

$\begin{cases} A_1 = (\cos(\theta_1)) \\ U_1 = (\sin(\theta_1)); \end{cases}$

et $\forall k \in \{1, \ldots, n-1\}, \begin{cases} A_{k+1} = \begin{pmatrix} A_k & 0 \\ -sin(\theta_{k+1})U_k^\star & \cos(\theta_{k+1}) \end{pmatrix} \\ U_{k+1} = \begin{pmatrix} \cos(\theta_{k+1})U_k \\ \sin(\theta_{k+1}) \end{pmatrix}. \end{cases}$

Au rang $k = 1$, on a bien sûr $\mathrm{I}_1 - A_1^\star A_1 = U_1U_1^\star$.

De plus, la question précédente prouve que pour tout $k \in \{1, \ldots, n-1\}$, $\mathrm{I}_k - A_k^\star A_k = U_kU_k^\star \Rightarrow \mathrm{I}_{k+1} - A_{k+1}^\star A_{k+1} = U_{k+1}U_{k+1}^\star$, donc par récurrence, il est clair que $\mathrm{I}_n - A_n^\star A_n = U_nU_n^\star$. D'après I.B.5., on en conclut que $A_n \in \mathcal{C}(\mathbb{R}^n)$, et il est clair par construction que cette matrice est bien triangulaire inférieure avec les valeurs propres souhaitées.

Par ailleurs, si $A \in \mathcal{C}(\mathbb{R}^n)$, d'après I.B.5., il existe $U \in \mathcal{M}_n(\mathbb{R})$ tel que $\mathrm{I}_n - A^\star A = UU^\star$. Comme le résultat de la question II.2. est une condition nécessaire et suffisante, cela prouve que si A est une matrice triangulaire inférieure de $\mathcal{C}(\mathbb{R}^n)$ alors elle est nécessairement obtenue par le procédé décrit ci-dessus. On en conclut que les éléments de $\mathcal{C}(\mathbb{R}^n)$ qui sont des matrices triangulaires inférieures sont de la forme $A = (a_{ij})_{1 \leq i,j \leq n}$ où

$$a_{ij} = \begin{cases} j > i & : & 0 \\ j = i & : & \cos(\theta_i) \\ j < i & : & -\sin(\theta_i)\sin(\theta_j)\displaystyle\prod_{l=j+1}^{i-1}\cos(\theta_l) \end{cases}, (\theta_1, \ldots, \theta_n) \in \mathbb{R}^n.$$

(Par convention, le produit sur un ensemble vide d'indices est égal à 1.)

Pour un tel élément A, un vecteur colonne satisfaisant l'équation $\mathrm{I}_n - A^\star A = UU^\star$ est donné par : $U = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$ où $u_j = \sin(\theta_j) \prod_{k=j+1}^{n} \cos(\theta_k)$.

III. Étude de $\mathcal{B}(E)$ et de $\mathcal{C}_0(E)$

A. *Décomposition d'un élément de* $\mathcal{B}(E)$

1.a. Il est clair que $F = \bigcap_{k\in\mathbb{N}} (f^k)^{-1}(E_f)$ où $(f^k)^{-1}(E_f)$ désigne, pour $k \in \mathbb{N}$, l'image réciproque de E_f par f^k. On a vu que pour $f \in \mathcal{B}(E)$, E_f est un sous-espace vectoriel de E. Donc F est un sous-espace vectoriel de E en tant qu'intersection de sous-espaces vectoriels de E.

1.b. Soit $x \in F$. Alors pour tout $k \in \mathbb{N}$, $f^k(f(x)) = f^{k+1}(x) \in E_f$ car $x \in F$. Donc $f(x) \in F$ et $f(F) \subset F$. On peut alors considérer l'endomorphisme induit par f sur F, noté φ. On voit que φ est injectif car : $F \subset E_f$ et $\forall x \in E_f$, $\|f(x)\| = \|x\|$, donc si $\varphi(x) = 0$ alors $\|x\| = \|\varphi(x)\| = 0$. Comme F est de dimension finie, φ est surjectif donc $f(F) = \varphi(F) = F$. D'autre part, si $x \in F$, alors $x \in E_f$ donc $x = f^\star(f(x))$. Comme $f(x) \in F$ alors $x \in f^\star(F)$ et $F \subset f^\star(F)$. Mais $\dim f^\star(F) \leq \dim F$ donc $F = f^\star(F)$.

1.c. D'après b. F est stable par $f^\star$. Donc $F^\perp$ est stable par $f^{\star\star}$, c'est à dire que G est stable par f.

2. La question précédente justifie que $\varphi = f_{|F}$ et $\psi = f_{|G}$ définissent bien deux endomorphismes sur F et G respectivement.

2.a. Soit $x \in G$. Alors $\|\psi(x)\| = \|f(x)\| \leq \|x\|$ car $f \in \mathcal{B}(E)$. Donc $\psi \in \mathcal{B}(G)$.

2.b. On a : $F \subset E_f$ donc pour tout $x \in F$, $\|\varphi(x)\| = \|f(x)\| = \|x\|$. Ceci caractérise les endomorphismes orthogonaux de F.

2.c. Si $k = 0$: $x \notin F$ donc $x \neq 0$ et (x) forme bien une famille libre de E.

On peut donc supposer $k \geq 1$. Par définition de k : $f^k(x) \notin E_f$ et pour tout entier $j < k$, $f^j(x) \in E_f$. Supposons qu'il existe des scalaires non tous nuls $\lambda_0, \ldots, \lambda_k$ tels que $\sum_{i=0}^{k} \lambda_i f^i(x) = 0$ et notons j le plus grand indice tel que $\lambda_j \neq 0$. En composant par f^{k-j}, on a $f^k(x) = -\sum_{i=0}^{j-1} \frac{\lambda_i}{\lambda_j} f^{i+k-j}(x)$. Comme E_f est un sous-espace vectoriel de E et pour tout $i \in \{0, \ldots, j-1\}$, $f^{i+k-j}(x) \in E_f$ alors $f^k(x) \in E_f$, ce qui est absurde. Ainsi la famille $(x, f(x), \cdots, f^k(x))$ est libre dans E.

On a donc $k + 1 \leq \dim E = n$ et $\|f^n(x)\| = \|f^{n-(k+1)}(f^{k+1}(x))\| \leq \|f^{k+1}(x)\|$ car $\|.\|$ est une norme d'algèbre sur $\mathcal{L}(E)$ et $f \in \mathcal{B}(E)$. D'autre part $f^k(x) \notin E_f$ et pour tout entier $j < k$, $f^j(x) \in E_f$, donc : $\|f^{k+1}(x)\| < \|f^k(x)\| = \|x\|$. On a bien : $\|f^n(x)\| < \|x\|$.

2.d. On rappelle que $\psi \in \mathcal{B}(G)$. Par compacité de la boule unité de G, il existe $x_0 \in G$, $\|x_0\| = 1$ et $\|\psi^n\| = \|\psi^n(x_0)\|$. Comme $x_0 \neq 0$, $x_0 \notin F$ car $G = F^\perp$. D'après la question précédente, $\|\psi^n\| = \|\psi^n(x_0)\| = \|f^n(x_0)\| < \|x_0\| = 1$. D'après le résultat rappelé par l'énoncé, $\rho(\psi) < 1$ et $\psi \in \mathcal{B}_0(G)$.

3. $(iii) \Rightarrow (ii)$: si $F = \{0\}$ alors $E = G$ et $f = f_{|G} = \psi$. On vient de voir que $\|\psi^n\| < 1$ donc on a (ii).

$(ii) \Rightarrow (i)$ est une conséquence immédiate du résultat rappelé par l'énoncé.

$(i) \Rightarrow (iii)$: supposons $F \neq \{0\}$. Pour $x \in F \setminus \{0\}$ et pour $k \in \mathbb{N}$ $\|f^k(x)\| = \|x\|$. Donc pour tout $k \in \mathbb{N}$, $\|f^k\| \geq 1$. Or, toujours grâce au résultat rappelé par l'énoncé, $\exists k \in \mathbb{N}$ tel que $\|f^k\| < 1$ car $f \in \mathcal{B}_0(E)$. Ceci est absurde.

B. *Caractérisation des éléments de $\mathcal{C}_0(E)$*

1. Comme $f \in \mathcal{C}(E)$ alors d'après le I.B.5., il existe effectivement $u \in E$ tel que $\mathrm{id} - f^\star f = uu^\star$.

1.a. On sait que $E_f = \ker(\mathrm{id} - f^\star f)$ et ici $\mathrm{id} - f^\star f = uu^\star$, donc $E_f = \{u\}^\perp$. Si $x \in F$ alors pour tout $k \in \mathbb{N}$, $f^k(x) \in E_f$ et $(f^k(x)|u) = 0$. Réciproquement si pour tout $k \in \{0, \dots, n-1\}$, $(f^k(x)|u) = 0$, alors pour tout $k \in \{0, \dots, n-1\}$ $f^k(x) \in E_f$, c'est à dire $\|f(f^k(x))\| = \|f^k(x)\|$. Donc $\|f^n(x)\| = \|x\|$ et d'après III.A.2.c., on en conclut que $x \in F$.

1.b. Pour tout $k \in \{0, \dots, n-1\}$, $(f^k(x)|u) = (x|(f^\star)^k(u))$. Ainsi, d'après a. $F = (u, f^\star(u), \dots, (f^\star)^{n-1}(u))^\perp$.

D'autre part puisque $f \in \mathcal{C}(E)$, $f \in \mathcal{C}_0(E) \Leftrightarrow f \in \mathcal{B}_0(E)$. Or d'après II.A.3., $f \in \mathcal{B}_0(E) \Leftrightarrow F = 0$. On en conclut que $f \in \mathcal{C}_0(E)$ si et seulement si $\mathrm{Vect}(u, f^\star(u), \dots, (f^\star)^{n-1}(u)) = E$. Comme cette famille est de cardinal n, on a le résultat.

2. Si $n = 1$ n'importe quel vecteur non nul fait l'affaire.

Si $n \geq 2$ on peut choisir $x \in (u, f^\star(u), \dots, (f^\star)^{n-2}(u))^\perp \setminus \{0\}$. Les calculs effectués au 1.a. montrent que $\|x\| = \|f(x)\| = \cdots = \|f^{n-1}(x)\|$. Ceci assure que pour tout $k \in \{0, \dots, n-1\}$, $\|f^k\| \geq 1$. Comme $f \in \mathcal{C}_0(E)$ alors, d'après III.A.3., pour tout $k \in \{0, \dots, n-1\}$, $\|f^k\| = 1$ et $\|f^n\| < 1$.

3. Si $n = 1$, il n'y a rien à démontrer.

Supposons $n \geq 2$. Comme $\|f\| = 1$, on a $\|x\| = \|f^{n-1}(x)\| \leq \|f^{n-2}(x)\| \leq \cdots \leq \|f(x)\| \leq \|x\|$. Les inégalités ci-dessus sont donc des égalités et pour tout $k \in \{0, \dots, n-2\}$, $f^k(x) \in E_f$. Comme $\|f^n\| < 1$, $f^{n-1}(x) \notin E_f$ et $n-1$ est le plus petit entier k tel que $f^k(x) \notin E_f$. Par III.A.2.c., $(x, f(x), \dots, f^{n-1}(x))$ est une famille libre de E, de cardinal n : c'est une base de E.

Il reste à voir que $f \in \mathcal{C}_0(E)$. Comme $f \in \mathcal{B}(E)$ et $\|f^n\| < 1$, il suffit de montrer que $\mathrm{rg}(\mathrm{id} - f^\star f) \leq 1$. Or pour tout $i \in \{0, \dots, n-2\}$, $f^i(x) \in E_f$ donc $(\mathrm{id} - f^\star f)(f^i(x)) = 0$. Comme $(f^i(x))_{0 \leq i \leq n-1}$ est une base de E, on a le résultat.

C. *Etude d'une base adaptée à un élément de $\mathcal{C}_0(E)$ et de sa matrice de Gram*

1. D'après III.B.2, il existe $x \in E \setminus \{0\}$ tel que $\|x\| = \|f^{n-1}(x)\|$, et $\|f^n\| < 1$. Cette dernière inégalité assure que $\|f^n(x)\| < \|x\|$. On peut poser $\nu_1 = \frac{1}{\sqrt{\|x\|^2 - \|f^n(x)\|^2}} x$ et on a bien $\|f^{n-1}(\nu_1)\| = \|\nu_1\|$ et $\|\nu_1\|^2 - \|f^n(\nu_1)\|^2 = 1$.

Puisque $f \in \mathcal{C}_0(E)$, III.B.2. prouve que f et ν_1 satisfont aux hypothèses de la question III.B.3. dont on applique le résultat : $(\nu_1, \dots, \nu_n)$ est une base de E. La matrice de f dans cette base est alors la matrice compagnon d'un polynôme Q. D'après I.C. son polynôme caractéristique est Q donc cette matrice est égale à C.

2.a. La formule du produit matriciel de 3 matrices donne pour tout $(i,j) \in \{1,\dots,n\}^2$,

$$(C^\star \Omega C)_{i,j} = \sum_{k=1}^{n}\sum_{l=1}^{n} C^\star_{i,k}\Omega_{k,l}C_{l,j} = \sum_{k=1}^{n}\sum_{l=1}^{n} \Omega_{k,l}C_{k,i}C_{l,j}.$$

Comme $\Omega_{k,l} = (\nu_k|\nu_l)$ alors par bilinéarité du produit scalaire, on a

$$(C^\star \Omega C)_{i,j} = \big(\sum_{k=1}^{n} C_{k,i}\nu_k | \sum_{l=1}^{n} C_{l,j}\nu_l\big).$$

On vient de voir que la matrice de f dans la base $(\nu_1,\dots,\nu_n)$ est C donc $(C^\star\Omega C)_{i,j} = (f(\nu_i)|f(\nu_j))$.

2.b.

$$\begin{array}{rcl}(\Omega - C^\star\Omega C)_{i,j} & = & (\nu_i|\nu_j) - (f(\nu_i)|f(\nu_j)) \text{ d'après le a.} \\ & = & (\nu_i|\nu_j - f^\star f(\nu_j)).\end{array}$$

Si $j \neq n$, $\nu_j \in E_f = \ker(\mathrm{id} - f^\star f)$ donc $(\Omega - C^\star\Omega C)_{i,j} = 0$.
Si $i = j = n$, $(\Omega - C^\star\Omega C)_{n,n} = \|\nu_n\|^2 - \|f(\nu_n)\|^2 = \|f^{n-1}(\nu_1)\|^2 - \|f^n(\nu_1)\|^2 = 1$ par construction de ν_1.

Comme $\Omega - C^\star\Omega C$ est symétrique alors tous ses coefficients sont nuls sauf celui en position (n,n) : $\Omega - C^\star\Omega C = E_n E_n^\star$.

IV. Résolution dans $\mathcal{M}_n(\mathbb{R})$ de l'équation à l'inconnue G : $G - C^\star G C = H$

1. D'après I.C., P est le polynôme caractéristique de C. L'hypothèse faite sur les racines de P assure que $\rho(C) < 1$ donc que $\lim_{k\to\infty} C^k = 0$. Comme $\|(C^\star)^k\| = \|C^k\|$, on a aussi $\lim_{k\to\infty}(C^\star)^k = 0$. Par continuité du produit matriciel, $(C^\star)^k A C^k$ tend vers 0 quand k tend vers l'infini. Or une récurrence évidente montre que pour tout $k \in \mathbb{N}$, $A = (C^\star)^k A C^k$ donc $A = 0$.

2.a. On considère $\Theta : \mathcal{M}_n(\mathbb{R}) \to \mathcal{M}_n(\mathbb{R})$ défini par $\Theta(M) = M - C^\star M C$. Θ est alors un endomorphisme de $\mathcal{M}_n(\mathbb{R})$ et le 1. prouve qu'il est injectif. C'est donc un isomorphisme : pour tout $B \in \mathcal{M}_n(\mathbb{R})$, il existe une unique matrice $A \in \mathcal{M}_n(\mathbb{R})$ telle que $B = \Theta(A)$.

2.b. En multipliant la relation $A - C^\star A C = B$ à gauche par $(C^\star)^p$ et à droite par C^p, on obtient que pour tout $p \in \mathbb{N}$, $(C^\star)^p A C^p = (C^\star)^{p+1} A C^{p+1} + (C^\star)^p B C^p$. On additionne les $k+1$ premières égalités ainsi obtenues et on en déduit que pour tout $k \in \mathbb{N}$, $A = (C^\star)^{k+1} A C^{k+1} + \sum_{p=0}^{k} (C^\star)^p B C^p$. On a déjà vu que $\lim_{k\to\infty}(C^\star)^{k+1} A C^{k+1} = 0$ ce qui prouve que la série $\big(\sum_p (C^\star)^p B C^p\big)$ est convergente dans $\mathcal{M}_n(\mathbb{R})$ et que sa somme vaut A.

3.a. On vient de voir que $G = \sum_{p=0}^{+\infty} (C^\star)^p H C^p$. On sait que $H \in \mathcal{S}^+(\mathbb{R}^n)$ donc pour tout $p \in \mathbb{N}$, $(C^\star)^p H C^p \in \mathcal{S}^+(\mathbb{R}^n)$. Comme $\mathcal{S}^+(\mathbb{R}^n)$ est un cône convexe fermé de $\mathcal{M}_n(\mathbb{R})$ alors G est aussi dans $\mathcal{S}^+(\mathbb{R}^n)$.

3.b. $(i) \Leftrightarrow (ii)$: D'après le I.A.5., si $\Phi \in \mathcal{S}^+(\mathbb{R}^n)$, $X \in \ker \Phi \Leftrightarrow (\Phi X|X) = 0$. Or $G \in \mathcal{S}^+(\mathbb{R}^n)$ donc $X \in \ker G \Leftrightarrow (GX|X) = 0$. Par continuité du produit scalaire, $(GX|X) = \sum_{p=0}^{+\infty}(HC^pX|C^pX)$ et comme $H \in \mathcal{S}^+(\mathbb{R}^n)$, $X \in \ker G \Leftrightarrow (\forall p \in \mathbb{N},\ C^pX \in \ker H)$.

$(ii) \Rightarrow (iii)$: évident.

$(iii) \Rightarrow (ii)$: par le théorème de Cayley-Hamilton, on sait que le polynôme caractéristique de C (c'est à dire P d'après le I.C.) annule C. Pour tout $k \geq n$, effectuons la division euclidienne de T^k par P : on trouve deux polynômes Q_k et R_k tels que $T^k = Q_kP + R_k$ avec $\deg(R_k) \leq n-1$. Comme $P(C) = 0$ alors $C^k = R_k(C)$. De plus, si pour tout $p \in \{0, \dots, n-1\}, HC^pX = 0$, alors pour tout polynôme R de degré inférieur ou égal à $n-1$, $HR(C)X = 0$. On en conclut que pour tout $k \geq n$, $HC^kX = HR_k(C)X = 0$. On a donc bien prouvé que $(iii) \Rightarrow (ii)$.

4. Notons d'abord que $UU^\star \in \mathcal{S}^+(\mathbb{R}^n)$, donc nous pouvons appliquer les résultats obtenus à la question précédente avec $H = UU^\star$. En particulier, on sait alors que $G \in \mathcal{S}^+(\mathbb{R}^n)$ donc G est définie positive si et seulement si $\ker G = \{0\}$. Par (iii), on a aussi $\ker G = \left\{X : \forall i \in \{0, \dots, n-1\}, C^iX \in \ker UU^\star\right\}$.

Ceci étant dit, remarquons que $X \in \ker UU^\star \Leftrightarrow (U|X) = 0$. On en conclut que G est définie positive si et seulement si $\left\{X : \forall i \in \{0, \dots, n-1\}, (C^iX|U) = 0\right\} = \{0\}$, ce qui est exactement la propriété (i).

Montrons que $(i) \Leftrightarrow (ii)$: on a évidemment

$$\begin{array}{rcl}(i) & \Leftrightarrow & \left\{X : \forall i \in \{0, \dots, n-1\}, (X|(C^i)^\star U) = 0\right\} = \{0\} \\ & \Leftrightarrow & (U, C^\star U, \dots, (C^\star)^{n-1}U)^\perp = \{0\} \\ & \Leftrightarrow & \mathrm{Vect}(U, C^\star U, \dots, (C^\star)^{n-1}U) = E.\end{array}$$

Comme les familles génératrices de cardinal n sont les bases de $\mathbb{R}^n$, on en conclut que $(i) \Leftrightarrow (ii)$.

5.a. On peut appliquer le résultat de la question précédente avec $G = \Omega$ et $U = E_n$. En particulier, montrer que $(E_n, C^\star E_n, \dots, (C^\star)^{n-1}E_n)$ est une base de $\mathbb{R}^n$ prouvera que Ω est définie positive :

lorsque $l + k \leq n, C^kE_l = E_{l+k}$ et $((C^\star)^kE_n|E_l) = (E_n|C^kE_l)$. on en déduit que si $l + k < n$ alors $((C^\star)^kE_n|E_l) = 0$ et si $l + k = n$ alors $((C^\star)^kE_n|E_l) = 1$. La matrice des vecteurs colonnes $\left((C^\star)^kE_n\right)_{0\leq k\leq n-1}$ exprimée dans la base $(E_n, \dots, E_1)$ est alors triangulaire supérieure et n'admet que des 1 sur la diagonale. La famille $(E_n, C^\star E_n, \dots, (C^\star)^{n-1}E_n)$ forme donc une base de $\mathbb{R}^n$.

5.b. Comme la famille $(E_n, C^\star E_n, \dots, (C^\star)^{n-1}E_n)$ est génératrice dans $\mathbb{R}^n$, pour tout $U \in \mathbb{R}^n$, il existe une famille de scalaires $(\lambda_0, \dots, \lambda_{n-1})$ telle que $U = \sum_{i=0}^{n-1} \lambda_i(C^\star)^iE_n$. Soit $Q(T) = \sum_{i=0}^{n-1} \lambda_iT^i$ alors $U = (Q(C))^\star E_n$ et $\deg Q \leq n-1$. De plus s'il existe deux polynômes Q_1 et Q_2 de degrés inférieurs ou égaux à $n-1$ vérifiant $(Q_1(C))^\star E_n = (Q_2(C))^\star E_n$ alors par liberté de la famille $(E_n, C^\star E_n, \dots, (C^\star)^{n-1}E_n)$, leurs coefficients sont égaux, ce qui prouve l'unicité d'un tel polynôme.

Par propriété de commutativité de l'algèbre des polynômes d'une matrice, on constate que $Q(C)^\star\Omega Q(C) - C^\star Q(C)^\star\Omega Q(C)C = Q(C)^\star(\Omega - C^\star\Omega C)Q(C) = UU^\star$ car $\Omega - C^\star\Omega C = E_nE_n^\star$. Or par le 2.a., G est l'unique solution de l'équation $G - C^\star GC = UU^\star$ donc $G = Q(C)^\star\Omega Q(C)$.

5.c. Par le I.A.6., on sait que $G - C^\star GC \in \mathcal{S}^+(\mathbb{R}^n)$ si et seulement si il existe $U_1, \dots, U_n \in \mathbb{R}^n$ tels que $G - C^\star GC = \sum_{i=1}^n U_iU_i^\star$.

D'après la question précédente, pour tout $i \in \{1, \ldots, n\}$, il existe $Q_i \in \mathbb{R}[T]$ tel que $G_i = (Q_i(C))^\star \Omega Q_i(C)$ soit la solution de l'équation $G_i - C^\star G_i C = U_i U_i^\star$. On en conclut que $G = \sum_{i=1}^n G_i$ est la solution de $G - C^\star G C = \sum_{i=1}^n U_i U_i^\star$ ce qui prouve que si $G - C^\star G C \in \mathcal{S}^+(\mathbb{R}^n)$ alors il existe n polynômes $Q_1, \ldots, Q_n \in \mathbb{R}[T]$ tels que $G = \sum_{i=1}^n (Q_i(C))^\star \Omega Q_i(C)$.

Réciproquement, s'il existe n polynômes $Q_1, \ldots, Q_n \in \mathbb{R}[T]$ tels que $G = \sum_{i=1}^n (Q_i(C))^\star \Omega Q_i(C)$ alors, en effectuant le même calcul qu'à la question précédente, il est facile de constater que $G - C^\star G C = \sum_{i=1}^n U_i U_i^\star$, où $U_i = (Q_i(C))^\star E_n$. A nouveau par le I.A.6, on en conclut que $G - C^\star G C \in \mathcal{S}^+(\mathbb{R}^n)$.

V.

A. *Existence d'éléments f de $\mathcal{C}_0(E)$ tels que $\chi_f = P$*

1. Il suffit, si $P = \prod_{i=1}^n (X - \lambda_i)$ (les λ_i sont éventuellement confondus), de reprendre l'algorithme de II.3. pour construire une matrice M triangulaire inférieure dont les valeurs propres sont les λ_i, et qui appartient à $\mathcal{C}(\mathbb{R}^n)$. Comme les racines de P sont de modules strictement inférieurs à 1, $\rho(M) < 1$ donc $M \in \mathcal{C}_0(\mathbb{R}^n)$.

On considère alors une base orthonormée B de E et on prend $f \in \mathcal{L}(E)$ qui admet M pour matrice dans B. Par définition, on a $\rho(f) = \rho(M)$ et $\|f\| = \|M\|$. D'autre part, la matrice de $f^\star$ dans B est $M^\star$ car B est orthonormée, donc $\mathrm{rg}(\mathrm{id} - f^\star f) = \mathrm{rg}(\mathrm{I} - M^\star M)$. Comme $M \in \mathcal{C}_0(\mathbb{R}^n)$ alors $f \in \mathcal{C}_0(E)$ et il est clair que $\chi_f = P$.

2.a. D'après IV.5.a., Ω est définie positive.

Soit $B = (b_1, \ldots, b_n)$ une base orthonormée de E et ω l'endomorphisme de E représenté par Ω dans cette base. ω est symétrique défini positif, donc on peut trouver une base orthonormée B' telle que $\mathrm{Mat}(\omega, B') = \mathrm{diag}(\mu_1, \ldots, \mu_n)$ avec pour tout $i \in \{1, \ldots, n\}, \mu_i > 0$. On définit alors $v \in \mathcal{L}(E)$ par $\mathrm{Mat}(v, B') = \mathrm{diag}(\sqrt{\mu_1}, \ldots, \sqrt{\mu_n})$, et on constate que v est un automorphisme symétrique de E tel que $\omega = v^2$.

Soit $\nu_i = v(b_i)$ pour $i \in \{1, \ldots, n\}$., alors $(\nu_1, \ldots, \nu_n)$ est une base de E car v est un automorphisme et pour tout $(i, j) \in \{1, \ldots, n\}^2$, $(\nu_i | \nu_j) = (v(b_i) | v(b_j)) = (b_i | \omega(b_j)) = \Omega_{ij}$. On a donc bien $G(\nu_1, \ldots, \nu_n) = \Omega$.

2.b. Considérons l'endomorphisme f de E dont la matrice dans la base $(\nu_1, \ldots, \nu_n)$ est C. Le I.C. nous assure immédiatement que $\chi_f = P$. En reprenant le calcul fait au III.C.2.a. on trouve que $C^\star \Omega C = G(f(\nu_1), \ldots, f(\nu_n))$. Comme $\Omega - C^\star \Omega C = E_n E_n^\star$, on a $((\mathrm{id} - f^\star f)(\nu_i) | \nu_j) = 0$ si $(i, j) \neq (n, n)$ et $((\mathrm{id} - f^\star f)(\nu_n) | \nu_n) = 1$.

$(\nu_1, \ldots, \nu_n)$ est une base de E donc pour tout $x \in E$, il existe $(\lambda_1, \ldots, \lambda_n) \in \mathbb{R}^n$ tel que $x = \sum_{i=1}^n \lambda_i \nu_i$. On a alors

$$((\mathrm{id} - f^\star f)(x) | x) = \sum_{i,j} \lambda_i \lambda_j ((\mathrm{id} - f^\star f)(\nu_i) | \nu_j) = \lambda_n^2.$$

Soit u tel que $u \in (\nu_1, \ldots, \nu_{n-1})^\perp$ et $(u | \nu_n) = 1$. Alors $((\mathrm{id} - f^\star f)(x) | x) = \lambda_n^2 = (u | x)^2$, pour tout $x \in E$. Par le I.B.5, on sait alors que $f \in \mathcal{C}(E)$. Comme $\chi_f = P$, $\rho(f) < 1$ et $f \in \mathcal{C}_0(E)$.

3. Il est évident que $(i) \Rightarrow (ii) \Rightarrow (iii)$.

Supposons (iii) et appelons D la matrice compagnon de $\chi_f = \chi_g$. D'après III.C., on peut trouver deux bases $B = (\nu_1, \ldots, \nu_n)$ et $B' = (\nu'_1, \ldots, \nu'_n)$ de E, telles que $\mathrm{Mat}(f; B) = D = \mathrm{Mat}(g; B')$. Si $\Omega = G(\nu_1, \ldots, \nu_n)$ et $\Omega' = G(\nu'_1, \ldots, \nu'_n)$ alors $\Omega - D^\star \Omega D = E_n E_n^\star$ et $\Omega' - D^\star \Omega' D = E_n E_n^\star$. D'après IV.2.a, on en déduit que $\Omega = \Omega'$. Soit r l'endomorphisme de E défini par $r(\nu_i) = \nu'_i$ pour tout $i \in \{1, \ldots, n\}$. De $\Omega = \Omega'$, on déduit que pour tout $(i, j) \in \{1, \ldots, n\}^2$, $(r(\nu_i)|r(\nu_j)) = (\nu_i|\nu_j)$ ce qui permet de conclure que $r \in O(E)$. Comme $\mathrm{Mat}(f; B) = \mathrm{Mat}(g, B')$ alors $rfr^{-1} = g$ et on a montré (i).

B. *Maximum de* $\|Q(g)\|$ *lorsque* $\|g\| \leq 1$ *et* $P(g) = 0$

1.a. Comme $P(g) = 0$ alors $\sum_{k=1}^n C_{k,n} g^{k-1}(u) = g^n(u)$. C est la matrice compagnon du polynôme P, donc en reprenant le calcul matriciel effectué au III.2.a. et en utilisant la forme de la matrice C, on trouve que $C^\star G C = G(g(u), \ldots, g^n(u))$. On prouve alors facilement par récurrence que pour tout $k \in \mathbb{N}$, $(C^\star)^k G C^k = G(g^k(u), \ldots, g^{n+k-1}(u))$, d'où l'on déduit que pour tout polynôme $Q \in \mathbb{R}[T]$,

$$Q(C)^\star G Q(C) = G(Q(g)(u), \ldots, Q(g)(g^{n-1}(u))).$$

On a alors pour tout $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$,

$$\begin{aligned} (Q(C)^\star G Q(C) X | X) &= \sum_{i,j=1}^n \big(Q(g)(g^{i-1}(u)) | Q(g)(g^{j-1}(u))\big) x_i x_j \\ &= \sum_{i,j=1}^n \big(x_i Q(g)(g^{i-1}(u)) | x_j Q(g)(g^{j-1}(u))\big). \end{aligned}$$

En notant $x = \sum_{i=1}^n x_i g^{i-1}(u)$, par bilinéarité du produit scalaire, on a bien la relation cherchée : $\|Q(g)(x)\|^2 = (Q(C)X)^\star G (Q(C)X)$.

1.b. Soit $X \in \mathbb{R}^n$.

$$\begin{aligned} X^\star (G - C^\star G C) X &= X^\star G X - X^\star C^\star G C X \\ &= X^\star G X - (CX)^\star G C X \\ &= \|x\|^2 - \|g(x)\|^2 \text{ d'après a. avec } Q(T) = T \\ &\geq 0 \text{ car } g \in \mathcal{B}(E). \end{aligned}$$

Donc $G - C^\star G C \in \mathcal{S}^+(\mathbb{R}^n)$.

1.c. D'après b. et IV.5.c, il existe n polynômes $Q_1, \ldots, Q_n$ tels que

$$G = \sum_{i=1}^n Q_i(C)^\star \Omega Q_i(C).$$

Reprenons la formule établie au a. : $\|Q(g)(x)\|^2 = (Q(C)X)^\star G (Q(C)X)$. Elle devient maintenant :

$$\|Q(g)(x)\|^2 = (Q(C)X)^\star \Big(\sum_{i=1}^n Q_i(C)^\star \Omega Q_i(C)\Big)(Q(C)X)$$

$$= \sum_{i=1}^{n} \big(Q(C)Q_i(C)X\big)^\star \Omega \big(Q(C)Q_i(C)X\big).$$

On a utilisé au passage le fait que $Q_i(C)$ et $Q(C)$ commutaient.

Comme $f \in \mathcal{C}_0(E)$, P est son polynôme caractéristique, C est la matrice compagnon associée à P alors les résultats du III.C. peuvent s'appliquer. On trouve alors une base $V = (v_1, \ldots, v_n)$ telle que $\mathrm{Mat}(f, V) = C$ et $G(v_1, \ldots, v_n)$ satisfait l'équation $G(v_1, \ldots, v_n) - C^\star G(v_1, \ldots, v_n) C = E_n E_n^\star$. Maintenant, rappelons que Ω a été choisie telle que $\Omega - C^\star \Omega C = E_n E_n^\star$ (au IV.5.) et par le IV.2.a., on en conclut que $G(v_1, \ldots, v_n) = \Omega$.

On vient juste de voir que la matrice du produit scalaire dans la base $(v_1, \ldots, v_n)$ est égale à Ω. Soit u_i le vecteur de E ayant pour matrice colonne $Q_i(C)X$ dans cette base, alors $Q(f)(u_i)$ a pour matrice colonne $Q(C)Q_i(C)X$ et $\|Q(f)(u_i)\|^2 = \big(Q(C)Q_i(C)X\big)^\star \Omega \big(Q(C)Q_i(C)X\big)$. A condition d'avoir choisi au départ $X = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, c'est à dire $x = u$, on a trouvé des vecteurs $(u_1, \ldots, u_n)$ tels que pour tout polynôme $Q \in \mathbb{R}[T]$,

$$\sum_{i=1}^{n} \|Q(f)(u_i)\|^2 = \|Q(g)(x)\|^2.$$

2. Soit $u \in E$. D'après 1.c., il existe $(u_1, \ldots, u_n) \in \mathbb{R}^n$ tel que pour tout polynôme réel R, on a : $\|R(g)(u)\|^2 = \sum_{i=1}^n \|R(f)(u_i)\|^2$.

Appliquons ce résultat à $R = 1$: $\|u\|^2 = \sum_{i=1}^n \|u_i\|^2$.

Appliquons aussi ce résultat à $R = Q$:

$$\begin{aligned} \|Q(g)(u)\|^2 = \sum_{i=1}^{n} \|Q(f)(u_i)\|^2 &\leq \sum_{i=1}^{n} \|Q(f)\|^2 \|(u_i)\|^2 \\ &= \sum_{i=1}^{n} \|Q(f)\|^2 \|(u_i)\|^2 = \|Q(f)\|^2 \sum_{i=1}^{n} \|u_i\|^2 \\ &= \|Q(f)\|^2 \|u\|^2 \end{aligned}$$

On en conclut que pour tout $u \in E$, $\|Q(g)(u)\| \leq \|Q(f)\| \, \|u\|$, ce qui assure que $\|Q(g)\| \leq \|Q(f)\|$.

2.3 Commentaires

Il s'agit d'un sujet d'algèbre linéaire et bilinéaire qui met en œuvre l'essentiel des notions et théorèmes relatif à la réduction des endomorphismes et à la manipulation des normes en dimension finie. Il est abordable dès le début de la préparation à l'agrégation.

Nous nous proposons de démontrer les deux équivalences admises par l'énoncé : pour tout endomorphisme $f \in \mathcal{L}(E)$,

$$\rho(f) < 1 \Longleftrightarrow \lim_{p \to +\infty} f^p = 0 \Longleftrightarrow \exists k \in \mathbb{N} \ : \ \|f^k\| < 1.$$

a. Commençons par établir la seconde équivalence :
Si $\lim_{p\to+\infty} f^p = 0$, il est clair que, pour k assez grand : $\|f^k\| < 1$.

Réciproquement, soit $k \in \mathbb{N}$ tel que : $\|f^k\| < 1$. Pour tout $n \in \mathbb{N}$, la division euclidienne de n par k s'écrit $n = q_n k + r_n$ où $0 \leq r_n < k$.

On a alors : $\|f^n\| = \|(f^k)^{q_n} f^{r_n}\| \leq \|f^k\|^{q_n}\|f^{r_n}\| \leq m_k\|f^k\|^{q_n}$ en posant $m_k = \sup_{0\leq j\leq k-1} \|f^j\|$ qui est indépendant de n. On remarque que $\lim_{n\to\infty} q_n = +\infty$ donc, comme $\|f^k\| < 1$, on a : $\lim_{n\to\infty} \|f^k\|^{q_n} = 0$. Ainsi, $\lim_{n\to\infty} \|f^n\| = 0$.

b. Nous nous intéressons maintenant à la première équivalence : commençons par remarquer que le passage en complexe est inévitable dans la mesure où la définition même de $\rho(f)$ est en terme de racines complexes de χ_f. Pour éviter de complexifier l'espace réel E (le lecteur pourra consulter à ce sujet le *tome 2 du cours de Mathématiques spéciales écrit par Ramis-Deschamps-Odoux édité chez Masson*), nous allons transférer le problème de la convergence dans $\mathcal{L}(E)$ vers un problème de convergence dans $\mathcal{M}_n(\mathbb{C})$. Plus précisément : $\mathcal{L}(E)$ est un espace vectoriel réel de dimension finie donc toutes les normes sur $\mathcal{L}(E)$ définissent la même topologie.

Soit $\|\cdot\|$ une norme d'algèbre sur $\mathcal{M}_n(\mathbb{C})$ et $(e_1, \ldots, e_n)$ une base de E. Pour tout $g \in \mathcal{L}(E)$, en notant $M_g = Mat(g; e_1, \ldots, e_n) \in \mathcal{M}_n(\mathbb{C})$, on définit l'application N de $\mathcal{L}(E)$ dans $\mathbb{R}^+$ par $N(g) = \|M_g\|$. On vérifie alors que N est une norme sur le $\mathbb{R}$-espace vectoriel $\mathcal{L}(E)$.

On pose $M = M_f$ et on a, pour tout $k \in \mathbb{N}$: $M^k = Mat(f^k; e_1, \ldots, e_n)$, c'est à dire $N(f^k) = \|M^k\|$. Ainsi, la convergence de f^k vers 0 dans $(\mathcal{L}(E), N)$ est équivalente à celle de M^k dans $(\mathcal{M}_n(\mathbb{C}), \|.\|)$.

Supposons $\rho(f) < 1$:

Le polynôme caractéristique χ_f est scindé sur $\mathbb{C}$. Soient $\lambda_1, \ldots, \lambda_s$ les racines distinctes de χ_f dans $\mathbb{C}$, on a : $\chi_f(T) = \prod_{j=1}^s (\lambda_j - T)^{\alpha_j}$ (avec $\alpha_j \geq 1$).
En notant m l'endomorphisme de $\mathbb{C}^n$ représenté par M dans la base canonique, le théorème de décomposition des noyaux et le théorème de Cayley-Hamilton (comme $\chi_f = \chi_m$ alors $\chi_f(m) = 0$) donne :

$$\mathbb{C}^n = \ker(m - \lambda_1 \mathrm{I})^{\alpha_1} \oplus \ldots \oplus \ker(m - \lambda_s \mathrm{I})^{\alpha_s}.$$

Ainsi, M est semblable à une matrice bloc-diagonale $\tilde{M}$, où chaque bloc est de la forme $\lambda_j \mathrm{I} + B_j$, avec B_j nilpotente d'ordre α_j (il suffit de considérer une base de chaque sous-espace caractéristique $\ker(m - \lambda_j \mathrm{I})^{\alpha_j}$). Soit P la matrice de passage correspondante, on a : $M^k = P\tilde{M}^k P^{-1}$ et $\|M^k\| \leq \|P\|\|P^{-1}\|\|\tilde{M}^k\|$. On remarque que $\tilde{M}^k$ est toujours bloc-diagonale. On peut en fait écrire $\tilde{M} = D + \sum_{j=1}^s A_j$, avec D diagonale (de termes $\lambda_1, \ldots, \lambda_s$) et A_j nilpotente d'ordre α_j. Ainsi, en tenant compte de la forme par bloc de D et des A_j, on a la relation :

$$\tilde{M}^k = \sum_{j=1}^{s} \sum_{l=0}^{k} C_k^l \lambda_j^{k-l} A_j^l = \sum_{j=1}^{s} \sum_{l=0}^{\alpha_j - 1} C_k^l \lambda_j^{k-l} A_j^l.$$

Donc $\|\tilde{M}^k\| \leq \sigma \sum_{j=1}^{s} \sum_{l=0}^{\alpha_j - 1} C_k^l |\lambda_j|^{k-l}$ avec $\sigma = \sup_{1\leq j\leq s} \sup_{0\leq l\leq \alpha_j - 1} \|A_j^l\|$ qui est fini.

On obtient $\|\tilde{M}^k\| \leq \sigma \sum_{j=1}^{s} \sum_{l=0}^{\alpha_j - 1} C_k^l \rho(f)^{k-l}$. Comme $\rho(f) < 1$, le terme de droite

converge vers 0 quand k tend vers l'infini donc, M^k converge vers 0 dans $(\mathcal{M}_n(\mathbb{C}), \|.\|)$. On en conclut que f^k converge vers 0 dans $(\mathcal{L}(E), N)$.

Réciproquement : supposons que f^k converge vers 0 dans $\mathcal{L}(E)$. L'endomorphisme f^k est représenté par M^k dans la base $(e_1, \ldots, e_n)$. Soit λ une racine de χ_f et X un vecteur propre de M associé, appartenant à $\mathbb{C}^n$: $M^k X = \lambda^k X$. En choisissant la norme d'opérateur sur $\mathbb{C}^n$ comme norme $\|\cdot\|$ sur $\mathcal{M}_n(\mathbb{C})$, on obtient :

$$\|M^k\| = \sup_{X \neq 0} \frac{\|M^k X\|}{\|X\|} \geq |\lambda^k|.$$

Soit N la norme sur $\mathcal{L}(E)$ associée à cette norme d'opérateur alors $N(f^k) \geq |\lambda^k|$. Par ailleurs l'hypothèse impose que $\lim_{k\to\infty} N(f^k) = 0$ donc $|\lambda| < 1$. On en déduit que $\rho(f) < 1$.

Signalons que $\rho(f)$ s'appelle d'habitude le rayon spectral de f. Cette série d'equivalence permet d'en obtenir la caractérisation usuelle suivante (indépendante de la norme choisie) :

$$\rho(f) = \lim_{n\to\infty} \|f^n\|^{1/n}.$$

D'abord la convergence de la suite $(\|f^n\|^{1/n})_{n\in\mathbb{N}}$ est un exercice classique. Cette limite est alors l'inverse du rayon de convergence de la série entière réelle $\sum \|f^n\| x^n$. En appliquant le lemme d'Abel et la première équivalence, ce rayon de convergence est aussi égal à $\frac{1}{\rho(f)}$.

Chapitre 3

Session de 1991

3.1 Sujet

3.2 Correction

A. Théorème de Gauss-Lucas, séries lacunaires.

I. *Le théorème de Gauss-Lucas.*

1. Enveloppe convexe d'une partie d'un espace affine réel E.

a. Soit $(C_i)_{i\in I}$ une famille quelconque de parties convexes de E.
Si $\bigcap_{i\in I} C_i = \emptyset$ alors elle est évidemment convexe.
Sinon, pour tout $x, y \in \bigcap_{i\in I} C_i$ on sait que pour tout $i \in I$, $x \in C_i$ et $y \in C_i$.
Comme C_i est convexe alors

$$\forall i \in I, [x, y] \subset C_i,$$

où $[x, y]$ désigne le segment reliant x à y. Ceci prouve que $[x, y] \subset \bigcap_{i\in I} C_i$ et que $\bigcap_{i\in I} C_i$ est convexe.

b. Soit $\mathcal{C} = \{C \subset E$ tel que C convexe et $A \subset C\}$. On a alors les deux propriétés suivantes : $\mathcal{C}$ est non vide car $E \in \mathcal{C}$ et pour tout $C \in \mathcal{C}$, $A \subset C$. On définit alors $C(A)$ par :

$$C(A) = \bigcap_{C\in\mathcal{C}} C.$$

D'après la question précédente, on sait que $C(A)$ est convexe et par construction, $C(A)$ vérifie la propriété :

$$(\mathcal{P}) \qquad \text{pour tout convexe } K \subset E,\ A \subset K \Leftrightarrow C(A) \subset K.$$

On a unicité de cet ensemble car si $C_1(A)$ et $C_2(A)$ sont deux convexes vérifiant $(\mathcal{P})$ alors : comme $A \subset C_1(A)$ et $C_2(A)$ vérifie $(\mathcal{P})$ alors $C_2(A) \subset C_1(A)$. De la même manière $C_1(A) \subset C_2(A)$ donc $C_1(A) = C_2(A)$.

c. Soit $B = \{$barycentres des systèmes (λ_i, M_i) tels que $\sum_{i=1}^{n} \lambda_i \neq 0, \lambda_i \geq 0\}$.
Par propriété de transitivité des barycentres, B est un convexe de l'espace affine E.

- Comme $A = \{M_1, \ldots, M_n\}$ alors il est évident que $A \subset B$.
- D'autre part, si K est un convexe de E contenant A alors par définition de la convexité, K contient tous les barycentres des systèmes (λ_i, M_i) avec $\sum_{i=1}^{n} \lambda_i \neq 0$ et $\lambda_i \geq 0$ donc $B \subset K$.

On a ainsi prouvé que B vérifie la propriété $(\mathcal{P})$ donc B est l'enveloppe convexe de A.

2. Le théorème de Gauss-Lucas.

a. On a $P = c\prod_{i=1}^{p}(X-\alpha_i)^{n_i}$ avec $n_i \geq 1$, c complexe non nul, et les nombres complexes α_i deux à deux distincts. On en déduit que

$$\begin{aligned} P' &= c\sum_{i=1}^{p} n_i(X-\alpha_i)^{n_i-1}\prod_{j\neq i}(X-\alpha_j)^{n_j} \\ &= \sum_{i=1}^{p} n_i \frac{P}{X-\alpha_i} \end{aligned}$$

et que

$$\frac{P'}{P} = \sum_{i=1}^{p}\frac{n_i}{X-\alpha_i}.$$

b. Soit z tel que $P'(z) = 0$ et $P(z) \neq 0$ alors par l'égalité précédente, on a

$$0 = \sum_{i=1}^{p}\frac{n_i}{z-\alpha_i}.$$

Or $\frac{1}{z-\alpha_i} = \frac{\overline{z-\alpha_i}}{|z-\alpha_i|^2}$ et $n_i \in \mathbb{N}$ donc en prenant le conjugué de cette expression,

$$0 = \sum_{i=1}^{p} n_i \frac{z-\alpha_i}{|z-\alpha_i|^2}.$$

c. On a $Z(P) = \{z \in \mathbb{C}; P(z) = 0\} = \{\alpha_1, \dots \alpha_p\}$ donc par le 1.c., $C(Z(P))$ est l'ensemble des barycentres des systèmes (λ_i, α_i) tels que $\sum_{i=1}^{p}\lambda_i \neq 0$ et $\lambda_i \geq 0$. Si $z \in Z(P')$ alors distinguons deux cas :
si $z \in Z(P)$ alors $z \in C(Z(P))$,
si $z \notin Z(P)$ alors par la question précédente, on sait que z est barycentre du système $\left(\alpha_i, \frac{n_i}{|z-\alpha_i|^2}\right)$ (c'est la définition même du barycentre). On a bien $\frac{n_i}{|z-\alpha_i|^2} \geq 0$ et $\sum_{i=1}^{p}\frac{n_i}{|z-\alpha_i|^2} \neq 0$ donc $z \in C(Z(P))$.
On a alors prouvé le théorème de Gauss-Lucas : $Z(P') \subset C(Z(P))$.

3. Application à la localisation des zéros dans un disque.

On suppose que $Z(P)) \subset D(0,R)$, disque de centre 0 et de rayon R. Comme $D(0,R)$ est convexe alors $C(Z(P)) \subset D(0,R)$. Le théorème de Gauss-Lucas assure que $Z(P') \subset C(Z(P))$ donc les zéros du polynôme dérivé sont aussi de module inférieur ou égal à R.

II. *Surjectivité des fonctions définies par une série lacunaire.*

Comme tous les complexes a_k sont distincts de 0, P_d est un polynôme de valuation $n_0 = 0$ et de degré n_d, Q_d est un polynôme de degré n_d et de valuation 0 et R_d est un polynôme de valuation 0 et de degré $n_d - 1$.

a. Comme $Q_d(X) = X^{n_d}P_d(\frac{1}{X})$ et $val(Q_d) = 0$ alors

$$Z(Q_d) = \{z \in \mathbb{C}, \frac{1}{z} \in Z(P_d)\}.$$

Comme $R_d(X) = X^{n_d-1}Q'_d(\frac{1}{X})$ et $val(R_d) = 0$ alors

$$Z(R_d) = \{z \in \mathbb{C}, \frac{1}{z} \in Z(Q'_d)\}.$$

Si P_d n'a pas de zéros dans $D(0,\rho)$ alors $Z(Q_d) \subset D(0,1/\rho)$. Par le I.3. on en déduit que $Z(Q'_d) \subset D(0,1/\rho)$ donc R_d n'a pas de zéros dans $D(0,\rho)$.

b. Par définition de Q_d et de R_d, on a clairement :

$$\begin{aligned} Q_d(X) &= \sum_{k=0}^{d} a_k X^{n_d-n_k}, \\ Q'_d(X) &= \sum_{k=0}^{d-1} a_k(n_d-n_k)X^{n_d-n_k-1}, \\ R_d(X) &= \sum_{k=0}^{d-1} a_k(n_d-n_k)X^{n_k} = n_d-(n_d-1)X+\sum_{k=2}^{d-1} a_k(n_d-n_k)X^{n_k}. \end{aligned}$$

c. Prouvons ce résultat par récurrence. Soit $H(d)$ l'hypothèse :
pour toute série entière lacunaire $1-z+\sum_{k=2}^{+\infty} a_k z^{n_k}$, *le polynôme* $P_d = \sum_{k=0}^{d} a_k z^{n_k}$ *admet un zéro de module inférieur ou égal à* ρ_d.
L'hypothèse est vraie au rang 1 car dans ce cas, pour toute série entière lacunaire de ce type, on a $P_1 = 1-z$ donc P_1 admet une unique racine $z = 1$ de module inférieur ou égal à 1.
Supposons $H(d-1)$ vraie et prouvons $H(d)$. On considère une série entière lacunaire

$$1-z+\sum_{k=2}^{+\infty} a_k z^{n_k} \text{ et } P_d = \sum_{k=0}^{d} a_k z^{n_k}.$$

Dans ce cas, $R_d = n_d-(n_d-1)X+\sum_{k=2}^{d-1} a_k(n_d-n_k)X^{n_k}$. Comme $(n_k)_{k\in\mathbb{N}}$ est une suite strictement croissante, $n_1 = 1$ et $d \geq 2$ alors $n_d \geq 2$. Soit

$$S = 1-X+\sum_{k=2}^{d-1} a_k \frac{n_d-n_k}{n_d}\left(\frac{n_d}{n_d-1}\right)^{n_k} X^{n_k}$$

de telle sorte que $R_d = n_d S\left(\frac{n_d-1}{n_d}X\right)$. On définit la série entière lacunaire, $1-z+\sum_{k=2}^{+\infty} b_k z^{n_k}$, avec

$$\begin{cases} \forall\, 2 \leq k \leq d-1, & b_k = a_k \dfrac{n_d-n_k}{n_d}\left(\dfrac{n_d}{n_d-1}\right)^{n_k} \\ \forall\, k \geq d, & b_k = a_k. \end{cases}$$

D'après $H(d-1)$, on sait que le polynôme S admet un zéro de module inférieur ou égal à ρ_{d-1} ce qui prouve que R_d admet un zéro de module inférieur ou égal à $\rho_d = \frac{n_d}{n_d-1}\rho_{d-1}$. Par contraposée du a., P_d admet un zéro de module inférieur ou égal à ρ_d donc $H(d)$ est vraie.

2. Existence d'un zéro de f.

a. On vient de voir que pour tout $d \in \mathbb{N}^\star$, il existe $z \in \mathbb{C}$ tel que $P_d(z) = 0$ et $|z| \leq \rho_d$. Or pour tout $d \geq 2$,

$$\ln \rho_d = \sum_{k=2}^{d} \ln \frac{1}{1 - \frac{1}{n_k}}$$

Comme (n_k) est une suite d'entiers strictement croissante, $\lim\limits_{k\to\infty} n_k = \infty$ et $\ln \dfrac{1}{1 - \frac{1}{n_k}} \sim \dfrac{1}{n_k}$. La série $\sum \frac{1}{n_k}$ est convergente donc par critère de comparaison des séries à termes positifs, $\sum \ln \frac{1}{1-\frac{1}{n_k}}$ est convergente ce qui prouve que $(\rho_d)_{d\geq 2}$ est une suite bornée de $\mathbb{C}$. Soit $M = \sup\limits_{d\geq 1} |\rho_d|$ alors

$$\forall d \in \mathbb{N}^\star, \exists z \in \mathbb{C} \text{ tel que } P(z) = 0 \text{ et } |z| \leq M.$$

b. Par le a., pour tout $d \in \mathbb{N}^\star$, il existe $z_d \in D(0, M)$ tel que $P(z_d) = 0$. La suite $(z_d)_{d\in\mathbb{N}}$ a donc tous ses éléments contenus dans le compact $D(0, M)$. On peut en extraire une sous-suite convergente vers $z \in D(0, M)$. Comme $f(z_d) = f(z_d) - P_d(z_d)$ alors

$$|f(z_d)| \leq \sup_{z\in D(0,M)} |f(z) - P_d(z)|.$$

Or P_d converge uniformément vers f sur $D(0, M)$ (le rayon de convergence de la série entière lacunaire est infini et on a même convergence normale sur tous les compacts de $\mathbb{C}$) donc $\lim\limits_{d\to\infty} |f(z_d)| = 0$. Comme f est continue et $\lim\limits_{d\to\infty} z_d = z$ alors $f(z) = 0$.

3. On a

$$g(z) = g(0) + g'(0)z + \sum_{k=2}^{\infty} b_k z^{n_k}.$$

Soit $y \in \mathbb{C}$. Si $y = g(0)$ alors on a trouvé un antécédent de y
Si $y \neq g(0)$ alors $g(z) = y$ s'écrit (car $g'(0) \neq 0$) :

$$1 - \frac{g'(0)}{y - g(0)}\, z - \sum_{k=2}^{\infty} \frac{b_k}{y - g(0)} \left(\frac{y - g(0)}{g'(0)}\right)^{n_k} \left(\frac{g'(0)z}{y - g(0)}\right)^{n_k} = 0.$$

En posant $Z = \dfrac{g'(0)z}{y - g(0)}$, $a_k = \dfrac{b_k}{y - g(0)} \left(\dfrac{y - g(0)}{g'(0)}\right)^{n_k}$ et en définissant f la série entière lacunaire associée à cette suite :

$$f(Z) = 1 - Z + \sum_{k=2}^{\infty} a_k Z^{n_k},$$

on a

$$g(z) = y \iff \left(f(Z) = 0 \text{ et } z = \frac{y - g(0)}{g'(0)}\, Z \right).$$

Comme g est une série entière lacunaire de rayon de convergence infini, il en est de même pour f et f vérifie les hypothèses du 1. et 2. ce qui permet de conclure par le 2.b. que f admet un zéro dans $\mathbb{C}$. On a alors trouvé un antécédent de y par g.

B. Localisation des zéros d'un polynôme.

1. Localisation des valeurs propres d'une matrice.

a. On suppose que $\alpha > 0$. Soit i_0 tel que $\|X\| = |x_{i_0}| = \max_{1\leq i\leq n} |x_i|$. On a alors $\|AX\| \geq |(AX)_{i_0}|$. Or

$$|(AX)_{i_0}| = |\sum_{j=1}^{n} A_{i_0 j} x_j| \geq |A_{i_0 i_0} x_{i_0}| - \sum_{j\neq i_0} |A_{i_0 j}||x_j|$$

et pour tout $j \neq i_0$, $|x_j| \leq \|X\| = |x_{i_0}|$ donc

$$\|AX\| \geq |(AX)_{i_0}| \geq \|X\| L_{i_0} \geq \alpha \|X\|.$$

On en déduit que si $AX = 0$ alors $\|X\| = 0$ donc $X = 0$ ce qui prouve que A est injective. Comme la dimension est finie, A est inversible.

b. Soit $B = \lambda \mathrm{I} - A$ avec $\lambda \in \left(\bigcup_1^n D(A_{ii}, \sum_{j\neq i} |A_{ij}|) \right)^c$. Pour tout $i = 1, \ldots, n$

$$|B_{ii}| = |\lambda - A_{ii}| > \sum_{j\neq i} |A_{ij}| = \sum_{j\neq i} |B_{ij}|.$$

Soit $\alpha = \min_{1\leq i\leq n} \{|B_{ii}| - \sum_{j\neq i} |B_{ij}|\}$ alors $\alpha > 0$ (car le nombre d'indices est fini) et par le a., on en conclut que B est inversible. Pour toute valeur propre λ de A, la matrice $\lambda \mathrm{I} - A$ est non inversible donc par contraposée,

$$\lambda \in \bigcup_1^n D(A_{ii}, \sum_{j\neq i} |A_{ij}|).$$

2. Application aux polynômes.
On établit par récurrence que P est au signe près le polynôme caractéristique de A (il s'agit même du polynôme minimal, voir la question I.C. du sujet de 1990) donc par le 1.b., tout zéro de P est dans l'ensemble

$$D(0,1) \cup D(-a_{n-1}, \sum_{j=0}^{n-2} |a_j|).$$

3. Par le A.I.2.a. on a vu que lorsque $P = c \prod_{i=1}^{p} (X - \alpha_i)^{n-i}$,

$$\frac{P'}{P} = \sum_{j=1}^{p} \frac{n_j}{X - \alpha_j}.$$

Ainsi,

$$\frac{1}{2i\pi}\int_\Gamma \frac{P'(z)}{P(z)}dz = \sum_{j=1}^{p} \frac{1}{2i\pi}\int_\Gamma \frac{n_j}{z-\alpha_j}dz.$$

Par le théorème des résidus, on sait que si $\alpha_j \in D$, $\frac{1}{2i\pi}\int_\Gamma \frac{dz}{z-\alpha_j} = 1$ et si $\alpha_j \notin D$, $\frac{1}{2i\pi}\int_\Gamma \frac{dz}{z-\alpha_j} = 0$ donc

$$\frac{1}{2i\pi}\int_\Gamma \frac{P'(z)}{P(z)}dz = \sum_{j \text{ tel que } \alpha_j \in D} n_j.$$

C. Le théorème de Grace.

1. Action de $\mathrm{GL}_2(\mathbb{C})$ sur la sphère de Riemann.

a. Soit ϕ le morphisme surjectif de $\mathrm{GL}_2(\mathbb{C})$ sur $\mathbb{H}$ défini par $\phi(A) = H_A$. L'élément neutre du groupe multiplicatif $\mathbb{H}$ est l'identité et $\phi(A) = \mathrm{I}$ si et seulement si pour tout $z \in \mathbb{C}$, $H_A(z) = z$ et $H_A(\infty) = \infty$. Par définition, en notant $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a $H_A(\infty) = \frac{a}{c} = \infty$, $H_A(0) = \frac{b}{d} = 0$ et $H_A(1) = \frac{a+b}{c+d}$ donc $b = c = 0$ et $a = d$. Réciproquement, il est clair que si $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, avec $a \in \mathbb{C}^\star$, alors $\phi(A) = \mathrm{I}$. On en conclut que

$$\ker\phi = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \in \mathbb{C}^\star \right\}.$$

b. Soit $M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $M_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $N_k = \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}$ avec $k \in \mathbb{C}^\star$.
Par un calcul élémentaire sur les matrices 2×2, on constate que :
Multiplier la matrice A par la matrice M_1 revient à échanger les colonnes de la matrice tandis que multiplier la matrice M_1 par la matrice A revient à échanger les lignes de la matrice.
Multiplier la matrice A par la matrice M_2 revient à garder inchangée la première colonne de la matrice et à additionner les deux colonnes de la matrice tandis que multiplier la matrice M_2 par la matrice A revient à additionner les deux lignes de la matrice et à garder inchangée la seconde ligne de la matrice.
Multiplier la matrice A par la matrice N_k revient à multiplier par k la première colonne de la matrice et à garder inchangée la seconde colonne de la matrice tandis que multiplier la matrice N_k par la matrice M revient à multiplier par k la première ligne de la matrice et à garder inchangée la seconde ligne de la matrice.

En multipliant par ces matrices, on peut effectuer toutes les opérations élémentaires possibles sur les lignes et les colonnes. Or lorsque $M \in \mathrm{GL}_2(\mathbb{C})$, on sait que M est transformée en l'identité après une suite d'opérations élémentaires sur les lignes et les colonnes (méthode du pivot de Gauss). L'ensemble des matrices

$$\left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} \text{ où } k \in \mathbb{C}^\star. \right\}$$

engendre donc $\mathrm{GL}_2(\mathbb{C})$.

c. Comme ϕ est un morphisme surjectif de $\mathrm{GL}_2(\mathbb{C})$ sur le groupe des homographies alors l'image par ϕ de cet ensemble générateur de $\mathrm{GL}_2(\mathbb{C})$ est une partie génératrice de $\mathbb{H}$, c'est à dire : $\{H_1, H_2, h_k \text{ où } k \in \mathbb{C}^\star\}$ engendre $\mathbb{H}$ avec

$$\forall z \in S, H_1(z) = \frac{1}{z}, H_2(z) = z + 1, h_k(z) = kz.$$

2. Géométrie de la sphère de Riemann. On rappelle que le birapport de z_1, z_2, z_3, z_4 éléments distincts de S est défini par

$$[z_1, z_2; z_3, z_4] = \frac{z_4 - z_2}{z_4 - z_1} \Big/ \frac{z_3 - z_2}{z_3 - z_1}$$

avec la convention que $\frac{\infty}{\infty} = 1$. Ainsi, un $S-$cercle Γ est caractérisé par trois éléments z_1, z_2, z_3 de S tels que

$$\Gamma = \{z \in \mathbb{C} \text{ tel que } [z, z_1; z_2, z_3] \in \mathbb{R}\}.$$

a. Le birapport d'éléments distincts de S est conservé par les homographies H_1, H_2 et h_k donc le birapport est conservé par toute homographie (puisque H_1, H_2 et h_k engendre $\mathbb{H}$) ce qui prouve que l'image d'un $S-$cercle par une homographie est un $S-$cercle.

D'autre part, H_1, H_2 et h_k sont continues pour la topologie associée à la sphère de Riemann (en particulier, une base de voisinages de l'∞ est constituée des complémentaires des disques fermés de $\mathbb{C}$) et elles sont bijectives sur S donc il en est de même pour toutes les homographies. La frontière d'un $S-$disque fermé est un $S-$cercle donc par continuité, l'image d'un $S-$disque fermé par une homographie est incluse dans un $S-$disque fermé (car les propriétés de connexité sont conservées) et par bijectivité, l'image est un $S-$disque fermé.

b. Si C est un cercle de $\mathbb{C}$ alors C est l'image de Γ_0 par une similitude. Si C est une $S-$droite alors par translation puis par rotation, on transforme cette $S-$droite en la droite d'équation $\Re(z) = 1/2$. Cette droite est l'image par H_1 du translaté de Γ_0 par $1 : \{z \in \mathbb{C}, |z-1| = 1\}$. Ainsi, tout $S-$ cercle est l'image par au moins une homographie de Γ_0.

Il est clair que l'image par H_1 du disque unité est le complémentaire du disque unité ouvert donc de la même manière, tout $S-$disque fermé est l'image par une homographie du disque unité de $\mathbb{C}$.

3. Action de $\mathrm{GL}_2(\mathbb{C})$ sur les polynômes et sur la forme d'apolarité.

a. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ deux éléments de $\mathrm{GL}_2(\mathbb{C})$. On a $AB = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$ donc pour tout polynôme $P \in \mathbb{C}_n[X]$,

$$(AB)(P) = \Big(-(ce+dg)X + ae + bg \Big)^n P\Big(\frac{(cf+dh)X - (af+bh)}{-(ce+dg)X + ae + bg} \Big).$$

D'autre part, $B(P) = (-gX+e)^n P\big(\frac{hX-f}{-gX+e}\big)$ donc

$$\begin{aligned} A(B(P)) &= (-cX+a)^n \bigg(-g\,\frac{dX-b}{-cX+a} + e \bigg)^n P\bigg(\frac{h\,\frac{dX-b}{-cX+a} - f}{-g\,\frac{dX-b}{-cX+a} + e} \bigg) \\ &= (AB)(P). \end{aligned}$$

Ce résultat prouve que l'on définit bien une action de $\mathrm{GL}_2(\mathbb{C})$ sur $\mathbb{C}_n[X]$. En particulier, comme $\{M_1, M_2, N_k \text{ avec } k \in \mathbb{C}^\star\}$ engendre $\mathrm{GL}_2(\mathbb{C})$, il nous suffira d'étudier l'action de ces matrices sur $\mathbb{C}_n[X]$ pour obtenir des résultats sur l'action de n'importe quelle matrice.

b. On a $A_t(P) = P(X+t)$ et $A_t(Q) = Q(X+t)$ donc

$$G_n(A_t(P), A_t(Q)) = \sum_{k=0}^{n} (-1)^k P^{(k)}(t) Q^{(n-k)}(t).$$

Appelons f cette fonction de t : elle est holomorphe sur $\mathbb{C}$ et

$$\begin{aligned} f'(t) &= \sum_{k=0}^{n} (-1)^k \Big(P^{(k+1)}(t) Q^{(n-k)}(t) + P^{(k)}(t) Q^{(n-k+1)}(t) \Big) \\ &= P(t) Q^{(n+1)}(t) + (-1)^n P^{(n+1)}(t) Q(t). \end{aligned}$$

Or $P, Q \in \mathbb{C}_n[X]$ donc $f'(t) = 0$ et pour tout $t \in \mathbb{C}$,

$$G_n(A_t(P), A_t(Q)) = f(t) = f(0) = G_n(P, Q).$$

c. Soit $P = \sum_{j=0}^{n} p_j X^j \in \mathbb{C}_n[X]$ et $Q = \sum_{j=0}^{n} q_j X^j \in \mathbb{C}_n[X]$, il est clair que

$$G_n(P, Q) = \sum_{j=0}^{n} (-1)^j j!\,(n-j)!\, p_j q_{n-j}.$$

Par le a., il suffit de prouver le résultat pour les matrices M_1, M_2, N_k avec $k \in \mathbb{C}^\star$.
On vient de voir que $G_n(P, Q) = G_n(M_2(P), M_2(Q))$ car $A_{-1} = M_2$.
De plus, pour tout polynôme $P \in \mathbb{C}_n[X]$, pour tout $k \in \mathbb{C}^\star$ on a :

$$\begin{aligned} M_1(P) &= (-1)^n X^n P(\frac{1}{X}) = (-1)^n \sum_{j=0}^{n} p_{n-j} X^j \\ \text{et} \quad N_k(P) &= k^n P(\frac{X}{k}) = k^n \sum_{j=0}^{n} \frac{p_j}{k^j} X^j \end{aligned}$$

ce qui donne

$$G_n(M_1(P), M_1(Q)) = \sum_{j=0}^{n} (-1)^j j!\,(n-j)!\, p_{n-j} q_j = (-1)^n G_n(P, Q)$$

$$\begin{aligned} \text{et } G_n(N_k(P), N_k(Q)) &= k^{2n} \sum_{j=0}^{n} (-1)^j j!\,(n-j)!\, \frac{p_j q_{n-j}}{k^j k^{n-j}} X^j \\ &= k^n G_n(P, Q). \end{aligned}$$

Le résultat est alors évident.

4. Effet de l'action de $\mathrm{GL}_2(\mathbb{C})$ sur les zéros des polynômes.

a. Soit P un élément non nul de $\mathbb{C}_n[X]$. Par la théorie classique des polynômes symétriques, on sait que $x_1, \ldots, x_{n-k}$ sont les racines de P comptées avec leur multiplicité si et seulement si il existe $c \in \mathbb{C}^\star$ tel que :

$$P = c \sum_{j=0}^{n-k} (-1)^j \sigma_j(x_1, \ldots, x_{n-k}) X^{n-k-j}.$$

Après changement d'indice, on constate que P s'écrit

$$P = c \sum_{j=k}^{n} (-1)^{j-k} \sigma_{j-k}(x_1, \ldots, x_{n-k}) X^{n-j}.$$

Or la convention adoptée pour étendre les fonctions symétriques élémentaires à S assure que :

$$P = (-1)^k c \sum_{j=0}^{n} (-1)^j \sigma_j(x_1, \ldots, x_{n-k}, \infty, \ldots, \infty) X^{n-j},$$

où l'∞ est un zéro de multiplicité k.

b. Comme précédemment, il suffit de prouver le résultat pour les matrices M_1, M_2, N_k, avec $k \in \mathbb{C}^\star$. On a vu au 3.c. que pour tout polynôme $P \in \mathbb{C}_n[X]$, pour tout $k \in \mathbb{C}^\star$,

$$\begin{cases} M_1(P) &= (-1)^n X^n P(\dfrac{1}{X}) \\ M_2(P) &= P(X+1) \\ N_k(P) &= k^n P(\dfrac{X}{k}) \end{cases}$$

donc il est clair que la famille des zéros de $M_1(P)$ dans S (respectivement $M_2(P)$, $N_k(P)$) est l'image par l'homographie H_1 (respectivement H_2, h_k) des zéros de P dans S.

5. Le théorème de Grace.

a. On note F le $S-$disque fermé contenant les zéros dans S de P et ne contenant pas ceux de Q. Par le 3.a., il suffit de trouver une matrice A telle que $A(P)$ et $A(Q)$ vérifient les hypothèses énoncées.

Supposons Q de degré n :
on considère H_A une homographie qui envoie un des zéros de Q sur l'∞. Par le 4.b., la famille des zéros dans S de $A(Q)$ est l'image par l'homographie H_A de celle des zéros dans S de Q donc $A(Q)$ admet l'∞ comme zéro d'ordre de multiplicité 1 et le degré de $A(Q)$ est strictement inférieur à n.
Par le 4.b., la famille des zéros dans S de $A(P)$ est contenu dans l'image par H_A de F. S'il existait $z \in H_A(F)$ zéro dans S de $A(Q)$ alors en faisant agir par

A^{-1}, on trouverait un zéro de Q dans F ce qui est contradictoire donc $H_A(F)$ ne contient aucun zéro dans S de $A(Q)$.
Mais par le 2.a., $H_A(F)$ est un $S-$disque fermé et comme ∞ est une racine de $A(Q)$ alors $H_A(F)$ ne contient pas l'∞. Il s'agit donc d'un disque fermé de $\mathbb{C}$ et on a bien les trois hypothèses désirées.

Si Q est de degré inférieur strictement à n alors l'∞ est zéro de Q et la dernière partie du raisonnement montre qu'il n'y a pas à changer P et Q pour avoir ces hypothèses.

b. Comme Q est de degré inférieur ou égal à $n-1$ alors $G_{n-1}(P', Q)$ a un sens et

$$\begin{aligned} G_{n-1}(P', Q) &= \sum_{k=0}^{n-1} (-1)^k P^{(k+1)}(0) Q^{(n-1-k)}(0) \\ &= -\sum_{k=1}^{n} (-1)^k P^{(k)}(0) Q^{(n-k)}(0). \end{aligned}$$

Or $Q^{(n)}(0) = 0$ donc $G_{n-1}(P', Q) = -G_n(P, Q) = 0$.

c. Prouvons le théorème de Grace par récurrence. Soit $H(n)$ l'hypothèse : *Pour tout P, $Q \in \mathbb{C}_n[X]$ non nuls tels que $G_n(P, Q) = 0$, tout $S-$disque fermé contenant tous les zéros dans S de P contient au moins un zéro dans S de Q.*

Au rang 1, on a $P = aX + b$, $Q = cX + d$ non nuls et $G_1(P, Q) = 0$ assure que $ad - bc = 0$. On en conclut que P et Q ont les mêmes racines donc le résultat est évident.

Supposons l'hypothèse vriae au rang $n-1$. Montrons la au rang n en raisonnant par l'absurde (comme cela est suggeré au début de cette question 5.). Par le a. et le b., on trouve deux polynômes P et Q vérifiant :

(i) Q est degré inférieur ou égal à $n-1$.

(ii) D est un disque fermé de $\mathbb{C}$ contenant tous les zéros dans S de P.

(iii) aucun des zéros dans S de Q n'appartient à D.

(iv) $G_{n-1}(P', Q) = 0$.

Par le théorème de Gauss-Lucas (A.I.3.), on sait que tous les zéros de P' sont dans D, disque fermé de $\mathbb{C}$. Comme $P', Q \in \mathbb{C}_{n-1}[X]$ (cf (i)), et $G_{n-1}(P', Q) = 0$ (cf(iv)), on peut appliquer l'hypothèse de récurrence et D contient au moins un zéro dans S de Q. Ceci est contradictoire avec (iii) donc l'hypothèse de récurrence est vraie au rang n.

6. Autre forme du théorème de Grace.
Soit $Q = \sum_{j=0}^{n} (-1)^j \sigma_j(x_1, \ldots, x_n) X^{n-j}$. Par le 4.a. on sait que $x_1, \ldots, x_n$ sont les zéros de Q comptés avec leur multiplicité. On peut alors exprimer l'hypothèse sur les a_j en terme d'apolarité :

$$\begin{aligned} G_n(Q, P) &= (-1)^n G_n(P, Q) \\ &= (-1)^n \sum_{j=0}^{n} (-1)^j j!\,(n-j)!\, C_n^j a_j (-1)^j \sigma_j(x_1, \ldots, x_n) \\ &= (-1)^n n! \sum_{j=0}^{n} a_j \sigma_j(x_1, \ldots, x_n) = 0. \end{aligned}$$

Comme D est un $S-$disque fermé contenant tous les zéros de Q alors par le théorème de Grace, le polynôme P a au moins un zéro dans S, éventuellement ∞, appartenant à D.

7. Application.

L'égalité $H(u) = 0$ s'écrit $\sum_{j=0}^{n} C_n^j a_j b_j u^k = 0$. Soit Q_1 défini par $Q_1 = X^n Q(-\frac{u}{X})$ alors

$$Q_1 = \sum_{j=0}^{n} (-1)^j C_n^j b_j u^k X^{n-j}.$$

On a alors $H(u) = 0 \iff G_n(P, Q_1) = 0$. Comme tous les zéros dans S de P sont de module inférieur ou égal à R_1 alors par le théorème de Grace, il existe un zéro z_1 de Q_1 tel que $|z_1| \leq R_1$.

Or 0 n'est pas racine de Q_1 car Q est de degré exactement n et $b_n \neq 0$ donc

$$Q_1(z) = 0 \iff Q(-\frac{u}{z}) = 0.$$

Comme les zéros de Q dans S sont de module inférieur ou égal à R_2 alors

$$\left|\frac{u}{z_1}\right| \leq R_2 \text{ et } |z_1| \leq R_1,$$

ce qui prouve que $|u| \leq R_1 R_2$.

C. Le théorème de Biernacki sur les sommes des séries lacunaires.

1. Préliminaire : zéros de la dérivée d'un produit.

a. Comme z est un zéro de Π' alors $\Pi_1(z)\Pi_2'(z) + \Pi_2(z)\Pi_1'(z) = 0$. Or

$$\begin{cases} \Pi_1(z) &= \sum_{j=0}^{p} (-1)^j \sigma_j(\alpha_1, \ldots, \alpha_p) z^{p-j} \\ \Pi_1'(z) &= \sum_{j=0}^{p-1} (p-j)(-1)^j \sigma_j(\alpha_1, \ldots, \alpha_p) z^{p-1-j}, \end{cases}$$

donc l'égalité $\Pi_1(z)\Pi_2'(z) + \Pi_2(z)\Pi_1'(z) = 0$. se traduit par

$$\sum_{j=0}^{p} a_j \sigma_j(\alpha_1, \ldots, \alpha_p) = 0$$

où pour tout $0 \leq j \leq p$, $a_j = (-1)^j z^{p-1-j}\big(z\Pi_2'(z) + (p-j)\Pi_2(z)\big)$. Par le C.6., le polynôme $P = \sum_{j=0}^{p} C_p^j a_j X^j$ a au moins un zéro dans S appartenant à D_1 car D_1 est un disque fermé complexe contenat tous les α_i.

D'autre part,

$$\begin{cases} (z-X)^p &= \displaystyle\sum_{j=0}^{p} C_p^j (-1)^j z^{p-j} X^j \\ \text{et } p(z-X)^{p-1} &= \displaystyle\sum_{j=0}^{p-1} p\, C_{p-1}^j (-1)^j z^{p-1-j} X^j. \end{cases}$$

Comme $p\, C_{p-1}^j = (p-j)C_p^j$ alors

$$\begin{aligned} &(z-X)^p \Pi_2'(z) + p(z-X)^{p-1}\Pi_2(z) \\ &= (-1)^p \Pi_2'(z) X^p + \sum_{j=0}^{p-1} (-1)^j z^{p-1-j} C_p^j \big(z\Pi_2'(z) + (p-j)\Pi_2(z)\big) X^j \\ &= \sum_{j=0}^{p} C_p^j a_j X^j = P. \end{aligned}$$

On sait alors qu'il existe $\alpha \in D_1$ tel que $P(\alpha) = 0$, c'est à dire :

$$(z-\alpha)^p \Pi_2'(z) + p(z-\alpha)^{p-1}\Pi_2(z) = 0.$$

Soit $P_1(X) = (X-\alpha)^p$ alors z est racine de $(\Pi_2 P_1)'$. De la même manière que précédemment, on trouve $\beta \in D_2$ tel que

$$(z-\beta)^q P_1'(z) + q(z-\beta)^{q-1} P_1(z) = 0,$$

c'est à dire

$$p(z-\alpha)^{p-1}(z-\beta)^q + q(z-\beta)^{q-1}(z-\alpha)^p = 0.$$

Ce résultat est valable pour tout zéro de Π' (infini ou non). Maintenant, comme $z \notin D_1$, $p \geq 1$, $q \geq 1$ alors $z - \alpha \neq 0$ et β ne peut pas être l'∞.

b. Soit z un zéro de Π' tel que $z \notin D_1 \cup D_2$. Par le a., il existe $\alpha \in D_1$, $\beta \in D_2 \setminus \{\infty\}$ tels que

$$p(z-\alpha)^{p-1}(z-\beta)^q + q(z-\beta)^{q-1}(z-\alpha)^p = 0.$$

Or $z \notin D_1 \cup D_2$ donc $z - \alpha \neq 0$ et $z - \beta \neq 0$ donc $p(z-\beta) + q(z-\alpha) = 0$ et

$$z = \frac{p\beta + q\alpha}{p+q}.$$

Ceci prouve que z est combinaison convexe de $\big((\beta, p/(p+q)), (\alpha, q/(p+q))\big)$ donc

$$z \in D_3 = D\left(\frac{pA_2 + qA_1}{p+q}, \frac{pR_2 + qR_1}{p+q}\right)$$

Comme D_1, D_2, D_3 sont des disques fermés disjoints alors il existe trois cercles Γ_1, Γ_2, Γ_3 tels que les disques de frontière Γ_i contiennent strictement D_i et soient disjoints. Cette construction assure que Π' ne s'annule sur aucun des Γ_i. Par le B.3., on a

$$\#\{z \in D_i, \Pi'(z) = 0\} = \frac{1}{2i\pi} \int_{\Gamma_i} \frac{\Pi''(z)}{\Pi'(z)} dz.$$

Fixons $\beta_1, \ldots, \beta_q$ et faisons varier $\alpha_1, \ldots, \alpha_p$: soit

$$\begin{array}{rcl} \phi_i : D_1^p & \to & \mathbb{N} \\ (\alpha_1, \ldots, \alpha_p) & \mapsto & \dfrac{1}{2i\pi} \displaystyle\int_{\Gamma_i} \frac{\Pi''(z)}{\Pi'(z)} dz. \end{array}$$

D'après les propriétés de continuité des intégrales dépendant d'un paramètre, ϕ_i est continue. Or D_1^p est connexe et ϕ_i est à valeurs entières donc ϕ_i est constante sur D_1^p. On peut alors considérer que $\alpha_1 = \ldots = \alpha_p = A_1$.
De la même manière, en faisant varier les β_i, on peut considérer par propriété de connexité et de continuité que $\beta_1 = \ldots = \beta_q = A_2$. Soit $P = (X-A_1)^p(X-A_2)^q$ alors

$$\#\{z \in D_i, \Pi'(z) = 0\} = \#\{z \in D_i, P'(z) = 0\}.$$

Or $P' = (X - A_1)^{p-1}(X - A_2)^{q-1}\big(p(X - A_2 + q(X - A_1)\big)$ donc

$$\frac{P''}{P'} = \frac{p-1}{X - A_1} + \frac{q-1}{X - A_2} + \frac{1}{X - \frac{pA_2 + qA_1}{p+q}}.$$

Il est clair par hypothèse que $\dfrac{pA_2 + qA_1}{p+q} \notin D_1 \cup D_2$ car D_1, D_2 et D_3 sont deux à deux disjoints donc

$$\left\{ \begin{array}{rcl} \#\{z \in D_1, \Pi'(z) = 0\} & = & \dfrac{1}{2i\pi} \displaystyle\int_{\Gamma_1} \frac{P''}{P'} = p - 1 \\ \#\{z \in D_2, \Pi'(z) = 0\} & = & \dfrac{1}{2i\pi} \displaystyle\int_{\Gamma_2} \frac{P''}{P'} = q - 1 \\ \#\{z \in D_3, \Pi'(z) = 0\} & = & \dfrac{1}{2i\pi} \displaystyle\int_{\Gamma_3} \frac{P''}{P'} = 1. \end{array} \right.$$

c. Tout d'abord, il existe $R_1 < R$ tel que pour tout $1 \leq i \leq p$, $\alpha_i \in D_1 = D(0, R_1)$. Soit $D_2 = \big(d(0, (p + 2q)R/p)\big)^c$ en notant par $d(\cdot)$ le disque ouvert correspondant.
Montrons que Π' ne s'annule pas sur le cercle Γ_R de centre 0 et de rayon R. En effet, supposons z zéro de Π' :
Si $z \in D_1 \cup D_2$, $|z| < R$ ou $|z| > (p + 2q)R/p > R$ donc $z \notin \Gamma_R$.
Si $z \notin D_1 \cup D_2$ et $z \neq \infty$ alors par le a., il existe $\alpha \in D_1$, $\beta \in D_2 \setminus \{\infty\}$ tels que

$$p(z - \alpha)^{p-1}(z - \beta)^q + q(z - \beta)^{q-1}(z - \alpha)^p = 0.$$

donc $z = \dfrac{p\beta + q\alpha}{p+q}$. Or $|\beta| > (p + 2q)R/p$ et $|\alpha| < R$ donc

$$|z| > \frac{(p + 2q)R}{p+q} - \frac{qR}{p+q} = R.$$

On en déduit que si $z \in \Pi'$ alors soit $z \in D_1$, soit $z \notin \big(d(0, R)\big)^c$ c'est à dire que Π' ne s'annule pas sur Γ_R. Par le B.3., on sait alors que

$$\#\{z \in D(0, R), \Pi'(z) = 0\} = \frac{1}{2i\pi} \int_{\Gamma_R} \frac{\Pi''}{\Pi'}.$$

De la même manière qu'à la question précédente, par connexité et continuité, on se ramène au cas où $\alpha_1 = \ldots = \alpha_p = 0 \in D_1$ et $\beta_1 = \ldots = \beta_q = \beta \in D_2$ avec $|\beta| > (p+2q)R/p$. Comme au b., on a

$$\#\{z \in D_1, \Pi'(z) = 0\} = p-1 \text{ avec } D_1 = D(0, R_1) \text{ et } R_1 < R.$$

2. Application à la localisation des zéros dans un disque.
Montrons le résultat par récurrence descendante. Soit $H(p)$ l'hypothèse :
Pour tout polynôme de degré n et de zéros $\alpha_1, \ldots, \alpha_n$ avec $|\alpha_1| \leq \ldots \leq |\alpha_n|$, si $R \in \mathbb{R}_+^\star$ est tel que $|\alpha_p| \leq R$ alors P' a au moins $p-1$ zéros de module inférieur ou égal à $R \displaystyle\prod_{k=0}^{n-p} \frac{n+k}{n-k}$.

Cette hypothèse est vraie pour $p = n$ car dans ce cas, pour tout i, $|\alpha_i| \leq R$ et par le théorème de Gauss-Lucas (A.I.3), P' a tous ses zéros contenus dans le disque de centre 0 et de rayon R. Le degré de P' vaut $n-1$ donc P' a $(n-1)$ zéros de module majoré par R.

Supposons $H(p+1)$ vraie et montrons $H(p)$: on suppose que

$$P = \prod_{i=1}^{n}(X - \alpha_i) \text{ avec } |\alpha_1| \leq \ldots \leq |\alpha_n| \text{ et } |\alpha_p| \leq R.$$

On constate que P s'écrit $P = \Pi_1\Pi_2$ avec

$$\Pi_1 = \prod_{k=0}^{p}(X - \alpha_k) \text{ et } \Pi_2 = \prod_{k=p+1}^{n}(X - \alpha_k).$$

Le degré de Π_1 est p et celui de Π_2 est $n-p$. Comme $|\alpha_p| \leq R$ alors les zéros de Π_1 sont dans le disque $D(0,R)$ et comme les α_i sont rangés par ordre croissant en module, les zéros de Π_2 sont de module supérieur ou égal à $|\alpha_{p+1}|$.
Si $|\alpha_{p+1}| > \frac{p+2(n-p)}{p}R = (2n-p)R/p$ alors d'après le 1.c. (en remplaçant R par $R + \varepsilon > R$ puis en faisant tendre ε vers 0), on sait que P' admet exactement $(p-1)$ zéros de module inférieur ou égal à R. Il est évident que $R \leq R \displaystyle\prod_{k=0}^{n-p} \frac{n+k}{n-k}$.
Si $|\alpha_{p+1}| \leq (2n-p)R/p$ alors P vérifie les hypothèses de la récurrence au rang $p+1$ avec $R' = (2n-p)R/p$. On en déduit que P' admet au moins p zéros de module inférieur ou égal à $R' \displaystyle\prod_{k=0}^{n-p-1} \frac{n+k}{n-k}$. Or $R' = (2n-p)R/p$ donc

$$R' \prod_{k=0}^{n-p-1} \frac{n+k}{n-k} = R \prod_{k=0}^{n-p} \frac{n+k}{n-k}.$$

On en conclut que dans tous les cas, P' admet au moins $(p-1)$ zéros de module inférieur ou égal à $R \displaystyle\prod_{k=0}^{n-p} \frac{n+k}{n-k}$ ce qui prouve $H(p)$.

3. Existence d'une infinité de zéros pour la somme d'une série lacunaire.

a. Ecrivons Q sous la forme

$$Q = \sum_{i=0}^{q} C_{n_q}^{n_i}\big(\frac{a_i}{C_{n_q}^{n_i}}\big)\,(n_r - n_i)\dots(n_{q+1} - n_i)X^{n_i}.$$

Par le C.7., il suffit de localiser les zéros des deux polynômes P_1 et P_2 où

$$P_1 = \sum_{i=0}^{q} a_i X^{n_i} \text{ et } P_2 = \sum_{i=0}^{q} C_{n_q}^{n_i}(n_r - n_i)\dots(n_{q+1} - n_i)X^{n_i}.$$

Par hypothèse, les zéros de $P_1 = P_d$ sont de module inférieur ou égal à R. Normalisons le polynôme P_2 : $P_2 = g_{r-q}(n_q)\tilde{P}_2$ avec

$$\tilde{P}_2 = \sum_{i=0}^{q} C_{n_q}^{n_i} \prod_{j=q+1}^{r} \frac{n_j - n_i}{n_j - n_q}\, X^{n_i}.$$

Par le B.2., les zéros de $\tilde{P}_2$ (et donc ceux de P_2) sont contenus dans

$$D(0,1) \cup D\Big(- C_{n_q}^{n_{q-1}} \prod_{j=q+1}^{r} \frac{n_j - n_{q-1}}{n_j - n_q}, \sum_{i=0}^{q-2} C_{n_q}^{n_i} \prod_{j=q+1}^{r} \frac{n_j - n_i}{n_j - n_q}\Big).$$

Or $n_i \geq 0$ et $\displaystyle\sum_{i=0}^{q-2} C_{n_q}^{n_i} \leq \sum_{k=0}^{n_q} C_{n_q}^{k} = 2^{n_q} = 2^p$ donc

$$\begin{aligned} \sum_{i=0}^{q-2} C_{n_q}^{n_i} \prod_{j=q+1}^{r} \frac{n_j - n_i}{n_j - n_q} &\leq \Big(\prod_{j=q+1}^{r} \frac{n_j}{n_j - n_q} \Big) \sum_{i=0}^{q-2} C_{n_q}^{n_i} \\ &\leq 2^p \prod_{j=q+1}^{r} \frac{n_j}{n_j - n_q}. \end{aligned}$$

Comme $\frac{n_j}{n_j - n_q} \geq 1$ et $2^p \geq 1$, les zéros de P_2 sont de module inférieur ou égal à $2^p \displaystyle\prod_{j=q+1}^{r} \frac{n_j}{n_j - n_q}$. En appliquant le C.7., on en conclut que les zéros de Q sont de module majoré par

$$R(p,r) = R \cdot 2^p \prod_{j=q+1}^{r} \frac{n_j}{n_j - n_q}.$$

b. Montrons par récurrence sur j que

$$F_j = \sum_{k=0}^{r-j} a_k \left(\prod_{i=0}^{j-1} (n_{r-i} - n_k) \right) X^{n_{r-j} - n_k}.$$

Au rang 0, on a déjà vu au A.II.2.b. que

$$X^{n_r} P_r(\frac{1}{X}) = \sum_{k=0}^{r} a_k X^{n_r - n_k},$$

ce qui prouve l'hypothèse au rang 0.
Supposons la vraie au rang j et montrons la au rang $j+1$. Par définition,

$$X^{n_{r-j}-n_{r-j-1}-1}F_{j+1}(X) = F_j'(X)$$

et d'après l'hypothèse, on sait que

$$F_j'(X) = \sum_{k=0}^{r-j-1} a_k \prod_{i=0}^{j}(n_{r-i}-n_k)\, X^{n_{r-j}-n_k-1}.$$

On en déduit que

$$F_{j+1} = \sum_{k=0}^{r-j-1} a_k \prod_{i=0}^{j}(n_{r-i}-n_k)\, X^{n_{r-j-1}-n_k}$$

ce qui prouve l'hypothèse au rang $j+1$.

On constate que

$$F_{r-q} = \sum_{k=0}^{q} a_k \left(\prod_{i=0}^{r-q-1} (n_{r-i}-n_k)\right) X^{n_q-n_k}.$$

Mais $X^p Q(\frac{1}{X}) = \sum_{k=0}^{q} g_{r-q}(n_k) a_k X^{n_q-n_k}$ et $g_{r-q}(n_k) = \prod_{i=0}^{r-q-1} (n_{r-i}-n_k)$ donc

$$F_{r-q}(X) = X^p Q(\frac{1}{X}).$$

c. Raisonnons par l'absurde : soit $j \in \{0,\dots,r-q\}$ et supposons que F_j a au moins $n_{r-j}-n_q+1$ zéros de module strictement inférieur à

$$R_j = \left(R(p,r) \prod_{\substack{k\in\{0,\dots,p-1\}\\ i\in\{q+1,\dots,r-j\}}} \frac{n_i+k}{n_i-k}\right)^{-1}.$$

On a $deg(F_j) = n_{r-j}$ car les complexes a_k sont non nuls et par le 2., on sait que F_j' a au moins $n_{r-j}-n_q$ zéros de module strictement inférieur à

$$R_j \prod_{k=0}^{n_q-1} \frac{n_{r-j}+k}{n_{r-j}-k} = R_{j+1}.$$

Par définition $X^{n_{r-j}-n_{r-j-1}-1}F_{j+1} = F_j'$ et vu la formule obtenue pour les F_j, on constate que si 0 est zéro de F_j' alors $n_{r-j}-n_{r-j-1}-1 = 0$ et $F_{j+1} = F_j'$. On en déduit que les zéros de F_{j+1} sont exactement les zéros de F_j'. De plus, la suite (n_k) est strictement croissante donc $n_{r-j} \geq n_{r-j-1}+1$ et F_{j+1} a au moins $n_{r-j-1}-n_q+1$ zéros de module strictement inférieur à R_{j+1}.
En réitérant ce procédé, on trouve que F_{r-q} a au moins 1 zéro de module inférieur à R_{r-q}. Mais $R_{r-q} = 1/R(p,r)$ et d'après le a. et le b., tous les zéros de F_{r-q} sont de module supérieur à $1/R(p,r)$ donc ceci est contradictoire.

On a $F_0(X) = X^{n_r} P_r(\frac{1}{X})$ donc P_r a au plus $n_r - n_q$ zéros de module strictement supérieur à $1/R_0$ et comme $deg(P_r) = n_r$ alors P_r a au moins p zéros de module inférieur ou égal à

$$1/R_0 = R(p,r) \prod_{\substack{k\in\{0,\dots,p-1\}\\ i\in\{q+1,\dots,r\}}} \frac{n_i + k}{n_i - k}.$$

d. Pour tout $p = n_q$, on va montrer que f admet au moins p zéros et comme la suite (n_k) est un suite d'entiers strictement croissante, cela prouvera que f admet une infinité de zéros.

Soit $p = n_q$ fixé, R le plus grand des modules des zéros de P_q. On vient de voir au c. que pour tout $r > q$, P_r admet au moins p zéros $z_1^r, \dots, z_p^r$ de module inférieur ou égal à

$$R \cdot 2^p \prod_{j=q+1}^{r} \frac{1}{1 - \frac{n_q}{n_j}} \prod_{\substack{k\in\{0,\dots,p-1\}\\ i\in\{q+1,\dots,r\}}} \frac{1 + \frac{k}{n_i}}{1 - \frac{k}{n_i}}.$$

La convergence de la série $\sum \frac{1}{n_k}$ assure que pour tout $k = 0, \dots, p$, le produit infini $\prod_{i=q+1}^{\infty} (1 + \frac{k}{n_i})$ est convergent, ainsi que $\prod_{i=q+1}^{\infty} (1 - \frac{k}{n_i})$. On en déduit que :

$$\exists\, M \in \mathbb{R}_+^\star, \forall\, r > q, \exists\, z_1^r, \dots, z_p^r \text{ tels que } P_r(z_i^r) = 0 \text{ et } |z_i^r| \leq M.$$

Comme les suites $(z_i^r)_{r\geq q+1}$ sont contenues dans le compact $D(0,M)$ alors par un procédé d'extraction diagonale, on peut supposer que ces p suites sont convergentes vers z_i. La série entière f a un rayon de convergence infini donc P_r converge uniformément vers f sur $D(0,M)$ et de la même manière qu'au A.II.2.b., on conclut que pour tout $i = 1, \dots, p$, f s'annule en z_i.

4. Le théorème de Biernacki.
On pose $f(z) = g(z) - y$ et f vérifie évidemment les hypothèse du 4. donc f admet une infinité de zéros et l'équation $g(z) = y$ admet une infinité de solutions dans $\mathbb{C}$.

3.3 Commentaires

Ce problème est typique d'une épreuve de mathématiques générales à l'agrégation. On y utilise des techniques d'algèbre, d'analyse et de géométrie. Le début du problème peut être considéré comme du cours sur la localisation des zéros des polynômes, la géométrie de la sphère de Riemann ainsi que les homographies. L'étude d'une action de groupe de $\mathrm{GL}_2(\mathbb{C})$ sur $\mathbb{C}_n[X]$ permet d'établir le théorème de Grace sur la localisation des zéros dans la sphère de Riemann d'un polynôme. Enfin, la dernière partie demande de bien maîtriser les différents outils introduits dans les parties précédentes pour démontrer le théorème de Biernacki :
pour toute série entière lacunaire g de rayon de convergence infini, l'équation $g(z) = y$ admet une infinité de solutions dans $\mathbb{C}$.

Chapitre 4

Session de 1992

4.1 Sujet

4.2 Correction

I. L'espace vectoriel $H_0(A)$

A. *Préliminaires*

1. L'application T est clairement linéaire. Pour tous $a, a' \in A^2, aa' - a'a \in [A, A]$ donc $T(aa' - a'a) = 0$ par définition de T. D'où $T(aa') - T(a'a) = 0$, donc $T(aa') = T(a'a)$: T est une trace.

2. On a $[A, A] \subset \ker \tau$ car :

$$\tau\big(\sum_{i=1}^{n} \lambda_i(a_i a_i' - a_i' a_i)\big) = \sum_{i=1}^{n} \lambda_i(\tau(a_i a_i') - \tau(a_i' a_i)) = 0.$$

On en déduit que τ se factorise à travers $A/[A, A] = H_0(A)$. Précisons le raisonnement, et pour cela partons de $\alpha \in H_0(A)$. Prenons un représentant a de α (i.e. $T(a) = \alpha$) et posons $\overline{\tau}(\alpha) = \tau(a)$. Cela définit bien $\overline{\tau}$: en effet si $b \in A$ est un autre représentant de α (i.e. $T(b) = \alpha$) on a $a - b \in [A, A]$ donc $0 = \tau(a - b) = \tau(a) - \tau(b)$. On a fait ce qu'il fallait pour que $\overline{\tau} \circ T = \tau$. Il est clair qu'alors $\overline{\tau}$ est linéaire car T est linéaire surjective et τ est linéaire. Enfin l'unicité de $\overline{\tau}$ est une conséquence triviale de la surjectivité de T ; soit en effet $\alpha \in H_0(A)$ et a un de ses représentants : $\overline{\tau}(\alpha) = \tau(a)$ donc $\overline{\tau}(\alpha)$ est uniquement déterminé.
Soit

$$\begin{array}{rccc} \varphi : L(H_0(A), V) & \to & T(A, V) \\ t & \mapsto & t \circ T. \end{array}$$

A priori φ est à valeurs dans $L(A, V)$ mais si $a, a' \in A$:

$$t \circ T(aa') - t \circ T(a'a) = t \circ T(aa' - a'a) = t \circ T([a, a']) = t \circ T(0) = 0,$$

donc $t \circ T(aa') = t \circ T(a'a)$ et $t \circ T$ est une trace : $t \circ T \in T(A, V)$.
L'application φ est linéaire. L'existence de la factorisation précédente par $\overline{\tau}$ assure sa surjectivité et l'unicité de cette factorisation assure son injectivité : φ est un isomorphisme.

3.a. On note T_A et T_B les projections canoniques sur $H_0(A)$ et $H_0(B)$. Puisque f est un morphisme d'algèbres il est facile de voir que $f([A, A]) \subset [B, B]$. Or $[B, B] = \ker T_B$ donc $[A, A] \subset \ker(T_B \circ f)$: d'après 2., l'application linéaire $T_B \circ f$ se factorise à travers le quotient $A/[A, A]$ qui est $H_0(A)$.

L'application linéaire quotient $H_0(f)$ de $H_0(A)$ vers $H_0(B)$ ainsi obtenue vérifie la relation $H_0(f) \circ T_A = T_B \circ f$. Compte tenu de la surjectivité de T_A cette dernière égalité détermine $H_0(f)$ de façon unique.

3.b. On est dans la situation de la question précèdente avec $B = A$. Soit $\alpha \in H_0(A)$ et a un représentant de α dans A. Comme T est une trace, $T(uau^{-1}) = T(au^{-1}u) = T(a)$ et

$$\begin{array}{rcl} (H_0(f))(\alpha) & = & (H_0(f))(T(a)) \\ & = & T \circ f(a) \\ & = & T(uau^{-1}) \\ & = & T(a) \\ & = & \alpha. \end{array}$$

Donc $H_0(f) = Id_{H_0(A)}$.

B. *Les algèbres de matrices*

1. L'application $T \circ Tr$ est bien définie de $M_n(A)$ vers $H_0(A)$ et est linéaire comme composée d'applications linéaires. Soient M et $N \in M_n(A)$:

$$\begin{aligned}
T\circ Tr(MN) - T\circ Tr(NM) &= T\circ Tr(MN-NM)\\
&= T\Big(\sum_{j=1}^{n}(MN-NM)_{j,j}\Big)\\
&= T\Big(\sum_{j=1}^{n}\sum_{i=1}^{n} m_{j,i}n_{i,j} - \sum_{j=1}^{n}\sum_{i=1}^{n} n_{j,i}m_{i,j}\Big)\\
&= T\Big(\sum_{j=1}^{n}\sum_{i=1}^{n} m_{j,i}n_{i,j} - \sum_{i'=1}^{n}\sum_{j'=1}^{n} n_{i',j'}m_{j',i'}\Big)\\
&= T\Big(\sum_{j=1}^{n}\sum_{i=1}^{n} m_{j,i}n_{i,j} - \sum_{i=1}^{n}\sum_{j=1}^{n} n_{i,j}m_{j,i}\Big)\\
&= T\Big(\sum_{i,j=1}^{n}[m_{j,i},n_{i,j}]\Big)\\
&= 0 \quad (\text{car } \sum_{i,j=1}^{n}[m_{j,i},n_{i,j}] \in [A,A]).
\end{aligned}$$

Donc $T \circ Tr$ est bien une trace de $M_n(A)$ vers $H_0(A)$.

2.a. On a :

$$[E_{ij}(a), E_{kl}(b)] = E_{ij}(a)E_{kl}(b) - E_{kl}(b)E_{ij}(a) = \delta_{jk}E_{il}(ab) - \delta_{il}E_{kj}(ba).$$

2.b. Faisons $l = i, j = k = 1, b = 1$ et utilisons alors le calcul précédent. Il vient :

$$[E_{i1}(a), E_{1i}(1)] = F_i(a).$$

2.c. Soit $m \in M_n(A)$. Posons :

$$a = \sum_{1\le i\neq j\le n} E_{ij}(m_{i,j}) + \sum_{2\le i\le n} F_i(m_{ii}) + E_{11}(Tr(m)).$$

Soient $1 \le k, l \le n$:

Si $k \neq l$ alors $a_{kl} = m_{kl}$.

Si $k = l$ on distingue deux cas : si $k \neq 1$, $a_{kl} = m_{kl}$, et si $k = 1$, $a_{11} = -\sum_{k\neq 1} m_{kk} + Tr(m) = m_{11}$.

Donc $a = m$ et on a démontré l'existence de l'écriture demandée.

Enfin on sait que si $D_n = \{m \in M_n(A)\ ;\ m_{ij} = 0 \text{ si } i \neq j\}$ et si $C_n = \{m \in M_n(A)\ ;\ m_{ij} = 0 \text{ si i = j}\}$, on a $M_n(A) = C_n \bigoplus D_n$. Comme il est clair que $E_{ij}(1)_{i\neq j}$ est une base du $A-$module C_n (donc à fortiori une famille libre sur

k) et que $E_{11}(1) \cup \{F_i(1)\}_{i\neq 1}$ est une $A-$base de D_n (donc une famille libre sur k) on a l'unicité de l'écriture demandée.

2.d. Soit $m \in M'_n(A)$: on a $Tr(m) \in \ker T$ i.e. $Tr(m) \in [A, A]$.

Si $i \neq j$, $E_{ij}(m_{ij}) = [E_{i1}(m_{ij}), E_{1j}(1)]$ d'après a.. En particulier $E_{ij}(m_{ij}) \in [M_n(A), M_n(A)]$.

D'après b., $F_i(m_{ii}) \in [M_n(A), M_n(A)]$.

$Tr(m) \in [A, A]$ donc $Tr(m)$ peut s'écrire sous la forme $\sum \lambda_i [a_i, a_{i'}]$. Alors $E_{11}(Tr(m)) = \sum \lambda_i E_{11}([a_i, a_{i'}])$. Mais le a. prouve que :

$$E_{11}([a_i, a_{i'}]) = [E_{11}(a_i), E_{11}(a_{i'})].$$

On en déduit facilement que $E_{11}(Tr(m)) \in [M_n(A), M_n(A)]$.

Compte tenu de la décomposition de m obtenue au c. tout ceci assure que $m \in [M_n(A), M_n(A)]$. On a donc prouvé que $M'_n(A) \subset [M_n(A), M_n(A)]$. Enfin $M'_n(A)$ étant défini comme un noyau, c'est un sev de $M_n(A)$, que l'on peut voir aussi comme un sev de $[M_n(A), M_n(A)]$.

2.e. D'après a., $T \circ Tr$ est une trace donc en appliquant A.2. on sait que $T \circ Tr = \overline{T \circ Tr} \circ T_{M_n(A)}$ (cette notation ayant un sens évident).

Les applications T et Tr sont surjectives donc $T \circ Tr$ l'est aussi et cette factorisation prouve que $\overline{T \circ Tr}$ l'est également.

Soit $\mu \in \ker \overline{T \circ Tr}$ et $m \in M_n(A)$ un représentant de μ : $T_{M_n(A)}(m) = \mu$. Il vient $T \circ Tr(m) = \overline{T \circ Tr} \circ T_{M_n(A)}(m) = \overline{T \circ Tr}(\mu) = 0$ donc $m \in M'_n(A)$ et d'après d., $m \in [M_n(A), M_n(A)]$. On en déduit que $\mu = T_{M_n(A)}(m) = 0$ et cela prouve l'injectivité de $\overline{T \circ Tr}$.

Finalement il s'agit bien d'un isomorphisme.

C. *L'algèbre d'un groupe fini*

1. Posons $\alpha \in k[G]$ définie par $\alpha = \sum_{g\in G} f(g)\chi_g$ (somme finie). Pour tout $h \in G$ on a :

$$\begin{aligned} \alpha(h) &= \sum_{g\in G} f(g)\chi_g(h) \\ &= f(h)\chi_h(h) + \sum_{g\neq h} f(g)\chi_g(h) \\ &= f(h)1 + 0 \\ &= f(h), \end{aligned}$$

donc $\alpha = f$. Ceci prouve que la famille $\{\chi_g\}_{g\in G}$ est une partie génératrice de l'espace vectoriel $k[G]$.

Supposons maintenant qu'on ait des $\lambda_g \in k$ tels que : $\sum_{g\in G} \lambda_g \chi_g = 0_{k[G]}$. Prenons $h \in G$ quelconque et appliquons lui cette relation fonctionnelle : il vient exactement $\lambda_h = 0$. Comme h est choisi quelconque, la famille $\{\chi_g\}_{g\in G}$ est une partie libre de l'espace vectoriel $k[G]$. C'est finalement une base.

2. Soit $t \in G$: $\chi_g\chi_{g'}(t) = \sum_{h\in G} \chi_g(h)\chi_{g'}(h^{-1}t)$. Si $h = g$ et $h^{-1}t = g'$ alors $\chi_g(h)\chi_{g'}(h^{-1}t) = 1$ et sinon $\chi_g(h)\chi_{g'}(h^{-1}t) = 0$. Donc quand $t = gg'$, $\chi_g(h)\chi_{g'}(h^{-1}t) = 1$ (si $h = g$) ou 0 (si $h \neq g$) et quand $t \neq gg'$ on a

$\chi_g(h)\chi_{g'}(h^{-1}t) = 0$ quel que soit h. Finalement $\chi_g\chi_{g'}(t) = 1$ si $t = gg'$ et 0 sinon :

$(*)$ $\quad \chi_g\chi_{g'} = \chi_{gg'}$.

La bilinéarité de ce produit de convolution est évidente. On va vérifier son associativité sur les éléments de la base :

$$(\chi_g\chi_{g'})\chi_{g''} = \chi_{gg'}\chi_{g''} = \chi_{(gg')g''} = \chi_{g(g'g'')} = \chi_g\chi_{g'g''} = \chi_g(\chi_{g'}\chi_{g''})$$

(en utilisant la relation que nous venons de démontrer et l' associativité dans G). On a ainsi muni $k[G]$ d'une structure d'algèbre. Il est évident que χ_e en est l'unité (car $\chi_e\chi_g = \chi_{eg} = \chi_g$ et de même $\chi_g\chi_e = \chi_{ge} = \chi_g$).

3. L'application T_C est clairement linéaire. Soient $f, f' \in k[G]$:

$$\begin{aligned} T_C(ff') &= \sum_{g\in C} ff'(g) \\ &= \sum_{g\in C}\sum_{h\in G} f(h)f'(h^{-1}g). \\ T_C(f'f) &= \sum_{g\in C}\sum_{h\in G} f'(h)f(h^{-1}g) \\ &= \sum_{g\in C}(\sum_{h\in G} f(h^{-1}g)f'(h)) \\ &= \sum_{g\in C}(\sum_{t\in G} f(t)f'(gt^{-1})) \text{ (avec } t = h^{-1}g) \end{aligned}$$

Donc $T_C(ff') - T_C(f'f) = \sum_{h\in G} f(h)(\sum_{g\in C} f'(h^{-1}g) - f'(gh^{-1}))$ ou encore :

$$T_C(ff') - T_C(f'f) = \sum_{h\in G} f(h)(\sum_{g\in C} f'(h^{-1}g) - \sum_{g\in C} f'(gh^{-1})).$$

Fixons $h \in G$. Pour tout $g \in C$ il existe un unique $g' \in C$ tel que $h^{-1}gh = g'$ c'est-à-dire $h^{-1}g = g'h^{-1}$. Posons $g' = \varphi(g)$: φ définit une application de C dans C.
Si $\varphi(g_1) = \varphi(g_2)$ alors $h^{-1}g_1 = \varphi(g_1)h = \varphi(g_2)h = h^{-1}g_2$ donc $g_1 = g_2$: φ est injective. C étant finie, φ est bijective. Donc :

$$\sum_{g'\in C} f'(g'h^{-1}) = \sum_{g\in C} f'(\varphi(g)h^{-1})) = \sum_{g\in C} f'(h^{-1}g).$$

En injectant cette égalité dans le calcul précédent on obtient enfin que $T_C(ff') - T_C(f'f) = 0$ et donc T_C est une trace.

4.a. Soit $\alpha \in (k[G])^*$ (espace dual de $k[G]$). Pour tout $g \in G$ posons $a(g) = \alpha(\chi_g)$. Ceci définit bien un élément a de $k[G]$. Pour tout $f \in k[G]$ on sait d'après 1. que $f = \sum_{g\in G} f(g)\chi_g$.
On a alors $\alpha(\sum_{g\in G} f(g)\chi_g) = \sum_{g\in G} f(g)\alpha(\chi_g) = \sum_{g\in G} a(g)f(g)$.

4.b. En particulier une trace de $k[G]$ à valeurs dans k est une forme linéaire sur $k[G]$. Donc si α est une telle trace, il existe $a \in k[G]$ tel que pour tout $f \in k[G]$ on ait $\alpha(f) = \sum_{g\in G} a(g)f(g)$ (en invoquant la question précédente a.).

Considérons g_1 et g_2 appartenant à une même classe de conjugaison : il existe $h_0 \in G$ tel que $g_1 = h_0 g_2 h_0^{-1}$. On a :

$$\begin{aligned} a(g_1) &= \alpha(\chi_{g_1}) = \alpha(\chi_{h_0 g_2 h_0^{-1}}) \\ &= \alpha(\chi_{h_0}\chi_{g_2}\chi_{h_0^{-1}}) \text{ (d'après } * \\ &= \alpha(\chi_{h_0^{-1}}\chi_{h_0}\chi_{g_2}) \text{ car } \alpha \text{ est une trace} \\ &= \alpha(\chi_{g_2}) \text{ (d'après } * \\ &= a(g_2). \end{aligned}$$

Donc en fait si C est une classe de conjugaison donnée il existe $a_C \in k$ tel que pour tout $g \in C$ on ait $a(g) = a_C$. On a alors pour tout $f \in k[G]$:

$$\begin{aligned} \alpha(f) &= \sum_{g\in G} a(g)f(g) \\ &= \sum_{C\in\mathcal{C}} \sum_{g\in C} a(g)f(g) \text{ (la première somme porte sur l'ensemble } \mathcal{C} \text{ des} \\ &\quad \text{classes de conjugaison car celles} - \text{ci partitionnent } G) \\ &= \sum_{C\in\mathcal{C}} \sum_{g\in C} a_C f(g) \\ &= \sum_{C\in\mathcal{C}} a_C \sum_{g\in C} f(g) \\ &= \sum_{C\in\mathcal{C}} a_C T_C(f), \end{aligned}$$

ce qui prouve le résultat.

5. Par le 3., $\{T_C\}_{C\in\mathcal{C}} \subset T(k[G],k)$ et le 4.b. assure que cette famille est génératrice de $T(k[G],k)$.

Supposons que $\sum_C \lambda_C T_C = 0_{T(k[G],k)}$. Fixons une classe de conjugaison C_0 et f la fonction valant 1 sur C_0 et 0 ailleurs. On a $(\sum_C \lambda_C T_C)(f) = 0$, donc $\sum_C \lambda_C T_C(f) = 0$, soit $\lambda_{C_0}\text{card}(C_0) = 0$, et finalement $\lambda_{C_0} = 0$. Comme C_0 était choisie quelconque cela prouve que la famille est libre : elle forme bien une base de $T(k[G],k)$.

On applique le résultat de la question A.2. avec $A = k[G]$ et $V = k$. La situation est la suivante :

$$\begin{aligned} \varphi \quad : T(k[G],k) &\to (H_0(k[G]))^* \\ \tau = \overline{\tau}\circ T &\mapsto \overline{\tau}. \end{aligned}$$

Il s'agit d'un isomorphisme. Comme il transforme la famille des T_C, qui est une base de $T(k[G],k)$, en la famille des $\overline{T_C}$, cette dernière est à son tour une base de $(H_0(k[G]))^*$.

6. Pour un espace vectoriel de dimension finie, on sait que : $\dim E = \dim E^*$. Donc $\dim H_0(k[S_4]) = \dim(H_0(k[S_4]))^*$. Mais $\dim(H_0(k[S_4]))^*$ est le nombre de classes de conjugaison de S_4 d'après la question 5.. Il y en a 5 : les 4-cycles, les 3-cycles, les produits de deux transpositions à supports disjoints, les transpositions, l'identité. Donc finalement $\dim H_0(k[S_4]) = 5$.

II. Indécomposabilité de $\mathbb{Z}[G]$

A. *Idempotents*

1.a. $(e+f)^2 = (e+f)(e+f) = e^2 + ef + fe + f^2 = e + 0 + 0 + f = e + f$ donc $e + f \in P(A)$.

1.b. $(1-e)^2 = 1 - e - e + e^2 = 1 - e - e + e = 1 - e$ donc $1 - e \in P(A)$.

$e(1-e) = e - e^2 = e - e = 0$ et $(1-e)e = e - e^2 = e - e = 0$ donc e et $1-e$ sont orthogonaux.

2. Soit $e \in P(A)$. Alors d'après 1. $1 - e$ est idempotent et e et $1 - e$ sont orthogonaux donc d'après $(R3)$ on a : $r(e + 1 - e) = r(e) + r(1 - e)$.
Mais $r(e + 1 - e) = r(1) = 1$ (d'après $(R1)$) donc $r(e) + r(1 - e) = 1$.
Or $r(e) \in \mathbb{N}$ et $r(1 - e) \in \mathbb{N}$ donc $r(e) = 0$ ou $r(1 - e) = 0$. Si $r(e) = 0$ alors d'après $(R2)$ $e = 0$. Sinon $r(1 - e) = 0$ et pour la même raison $1 - e = 0$ donc $e = 1$.

3. Supposons que A ne soit pas indécomposable. Alors, par définition, il existe deux anneaux A_1 et A_2 non triviaux et φ un isomorphisme d'anneaux de A sur $A_1 \times A_2$. Soit ψ l'isomorphisme réciproque et posons $\alpha = (1_{A_1}, 0_{A_2})$.
$0_{A_1 \times A_2} = (0_{A_1}, 0_{A_2})$ donc $\alpha \neq 0_{A_1 \times A_2}$ ce qui force $\psi(\alpha) \neq 0_A$.
$1_{A_1 \times A_2} = (1_{A_1}, 1_{A_2})$ donc $\alpha \neq 1_{A_1 \times A_2}$ ce qui force $\psi(\alpha) \neq 1_A$.
Mais $(1_{A_1}, 0_{A_2})(1_{A_1}, 0_{A_2}) = (1_{A_1}1_{A_1}, 0_{A_2}0_{A_2}) = (1_{A_1}, 0_{A_2})$ donc α est idempotent. On a alors $\psi(\alpha)^2 = \psi(\alpha^2) = \psi(\alpha)$ ce qui prouve que $\psi(\alpha)$ est un idempotent de A. C'est absurde car les seuls idempotents de A sont 0_A et 1_A.

4. Si $e \in M_n(k)$ est idempotente alors e annule le polynome $X^2 - X = X(X-1)$ qui est scindé à racines simples sur k. Donc e est diagonalisable et ses seules valeurs propres possibles sont les racines de ce polynôme : 0 et 1. Il existe $P \in GL_n(k)$ telle que $P^{-1}eP = \mathrm{diag}(1, \ldots, 1, 0, \ldots, 0)$. Si m est le nombre de 1 dans cette matrice diagonale, on a $rg(e)1 = rg(P^{-1}eP)1 = m1$ et

$$Tr(e) = Tr(P^{-1}eP) = \underbrace{1 + \ldots + 1}_{m \text{ termes}} = m1$$

donc on a l'identité voulue.

B. *Indécomposabilité*

1. $\mathbb{Z}[G]$ est clairement un sous-groupe additif de $\mathbb{Q}[G]$. Il contient l'unité χ_e. Il est clairement stable par multiplication (car si a et b sont des entiers $a\chi_g b\chi_{g'} = ab\chi_{gg'}$: ab est un entier et on conclut par bilinéarité). Comme $\mathbb{Q}[G]$ est un anneau, cela prouve que $\mathbb{Z}[G]$ en est un sous-anneau.

2. Soit $x \in \mathbb{Z}[G]$. Alors x s'écrit $\sum_{h \in G} n(h)\chi_h$, les $n(h)$ étant entiers.

Pour tout $g \in G$ on a :

$$\begin{aligned}
\tilde{x}(\chi_g) &= x\chi_g \\
&= (\sum_{h \in G} n(h)\chi_h)\chi_g \\
&= n(e)\chi_g + \sum_{h \neq e} n(h)\chi_{hg} \\
&= n(e)\chi_g + \sum_{u \neq g} n(ug^{-1})\chi_u.
\end{aligned}$$

Rappelons que les χ_g forment une base de $\mathbb{Q}[G]$. Ce petit calcul justifie donc que $Tr(\tilde{x}) = \sum_{g\in G} n(e) = Nn(e)$. Mais par définition $n(e) = \tau(x)$ donc :

$$Tr(\tilde{x}) = N\tau(x).$$

3. Soit $x \in P(\mathbb{Z}[G])$ et $\tilde{x}$ l'endomorphisme correspondant de $\mathbb{Q}[G]$. Si $y \in \mathbb{Q}[G]$ on a

$$\tilde{x} \circ \tilde{x}(y) = \tilde{x}(xy) = x(xy) = x^2y = xy = \tilde{x}(y).$$

Ceci prouve que $\tilde{x}$ est un idempotent de l'anneau $L(\mathbb{Q}[G])$. Comme $\mathbb{Q}[G]$ est fini de dimension N on peut appliquer le A.4. en confondant $\tilde{x}$ avec sa matrice représentative (élément de $M_n(\mathbb{Q})$) dans la base des χ_g. On obtient $\mathrm{rg}(\tilde{x}) = Tr(\tilde{x})$. D'après 2., $N\tau(x) = \mathrm{rg}(\tilde{x})$ ce qui assure $\tau(x) \geq 0$. Or τ est à valeurs dans $\mathbb{Z}$ donc sa restriction à $P(\mathbb{Z}[G])$ est à valeurs dans $\mathbb{N}$.

Par définition $\tau(\chi_e) = 1$ et $\tau(0) = 0$: $(R1)$ est vérifiée.

Si $x \in P(\mathbb{Z}[G])$ est non nul alors on a aussi $\tilde{x} \neq 0$ car $\tilde{x}(\chi_e) = x$. Dans ce cas $rg(\tilde{x}) > 0$ et donc $\tau(x) > 0$: $(R2)$ est vérifiée.

$\tau(x_1 + x_2) = n_1(e) + n_2(e) = \tau(x_1) + \tau(x_2)$: $(R3)$ est vérifiée.

On sait alors en utilisant A.2. que les seuls idempotents de $\mathbb{Z}[G]$ sont 0 et $1(= \chi_e)$. On peut donc invoquer A.3. pour enfin obtenir l'indécomposabilité de $\mathbb{Z}[G]$.

III. L'espace vectoriel $H_1(A)$

1. Soit p la projection canonique $X_A \to C(A) = X_A/Y_A$. Soient $\overline{x} \in C(A)$ et $x \in X_A$ un représentant de $\overline{x}$: $p(x) = \overline{x}$.

On a $x = \sum_{(a,b)\in A\times A} \lambda_{(a,b)} X_{(a,b)}$ avec une famille de $\lambda_{(a,b)}$ nulle sauf pour un nombre fini de termes.

$$\begin{aligned}
\overline{x} &= p(x) \\
&= p\Big(\sum_{(a,b)\in A\times A} \lambda_{(a,b)} X_{(a,b)}\Big) \\
&= p\Big(\sum_{(a,b)\in A\times A} \lambda_{(a,b)} X_{(a,b)}\Big) + p\Big(\sum_{(a,b)\in A\times A, \lambda_{(a,b)}\neq 0} \gamma(a,b,\lambda_{(a,b)})\Big) \\
&\quad (\text{car } \gamma(a,b,\lambda_{(a,b)}) \in Y_A) \\
&= p\Big(\sum_{(a,b)\in A\times A, \lambda_{(a,b)}\neq 0} \lambda_{(a,b)} X_{(a,b)} + \gamma(a,b,\lambda_{(a,b)})\Big) \\
&= p\Big(\sum_{(a,b)\in A\times A, \lambda_{(a,b)}\neq 0} X(\lambda_{(a,b)} a, b)\Big) \\
&= \sum_{(a,b)\in A\times A, \lambda_{(a,b)}\neq 0} p(X(\lambda_{(a,b)} a, b)) \\
&= \sum_{(a,b)\in A\times A, \lambda_{(a,b)}\neq 0} [(\lambda_{(a,b)} a) \wedge b].
\end{aligned}$$

On a donc exprimé tout élément de $C(A)$ sous la forme désirée.

2. Pour tout $(a,b) \in A \times A$ on a $\alpha(a,b) = X_{(a,b)} + X_{(b,a)} \in Y_A$. Donc :

$$0 = p(\alpha(a,b)) = p(X_{(a,b)} + X_{(b,a)}) = p(X_{(a,b)}) + p(X_{(b,a)}) = a \wedge b + b \wedge a,$$

ce qui prouve que $a \wedge b = -b \wedge a$.

De même $\beta(a,b,c) = X(ab,c) - X(a,bc) + X(ca,b) \in Y_A$ et en projetant par p, linéaire, sur X_A/Y_A, il vient :

$$0 = ab \wedge c - a \wedge bc + ca \wedge b,$$

soit la seconde identité cherchée en changeant de membre.

Enfin faisons $b = c = 1$ dans cette dernière identité : il vient $a \wedge 1 = 0$, et la première force alors aussi $1 \wedge a = 0$.

3. La famille $\{X_{(a,b)}\}_{(a,b)\in A\times A}$ constitue une base de F_A, donc pour définir une application linéaire de F_A dans V il suffit d'imposer arbitrairement des valeurs sur ses éléments. Ainsi on appelle $\tilde{f}$ l'application linéaire de F_A dans V définie par $\tilde{f}(X(a,b)) = f(a,b)$ pour tout $(a,b) \in A \times A$. Si $a,b,c \in A$ et $\lambda \in k$ on a :

$\tilde{f}(\alpha(a,b)) = \tilde{f}(X(a,b) + X(b,a)) = f(a,b) + f(b,a) = 0$.

$\tilde{f}(\beta(a,b,c)) = 0$ car $f(a,bc) = f(ab,c) + f(ca,b)$.

$\tilde{f}(\gamma(a,b,\lambda)) = \tilde{f}(\delta(a,b,c)) = 0$ car f est bilinéaire.

On a alors $Y_A \subset \ker \tilde{f}$ et d'après un théorème de factorisation, il existe $\hat{f} \in L(X_A/Y_A, V)$ (c'est-à-dire $L(C(A),V)$) tel que $\tilde{f} = \hat{f} \circ p$. En appliquant cette relation à $X(a,b)$ on obtient $\tilde{f}(X(a,b)) = \hat{f}(a \wedge b)$. Compte tenu de la définition de $\tilde{f}$ cela signifie que $f(a,b) = \hat{f}(a \wedge b)$. Enfin on sait depuis le 1. que les $a \wedge b$ engendrent l'espace vectoriel $C(A)$ donc cette dernière relation assure, par linéarité, l'unicité de $\hat{f}$.

4.a. On reprend les notations de la question 3. avec $V = A$ et f le crochet de A. Il est immédiat de constater que ce crochet de commutation est bien bilinéaire, antisymétrique, et satisfait à l'identité de Jacobi, comme l'application f dans cette question. On en applique donc le résultat en appelant θ_A l'application $\hat{f}$: θ_A répond à la question.

4.b. Il est clair, par définition de θ_A, que $\mathrm{im}\theta_A = [A,A]$. (Un argument rigoureux pour le montrer invoquerait bien sûr le 1. et le a.). Donc $\theta_A(C_A) = [A,A]$. Alors par définition de $H_0(A)$ on a $A/\theta_A(C_A) = H_0(A)$.

5.a. On a :

$$\begin{aligned} Tr'(E_{ij}(a), E_{kl}(b)) &= \sum_{\alpha,\beta=1}^{p} (E_{ij}(a))_{\alpha\beta} \wedge (E_{kl}(b))_{\beta\alpha} \\ &= a \wedge (E_{kl}(b))_{ji} \\ &= a \wedge (\delta_{kj}\delta_{li} b) \\ &= \delta_{kj}\delta_{li} a \wedge b. \end{aligned}$$

5.b. Il suffit d'appliquer le résultat de 3. avec V remplacé par $C(A)$, A remplacé par $M_p(A)$ et f remplacée par Tr'. Pour cela on constate d'abord que Tr' est bilinéaire (ce qui est une conséquence de la bilinéarité du produit

extérieur $\wedge$). Ensuite pour vérifier les hypothèses de la question 3. on développe $Tr'(m,n)$ par bilinéarité suivant les $E_{ij}(a)$ et enfin, compte tenu du calcul du a., on conclut à l'aide des deux premières relations obtenues au 2.

5.c. Montrons que $\theta_A \circ \widehat{Tr'} = Tr \circ \theta_{M_p(A)}$. Pour cela partons de $\alpha \in C(M_p(A))$. On sait depuis 1. que $\alpha = \sum_{\lambda\in\Lambda} m_\lambda \wedge n_\lambda$ où Λ est un ensemble fini. Ici $m_\lambda = \sum_{i,j=1}^{p} E_{ij}(m_{\lambda_{ij}})$ et $n_\lambda = \sum_{k,l=1}^{p} E_{kl}(n_{\lambda_{kl}})$. On a :

$$\begin{aligned}
(\theta_A \circ \widehat{Tr'})(\alpha) &= \theta_A(\widehat{Tr'}(\sum_{\lambda\in\Lambda} m_\lambda \wedge n_\lambda)) \\
&= \sum_{\lambda\in\Lambda} \theta_A(\widehat{Tr'}(m_\lambda \wedge n_\lambda)) \\
&= \sum_{\lambda\in\Lambda} \theta_A(Tr'(m_\lambda, n_\lambda)) \\
&= \sum_{\lambda\in\Lambda} \theta_A(\sum_{i,j=1}^{p} m_{\lambda_{ij}} \wedge n_{\lambda_{ji}}) \\
&= \sum_{\lambda\in\Lambda} \sum_{i,j=1}^{p} \theta_A(m_{\lambda_{ij}} \wedge n_{\lambda_{ji}}) \\
&= \sum_{\lambda\in\Lambda} \sum_{i,j=1}^{p} [m_{\lambda_{ij}}, n_{\lambda_{ji}}].
\end{aligned}$$

On a aussi :

$$\begin{aligned}
(Tr \circ \theta_{M_p(A)})(\alpha) &= Tr(\theta_{M_p(A)}(\sum_{\lambda\in\Lambda} m_\lambda \wedge n_\lambda)) \\
&= \sum_{\lambda\in\Lambda} Tr(\theta_{M_p(A)}(m_\lambda \wedge n_\lambda)) \\
&= \sum_{\lambda\in\Lambda} Tr([m_\lambda, n_\lambda]) \\
&= \sum_{\lambda\in\Lambda} Tr(m_\lambda n_\lambda - n_\lambda m_\lambda) \\
&= \sum_{\lambda\in\Lambda} (\sum_{i=1}^{p} (m_\lambda n_\lambda)_{ii} - (n_\lambda m_\lambda)_{ii}) \\
&= \sum_{\lambda\in\Lambda} (\sum_{i,j=1}^{p} m_{\lambda_{ij}} n_{\lambda_{ji}} - \sum_{i,j=1}^{p} n_{\lambda_{ij}} m_{\lambda_{ji}}) \\
&= \sum_{\lambda\in\Lambda} (\sum_{i,j=1}^{p} m_{\lambda_{ij}} n_{\lambda_{ji}} - \sum_{i,j=1}^{p} n_{\lambda_{ji}} m_{\lambda_{ij}}) \\
&= \sum_{\lambda\in\Lambda} (\sum_{i,j=1}^{p} [m_{\lambda_{ij}}, n_{\lambda_{ji}}]).
\end{aligned}$$

Donc on a $\theta_A \circ \widehat{Tr'}(\alpha) = Tr \circ \theta_{M_p(A)}(\alpha)$ ce qui assure le résultat voulu.

Soit maintenant $\alpha \in H_1(M_p(A)) = \ker \theta_{M_p(A)}$. Grâce à ce qui précède,

$$\theta_A \circ \widehat{Tr'}(\alpha) = Tr \circ \theta_{M_p(A)}(\alpha) = Tr(0) = 0,$$

donc $\widehat{Tr'}(\alpha) \in \ker \theta_A = H_1(A)$: Tr_1 est à valeurs dans $H_1(A)$.

5.d. Soit $\alpha \in H_1(A)$: $\alpha = \sum_{\lambda=1}^{n} a_\lambda \wedge b_\lambda$. D'après a., pour tout λ on a :

$$a_\lambda \wedge b_\lambda = Tr'(E_{11}(a_\lambda), E_{11}(b_\lambda)) = \widehat{Tr'}(E_{11}(a_\lambda) \wedge E_{11}(b_\lambda)).$$

Donc $\alpha = \sum_{\lambda=1}^{n} \widehat{Tr'}(E_{11}(a_\lambda) \wedge E_{11}(b_\lambda)) = \widehat{Tr'}(\sum_{\lambda=1}^{n} E_{11}(a_\lambda) \wedge E_{11}(b_\lambda))$.

On pose alors $\beta = \sum_{\lambda=1}^{n} E_{11}(a_\lambda) \wedge E_{11}(b_\lambda)$: on a $\alpha = \widehat{Tr'}(\beta)$.

$$\begin{aligned}
\theta_{M_p(A)}(\beta) &= \theta_{M_p(A)}(\sum_{\lambda=1}^{n} E_{11}(a_\lambda) \wedge E_{11}(b_\lambda)) \\
&= \sum_{\lambda=1}^{n} \theta_{M_p(A)}(E_{11}(a_\lambda) \wedge E_{11}(b_\lambda)) \\
&= \sum_{\lambda=1}^{n} [E_{11}(a_\lambda), E_{11}(b_\lambda)] \\
&= \sum_{\lambda=1}^{n} E_{11}([a_\lambda, b_\lambda]) \quad \text{(d'après I.B.2.a.)} \\
&= \sum_{\lambda=1}^{n} E_{11}(\theta_A(a_\lambda \wedge b_\lambda)) \\
&= E_{11}(\theta_A(\sum_{\lambda=1}^{n} a_\lambda \wedge b_\lambda)) \\
&= E_{11}(\theta_A(\alpha)) \\
&= E_{11}(0) \quad (\text{car } \alpha \in \mathrm{H_1(A)} = \ker \theta_\mathrm{A}) \\
&= 0.
\end{aligned}$$

Donc $\beta \in \ker \theta_{M_p(A)} = H_1(M_p(A))$ ce qui prouve que Tr_1 est surjective.

6.a. On pose $P = \sum_{n\in\mathbb{Z}} p_n t^n$ et $Q = \sum_{n\in\mathbb{Z}} q_n t^n$. On a alors :

$$P' = \sum_{n\in\mathbb{Z}} (n+1) p_{n+1} t^n \text{ et } Q' = \sum_{n\in\mathbb{Z}} (n+1) q_{n+1} t^n.$$

Par définition du produit dans l'algèbre $k[t, t^{-1}]$ il vient :

$$PQ = \sum_{n\in\mathbb{Z}} (\sum_{i+j=n} p_i q_j) t^n \text{ donc } (PQ)' = \sum_{n\in\mathbb{Z}} (n+1)(\sum_{i+j=n+1} p_i q_j) t^n.$$

Ensuite :

$$P'Q = \sum_{n\in\mathbb{Z}} (\sum_{i+j=n} (i+1) p_{i+1} q_j) t^n \text{ et } PQ' = \sum_{n\in\mathbb{Z}} (\sum_{i+j=n} p_i (j+1) q_{j+1}) t^n.$$

On fait les changements d'indices $k = i+1$ et $l = j+1$ dans ces deux dernières expressions :

$$P'Q = \sum_{n\in\mathbb{Z}} (\sum_{k+j=n+1} k p_k q_j) t^n \text{ et } PQ' = \sum_{n\in\mathbb{Z}} (\sum_{i+l=n+1} p_i l q_l) t^n.$$

Et en les additionnant on obtient :

$$\begin{aligned} P'Q + PQ' &= \sum_{n\in\mathbb{Z}}\Big(\sum_{k+j=n+1} kp_kq_j + \sum_{i+l=n+1} lp_iq_l\Big)t^n \\ &= \sum_{n\in\mathbb{Z}}\Big(\sum_{i+j=n+1} ip_iq_j + \sum_{i+j=n+1} jp_iq_j\Big)t^n \\ &= \sum_{n\in\mathbb{Z}}\Big(\sum_{i+j=n+1} (i+j)p_iq_j\Big)t^n \\ &= \sum_{n\in\mathbb{Z}}(n+1)\Big(\sum_{i+j=n+1} p_iq_j\Big)t^n \\ &= (PQ)'. \end{aligned}$$

Par ailleurs $res(P') = (n+1)p_{n+1}$ pour $n = -1$, donc $res(P') = 0$.

6.b. Encore une fois il suffit de vérifier que l'application de $k[t,t^{-1}]\times k[t,t^{-1}]$ dans k qui à (P,Q) associe $res(PQ')$ satisfait aux hypothèses de la question 3. (avec ici $A = k[t,t^{-1}]$ et $V = k$).

Il est immédiat de vérifier la bilinéarité de cette application.

De plus :

$$\begin{aligned} res(PQ') + res(QP') &= res(PQ' + P'Q) \\ &= res((PQ)') \quad (\text{d'après a.}) \\ &= 0 \quad (\text{toujours d'après a.}). \end{aligned}$$

$$\begin{aligned} res(P(QR)') &= res(P(QR' + Q'R)) \\ &= res(PQR') + res(PQ'R) \\ &= res((PQ)R') + res((RP)Q'). \end{aligned}$$

Donc les deux identités fixées au 3. sont bien démontrées dans ce cas et on obtient en appliquant le résultat de cette question l'existence de $\hat{f}$, que l'on note ici Res, et qui possède les caractéristiques requises.

6.c. Montrons par récurrence sur $n \in \mathbb{N}$ que pour tout $P \in k[t,t^{-1}]$ on a $P \wedge t^n = nPt^{n-1} \wedge t$.

Si $n = 0$ la propriété s'écrit $P \wedge 1 = 0$ ce que l'on a démontré au 2..

Supposons la propriété vérifiée au rang n et étudions le rang $n+1$. D'après l'identité de Jacobi (la seconde relation du 2.),

$$P \wedge t^{n+1} = P \wedge (t^n t) = Pt^n \wedge t + tP \wedge t^n.$$

Mais d'après l'hypothèse de récurrence au rang n appliquée à tP on a :

$$tP \wedge t^n = ntPt^{n-1} \wedge t = nPt^n \wedge t.$$

Donc il vient :

$$P \wedge t^{n+1} = Pt^n \wedge t + nPt^n \wedge t = (n+1)Pt^n \wedge t,$$

ce qui achève la récurrence.

Pour montrer la propriété sur $\mathbb{Z} \setminus \mathbb{N}$, on constate d'après l'identité de Jacobi que

$$0 = Pt^{-n} \wedge 1 = Pt^{-n} \wedge t^{-n}t^n = P \wedge t^{-n} + Pt^{-2n} \wedge t^n.$$

Comme $Pt^{-2n} \in k[t,t^{-1}]$, on sait alors que pour $n \geq 0$, $Pt^{-2n} \wedge t^n = nt^{-n-1}P \wedge t$ ce qui prouve que

$$P \wedge t^{-n} = -nt^{-n-1}P \wedge t.$$

On rappelle que le produit $\wedge$ est bilinéaire (en étudiant les classes de γ et δ on obtient la linéarité par rapport à la première variable, ce qui est suffisant par antisymétrie.) Posons $P = \sum_{n\in\mathbb{Z}} p_n t^n$ et $Q = \sum_{n\in\mathbb{Z}} q_n t^n$. Alors :

$$\begin{aligned}
P \wedge Q &= \sum_{n\in\mathbb{Z}} q_n P \wedge t^n \\
&= \sum_{n\in\mathbb{Z}} q_n nPt^{n-1} \wedge t \quad \text{(formule précédente)} \\
&= P(\sum_{n\in\mathbb{Z}} nq_n t^{n-1}) \wedge t \\
&= P(\sum_{n'\in\mathbb{Z}} (n'+1)q_{n'+1} t^n) \wedge t \\
&= PQ' \wedge t.
\end{aligned}$$

On a aussi $Q \wedge P = QP' \wedge t$. Comme $P \wedge Q = -Q \wedge P$ on a bien également $P \wedge Q = -QP' \wedge t$.

Enfin on a :

$$\begin{aligned}
PQ' \wedge t &= -QP' \wedge t \\
PQ' \wedge t + QP' \wedge t &= 0 \\
(PQ' + QP') \wedge t &= 0 \\
(PQ)' \wedge t &= 0.
\end{aligned}$$

En particulier si $Q = 1$ cela donne $P' \wedge t = 0$.

6.d. Il est clair que $k[t,t^{-1}]$ est une algèbre commutative donc $\theta_{k[t,t^{-1}]}$ est l'application nulle : $H_1(k[t,t^{-1}]) = C(k[t,t^{-1}])$.

$Res(t^{-1} \wedge t) = res(t^{-1}(t)') = res(t^{-1}) = 1$ donc Res est non nulle. Comme c'est une forme linéaire elle est nécessairement surjective.

Intéressons nous maintenant à son éventuelle injectivité ; pour cela on va d'abord démontrer le résultat suivant :
Pour tout $P \in k[t,t^{-1}]$, il existe $Q \in k[t,t^{-1}]$ tel que $P = (resP)t^{-1} + Q'$.
En effet si $P = \sum_{n\in\mathbb{Z}} p_n t^n$ il suffit de considérer $Q = \sum_{n\in\mathbb{Z}-\{-1\}} q_n t^n$ avec pour tout $n \neq -1$, $q_{n+1} = p_n(n+1)^{-1}$ (ce qui est licite car dans ce cas $n+1 \neq 0$ dans k, puisque k est de caractéristique nulle).

Maintenant si A et $B \in k[t,t^{-1}]$ on a $A \wedge B = AB' \wedge t$ d'après c.. Avec ce qui précède on sait donc qu'il existe $C \in k[t,t^{-1}]$ tel que :

$$A \wedge B = (res(AB'))t^{-1} + C') \wedge t = res(AB')t^{-1} \wedge t + C' \wedge t.$$

Mais encore d'après c., $C' \wedge t = 0$ donc finalement $A \wedge B = res(AB')t^{-1} \wedge t$.
D'après 1., pour tout $\alpha \in C(k[t,t^{-1}])$, $\alpha = \sum_{i=1}^{n} A_i \wedge B_i$ et il devient clair que $C(k[t,t^{-1}]) = \text{vect}(t^{-1} \wedge t)$. Ceci prouve que $H_1(k[t,t^{-1}]) = C(k[t,t^{-1}])$ est de dimension 1. En particulier puisque Res est non nulle, Res est injective.

En définitive on a bien montré que Res est un isomorphisme de $H_1(k[t,t^{-1}])$ sur k.

IV. Extensions

A. *Généralités*

1.a. Pour tous $(u,x),(v,y),(w,z) \in U \times E$ on a $< u,v > + < v,u >= 0$ d'après $(L1)$ et $\alpha(u,v)+\alpha(v,u)=0$ d'après $(C1)$ donc :

$$\begin{aligned}\{(u,x),(v,y)\}+\{(v,y),(u,x)\} &= (< u,v >, \alpha(u,v)) + (< v,u >, \alpha(v,u)) \\ &= (< u,v > + < v,u >, \alpha(u,v)+\alpha(v,u)) \\ &= (0,0) \\ &= 0_{U\times E}.\end{aligned}$$

Donc $\{\ ,\ \}$ vérifie $(L1)$.

$\{(u,x),\{(v,y),(w,z)\}\}+\{(v,y),\{(w,z),(u,x)\}\}+\{(w,z),\{(u,x),(v,y)\}\}$
$=\{(u,x),(< v,w >,\alpha(v,w))\}+\{(v,y),(< w,u >,\alpha(w,u))\}+\{(w,z),(< u,v >,\alpha(u,v))\}$
$=(< u,< v,w >>,\alpha(u,< v,w >)) + (< v,< w,u >>,\alpha(v,< w,u >))$
$+(< w,< u,v >>,\alpha(w,< u,v >))$
$=(< u,< v,w >> + < v,< w,u >> + < w,< u,v >>,$
$\alpha(u,< v,w >)+\alpha(v,< w,u >)+\alpha(w,< u,v >))$.
Or $< u,< v,w >> + < v,< w,u >> + < w,< u,v >>= 0$ d'après $(L2)$ et $\alpha(u,< v,w >)+\alpha(v,< w,u >)+\alpha(w,< u,v >)=0$ d'après $(C2)$ donc :
$\{(u,x),\{(v,y),(w,z)\}\} + \{(v,y),\{(w,z),(u,x)\}\} + \{(w,z),\{(u,x),(v,y)\}\} = (0,0) = 0_{U\times E}$. Donc $\{\ ,\ \}$ vérifie $(L2)$.

1.b. Clairement, p est linéaire. De plus si (u,x) et $(v,y) \in U \times E$ on a :

$$< p(u,x),p(v,y) >=< u,v >= p(< u,v >,\alpha(u,v)) = p\{(u,x),(v,y)\}.$$

Donc p est un ℓ-morphisme de $L(\alpha)$ sur L.

1.c. Supposons qu'il existe une application linéaire f de U dans E telle que pour tous $u,v \in U$ on ait $\alpha(u,v) = f(< u,v >)$. Posons alors :

$$\begin{aligned} s\ : U &\to U \times E \\ u &\mapsto (u, f(u)).\end{aligned}$$

Il est clair que s est linéaire. De plus pour tous $u,v \in U$ on a :

$$\begin{aligned}\{s(u),s(v)\} &= \{(u,f(u)),(v,f(v))\} \\ &= (< u,v >, \alpha(u,v)) \\ &= (< u,v >, f(< u,v >)) \\ &= s(< u,v >).\end{aligned}$$

Ceci prouve que s est un ℓ-morphisme de L dans $L(\alpha)$.
De plus pour tout $u \in U$, $p \circ s(u) = p(u,f(u)) = u$: $p \circ s = Id_U$.

Réciproquement supposons que s soit un ℓ-morphisme de L dans $L(\alpha)$ vérifiant $p \circ s = Id_U$. Si $u \in U$ posons $(v,x) = s(u)$. Comme $p \circ s(u) = u$ on a en fait $v = u$. On a donc montré que pour tout $u \in U$ il existait un unique $x \in E$ tel que $s(u) = (u,x)$. Notons alors :

$$\begin{aligned} g\ : U &\to E \\ u &\mapsto x.\end{aligned}$$

La linéarité de s entraîne celle de g de façon évidente.
Enfin s est un ℓ-morphisme donc pour tous $u, v \in U$ on a :

$$\{s(u), s(v)\} = s(< u, v >) = (< u, v >, g(< u, v >)).$$

Comme on a également :

$$\{s(u), s(v)\} = \{(u, g(u)), (v, g(v))\} = (< u, v >, \alpha(u, v)),$$

on obtient en identifiant $\alpha(u, v) = g(< u, v >)$, donc g est l'application f cherchée.

2.a. Pour tous $a, b \in A$,

$$[a, b] + [b, a] = (ab - ba) + (ba - ab) = 0,$$

donc [,] vérifie $(L1)$ (l'antisymétrie).
Pour tous $a, b, c \in A$, posons $J(a, b, c) = [a, [b, c]] + [b, [c, a]] + [c, [a, b]]$. On a :

$$\begin{aligned}
&J(a, b, c) = [a, bc - cb] + [b, ca - ac] + [c, ab - ba] \\
&= a(bc - cb) - (bc - cb)a + b(ca - ac) - (ca - ac)b + c(ab - ba) - (ab - ba)c \\
&= abc - acb - bca + cba + bca - bac - cab + acb + cab - cba - abc + bac \\
&= 0.
\end{aligned}$$

Donc [,] vérifie $(L2)$ (l'identité de Jacobi). Comme elle est clairement bilinéaire, c'est un crochet sur A.

2.b. Remarque : on utilisera librement les relations du III.2..
Pour tous $a, b \in A$ on a :

$$\alpha_\varphi(a, b) + \alpha_\varphi(b, a) = \varphi(a \wedge b) + \varphi(b \wedge a) = \varphi(a \wedge b + b \wedge a) = \varphi(0) = 0.$$

Donc α_φ vérifie $(C1)$.
Pour tous a, b, $c \in A$, posons

$$J_{\alpha_\varphi}(a, b, c) = \alpha_\varphi(a, [b, c]) + \alpha_\varphi(b, [c, a]) + \alpha_\varphi(c, [a, b]).$$

On a :

$$\begin{aligned}
J_{\alpha_\varphi}(a, b, c) &= \varphi(a \wedge [b, c]) + \varphi(b \wedge [c, a]) + \varphi(c \wedge [a, b]) \\
&= \varphi(a \wedge [b, c] + b \wedge [c, a] + c \wedge [a, b]) \\
&= \varphi(a \wedge (bc - cb) + b \wedge (ca - ac) + c \wedge (ab - ba)) \\
&= \varphi(a \wedge bc - a \wedge cb + b \wedge ca - b \wedge ac + c \wedge ab - c \wedge ba) \\
&= \varphi(a \wedge bc - a \wedge cb - ca \wedge b + ac \wedge b - ab \wedge c + ba \wedge c) \\
&= \varphi\big((a \wedge bc - (ab \wedge c + ca \wedge b)) + ((ac \wedge b + ba \wedge c) - a \wedge cb)\big) \\
&= 0.
\end{aligned}$$

Donc α_φ vérifie $(C2)$. De plus on a déjà dit que $\wedge$ était bilinéaire donc la linéarité de φ entraine la bilinéarité de α_φ : finalement α_φ est un cocycle.

2.c. D'après 1.c. $L(A)(\alpha_\varphi)$ est triviale si et seulement si il existe une application linéaire f de A dans E telle que $\alpha_\varphi(a, b) = f([a, b])$ pour tous $a, b \in A$. Cela peut s'écrire $\varphi(a \wedge b) = f([a, b])$.

Supposons qu'il existe une telle application f et considérons $\alpha \in H_1(A)$: $\alpha = \sum_{i=1}^{n} a_i \wedge b_i$ (toujours III.1.). On a :

$$\begin{aligned}
\varphi(\alpha) &= \varphi(\sum_{i=1}^{n} a_i \wedge b_i) = \sum_{i=1}^{n} \varphi(a_i \wedge b_i) \\
&= \sum_{i=1}^{n} f([a_i, b_i]) = f(\sum_{i=1}^{n} [a_i, b_i]) \\
&= f(\sum_{i=1}^{n} \theta_A(a_i \wedge b_i)) = f(\theta_A(\sum_{i=1}^{n} a_i \wedge b_i)) \\
&= f(\theta_A(\alpha)) = f(0) \quad (\text{car } \alpha \in \mathrm{H_1(A)} = \ker \theta_\mathrm{A}) \\
&= 0.
\end{aligned}$$

Donc la restriction de φ à $H_1(A)$ est nulle.

Réciproquement si la restriction de φ à $H_1(A)$ est nulle, on définit g sur $[A, A]$ comme étant l'application linéaire valant $\varphi(a \wedge b)$ sur $[a, b]$ quel que soit le couple (a, b) d'éléments de A. Pour justifier cette définition il faut vérifier que si $\sum_{i=1}^{n} \lambda_i [a_i, b_i] = \sum_{j=1}^{m} \mu_j [c_j, d_j]$ alors $\sum_{i=1}^{n} \lambda_i \varphi(a_i \wedge b_i) = \sum_{j=1}^{m} \mu_j \varphi(c_j \wedge d_j)$. Faisons le ; pour cela on commence par écrire que :

$$\sum_{i=1}^{n} \lambda_i \varphi(a_i \wedge b_i) - \sum_{j=1}^{m} \mu_j \varphi(c_j \wedge d_j) = \varphi(\sum_{i=1}^{n} \lambda_i (a_i \wedge b_i) - \sum_{j=1}^{m} \mu_j (c_j \wedge d_j)).$$

Mais on a :

$$\begin{aligned}
\theta_A(\sum_{i=1}^{n} \lambda_i (a_i \wedge b_i) - \sum_{j=1}^{m} \mu_j (c_j \wedge d_j)) &= \sum_{i=1}^{n} \lambda_i \theta_A(a_i \wedge b_i) - \sum_{j=1}^{m} \mu_j \theta_A(c_j \wedge d_j) \\
&= \sum_{i=1}^{n} \lambda_i [a_i, b_i] - \sum_{j=1}^{m} \mu_j [c_j, d_j] \\
&= 0.
\end{aligned}$$

Donc $\sum_{i=1}^{n} \lambda_i (a_i \wedge b_i) - \sum_{j=1}^{m} \mu_j (c_j \wedge d_j) \in H_1(A)$ ce qui prouve que son image par φ est nulle, ce que nous voulions démontrer. Donc g est bien définie sur $[A, A]$. On l'étend à A linéairement (sans autre condition, par exemple nulle sur un supplémentaire quelconque de $[A, A]$ dans A) pour obtenir l'application f voulue.

B. *Extensions affines*

1. Il est clair que $\{t^n\}_{n \in \mathbb{Z}}$ forme une base, donc en particulier une famille libre, de $k[t, t^{-1}]$ sur k. On en déduit par un raisonnement d'extension classique que $\{E_{ij}(t^n)\}_{1 \leq i,j \leq p, n \in \mathbb{Z}}$ est encore libre sur k ; en effet supposons que :

$$\sum_{1 \leq i,j \leq p, n \in \mathbb{Z}} \lambda_{ijn} E_{ij}(t^n) = 0_{M_p(A)}.$$

Alors $\sum_{1\leq i,j\leq p} E_{ij}(\sum_{n\in\mathbb{Z}} \lambda_{ijn}t^n) = 0_{M_p(A)}$ donc pour tout couple (i,j) on a l'identité suivante : $\sum_{n\in\mathbb{Z}} \lambda_{ijn}t^n = 0_A$. D'après la remarque initiale cela force $\lambda_{ijn} = 0$ pour tout triplet (i,j,n).

Montrons maintenant que $\{E_{ij}(t^n)\}_{1\leq i,j\leq p,n\in\mathbb{Z}}$ est génératrice de $M_p(A)$ sur k. Pour cela considérons $m \in M_p(A)$ quelconque : m s'écrit $\sum_{1\leq i,j\leq p} E_{ij}(m_{ij})$. Comme $\{t^n\}_{n\in\mathbb{Z}}$ forme une base de $k[t,t^{-1}]$ sur k on peut écrire pour tout couple (i,j) : $m_{ij} = \sum_{n\in\mathbb{Z}} \lambda_{ijn}t^n$. On injecte ces expressions dans celle de m et la linéarité donne le résultat.
En définitive tout ceci prouve que $\{E_{ij}(t^n)\}_{1\leq i,j\leq p,n\in\mathbb{Z}}$ est une base de $M_p(A)$ sur k. Il est alors évident que $\{c\}\cup\{e_{ij}(t^n)\}_{1\leq i,j\leq p,n\in\mathbb{Z}}$ est une base de $M_p(A)\times k$ sur k. Vérifions les relations demandées :

$\{c,c\} = \{(0,1),(0,1)\} = ([0,0],\alpha_\varphi(0,0)) = (0,0)$.

$\{c,e_{ij}(t^n)\} = \{(0,1),(E_{ij}(t^n),0)\} = ([0,E_{ij}(t^n)],\alpha_\varphi(0,E_{ij}(t^n))) = (0,0)$.

$\{e_{ij}(t^n),c\} = -\{c,e_{ij}(t^n)\}$ d'après $(L1)$, donc $\{e_{ij}(t^n),c\} = (0,0)$.

Enfin on a :

$$\begin{aligned}\{e_{ij}(t^n),e_{kl}(t^m)\} &= \{(E_{ij}(t^n)),0),(E_{kl}(t^m),0)\}\\ &= ([E_{ij}(t^n),E_{kl}(t^m)],\alpha_\varphi(E_{ij}(t^n),E_{kl}(t^m))).\end{aligned}$$

Mais on sait depuis I.B.2.a. que :

$$[E_{ij}(t^n),E_{kl}(t^m)] = \delta_{jk}E_{il}(t^nt^m) - \delta_{li}E_{kj}(t^mt^n) = \delta_{jk}E_{il}(t^{n+m}) - \delta_{il}E_{kj}(t^{n+m}).$$

On a également :

$$\begin{aligned}\alpha_\varphi(E_{ij}(t^n),E_{kl}(t^m)) &= \varphi(E_{ij}(t^n)\wedge E_{kl}(t^m))\\ &= Res(\widehat{Tr'}(E_{ij}(t^n)\wedge E_{kl}(t^m))\\ &= Res(Tr'(E_{ij}(t^n),E_{kl}(t^m))\\ &= Res(\delta_{il}\delta_{jk}t^n\wedge t^m) \text{ (III.5.a.)}\\ &= \delta_{il}\delta_{jk}Res(t^n\wedge t^m)\\ &= \delta_{il}\delta_{jk}res(mt^{n+m-1}) \text{ (III.6.b.)}.\end{aligned}$$

Si $n+m\neq 0$, $res(mt^{n+m-1}) = 0$ et si $n = -m$, $res(mt^{n+m-1}) = m$. Donc finalement si $n+m\neq 0$, $\{e_{ij}(t^n),e_{kl}(t^m)\} = \delta_{jk}e_{il}(t^{n+m}) - \delta_{il}e_{kj}(t^{n+m})$ et par ailleurs $\{e_{ij}(t^{-m}),e_{kl}(t^m)\} = \delta_{jk}e_{il}(1) - \delta_{il}e_{kj}(1) + \delta_{il}\delta_{jk}mc$.

2. D'après A.1.c., $L(M_p(A))(\alpha_\varphi)$ est triviale ssi $\varphi(H_1(M_p(A))) = \{0\}$.
Or $\varphi(H_1(M_p(A))) = Res(\widehat{Tr'}(H_1(M_p(A)))) = Res(H_1(A))$ (d'après III.5.d.) $= k$ (d'après III.6.d.). Donc $L(M_p(A))(\alpha_\varphi)$ n'est pas triviale.

C. *Opérateurs différentiels*

1.a. Posons $\widetilde{P} = f(P)$ et prenons R dans A. On a :
$f(\lambda P+\mu Q)(R) = (\lambda P+\mu Q)R = \lambda PR + \mu QR = \lambda f(P)(R) + \mu f(Q)(R) = (\lambda f(P) + \mu f(Q))(R)$. Comme c'est vrai quel que soit $R\in A$, on a :

$$f(\lambda P+\mu Q) = \lambda f(P) + \mu f(Q).$$

$f(PQ)(R) = PQR = P(QR) = f(P)(QR) = f(P)(f(Q)(R))$ donc :

$$f(PQ) = f(P) \circ f(Q).$$

$f(1)(R) = 1R = R = Id_A(R)$ donc $f(1) = 1_{End(A)}$.
Il s'agit donc bien d'un morphisme d'algèbres.

1.b. Montrons par récurrence sur $q \in \mathbb{N}$ que pour tous $P, R \in A$ on a : $d^q(PR) = \sum_{l=0}^{q} \binom{q}{l} P^{(l)} R^{(q-l)}$ (ce qui correspond à la formule de Leibniz).
Quand $q = 0$ cette égalité s'écrit juste $PR = PR$.
Supposons l'égalité vérifiée jusqu'au rang q et étudions $d^{q+1}(PR)$:

$$\begin{aligned}
d^{q+1}(PR) &= d(d^q(PR)) \\
&= d(\sum_{l=0}^{q} \binom{q}{l} P^{(l)} R^{(q-l)}) \\
&= \sum_{l=0}^{q} \binom{q}{l} d(P^{(l)} R^{(q-l)}) \quad \text{(car d est linéaire)} \\
&= \sum_{l=0}^{q} \binom{q}{l} (P^{(l+1)} R^{(q-l)} + P^{(l)} R^{(q-l+1)}) \quad \text{(III.6.a.)} \\
&= \sum_{l=0}^{q} \binom{q}{l} P^{(l+1)} R^{((q+1)-(l+1))} + \sum_{l=0}^{q} \binom{q}{l} P^{(l)} R^{((q+1)-l)} \\
&= \sum_{u=1}^{q+1} \binom{q}{u-1} P^{(u)} R^{((q+1)-u)} + \sum_{u=0}^{q} \binom{q}{u} P^{(u)} R^{((q+1)-u)} \\
&= \sum_{u=1}^{q} \left(\binom{q}{u-1} + \binom{q}{u} \right) P^{(u)} R^{((q+1)-u)} \\
&\quad + \tbinom{q}{q} P^{(q+1)} R + \tbinom{q}{0} P R^{(q+1)} \\
&= \sum_{u=1}^{q} \left(\binom{q}{u-1} + \binom{q}{u} \right) P^{(u)} R^{((q+1)-u)} \\
&\quad + \tbinom{q+1}{q+1} P^{(q+1)} R + \tbinom{q+1}{0} P R^{(q+1)}.
\end{aligned}$$

Or d'après la formule du triangle de Pascal $\binom{q}{u-1} + \binom{q}{u} = \binom{q+1}{u}$. Donc on a en fait obtenu la formule souhaitée au rang $q+1$.
Fixons maintenant $R \in A$. On a :

$$\begin{aligned}
(d^q \circ \widetilde{P})(R) &= d^q(\widetilde{P}(R)) \\
&= d^q(PR) \\
&= \sum_{l=0}^{q} \binom{q}{l} P^{(l)} R^{(q-l)} \quad \text{(calcul préliminaire)} \\
&= \sum_{l=0}^{q} \binom{q}{l} \widetilde{P^{(l)}}(R^{(q-l)}) \\
&= \sum_{l=0}^{q} \binom{q}{l} (\widetilde{P^{(l)}} \circ d^{q-l})(R).
\end{aligned}$$

Ceci étant vrai pour tout R cela signifie que :

$$d^q \circ \widetilde{P} = \sum_{l=0}^{q} \binom{q}{l} \widetilde{P^{(l)}} \circ d^{q-l}.$$

2.a. Soit $\alpha \in D$. Par définition $\alpha = \sum_{i \in I} \widetilde{P}_i d^i$ avec I fini. Posons pour tout $i \in I$: $P_i = \sum_{l \in \mathbb{Z}} p_{il} t^l$ (il s'agit de sommes finies). On a alors :

$$\alpha = \sum_{i \in I} (\widetilde{\sum_{l \in \mathbb{Z}} p_{il} t^l}) d^i.$$

Mais $(\widetilde{\sum_{l \in \mathbb{Z}} p_{il} t^l}) = \sum_{l \in \mathbb{Z}} p_{il} \widetilde{t^l}$ d'après 1.a. donc $(\widetilde{\sum_{l \in \mathbb{Z}} p_{il} t^l}) = \sum_{l \in \mathbb{Z}} p_{il} u^l$ et finalement $\alpha = \sum_{i \in I} \sum_{l \in \mathbb{Z}} p_{il} u^l d^i$. Cela prouve que $\{u^p d^q\}_{p \in \mathbb{Z}, q \in \mathbb{N}}$ est une famille génératrice de D.

Supposons maintenant que cette famille ne soit pas libre. On peut donc exhiber une relation de liaison avec des coefficients tous non nuls de la forme suivante : $\sum_{(p,q) \in I} \lambda_{(p,q)} u^p d^q = 0_{End(A)}$ où I est une partie finie de $\mathbb{Z} \times \mathbb{N}$. Posons maintenant d'une part :

$$q_0 = \inf\{q \in \mathbb{N} \text{ tel qu'il existe } p \in \mathbb{Z} \text{ avec } (p,q) \in I\},$$

et d'autre part :

$$J = \{p \in \mathbb{Z} \text{ tel que } (p, q_0) \in I\}.$$

Appliquons $\sum_{(p,q) \in I} \lambda_{(p,q)} u^p d^q$ à t^{q_0} : il vient $(\sum_{(p,q) \in I} \lambda_{(p,q)} u^p d^q)(t^{q_0}) = 0_A$. Mais par ailleurs on a :

$$\begin{aligned} (\sum_{(p,q) \in I} \lambda_{(p,q)} u^p d^q)(t^{q_0}) &= \sum_{(p,q) \in I} \lambda_{(p,q)} u^p (d^q)(t^{q_0}) \\ &= \sum_{p \in J} \lambda_{(p,q_0)} u^p (q_0!) \\ &= \sum_{p \in J} \lambda_{(p,q_0)} q_0! t^p. \end{aligned}$$

Donc $\sum_{p \in J} \lambda_{(p,q_0)} q_0! t^p = 0_A$. Comme les t^p forment une famille libre dans A tous les $\lambda_{(p,q_0)}$ sont nuls. Ceci est absurde donc notre famille initiale est libre. Comme elle était aussi génératrice, c'est une base de D.

2.b. Il suffit de le montrer sur les éléments d'une base (par exemple celle du a.) puis d'étendre le résultat par bilinéarité du produit dans une algèbre (ici $End(A)$). Soient donc $u^p d^q$ et $u^{p'} d^{q'}$ deux éléments de cette base. On a :

$$\begin{aligned} u^p d^q u^{p'} d^{q'} &= u^p (d^q u^{p'}) d^{q'} \\ &= u^p (d^q \widetilde{(t)^{p'}}) d^{q'} \\ &= u^p (d^q \widetilde{(t^{p'})}) d^{q'} \\ &= u^p (\sum_{l=0}^{q} \binom{q}{l} (\widetilde{(t^{p'})^{(l)}}) d^{q-l}) d^{q'} \quad (1.b.) \\ &= \sum_{l=0}^{q} \binom{q}{l} u^p (\widetilde{(t^{p'})^{(l)}}) d^{q+q'-l}. \end{aligned}$$

Mais $(\widetilde{(t^{p'})^{(l)}})$ est de la forme $\widetilde{\lambda t^n}$ c'est-à-dire λu^n car $\widetilde{\ }$ est un morphisme d'algèbres. En injectant cette forme dans le calcul précédent, et compte tenu de $u^p u^n = u^{p+n}$, on obtient une écriture de $u^p d^q u^{p'} d^{q'}$ comme combinaison linéaire de vecteurs de la base, ce qui achève la démonstration : D est stable par composition.

Comme D est un sev de $End(A)$, il ne reste plus qu'à vérifier que $1_{End(A)} \in D$ pour établir que D est une sous-algèbre de $End(A)$. C'est facile : $1_{End(A)} = \mathrm{I}_A = u^0 d^0$.

3. Si $r = 0$, il est clair que ce commutateur est nul. Sinon $(r \geq 1)$ $[u, u^q d^r] = u^{q+1} d^r - u^q d^r u = u^{q+1} d^r - u^q (u d^r + r d^{r-1})$ en appliquant la formule du 1.b. Donc $[u, u^q d^r] = u^{q+1} d^r - u^{q+1} d^r - r u^q d^{r-1} = -r u^q d^{r-1}$.

On en déduit que si $(q, r) \in \mathbb{Z} \times \mathbb{N}$, on a : $u^q d^r = -(r+1)^{-1} [u, u^q d^{r+1}]$. En particulier $u^q d^r \in [D, D]$. Comme les $u^q d^r$ engendrent D cela force $D \subset [D, D]$, donc $D = [D, D]$ (puisque D est une sous-algèbre de $End(A)$) : par définition on a $H_0(D) = \{0\}$.

Enfin on sait depuis I.A.2. que si V est un $k-$espace vectoriel, $T(D, V)$ est isomorphe à $L(H_0(D), V)$, donc à $L(\{0\}, V)$: $T(D, V) = \{0\}$. Ceci signifie que toute trace sur D est nulle car V est quelconque.

D. *Extension de Virasoro*

1. Compte tenu de la définition de W, on peut dire qu'il est composé des éléments de D qui peuvent s'écrire $\widetilde{P} d$ pour $P \in A$. On peut tout de suite préciser que les $u^p d$ pour p parcourant $\mathbb{Z}$ forment une base de W : c'est une famille génératrice par définition de W, et libre d'après C.2.a.. Ceci étant dit, calculons le crochet $[\widetilde{P} d, \widetilde{Q} d]$. On a :

$$\begin{aligned} [\widetilde{P} d, \widetilde{Q} d] &= \widetilde{P} d \widetilde{Q} d - \widetilde{Q} d \widetilde{P} d \\ &= (\widetilde{P} d \widetilde{Q} - \widetilde{Q} d \widetilde{P}) d \\ &= (\widetilde{P} (\widetilde{Q} d + \widetilde{Q'}) - \widetilde{Q} (\widetilde{P} d + \widetilde{P'})) d \quad (C.1.b.) \\ &= (\widetilde{P} \widetilde{Q} d + \widetilde{P} \widetilde{Q'} - \widetilde{Q} \widetilde{P} d - \widetilde{Q} \widetilde{P'}) d. \end{aligned}$$

Or $PQ = QP$ donc $\widetilde{PQ} = \widetilde{QP}$ et $\widetilde{P}\widetilde{Q} = \widetilde{Q}\widetilde{P}$ puisqu'on a un morphisme d'algèbres. On en déduit que $\widetilde{P} \widetilde{Q} d = \widetilde{Q} \widetilde{P} d$. Le calcul précédent se simplifie en $[\widetilde{P} d, \widetilde{Q} d] = (\widetilde{P} \widetilde{Q'} - \widetilde{Q} \widetilde{P'}) d$. En invoquant encore une fois le fait que $\widetilde{\ }$ est un morphisme d'algèbres on réécrit $\widetilde{P} \widetilde{Q'} - \widetilde{Q} \widetilde{P'}$ sous la forme $\widetilde{(PQ' - QP')}$ ce qui donne la formule demandée.

La restriction de $[\ ,\ ]$ à $W \times W$ est donc à valeurs dans W. Sa bilinéarité étant évidente, il suffit de vérifier les identités (L1) et (L2) sur les éléments de

la base de W constituée des $u^p d$ pour en déduire que $(W, [\ ,\ ])$ est un l-espace. Mais ceci est évident (il suffit de relire le A.2.a. pour s'en convaincre).

2. Pour tous P, $Q \in A$, on a :

$$\begin{aligned}\alpha(\tilde{P}d, \tilde{Q}d) + \alpha(\tilde{Q}d, \tilde{P}d) &= \tfrac{1}{12} res(P'Q'' - Q'P'') + res(Q'P'' - P'Q'') \\ &= \tfrac{1}{12} res(0) \text{ (par linéarité de res.)} \\ &= 0.\end{aligned}$$

Ceci prouve (C1).

Encore une fois il est clair que α est bilinéaire donc il suffit de vérifier (C2) sur les éléments de la base. Soient donc $p, q, r \in \mathbb{Z}$ et notons :

$$J(p,q,r) = \alpha(u^p d, [u^q d, u^r d]) + \alpha(u^q d, [u^r d, u^p d]) + \alpha(u^r d, [u^p d, u^q d]).$$

En utilisant la formule démontrée au 1., on obtient pour $J(p,q,r)$ l'expression suivante :

$$\alpha(u^p d, (r-q)u^{q+r-1} d) + \alpha(u^q d, (p-r)u^{p+r-1} d) + \alpha(u^r d, (q-p)u^{q+p-1} d).$$

Il est clair que chacun des trois termes est de la forme $\frac{1}{12} res(\lambda t^{p+q+r-4})$ avec $\lambda \in k$. Donc si $p+q+r \neq 3$, c'est-à-dire si $p+q+r-4 \neq -1$, on a immédiatement $J(p,q,r) = 0$. Reste à étudier le cas $p+q+r = 3$:

$$\begin{aligned}&\alpha(u^p d, (r-q)u^{q+r-1} d) = \alpha(u^p d, (r-q)u^{2-p} d) \\ &= \tfrac{1}{12} res\big(pt^{p-1}(r-q)(2-p)(1-p)t^{-p} - p(p-1)t^{p-2}(r-q)(2-p)t^{1-p}\big) \\ &= \tfrac{1}{12} res\big((p(r-q)(2-p)(1-p) - p(p-1)(r-q)(2-p))t^{-1}\big) \\ &= \tfrac{1}{12}(p(r-q)(2-p)(1-p) - p(p-1)(r-q)(2-p)) \\ &= \tfrac{1}{6} p(r-q)(2-p)(1-p).\end{aligned}$$

On calcule pareillement les deux autres termes et on additionne pour obtenir : $J(p,q,r) = \frac{1}{6}[p(r-q)(2-p)(1-p) + q(p-r)(2-q)(1-q) + r(q-p)(2-r)(1-r)]$. En développant puis en simplifiant, il vient pour $J(p,q,r)$ cette expression : $\frac{1}{6}(p^3 r - 3p^2 r - p^3 q + 3p^2 q + q^3 p - 3q^2 p - q^3 r + 3q^2 r + r^3 q - 3r^2 q - r^3 p + 3r^2 p)$. Mais cette dernière somme se factorise sous la forme suivante : $(p+q+r-3)(-q^2 r + p^2 r - p^2 q + q^2 p + r^2 q - r^2 p)$. Puisque $p+q+r = 3$, elle est nulle, et on a donc bien obtenu $J(p,q,r) = 0$ dans tous les cas, ce qui démontre (C2). Finalement α est bien un cocycle sur W.

3. $W(\alpha) = (W \times k, \{\ ,\ \})$ avec $\{(w_1, \lambda_1), (w_2, \lambda_2)\} = ([w_1, w_2], \alpha(w_1, w_2))$. On pose $c = (0, 1)$ et pour tout $n \in \mathbb{Z}$, $L_n = (u^{n+1} d, 0)$. On sait déjà que $\{u^{n+1} d\}_{n \in \mathbb{Z}}$ est une base de W donc il est clair que $\{c\} \cup \{L_n\}_{n \in \mathbb{Z}}$ est une base de $W \times k$ qui est l'espace vectoriel sous-jacent à Vir.
Les bilinéarités de $[\ ,\ ]$ et de α assurent immédiatement que :

$$\{c, c\} = \{c, L_n\} = \{L_n, c\} = 0.$$

Si $n + m \neq 0$ on a : D'autre part

$$\begin{aligned}\{L_n, L_m\} &= ([u^{n+1} d, u^{m+1} d], \alpha(u^{n+1} d, u^{m+1} d)) \\ &= (((m+1) - (n+1))u^{(m+1)+(n+1)-1} d, \\ &\quad \tfrac{1}{12} res((n+1)t^n (m+1) m t^{m-1} - (m+1)t^m (n+1) n t^{n-1}) \\ &\quad \text{(en utilisant la formule du 1.)} \\ &= ((m-n)u^{n+m+1} d, \tfrac{1}{12} res((n+1)(m+1)(m-n)t^{n+m-1}))\end{aligned}$$

Si $n+m \neq 0$ alors $\{L_n, L_m\} = ((m-n)u^{n+m+1}d, 0) = (m-n)L_{n+m}$.
Si $n+m = 0$, c'est-à-dire si $n = -m$,

$$\{L_{-m}, L_m\} = 2mL_0 - \frac{m^3 - m}{6}c.$$

4.a. D'après A.1.c. on a l'équivalence : Vir est triviale si et seulement si il existe une application linéaire $f : W \to k$ telle que $\alpha(w_1, w_2) = f([w_1, w_2])$ pour tous w_1, w_2 dans W. Supposons que cela soit vrai et appliquons ceci à $w_1 = u^{-m+1}d$ et $w_2 = u^{m+1}d$ pour un $m \in \mathbb{Z}$ quelconque. Le calcul effectué à la question précédente (dans le cas $n = -m$) donne $-\frac{m^3-m}{6} = 2mf(ud)$ quel que soit $m \in \mathbb{Z}$. C'est évidemment absurde (un polynôme non nul n'admet qu'un nombre fini de racines) donc l'extension Vir n'est pas triviale.

4.b. D'après a., il n'existe pas d'application linéaire $f : W \to k$ telle que $\alpha(w_1, w_2) = f([w_1, w_2])$ pour tous w_1, w_2 dans W. A fortiori comme $W \subset D$, il n'existe pas d'application linéaire $g : D \to k$ telle que $\alpha(d_1, d_2) = g([d_1, d_2])$ pour tous d_1, d_2 dans D donc $L(D)(\alpha)$ n'est pas triviale.

Si on admet que le cocycle α est de la forme α_φ avec φ une forme linéaire sur $C(D)$ alors on peut appliquer le résultat de A.2.c. avec $A = D$. Ceci implique nécessairement que l'espace vectoriel $H_1(D)$ n'est pas nul.

4.3 Commentaires

Ce problème exige une bonne familiarité avec les notions d'algèbre linéaire ou multilinéaire, notamment celle de base, celle d'application (multi)linéaire et celle omniprésente de passage au quotient. Peu de connaissances théoriques sophistiquées sont réellement mises en jeu, même si l'on manipule groupes, algèbres, polynômes ou matrices. On peut mentionner qu'il fallait par exemple connaître les classes de conjugaison de $\mathcal{S}_4$ ou savoir que le rang d'un projecteur est donné par sa trace. Il est donc raisonnable de dire que ce problème est plutôt moins difficile que la plupart de ceux traditionnellement posés lors de cette épreuve de mathémathiques générales, tant du point de vue conceptuel que du point de vue de l'érudition requise. A ce titre, il peut servir de base de travail dès le début d'une année de préparation au concours. Toutefois il nécessite une habilité certaine dans les calculs et même parfois une bonne dose de persévérance ! Ce sera de toute façon un excellent test.

Chapitre 5

Session de 1993

5.1 Sujet

5.2 Correction

I. Exemples de fonctions vérifiant des équations différentielles algébriques sur $\mathbb{C}$.

1. *L'application exponentielle réelle.*

1.a. Soit $P \in \mathbb{C}[X_0]$ tel que $P(f) = 0$. On a pour tout $u \in \mathbb{R}$, $P(e^u) = 0$ donc le polynôme P s'annule sur l'ensemble infini $\mathbb{R}^{*+}$. On en déduit que P est nul.

1.b. Soit $Q = X_1 - X_0 \in \mathbb{C}[X_0, X_1]$. Le polynôme Q est clairement non nul. Comme $Q(f, f') = f' - f = 0$, le polynôme Q convient.

Remarque importante. Dans la suite, on identifie $A[X_0, \ldots, X_{n+1}]$ et $A[X_0, \ldots, X_n][X_{n+1}]$ où A est un anneau commutatif intègre unitaire. On rappelle d'ailleurs que si A est un anneau commutatif intègre unitaire, alors $A[X]$ aussi.

1.c. Fixons $P \in \mathbb{C}[X_0, X_1]$. Supposons que P s'écrive $(X_1 - X_0)R$ avec $R \in \mathbb{C}[X_0, X_1]$. Alors $P(f, f') = (f' - f)R(f, f') = 0$.

Réciproquement, on définit $V = X_1 - X_0$. On remarque que $P, V \in \mathbb{C}[X_0][X_1]$ et le coefficient dominant de V est 1 donc inversible dans $\mathbb{C}[X_0]$. On peut donc effectuer la division euclidienne du polynôme P par le polynôme V. Il existe ainsi $Q, R \in \mathbb{C}[X_0][X_1]$ tels que $P = VQ + R$ et le degré de R soit strictement inférieur à celui de V donc V est nul ou de degré nul. Autrement dit R est un polynôme constant (éventuellement nul) de $\mathbb{C}[X_0][X_1]$ soit $R = r$ où $r \in \mathbb{C}[X_0]$. On a : $P(f, f') = V(f, f')Q(f, f') + r(f)$. Comme $P(f, f') = 0$ par hypothèse, on obtient : $r(f) = 0$. Enfin, on applique la question 1.a et $r = 0$ soit $R = 0$. Finalement, $P = (X_1 - X_0)Q$.

1.d. Fixons $P \in \mathbb{C}[X_0, X_1, X_2]$.

Supposons que P s'écrive $(X_1 - X_0)R + (X_2 - X_0)S$ avec $R, S \in \mathbb{C}[X_0, X_1, X_2]$ alors $P(f, f', f'') = (f' - f)R(f, f', f'') + (f'' - f)S(f, f', f'') = 0$.

Réciproquement, on définit $V(X_0, X_1, X_2) = X_2 - X_0 \in \mathbb{C}[X_0, X_1][X_2]$. On a $P, V \in \mathbb{C}[X_0, X_1][X_2]$ et le coefficient dominant de V est 1 donc inversible dans $\mathbb{C}[X_0, X_1]$. On peut donc effectuer la division euclidienne du polynôme P par le polynôme V. Il existe ainsi $S, T \in \mathbb{C}[X_0, X_1][X_2]$ tels que $P = VS + T$. De plus, le degré de T est strictement inférieur à celui de V donc est nul. On peut donc écrire $T = t \in \mathbb{C}[X_0, X_1]$. Comme $0 = P(f, f', f'') = (f'' - f)S(f, f', f'') + t(f, f')$, on obtient $t(f, f') = 0$. D'après 1.c, le polynôme t sécrit $(X_1 - X_0)R$ avec $R \in \mathbb{C}[X_0, X_1]$.

Finalement, $P = (X_2 - X_0)S + (X_1 - X_0)R$ avec $R, S \in \mathbb{C}[X_0, X_1, X_2]$.

1.e. Soient $P \in J$ et $Q \in \mathbb{C}[X_0, X_1, X_2]$.

On a $(PQ)(f, f', f") = Q(f, f', f")P(f, f', f") = 0$ car $P \in J$. On en déduit que $QP = PQ \in J$. De plus, si $P, Q \in J$, on a clairement $P - Q \in J$ donc J est un sous-groupe additif de $\mathbb{C}[X_0, X_1, X_2]$. On conclut que J est un idéal.

Supposons que J soit principal, il existe un polynôme $P \in J$ qui engendre cet idéal, c'est à dire que $J = P.\mathbb{C}[X_0, X_1, X_2]$. Comme J n'est pas réduit à

$\{0\}$ (par exemple $X_1 - X_0 \in J$), P n'est pas nul. Il est clair que $X_2 - X_0$ et $X_1 - X_0 \in J$ donc il existe Q_1 et $Q_2 \in \mathbb{C}[X_0, X_1, X_2]$ tels que $X_2 - X_0 = PQ_2$ et $X_1 - X_0 = PQ_1$.

En raisonnant dans $\mathbb{C}[X_0, X_1][X_2]$, le degré en X_2 de $X_1 - X_0$ est nul donc celui de P aussi. De même, en raisonnant dans $\mathbb{C}[X_0, X_2][X_1]$, le degré en X_1 de $X_2 - X_0$ est nul donc celui de P aussi.

A fortiori, $P = p \in \mathbb{C}[X_0]$. Comme $P \in J$, on $p(f) = P(f, f', f'') = 0$. D'après 1.a, $p = 0$. Ainsi $P = 0$ et $J = \{0\}$, ce qui est faux. On conclut donc que J n'est pas principal.

2. *L'application* $u \mapsto \sin u$.

2.a. Soit $P \in \mathbb{C}[X_0]$ tel que $P(f) = 0$. On a pour tout $u \in \mathbb{R}$, $P(\sin u) = 0$ donc le polynôme P s'annule sur l'ensemble infini $[-1, 1]$. On en déduit que P est nul.

2.b. Le polynôme $Q(X_0, X_1) = X_1^2 + X_0^2 - 1 \in \mathbb{C}[X_0, X_1]$ convient car $Q(f, f')(u) = \cos^2 u + \sin^2 u - 1 = 0$. De plus, Q est non nul.

2.c. Soient $U, V \in \mathbb{C}[X_0]$ tels que $U(f)f' + V(f) = 0$.

On a alors $\big(U(f)f'\big)^2 = \big(V(f)\big)^2$. On a donc $T(f) = 0$ où T est le polynôme $U^2(1 - X_0^2) - V^2$. D'après 2.a, $T = 0$ donc $U^2 = U^2X_0^2 + V^2$.

En comparant les degrés, $U^2X_0^2$ et V^2 ont nécessairement le même, sinon le degré de U^2 est le maximum des degrés de $U^2X_0^2$ et V^2 donc est strictement supérieur à celui de U^2. Notons a (resp. b) le coefficient de plus haut degré de U (resp. de V). On a : $a^2 = a^2 + b^2$ donc $b = 0$. Ainsi, $V = 0$ et $U^2(1 - X_0^2) = 0$ donc $U = 0$.

2.d. L'ensemble J est clairement un idéal.

Soit $Q(X_0, X_1) = X_1^2 + X_0^2 - 1 \in \mathbb{C}[X_0, X_1]$. On a $Q.\mathbb{C}[X_0, X_1] \subset J$ car $Q \in J$ d'après 1.b.

Réciproquement, si $P \in J$, on effectue la division euclidienne dans $\mathbb{C}[X_0][X_1]$ de P par Q dont le coefficient dominant (c'est 1) est inversible dans $\mathbb{C}[X_0]$. Il existe donc $S, T \in \mathbb{C}[X_0][X_1]$ tels que $P = QS + T$. De plus, le degré de T est strictement inférieur à celui de V. On peut donc écrire $T = UX_1 + V$ où $U, V \in \mathbb{C}[X_0]$. Comme $P, Q \in J$ qui est un idéal, on a $T \in J$ ie $T(f, f') = 0$ soit $U(f)f' + V(f) = 0$. D'après 2.c, les polynômes U et V sont nuls donc T est nul. Finalement, $P = QS$ avec $S \in \mathbb{C}[X_0, X_1]$.

On conclut que $J = Q.\mathbb{C}[X_0, X_1]$ donc J est un idéal principal de $\mathbb{C}[X_0, X_1]$.

2.e. L'ensemble L est clairement un idéal de $\mathbb{C}[X_0, X_1, X_2]$. On définit $Q = X_1^2 + X_0^2 - 1$ et $R = X_2 + X_0$, ce sont des éléments de L. Supposons que L soit principal. On a alors l'existence de $P \in L$ tel que $L = P.\mathbb{C}[X_0, X_1, X_2]$. Comme L n'est pas réduit à $\{0\}$ (par exemple $R \neq 0$), P n'est pas nul. Il existe T_1 et $T_2 \in \mathbb{C}[X_0, X_1, X_2]$ tels que $R = PT_1$ et $Q = PT_2$.

En raisonnant dans $\mathbb{C}[X_0, X_1][X_2]$, le degré en X_2 de Q est nul donc celui de P aussi. De même, en raisonnant dans $\mathbb{C}[X_0, X_2][X_1]$, le degré en X_1 de R est nul donc celui de P aussi.

A fortiori, $P = p \in \mathbb{C}[X_0]$. Comme $P \in L$, on $p(f) = P(f, f', f'') = 0$. D'après 2.a, $p = 0$. Ainsi $P = 0$ et $L = \{0\}$, ce qui est faux. On conclut donc que L n'est pas principal.

3. *L'application* $u \mapsto e^{u^2}$.

3.a. Soit $P \in \mathbb{C}[X_0, X_1]$ tel que $P(f, f') = 0$. On écrit

$$P(X_0, X_1) = \sum_{i,j \geq 0} a_{i,j} X_0^i X_1^j.$$

Supposons que P soit non nul, on peut alors définir $N = \max\{i+j |\ a_{i,j} \neq 0\}$ et $d = \max\{j |\ 0 \leq j \leq N,\ a_{N-j,j} \neq 0\}$.

On a pour tout $u \in \mathbb{R}$, $P(e^{u^2}, 2ue^{u^2}) = 0$, ce qui s'écrit encore

$$\sum_{\substack{0 \leq n \leq N \\ i+j=n}} a_{i,j} (2u)^j e^{nu^2} = 0.$$

En divisant cette relation par $u^d . e^{Nu^2}$, on obtient pour tout $u \in \mathbb{R}^*$

$$\sum_{\substack{0 \leq n < N \\ i+j=n}} a_{i,j} 2^j . u^{j-d} e^{(n-N)u^2} + \sum_{j=0}^{d} a_{N-j,j} . 2^j . u^{j-d} = 0.$$

En faisant tendre u vers $+\infty$, il vient $a_{N-d,d} . 2^d = 0$ ce qui contredit la définition de d. Ainsi P est nul.

3.b. Pour tout $u \in \mathbb{R}$, on a $f'(u) = 2ue^{u^2}$ et $f''(u) = 2(2u^2+1)e^{u^2}$. On a alors $ff'' = (f')^2 + 2f^2$. Ainsi le polynôme $Q = X_0 X_2 - X_1^2 - 2X_0^2$ convient.

3.c. L'ensemble J est clairement un idéal.

Comme $Q \in J$, on a $Q.\mathbb{C}[X_0, X_1, X_2] \subset J$. Réciproquement, soit $P \in J$. On considère l'anneau commutatif intègre unitaire : $A = \mathbb{C}[X_0, \dfrac{1}{X_0}, X_1]$ (comme sous-anneau de $\mathbb{C}(X_0, X_1)$). L'élément X_0 est inversible dans A donc le coefficient dominant de $Q \in \mathbb{C}[X_0, X_1][X_2]$ (que l'on considère de façon naturelle comme élément de A) est inversible dans A. On effectue alors la division euclidienne de P (que l'on considère aussi de façon naturelle comme élément de A) par Q dans $A[X_2]$. Il existe $R, S \in A[X_2]$ tels que $P = RQ + S$ où le degré de S est strictement inférieur à celui de Q soit $S = s \in A$. Comme $\dfrac{1}{f} \in C_\infty$, on a : $s(f, \dfrac{1}{f}, f') = 0$.

Soit n le degré de S en l'indéterminé $\dfrac{1}{X_0}$. On a $S_0 = X_0^n S \in \mathbb{C}[X_0, X_1]$ et on a $S_0(f, f') = 0$. D'après 3.a, S_0 est nul donc S aussi.

Attention : ce n'est pas fini ! On a montré $P = RQ$ mais pour l'instant $R \in A$.

Il existe un entier n et $R_0 \in \mathbb{C}[X_0, X_1]$ tels que $R = \dfrac{R_0}{X_0^n}$. On a donc $PX_0^n = R_0 Q$ et cette égalité a lieu dans $\mathbb{C}[X_1, X_2][X_0]$. La valuation de $R_0 Q$, val$(R_0 Q)$, est donc supérieure à n. D'autre part, val$(R_0 Q)$ =val(R_0)+val(Q) or val$(Q) = 0$. On en déduit que val$(R_0) \geq n$ i.e. X_0^n divise R_0 donc $P = TQ$ où $T \in \mathbb{C}[X_1, X_2][X_0]$.

On aurait pu aussi raisonner de façon plus théorique dans $\mathbb{C}[X_0, X_1, X_2]$: X_0^n divise $R_0 Q$, X_0 ne divise pas Q et X_0 est irréductible. Comme $\mathbb{C}[X_0, X_1, X_2]$ est factoriel, on applique le théorème de Gauss et on déduit que X_0^n divise R_0.

On conclut que $P \in Q.\mathbb{C}[X_0, X_1, X_2]$.
Finalement, $J = Q.\mathbb{C}[X_0, X_1, X_2]$ et J est principal.

II. Solutions holomorphes d'une équation fonctionnelle.

1.a. Soient $\rho \in [0, 1[$ et $n \in \mathbb{N}$. Montrons par récurrence que :

$$(H_n) \qquad \prod_{k=0}^{n}(1+\rho^{2^k}) = \frac{1-\rho^{2^{n+1}}}{1-\rho}\cdot$$

(H_0) est clairement vraie : $(1+\rho) = \dfrac{1-\rho^2}{1-\rho}\cdot$
Supposons (H_n) vraie alors

$$\prod_{k=0}^{n+1}(1+\rho^{2^k}) = (1+\rho^{2^{n+1}})\prod_{k=0}^{n}(1+\rho^{2^k}) = (1+\rho^{2^{n+1}})\frac{1-\rho^{2^{n+1}}}{1-\rho} = \frac{1-\rho^{2^{n+2}}}{1-\rho}\cdot$$

Ainsi, (H_{n+1}) est vraie.
Par récurrence, (H_n) est vraie pour tout n.
Comme $\rho \in [0, 1[$, on conclut alors $\displaystyle\prod_{k=0}^{n}(1+\rho^{2^k}) = \frac{1-\rho^{2^{n+1}}}{1-\rho} \leq \frac{1}{1-\rho}\cdot$

1.b. Pour tout $z \in \Delta$, on a la factorisation suivante

$$\theta_n(z) - \theta_{n+1}(z) = z^{2^{n+1}}\prod_{k=0}^{n}(1-z^{2^k}).$$

d'où la majoration en module :

$$|\theta_n(z) - \theta_{n+1}(z)| \leq |z|^{2^{n+1}}\prod_{k=0}^{n}(1+|z|^{2^k}) \leq \frac{|z|^{2^{n+1}}}{1-|z|}\cdot$$

où la dernière inégalité provient de (H_n) avec $\rho = |z| < 1$.

1.c. Pour tout $z \in \Delta$ et tous $q > p \in \mathbb{N}$, on constate que

$$\theta_p(z) - \theta_q(z) = \sum_{n=p}^{q-1}\theta_n(z) - \theta_{n+1}(z).$$

Ainsi, via 1.b,

$$|\theta_p(z) - \theta_q(z)| \leq \sum_{n=p}^{q-1}|\theta_n(z) - \theta_{n+1}(z)| \leq \sum_{n=p}^{q-1}\frac{|z|^{2^{n+1}}}{1-|z|} \leq \frac{1}{1-|z|}\cdot\frac{|z|^{2^{p+1}}}{1-|z|}\cdot$$

Fixons $z \in \Delta$ et $\varepsilon > 0$, comme $|z| < 1$, il existe $n_0 \in \mathbb{N}$ tel que $\dfrac{|z|^{2^{n_0+1}}}{(1-|z|)^2} < \varepsilon$.

On a alors pour tous $q > p \geq n_0$, $|\theta_p(z) - \theta_q(z)| \leq \dfrac{|z|^{2^{n_0+1}}}{(1-|z|)^2} < \varepsilon$.

D'après le critère de Cauchy, la suite $(\theta_n(z))_n$ est convergente vers une limite $\theta(z)$. Autrement dit, $(\theta_n)_n$ est simplement convergente vers θ sur Δ.

1.d. Soit $r \in]0,1[$. Il existe $n_0 \in \mathbb{N}$ tel que $\dfrac{r^{2^{n_0+1}}}{(1-r)^2} < \varepsilon$.

Pour tous $q > p \geq n_0$ et tout $z \in r\Delta = \{z \in \mathbb{C};\ |z| < r\}$, on a :

$$|\theta_p(z) - \theta_q(z)| \leq \frac{|z|^{2^{n_0+1}}}{(1-|z|)^2} \leq \frac{r^{2^{n_0+1}}}{(1-r)^2} < \varepsilon.$$

Autrement dit, $(\theta_n)_n$ est uniformément convergente vers θ sur $r\Delta$. Comme pour tout n, θ_n est holomorphe sur $r\Delta$, la fonction θ est elle-même holomorphe sur $r\Delta$. Ceci est valable pour tout $r < 1$ donc la fonction θ est holomorphe sur Δ.

2.a. Fixons $z \in \Delta$ et $n \in \mathbb{N}$. On a

$$\theta_n(z^2) = \prod_{k=0}^{n}(1-(z^2)^{2^k}) = \prod_{k=0}^{n}(1-z^{2^{k+1}}) = \prod_{k=1}^{n+1}(1-z^{2^k})$$

(on a effectué le changement d'indice $k+1 \to k$).

Donc, $(1-z)\theta_n(z^2) = \prod_{k=0}^{n+1}(1-z^{2^k}) = \theta_{n+1}(z)$. En passant à la limite quand n tend vers $+\infty$, on obtient : $(1-z)\theta(z^2) = \theta(z)$.

2.b. Supposons que $\theta(z) = 0$, où $z \in \Delta$ (en particulier $z \neq 1$). On a d'après 2.a, $\theta(z^2) = 0$. Par une récurrence immédiate, pour tout $p \in \mathbb{N}$, z^{2^p} est zéro de θ. Comme $(z^{2^p})_p$ converge vers 0 (car $|z| < 1$), on a $\theta(0) = 0$ par continuité de θ. Or $\theta_n(0) = 1$ pour tout n, a fortiori, $\theta(0) = 1$. On a une contradiction donc θ ne s'annule pas sur Δ.

2.c. Comme θ ne s'annule pas sur Δ, on peut définir $h(z) = \dfrac{f(z)}{\theta(z)}$ pour $z \in \Delta$.

On a pour $z \in \Delta$, $h(z^2) = \dfrac{f(z^2)}{\theta(z^2)} = \dfrac{f(z)}{\theta(z)} = h(z)$. Par une récurrence immédiate, pour tout $p \in \mathbb{N}$, $h(z) = h(z^{2^p})$. Comme f est continue sur Δ, h est continue sur Δ et par passage à la limite sur p, on obtient $h(z) = h(0)$. En posant $\lambda = h(0)$, on a $h(z) = \lambda$ ie $f(z) = \lambda\theta(z)$.

3.a. Pour $t \in \Pi$, on a $|e^t| = e^{Re(t)} < 1$ car $Re(t) < 0$. De plus, θ ne s'annule pas sur Δ et ϕ est bien définie. Comme θ est holomorphe sur Δ, θ' aussi. Comme θ ne s'annule pas sur Δ, $\dfrac{1}{\theta}$ est aussi holomorphe sur Δ. Enfin, l'application $\Pi \to \Delta\ :\ t \mapsto e^t$ est holomorphe. On conclut que ϕ est holomorphe sur Π.

3.b. Remarquons que $t \in \Pi$ si et seulement si $2t \in \Pi$.

D'après 2.a, on a avec $z = e^t$, $(1-e^t).\theta(e^{2t}) = \theta(e^t)$. En dérivant cette relation, il vient $2e^{2t}(1-e^t)\theta'(e^{2t}) - e^t\theta(e^{2t}) = e^t.\theta'(e^t)$. Puis en divisant par $(1-e^t)\theta(e^{2t})$, on obtient

$$2e^{2t}\frac{\theta'(e^{2t})}{\theta(e^{2t})} - \frac{e^t}{(1-e^t)} = e^t \cdot \frac{\theta'(e^t)}{(1-e^t)\theta(e^{2t})} = e^t \cdot \frac{\theta'(e^t)}{\theta(e^t)}.$$

Finalement, cela s'écrit $2\phi(2t) + \dfrac{e^t}{(e^t-1)} = \phi(t)$.

3.c. Pour tout $k \in \mathbb{N}$, on pose
(H_k) $\forall t \in \Pi,\ \phi^{(k)}(t) = 2^{k+1}\phi^{(k)}(2t) + S_k(e^t)$ avec $S_{k+1}(z) = z.S_k'(z)$ où $S_k \in \mathbb{C}(z)$.

Pour $k = 0$, on définit $S_0(z) = \dfrac{z}{(z-1)}$ et 3.b montre que (H_0) est vraie.

Supposons que (H_k) soit vraie et dérivons (H_k). Il vient pour $t \in \Pi$,

$$\phi^{(k+1)}(t) = 2^{k+2}\phi^{(k+1)}(2t) + e^t.S_k'(e^t).$$

Donc (H_{k+1}) est vraie avec $S_{k+1}(z) = z.S_k'(z)$.

Par récurrence, (H_k) est vraie pour tout k.

III. Quelques résultats sur les fractions rationnelles et les polynômes.

A. *Fractions rationnelles à une indéterminée.*

1.a. Soit $R \in \mathbb{C}(z)$. Si R s'écrit $\dfrac{U}{V}$ et $\dfrac{P}{Q}$ où $U, V, P, Q \in \mathbb{C}[z]$ (Q, V non nuls), on a $UQ = VP$. On note $\deg(U)$ le degré de U. En égalant les degrés, il vient $\deg(U)+\deg(Q) = \deg(V)+\deg(P)$. Donc $\deg(U)-\deg(V) = \deg(P)-\deg(Q)$. Ainsi $\deg(R)$ est indépendant du choix du représentant $\dfrac{P}{Q}$ de R.

Soient $R, S \in \mathbb{C}(z)$. On pose $R = \dfrac{U}{V}$ et $S = \dfrac{P}{Q}$. On a $R + S = \dfrac{UQ+VP}{QV}$. On a donc

$$\deg(R+S) = \deg(UQ+VP) - \deg(QV) = \deg(UQ+VP) - \deg(Q) - \deg(V).$$

Pour fixer les idées, supposons que $\deg(R) = \max\{\deg(R), \deg(S)\}$. On a donc $\deg(U) - \deg(V) \geq \deg(P) - \deg(Q)$ soit $\deg(UQ) \geq \deg(VP)$. Ainsi, on a $\deg(UQ+VP) \leq \max\{\deg(UQ), \deg(VP)\} = \deg(UQ)$. D'où :

$$\begin{array}{rcl} \deg(R+S) & \leq & \deg(UQ) - \deg(Q) - \deg(V) \\ & = & \deg(U) + \deg(Q) - \deg(Q) - \deg(V) \\ & = & \deg(U) - \deg(V) = \deg(R) \\ & = & \max\{\deg(R), \deg(S)\}. \end{array}$$

1.b. On sait que $\mathbb{C}(z)$ est un $\mathbb{C}$-espace vectoriel.

Soient $\lambda \in \mathbb{C}$ et $F = \dfrac{P}{Q} \in \mathbb{C}_0(z)$. On a $\lambda F = \dfrac{\lambda P}{Q}$ et $\deg(\lambda F) = \deg(\lambda P) - \deg(Q) \leq \deg(P) - \deg(Q) = \deg(F) \leq 0$. Ainsi $\lambda F \in \mathbb{C}_0(z)$.

Soient $R, S \in \mathbb{C}_0(z)$. D'après 1.a, $\deg(R+S) \leq \max\{\deg(R), \deg(S)\} \leq 0$. Donc $R + S \in \mathbb{C}_0(z)$.

On conclut que $\mathbb{C}_0(z)$ est un sous-espace vectoriel de $\mathbb{C}(z)$.

Pour tout $\gamma \in \mathbb{C}$ et $n \in \mathbb{N}$, on a $\deg\Big(\dfrac{1}{(z-\gamma)^n}\Big) = -n \leq 0$ donc V et W sont inclus dans $\mathbb{C}_0(z)$. Par définition, V et W sont des $\mathbb{C}$-espaces vectoriels pour la même structure d'espace vectoriel (l'addition interne et la multiplication par un scalaire) que $\mathbb{C}_0(z)$. Ainsi, V et W sont des sous-espaces vectoriels de $\mathbb{C}_0(z)$.

1.c. Il suffit d'invoquer l'existence et l'unicité de la décomposition en éléments simples, compte-tenu que, ici, la partie entière est réduite aux polynômes constants.

2. D'après 1.c, pour tout $F \in \mathbb{C}_0(z)$, il existe $\lambda \in \mathbb{C}$ et une famille $(b_{\gamma,n})_{\gamma,n}$ presque nulle telle que

$$F = \lambda + \sum_{\substack{\gamma\in\mathbb{C}\\ n\geq 1}} \frac{b_{\gamma,n}}{(z-\gamma)^n}.$$

On note D l'opérateur de dérivation de $\mathbb{C}_0(z)$ dans $\mathbb{C}(z)$. On a alors

$$D(F) = F' = \sum_{\substack{\gamma\in\mathbb{C}\\ n\geq 1}} \frac{-nb_{\gamma,n}}{(z-\gamma)^{n+1}} \in W.$$

Donc $\mathrm{Im}(D) \subset W$.

Réciproquement, pour tout $w \in W$, on a $w = \displaystyle\sum_{\substack{\gamma\in\mathbb{C}\\ n\geq 2}} \frac{b_{\gamma,n}}{(z-\gamma)^n} = D(F)$ avec

$F = \displaystyle\sum_{\substack{\gamma\in\mathbb{C}\\ n\geq 2}} \frac{-b_{\gamma,n}}{(n-1)(z-\gamma)^{n-1}} \in \mathbb{C}_0(z)$.

Finalement, $\mathrm{Im}(D) = W$.

3. L'application μ est linéaire donc il suffit de vérifier que $\mu(v) \in V$ quand v décrit une partie génératrice de V. Ainsi, pour $v = \dfrac{1}{(z-\gamma)}$ où $\gamma \in \mathbb{C}$, il existe $a \in \mathbb{C}$ tel que $\gamma = a^2$ et on a alors

$$\mu(v)(z) = z\frac{1}{(z^2-\gamma)} = z\frac{1}{(z^2-a^2)} = \frac{1}{2}\Big(\frac{1}{(z-a)} + \frac{1}{(z+a)}\Big) \in V.$$

Donc V est stable par μ.

Pour $w \in W$, d'après 2, il existe $F \in \mathbb{C}_0(z)$ telle que $w = D(F)$. On a alors $\mu(w)(z) = zF'(z^2) = \dfrac{1}{2}(F(z^2))' \in \mathrm{Im}(D) = W$ car $F(z^2) \in \mathbb{C}_0(z)$. Donc W est stable par μ.

4. Ici la partie entière est nulle car le degré de R est strictement négatif.

$$R(z) = \sum_{k=1}^{n} \frac{r(a,k)}{(z-a)^k} + \sum_{k=1}^{n} \frac{r(-a,k)}{(z+a)^k}.$$

En multipliant cette relation par $(z-a)^n$, il vient

$$\frac{1}{(z+a)^n} = (z-a)^n R(z) = \sum_{k=1}^{n} r(a,k)(z-a)^{n-k} + \sum_{k=1}^{n} \frac{r(-a,k).(z-a)^n}{(z+a)^k}.$$

En prenant la valeur $z = a$, on a finalement

$$r(a,n) = \frac{1}{(2a)^n}.$$

B. *Polynômes à* $(n+1)$ *indéterminées.*

1. *Ordre sur* $\mathbb{N}^{n+1}$.

Il s'agit de l'ordre lexicographique lorsqu'on écrit de droite à gauche.

1.a. Montrons cela par récurrence sur n. Pour $n = 0$, c'est l'ordre usuel sur $\mathbb{N}$.

Supposons que $\mathcal{R}_n$ soit une relation d'ordre sur $\mathbb{N}^{n+1}$. Soit $\alpha \in \mathbb{N}^{n+2}$. On a bien sûr $\alpha_{n+1} = \alpha_{n+1}$ et $(\alpha_0,\dots,\alpha_n)\mathcal{R}_n(\alpha_0,\dots,\alpha_n)$ car $\mathcal{R}_n$ est réflexive par hypothèse de récurrence. Ainsi $(\alpha_0,\dots,\alpha_{n+1})\mathcal{R}_{n+1}(\alpha_0,\dots,\alpha_{n+1})$ donc $\mathcal{R}_{n+1}$ est elle-même réflexive.

Soient $\alpha,\beta \in \mathbb{N}^{n+2}$ tels que $\alpha\mathcal{R}_{n+1}\beta$ et $\beta\mathcal{R}_{n+1}\alpha$. Comme $\alpha\mathcal{R}_{n+1}\beta$, on a $\alpha_{n+1} \leq \beta_{n+1}$. De même, $\beta\mathcal{R}_{n+1}\alpha$ donc $\beta_{n+1} \leq \alpha_{n+1}$. Ainsi, $\alpha_{n+1} = \beta_{n+1}$. On a donc $(\alpha_0,\dots,\alpha_n)\mathcal{R}_n(\beta_0,\dots,\beta_n)$ et $(\beta_0,\dots,\beta_n)\mathcal{R}_n(\alpha_0,\dots,\alpha_n)$. Comme $\mathcal{R}_n$ est antisymétrique, on a $(\beta_0,\dots,\beta_n) = (\alpha_0,\dots,\alpha_n)$. Finalement, $\alpha = \beta$ donc $\mathcal{R}_{n+1}$ est antisymétrique.

Soient $\alpha,\beta,\gamma \in \mathbb{N}^{n+2}$ tels que $\alpha\mathcal{R}_{n+1}\beta$ et $\beta\mathcal{R}_{n+1}\gamma$. En particulier, on a $\alpha_{n+1} \leq \beta_{n+1}$ et $\beta_{n+1} \leq \gamma_{n+1}$. Si $\alpha_{n+1} < \gamma_{n+1}$ alors $\alpha\mathcal{R}_{n+1}\gamma$. Sinon, on a $\alpha_{n+1} = \beta_{n+1} = \gamma_{n+1}$ donc on a les relations $(\alpha_0,\dots,\alpha_n)\mathcal{R}_n(\beta_0,\dots,\beta_n)$ et $(\beta_0,\dots,\beta_n)\mathcal{R}_n(\gamma_0,\dots,\gamma_n)$. Comme $\mathcal{R}_n$ est transitive, on en déduit alors que $(\alpha_0,\dots,\alpha_n)\mathcal{R}_n(\gamma_0,\dots,\gamma_n)$ donc $\alpha\mathcal{R}_{n+1}\gamma$ et $\mathcal{R}_{n+1}$ est transitive.

Finalement, $\mathcal{R}_{n+1}$ est une relation d'ordre et par récurrence, pour tout entier n, $\mathcal{R}_n$ est une relation d'ordre.

1.b. Là encore, on raisonne par récurrence sur n. Soit donc à $n \in \mathbb{N}$ fixé,

(H_n) Tout ensemble non vide $E \subset \mathbb{N}^{n+1}$ admet un plus petit élément.

Pour $n = 0$, il s'agit d'un des axiomes de Peano qui caractérisent $\mathbb{N}$ donc (H_0) est vraie.

Supposons (H_n) vraie et fixons $E \subset \mathbb{N}^{n+2}$. Comme E est non vide, on peut définir

$$\alpha_{n+1} = \min\{a \in \mathbb{N};\ \exists a_0,\dots,a_n \in \mathbb{N},\ (a_0,\dots,a_n,a) \in E\}$$

et

$$E' = \{(a_0,\dots,a_n) \in \mathbb{N}^{n+1};\ (a_0,\dots,a_n,\alpha_{n+1}) \in E\}.$$

E' est une partie non vide de $\mathbb{N}^{n+1}$ (par définition de α_{n+1}) donc d'après (H_n), admet un minimum $(\alpha_0,\dots,\alpha_n)$. On pose $\alpha = (\alpha_0,\dots,\alpha_n,\alpha_{n+1})$. Pour tout $\beta \in E$, on a par définition de α_{n+1}, $\beta_{n+1} \geq \alpha_{n+1}$. Si $\beta_{n+1} > \alpha_{n+1}$, $\alpha\mathcal{R}_{n+1}\beta$. Sinon $\beta_{n+1} = \alpha_{n+1}$ et $(\beta_0,\dots,\beta_n) \in E'$ donc par définition de $(\alpha_0,\dots,\alpha_n)$, on a $(\alpha_0,\dots,\alpha_n)\mathcal{R}_n(\beta_0,\dots,\beta_n)$ soit $\alpha\mathcal{R}_{n+1}\beta$.

Donc α est le plus petit élément de E et (H_{n+1}) est vraie.

Par récurrence, (H_n) est vraie pour tout $n \in \mathbb{N}$.

1.c. Soient $\alpha, \beta \in \mathbb{N}^{n+1}$, on définit $E = \{\alpha, \beta\}$ qui est non vide donc admet un plus petit élément d'après 1.b. Il s'agit de α ou β donc $\alpha \mathcal{R}_n \beta$ ou $\beta \mathcal{R}_n \alpha$. La relation $\mathcal{R}_n$ est donc totale.

1.d. Ceci se démontre une fois de plus par récurrence. Soit donc à $n \in \mathbb{N}$ fixé,

(H_n) Tout ensemble fini non vide $E \subset \mathbb{N}^{n+1}$ admet un plus grand élément.

Pour $n = 0$, il s'agit d'un des axiomes de Peano donc (H_0) est vraie.

Supposons (H_n) vraie et fixons $E \subset \mathbb{N}^{n+2}$ fini. Comme E est non vide et fini, on peut définir

$$\alpha_{n+1} = \max\{a \in \mathbb{N};\ \exists a_0, \dots, a_n \in \mathbb{N},\ (a_0, \dots, a_n, a) \in E\}$$

et

$$E' = \{(a_0, \dots, a_n) \in \mathbb{N}^{n+1};\ (a_0, \dots, a_n, \alpha_{n+1}) \in E\}.$$

E' est une partie finie non vide de $\mathbb{N}^{n+1}$ (par définition de α_{n+1}) donc d'après (H_n), admet un maximum $(\alpha_0, \dots, \alpha_n)$. On montre exactement comme en 1.b (en remplaçant min par max) que $(\alpha_0, \dots, \alpha_n, \alpha_{n+1})$ est le maximum de E.

On pouvait aussi utiliser la question précédente. On raisonne alors par récurrence sur le cardinal. Soit E non vide fini, $E = (a_1, \dots, a_c)$ où $c =$card E. Soit $E' = (a_1, \dots, a_{c-1})$ et $m = \max E'$ (par hypothèse de récurrence) et $\max E = \max\{a_c, m\}$ qui existe car $\mathcal{R}_n$ est totale (le maximum de deux éléments distincts est celui qui n'est pas le minimum !).

2.a. Soient $P, Q \in \mathbb{K}[X_0, X_1, \dots, X_n]$, non nuls, on définit : $R = p_\delta Q - q_\delta P$. Si R est non nul, on peut définir $d = d(R)$. Le coefficient de X^δ dans R est nul donc $d \neq \delta$.

Si $\delta \mathcal{R}_n d$, en identifiant les coefficients de X^d dans la relation $Q = p_\delta^{-1}(R + -q_\delta P)$ (par définition $p_\delta \neq 0$), on obtient, comme $\delta \neq d : 0 = p_\delta^{-1} r_d \neq 0$. Cette impossibilité montre que $\delta \mathcal{R}_n d$ est faux soit $d \mathcal{R}_n \delta$ (car $\mathcal{R}_n$ est totale).

Ainsi, si $p_\delta Q - q_\delta P$ est non nul, $\delta \neq d(p_\delta Q - q_\delta P)$ et $d(p_\delta Q - q_\delta P) \mathcal{R}_n \delta$.

2.b. On considère l'ensemble $E = \big\{d(P);\ P \in J \setminus \{0\}\big\}$. L'ensemble E est une partie non vide (car $J \neq \{0\}$) de $\mathbb{N}^{n+1}$ donc admet un plus petit élément d d'après 1.b. Par définition, il existe $M \in J \setminus \{0\}$ tel que $d = d(M)$. Soit $P \in J \setminus \{0\}$, si $d(P) \mathcal{R}_n d(M)$ alors $d(P) = d(M)$ par définition de $d = d(M)$. Soit $R = m_d P - p_d M$, on a alors d'après 2.a, $R = 0$ ou $d(R) \mathcal{R}_n d(M)$ et $d(R) \neq d(M)$. Mais la seconde éventualité est impossible par définition de $d(M) = d$. Ainsi $R = 0$ ie $P = m_d^{-1} p_d M$. Finalement, $P = cM$ où $c \in \mathbb{K}$.

3. Pour $j \in \{0, \cdots, n\}$, on définit

$$d_j = \max\Big\{a_j \in \mathbb{N};\ \exists (a_i)_{i \neq j} \in \mathbb{N}^n,\ \text{pour } a = (a_0, \dots, a_n), p_a \neq 0\Big\}.$$

Comme P n'est pas constant, il existe $j \in \{0, \cdots, n\}$ tel que $d_j \geq 1$. Soit

$$i = (d_0, \dots, d_{j-1}, d_j - 1, d_{j+1}, \dots, d_n)$$

On a alors $\dfrac{\partial^i P}{\partial X^i} = \displaystyle\sum_\alpha p_\alpha \frac{\partial^i X^\alpha}{\partial X^i}$ or

$$\frac{\partial^i X^\alpha}{\partial X^i} = \Big(\prod_{\substack{0 \leq k \leq n \\ k \neq j}} \frac{\partial^{d_k} X_k^{\alpha_k}}{\partial X_k^{d_k}} \Big) \frac{\partial^{d_j - 1} X_j^{\alpha_j}}{\partial X_j^{d_j - 1}}$$

où $\dfrac{\partial^{d_k} X_k^{\alpha_k}}{\partial X_k^{d_k}} = c_{\alpha_k} \in \mathbb{K}$ pour $k \neq j$; $\dfrac{\partial^{d_j-1} X_j^{\alpha_j}}{\partial X_j^{d_j-1}} = c_{\alpha_j} \in \mathbb{K}$ si $\alpha_j \leq d_j - 1$ et $\dfrac{\partial^{d_j-1} X_j^{\alpha_j}}{\partial X_j^{d_j-1}} = c_{\alpha_j} X_j \neq 0$ si $\alpha_j = d_j$.

On a donc le résultat demandé.

IV. On se propose de montrer que la fonction θ définie à la question II.1.c ne vérifie pas d'équation différentielle algébrique sur $\mathbb{C}(z)$.

1.a. On raisonne par récurrence sur $k \geq 1$. Pour $k = 1$, on a $\dfrac{\theta'}{\theta} = g = Q_1(g)$ où $Q_1(Z_0) = Z_0$. Donc c'est vrai pour $k = 1$.

Supposons que le résultat soit vrai pour un entier $k \in \mathbb{N}$, $k \geq 1$, où on peut écrire $Q_k = Z_{k-1} + R_k(Z_0, \ldots, Z_{k-2})$. En dérivant $\theta^{(k)}$, il vient :

$$\theta^{(k+1)} = \theta' Q_k(g, \ldots, g^{(k-1)}) + \theta . \sum_{p=0}^{k-1} g^{(p+1)} \frac{\partial Q_k}{\partial Z_p}(g, \ldots, g^{(k-1)}).$$

On remarque que $\theta' = \theta.g$. On en déduit que $\theta^{(k+1)} = \theta Q_{k+1}(g, \ldots, g^{(k)})$ avec $Q_{k+1} = Z_k + Z_0 Q_k + \sum_{p=0}^{k-2} Z_{p+1} \dfrac{\partial R_k}{\partial Z_p}$. Le multidegré de Q_{k+1} est $(0, \ldots, 0, 1)$ et son coefficient dominant est 1. Le résultat est donc vrai au rang $k + 1$.

Par récurrence, le résultat est vrai pour tout $k \geq 1$.

1.b. Comme H est non nul, on peut considérer son multidegré $d(H) = \delta$. On pose $\delta = (\delta_0, \ldots, \delta_n)$. On note $r < s$ pour $r \mathcal{R}_{n-1} s$ et $r \neq s$. On peut écrire

$$H = \sum_a h_a T_0^a T_1^{\delta_1} \ldots T_n^{\delta_n} + \sum_{\substack{(\alpha_1, \ldots, \alpha_n) \\ (\alpha_1, \ldots, \alpha_n) < (\delta_1, \ldots, \delta_n)}} h_{(\alpha_0, \ldots, \alpha_n)} T_0^{\alpha_0} T_1^{\alpha_1} \ldots T_n^{\alpha_n}.$$

Par hypothèse, le polynôme H est homogène donc la première somme est réduite à $h_\delta T_0^{\delta_0} T_1^{\delta_1} \ldots T_n^{\delta_n}$. On a

$$H(1, Q_1, \ldots, Q_n) = h_\delta Q_1^{\delta_1} \ldots Q_n^{\delta_n} + \sum_{\substack{(\alpha_0, \ldots, \alpha_n) \\ (\alpha_1, \ldots, \alpha_n) < (\delta_1, \ldots, \delta_n)}} h_{(\alpha_0, \ldots, \alpha_n)} Q_1^{\alpha_1} \ldots Q_n^{\alpha_n}.$$

Si tous les δ_i sont nuls pour $i \geq 1$, $H = h T_0^{\delta_0}$ où $h \neq 0$. On a alors $H(1, Q_1, \ldots, Q_n) = h \neq 0$.

Sinon, on peut définir $j = \max\{k \geq 1 ;\ \delta_k \neq 0\}$. D'après la question 1.a,

$$Q_1^{\delta_1} \ldots Q_n^{\delta_n} = Q_1^{\delta_1} \ldots Q_j^{\delta_j} = Z_1^{\delta_1} \ldots Z_j^{\delta_j} + R(Z_1, \ldots, Z_{j-1})$$

où $d(R)$ est de la forme $(r_1, \ldots, r_j, 0, \ldots, 0)$ avec $r_j < \delta_j$. Donc

$$H(1, Q_1, \ldots, Q_n) = h_\delta Z_1^{\delta_1} \ldots Z_j^{\delta_j} + R_H(Z_1, \ldots, Z_n) \quad \text{avec } d(R_H) < \delta.$$

Donc $H(1, Q_1, \ldots, Q_n) \neq 0$.

2. L'hypothèse de l'énoncé nous permet de considérer un entier n tel qu'il existe $P \in \mathbb{C}(z)[Z_0, Z_1, \ldots, Z_n]$, non nul vérifiant $P(\theta, \ldots, \theta^{(n)}) = 0$. Cela s'écrit, en notant $|(\alpha_0, \ldots, \alpha_n)| = \alpha_0 + \ldots + \alpha_n$ et N le degré total de P (autrement dit le plus grand $|\alpha|$ tel que $p_\alpha \neq 0$) :

$$\sum_{j=0}^{N} \theta^j \sum_{|\alpha|=j} p_\alpha Q_1^{\alpha_1}(g) \ldots Q_n^{\alpha_n}(g, \ldots, g^{(n-1)}) = 0.$$

Notons $A_j = \sum_{|\alpha|=j} p_\alpha Q_1^{\alpha_1}(Z_0) \ldots Q_n^{\alpha_n}(Z_0, \ldots, Z_{n-1})$ et $a_j = A_j(g, \ldots, g^{(n-1)})$.

D'après la question 1.b, on remarque que A_j est non nul dès que le polynôme homogène $\sum_{|\alpha|=j} p_\alpha T_1^{\alpha_1} \ldots T_n^{\alpha_n}$ est non nul.

On a l'équation algébrique (ordinaire) sur le corps $\mathbb{K}_n = \mathbb{C}(z)(g, \ldots, g^{(n-1)})$

$$(E) \qquad \sum_{j=0}^{N} a_j \theta^j = 0.$$

avec $a_j = A_j(g, \ldots, g^{(n-1)})$ où $A_j \in \mathbb{C}(z)[Z_0, Z_1, \ldots, Z_n]$.

On considère d le plus petit entier N vérifiant une relation de type (E) avec $a_j \in \mathbb{K}$ où $\mathbb{K} = \mathbb{K}_\infty$ est le corps $\mathbb{C}(z)(g, g', g'', \ldots)$ (en fait on veut la clôture par dérivation de $\mathbb{K}_n$).

Si $d = 0$, on a $a_0 = 0$ et A_0 est non nul donc le résultat est démontré.

Sinon, par définition de d, on a $a_d \neq 0$ donc quitte à diviser par a_d, on peut supposer $a_d = 1$. En fait, quitte à tout multiplier par un élément convenable de $\mathbb{C}(z)[g, g', \ldots]$, on peut supposer $a_j \in \mathbb{C}(z)[g, g', \ldots]$. De plus, on peut choisir m minimal pour que tous les a_j s'écrivent $A_j(g, \ldots, g^{(m-1)})$ où $A_j \in \mathbb{C}(z)[Z_0, Z_1, \ldots, Z_{m-1}]$.

En dérivant la relation (E), on obtient

$$\sum_{j=1}^{d} \Big(j a_j \theta^{j-1} \theta' + a_j' \theta^j \Big) = 0.$$

Comme $\theta' = g\theta$, on obtient :

$$(E') \qquad \sum_{j=0}^{d} (j a_j g + a_j') \theta^j = 0.$$

On opère $(E') - dg \times (E)$ et on obtient l'équation algébrique suivante qui est encore à coefficients dans $\mathbb{K}$

$$\sum_{j=0}^{d-1} ((j-d) a_j g + a_j') \theta^j = 0.$$

Par définition de la minimalité de d, pour tout $j \in \{0,\dots,d-1\}$, on a nécessairement $(j-d)a_j g + a_j' = 0$. Ainsi, pour tout $j \in \{0,\dots,d-1\}$, on a $B_j(g,\dots,g^{(m)}) = 0$ avec $B_j = (j-d)Z_0 A_j + \sum_{p=0}^{m-1} Z_{p+1}\cdot\frac{\partial A_j}{\partial Z_p} + A_j'$, où A_j' signifie clairement que l'on dérive les coefficients de A_j (qui sont dans $\mathbb{C}(z)$).

Pour conclure, il suffit donc de montrer qu'il existe $j \in \{0,\dots,d-1\}$ tel que B_j est non nul. Or le coefficient dominant de B_j en Z_m vaut $\frac{\partial A_j}{\partial Z_{m-1}}$ car les polynômes A_i ($i \leq d-1$) n'ont aucun terme en Z_m d'après 1.a.

Si le degré partiel en Z_{m-1} de tous les polynômes A_i non nuls ($i \leq d-1$) est nul alors ceci contredit la minimalité de m. On conclut donc qu'il existe $i \leq d-1$ tel que le degré partiel en Z_{m-1} de A_i est non nul ie $\frac{\partial A_i}{\partial Z_{m-1}}$ est non nul donc B_i est non nul. Ceci achève la démonstration du résultat demandé.

3. Comme $g(e^t) = e^{-t}\phi(e^t)$, une récurrence immédiate donne pour tout entier j : $g^{(j)} \circ \exp = A_j(\phi,\dots,\phi^{(j)})$ où $A_j \in \mathbb{L}[Z_0,Z_1,\dots,Z_j]$ et le coefficient dominant de A_j en Z_j est $\exp^{-j-1}$.

Si $B(g,\dots,g^{(n)}) = 0$ où $B \in \mathbb{C}(z)[Z_0,Z_1,\dots,Z_n]$ est non nul, on a alors $\tilde{B}(\phi,\dots,\phi^{(n)}) = 0$ où $\tilde{B} \in \mathbb{L}[Z_0,Z_1,\dots,Z_n]$. En notant $\delta = d(B)$, on a $d(\tilde{B}) = \delta$ et $\tilde{B}_\delta = B_\delta(\exp)^{-D} \neq 0$ où $D = \sum_j (j+1)\delta_j$ donc $\tilde{B}$ est non nul.

ϕ vérifie donc une équation différentielle algébrique sur $\mathbb{L}$.

4. On considère l'ensemble $J = \{Q \in \mathbb{L}[X_0,\dots,X_n];\ Q(\phi,\dots,\phi^{(n)}) = 0\}$ où n est tel qu'il existe $B \in \mathbb{L}[Z_0,Z_1,\dots,Z_n]$ non nul avec $B(\phi,\dots,\phi^{(n)}) = 0$.

J est clairement un idéal non réduit à $\{0\}$. D'après III.B.2.b, il existe $M \in J \setminus \{0\}$ tel que pour tout $P \in J \setminus \{0\}$, $d(P)\mathcal{R}_n d(M)$ implique l'existence de $c \in \mathbb{L}$ tel que $P = cM$. M est non constant car un polynôme constant de J est nécessairement nul.

On considère alors $P = M^*\Big(\frac{1}{2}(X_0 - R_0),\dots,\frac{1}{2^{n+1}}(X_n - R_n)\Big)$. Pour tout $t \in \Pi$, on a

$$\begin{aligned} P(\phi,\dots,\phi^{(n)})(t) &= M^*\Big(\frac{1}{2}(\phi - R_0),\dots,\frac{1}{2^{n+1}}(\phi^{(n)} - R_n)\Big)(t) \\ &= M(\phi,\dots,\phi^{(n)})(2t) = 0 \end{aligned}$$

car pour tout j et tout $t \in \Pi$, on a $\frac{1}{2^{j+1}}\big(\phi^{(j)}(t) - R_j(t)\big) = \phi^{(j)}(2t)$ (cf. II.3.c).

Ainsi $P \in J \setminus \{0\}$ et clairement $d(P)\mathcal{R}_n d(M)$. La définition de M implique l'existence de $\lambda \in \mathbb{L}$ tel que $P = \lambda M$ ie

$$M^*\Big(\frac{1}{2}(X_0 - R_0),\dots,\frac{1}{2^{n+1}}(X_n - R_n)\Big) = \lambda M.$$

5.a. Comme $M \notin \mathbb{L}$, d'après la question III.B.3, il existe $(i_0,\dots,i_n)$ tel que $U = \frac{\partial^{|i|} M}{\partial X_0^{i_0}\dots\partial X_n^{i_n}}$ soit affine et non constant (on rappelle que $|i| = i_0+\dots+i_n$). On a alors

$$\lambda U = \frac{\partial^{|i|}}{\partial X_0^{i_0}\dots\partial X_n^{i_n}}\Big(M^*\big(\frac{1}{2}(X_0 - R_0),\dots,\frac{1}{2^{n+1}}(X_n - R_n)\big)\Big).$$

Or

$$\frac{\partial^j}{\partial X_s^j}\Big(M^*\big(\frac{1}{2}(X_0-R_0),\dots,\frac{1}{2^{n+1}}(X_n-R_n)\big)\Big)$$
$$=\frac{1}{2^{j(s+1)}}\cdot\Big(\frac{\partial^j M}{\partial X_s^j}\Big)^*\Big(\frac{1}{2}(X_0-R_0),\dots,\frac{1}{2^{n+1}}(X_n-R_n)\Big)$$

donc

$$\lambda U=\Big[\prod_{s=0}^{n}\frac{1}{2^{i_s(s+1)}}\Big]\cdot\Big(\frac{\partial^{|i|}M}{\partial X_0^{i_0}\dots\partial X_n^{i_n}}\Big)^*\Big(\frac{1}{2}(X_0-R_0),\dots,\frac{1}{2^{n+1}}(X_n-R_n)\Big).$$

Finalement, $U^*\Big(\frac{1}{2}(X_0-R_0),\dots,\frac{1}{2^{n+1}}(X_n-R_n)\Big)=\mu U$ où $\mu\in\mathbb{L}$.

5.b. Le polynôme U est affine donc $U=\sum_{j=0}^{n}p_jX_j+q$. La relation de la question 5.a s'écrit donc

$$\sum_{j=0}^{n}\frac{1}{2^{j+1}}p_j^*(X_j-R_j)+q^*=\mu\sum_{j=0}^{n}p_jX_j+\mu q.$$

Ainsi, pour tout $j\in\{0,\dots,n\}$, $\mu p_j=\frac{1}{2^{j+1}}p_j^*$ et

$$(E)\qquad\sum_{j=0}^{n}\frac{1}{2^{j+1}}p_j^*(-R_j)+q^*=\mu q.$$

On est amené à étudier une équation (E_a) du type $au=u^*$. On pose pour $t\in\Pi$: $u(t)=v(\exp(t))$ où $v\in M(\Delta)$. L'équation (E_a) s'écrit alors pour tout $t\in\Pi$, $av(\exp(t))=v(\exp(2t))$ soit pour tout $z\in\Delta$: $av(z)=v(z^2)$. Supposons u (donc v) non nulle, comme v est méromorphe, il existe $\alpha\in\mathbb{Z}$ tel que pour z au voisinage de zéro, on ait $v(z)=z^\alpha w(z)$ où $w(0)\neq 0$ et w holomorphe au voisinage de zéro. L'équation (E_a) sécrit alors pour z au voisinage de zéro $az^\alpha w(z)=z^{2\alpha}w(z^2)$ soit $aw(z)=z^\alpha w(z^2)$. Comme a est non nul (sinon u^* donc u est nulle), on a nécessairement (en regardant le comportement en zéro) : $\alpha=0$ et a fortiori, en $z=0$, cela donne $a=1$ (car $w(0)\neq 0$). Ainsi, pour $z\in\Delta$, $v(z)=v(z^2)=\ldots=v(z^{2^r})$ pour tout entier r. Faisant tendre r vers $+\infty$, on obtient $v(z)=v(0)$, autrement dit v donc u est constante.

Pour tout $j\in\{0,\dots,n\}$, l'équation $(E_{2^{j+1}\mu})$ donne : soit $p_j=0$, soit μ est non nul, $2^{j+1}\mu=1$ et p_j est constante. On rappelle que le cas $\mu=0$ implique $p_j=0$.

On remarque donc que si μ est nul alors tous les p_j sont nuls et U est constante ce qui est faux.

Ainsi μ est non nul et pour tout $j\in\{0,\dots,n\}$, $p_j=0$ ou $2^{j+1}\mu=1$ et p_j est constante. Il est clair qu'on ne peut avoir $2^{j+1}\mu=1$ et $2^{i+1}\mu=1$ pour i et j distincts donc tous les p_j sont nuls sauf exactement un (puisqu'ils ne sont pas tous nuls), disons pour $j=m$. On a alors $2^{m+1}\mu=1$ et pour tout $j\neq m$, $p_j=0$. De plus, p_m est constante.

L'équation (E) devient donc $2^{-(m+1)}p_m^*(-R_m)+q^*=\mu q=2^{-(m+1)}q$. On en déduit en posant $p_m=C\in\mathbb{C}$ que $R_m=2^{m+1}\big(\frac{q}{C}\big)^*-\frac{q}{C}$. Ainsi, il existe $u\in\mathbb{L}$ tel que $R_m=2^{m+1}u^*-u$.

5.c. On écrit $R_m(t) = S_m(e^t)$ et $u(t) = \mu(e^t)$ où $t \in \Pi$ et $S_m, \mu \in \mathbb{C}(z)$. Le résultat de la question précédente donne alors $S_m(e^t) = 2^{m+1}\mu(e^2t) - \mu(e^t)$. Donc pour tout $z \in \Delta$, $S_m(z) = 2^{m+1}\mu(z^2) - \mu(z)$.

6. On commence par remarquer que, comme $S_0(z) = \dfrac{z}{1-z}$, 1 est pôle simple de S_0. Puis par récurrence immédiate, 1 est pôle d'ordre $k+1$ de S_k.

μ admet donc nécessairement 1 pour pôle. Notons n l'ordre de multiplicité du pôle 1 pour μ. On peut donc écrire :

$$\mu(z) = \frac{V(z)}{(z-1)^n}.$$

où $V \in M(\Delta)$ est holomorphe au voisinage de 1 et n'admet 1 ni comme zéro ni comme pôle.

Le résultat de la question précédente donne donc

$$(P) \qquad S_m(z) = 2^{m+1}\frac{V(z^2)}{(z^2-1)^n} - \frac{V(z)}{(z-1)^n}.$$

On décompose $\dfrac{1}{(z^2-1)^n}$ en éléments simples et III.A4 donne

$$\frac{1}{(z^2-1)^n} = \frac{1}{(z-1)^n}\Big(\frac{1}{2^n} + (z-1)C(z)\Big)$$

où $C \in \mathbb{C}(z)$ et admet uniquement -1 comme pôle.

La relation (P) s'écrit alors (en posant $N(z) = V(z^2).C(z)$)

$$S_m(z) = \frac{1}{(z-1)^n}\Big(2^{m+1-n}V(z^2) - V(z) + (z-1)N(z)\Big).$$

Comme 1 est pôle d'ordre $m+1$ de S_m, on a $n = m+1$. En effet, si $n \neq m+1$, alors nécessairement $n > m+1$ et il faudrait alors que 1 soit zéro de $2^{m+1-n}V(z^2) - V(z) + (z-1)N(z)$ donc zéro de $2^{m+1-n}V(z^2) - V(z)$ ce qui imposerait $(2^{m+1-n}-1)V(1) = 0$ alors que $V(1) \neq 0$.

Comme V est holomorphe au voisinage de 1, on peut écrire $V(z) = V(1) + (z-1)h(z)$ où $h \in M(\Delta)$ est holomorphe au voisinage de 1 (donc n'admet pas 1 comme pôle). On obtient $V(z^2) - V(z) = (z-1)[(z+1)h(z^2) - h(z)]$ donc

$$S_m(z) = \frac{1}{(z-1)^m}\Big((z+1)h(z^2) - h(z) + N(z)\Big).$$

donc 1 est pôle de S_m d'ordre inférieur à m ce qui est faux.

On a donc une contradiction qui ne peut provenir que de l'hypothèse du début de question IV.2. On conclut que θ ne vérifie pas d' équation différentielle algébrique sur $\mathbb{C}(z)$.

V. Généralisation.

1.a. Pour tout entier $n \in \mathbb{N}$ et tout $z \in \Delta$ (toutes les puissances de z sont encore dans Δ), on définit $\theta_n(z) = \prod_{k=0}^{n} R(z^{2^k})$. On a $\theta_n \in H(\Delta)$ car $R \in H(\Delta)$ et $\theta_n(0) = 1$.

On écrit $R(z) = 1 + zr(z)$ où r est holomorphe sur Δ.

Fixons $\rho < 1$. Etant continue, r est en particulier bornée sur l'adhérence de $\rho\Delta$ (qui est strictement incluse dans Δ) par m_ρ. Pour tout $z \in \rho\Delta$, on a la majoration

$$|\prod_{k=0}^{n} R(z^{2^k})| \leq \prod_{k=0}^{n}(1 + |r(z)|.|z|^{2^k}) \leq \prod_{k=0}^{n}(1 + m_\rho\rho^{2^k}).$$

Comme $\rho < 1$, la suite $\Big(\prod_{k=0}^{n}(1 + m_\rho\rho^{2^k})\Big)_n$ est majorée (en fait, on a mieux : comme cette suite est croissante, puisque $(1 + m_\rho\rho^{2^k}) \geq 1$, le produit infini $\prod_{k=0}^{\infty}(1 + m_\rho\rho^{2^k})$ est convergent). En effet, en passant au log, il vient

$$0 \leq \log \prod_{k=0}^{n}(1 + m_\rho\rho^{2^k}) = \sum_{k=0}^{n} \log(1 + m_\rho\rho^{2^k}) \leq \sum_{k=0}^{n} m_\rho\rho^{2^k}$$

et le dernier terme est convergent (donc majoré) quand n tend vers $+\infty$. On a donc bien l'existence de $M_\rho \in \mathbb{R}$ tel que $\prod_{k=0}^{n}(1 + m_\rho\rho^{2^k}) \leq M_\rho$ pour tout n.

On a pour tout $z \in \rho\Delta$: $\theta_{n+1}(z) - \theta_n(z) = \Big(1 - R(z^{2^{n+1}})\Big).\prod_{k=0}^{n} R(z^{2^k})$. On en déduit la majoration

$$|\theta_{n+1}(z) - \theta_n(z)| \leq |1 - R(z^{2^{n+1}})|M_\rho \leq M_\rho|z|^{2^{n+1}}|r(z^{2^{n+1}})| \leq M_\rho m_\rho\rho^{2^{n+1}}.$$

Ainsi, la série de fonctions $\sum_n(\theta_{n+1} - \theta_n)$ converge uniformément sur $\rho\Delta$ pour tout $\rho < 1$. On en déduit que (θ_n) converge simplement vers une fonction θ sur Δ et que (θ_n) converge uniformément vers θ sur $\rho\Delta$ pour tout $\rho < 1$. En particulier θ est holomorphe sur $\rho\Delta$ pour tout $\rho < 1$ donc θ est holomorphe sur Δ.

On remarque que pour tout $z \in \Delta$, $\theta_{n+1}(z) = R(z).\theta_n(z^2)$ et $\theta_n(0) = 1$. En passant à la limite sur n, on obtient les relations $\theta(z) = R(z).\theta(z^2)$ et $\theta(0) = 1$.

Il reste à établir l'unicité de θ. On ne peut malheureusement pas raisonner comme au II.2 car R peut a priori s'annuler sur Δ. Soit T holomorphe sur Δ telle que $T(0) = 1$ et $T(z) = R(z)T(z^2)$.

En 0, θ et R sont non nulles. Par continuité, il existe $\alpha \in]0, 1[$ tel que pour tout $z \in \alpha\Delta$: $h(z) = \dfrac{T(z)}{\theta(z)}$ est définie (en particulier θ donc R est non nulle sur ce voisinage) et on a alors $h(z) = h(z^2) = \ldots = h(z^{2^r})$ puis par passage à la limite sur r vers $+\infty$: $h(z) = h(0) = 1$. Ainsi, $T(z) = \theta(z)$ sur $\alpha\Delta$. D'après

le théorème du prolongement analytique (T et θ sont holomorphes sur l'ouvert Δ et coincident sur l'ouvert $\alpha\Delta$) $T = \theta$ sur Δ. Ceci établit donc l'unicité de θ.

1.b. On raisonne par récurrence sur k. Pour $k = 0$, on dérive la relation $\theta(e^t) = R(e^t).\theta(e^{2t})$ où $t \in \Pi$ pour obtenir

$$e^t\theta'(e^t) = e^tR'(e^t).\theta(e^{2t}) + 2e^{2t}R(e^t).\theta'(e^{2t}).$$

$$\text{D'où} \quad f(t) = \frac{e^t\theta'(e^t)}{\theta(e^t)} = \frac{e^tR'(e^t)}{R(e^t)} + \frac{2e^{2t}\theta'(e^{2t})}{\theta(e^{2t})} = 2f(2t) + S_0(e^t).$$

avec $S_0(z) = \dfrac{zR'(z)}{R(z)}$.

Supposons alors que le résultat soit vrai pour $k \in \mathbb{N}$. On dérive la relation

$$f^{(k)}(t) = 2^{k+1}f^{(k)}(2t) + S_k(e^t) \qquad \text{où} \quad S_k \in \mathbb{C}(z)$$

pour obtenir

$$f^{(k+1)}(t) = 2^{k+2}f^{(k+1)}(2t) + S_{k+1}(e^t) \qquad \text{où} \quad S_{k+1}(z) = zS_k'(z).$$

Le résultat est donc vrai à l'ordre $k+1$ et par récurrence, il est vrai pour tout k.

2. On suppose qu'il existe $m \in \mathbb{N}$ tel que

$$(E_m) \qquad S_m(z) = 2^{m+1}\nu(z^2) - \nu(z) \qquad \text{où } \nu \in \mathbb{C}(z).$$

On remarque par une récurrence immédiate que S_m n'admet pas 0 comme pôle et que $S_m \in \mathbb{C}_0(z)$. La relation de récurrence sur S_k montre alors que 0 est racine de S_m (car 0 n'est ni pôle ni racine de R). Nous affirmons que ν n'admet pas 0 comme pôle.

En effet, si 0 est pôle de ν, disons d'ordre $n \geq 1$, ν s'écrit $\dfrac{1}{z^n}B(z)$ où $B(0) \neq 0$ et B est méromorphe sur Δ. On a la relation $S_m(z) = \dfrac{2^{m+1}}{z^{2n}}B(z^2) - \dfrac{1}{z^n}B(z)$. Ainsi, $\lim\limits_{z\to 0} z^{2n}S_m(z) = 2^{m+1}B(0) \neq 0$ or S_m n'admet pas 0 comme pôle. Nous avons donc une contradiction et ν n'admet pas 0 comme pôle.

Si $m = 0$, le choix $G = \nu$ convient.

Supposons que $m \geq 1$. On a $zS_{m-1}'(z) = S_m(z) = 2^{m+1}\nu(z^2) - \nu(z)$ soit

$$(*) \qquad S_{m-1}'(z) = 2^{m+1}\frac{\nu(z^2)}{z} - \frac{\nu(z)}{z}.$$

On remarque que nécessairement le degré de $\dfrac{\nu(z)}{z}$ est inférieur à -1. En effet, le degré de $\dfrac{\nu(z^2)}{z}$ est différent de celui de $\dfrac{\nu(z)}{z}$ dès que le degré de ν n'est pas 0. Comme le degré de S_{m-1}' est inférieur à -1, le degré de $\dfrac{\nu(z)}{z}$ est inférieur à -1 sauf éventuellement si le degré de ν vaut 0. Auquel cas, a posteriori, le degré de $\dfrac{\nu(z)}{z}$ est aussi inférieur à -1. Ainsi, notre affirmation est vérifiée.

On peut donc écrire (cf. III.A.1.c) $\dfrac{\nu(z)}{z} = v(z) + w(z)$ où $v \in V$ et $w \in W$.

Comme en particulier $\frac{\nu(z)}{z} \in \mathbb{C}_0(z)$, on peut opérer μ (cf. III.A.2) et on obtient la relation

$$\mu\big(\frac{\nu}{z}\big)(z) = \frac{\nu(z^2)}{z} = 2^{-(m+1)}\big(S'_{m-1}(z) + \frac{\nu(z)}{z}\big).$$

$$\text{Donc} \quad \mu(v) + \mu(w) = 2^{-(m+1)}\big(S'_{m-1} + v + w\big).$$

Par définition, $S'_{m-1} \in W$. On rappelle que V et W sont en somme directe et sont stables par μ donc

$$\mu(v) = 2^{-(m+1)}v \qquad \text{et} \qquad \mu(w) = 2^{-(m+1)}\big(S'_{m-1} + w\big).$$

En particulier, la première relation permet d'affirmer que si a est un pôle de v alors les deux racines carrées de a aussi. En particulier si $a = te^{is}$ ($0 < s \leq 2\pi$, $t > 0$) est un pôle non nul de v alors tous les complexes $t^{\frac{1}{n}}e^{\frac{is}{n}}$ aussi. Donc v admettrait une infinité de pôles, ce qui est impossible. On en déduit que $v = 0$ ou v n'admet que 0 comme pôle. Supposons v non nul, la relation $zv(z^2) = 2^{-(m+1)}v(z)$ implique que 0 est pôle d'ordre 1 de v donc $v(z) = \frac{p(z)}{z}$ où p est un polynôme qui vérifie la relation : $p(z^2) = 2^{-(m+1)}p(z)$. Le polynôme p est donc clairement nul (pour des raisons de degrés, il est constant, égal à C disons, puis $C = 2^{-(m+1)}C$ impose $C = 0$). Ainsi, $v = 0$.

On en déduit que $\frac{\nu(z)}{z} = w \in W = \mathrm{Im}D$, c'est à dire qu'il existe une fraction G (on la choisit telle que $G(0) = 0$) telle que $G'(z) = \frac{\nu(z)}{z}$. Comme 0 n'est pas pôle de $\frac{\nu(z)}{z}$, 0 n'est pas pôle de G. De plus, la relation $(*)$ devient

$$S'_{m-1}(z) = 2^m(2z\frac{\nu(z^2)}{z^2}) - \frac{\nu(z)}{z} = 2^m G(z^2)' - G'(z).$$

Par intégration, $S_{m-1}(z) = 2^m G(z^2) - G(z)$ (on rappelle que $S_{m-1}(0) = 0$) et on a l'équation (E_{m-1}).

Enfin, par récurrence, on a les équations (E_{m-1}), (E_{m-2}),...,(E_0). Le cas $m = 0$ a déjà été traité et le résultat est démontré.

3.a.

$$G(z) = E(z) + \sum_{\substack{\gamma \in \mathbb{C}^* \\ n \geq 1}} \frac{g(\gamma, n)}{(z-\gamma)^n}.$$

On commence par remarquer que la fraction $z\frac{R'}{R}$ n'admet que des pôles simples.

Fixons $\gamma = a^2$ un pôle de G et notons n (resp. N, éventuellement nul) l'ordre de multiplicité de γ (resp. a) en tant que pôle de G.

On a $G(z) = \frac{A(z)}{(z-a)^N}$ où $A \in \mathbb{C}(z)$ et $A(a) = g(a, N)$. De même, $G(z) = \frac{B(z)}{(z-\gamma)^n}$ où $B \in \mathbb{C}(z)$ et $B(\gamma) = g(\gamma, n) \neq 0$ donc $G(z^2) = \frac{B(z^2)}{(z^2-a^2)^n}$.

L'équation (E_0) devient

$$z\frac{R'(z)}{R(z)} = \frac{1}{(z-a)^n}.\frac{2B(z^2)}{(z+a)^n} - \frac{A(z)}{(z-a)^N}.$$

Si $n \geq 2$, il faut $N = n$ sinon a est pôle double de $z\dfrac{R'(z)}{R(z)}$. Ainsi a est aussi pôle de G. Finalement, si γ est pôle de G d'ordre $n \geq 2$, ses racines carrées sont aussi pôles d'ordre n. On conclut comme dans la question précédente que G aurait alors une infinité de pôles ce qui est impossible.

Finalement, $n \leq 1$, ce qu'il fallait démontrer.

3.b. Le degré de $z\dfrac{R'(z)}{R(z)}$ est négatif donc la partie entière de G est constante. En reprenant les calculs de la question précédente et compte-tenu que tous les pôles sont simples, on peut écrire pour tout a

$$z\frac{R'(z)}{R(z)} = \frac{1}{(z-a)}\Big(\frac{g(a^2,1)}{a} - g(a,1)\Big) + Q(z) \qquad \text{où } a \text{ n'est pas pôle de } Q.$$

On pose

$$\frac{R'(z)}{R(z)} = \frac{n_a}{z-a} + T(z)$$

où a n'est pas pôle de T et n_a est un entier relatif (en fait, $|n_a|$ est l'ordre de multiplicité de a comme racine ou comme pôle de R).

On a alors, en identifiant les équivalents en a :

$$n_a.a = \frac{g(a^2,1)}{a} - g(a,1)$$

et ceci est vrai pour tout a. Ceci s'écrit encore $n_a = \dfrac{g(a^2,1)}{a^2} - \dfrac{g(a,1)}{a}$ donc pour tout entier p

$$pn_a = \frac{g(a^{2^{p+1}},1)}{a^{2^{p+1}}} - \frac{g(a^{2^p},1)}{a^{2^p}} + \ldots + \frac{g(a^2,1)}{a^2} - \frac{g(a,1)}{a} = \frac{g(a^{2^{p+1}},1)}{a^{2^{p+1}}} - \frac{g(a,1)}{a}.$$

Fixons γ un pôle de G. Comme il y a un nombre fini de pôles, le raisonnement de la question 2 nous donne l'existence de p et a tels que $\gamma = a^{2^{p+1}}$ et $g(a,1)$ est nul.

Ainsi, pour tout pôle γ de G, on a $\dfrac{g(\gamma,1)}{\gamma} = q_\gamma \in \mathbb{Z}$. On peut alors écrire

$$G(z) = E + \sum_{\gamma\in\mathbb{C}^*} \frac{q_\gamma.\gamma}{z-\gamma}.$$

d'où

$$\frac{R'(z)}{R(z)} = \frac{2G(z^2) - G(z)}{z} = \frac{E}{z} + \sum_{\gamma\in\mathbb{C}^*} \frac{2q_\gamma.\gamma}{z(z^2-\gamma)} - \sum_{\gamma\in\mathbb{C}^*} \frac{q_\gamma.\gamma}{z(z-\gamma)}.$$

On remarque que $E = \lim\limits_{\infty} z\dfrac{R'(z)}{R(z)} \in \mathbb{Z}$. De plus, on a $\dfrac{\gamma}{z(z-\gamma)} = \dfrac{-1}{z} + \dfrac{1}{z-\gamma}$ et $\dfrac{\gamma}{z(z^2-\gamma)} = \dfrac{-1}{z} + \dfrac{z}{z^2-\gamma}$. La fraction $\dfrac{2G(z^2) - G(z)}{z}$ apparaît donc comme la dérivée logarithmique de $z^{E-q}\dfrac{F(z)}{F(z^2)}$ où $F(z) = \prod\limits_{\gamma\in\mathbb{C}^*} (z-\gamma)^{-q_\gamma}$ et $q = \sum\limits_{\gamma\in\mathbb{C}^*} q_\gamma$.

On obtient donc la relation $R = cz^{E-q}\dfrac{F(z)}{F(z^2)}$ où $c \in \mathbb{C}$. Comme 0 n'est ni pôle ni racine de R, $E - q = 0$. De plus, $c = R(0) = 1$. Finalement, $F(z) = R(z)F(z^2)$.

Pour utiliser l'unicité de θ (cf V.1.a) et conclure $\theta = F \in \mathbb{C}(z)$, il faut encore établir le caractère holomorphe de F sur Δ. Pour cela, il suffit de montrer que F n'admet aucun pôle dans Δ. Mais sinon, comme R n'admet aucun pôle dans Δ, les pôles dans Δ de $F(z)$ et $F(z^2)$ sont les mêmes. Mais le raisonnement du V.2 (toujours le même) montre que alors F admet une infinité de pôles dans Δ, ce qui est faux. F est donc holomorphe sur Δ et on conclut $\theta \in \mathbb{C}(z)$.

5.3 Commentaires

Le problème concerne surtout la fonction génératrice associée à la suite de Thue-Morse. Il s'agit de montrer qu'elle ne vérifie aucune équation différentielle algébrique non triviale. Ce résultat est généralisé à d'autres types de fonctions dans la dernière partie. L'épreuve est toutefois éclectique et les thèmes abordés sont : l'algèbre des polynômes à plusieurs indéterminées, leurs idéaux et leur caractère éventuellement principal, les fonctions holomorphes (de façon très élémentaire), la décomposition des fractions rationnelles en éléments simples.

Chapitre 6

Session de 1994

6.1 Sujet

6.2 Correction

Partie I. Préliminaires

1.1. Procédons par récurrence sur l'entier $l \in \mathbb{N}^*$.

Soit H_l l'énoncé suivant : si $A_1, \ldots, A_l$ sont des parties infinies de k et si P est un polynôme de $k[X_1, \ldots, X_l]$ dont la fonction associée s'annule sur $A_1 \times \ldots \times A_l$ alors P est le polynôme nul.

H_1 est vrai : un polynôme à une indéterminée qui a une infinité de racines dans k est le polynôme nul.

Supposons H_l vrai et montrons H_{l+1}. Soient $A_1, \ldots, A_{l+1}$ des parties infinies de k et soit $P \in k[X_1, \ldots, X_{l+1}]$ dont la fonction associée s'annule sur $A_1 \times \ldots \times A_{l+1}$.

On peut écrire $P = \sum_{i=0}^{d} Q_i X_{l+1}^i$ où d est un entier et où $Q_i \in k[X_1, \ldots, X_l]$ pour $0 \leq i \leq d$. On a par hypothèse :

$$\forall (x_1, \ldots, x_l, x_{l+1}) \in A_1 \times \ldots \times A_l \times A_{l+1} \quad \sum_{i=0}^{d} \widetilde{Q_i}(x_1, \ldots, x_l)\, x_{l+1}^i = 0$$

(pour $0 \leq i \leq d$, $\widetilde{Q_i}$ désigne la fonction associée à Q_i).

Fixons alors $(x_1, \ldots, x_l) \in A_1 \times \ldots \times A_l$ et considérons le polynôme :

$$R = \sum_{i=0}^{d} \widetilde{Q_i}(x_1, \ldots, x_l)\, X^i \ .$$

La fonction associée à R s'annule sur A_{l+1} qui est une partie infinie de k : le cas $l = 1$ affirme alors que R est le polynôme nul.

Ainsi, pour tout $i \in \{0, \ldots, d\}$, $\widetilde{Q_i}(x_1, \ldots, x_l) = 0$. Ceci est bien entendu valable pour tout $(x_1, \ldots, x_l) \in A_1 \times \ldots \times A_l$ et on peut alors appliquer l'hypothèse de récurrence pour obtenir : $Q_i = 0$ pour $0 \leq i \leq d$ et ceci entraine clairement la nullité de P.

1.2. Les normes sont équivalentes en dimension finie. On peut donc supposer que la topologie de k^n est celle induite par la norme $\|.\|_\infty$ où

$$\|(x_1, \ldots, x_n)\|_\infty = \sup_{1 \leq i \leq n} |x_i| \ .$$

U contient alors une boule ouverte de k^n qui est de la forme $I_1 \times \ldots \times I_n$ où I_p est un ouvert non vide de k pour $1 \leq p \leq n$ (si $k = \mathbb{R}$, I_p est un intervalle, si $k = \mathbb{C}$, I_p est un disque). La question 1. entraine que P est le polynôme nul (il est clair que les I_p sont infinis).

1.3.1. Il est clair que pour $f \in F(V)$ et pour $g \in G$, $g.f \in F(V)$. Il est également clair que pour $g \in G$, $f, h \in F(V)$ et $\lambda \in k$, $g.(\lambda f + h) = \lambda g.f + g.h$.

On définit ainsi une application $\rho : G \to L(F(V))$ par $\rho(g) : f \mapsto g.f$. Montrons que pour tous $g_1,\ g_2 \in G$, $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$.

Soient $g_1,\ g_2 \in G$, $f \in F(V)$ et $v \in V$. On a :

$$\rho(g_1)(\rho(g_2)(f))(v) = [\rho(g_2)(f)](g_1^{-1}.v) = f(g_2^{-1}.(g_1^{-1}.v) = f([g_1 g_2]^{-1}.v).$$

D'où l'assertion.

D'autre part, on a clairement, si e désigne l'élément neutre de G et si $f \in F(V)$:

$$\forall v \in V, \quad (\rho(e)(f))(v) = f(e.v) = f(v).$$

Donc $\rho(e)$ est l'application identique de $F(V)$. Ces deux derniers faits mis ensemble assurent que si $g \in G$, alors $\rho(g) \in GL(F(V))$ et $[\rho(g)]^{-1} = \rho(g^{-1})$. Le résultat en découle aussitôt.

1.3.2. Soit $g \in G$. Alors $h(g.v) = (g^{-1}.h)(v) = h(v)$ car $h \in F(V)^G$. Ainsi h est bien constant sur $\mathcal{O}_v$.

Réciproquement, soit $f \in F(V)$ constante sur toutes les G-orbites. Soit $v \in V$, f est alors constante égale à $f(v)$ sur $\mathcal{O}_v$ (car $v \in \mathcal{O}_v$). Donc pour tout $g \in G$, comme $g^{-1}.v \in \mathcal{O}_v$, on a : $(g.f)(v) = f(g^{-1}.v) = f(v)$. On a donc : $g.f = f$ pour $g \in G$ et $f \in F(V)^G$.

1.4.1. Précisons un peu l'action de μ_r sur $k[X]$.

Tout d'abord, si $P = \sum_n a_n X^n \in k[X]$ (la somme étant bien entendue finie), on a par linéarité :

$$\rho(\omega)(P) = \sum_n a_n \rho(\omega)(X^n) = \sum_n a_n \omega^n X^n = P(\omega X).$$

Pour $i \in \mathbb{N}^*$, on a alors pour $n \in \mathbb{N}$: $\rho(\omega^i)(X^n) = \omega^{in} X^n$. Ceci se montre par récurrence sur i.

C'est vrai si $i = 1$ de par la définition de $\rho(\omega)(X^n)$. Supposons le résultat vrai pour i. Soit $n \in \mathbb{N}$, alors :

$$\rho(\omega^{i+1})(X^n) = \rho(\omega)[(\rho(\omega^i)(X^n)] = \rho(\omega)(\omega^{in} X^n) = \omega^{in}\omega^n X^n = \omega^{n(i+1)} X^n.$$

Il revient au même de dire que pour $g \in \mu_r$, $\rho(g)(X^n) = g^n X^n$ et ceci entraine par linéarité que $\rho(g)(P) = \sum_n a_n g^n X^n = P(gX)$ pour $g \in \mu_r$.

Le résultat est alors clair.

1.4.2. Soit $Q \in k[X^r]$ et $g \in \mu_r$. On écrit $Q = P(X^r)$, où $P \in k[X]$. On a alors :

$$\rho(g)(Q) = Q(gX) = P(g^r X^r) = P(X^r) = Q$$

car $g^r = 1$. Donc $Q \in k[X]^{\mu_r}$.

Réciproquement, soit $Q = \sum_n a_n X^n$ un élément de $k[X]^{\mu_r}$.
On a $Q(\omega X) = Q(X)$, ce qui donne en identifiant les coefficients :

$$\forall n \in \mathbb{N}, \quad a_n(\omega^n - 1) = 0$$

Les hypothèses faites sur k et le fait que ω soit une racine primitive r -ième de 1 font que $\omega^n = 1 \iff r$ divise n. Donc, si r ne divise pas n, $a_n = 0$. Il en résulte immédiatement que $Q \in k[X^r]$.

1.5.1. Soient $g \in G$ et $(x_1, \ldots, x_n) \in k^n$. Notons $y = g^{-1}x$. Les coordonnées de y sont des fonctions linéaires des x_i. Il est alors immédiat que $P(y)$ est une

fonction polynomiale des x_i. La fonction $g.P$ est donc associée à un polynôme de $k[x_1, \ldots, x_n]$.

1.5.2. Montrons que l'orbite de v par G est $k^n \setminus \{0\}$.

Tout d'abord, comme $v \neq 0$ et que tout élément de G représente une application linéaire injective, $g.v \neq 0$ et $\mathcal{O}_v \subset k^n \setminus \{0\}$.

Donnons nous $u \in k^n$, $u \neq 0$. Soient $e_1, \ldots, e_{n-1}$, $f_1, \ldots, f_{n-1}$ des vecteurs de k^n tels que $(v, e_1, \ldots, e_{n-1})$ et $(u, f_1, \ldots, f_{n-1})$ soient des bases de k^n. Soit h l'unique application linéaire de k^n dans k^n définie par $h(v) = u$ et par $h(e_i) = f_i$ pour $1 \leq i \leq n-1$. Transformant base en base, h est bijective. Si g désigne la matrice de h dans la base canonique, alors $g \in G$ et $g.v = u$ i.e $u \in \mathcal{O}_v$.

1.5.3. Soit f une fonction polynomiale sur k^n invariante par G. Si v est un vecteur non nul de k^n, f est alors constante sur l'orbite de v par G, c'est à dire sur $k^n \setminus \{0\}$. f étant une fonction continue, elle est alors constante sur k^n. Il est d'autre part clair que les fonctions constantes sont invariantes par G, d'où le résultat.

Partie II. Polynômes et actions sur les algèbres

On remarque en toute généralité que si A est une algèbre et $f_1, \ldots, f_n$ des éléments de A, alors $k[f_1, \ldots, f_n]$ est la plus petite sous-algèbre de A qui contient les f_i.

1.1. Donnons nous une autre base $(f_i)_{1 \leq i \leq n}$ de V et notons $(Y_1, \ldots, Y_n)$ la base duale. Les X_i^0 s'expriment linéairement en fonction des Y_i ($1 \leq i \leq n$). Donc pour $1 \leq i \leq n$, $X_i^0 \in k[Y_1, \ldots, Y_n]$ qui est une sous-algèbre de A. Par conséquent, $k[X_1^0, \ldots, X_n^0] \subset k[Y_1, \ldots, Y_n]$. On a l'inclusion inverse par symétrie : $S(V)$ ne dépend pas du choix de la base de V.

1.2. Notons π ce morphisme. π est surjectif par définition de $S(V)$. Remarquons que pour $P \in k[X_1, \ldots, X_n]$ et pour $x = \sum x_i e_i \in V$, on a

$$\pi(P)(x) = \widetilde{P}(x_1, \ldots, x_n) \ ,$$

$\widetilde{P}$ désignant la fonction associée à P sur k^n. L'injectivité de π résulte alors de I.1.

1.3. Soit $(f_i)_{1 \leq i \leq n}$ une autre base de V et notons $(Y_1, \ldots, Y_n)$ la base duale associée. Pour $1 \leq i \leq n$, on peut écrire $X_i^0 = \sum_j a_j Y_j$. Pour tout $\alpha \in \mathbb{N}$, $(X_i^0)^\alpha$ est alors un polynôme homogène de degré α en les Y_j car X_i^0 est un polynôme homogène de degré 1 en les Y_j. Il en résulte que tout polynôme homogène élémentaire de degré d en les X_i^0 est également un polynôme homogène de degré d en les Y_j, puis que tout polynôme homogène de degré d en les X_i^0 (somme de polynômes homogènes élémentaires de degré d) est un polynôme homogène de degré d en les Y_j.

Par symétrie, on a aussi que tout polynôme homogène de degré d en les Y_i est un polynôme homogène de degré d en les X_j. $S(V)_d$ ne dépend pas du choix de la base de V.

2.1. Soit $g \in G$ et $f_1, f_2 \in F(V)$. Pour $v \in V$ on a alors :

$$\begin{aligned}[\rho(g)(f_1 f_2)](v) = [f_1 f_2](g^{-1}.v) &= f_1(g^{-1}.v)\, f_2(g^{-1}.v) \\ &= [\rho(g)(f_1)](v)\, [\rho(g)(f_2)](v).\end{aligned}$$

Il est d'autre part évident que $\rho(g)(1) = 1$. Donc ρ est aussi une action de G sur l'algèbre $F(V)$.

2.2. Soit $g \in G$. Pour $1 \leq i \leq n$, on remarque que $\rho(g)(X_i)$ est linéaire. En effet, si $v_1, v_2 \in V$ et si $\lambda \in k$, on a :

$$\begin{aligned}[\rho(g)(X_i)](\lambda v_1 + v_2) &= X_i(g^{-1}.(\lambda v_1 + v_2)) \\ &= X_i(\lambda g^{-1}.v_1 + g^{-1}.v_2) \\ &= \lambda X_i(g^{-1}.v_1) + X_i(g^{-1}.v_2) \\ &= \lambda[\rho(g)(X_i)](v_1) + [\rho(g)(X_i)](v_2).\end{aligned}$$

Pour $1 \leq i \leq n$, $\rho(g)(X_i)$ est alors combinaison linéaire des X_j, i.e un polynôme homogène de degré 1 en les X_j. Donc, pour $\alpha \in \mathbb{N}$, $(\rho(g)(X_i))^\alpha$ est un polynôme homogène de degré α.

Soit alors $\alpha_1, \ldots, \alpha_n$ des entiers de somme d. D'après la question précédente, on a : $\rho(g)(X_1^{\alpha_1} \ldots X_n^{\alpha_n}) = [\rho(g)(X_1)]^{\alpha_1} \ldots [\rho(g)(X_n)]^{\alpha_n}$. C'est donc un polynôme homogène de degré $\alpha_1 + \ldots + \alpha_n = d$.

Donc l'image par $\rho(g)$ d'un polynôme homogène élémentaire de degré d est dans $S(V)_d$. Comme tout élément de $S(V)_d$ est combinaison linéaire de tels polynômes, on a le résultat par linéarité de $\rho(g)$.

2.3. On sait que la somme $\displaystyle\sum_{d\geq 0} S(V)_d$ est directe.

A fortiori, $\sum_{d\geq 0} S(V)_d \cap S(V)^G$ est directe et on a aussi l'inclusion évidente

$$\bigoplus_{d\geq 0} S(V)_d \cap S(V)^G \subset S(V)^G$$

Soit alors $P \in S(V)$ invariant par G. On écrit $P = \sum_d P_d$ où $P_d \in S(V)_d$ pour tout d (la somme est finie, bien entendu).

Si $g \in G$, on a alors $\rho(g)(P) = P = \sum_d \rho(g)(P_d)$. D'après ce qui précède, $\rho(g)(P_d) \in S(V)_d$ pour tout d. Par unicité de la décomposition de P, on a alors pour tout d : $\rho(g)(P_d) = P_d$. Donc, pour tout d, $P_d \in S(V)^G$, ce qu'il fallait prouver.

Partie III. Exemples

3. Groupe spécial linéaire.

3.1. Si $r > n$ alors U_r est vide, donc ouvert.

Supposons $r \leq n$.

Pour toute matrice A à n lignes et r colonnes à coefficients dans k, on note $\Omega(A)$ l'ensemble des matrices carrées d'ordre r extraites de A (il y en a $N = C_n^r$). Les éléments de $\Omega(A)$ seront notés $\omega_1(A), \ldots, \omega_N(A)$.

Fixons une base e de V.

Considérons l'application $\varphi : V^r \to \mathbb{R}$ définie de la manière suivante. Si $(v_1, \ldots, v_r) \in V^r$, on note $M = Mat_e(v_1, \ldots, v_r)$ et on pose :

$$\varphi(v_1, \ldots, v_r) = |\det_e(\omega_1(M))| + \ldots + |\det_e(\omega_N(M))|$$

L'application φ ainsi définie est continue (les déterminants qui interviennent sont des fonctions polynomiales des coordonnées des v_i dans la base e).

On a alors $U_r = \varphi^{-1}(\mathbb{R}_+^*)$. Image réciproque d'un ouvert par une application continue, U_r est un ouvert de V^r.

3.2. Soient $(u_1, \ldots, u_r)$ et $(v_1, \ldots, v_r)$ des éléments de U_r. On peut considérer des vecteurs de V : $u_{r+1}, \ldots, u_n$ et $v_{r+1}, \ldots, v_n$ tels que $u = (u_i)_{1 \leq i \leq n}$ et $v = (v_i)_{1 \leq i \leq n}$ soient des bases de V. Soit $M = Mat_u(v_1, \ldots, v_n)$. M est inversible. Soit h l'unique application linéaire de V dans V définie par $h(u_i) = v_i$ pour $i \leq n-1$ et $h(u_n) = \alpha v_n$ où α est un scalaire non nul à préciser. On a : $\det h = \alpha \det M$. On prend alors $\alpha = 1/\det M$ pour obtenir $\det h = 1$ et $(v_1, \ldots, v_r) = h.(u_1, \ldots, u_r)$. U_r est ainsi une orbite de G.

Il est clair que les constantes sont dans $S(V^r)^G$. Soit alors $f \in S(V^r)^G$. f est constante sur U_r. Soit ℓ cette constante. Alors $f - \ell$ s'annule sur U_r qui est un ouvert non vide de V^r. On sait alors d'après I.2. que $f - \ell$ est nul. Dont acte.

3.3.1. Soit $g \in G$ et $(v_1, \ldots, v_n) \in V^r$. On a, par définition du déterminant d'un endomorphisme :

$$\det_e(g^{-1}(v_1), \ldots, g^{-1}(v_n)) = \big(\det g^{-1}\big)\,\big(\det_e(v_1, \ldots, v_n)\big) = \det_e(v_1, \ldots, v_n)$$

c'est à dire que $(g.f)(v_1, \ldots, v_n) = f(v_1, \ldots, v_n)$ et $f \in S(V^n)^G$.

3.3.2. Soit $(v_1, \ldots, v_n) \in U_n$, $(v_1, \ldots, v_n)$ est donc une base de V. Supposons l'existence de $g \in G$ tel que $g.(v_1, \ldots, v_n) = (e_1, \ldots, e_{n-1}, \alpha e_n)$. g est alors nécessairement l'unique application linéaire définie par ses valeurs sur la base $(v_1, \ldots, v_n)$ par $g(v_i) = e_i$ si $i \leq n-1$ et par $g(v_n) = \alpha e_n$. On a alors

$$\alpha = \det_e(g(v_1), \ldots, g(v_n)) = \big(\det g\big) f(v_1, \ldots, v_n) = f(v_1, \ldots, v_n).$$

Ceci montre l'unicité, mais aussi l'existence : il suffit de définir g sur la base $(v_1, \ldots, v_n)$ par $g(v_i) = e_i$ si $i \leq n-1$ et par $g(v_n) = f(v_1, \ldots, v_n)\, e_n$. On a alors

$$f(v_1, \ldots, v_n) = \det_e(g(v_1), \ldots, g(v_n)) = \big(\det g\big) f(v_1, \ldots, v_n).$$

Donc $\det g = 1$ car $f(v_1, \ldots, v_n) \neq 0$.

On a bien entendu $k[f] \subset S(V^n)^G$. Soit alors $h \in S(V^n)^G$. Soit $(v_1, \ldots, v_n) \in U_n$. On sait que h est constant sur l'orbite de $(v_1, \ldots, v_n)$. La fonction

$$t \in k \to h(e_1, \ldots, e_{n-1}, te_n)$$

est une fonction polynomiale P de t car $h \in S(V^n)$.

On en déduit d'après ce qui précède que :

$$\begin{aligned} h(v_1, \ldots, v_n) &= h\big(g(v_1), \ldots, g(v_n)\big) \\ &= h\big(e_1, \ldots, e_{n-1}, f(e_1, \ldots, e_n)\, e_n\big) = P(f(v_1, \ldots, v_n)). \end{aligned}$$

Ainsi $h - P(f)$ s'annule sur l'ouvert non vide U_n, c'est donc le polynôme nul par I.2. On a donc $h = P(f) \in k[f]$.

4. Quelques groupes finis.

4.1. L'algèbre $k[X_1, \ldots, X_n]^{\Sigma_n}$ est celle des polynômes symétriques. Elle est engendrée par les polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_n$ qui sont algébriquement libres : c'est donc une algèbre de polynômes.

4.2.1. Il est clair que $k[X_1^2, \ldots, X_iX_j, \ldots, X_n^2] \subset k[X_1, \ldots, X_n]^G$.

Soit $P \in k[X_1, \ldots, X_n]$ invariant par G, P est combinaison linéaire de monômes du type $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$. L'action de G sur un tel monôme ne change pas le n-uple $(\alpha_1, \ldots, \alpha_n)$. On en déduit que les monômes qui composent P doivent être aussi invariants par G. Cherchons donc à quelle condition un tel monôme est invariant par G.

On doit avoir $(-1)^{\alpha_1 + \ldots + \alpha_n} = 1$.

Ceci impose que le nombre d'éléments α_i impairs est pair. On peut donc grouper deux par deux les α_i impairs. Donnons nous alors un tel couple (α_i, α_j). On peut écrire, si $\alpha_i \leq \alpha_j$ (par exemple) :

$$X_i^{\alpha_i} X_j^{\alpha_j} = (X_iX_j)^{\alpha_i} X_j^{\alpha_j - \alpha_i} \in k[X_j^2, X_iX_j]$$

car $\alpha_j - \alpha_i$ est pair.

On voit donc qu'un tel monôme est élément de $k[X_1^2, \ldots, X_iX_j, \ldots, X_n^2]$ et ceci entraîne l'assertion.

4.2.2. Commençons par prouver que $k[X^2, XY, Y^2]$ n'est pas factoriel.

Les seuls diviseurs de X^2 dans $k[X, Y]$ sont les constantes, λX, et λX^2 où $\lambda \in k^*$. On en déduit que X^2 est irréductible dans $k[X^2, XY, Y^2]$: en effet, un diviseur de X^2 dans $k[X^2, XY, Y^2]$ est aussi un diviseur de X^2 dans $k[X, Y]$. De même, Y^2 est irréductible dans $k[X^2, XY, Y^2]$

De même, les seuls diviseurs de XY dans $k[X, Y]$ sont les constantes, λX, λY et λXY où $\lambda \in k^*$. On en déduit que XY est irréductible dans $k[X^2, XY, Y^2]$.

Or, on a : $X^2\,Y^2 = (XY)^2$ et il n'y a pas unicité de la factorisation en produit d'irréductibles.

Donc $k[X^2, XY, Y^2]$ n'est pas factoriel.

Pour $n \geq 2$, il suffit de considérer de la même façon l'égalité :

$$(X_1X_2)^2 = X_1^2\,X_2^2$$

pour s'apercevoir que $k[X_1^2, \ldots, X_iX_j, \ldots, X_n^2]$ n'est pas factoriel.

On en déduit déjà que pour $n \geq 2$, $k[X_1, \ldots, X_n]^G$ n'est pas une algèbre de polynômes car $k[X_1, \ldots, X_n]$ est factoriel.

Pour $n = 1$, on a $k[X]^G = k[X^2]$ et $k[X^2]$ est isomorphe à $k[X]$ via

$$P \in k[X] \to P(X^2).$$

$k[X]^G$ est une algèbre de polynômes.

4.2.3. Identifions $k[U, V, W]$ et $(k[U, W])[V]$. L'anneau $k[U, W]$ est commutatif, unitaire et intègre et le polynôme $V^2 - UW$ est unitaire. On peut donc effectuer la division euclidienne de P par $V^2 - UW$.

On écrit $P = Q(V^2 - UW) + R$, avec $\deg R \leq 1$. R s'écrit donc

$$R = S(U,W)V + T(U,W).$$

Or $P(X^2, XY, Y^2) = 0$ et cela donne $S(X^2, Y^2)XY = -T(X^2, Y^2)$. Mais $T((-X)^2, Y^2) = T(X^2, Y^2)$. Ceci implique alors $S(X^2, Y^2) = 0$ et S est nul. Dès lors, T est nul et R est nul. Donc $V^2 - UW$ divise P.

4.2.4. Considérons le morphisme $\psi : k[U,V,W] \to k[X^2, XY, Y^2]$ qui à un polynôme P associe le polynôme $P(X^2, XY, Y^2)$. ψ est bien sûr surjectif et d'après la question précédente, le noyau de ψ est l'idéal engendré par $V^2 - UW$. Il suffit alors d'appliquer le théorème d'isomorphisme : $\mathrm{im}\psi$ est isomorphe à $k[U,V,W]/\ker\psi$.

5. et 6. Groupe orthogonal.

5.1. Soit $v \in V$. S'il existe un élément $a\,e_1$ (avec $a \geq 0$) dans l'orbite de v sous $O(V)$, on peut trouver $g \in O(V)$ tel que $g(v) = a\,e_1$. On a alors $\|v\| = \|g(v)\| = |a| = a$. Ainsi, a est déterminé de façon unique. Montrons l'existence. Si $v = 0$, il suffit de prendre $a = 0$. Si $v \neq 0$, on pose $e'_1 = v/\|v\|$, on complète e'_1 en une base orthonormée $(e'_1, \ldots, e'_n)$ de V et on considère $g \in L(V)$ défini par $g(e'_i) = e_i$ pour $1 \leq i \leq n$. Alors $g \in O(V)$ car g transforme une base orthonormée en une autre et on a : $g(v) = g(\|v\|\,e'_1) = \|v\|\,e_1$.

5.2. Il est clair que $\mathbb{R}[X_1^2 + \ldots + X_n^2] \subset S(V)^{O(V)}$.

Soit $f \in S(V)^{O(V)}$. Considérons le polynôme $P \in \mathbb{R}[X]$ tel que pour $t \in \mathbb{R}$, $P(t) = f(t\,e_1)$. Remarquons que ce polynôme est pair : pour $v \in V$, $-v$ est dans l'orbite de v car $-Id_V \in O(V)$. Comme $f \in S(V)^{O(V)}$, $P(-t) = f(-t\,e_1) = f(t\,e_1) = P(t)$ pour $t \in \mathbb{R}$. On peut donc écrire $P = Q(X^2)$ où $Q \in \mathbb{R}[X]$. Soit alors $v \in V$. D'après la question précédente, on a $f(v) = f(\|v\|\,e_1) = Q(\|v\|^2)$. Il en résulte que $f \in \mathbb{R}[X_1^2 + \ldots + X_n^2]$. D'où le résultat.

6.1. Soit $g \in G$, et $(x,y) \in V$. Comme g^{-1} conserve la norme et le produit scalaire, on a :

$$\begin{aligned} g.L(x,y) = L(g^{-1}.x, g^{-1}.y) &= H(g^{-1}(x).g^{-1}(y), \|g^{-1}(x)\|^2, \|g^{-1}(y)\|^2) \\ &= H(x.y, \|x\|^2, \|y\|^2) \\ &= L(x,y). \end{aligned}$$

et L est bien G-invariant.

6.2. Considérons s la symétrie orthogonale d'axe $\mathbb{R}\,e_1$. Soient $a, b, c \in \mathbb{R}$. On a : $s(a,0) = (a,0)$ et $s(b,c) = (b,-c)$. Par définition, F est invariant par s, il en résulte que $K(a,b,c) = K(a,b,-c)$. Donc K est pair en la variable c et on peut écrire, pour $a, b, c \in \mathbb{R}$, $K(a,b,c) = \sum_i Q_i(a,b)c^{2i}$ où $Q_i \in \mathbb{R}[X,Y]$. F est aussi invariant par $-Id_E$, et ceci donne $K(-a,-b,-c) = K(a,b,c)$ pour tous $a, b, c \in \mathbb{R}$. On a donc pour tout i, $Q_i(-a,-b) = Q_i(a,b)$ et d'après 4.2.1, Q_i est un polynôme en a^2, b^2, ab. Ainsi K est bien un polynôme en a^2, b^2, c^2, ab.

6.3. Soit $(x,y) \in V$. Si $x = 0$, n'importe quel élément de G fait l'affaire. Supposons que $x \neq 0$. Soit $f_1 = x/\|x\|$ et soit f_2 un vecteur de E de norme 1, orthogonal à u. Soit $g \in G$ tel que $g(f_1) = e_1$ et $g(f_2) = e_2$. On a alors $g(x) = \|x\|\,e_1$. Donc (x,y) a bien dans son orbite sous G un élément (u,v) tel que u est proportionnel à e_1. Avec les notations précédentes, on peut prendre

$u = \|x\| e_1$ et $v = g(y)$. Le vecteur y s'écrit $y = (y.f_1) f_1 + (y.f_2) f_2$, donc $g(y) = (y.f_1) e_1 + (y.f_2) e_2$. On a donc

$$F(x,y) = F(u,v) = K(\|x\|, y.f_1, y.f_2).$$

D'après 6.2., c'est donc un polynôme en $\|x\|^2 = x.x$, $(y.f_1)^2$, $(y.f_2)^2$, $\|x\| y.f_1$. Or, on a :

$$(y.f_1)^2 = \frac{(x.y)^2}{x.x} \quad \text{et} \quad \|x\| y.f_1 = x.y.$$

D'autre part, on a

$$y.y = (y.f_1)^2 + (y.f_2)^2 \ ,$$

donc

$$(y.f_2)^2 = y.y - \frac{(x.y)^2}{x.x}.$$

On voit ainsi que $F(x,y)$ devient un polynôme en $x.x$, $y.y$, $x.y$, $\dfrac{1}{x.x}$. En multipliant par une puissance convenable de $x.x$, on obtient alors un polynôme en $x.x$, $y.y$, $x.y$. Il existe donc $M \in \mathbb{R}[U,V,W]$ et $\alpha \in \mathbb{N}$ tels que pour $x \neq 0$,

$$F(x,y) = \frac{M(x.y, x.x, y.y)}{(x.x)^\alpha}.$$

6.4. Soit $R = W^p P(U,V,W) - V^q Q(U,V,W)$. Montrons que R s'annule sur un ouvert de $\mathbb{R}^3$. Considérons $\Omega = [-1/4, 1/4] \times [1/2, 1] \times [1/2, 1]$. On va montrer que R s'annule sur Ω, qui contient un ouvert de $\mathbb{R}^3$: R est alors nul. Donnons-nous $(a,b,c) \in \Omega$. Remarquons que $a/\sqrt{bc} \in [-1,1]$, ce qui permet de considérer $\varphi \in [0,\pi]$ tel que $\cos\varphi = a/\sqrt{bc}$. Soit alors $x \in E$ de norme $\sqrt{b}$. On peut trouver $y \in E$ de norme $\sqrt{c}$ tel que l'angle des vecteurs x et y soit φ. On a alors $x.y = \sqrt{bc}\cos\varphi = a$. D'où $R(a,b,c) = R(x.y, x.x, y.y) = 0$ (x et y sont non nuls).

6.5. D'après 6.1., on a

$$\mathbb{R}[X_1Y_1 + X_2Y_2, X_1^2 + X_2^2, Y_1^2 + Y_2^2] \subset \mathbb{R}[X_1, X_2, Y_1, Y_2]^G.$$

Soit alors $F \in \mathbb{R}[X_1, X_2, Y_1, Y_2]^G$. D'après ce qui précède, on peut trouver $M \in \mathbb{R}[U,V,W]$ et $\alpha \in \mathbb{N}$ tels que pour $x \neq 0$,

$$F(x,y) = \frac{M(x.y, x.x, y.y)}{(x.x)^\alpha}.$$

En raisonnant de manière analogue, on montre qu'il existe $N \in \mathbb{R}[U,V,W]$ et $\beta \in \mathbb{N}$ tels que pour $y \neq 0$,

$$F(x,y) = \frac{N(x.y, x.x, y.y)}{(y.y)^\beta}.$$

On montre tout d'abord que $K_1(a,b,c) = F(a,b,0,c)$ est un polynôme en a^2, b^2, c^2, bc en considérant la symétrie orthogonale d'axe $\mathbb{R}e_2$, puis que tout élément $(x,y) \in V$ a dans son orbite un élément (u,v) où v est proportionnel à e_2.

On a alors :

$$\forall x, y \in E \setminus \{0\} \ : \quad \frac{M(x.y, x.x, y.y)}{(x.x)^\alpha} = \frac{N(x.y, x.x, y.y)}{(y.y)^\beta}$$

D'après 6.4., $W^\beta M(U,V,W) = V^\alpha N(U,V,W)$. Or V et W sont irréductibles dans $\mathbb{R}[U,V,W]$ qui est factoriel. On en déduit que V^α divise M. On peut donc écrire $M = V^\alpha S$ et on en déduit que pour $x \neq 0$, $F(x,y) = S(x.y, x.x, y.y)$ et il y a égalité en 0 par continuité. F est bien un polynôme en $x_1y_1 + x_2y_2$, $x_1^2 + x_2^2$, $y_1^2 + y_2^2$.

7. Conjugaison.

7.1. Pour tout $f \in V$, on note P_f le polynôme caractéristique de f. On désigne par $\mathbb{C}_n[X]$ le $\mathbb{C}$-espace vectoriel des polynômes de degré inférieur à n à coefficients dans $\mathbb{C}$. L'application Ψ de $L(E)$ dans $\mathbb{C}_n[X]$ qui à un endomorphisme f associe P_f est continue (les coefficients de P_f sont des polynômes en les coefficients de la matrice de f dans une base de E). D'autre part l'application Θ de $\mathbb{C}_n[X]$ dans $\mathbb{C}$ qui à un polynôme P fait correspondre le résultant de P et P' est aussi continue ($\Theta(P)$ est en effet un polynôme en les coefficients de P). Rappelons que si $R(T,S)$ désigne le résultant des polynômes T et S, alors $R(T,S) = 0$ si et seulement si T et S ont une racine commune. On a alors $U = (\Theta \circ \Psi)^{-1}(\mathbb{C}^*)$. U apparait ainsi comme image réciproque d'un ouvert par une application continue : U est donc ouvert.

L'orbite de u est la classe de similitude de u. Ici, u possède n valeurs propres distinctes. u est en particulier diagonalisable. Si v est dans l'orbite de u, v possède les mêmes valeurs propres que u. Réciproquement, si $f \in V$ possède les mêmes valeurs propres que u, f est diagonalisable car f admet n valeurs propres distinctes. Il est clair que u et f ont mêmes matrices dans des base convenables. u et f sont donc semblables. L'orbite de u est ainsi l'ensemble des endomorphismes v de V qui ont les mêmes valeurs propres que u.

7.2. Ceci résulte immédiatement du fait que deux endomorphismes semblables ont même polynôme caractéristique.

7.3. La question qui précède assure que $k[\tau_1, \ldots, \tau_n] \subset S(V)^G$.

Soit alors $F \in S(V)^G$. Fixons une base $B = (e_1, \ldots, e_n)$ de E. Une base de V est alors la famille d'endomorphismes $(f_{ij})_{1 \leq i,j \leq n}$ définie par : pour tous i, j, k dans $\{1, \ldots, n\}$, $f_{ij}(e_k) = \delta_{ik} e_j$. Soit P le polynôme de $\mathbb{C}[X_1, \ldots, X_n]$ tel que $P(x_1, \ldots, x_n) = F(\sum_{i=1}^{n} x_i\, f_{ii})$ (ce polynôme ne dépend que de F). P est en fait un polynôme symétrique. En effet, soit $(x_1, \ldots, x_n) \in \mathbb{C}^n$ et soit σ une permutation de $\{1, \ldots, n\}$. Les endomorphismes $v = \sum_{i=1}^n x_i\, f_{ii}$ et $w = \sum_{i=1}^n x_{\sigma(i)}\, f_{ii}$ sont tous les deux diagonalisables : pour $1 \leq i \leq n$, on a $v(e_i) = x_i\, e_i$ et $w(e_i) = x_{\sigma(i)}\, e_i$. La matrice de v dans la base $(e_{\sigma(1)}, \ldots, e_{\sigma(n)})$ est la même que celle de w dans la base B, v et w sont donc semblables et $P(x_1, \ldots, x_n) = F(v) = F(w) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. On peut alors exprimer P comme un polynôme en les polynômes symétriques élémentaires $\pi_1, \ldots, \pi_n$. On écrit $P = Q(\pi_1, \ldots, \pi_n)$.

Maintenant, si $u \in V$ est diagonalisable de valeurs propres (distinctes ou non) $x_1, \ldots, x_n$, u est semblable à $v = \sum_{i=1}^n x_i\, f_{ii}$, donc

$$F(u) = F(v) = Q(\pi_1(x_1, \ldots, x_n), \ldots, \pi_n(x_1, \ldots, x_n)) = Q(\tau_1(u), \ldots, \tau_n(u)).$$

F et $Q(\tau_1,\dots,\tau_n)$ coïncident en particulier sur l'ouvert U, donc partout et on a bien :

$$F \in \mathbb{C}[\tau_1,\dots,\tau_n].$$

PARTIE IV Les formes binaires

8. Un exemple ($d=2$)

8.1. Par définition, on a $\big(\pi_2(g)P\big)(u,v,w) = P(g^{-1}.[uX^2+vXY+wY^2])$. Il s'agit donc ici de calculer

$$g^{-1}.[uX^2+vXY+wY^2] = u\,(g^{-1}.X)^2 + v\,g^{-1}.X\,g^{-1}.Y + w\,(g^{-1}.Y)^2$$

Lançons-nous donc dans les calculs sans rechigner. On a :

$$\begin{array}{c}(g^{-1}.X)^2 = (\alpha X+\beta Y)^2 = \alpha^2X^2+\beta^2Y^2+2\alpha\beta XY\\ (g^{-1}.Y)^2 = (\gamma X+\delta Y)^2 = \gamma^2X^2+\delta^2Y^2+2\gamma\delta XY\\ (g^{-1}.X)\,(g^{-1}.Y) = \alpha\gamma X^2+(\alpha\delta+\beta\gamma)\,XY+\beta\delta Y^2.\end{array}$$

On en déduit que :

$$\begin{array}{rcl} g^{-1}.[uX^2+vXY+wY^2] & = & (\alpha^2\,u+\gamma^2\,w+\alpha\gamma\,v)X^2\\ & & +(2\alpha\beta\,u+2\gamma\delta\,w+(\alpha\delta+\beta\gamma)v)\,XY\\ & & +(\beta^2\,u+\delta^2\,w+\beta\delta\,v)\,Y^2.\end{array}$$

Le résultat demandé en découle immédiatement.

Montrons maintenant que $\Delta(u,v,w)=v^2-4uw$ appartient à $S(R_2)^G$. Soit $g=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in SL_2(k)$. Montrons que

$$\Delta(\alpha^2\,u+\gamma^2\,w+\alpha\gamma\,v,\,2\alpha\beta\,u+2\gamma\delta\,w+(\alpha\delta+\beta\gamma)v,\,\beta^2\,u+\delta^2\,w+\beta\delta\,v) = \Delta(u,v,w).$$

On a :

$$\begin{array}{rcl}(2\alpha\beta\,u+2\gamma\delta\,w+(\alpha\delta+\beta\gamma)v)^2 & = & 4\alpha^2\beta^2u^2+(\alpha\delta+\beta\gamma)^2v^2+4\gamma^2\delta^2\,w^2\\ & & +2\,[2\alpha\beta\,(\alpha\delta+\beta\gamma)]\,uv\\ & & +2\,[2\gamma\delta\,(\alpha\delta+\beta\gamma)]\,vw\\ & & +2\,[2\alpha\beta\,2\gamma\delta]uw.\end{array}$$

D'autre part :

$$\begin{array}{rcl}(\alpha^2\,u+\alpha\gamma\,v+\gamma^2\,w)\,(\beta^2\,u+\delta^2\,w+\beta\delta\,v) & = & \alpha^2\beta^2\,u^2+\alpha\beta\gamma\delta\,v^2+\gamma^2\delta^2\,w^2\\ & & +[\alpha\beta(\alpha\delta+\beta\gamma)]\,uv\\ & & +[\alpha^2\delta^2+\gamma^2\beta^2]\,uw\\ & & +[\gamma\delta(\alpha\delta+\beta\gamma)]\,vw.\end{array}$$

Il vient donc :

$$\begin{array}{rcl}(\pi_2(g)\Delta)(u,v,w) & = & v^2\,[(\alpha\delta+\beta\gamma)^2-4\alpha\beta\gamma\delta]+uw\,[8\alpha\beta\gamma\delta-4\alpha^2\delta^2-4\gamma^2\beta^2]\\ & = & (\alpha\delta-\beta\gamma)^2\,(v^2-4\,uw)\\ & = & (\det g)^2\Delta(u,v,w)=\Delta(u,v,w)\quad\text{car }\det g=1.\end{array}$$

D'où le résultat.

8.2. Comme k est algébriquement clos, le polynôme $X^2 - u$ possède une racine $z \in k$. Comme $u \neq 0$, on a $z \neq 0$ et z est inversible car k est de caractéristique nulle. On peut alors écrire :

$$\begin{aligned} u\,X^2 + v\,XY + w\,Y^2 &= (z\,X + \tfrac{v}{2z}Y)^2 - \tfrac{v^2 - 4z^2\,w}{4z^2}Y^2 \\ &= (z\,X + \tfrac{v}{2z}Y)^2 - \tfrac{\Delta(u,v,w)}{4z^2}Y^2 \end{aligned}$$

On voit alors que $u\,X^2 + v\,XY + w\,Y^2 = \pi_2(g^{-1})(X^2 - \dfrac{\Delta(u,v,w)}{4}Y^2)$ en posant $g = \begin{pmatrix} z & \frac{v}{2z} \\ 0 & z^{-1} \end{pmatrix}$ et on a bien $g \in SL_2(k)$. Donc, $X^2 - \dfrac{\Delta(u,v,w)}{4}Y^2$ et $u\,X^2 + v\,XY + w\,Y^2$ sont dans la même orbite.

Montrons alors que $S(R_2)^G = k[\Delta]$. D'après 8.1., on a déjà $k[\Delta] \subset S(R_2)^G$.

Soit alors $P \in S(R_2)^G$. Soit $Q \in k[T]$ défini par $Q = P(1, 0, \dfrac{-T}{4})$. D'après ce qui précède, P et $Q(\Delta)$ coïncident sur $k^* \times k \times k$. On en déduit alors que $P = Q(\Delta)$ grâce à la partie I. Ceci entraîne bien entendu le résultat.

9. Cas général.

9.1. Soit (i, j) un couple d'entiers de $\{0, \ldots, d\}$ tels que $i + j = d$. Par définition de ρ_d, on a :

$$(\rho_d(g_a))(X^iY^j) = (a^{-1}X)^i\,(aY)^j = a^{j-i}\,X^iY^j.$$

Il en résulte que la matrice de $(\rho_d(g_a))$ dans la base $(X^d, X^{d-1}Y, \ldots, Y^d)$ est diagonale, le i-ème coefficient diagonal valant a^{-d+2i} pour $0 \leq i \leq d$. On a alors :

$$\mathrm{tr}(\rho_d(g_a)) = a^{-d}\sum_{i=0}^{d} a^{2i} = a^{-d}\frac{1 - a^{2(d+1)}}{1 - a^2} = \frac{a^{-d} - a^{d+2}}{1 - a^2} = \frac{a^{d+1} - a^{-(d+1)}}{a - a^{-1}}.$$

9.2. On a $R_0 = k$ (un polynôme homogène de degré 0 est constant) et il est clair que les fonctions constantes sont invariantes par G, donc $R_0^G = k$.

Soit alors $d > 0$. Donnons-nous $P \in R_d^G$. On écrit $P = \sum_{i=0}^{d} \lambda_i X^iY^{d-i}$. On a en particulier pour tout $a \in k^*$, $(\rho_d(g_a))(P) = P$, c'est à dire que

$$P = \sum_{i=0}^{d} a^{d-2i}\lambda_i X^iY^{d-i}.$$

Donc pour $0 \leq i \leq d$, on a $\lambda_i(1 - a^{d-2i}) = 0$.

Ceci impose $\lambda_i = 0$ dès que $2i \neq d$: en effet, le polynôme non constant $X^{|d-2i|} - 1$ n'a qu'un nombre fini de racines dans k et k est infini car de caractéristique nulle ; on peut donc trouver une infinité de scalaires non nuls a tels que $1 - a^{d-2i} \neq 0$. Reste à examiner le cas où d est pair. On écrit $d = 2l$, et P s'écrit alors $P = \lambda_l X^lY^l$ (tous les autres λ_i son nuls par ce qui précède). Soit

$g = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. On a $g.P = \lambda_l (X+Y)^l Y^l = \lambda_l X^l Y^l$. Ceci impose clairement $\lambda_l = 0$. P est bien le polynôme nul.

9.3. Considérons pour tout $i \in I$ une base B_i de V_i et soit d'autre part φ_i l'application de V_i dans $\bigoplus_{k\in I} V_k$ définie par $\varphi_i(x) = (0, \ldots, x, \ldots, 0)$ (x est à la i-ème place). Il est clair que $B = \bigcup_{i\in I} \varphi_i(B_i)$ est alors une base de $\bigoplus_{k\in I} V_k$. La matrice de $\pi(h)$ dans cette base est diagonale par blocs, les blocs diagonaux étant les matrices de $\pi_i(h)$ dans B_i. Il en résulte alors que $\mathrm{tr}\pi(h) = \sum_{i\in I} \mathrm{tr}\pi_i(h)$.

9.4.1. On a

$$\begin{aligned} \mathrm{tr}\lambda(g_a) &= \mathrm{tr}(\theta^{-1} \circ \lambda(g_a) \circ \theta) \\ &= \mathrm{tr} \bigoplus_{d\geq 0} \rho_d^{n(d)}(g_a) \\ &= \sum_{d\geq 0} \mathrm{tr}\rho_d^{n(d)}(g_a) \\ &= \sum_{d\geq 0} n(d)\mathrm{tr}\rho_d(g_a) \\ &= \sum_{d\geq 0} n(d) \frac{a^{d+1} - a^{-(d+1)}}{a - a^{-1}}. \end{aligned}$$

On a utilisé deux fois la question 9.3. : une fois pour écrire que

$$\mathrm{tr} \bigoplus_{d\geq 0} \rho_d^{n(d)}(g_a) = \sum_{d\geq 0} \mathrm{tr}\rho_d^{n(d)}(g_a)$$

, et une autre pour écrire

$$\mathrm{tr}\rho_d^{n(d)}(g_a) = n(d)\mathrm{tr}\rho_d(g_a).$$

9.4.2. Soit $N \in \mathbb{N}$ tel que $n(d) = 0$ si $d > N$. Pour tout $a \in k^*$ on a donc

$$(a - a^{-1})\mathrm{tr}\lambda(g_a) = \sum_{d=0}^{N} n(d)(a^{d+1} - a^{-(d+1)}) \ ,$$

et donc

$$a^{N+1}(a - a^{-1})\mathrm{tr}\lambda(g_a) = \sum_{d=0}^{N} n(d)\,(a^{N+d+2} - a^{N-d}).$$

Ainsi $n(d)$ est le coefficient de a^{N+d+2} dans le polynôme

$$P = \sum_{d=0}^{N} n(d)\,(a^{N+d+2} - a^{N-d})$$

qui ne dépend que de λ d'après l'égalité précédente. Donc λ détermine les entiers $n(d)$ de façon unique.

9.4.3. V est isomorphe à $\bigoplus_{d\geq 0} R_d^{n(d)}$.

V^G est alors isomorphe à $\left(\bigoplus_{d\geq 0} R_d^{n(d)}\right)^G$.

Par définition d'une somme directe d'actions, on a clairement un isomorphisme entre $\left(\bigoplus_{i\in I} V_i\right)^G$ et $\bigoplus_{i\in I} V_i^G$ avec les notations de la définition 11. Ici, V^G est isomorphe à $\bigoplus_{d\geq 0}[R_d^{n(d)}]^G$, et on a encore pour tout $d \geq 0$, $(R_d^{n(d)})^G$ isomorphe à $(R_d^G)^{n(d)}$ (l'action de G sur $R_d^{n(d)}$ est encore la somme directe des actions ρ_d sur R_d). Or on a vu que si $d > 0$, $R_d^G = 0$. Finalement, V^G est isomorphe à $R_0^{n(0)} = k^{n(0)}$. La dimension de V^G est donc $n(0)$ qui est bien le coefficient de a dans le polynôme de Laurent $(a - a^{-1})\mathrm{tr}\lambda(g_a) = \sum_{d=0}^{N} n(d)(a^{d+1} - a^{-(d+1)})$.

9.5.1. On sait que les inversibles de $k[[T]]$ sont les séries formelles dont le premier terme est non nul (en fait inversible dans k). Ici, si P désigne le polynôme $\det(I_n - B^{-1}T)$, $P(0) = \det I_n = 1$. D'où l'existence de l'inverse de P dans $k[[T]]$.

9.5.2. B est triangulaire supérieure, il en est donc de même de B^{-1} ; de plus, les coefficients diagonaux de B^{-1} sont $b_{11}^{-1}, \ldots, b_{nn}^{-1}$. La matrice $I_n - B^{-1}T$ est également triangulaire supérieure et ses coefficients diagonaux sont $1 - b_{11}^{-1}T, \ldots, 1 - b_{nn}^{-1}T$. On a donc

$$\det(I_n - B^{-1}T) = \prod_{i=1}^{n}\left(1 - b_{ii}^{-1}T\right).$$

Soit $1 \leq i \leq n$, $1 - b_{ii}^{-1}T$ est inversible dans $k[[T]]$, d'inverse $\sum_{k\geq 0} \frac{T^k}{b_{ii}^k}$ (il suffit d'utiliser $\frac{1}{1-U} = \sum_{k\geq 0} U^k$). On en déduit alors l'inverse de $\det(I_n - B^{-1}T)$ dans $k[[T]]$.

$$(\det(I_n - B^{-1}T))^{-1} = \sum_{k\geq 0} c_k T^k$$

où pour $k \in \mathbb{N}$, par définition du produit de séries formelles :

$$c_k = \sum_{\alpha_1+\ldots+\alpha_n=k} \frac{1}{b_{11}^{\alpha_1}} \cdots \frac{1}{b_{nn}^{\alpha_n}}.$$

Soit alors $e \in \mathbb{N}$. Une base de $k[X_1, \ldots, X_n]_e$ est donnée par les éléments du type $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ où $(\alpha_1, \ldots, \alpha_n)$ décrit l'ensemble des n-uplets d'entiers vérifiant $\alpha_1 + \ldots + \alpha_n = e$. Notons $B^{-1} = [a_{ij}]$ $\quad(a_{ii} = 1/b_{ii})$. On a

$$\begin{array}{rcl} B.(X_1^{\alpha_1} \ldots X_n^{\alpha_n}) & = & (b_{11}^{-1}X_1 + a_{12}X_2 + \ldots + a_{1n}X_n)^{\alpha_1} \\ & \times & (b_{22}^{-1}X_2 + a_{23}X_3 + \ldots + a_{2n}X_n)^{\alpha_2} \\ & & \vdots \\ & \times & (b_{nn}^{-1}X_n)^{\alpha_n}. \end{array}$$

La composante de $B.(X_1^{\alpha_1} \ldots X_n^{\alpha_n})$ suivant $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ est alors $\frac{1}{b_{11}^{\alpha_1}} \cdots \frac{1}{b_{nn}^{\alpha_n}}$; il suffit de développer le produit précédent : on retrouve le produit $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$

en gardant $(b_{11}^{-1}X_1)^{\alpha_1}$ dans le premier facteur, puis $(b_{22}^{-1}X_2)^{\alpha_2}$ dans le second, et ainsi de suite jusqu'au dernier facteur. On a alors

$$\mathrm{tr}_e B = \sum_{\alpha_1+\ldots+\alpha_n=e} \frac{1}{b_{11}^{\alpha_1}} \cdots \frac{1}{b_{nn}^{\alpha_n}}.$$

D'où l'égalité des séries formelles $\sum_{e\geq 0} \mathrm{tr}_e(B)T^e$ et $(\det(I_n - B^{-1}T))^{-1}$.

9.5.3. k est algébriquement clos, donc le polynôme caractéristique de B est scindé sur k. On sait alors que B est semblable à une matrice triangulaire supérieure A. D'après la question précédente, les séries formelles $\sum_{e\geq 0} \mathrm{tr}_e(A)T^e$ et $(\det(I_n - A^{-1}T))^{-1}$ sont égales dans $k[[T]]$. Comme B^{-1} est semblable à A^{-1}, les polynômes $\det(I_n - A^{-1}T)$ et $\det(I_n - B^{-1}T)$ sont égaux (pour tout $\lambda \in k$, $I_n - \lambda A^{-1}$ et $I_n - \lambda B^{-1}$ sont semblables, donc ont même déterminant). On a donc l'égalité des séries formelles $(\det(I_n - A^{-1}T))^{-1}$ et $(\det(I_n - B^{-1}T))^{-1}$.

D'autre part, changeons légèrement de notation et notons pour toute matrice $D \in GL_n(k)$: $\rho(D)$ l'automorphisme de $k[X_1, \ldots, X_n]$ induit par D. En fait, on a immédiatement que $\rho(D_1D_2) = \rho(D_1) \circ \rho(D_2) \quad (\forall D_1,\ D_2 \in GL_n(k))$ (ρ est donc une action de groupe). Soit $C \in GL_n(k)$ tel que $B = C^{-1}AC$. Alors $\rho(B) = \rho(C)^{-1} \circ \rho(A) \circ \rho(C)$. Ainsi les automorphismes $\rho(A)$ et $\rho(B)$ sont semblables. Il en résulte alors que pour tout $e \geq 0 \quad \mathrm{tr}_e(A) = \mathrm{tr}_e(B)$. D'où le résultat.

9.6. D'après ce qui précède, on a $\sum_{e\geq 0} \chi_{d,e}(a)T^e = (\det(I_n - [\rho_d(g_a)]^{-1}T))^{-1}$.
Or, on a vu que la matrice de $\rho_d(g_a)$ dans la base $(X^d, X^{d-1}Y, \ldots, Y^d)$ est

$$\begin{pmatrix} a^{-d} & & & \\ & a^{-d+2} & & \\ & & \ddots & \\ & & & a^d \end{pmatrix},$$

donc la matrice de $[\rho_d(g_a)]^{-1}$ dans cette base est

$$\begin{pmatrix} a^{d} & & & \\ & a^{d-2} & & \\ & & \ddots & \\ & & & a^{-d} \end{pmatrix}.$$

On a donc tout de suite

$$\begin{aligned} \det(I_n - [\rho_d(g_a)]^{-1}T) &= (1 - a^dT)(1 - a^{d-2}T)\ldots(1 - a^{-d+2}T)(1 - a^{-d}T) \\ &= (1 - a^{-d}T)(1 - a^{-d+2}T)\ldots(1 - a^dT). \end{aligned}$$

D'où le résultat.

9.7. Le terme constant de $F_U(W)$ (obtenu pour $W = 0$) est 1 qui est inversible dans $\mathbb{Z}[U]$. $F_U(W)$ est alors inversible dans $\mathbb{Z}[U][[W]]$, d'où l'existence des polynômes $M_{d,e}(U) \in \mathbb{Z}[U]$ tels que

$$[F_U(W)]^{-1} = \sum_{e\geq 0} M_{d,e}(U)W^e.$$

9.8. On a :

$$\begin{aligned}\sum_{e\geq 0}\chi_{d,e}(a)W^e &= [(1-a^{-d}W)(1-a^{-d+2}W)\dots(1-a^{-d}W)]^{-1}\\ &= [(1-a^0\tfrac{W}{a^d})(1-a^2\tfrac{W}{a^d})\dots(1-(a^2)^d\tfrac{W}{a^d})]^{-1}\\ &= \sum_{e\geq 0}M_{d,e}(a^2)\left(\frac{W}{a^d}\right)^e\end{aligned}$$

D'où :

$$\chi_{d,e}(a) = a^{-de}M_{d,e}(a^2)$$

9.9. D'après la question 9.4.3., $m_{d,e}$ est le coefficient de a dans le polynôme de Laurent $(a-a^{-1})\chi_{d,e}(a)$. Or on a :

$$\begin{aligned}(a-a^{-1})\chi_{d,e}(a) &= (a-a^{-1})a^{-de}M_{d,e}(a^2)\\ &= (a-a^{-1})\sum_{i\geq 0}c(d,e,i)a^{2i-de}\\ &= \sum_{i\geq 0}c(d,e,i)a^{2i-de+1} - \sum_{i\geq 0}c(d,e,i)a^{2i-de-1}\end{aligned}$$

Il vient donc si de est impair, $m_{d,e}=0$ et si de est pair, $m_{d,e} = c(d,e,de/2) - c(d,e,(de/2)+1)$. Il y avait donc une petite erreur d'énoncé.

PARTIE V. GROUPE SYMÉTRIQUE

10. Polarisation.

10.1. L'application λ est dérivable et

$$\lambda'(t) = \sum_{i=1}^{n} Y_i \frac{\partial f}{\partial U_i}(U_1+tY_1,\dots,U_n+tY_n)$$

On a donc bien $\lambda'(0) = D_{U,Y}f$.

On en déduit que $f \mapsto D_{U,Y}f$ est une dérivation de $B[U]$ dans $B[U,Y]$. Pour $f\in B[U]$, notons $\lambda(f)$ l'application $t\in\mathbb{R}\mapsto f(U_1+tY_1,\dots,U_n+tY_n)$. Il est clair que $f\in B[U]\mapsto\lambda(f)$ est linéaire et que si $f,\ g\in B[U]$ on a $\lambda(fg)=\lambda(f)\lambda(g)$. Soient alors $a,\ b\in\mathbb{R}$, $f,\ g\in B[U]$. On a

$$\begin{aligned}D_{U,Y}(af+bg) = [\lambda(af+bg)]'(0) &= [a\lambda(f)+b\lambda(g)]'(0)\\ &= a[\lambda(f)]'(0)+b[\lambda(g)]'(0)\\ &= aD_{U,Y}(f)+bD_{U,Y}(g).\end{aligned}$$

et d'autre part

$$\begin{aligned}D_{U,Y}(fg) = [\lambda(fg)]'(0) &= [\lambda(f)\lambda(g)]'(0)\\ &= [\lambda(f)]'(0)[\lambda(g)](0)+[\lambda(f)](0)[\lambda(g)]'(0)\\ &= D_{U,Y}(f)\ g + D_{U,Y}(g)\ f.\end{aligned}$$

10.2. f est combinaison linéaire d'éléments du type $h_1^{\alpha_1}\dots h_p^{\alpha_p}$. Par linéarité, il suffit donc de montrer le résultat pour ces derniers éléments. On procède par récurrence sur p.

Le résultat est vrai pour $p=1$: soit $\alpha_1\in\mathbb{N}^*$ (le cas $\alpha_1=0$ est clair). $D_{U,Y}$ est une dérivation, on a donc immédiatement (il suffit d'effectuer une récurrence sur α_1) $D_{U,Y}(h_1^{\alpha_1})=(\alpha_1-1)h_1^{\alpha_1-1}D_{U,Y}(h_1)\in B[h_1,D_{U,Y}h_1]$.

Supposons le résultat vrai pour l'entier $p-1$. Soient $\alpha_1,\dots,\alpha_p$ des entiers. On a alors :

$$D_{U,Y}(h_1^{\alpha_1}\dots h_p^{\alpha_p})=D_{U,Y}(h_1^{\alpha_1}\dots h_{p-1}^{\alpha_{p-1}})\,h_p^{\alpha_p}+(h_1^{\alpha_1}\dots h_{p-1}^{\alpha_{p-1}})D_{U,Y}(h_p^{\alpha_p}).$$

Or par hypothèse,

$$D_{U,Y}(h_1^{\alpha_1}\dots h_{p-1}^{\alpha_{p-1}})\in B[h_1,\dots,h_{p-1},D_{U,Y}h_1,\dots,D_{U,Y}h_{p-1}]$$

et d'après le cas $p=1$, $D_{U,Y}h_p^{\alpha_p}\in B[h_p,D_{U,Y}h_p]$. On voit donc que

$$D_{U,Y}(h_1^{\alpha_1}\dots h_p^{\alpha_p})\in B[h_1,\dots,h_p,D_{U,Y}h_1,\dots,D_{U,Y}h_p].$$

10.3. Donnons-nous $F\in k[U]$ et $g\in G$. Exprimons $g.D_{U,Y}F$.
Notons $[a_{ij}]$ la matrice de g^{-1} (plus précisément de $\rho(g^{-1})$ si ρ est l'action de G sur k^n) dans la base canonique de k^n. On a par définition de l'action de G sur $k[U,Y]$:

$$g.D_{U,Y}F=D_{U,Y}F(g^{-1}.U,g^{-1}.Y)=\sum_{k=1}^{n}\big((g^{-1}.Y)\big)_k\frac{\partial F}{\partial U_k}(g^{-1}.U).$$

Or, on a pour $1\le k\le n$: $\big((g^{-1}.Y)\big)_k=\sum_{l=1}^{n}a_{kl}Y_l$. On en déduit donc que :

$$\begin{aligned}g.D_{U,Y}F&=\sum_{k=1}^{n}\Big(\frac{\partial F}{\partial U_k}(g^{-1}.U)\sum_{l=1}^{n}a_{kl}Y_l\Big)\\&=\sum_{l=1}^{n}\Big(\sum_{k=1}^{n}a_{kl}\frac{\partial F}{\partial U_k}(g^{-1}.U)\Big)Y_l.\end{aligned}$$

Soit alors $H=g.F=F(g^{-1}.U)$. On a , par composition :

$$\forall l\in\{1,\dots,n\}\quad\frac{\partial H}{\partial U_l}=\sum_{k=1}^{n}\frac{\partial\big((g^{-1}.U)_k\big)}{\partial U_l}\frac{\partial F}{\partial U_k}(g^{-1}.U)$$

Or, pour $1\le k\le n$: $\big((g^{-1}.U)\big)_k=\sum_{p=1}^{n}a_{kp}U_p$. On a donc :

$$(\forall k\in\{1,\dots,n\})\quad(\forall l\in\{1,\dots,n\})\quad\frac{\partial\big((g^{-1}.U)_k\big)}{\partial U_l}=a_{kl}.$$

Finalement,

$$g.D_{U,Y}F = \sum_{l=1}^{n} \frac{\partial H}{\partial U_l} Y_l = D_{U,Y}H = D_{U,Y}(g.F).$$

Il en résulte immédiatement que si $f \in k[U]$ est invariant pour l'action de G sur $k[U]$, alors $D_{U,Y}f$ est invariant pour l'action de g sur $k[U,Y]$.

10.4.1. P est un polynôme homogène de degré d en les indéterminées $U^{[1]} = (U_1^{[1]}, \ldots, U_n^{[1]})$, donc on a

$$P(X\,U^{[1]}, U^{[2]}, \ldots, U^{[N]}) = X^d\, P(U^{[1]}, \ldots, U^{[N]})$$

où $X\,U^{[1]} = (X\,U_1^{[1]}, \ldots, X\,U_n^{[1]})$. Dérivons cette relation par rapport à X :

$$\sum_{i=1}^{n} U_i^{[1]} \frac{\partial P}{\partial U_i^{[1]}}(X\,U^{[1]}, U^{[2]}, \ldots, U^{[N]}) = dX^{d-1}\, P(U^{[1]}, \ldots, U^{[N]}).$$

On spécialise alors en $X = 1$ pour obtenir

$$\sum_{i=1}^{n} U_i^{[1]} \frac{\partial P}{\partial U_i^{[1]}}(U^{[1]}, U^{[2]}, \ldots, U^{[N]}) = d\, P(U^{[1]}, \ldots, U^{[N]}).$$

Comme

$$Q(U^{[1]}, \ldots, U^{[N+1]}) = \sum_{i=1}^{n} U_i^{[N+1]} \frac{\partial P}{\partial U_i^{[1]}}(U^{[1]}, \ldots, U^{[N]})\ ,$$

on a bien le résultat annoncé :

$$Q(U^{[1]}, \ldots, U^{[N]}, U^{[1]}) = d\, P(U^{[1]}, \ldots, U^{[N]}).$$

10.4.2. Remarquons tout d'abord que si $F \in B[U]$ est homogène de degré d, alors $D_{U,Y}F$ est homogène de degré $d-1$ vis-à-vis de U. En effet, par linéarité, il suffit de prouver ceci lorsque F est de la forme $U_1^{\alpha_1} \ldots U_n^{\alpha_n}$ avec $\alpha_1 + \ldots + \alpha_n = d$. Or, dans ce cas, on a pour $i \in \{1, \ldots, n\}$,

$$\frac{\partial F}{\partial U_i} = \begin{cases} U_i^{\alpha_i - 1} \displaystyle\prod_{j \neq i} U_j^{\alpha_j} & \text{si} \quad \alpha_i \geq 1 \\ 0 & \text{si} \quad \alpha_i = 0 \end{cases}.$$

Donc $\dfrac{\partial F}{\partial U_i}$ est soit homogène de degré $d-1$, soit nul. Si F n'est pas constant ($d \geq 1$), l'un des $\dfrac{\partial F}{\partial U_i}$ est non nul et ceci entraîne bien que $D_{U,Y}F$ est homogène de degré $d-1$ vis-à-vis de U. Appliquons cette remarque à f, qui est homogène de degré r : on obtient tout de suite par récurrence que si $p \in \{1, \ldots, r+1\}$, $\widehat{f}_p$ est homogène de degré $r - p + 1$ vis-à-vis de $U^{[1]}$. En particulier, $\widehat{f}_{r+1}$ est homogène de degré 0, donc constant vis-à-vis de $U^{[1]}$. Il en résulte tout de suite que si $p > r+1$, $\widehat{f}_p = 0$.

Démontrons à présent le résultat demandé. On se donne un entier p dans $\{1,\dots,N\}$.
Supposons dans un premier temps $p < r$.
$\widehat{f}_{r-1}$ est un polynôme homogène de degré 2 vis-à-vis de $U^{[1]}$ et on a par définition

$$\widehat{f}_r = D_{U^{[1]},U^{[r]}}\widehat{f}_{r-1}.$$

D'après la question précédente, on a

$$\widehat{f}_{r-1} = \frac{1}{2}\widehat{f}_r(U^{[1]},\dots,U^{[r-1]},U^{[1]}).$$

$\widehat{f}_{r-2}$ est un polynôme homogène de degré 3 vis-à-vis de $U^{[1]}$ et on obtient de même :

$$\widehat{f}_{r-2} = \frac{1}{3}\widehat{f}_{r-1}(U^{[1]},\dots,U^{[r-2]},U^{[1]}).$$

D'où

$$\widehat{f}_{r-2} = \frac{1}{3\times 2}\widehat{f}_r(U^{[1]},\dots,U^{[r-2]},U^{[1]},U^{[1]}).$$

On réitère alors cette méthode $r-p$ fois pour obtenir :

$$\widehat{f}_p = \frac{1}{(r-p+1)\,!}\widehat{f}_r(U^{[1]},\dots,U^{[p]},U^{[1]},\dots,U^{[1]}).$$

L'existence de la suite $(\alpha_1,\dots,\alpha_r)$ vérifiant les conditions en découle aussitôt.
Pour $p = r$ (ce qui suppose $N \geq r$), le résultat est évident.
Pour $p > r+1$ (ce qui suppose $N \geq r+2$), on a $\widehat{f}_p = 0$ et la suite $(\alpha_1,\dots,\alpha_r)$ telle que $\alpha_i = 1$ pour tout i fait l'affaire.
Reste le cas $p = r+1$ (ce qui suppose $N \geq r+1$). On sait que $\widehat{f}_r$ est homogène de degré 1 vis-à-vis de $U^{[1]}$. On peut donc écrire :

$$\widehat{f}_r = \sum_{i=1}^{n} P_i(U^{[2]},\dots,U^{[r]})\,U_i^{[1]}$$

où les P_i sont des polynômes en $(U^{[2]},\dots,U^{[r]})$. On a alors tout de suite :

$$\widehat{f}_{r+1}(U^{[1]},\dots,U^{[r+1]}) = \sum_{i=1}^{n} P_i(U^{[2]},\dots,U^{[r]})\,U_i^{[r+1]}.$$

Ainsi

$$\widehat{f}_{r+1} = \widehat{f}_r(U^{[r+1]},U^{[2]},\dots,U^{[r]}).$$

La suite $(r+1,2,\dots,r)$ convient donc.

11 Action diagonale du groupe symétrique.

11.1. Soit r un entier fixé dans $\{1,\dots,n\}$ et soit $(i_1,\dots,i_r)$ des entiers vérifiant $1 \leq i_1 < i_2 < \dots < i_r \leq n$. Soit $f_{(i_1,\dots,i_r)} = U_{i_1}^{[1]}\dots U_{i_r}^{[1]}$. Il est clair que la polarisation totale de φ_r est la somme des polarisations totales des $f_{(i_1,\dots,i_r)}$ lorsque $(i_1,\dots,i_r)$ décrit l'ensemble des r-uplets d'entiers vérifiant $1 \leq i_1 < i_2 < \dots < i_r \leq n$.

Fixons un tel r-uplet $(i_1, \ldots, i_r)$ et étudions la polarisation totale de $f_{(i_1,\ldots,i_r)}$ que nous notons provisoirement f par commodité. Montrons que si p est un entier compris entre 1 et $r-1$, alors :

$$D_{U^{[1]},U^{[p+1]}} \ldots D_{U^{[1]},U^{[2]}} f = \sum_{(j_1,\ldots,j_p)} \Big(U_{j_1}^{[2]} \ldots U_{j_p}^{[p+1]} \prod_k U_k^{[1]} \Big).$$

La somme précédente porte sur tous les p-uplets d'entiers distincts de l'ensemble $\{i_1, \ldots, i_r\}$. Lorsqu'un tel p-uplet $(j_1, \ldots, j_p)$ est fixé, le produit qui apparaît porte sur les k appartenant au complémentaire de $\{j_1, \ldots, j_p\}$ dans $\{i_1, \ldots, i_r\}$.

Montrons cette formule par récurrence sur p. pour $p = 1$, on a :

$$D_{U^{[1]},U^{[2]}} f = \sum_{i=1}^{n} U_i^{[2]} \frac{\partial f}{\partial U_i^{[1]}}.$$

Or, il est immédiat que $\dfrac{\partial f}{\partial U_i^{[1]}} = 0$ si $i \notin \{i_1, \ldots, i_r\}$. De plus, si $k \in \{1, \ldots, r\}$, on a :

$$\frac{\partial f}{\partial U_{i_k}^{[1]}} = \prod_{j \in \{i_1,\ldots,i_r\} \setminus \{i_k\}} U_j^{[1]}.$$

Ceci entraîne la véracité de la formule pour $p = 1$.
Supposons la formule vraie pour l'entier p et montrons la au rang $p+1$. En utilisant l'hypothèse de récurrence et la linéarité de $D_{U^{[1]},U^{[p+2]}}$, on obtient :

$$D_{U^{[1]},U^{[p+2]}} \ldots D_{U^{[1]},U^{[2]}} f = \sum_{(j_1,\ldots,j_p)} \Big(U_{j_1}^{[2]} \ldots U_{j_p}^{[p+1]} D_{U^{[1]},U^{[p+2]}} \big(\prod_k U_k^{[1]} \big) \Big).$$

Fixons $(j_1, \ldots, j_p)$ un p-uplets d'entiers distincts de $\{i_1, \ldots, i_r\}$. Notons I l'ensemble $I = \{i_1, \ldots, i_r\} \setminus \{j_1, \ldots, j_p\}$. D'après le cas $p = 1$, on a :

$$D_{U^{[1]},U^{[p+2]}} \big(\prod_{k \in I} U_k^{[1]} \big) = \sum_{i \in I} U_i^{[p+2]} \prod_{j \in I \setminus \{i\}} U_k^{[1]}$$

Ceci entraîne le résultat.

En particulier, on obtient :

$$\widehat{f_r} = \sum_{(j_1,\ldots,j_{r-1})} \Big(U_{j_1}^{[2]} \ldots U_{j_{r-1}}^{[r]} \prod_k U_k^{[1]} \Big).$$

Lorsque $(j_1, \ldots, j_{r-1})$ est fixé dans $\{i_1, \ldots, i_r\}$, le produit qui apparaît est réduit au facteur $U_{j_r}^{[1]}$ où $\{j_r\} = \{i_1, \ldots, i_r\} \setminus \{j_1, \ldots, j_{r-1}\}$. On a donc

$$\widehat{f_r} = \sum_{(j_1,\ldots,j_r)} U_{j_1}^{[1]} U_{j_1}^{[2]} \ldots U_{j_r}^{[r]} \ ,$$

et la somme porte sur toutes les suites $(j_1, \ldots, j_r)$ d'entiers distincts de l'ensemble $\{i_1, \ldots, i_r\}$ (il y a $r\,!$ termes dans cette somme : autant que de permutations de $\{i_1, \ldots, i_r\}$).

On obtient alors le résultat en sommant les polarisations des $f_{(i_1,\ldots,i_r)}$.

11.2. G agit sur k^n via $\sigma.(x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$. G agit alors sur k^{nN} via $g.(u_1, \ldots, u_N) = (g.u_1, \ldots, g.u_N)$, ce qui définit une action de G

sur $k[U^{[1]},\dots,U^{[N]}]$: c'est l'action qui est proposée par l'énoncé. En 10.3., on a vu que si $f \in k[U]$ est invariant pour l'action de G sur $k[U]$, alors $D_{U,Y}f$ est invariant pour l'action de G sur $k[U,Y]$. On généralise alors facilement au cas de p dérivations successives pour en déduire que pour tout $p \leq N$, $\widehat{f_p}$ est invariant pour l'action de G sur $k[U^{[1]},\dots,U^{[p]}]$. En particulier, $\widehat{f_r}$ est invariant pour l'action de G sur $k[U^{[1]},\dots,U^{[r]}]$.
Dans la présente situation, φ_r est invariant pour l'action de G sur $k[U^{[1]}]$. Donc $\widehat{\varphi}_r$ est invariant pour l'action de G sur $k[U^{[1]},\dots,U^{[r]}]$ pour $1 \leq r \leq n$. Il en résulte immédiatement que les $\psi_{\underline{\alpha}}$ sont invariants pour l'action de G sur A si $\underline{\alpha}$ est dans M.

11.3. La polarisation totale de $\sigma_\nu(U)$ est la somme des polarisations totales des polynômes $(U_j)^\nu$ pour $1 \leq j \leq n$. La polarisation totale de $(U_j)^\nu$ est immédiate à calculer : c'est

$$\widehat{(U_j)^\nu} = \nu\,!\,U_j^{[1]}\dots U_j^{[\nu]}.$$

On a donc

$$\widehat{\sigma_\nu}(U^{[1]},\dots,U^{[\nu]}) = \nu\,!\sum_{j=1}^{n} U_j^{[1]}\dots U_j^{[\nu]}.$$

Si $\gamma_1,\dots,\gamma_\nu$ sont des entiers entre 1 et N, on a :

$$\widehat{\sigma_\nu}(U^{[\gamma_1]},\dots,U^{[\gamma_\nu]}) = \nu\,!\sum_{j=1}^{n} U_j^{[\gamma_1]}\dots U_j^{[\gamma_\nu]}.$$

On prend alors par exemple les a_1 premiers γ égaux à 1, les a_2 suivants égaux à 2, jusqu'aux a_N derniers égaux à N, ce qui est possible par définition de ν. Avec cette suite $\gamma_1,\dots,\gamma_\nu$, on obtient :

$$P_{\underline{a}}(U^{[1]},\dots,U^{[N]}) = \frac{1}{\nu\,!}\widehat{\sigma_\nu}(U^{[\gamma_1]},\dots,U^{[\gamma_\nu]}).$$

On sait que σ_ν est un polynôme en $\varphi_1,\dots,\varphi_n$ (σ_ν est symétrique). Il est clair que grâce aux propriétés des dérivations, $\widehat{\sigma_\nu}$ est un polynôme en les φ_i ainsi qu'en les diverses dérivations des φ_i. D'après 10.4.2., chacune de ces dernières fonctions est proportionnelle à un certain $\psi_{\underline{\alpha}}$ pour un $\underline{\alpha} \in M$. $\widehat{\sigma_\nu}$ est donc un polynôme en les $\psi_{\underline{\alpha}}$, et il en est ainsi de même de $P_{\underline{a}}$.

11.4. La relation $\overline{\varphi_1}(\overline{U}) = \varphi_1(U) - U_1$ est bien claire. Pour r entre 2 et $n-1$, on a :

$$\begin{aligned}\varphi_r(U) &= \sum_{1\leq i_1<\dots<i_r\leq n} U_{i_1}\dots U_{i_r}\\ &= \sum_{2\leq i_1<\dots<i_r\leq n} U_{i_1}\dots U_{i_r} + \sum_{1=i_1<i_2<\dots<i_r\leq n} U_{i_1}\dots U_{i_r}\\ &= \overline{\varphi_r}(\overline{U}) + U_1\overline{\varphi_{r-1}}(\overline{U}).\end{aligned}$$

Montrons que les polarisations totales des $\overline{\varphi_r}$ peuvent s'écrire comme des polynômes en les $\psi_{\underline{\alpha}}$ avec des coefficients dans $k[U_1^{[1]},\dots,U_1^{[N]}]$.

Cette assertion est vraie *de visu* pour $\overline{\varphi_1}$. Supposons que l'assertion soit vraie pour l'entier $r-1$ et montrons qu'elle est vraie pour r.
D'après ce qui précède et la linéarité de la dérivation, on a tout de suite :

$$\widehat{\overline{\varphi_r}} = \widehat{\varphi_r} - \big(\widehat{U_1\overline{\varphi_{r-1}}}(\overline{U})\big).$$

Comme $\widehat{\varphi_r}$ est l'un des $\psi_{\underline{\alpha}}$ (à un coefficient près), tout revient donc à montrer que $\big(\widehat{U_1\overline{\varphi_{r-1}}}(\overline{U})\big)$ est un polynôme en les $\psi_{\underline{\alpha}}$ à coefficients dans $k[U_1^{[1]},\dots,U_1^{[N]}]$. Or on montre facilement par récurrence sur k (on vous conseille d'effectuer les calculs pour $1 \le k \le 4$) que :

$$\begin{aligned} D_{U^{[1]},U^{[k]}} \dots D_{U^{[1]},U^{[2]}} \big(\widehat{U_1\overline{\varphi_{r-1}}}(\overline{U})\big) &= U_1 D_{U^{[1]},U^{[k]}} \dots D_{U^{[1]},U^{[2]}} \overline{\varphi_{r-1}} \\ &\quad + \sum_{j=2}^{k} U_1^{[j]} \prod_{k\ge i\ge 2, i\ne j} D_{U^{[1]},U^{[i]}} \overline{\varphi_{r-1}}. \end{aligned}$$

En particulier, on obtient

$$\big(\widehat{U_1\overline{\varphi_{r-1}}}(\overline{U})\big) = D_{U^{[1]},U^{[r]}} \widehat{\overline{\varphi_{r-1}}} + \sum_{j=2}^{r} U_1^{[j]} \prod_{r\ge i\ge 2, i\ne j} D_{U^{[1]},U^{[i]}} \overline{\varphi_{r-1}}.$$

Fixons $j \in \{2,\dots,r\}$, $\prod_{r\ge i\ge 2, i\ne j} D_{U^{[1]},U^{[i]}} \overline{\varphi_{r-1}}$ est alors le polynôme

$$\widehat{\overline{\varphi_{r-1}}}(U^{[1]},\dots,U^{[j-1]},U^{[j+1]},\dots,U^{[r]}) \ ,$$

qui est par hypothèse de récurrence un polynôme en les $\psi_{\underline{\alpha}}$ à coefficients dans $k[U_1^{[1]},\dots,U_1^{[N]}]$. On a aussi vu que $D_{U^{[1]},U^{[r]}} \widehat{\overline{\varphi_{r-1}}}$ est le polynôme

$$\widehat{\overline{\varphi_{r-1}}}(U^{[r]},U^{[2]},\dots,U^{[r-1]}) \ ,$$

qui est aussi un polynôme en les $\psi_{\underline{\alpha}}$ à coefficients dans $k[U_1^{[1]},\dots,U_1^{[N]}]$. Le résultat en découle tout de suite.

11.5. Pour $n = 1$, le résultat est trivial.
Supposons le résultat vrai pour l'entier $n-1$. Nommons $\mathcal{B}$ la k-algèbre engendrée par les polynômes $\psi_{\underline{\alpha}}$ où $\underline{\alpha}$ prend toute les valeurs possibles dans M et soit S_n le groupe symétrique d'ordre n.
D'après 11.2., on a $\mathcal{B} \subset A^{S_n}$. Soit alors $P \in A^{S_n}$. On peut écrire de façon unique :

$$P = \sum_a (U_1^{[1]})^{a_1} \dots (U_1^{[N]})^{a_N} T_a$$

où $T_a \in \{k(U_i^{[j]}) ; \quad 1 \le j \le N \quad , \ 2 \le i \le n\}$. Notons S_{n-1} le groupe des permutations de $\{2,\dots,n\}$. P est invariant par S_{n-1} et chaque $(U_1^{[1]})^{a_1} \dots (U_1^{[N]})^{a_N}$ est invariant par S_{n-1}. Il en résulte que pour tout a, $T_a \in A^{S_{n-1}}$. Donc T_a est par hypothèse de récurrence un polynôme en les $\widehat{\overline{\varphi_r}}$ pris en $\overline{U}^{[\alpha_1]},\dots,\overline{U}^{[\alpha_r]}$ et d'après la question 11.4., T_a est un polynôme en les $\psi_{\underline{\alpha}}$ à coefficients dans $k[U_1^{[1]},\dots,U_1^{[N]}]$.
On peut donc écrire

$$P = \sum_b (U_1^{[1]})^{b_1} \dots (U_1^{[N]})^{b_N} Q_b$$

où pour tout b, Q_b est un polynôme en les $\psi_{\underline{\alpha}}$ à coefficients dans k. Q_b est en particulier invariant par S_n. Pour tout $2 \le j \le n$, écrivons que P est invariant par la transposition qui échange 1 et j. On obtient :

$$P = \sum_b (U_j^{[1]})^{b_1} \dots (U_j^{[N]})^{b_N} Q_b.$$

On en déduit alors que

$$P = \frac{1}{n}\sum_b \Big(\sum_{j=1}^n (U_j^{[1]})^{b_1}\dots(U_j^{[N]})^{b_N}\Big)Q_b$$

Or d'après 11.3., pour tout b, $\displaystyle\sum_{j=1}^n (U_j^{[1]})^{b_1}\dots(U_j^{[N]})^{b_N}$ est un polynôme en les $\psi_{\underline{\alpha}}$ à coefficients dans k. Il en est donc de même de P.

12. Application

12.1. On a :

$$\begin{aligned}\widetilde{J}(u_1^{[1]},\dots,u_j^{[i]},\dots,u_n^{[N]}) &= \frac{1}{n}\sum_{j=1}^n J(u_j^{[1]},\dots,u_j^{[N]})\\ &= \frac{1}{n}\sum_{j=1}^n J(g_j.u)\\ &= \frac{1}{n}\sum_{j=1}^n J(u)\\ &= J(u).\end{aligned}$$

On a utilisé que J est invariant en écrivant $J(g_j.u) = J(u)$ pour $1 \le j \le n$.

12.2. Soit $\sigma \in S_n$. On a :

$$\begin{aligned}\sigma.\widetilde{J} &= \frac{1}{n}\sum_{j=1}^n \sigma.J(U_j^{[1]},\dots,U_j^{[N]})\\ &= \frac{1}{n}\sum_{j=1}^n J(U_{\sigma(j)}^{[1]},\dots,U_{\sigma(j)}^{[N]})\\ &= \frac{1}{n}\sum_{k=1}^n J(U_k^{[1]},\dots,U_k^{[N]})\\ &= \widetilde{J}.\end{aligned}$$

Donc $\widetilde{J}$ est invariant par S_n.

12.3. γ est une bijection de Σ sur l'ensemble des monômes non constants de $k[X_1,\dots,X_N]$ de degré total inférieur ou égal à n. En effet donnons-nous un tel monôme P. On peut écrire $P = X_1^{a_1}\dots X_N^{a_N}$ où $a_1,\dots,a_N$ sont des entiers positifs ou nuls tels que $1 \le r = a_1 + \dots + a_N \le n$. Au plus r entiers a_i sont non nuls. Appelons-les $a_{j_1},\dots,a_{j_q}$: les entiers a_{j_k} sont distincts non nuls, de somme r et P s'écrit $P = X_{j_1}^{a_{j1}}\dots X_{j_q}^{a_{j_q}}$ avec $j_1 < \dots < j_q$. Si $\underline{\alpha}$ est un élément de Σ tel que $\gamma(\underline{\alpha}) = P$, alors nécessairement la taille de $\underline{\alpha}$ vaut r (en effet le degré de $\gamma(\underline{\alpha})$ n'est autre que la taille de $\underline{\alpha}$). On voit alors que les a_{j_1} premiers éléments de $\underline{\alpha}$ doivent être pris égaux à j_1, les a_{j_2} suivants égaux à j_2, et ainsi de suite jusqu'aux a_{j_q} derniers égaux à j_q. Ceci montre l'injectivité de γ, mais aussi la surjectivité sans trop de fatigue.
Soit alors r un entier compris entre 1 et n. Comptons le nombre de monômes de $k[X_1,\dots,X_N]$ de degré r. Se donner un tel monôme revient à se donner un

N-uplet d'entiers $(a_1, \ldots, a_N)$ tels que $a_1 + \ldots + a_N = r$. Il est classique que le nombre cherché est

$$\Gamma_N^r = C_{N+r-1}^r = C_{N+r-1}^{N-1}.$$

Redémontrons ceci. Pour voir plus facilement les choses, on va associer un code à chaque N-uplet d'entiers $(a_1, \ldots, a_N)$ tels que $a_1 + \ldots + a_N = r$. Les codes sont formés de traits et de croix. On se donne $N-1$ traits verticaux qui déterminent N places (une à gauche du premier, une à droite du dernier et $N-2$ places entre les deux traits extrémaux). On met alors a_i croix à la i-ème place. Il y a donc r croix.
Par exemple, pour $N = 6$ et $r = 7$, le sextuplet $(1, 0, 3, 2, 0, 1)$ est représenté par le code

$$\times | \, | \ \times \times \times \ | \ \times \times \, | \, | \times$$

Il est clair qu'il y a une bijection entre les N-uplets d'entiers $(a_1, \ldots, a_N)$ tels que $a_1 + \ldots + a_N = r$ et les codes correspondants. D'autre part, un tel code est entièrement déterminé dès que l'on s'est donné la place des $N-1$ traits (ou des r croix) dans la succession des $r + N - 1$ symboles qui constituent le code. Il y a donc C_{N+r-1}^{N-1} tels codes. D'où le résultat. Cette démonstration se trouve par exemple dans le livre d'Alain Combrouze, *Probabilités /1, PUF*.
On en déduit que le nombre de monômes de $k[X_1, \ldots, X_N]$ de degré inférieur ou égal à n est :

$$\sharp = \sum_{r=1}^{n} C_{N+r-1}^{N-1} = \sum_{r=1}^{n} \Big(C_{N+r}^{N} - C_{N+r-1}^{N} \Big) = C_{n+N}^{N} - 1.$$

Le cardinal de Σ est donc

$$\sharp = C_{n+N}^{N} - 1 = \frac{(N+1)\ldots(N+n)}{n\,!} - 1.$$

12.4. Via 12.1., l'application qui à $J \in S(V)^G$ associe $\widetilde{J} \in A^{S_n}$ est injective. On sait d'après 11.5. que A^{S_n} est engendrée par un nombre fini d'éléments, il en est donc de même de $S(V)^G$. On sait que A^{S_n} est engendrée par les $\psi_{\underline{\alpha}}$ où $\underline{\alpha} \in M$. Mais d'après l'expression de $\widehat{\varphi_r}$ trouvée en 11.1., l'ensemble des $\psi_{\underline{\alpha}}$ où $\underline{\alpha} \in M$ est le même que celui des $\psi_{\underline{\alpha}}$ où $\underline{\alpha} \in \Sigma$: si $(\alpha_1, \ldots, \alpha_r)$ et $(\beta_1, \ldots, \beta_r)$ décrivent le même ensemble, alors on a

$$\widehat{\varphi_r}(U^{[\alpha_1]}, \ldots, U^{[\alpha_r]}) = \widehat{\varphi_r}(U^{[\beta_1]}, \ldots, U^{[\beta_r]}).$$

Le nombre de générateurs de A^{S_n} est ainsi majoré par le cardinal de Σ. Le nombre de générateurs de $S(V)^G$ est ainsi majoré par $\dfrac{(N+1)\ldots(N+n)}{n\,!} - 1$.

6.3 Commentaires

Le sujet est, c'est une tradition, excessivement long et deux bonnes dizaines d'heures de travail ne seront pas de trop pour en venir à bout. Cela dit, pratiquement toutes les questions seront à la portée du candidat qui aura fait l'effort de bien comprendre les définitions (ce qui réclame parfois une bonne capacité d'abstraction). Les connaissances requises restent à un niveau élémentaire. En

vrac, groupes, polynômes à plusieurs variables (il faut absolument savoir traiter la première question !), polynômes homogènes, symétriques, algèbre linéaire et bilinéaire de base, faits élémentaires sur les séries formelles et un brin de combinatoire vous attendent au détour de ce sujet. C'est là l'occasion d'éprouver la solidité de vos connaissances de base en algèbre. Ce sujet est à ce titre un excellent test, que nous ne pouvons que recommander.

Chapitre 7

Session de 1995

7.1 Sujet

7.2 Correction

I. Spectre des matrices positives

1. Notons $A = (a_{i,j})_{\substack{1\leq i\leq n\\ 1\leq j\leq n}}$ et $y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$.

a. Chaque coordonnée de z s'écrit $z_i = \sum_{j=1}^{n} a_{i,j}y_j + y_i$. Comme A et y sont positifs, il est clair que z est un vecteur positif de $\mathbb{C}^n$. Pour tout vecteur positif, soit $Z(y) = \{i \in \{1,\dots,n\}\,,\, y_i = 0\}$. On a

$$z_i = \sum_{j\notin Z(y)} a_{i,j}y_j + y_i \geq y_i \geq 0.$$

Si $z_i = 0$ alors nécessairement $y_i = 0$ donc $Z(z) \subset Z(y)$.

Supposons que $Z(y) \neq \emptyset$ alors $Z(y) = \{k_1,\dots,k_l\}$ où l est le cardinal de $Z(y)$. Si $Z(z) = Z(y)$ alors pour tout $i \in Z(y)$, $\sum_{j\notin Z(y)} a_{i,j}y_j = 0$. Or pour tout $j \notin Z(y)$, $y_j > 0$ donc nécessairement,

$$\forall i \in Z(y),\, \forall j \notin Z(y),\, a_{i,j} = 0.$$

Soit σ la permutation de $\{1,\dots,n\}$ telle que $\sigma(1) = k_1,\dots,\sigma(l) = k_l$ et P la matrice de permutation associée à σ dont les coefficients sont définis par $p_{i,j} = \delta_{\sigma(i),j}$ ($\delta_{i,j}$ désigne le symbole de Kronecker). On a alors $P^{-1} = (\delta_{i,\sigma(j)})_{\substack{1\leq i\leq n\\ 1\leq j\leq n}}$ donc pour tout $1 \leq i,j \leq n$,

$$(PAP^{-1})_{i,j} = \sum_{k=1}^{n} a_{\sigma(i),k}\delta_{\sigma(j),k} = a_{\sigma(i),\sigma(j)}.$$

Ainsi, pour tout $i = 1,\dots,l$, $j = l+1,\dots,n$, $(PAP^{-1})_{i,j} = 0$ puisque $\sigma(i) \in Z(y)$ et $\sigma(j) \notin Z(y)$, ce qui contredit le fait que A soit irréductible. On en conclut que si $Z(y) \neq \emptyset$, $\mathrm{card}Z(z) \leq \mathrm{card}Z(y) - 1$.

b. Si $Z(y) = \emptyset$ alors y est strictement positif . On vient de voir que $Z(z) \subset Z(y)$ donc $(\mathrm{I} + A)y$ est strictement positif d'où l'on déduit que $(I + A)^{n-1}y$ est strictement positif.

Sinon, $Z(y) \neq \emptyset$ donc $\mathrm{card}Z(y) \geq 1$. Comme y est positif, il est clair que $(\mathrm{I} + A)^{n-1}y$ est positif. Par une récurrence évidente, on sait par la question précédente que $\mathrm{card}Z((\mathrm{I} + A)^{n-1}y) \leq \max(0, \mathrm{card}Z(y) - (n-1))$. Or y est un vecteur non nul donc $\mathrm{card}Z(y) \leq n-1$ ce qui prouve que $(\mathrm{I} + A)^{n-1}y$ est strictement positif.

c. Les vecteurs e_i, $i = 1,\dots,n$ de la base canonique de $\mathbb{C}^n$ sont des vecteurs positifs non nuls. Ainsi, d'après la question précédente, pour tout $i = 1,\dots,n$, $(\mathrm{I} + A)^{n-1}e_i$ est strictement positif donc la matrice $(\mathrm{I} + A)^{n-1}$ est strictement positive.

2.a. Soit $R = \sup\{\rho \text{ tel que } \forall i, \rho x_i \leq (Ax)_i\}$. Prouvons que $R = r(x)$.

Pour tout $i \in I$, $r(x)x_i \leq (Ax)_i$. D'autre part, si $i \notin I$, $x_i = 0$ et comme A et x sont positifs, pour tout $i \notin I$, $(Ax)_i \geq 0$. On en déduit que $r(x) \leq R$.

De plus, par définition du supremum, pour tout $\varepsilon > 0$, il existe $\rho_\varepsilon \in [R-\varepsilon, R]$ tel que pour tout $i = 1, \ldots, n$, $\rho_\varepsilon x_i \leq (Ax)_i$. Donc $\rho_\varepsilon \leq r(x)$ et en faisant tendre ε vers zéro, on obtient $R \leq r(x)$.

b. Par définition, si $x \in Q^+$, $r(x) = \min\limits_{i=1,\ldots,n} \dfrac{(Ax)_i}{x_i}$. Or les applications définies sur Q^+ par $x \mapsto \frac{(Ax)_i}{x_i}$ sont continues. En utilisant la relation suivante permettant de determiner le minimum de deux nombres réels quelconques,

$$\min(a, b) = \frac{a + b - |a - b|}{2},$$

on montre facilement par récurrence que le minimum de n fonctions continues en un point est continue en ce point. L'application $r : Q^+ \to \mathbb{R}$ est ainsi continue.

c. (i) En tant qu'intersection d'un fermé borné et d'un fermé de $\mathbb{C}^n$, E est un fermé borné de $\mathbb{C}^n$. L'application $(\mathrm{I} + A)^{n-1}$ est linéaire donc continue sur $\mathbb{C}^n$. L'image de E par cette application est alors une partie compacte de $\mathbb{C}^n$. D'autre part, pour tout $x \in E$, x est un vecteur positif non nul puisque $x_i \geq 0$ et $\sum_{i=1}^n x_i^2 = 1$. Par le 1.b., on en déduit que pour tout $x \in E$, $(\mathrm{I} + A)^{n-1}x \in Q^+$.

(ii) D'après le 2.a., pour tout $x \in E$, pour tout $i = 1, \ldots, n$, on a $r(x)x_i \leq (Ax)_i$ donc le vecteur $z = ((Ax)_i - r(x)x_i)_{1 \leq i \leq n}$ est positif. Comme $(\mathrm{I}+A)^{n-1}$ est un polynôme en A, les matrices A et $(\mathrm{I}+A)^{n-1}$ commutent. Soit $y = (\mathrm{I}+A)^{n-1}x$ alors

$$Ay = (\mathrm{I} + A)^{n-1} \begin{pmatrix} (Ax)_1 \\ \vdots \\ (Ax)_n \end{pmatrix}.$$

Mais la matrice $(\mathrm{I}+A)^{n-1}$ est positive donc $(\mathrm{I}+A)^{n-1}z$ est positif ce qui donne pour tout $i = 1, \ldots, n$,

$$(Ay)_i - r(x)y_i = \big((\mathrm{I} + A)^{n-1}(Ax)\big)_i - r(x)y_i = \big((\mathrm{I} + A)^{n-1}(Ax - r(x)x)\big)_i \geq 0.$$

Ainsi pour tout $i = 1, \ldots, n$, $(Ay)_i \geq r(x)y_i$ d'où $r(y) \geq r(x)$.

(iii) Comme F est un compact de $\mathbb{C}^n$, $F \subset Q^+$ et r est continue sur Q^+, alors r est bornée et atteint son maximum sur F. Soit $y_0 \in F$ tel que $r(y_0) = \max\limits_{y \in F} r(y)$. Par la définition de r, on constate que pour tout $\lambda > 0$, $r(\lambda x) = r(x)$. Comme y_0 est strictement positif, $\|y_0\| \neq 0$ donc $x_0 = \frac{y_0}{\|y_0\|} \in E$ et vérifie $r(x_0) = r(y_0)$. Ainsi, $\max\limits_{x \in E} r(x) \geq \max\limits_{y \in F} r(y)$. Mais d'après le (ii), on sait que pour tout $x \in E$, $r(x) \leq r(y)$ où $y = (\mathrm{I} + A)^{n-1}x \in F$ ce qui prouve que pour tout $x \in E$, $r(x) \leq \max\limits_{y \in F} r(y)$. On a donc

$$\max_{x \in E} r(x) = \max_{y \in F} r(y)$$

(iv) Comme $F \subset Q^+$, $r = 0$ si et seulement si pour tout $y \in F$, Ay a au moins une coordonnée nulle. Or $F = \{(\mathrm{I} + A)^{n-1}x \,;\, x \in E\}$ donc

$$r = 0 \Leftrightarrow \{\forall x \in E, (\mathrm{I} + A)^{n-1}(Ax) \text{ a une coordonnée nulle}\},$$

car A et $(\mathrm{I}+A)^{n-1}$ commutent. Or A est positive et irréductible donc par le 1.c., $(\mathrm{I}+A)^{n-1}$ est strictement positive ce qui prouve que $r=0 \Leftrightarrow \{\forall x \in E, Ax=0\}$. Comme les vecteurs de la base canonique appartiennent à E, on en conclut que $r=0 \Leftrightarrow A=0$. Ici A est irréductible donc elle est non nulle et $r>0$.

d. Soit z tel que $r(z)=r$ et $t=(\mathrm{I}+A)^{n-1}z$. Par définition de z et r, $Az-rz$ est un vecteur positif. Supposons que $Az-rz$ soit non nul. Comme A et $(\mathrm{I}+A)^{n-1}$ commutent, $At-rt=(\mathrm{I}+A)^{n-1}(Az-rz)$. Par le 1.b., $At-rt$ est un vecteur strictement positif, donc $r(t)>r$ ce qui n'est pas possible car $t \in F$ et $r=\max_{y\in F} r(y)$. On en conclut que $z \in \ker(r\mathrm{I}-A) \neq \{0\}$ puisque $z \in E$..

e. Si $Z(z) \neq \emptyset$ alors comme $Az=rz$, pour tout $i \in Z(z), (Az)_i=0$. Mais $(Az)_i = \sum_{j\notin Z(z)} a_{i,j}z_j$ et pour tout $j \notin Z(z)$, $z_j>0$ donc

$$\forall i \in Z(z),\ \forall j \notin Z(z),\ a_{i,j}=0.$$

Comme dans le 1.a., on prouve alors que la matrice A est réductible ce qui est contradictoire. Ainsi, si $z \in E$ vérifie $r(z)=r$ alors z est strictement positif.

f. Comme y est vecteur propre de A associé à la valeur propre α alors pour tout $i=1,\ldots,n$, $\alpha y_i=\sum_{j=1}^n a_{i,j}y_j$ et par l'inégalité triangulaire, on en déduit que $|\alpha||y_i| \leq \sum_{j=1}^n |a_{i,j}||y_j|$. Or A est positive donc $|a_{i,j}|=a_{i,j}$ et $Ay_+-|\alpha|y_+$ est positif.

Un vecteur propre est par définition non nul. Soit $z=\frac{y_+}{\|y\|}$ alors $z \in E$ et on vient de voir que pour tout $i=1,\ldots,n$, $(Az)_i \geq |\alpha|z_i$ donc $r(z) \geq |\alpha|$. Cela prouve que $r \geq |\alpha|$.

g. Par le 2.c., on sait que $\ker(r\mathrm{I}-A) \neq \{0\}$ donc $\dim\ker(r\mathrm{I}-A) \geq 1$.

Soit y un vecteur propre de A associé à la valeur propre r. Par la question précédente, on sait que $Ay_+ \geq ry_+$ donc $r(y_+) \geq r$. Mais $\frac{y_+}{\|y\|} \in E$ et on a vu au 2.c.(iii). que $r(\frac{y_+}{\|y\|})=r(y_+)$ donc, par définition de r, $r=r(y_+)$. D'après le 2.d., on sait alors que $y_+ \in \ker(r\mathrm{I}-A)$. Par le 2.e., y_+ est strictement positif donc pour tout $i=1,\ldots,n$, $y_i \neq 0$. On en conclut que si $y \in \ker(r\mathrm{I}-A)$ alors soit $y=0$, soit toutes ses coordonnées sont non nulles.

D'autre part, soient v, w deux vecteurs propres de A associé à la valeur propre r. Par le résultat précédent, les coordonnées de v et de w sont non nulles. Posons $\lambda=\frac{v_1}{w_1}$ alors $v-\lambda w \in \ker(r\mathrm{I}-A)$ et sa première coordonnée est nulle donc nécessairement $v=\lambda w$ et $\dim\ker(r\mathrm{I}-A)=1$.

3. Soient y et z deux vecteurs propres positifs de A associés respectivement aux valeurs propres λ et μ. Comme A est positive, λ et μ sont deux réels positifs. On peut supposer que $\lambda \leq \mu$. Comme $y \geq 0$, $y \neq 0$, on sait par le 1.b. que $(\mathrm{I}+A)^{n-1}y$ est strictement positif. Or $(\mathrm{I}+A)^{n-1}y=(1+\lambda)^{n-1}y$ et $\lambda \geq 0$ donc y est strictement positif.

Soit $\alpha=\max_{1\leq i\leq n} \frac{z_i}{y_i}$ alors $\alpha y-z$ est positif et il existe i_0 tel que $\alpha y_{i_0}-z_{i_0}=0$. Si $\alpha y-z \neq 0$ alors par le 1.b., $(\mathrm{I}+A)^{n-1}(\alpha y-z)$ est strictement positif. En particulier, $(1+\lambda)^{n-1}\alpha y_{i_0} > (1+\mu)^{n-1}z_{i_0}$. Mais $\alpha y_{i_0}=z_{i_0}$ et $\lambda \leq \mu$ donc cette inégalité est impossible. On en conclut que y et z sont colinéaires et $\lambda=\mu$.

Remarque : on a vu au 2. qu'il existe un vecteur propre strictement positif associé à la valeur propre r. Cette question établit que seul le sous-espace propre $\ker(r\mathrm{I}-A)$ contient des vecteurs propres positifs.

4.a. Soit y un vecteur propre de B associé à la valeur propre γ. Pour tout $i = 1, \ldots, n$, $\gamma y_i = \sum_{j=1}^{n} b_{i,j} y_j$ et par l'inégalité triangulaire, on a

$$|\gamma||y_i| \leq \sum_{j=1}^{n} |b_{i,j}||y_j|.$$

Comme $|b_{i,j}| \leq a_{i,j}$ alors $Ay_+ \geq |\gamma| y_+$. En posant $z = \frac{y_+}{\|y\|}$, on constate que $z \in E$ et que $r(z) \geq |\gamma|$ ce qui prouve que $r \geq |\gamma|$.

b. Supposons que $|\gamma| = r$. Soit y un vecteur propre de B associé à la valeur propre γ alors comme B est positive, on a

$$Ay_+ \geq By_+ \geq |\gamma| y_+ = r y_+.$$

On en déduit que $r(y_+) = r$ et par le 2.d. que $Ay_+ = r y_+$. Par le 2.e., on sait alors que y_+ est strictement positif. On a aussi pour tout $i = 1, \ldots, n$,

$$r\,|y_i| \leq \sum_{j=1}^{n} b_{i,j}|y_j| \leq \sum_{j=1}^{n} a_{i,j}|y_j| = r|y_i|$$

et $0 \leq b_{i,j} \leq a_{i,j}$ donc nécessairement $A = B$ ce qui est contradictoire et prouve que $|\gamma| < r$.

5. Soit α une valeur propre de A telle que $|\alpha| = r$ et y un vecteur propre de A associé à la valeur propre α. On a $Ay = \alpha y$ donc $Ay_+ = r y_+$ car $|\alpha| \leq r(y_+) \leq r$. Par le 2.e., tous les y_i sont non nuls. De plus, on a aussi pour tout $i = 1, \ldots, n$

$$|\sum_{j=1}^{n} a_{i,j} y_j| = |(Ay)_i| = |\alpha y_i| = r|y|_i = \sum_{j=1}^{n} a_{i,j}|y_j|.$$

Comme A est strictement positive, tous les $y_j, j = 1, \ldots, n$ ont le même argument (cas d'égalité dans l'inégalité triangulaire pour les complexes) et pour tout $j = 1, \ldots, n$, $y_j = |y_j|\, e^{i\theta}, \theta \in [0, 2\pi\,[$. L'égalité $Ay = \alpha y$ s'écrit alors $Ay_+ = \alpha y_+$ ce qui prouve que $\alpha = r$. On en conclut que si α est une valeur propre de A autre que celle de module maximal r, on a $|\alpha| < r$.

6.a. Répondons à cette question par contraposée. Si A est réductible, il existe une matrice de permutation P telle que

$$PAP^{-1} = \begin{pmatrix} B & 0 \\ C & D \end{pmatrix},$$

avec B, D matrices carrées. Pour tout $p \in \mathbb{N}$, il existe une matrice C_p rectangulaire telle que

$$PA^pP^{-1} = \begin{pmatrix} B^p & 0 \\ C_p & D^p \end{pmatrix}.$$

On en conclut que la matrice PA^pP^{-1} ne peut être strictement positive pour aucun entier p et comme P est une matrice de permutation, pour tout $p \in \mathbb{N}$, A^p n'est pas strictement positive.

b. D'après le 2.d., $\ker(r\mathrm{I} - A) \neq \{0\}$. Comme on travaille sur le corps des complexes, toutes les valeurs propres de A^p sont de la forme α^p où α est

valeur propre de A (il suffit pour cela de trigonaliser A). En particulier, r^p est la valeur propre positive de module maximal de A^p et par le 2.g., on sait que $\dim\ker(r^p\mathrm{I} - A^p) = 1$. Or $\ker(r\mathrm{I} - A) \subset \ker(r^p\mathrm{I} - A^p)$ donc $\ker(r\mathrm{I} - A) = \ker(r^p\mathrm{I} - A^p)$.

Soit α une valeur propre de A (c'est à dire $\ker(\alpha\mathrm{I} - A) \neq \{0\}$) et supposons $|\alpha| = r$. Comme $\ker(\alpha\mathrm{I} - A) \subset \ker(\alpha^p\mathrm{I} - A^p)$ et A^p est strictement positive alors le 5. assure que $\alpha^p = r^p$. De plus $\dim\ker(r^p\mathrm{I} - A^p) = 1$ donc $\ker(\alpha\mathrm{I} - A) = \ker(r^p\mathrm{I} - A^p)$. On en déduit que $\ker(\alpha\mathrm{I} - A) = \ker(r\mathrm{I} - A)$ et que $\alpha = r$. Toute valeur propre $\alpha \neq r$ de A satisfait alors $|\alpha| < r$.

7. Commençons par donner une caractérisation "ensembliste" des matrices réductibles, redondantes, décomposables.

On a déjà vu au 1.a. que $C \in \mathcal{M}_\ell(\mathbb{C})$ est réductible si et seulement s'il existe une partition non triviale (I, J) de $\{1, \ldots, \ell\}$ telle que

$$\forall i \in I,\ \forall j \in J,\ c_{i,j} = 0. \tag{7.1}$$

Par définition, B est décomposable s'il existe des matrices de permutation $P \in \mathcal{M}_n(\mathbb{C})$ et $Q \in \mathcal{M}_m(\mathbb{C})$ telles que

$$PBQ = \begin{pmatrix} B' & 0 \\ 0 & B'' \end{pmatrix},$$

où $B' \in \mathcal{M}_{p,r}(\mathbb{C})$, $B'' \in \mathcal{M}_{n-p,n-r}(\mathbb{C})$ sont rectangulaires. Soit $\sigma \in \mathcal{S}_n$ telle que $P = (\delta_{\sigma(i),j})_{\substack{1\leq i\leq n\\ 1\leq j\leq n}}$ et $\tau \in \mathcal{S}_m$ telle que $Q = (\delta_{i,\tau(j)})_{\substack{1\leq i\leq m\\ 1\leq j\leq m}}$, alors on a $PBQ = (b_{\sigma(i),\tau(j)})_{\substack{1\leq i\leq n\\ 1\leq j\leq m}}$ et on trouve que B est décomposable s'il existe $\sigma \in \mathcal{S}_n$ et $\tau \in \mathcal{S}_m$ telles que

$$\begin{cases} \forall i \in \{\sigma(1), \ldots, \sigma(p)\},\ \forall j \in \{\tau(r+1), \ldots, \tau(m)\}, & b_{i,j} = 0 \\ \forall i \in \{\sigma(p+1), \ldots, \sigma(n)\},\ \forall j \in \{\tau(1), \ldots, \tau(r)\}, & b_{i,j} = 0. \end{cases}$$

Soit $I_1 = \{\sigma(1), \ldots, \sigma(p)\}$, $I_2 = \{\sigma(p+1), \ldots, \sigma(n)\}$, $J_1 = \{\tau(1), \ldots, \tau(r)\}$, $J_2 = \{\tau(r+1), \ldots, \tau(m)\}$, alors on conclut que B est décomposable s'il existe des partitions non triviales $(I_1,\ I_2)$ de $\{1, \ldots, n\}$ et $(J_1,\ J_2)$ de $\{1, \ldots, m\}$ telles que

$$\begin{cases} \forall i \in I_1,\ \forall j \in J_2,\ b_{i,j} = 0 \\ \forall i \in I_2,\ \forall j \in J_1,\ b_{i,j} = 0. \end{cases} \tag{7.2}$$

D'autre part, B est redondante lorsqu'une des deux partitions est triviale dans la caractérisation précédente.

a. Montrons que C réductible implique B non indécomposable.
Par la relation (7.1), on sait que C est réductible lorsqu'il existe une partition non triviale (L, K) de $\{1, \ldots, \ell\}$ telle que $\forall l \in L,\ \forall k \in K,\ c_{l,k} = 0$. Or par définition de C,

$$c_{l,k} = \begin{cases} b_{l,k-n} & \text{si } l \in \{1, \ldots, n\} \text{ et } k \in \{n+1, \ldots, \ell\} \\ b_{k,l-n} & \text{si } l \in \{n+1, \ldots, \ell\} \text{ et } k \in \{1, \ldots, n\} \\ 0 & \text{sinon.} \end{cases}$$

Soient $I_1 = L \cap \{1, \ldots, n\}$, $I_2 = K \cap \{1, \ldots, n\}$ et $J_1 = \{l - n\ ;\ l \in L \cap \{n+1, \ldots, \ell\}\}$, $J_2 = \{k-n\ ;\ k \in K \cap \{n+1, \ldots, \ell\}\}$. Comme (L, K) est une partition

de $\{1,\dots,\ell\}$, (I_1,I_2) (respectivement (J_1,J_2)) est une partition de $\{1,\dots,n\}$ (respectivement de $\{1,\dots,m\}$).

De plus, pour tout $i\in I_1, j\in J_2$, il existe $l\in L\cap\{1,\dots,n\}$ et $k\in K\cap\{n+1,\dots,\ell\}$ tels que $i=l$ et $j=k-n$ donc $b_{i,j}=b_{l,k-n}=c_{l,k}=0$. De même pour $i\in I_2, j\in J_1$, il existe $k\in K\cap\{1,\dots,n\}$ et $l\in L\cap\{n+1,\dots,\ell\}$ tels que $i=k$ et $j=l-n$ donc $b_{i,j}=b_{k,l-n}=c_{l,k}=0$. On a donc trouvé deux partitions (dont l'une est non triviale car (L,K) est une partition non triviale de $\{1,\dots,\ell\}$) telles que la relation (7.2) soit vérifiée ce qui prouve que B est décomposable ou que B est redondante.

Montrons que B non indécomposable implique B réductible.
Par la relation (7.2), on sait que B est non indécomposable lorsqu'il existe des partitions (dont l'une est non triviale) (I_1,I_2) de $\{1,\dots,n\}$ et (J_1,J_2) de $\{1,\dots,m\}$ telles que

$$\begin{cases} \forall i\in I_1,\ \forall j\in J_2,\ b_{i,j}=0\\ \forall i\in I_2,\ \forall j\in J_1,\ b_{i,j}=0. \end{cases}$$

Soient $K_1=\{j+n; j\in J_1\}$, $K_2=\{j+n; j\in J_2\}$, $L=I_1\cup K_1$, $K=I_2\cup K_2$ alors (L,K) est une partition non triviale de $\{1,\dots,\ell\}$. On distingue trois cas pour déterminer la valeur de $c_{l,k}$ lorsque $l\in L$, $k\in K$:

1. Si $(l,k)\in I_1\times I_2\subset\{1,\dots,n\}^2$ ou si $(l,k)\in K_1\times K_2\subset\{n+1,\dots,\ell\}^2$ alors par définition de C, $c_{l,k}=0$.
2. Si $l\in I_1$ et $k\in K_2$ alors il existe $i\in I_1$, $j\in J_2$ tels que $l=i$ et $k=n+j$ donc $c_{l,k}=c_{i,n+j}=b_{i,j}=0$ par définition de I_1 et J_2.
3. Si $l\in K_1$ et $k\in I_2$ alors il existe $i\in I_2$, $j\in J_1$ tels que $l=j+n$ et $k=i$ donc $c_{l,k}=c_{j+n,i}=b_{i,j}=0$ par définition de I_1 et J_2.

On en conclut que (L,K) est une partition non triviale de $\{1,\dots,\ell\}$ et que pour tout $l\in L$, pour tout $k\in K$, $c_{l,k}=0$ ce qui prouve d'après (7.1) que C est réductible.

b. Le raisonnement s'effectue par contraposée.

Si $B\,{}^tB$ est réductible, il existe une partition non triviale (I_1,I_2) de $\{1,\dots,n\}$ telle que pour tous $i\in I_1$, $j\in I_2$, $\sum_{k=1}^m b_{i,k}b_{j,k}=0$. Or B est positive donc $\forall i\in I_1,\forall j\in I_2,\forall k\in\{1,\dots,m\}$, $b_{i,k}b_{j,k}=0$ ce qui permet de définir une partition (J_1,J_2) de $\{1,\dots,m\}$ telle que

$$\begin{cases} \forall i\in I_1,\ \forall k\in J_2,\ b_{i,k}=0\\ \forall i\in I_2,\ \forall k\in J_1,\ b_{i,k}=0 \end{cases}$$

Par la relation (7.2), on sait que B est non indécomposable.
On constate que si ${}^tB$ est non indécomposable, B l'est aussi donc de la même manière, ${}^tBB$ réductible implique B non indécomposable.

D'autre part, $B\,{}^tB$ est symétrique et positive (au sens euclidien) donc elle est diagonalisable et ses valeurs propres sont positives. Ainsi toute valeur propre α de $B\,{}^tB$ distincte de la valeur propre maximale vérifie $0\leq\alpha<r$. On remarque aussi d'après le 2.g. que $\dim\ker(r\mathrm{I}-B\,{}^tB)=1$ donc l'ordre de multiplicité de r est égal à 1. Il en est de même pour ${}^tBB$.

II. Algèbres de matrices

1.a. Soit $x \in J$ non nul, c'est à dire qu'il existe $k, l \in \{1, \ldots, n\}$ tels que $x_{k,l} \neq 0$. Comme J est un idéal bilatère, pour tout $i, j \in \{1, \ldots, n\}$, $E_{i,k} x E_{k,j} \in J$. Or $E_{i,k} x E_{l,j} = x_{k,l} E_{i,j}$ et $x_{k,l} \neq 0$ donc $E_{i,j} \in J$. L'idéal J contient tous les éléments d'une base de M donc $J = M$.

b. Comme $\{E_{i,j}; i, j \in \{1, \ldots, n\}\}$ engendre M, on a

$$Z(M) = \{x \in M; \forall i, j \in \{1, \ldots, n\}, x E_{i,j} = E_{i,j} x\}.$$

Or tout élément x de M s'écrit $x = \sum_{p,q} x_{p,q} E_{p,q}$ donc

$$x E_{i,j} = \sum_{p=1}^{n} x_{p,i} E_{p,j} \text{ et } E_{i,j} x = \sum_{q=1}^{n} x_{j,q} E_{i,q}.$$

Comme $(E_{i,j})_{1 \leq i,j \leq n}$ est une famille libre de M, $x \in Z(M)$ si et seulement si pour tout $i \neq j$, $x_{i,j} = 0$ et $x_{i,i} = x_{j,j}$. On en conclut que

$$Z(M) = \{\lambda \mathrm{I}; \lambda \in \mathbb{C}\}$$

où I désigne l'identité de M.

2.a. Soit $p_i = \rho(E_{i,i})$. Comme ρ est un morphisme d'algèbres avec unité, $p_1, \ldots, p_n$ sont des idempotents orthogonaux et vérifient

$$\sum_{i=1}^{n} p_i = \rho(\sum_{i=1}^{n} E_{i,i}) = \rho(\mathrm{I}) = \mathrm{I}_V$$

où I_V est l'unité de $\mathrm{End}(V)$.
Soit $V_i = \mathrm{Im} p_i$ alors il est facile de constater par la relation précédente que pour tout $v \in V$, $v = \sum_i p_i(v)$ donc

$$V = \sum_i V_i.$$

D'autre part, si $z \in V_i \cap (\sum_{j \neq i} V_j)$ alors il existe $y_1 \in V_1, \ldots, y_n \in V_n$ tels que $z = p_i(y_i) = \sum_{j \neq i} p_j(y_j)$. Or les $(p_i)_{1 \leq i \leq n}$ sont des idempotents orthogonaux donc $p_i(z) = z = \sum_{j \neq i} p_i p_j(y_j) = 0$ ce qui prouve que $V_i \cap (\sum_{j \neq i} V_j) = \{0\}$. On a donc

$$V = \bigoplus_{i=1}^{n} V_i.$$

b. Par les propriétés de morphisme d'algèbres de ρ, on sait que pour tout $i, j, k, \ell \in \{1, \ldots, n\}$

$$\rho(E_{i,j}) \rho(E_{k,\ell}) = \delta_{j,k} \rho(E_{i,\ell}).$$

Si $j \neq k$ on a donc $\rho(E_{i,j}) \rho(E_{k,k}) = 0$ ce qui prouve que $\rho(E_{i,j})_{|V_k} = 0$. On en déduit que $\rho(E_{i,j})$ agit non trivialement uniquement sur le sous-espace V_j.

On sait aussi par cette relation que $\rho(E_{i,j})\rho(E_{j,j}) = \rho(E_{i,i})\rho(E_{i,j})$ donc $\mathrm{Im}\rho(E_{i,j}) \subset V_i$ et comme $\rho(E_{i,i}) = \rho(E_{i,j})\rho(E_{j,i})$ alors on peut écrire que

$$\mathrm{I}_{V_i} = (\rho(E_{i,j}))_{|V_j}(\rho(E_{j,i}))_{|V_i}.$$

De même on a

$$\mathrm{I}_{V_j} = (\rho(E_{j,i}))_{|V_i}(\rho(E_{i,j}))_{|V_j}$$

donc la restriction de $\rho(E_{i,j})$ à V_j définit un isomorphisme de V_j sur V_i.

c. Par la question précédente, il existe d tel que pour tout $j = 1, \ldots, n$, $\dim V_j = d$. Soit $W_k = \mathrm{Vect}\{\rho(E_{1,1})e_k, \ldots, \rho(E_{n,1})e_k\}$.

(i) Par le b., pour tout $j = 1, \ldots, n$, on a $\rho(E_{j,1})e_k \in V_j \setminus \{0\}$ car $e_k \neq 0$. Par le a., $V = \bigoplus_{j=1}^n V_j$ donc la famille $\{\rho(E_{1,1})e_k, \ldots, \rho(E_{n,1})e_k\}$ est libre. Comme elle engendre W_k, elle forme une base de W_k et $\dim W_k = n$.

(ii) D'après les propriétés de morphisme d'algèbres de ρ, il suffit de prouver que pour tous $i, j, \ell = 1, \ldots, n$, on a $\rho(E_{i,j})\rho(E_{\ell,1})e_k \in W_k$. Ce résultat est évident car $\rho(E_{i,j})\rho(E_{\ell,1}) = \delta_{j,\ell}\rho(E_{i,1})$ donc $\rho(E_{i,j})\rho(E_{\ell,1})e_k = \delta_{j,\ell}\rho(E_{i,1})e_k \in W_k$ par définition, donc pour tout $x \in M$,

$$\rho(x)W_k \subset W_k.$$

(iii) La question précédente assure que pour tout $x \in M$, $\rho(x)$ définit un endomorphisme sur W_k. En notant $x = \sum_{i,j} x_{i,j}E_{i,j}$, le $\ell^{\text{ème}}$ vecteur colonne de la matrice représentative est

$$\rho(x)\rho(E_{\ell,1})e_k = \sum_{i=1}^n x_{i,\ell}\rho(E_{i,1})e_k$$

ce qui prouve que la matrice de $\rho_k(x)$, endomorphisme induit par $\rho(x)$ sur W_k, dans la base décrite au (i) est x.

(iv) Par le b., $\rho(E_{i,1})$ définit un isomorphisme de V_1 sur V_i donc la famille $(\rho(E_{i,1})e_1, \ldots, \rho(E_{i,1})e_d)$ est une base de V_i. D'après le a., on sait que $V = \bigoplus_{j=1}^n V_j$ donc la famille $\mathcal{B} = (\rho(E_{i,1})e_k)_{\substack{1\leq i\leq n\\ 1\leq k\leq d}}$ est une base de V. Par le (i), $(\rho(E_{1,1})e_k, \ldots, \rho(E_{n,1})e_k)$ est une base de W_k alors

$$V = \bigoplus_{k=1}^d W_k.$$

(v) Par le (ii) et (iv), on sait que la matrice de $\rho(x)$ dans la base $\mathcal{B}$ est une matrice diagonale par blocs où chaque bloc est la matrice de ρ_k dans la base de W_k introduite au (i). D'après (iii), on en conclut que la matrice de $\rho(x)$ dans la base $\mathcal{B}$ est égale à

$$\begin{pmatrix} x & 0 & \ldots & 0 \\ 0 & x & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & x \end{pmatrix}.$$

d. Soit $\rho : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_m(\mathbb{C})$ un morphisme d'algèbres avec unité. On applique les résultats de la question précédente avec $M = \mathcal{M}_n(\mathbb{C})$ et $V = \mathbb{C}^m$. Par le 2.c.(iv) on a $\dim V = m = nd$ donc m est un multiple de n. Par le 2.c.(v), la matrice de $\rho(x)$ dans la base $\mathcal{B}$ est une matrice diagonale par blocs, tous égaux à x donc si $\rho(x) = 0$ alors $x = 0$ ce qui prouve que ρ est injectif.

3.a. On étudie dans cette question $\rho(M)'$. Le fait que A commute avec tous les $\rho(x), x \in M$ s'écrit dans la base $\mathcal{B}$:

$$\begin{pmatrix} A_{11} & \dots & A_{1d} \\ \vdots & \ddots & \vdots \\ A_{d1} & \dots & A_{dd} \end{pmatrix} \begin{pmatrix} x & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & x \end{pmatrix} = \begin{pmatrix} x & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & x \end{pmatrix} \begin{pmatrix} A_{11} & \dots & A_{1d} \\ \vdots & \ddots & \vdots \\ A_{d1} & \dots & A_{dd} \end{pmatrix},$$

ce qui prouve que pour tout $i, j \in \{1, \dots, d\}$, pour tout $x \in M$, $A_{ij}x = xA_{ij}$. D'après le 1.b., le centre de M est l'ensemble des matrices scalaires ce qui prouve que $A_{ij} = \lambda_{ij}\mathrm{I}_n$ avec $\lambda_{ij} \in \mathbb{C}$. Réciproquement, il est clair que toute matrice de ce type est dans le commutant de $\rho(M)$ donc

$$\rho(M)' = \left\{ \begin{pmatrix} \lambda_{11}\mathrm{I}_n & \dots & \lambda_{1d}\mathrm{I}_n \\ \vdots & \ddots & \vdots \\ \lambda_{d1}\mathrm{I}_n & \dots & \lambda_{dd}\mathrm{I}_n \end{pmatrix}, \lambda_{ij} \in \mathbb{C} \right\},$$

cette écriture se faisant dans la base $\mathcal{B}$.

b. L'application

$$\begin{array}{rl} \phi : \rho(M)' & \to \mathcal{M}_d(\mathbb{C}) \\ (\lambda_{ij} I_n)_{\substack{1 \le i \le d \\ 1 \le j \le d}} & \mapsto (\lambda_{ij})_{\substack{1 \le i \le d \\ 1 \le j \le d}} \end{array}$$

est clairement un isomorphisme d'algèbres de $\rho(M)'$ sur $\mathcal{M}_d(\mathbb{C})$ ce qui prouve que $\rho(M)'$ est une sous-algèbre de $\mathrm{End}V$ isomorphe à $\mathcal{M}_d(\mathbb{C})$.

On a évidemment $\rho(M) \subset \rho(M)''$. Soit A de matrice $(A_{k\ell})_{1 \le k,\ell \le d}$ dans la base $\mathcal{B}$ où $A_{k\ell} \in \mathcal{M}_n(\mathbb{C})$. Si $A \in \rho(M)''$ alors elle commute avec les matrices de la forme $E_{k\ell} = (\delta_{ik}\delta_{j\ell} I_n)_{1 \le i,j \le d}$. En effectuant le produit matriciel par blocs, on constate comme dans le 1.b. que $AE_{k\ell} = E_{k\ell}A$ pour tout $k, \ell \in \{1, \dots, d\}$ si et seulement s'il existe $x \in M$ tel que pour tout $k \neq \ell, A_{k\ell} = 0$ et $A_{kk} = x$. Par le 2.c.(v), $\rho(x)$ admet la même matrice que A dans la base $\mathcal{B}$ donc $A = \rho(x) \in \rho(M)$. On en conclut que $\rho(M) = \rho(M)''$.

4.a. Comme $p_i = (0, \dots, 0, \mathrm{I}_i, 0, \dots, 0)$, il est clair par définition du produit dans l'algèbre N que $p_i p_j = 0$ si $i \neq j$ et $p_i p_i = p_i$. Il est tout aussi évident que $\sum_{i=1}^{n} p_i = (\mathrm{I}_1, \dots, \mathrm{I}_m) = \mathrm{I}_N$.

b. Si $z \in Z(N)$, en écrivant $z = (z_1, \dots, z_n)$ avec $z_i \in A_i$, on constate que z commute avec tous les éléments $a \in N$ si et seulement si $z_i \in Z(A_i)$ pour tout $i = 1, \dots, n$. Or par le 1.b., $Z(A_i) = \{\lambda_i \mathrm{I}_i; \lambda_i \in \mathbb{C}\}$ donc

$$Z(N) = \{(\lambda_1 \mathrm{I}_1, \dots, \lambda_m \mathrm{I}_m); \lambda_1, \dots, \lambda_m \in \mathbb{C}\}.$$

c. Soit z un idempotent central de N alors $z = (\lambda_1 \mathrm{I}_1, \ldots, \lambda_m \mathrm{I}_m)$ et $z^2 = z$. Donc pour tout i, $\lambda_i^2 = \lambda_i$ ce qui prouve que $\lambda_i \in \{0, 1\}$. Réciproquement, si $z = \sum_{i=1}^{m} \lambda_i p_i$ avec $\lambda_i \in \{0, 1\}$ alors z est un idempotent central de N.

d. Soit p un idempotent central de N, c'est à dire $p = \sum_{i=1}^{m} \lambda_i p_i$ avec $\lambda_i \in \{0, 1\}$. Pour tout $j = 1, \ldots, n$, on a $pp_j = p_j p = \lambda_j p_j$. Comme p_j est un idempotent central de N alors, si p est minimal, pour tout $j = 1, \ldots, n$ tel que $\lambda_j \neq 0$, on a $p = p_j$. On en déduit que soit $p = 0$, soit $p = p_{j_0}$ pour un $j_0 \in \{1, \ldots, m\}$.

Réciproquement, $\{0, p_1, \ldots, p_n\}$ sont des idempotents centraux de N, minimaux. L'élément nul est évidemment un idempotent central de N, minimal. Supposons $p = p_i$. Pour tout $q = \sum_{i=1}^{m} \lambda_i p_i$, $\lambda_i \in \{0, 1\}$, on a $pq = \lambda_i p_i$ donc $pq \neq 0$ lorsque $\lambda_i = 1$. Dans ce cas, on a bien $pq = qp = p$ ce qui prouve que p est minimal.

5.a. D'après le 4.a., $p_1, \ldots, p_m$ sont des idempotents deux à deux orthogonaux et $\sum p_i = \mathrm{I}_N$. Comme ρ est un morphisme d'algèbres avec unité alors $\rho(p_1), \ldots, \rho(p_m)$ sont aussi des idempotents deux à deux orthogonaux et vérifient $\sum \rho(p_i) = \mathrm{I}_W$. De plus, ρ est supposé injectif donc $\rho(p_j)$ est non nul. Comme $W_j = \mathrm{Im}\rho(p_j)$ alors en copiant le raisonnement du 2.a., on prouve que

$$W = \bigoplus_{j=1}^{m} W_j.$$

b. Soit $y = \rho(a_j)$ avec $a_j \in A_j$. Par définition de p_j, on a

$$p_j a_j = a_j p_j = a_j$$

et par les propriétés de morphisme d'algèbres de ρ, on en conclut que si $j \neq k$,

$$y\rho(p_k) = \rho(a_j p_j p_k) = 0 \text{ et } y\rho(p_j) = \rho(p_j a_j p_j) = \rho(p_j) y = y$$

ce qui prouve que y envoie W_j dans lui-même et est nul sur W_k pour $k \neq j$.

c. Comme $A_j = \mathcal{M}_{n_j}(\mathbb{C})$, W_j est un espace vectoriel de dimension finie et $\rho(p_j) = \mathrm{I}_{W_j}$ alors $\rho : \mathcal{M}_{n_j}(\mathbb{C}) \to \mathrm{End}(W_j)$ est un morphisme d'algèbres avec unité. D'après le 2.d., on sait que ce morphisme est injectif et par le 2.c. qu'il existe une base de W_j telle que pour tout $x \in A_j$, la matrice de $\rho(x)$ dans cette base est

$$\begin{pmatrix} x & 0 & \ldots & 0 \\ 0 & x & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & x \end{pmatrix}.$$

d. Comme p_j est un idempotent central de N, on a

$$\rho(p_j) C(N) \rho(p_j) \subset C(N).$$

On a aussi $\mathrm{I}_W = \sum \rho(p_j)$ donc pour tout $u \in \mathrm{End}(W)$, $u = \sum_{j=1}^m u\rho(p_j)$. Lorsque $u \in C(N)$, $u\rho(p_j) = \rho(p_j)u = \rho(p_j^2)u = \rho(p_j)u\rho(p_j)$ donc

$$u = \sum_{j=1}^{m} \rho(p_j)u\rho(p_j)$$

ce qui prouve que $C(N) = \sum_1^m \rho(p_j)C(N)\rho(p_j)$.

D'autre part, si $\displaystyle\sum_{j=1}^{m} z_j = 0$ avec $z_j = \rho(p_j)u_j\rho(p_j), u_j \in C(N)$ alors comme $(\rho(p_1), \ldots, \rho(p_m))$ sont des idempotents deux à deux orthogonaux,

$$0 = \rho(p_i)(\sum_{j=1}^{m} z_j)\rho(p_i) = z_i$$

ce qui prouve que la somme est directe et que

$$C(N) = \bigoplus_{j=1}^{m} \rho(p_j)C(N)\rho(p_j).$$

e. Soit $\mathcal{B}_W$ la base de W obtenue en écrivant les bases de W_j à la suite les unes des autres. Dans cette base, tout endomorphisme $u \in \mathrm{End}(W)$ a pour matrice $u = (u_{ij})_{1\leq i,j\leq m}$ où les u_{ij} sont des matrices rectangulaires représentant un morphisme de W_j dans W_i. Dans cette base, la matrice de $\rho(p_j)$ n'a que des blocs nuls sauf le j^e bloc diagonal égal à I_{W_j}. Il ne reste plus qu'à travailler en effectuant des calculs matriciels. On constate que $\rho(p_j)u\rho(p_j)$ a pour matrice dans la base $\mathcal{B}_W$

$$\begin{pmatrix} 0 & \ldots & 0 & \ldots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \ldots & u_{jj} & \ldots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \ldots & 0 \end{pmatrix}.$$

Comme pour tout $u \in C(N), u = \displaystyle\sum_{j=1}^{m} \rho(p_j)u\rho(p_j)$ alors la matrice de u est diagonale par blocs, chaque bloc u_{jj} définissant un endomorphisme sur W_j appartenant au commutant de $\rho(A_j)$ dans $\mathrm{End}(W_j)$. Cette écriture matricielle montre que $\rho(p_j)C(N)\rho(p_j) = (\rho(A_j))'$, le commutant de $\rho(A_j)$ dans $\mathrm{End}(W_j)$. Or par le 3.b., $C(\rho(A_j)) \simeq \mathcal{M}_{d_j}(\mathbb{C})$ donc

$$C(N) \simeq \bigoplus_{j=1}^{m} \mathcal{M}_{d_j}(\mathbb{C}).$$

f. On a évidemment $\rho(N) \subset C(C(N))$. Soit $u \in C(C(N))$ alors pour tout $j = 1, \ldots, m$, $u\rho(p_j) = \rho(p_j)u$ donc W_j est stable par u. On en déduit aussi que l'endomorphisme u_j induit par u sur W_j appartient au commutant de $(\rho(A_j))'$ dans $\mathrm{End}(W_j)$. On sait par le 3.b. que $(\rho(A_j))'' = \rho(A_j)$ donc $u_j = \rho(a_j), a_j \in$

A_j ce qui prouve que $u = \rho(a_1, \ldots, a_m) \in \rho(N)$. On en conclut que $C(C(N)) = \rho(N)$.

6.a. (i) Tout d'abord, il est clair que qAq est une sous-algèbre non nul de A car q est non nul. Comme q est un idempotent de $\mathcal{M}_n(\mathbb{C})$ alors q est un projecteur de $\mathbb{C}^n$ et $\mathbb{C}^n = \ker q \oplus \mathrm{im} q$. A partir de cette décomposition en somme directe, on définit une base de $\mathbb{C}^n$. Montrons que $qAq \simeq \mathcal{M}_r(\mathbb{C})$ où $r = \operatorname{rg} q$. En effet, soit ψ le morphisme défini par

$$\begin{array}{rl} \psi : \mathcal{M}_r(\mathbb{C}) & \to qAq \\ U & \mapsto \begin{pmatrix} 0 & 0 \\ 0 & U \end{pmatrix}, \end{array}$$

l'écriture matricielle s'effectuant dans la base de $\mathbb{C}^n$ associée à $\ker q$ et $\mathrm{im} q$. Ce morphisme est bien défini car

$$q = \begin{pmatrix} 0 & 0 \\ 0 & \mathrm{I} \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 0 \\ 0 & U \end{pmatrix} = q \begin{pmatrix} 0 & 0 \\ 0 & U \end{pmatrix} q \in qAq.$$

Par construction, ψ est évidemment un isomorphisme d'algèbres avec unité (l'unité de qAq est q) donc $qAq \simeq \mathcal{M}_r(\mathbb{C})$.

Comme $\rho : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_m(\mathbb{C})$ est un morphisme d'algèbres avec unité alors on sait d'après le 2. qu'il existe une base de $\mathbb{C}^m$ dans laquelle on peut écrire pour tout $x \in A$,

$$\rho(x) = \begin{pmatrix} x & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & x \end{pmatrix},$$

cette écriture matricielle comportant d colonnes, c'est à dire $m = dn$. Cela permet de conclure que dans B, $\operatorname{rg} \rho(q) = d \operatorname{rg}(q) = dr$. De même que précé demment, on montre que $qBq \simeq \mathcal{M}_{dr}(\mathbb{C})$.

(ii) Comme qAq est isomorphe à une algèbre de matrices, on sait par le 3.b. que $C(A) = \rho(A)' \simeq \mathcal{M}_d(\mathbb{C})$ et que $C(qAq) = \rho(qAq)' \simeq \mathcal{M}_d(\mathbb{C})$.

Soit θ défini par

$$\begin{array}{rl} \theta : C(A) & \to qC(A)q \\ x & \mapsto qxq. \end{array}$$

Comme $q \in A$ et $q^2 = q$ alors pour tous $a, a' \in C(A)$,

$$\theta(aa') = qaa'q = qaqqa'q = \theta(a)\theta(a')$$

donc θ est un morphisme d'algèbres avec unité. On sait alors que $\ker \theta$ est un idéal bilatère de $C(A)$. Comme $C(A) \simeq \mathcal{M}_d(\mathbb{C})$ alors d'après le 1.a., $\ker \theta = \{0\}$ puisque θ est non nul. On en conclut que $\dim qC(A)q \geq \dim C(A) = d^2$.

D'autre part, $qC(A)q \subset C(qAq)$. En effet, pour tout $b \in C(A)$, $qb = bq$. On a alors $(qbq)(qaq) = qbaq = qabq = qabq^2 = (qaq)(qbq)$. Cela prouve que $qC(A)q \subset C(qAq)$.

Comme $\dim C(qAq) = d^2$ alors on en conclut que $qC(A)q = C(qAq)$

b. Soit q un projecteur non nul de $\rho(A)' = C(A) \subset B$.

(i) On définit l'application Θ par

$$\begin{array}{rl} \Theta : A & \to qAq \\ x & \mapsto q\rho(x)q. \end{array}$$

Comme $q \in C(A)$ et $q^2 = q$, on a pour tous $a, a' \in A$,

$$\Theta(aa') = q\rho(a)\rho(a')q = q\rho(a)qq\rho(a')q = \Theta(a)\Theta(a')$$

donc Θ définit un morphisme d'algèbres avec unité surjectif. On sait alors que $\ker\Theta$ est un idéal bilatère de $A = \mathcal{M}_n(\mathbb{C})$ et par le 1.a., Θ est injectif. On en conclut que $qAq \simeq \mathcal{M}_n(\mathbb{C})$.

(ii) Comme qAq est isomorphe à une algèbre de matrices, on sait par le 3.b. que $C(A) \simeq \mathcal{M}_d(\mathbb{C})$ est une algèbre de matrices incluse dans B. Comme q est un idempotent de $C(A)$ alors d'après le a., on a :

. $qC(A)q$ est une algèbre de matrices isomorphe à $\mathcal{M}_{\mathrm{rg}\,(q)}(\mathbb{C})$,

. le commutant de $qC(A)q$ dans qBq est égal à $qC(C(A))q$.

Ceci peut encore s'écrire $C(qC(A)q) = qC(C(A))q$. Or A et $qC(A)q$ sont des algèbres de matrices donc par le 3.b. (théorème du bicommutant),

$$C(C(A)) = A \text{ et } C(C(qC(A)q)) = qC(A)q.$$

Ainsi $qAq = C(qC(A)q)$ et $C(C(qC(A)q)) = qC(A)q$ donc on en conclut que $C(qAq) = C(C(qC(A)q)) = qC(A)q$.

III. Normes des matrices à coefficients entiers

1.a. Soit $P \in U$. D'après les relations liant les coefficients d'un polynôme et ses racines, $\mu_1, \ldots, \mu_\ell$, on sait que pour tout $k = 1, \ldots, \ell-1$, $a_k = \sigma_k(\mu_1, \ldots, \mu_\ell)$. Si $|\mu_i| \leq 1$ alors on a $|a_k| \leq \sigma_k(1, \ldots, 1)$. Or $\sigma_k(1, \ldots, 1) = \binom{\ell}{k}$ donc pour tout $k = 1, \ldots, \ell - 1$,

$$|a_k| \leq \binom{\ell}{k}.$$

b. Par la question précédente, on sait que pour tout $k = 1, \ldots, \ell - 1$, $a_k \leq \binom{\ell}{k}$. Comme $a_k \in \mathbb{Z}$, il n'y a qu'un nombre fini de valeurs possibles pour chaque a_k ce qui prouve qu'il n'existe qu'un nombre fini de polynômes vérifiant ces hypothèses.

c. Soit $P \in U$ tel que

$$P = \prod_{i=1}^{\ell}(X - \mu_i) \quad \text{et} \quad \forall 1 \leq i \leq \ell,\ |\mu_i| \leq 1.$$

(i) On a

$$P_k(X) = \sum_{i=1}^{\ell} \sigma_i(\mu_1^k, \ldots, \mu_\ell^k) X^{\ell-i} + X^\ell.$$

Soit $\sigma_{i,k} = \sigma_i(X_1^k, \ldots, X_\ell^k)$ alors $\sigma_{i,k}$ est clairement un polynôme symétrique à coefficients entiers. D'après le rappel énoncé au début de la partie III, il existe un polynôme S à coefficients entiers tel que

$$\sigma_{i,k}(X_1, \ldots, X_\ell) = S(\sigma_1, \ldots, \sigma_\ell).$$

Comme $P \in U$ alors $\sigma_i(\mu_1, \ldots, \mu_\ell) \in \mathbb{Z}$ donc

$$\sigma_i(\mu_1^k, \ldots, \mu_\ell^k) = \sigma_{i,k}(\mu_1^k, \ldots, \mu_\ell^k) = S(\sigma_1(\mu_1, \ldots, \mu_\ell), \ldots, \sigma_\ell(\mu_1, \ldots, \mu_\ell)) \in \mathbb{Z}$$

ce qui prouve que $P_k \in \mathbb{Z}[X_1, \ldots, X_\ell]$.

(*ii*) On a même prouvé que pour tout entier positif k, P_k est un polynôme satisfaisant les hypothèses du a.. Comme il n'existe qu'un nombre fini de tels polynômes, on trouve deux entiers distincts j, k tels que $P_j = P_k$.

On remarque que si $j = 0$ alors $P_j(X) = X^\ell$ et comme $P_j = P_k$ avec $j \neq k$ alors pour tout $i = 1, \ldots, \ell$, $\mu_i = 0$ ce qui veut dire que pour tout j, $k \in \mathbb{N}$, $P_j = P_k$.

On en conclut qu'il existe deux entiers distincts strictement positifs tels que $P_j = P_k$.

(*iii*) Comme $P_j = P_k$ avec $j \neq k$ alors par unicité de la décomposition en polynômes irréductibles, il existe une permutation σ de $\{1, \ldots, \ell\}$ telle que

$$\forall 1 \leq i \leq \ell,\ \mu_i^k = \mu_{\sigma(i)}^j.$$

On peut supposer $k > j > 0$ donc pour tout $i = 1, \ldots, \ell$, $\mu_{\sigma(i)} = \mu_i^{k-j}$. Or $\mathcal{S}_\ell$ est d'ordre $\ell\,!$ donc $\sigma^{\ell\,!}(i) = i$ ce qui donne

$$\forall 1 \leq i \leq \ell,\ \mu_i = \mu_i^{(k-j)^{\ell\,!}}.$$

On conclut que les racines de P sont soit nulles soit des racines de l'unité.

d. On considère $Q(X) = X^\ell P(X + \frac{1}{X})$. Comme $P \in U$ peut s'écrire $P(X) = X^\ell + \sum_{i=1}^{\ell} (-1)^i a_i X^{\ell-i}$ alors

$$\begin{aligned} Q(X) &= X^\ell \Big(\sum_{i=1}^{\ell} (-1)^i a_i (X + \frac{1}{X})^{\ell-i} + (X + \frac{1}{X})^\ell \Big) \\ &= (X^2+1)^\ell + \sum_{i=1}^{\ell} (-1)^i a_i (X^2+1)^{\ell-i} X^i. \end{aligned}$$

Le coefficient dominant est $X^{2\ell}$ donc $Q \in U$ de degré 2ℓ et comme $Q(0) = 1$ alors 0 n'est pas racine de Q. Cette dernière constatation permet de dire que α est racine de Q si et seulement si $\alpha + \frac{1}{\alpha}$ est racine de P. Soit μ une racine de P et résolvons l'équation du second degré $\alpha^2 - \alpha\mu + 1 = 0$. Comme $\mu \in [-2, 2]$ alors les racines sont

$$\alpha_0 = \frac{\mu + i\sqrt{4-\mu^2}}{2} \text{ et } \alpha_1 = \frac{\mu - i\sqrt{4-\mu^2}}{2}.$$

Ces deux racines sont de module 1 donc toutes les racines de Q sont de module 1 et Q vérifie les hypothèses du a.. D'après le c., les racines de Q sont des racines de l'unité (car 0 n'est pas une racine de Q). Ainsi $\alpha = e^{\frac{2i\pi p}{q}}$ avec p, $q \in \mathbb{Z}$ et comme $\mu = \alpha + \frac{1}{\alpha}$ alors $\mu = 2\cos(\frac{2\pi p}{q})$. On en conclut que si toutes les racines de P sont réelles, contenues dans $[-2, 2]$ alors pour toute racine μ de P, on peut trouver un rationnel r tel que $\mu = 2\cos(2\pi r)$.

e. (*i*) On sait que Q_n est irréductible sur $\mathbb{Z}$ donc il est irréductible sur $\mathbb{Q}$. Soit ω une racine primitive n^e de l'unité alors Q_n est le polynôme minimal de ω sur $\mathbb{Q}$ et $L \supset \mathbb{Q}$ est un corps de rupture de Q_n. De même si ρ est une autre racine primitive n^e de l'unité, $\mathbb{Q}[\rho]$ est un corps de rupture de Q_n. Comme Q_n est irréductible sur $\mathbb{Q}$, son corps de rupture est unique à isomorphisme près et on a même l'existence d'un unique $\mathbb{Q}$-isomorphisme ϕ de L sur $\mathbb{Q}[\rho]$ tel que $\phi(\omega) = \rho$.

(*ii*) Soit $\lambda = 2\cos(\frac{2\pi p}{q})$ une racine de P. Par définition de Q, $e^{\frac{2i\pi p}{q}}$ est une racine de Q. Comme $p \wedge q = 1$ alors ω est une racine primitive q^e de l'unité. Par la question précédente, comme $e^{\frac{2i\pi}{q}}$ est aussi une racine primitive q^e de l'unité, il existe un automorphisme $\mathbb{Q}$-linéaire ϕ qui envoie ω sur $e^{\frac{2i\pi}{q}}$. Comme $Q \in \mathbb{Z}[X]$ alors $Q \circ \phi = \phi \circ Q$ donc

$$Q(\omega) = 0 \Longrightarrow Q(e^{\frac{2i\pi}{q}}) = 0.$$

Ainsi $e^{\frac{2i\pi}{q}}$ est une racine de Q et par définition de Q, $e^{\frac{2i\pi}{q}} + e^{-\frac{2i\pi}{q}} = 2\cos(\frac{2\pi}{q})$ est une racine de P.

(*iii*) On établit de la même manière qu'au (ii) un résultat plus précis :
si $1 \leq p' \leq q-1$ *est tel que* $p' \wedge q = 1$ *et* $\lambda = 2\cos(\frac{2\pi p}{q})$ *est racine de* P *avec* $p \wedge q$, *alors* $e^{\frac{2i\pi p'}{q}}$ *est une racine primitive* q^e *de l'unité donc* $2\cos(\frac{2\pi p'}{q})$ *est encore une racine de* P.

D'après le d., toutes les racines de P sont de la forme $\lambda_i = 2\cos(\frac{2\pi p_i}{q_i})$ avec $p_i \wedge q_i = 1$. On peut supposer p_i et q_i positifs et que $0 \leq p_i \leq q_i - 1$ après avoir effectué une division euclidienne entre p_i et q_i. Comme $\lambda_i \in]-2, 2[$ alors on a en fait $1 \leq p_i \leq q_i - 1$.

Distinguons alors deux cas selon q_i pair ou impair.

Premier cas : si $q_i = 2q_i'$ est pair alors d'après (*ii*), $2\cos(\frac{\pi}{q_i'})$ est une racine de P. Comme $p_i \wedge q_i = 1$ alors $p_i \neq q_i'$ et $1 \leq p_i \leq q_i' - 1$ ou $q_i' + 1 \leq p_i \leq q - 1$. En étudiant les variations de la fonction $t \mapsto |\cos t|$, on en déduit que

$$|\cos(\frac{\pi p_i}{q_i'})| \leq \max\left(|\cos(\frac{\pi}{q_i'})|, |\cos(\frac{\pi(q_i'-1)}{q_i'})|\right) = |\cos(\frac{\pi}{q_i'})|.$$

Deuxième cas : si $q_i = 2q_i' + 1$ est impair alors $q_i \wedge q_i' = 1$ donc par la remarque effectuée au début de cette question, $2\cos(\frac{2\pi q_i'}{q_i})$ est encore une racine de P. De plus, $|\cos(\frac{2\pi q_i'}{q_i})| = |\cos(\frac{\pi}{q_i})|$ et à nouveau d'après l'étude des variations de la fonction $t \mapsto |\cos t|$, comme $1 \leq p_i \leq q_i' - 1$ ou $q_i' + 1 \leq p \leq q - 1$ alors

$$|\cos(\frac{2\pi p_i}{q_i})| \leq |\cos(\frac{\pi}{q_i})| = |\cos(\frac{2\pi q_i'}{q_i})|.$$

L'étude de ces deux cas permet d'établir que

$$\max\{|\lambda_j|,\, j = 1, \ldots, \ell\} = 2\cos(\frac{\pi}{q})$$

avec $q \geq 2$. D'autre part, si $q = 2$ alors $P = X^\ell$ ce qui est exclu donc $q \geq 3$.

2.a. Montrons tout d'abord que $\|B\| = \|{}^tB\|$. En effet

$$\|B\| = \sup_{x \in \mathbb{R}^m, \|x\|=1} \|Bx\| = \sup_{x \in \mathbb{R}^m, \|x\|=1} \sup_{y \in \mathbb{R}^n, \|y\|=1} \langle Bx, y\rangle,$$

par définition de la dualité dans l'espace euclidien $\mathbb{R}^n$. Par définition de la transposition, on en conclut que

$$\|B\| = \sup_{x\in\mathbb{R}^m,\|x\|=1}\ \sup_{y\in\mathbb{R}^n,\|y\|=1} \langle Bx, y\rangle = \sup_{\substack{x\in\mathbb{R}^m,\|x\|=1\\ y\in\mathbb{R}^n,\|y\|=1}} \langle x, {}^tBy\rangle = \|{}^tB\|.$$

Ensuite on prouve que $\|B\| = \|{}^tBB\|^{1/2}$. Comme ${}^tBB$ est symétrique alors

$$\begin{aligned}\|{}^tBB\| &= \sup_{x\in\mathbb{R}^m,\|x\|=1} \langle {}^tBBx, x\rangle = \sup_{x\in\mathbb{R}^m,\|x\|=1} \langle Bx, Bx\rangle\\ &= \sup_{x\in\mathbb{R}^m,\|x\|=1} \|Bx\|^2 = \|B\|^2.\end{aligned}$$

En échangeant les rôles de B et ${}^tB$, on a aussi $\|{}^tB\| = \|B{}^tB\|^{1/2}$.

Enfin, prouvons que $\|C\| = \|B\|$. On a

$$\|C\| = \sup_{\substack{x\in\mathbb{R}^m, y\in\mathbb{R}^n\\ \|x\|^2+\|y\|^2=1}} (\|Bx\|^2 + \|{}^tBy\|^2)^{1/2}.$$

Comme $\|B\| = \|{}^tB\|$ alors il est clair que $\|C\| \leq \|B\|$. D'autre part, en prenant $y = 0$ dans l'expression précédente du supremum, on a $\|C\| \geq \|B\|$ ce qui prouve le résultat annoncé.

b. Soit $B \in \mathcal{M}_{m,n}(\mathbb{Z})$ alors on vient d'établir que $\|B\| = \|C\|$ où

$$C = \begin{pmatrix} 0 & B\\ {}^tB & 0\end{pmatrix} \in \mathcal{M}_\ell(\mathbb{C}).$$

Comme C est symétrique alors elle est diagonalisable dans une base orthonormée de vecteurs propres et ses valeurs propres sont réelles. Donc $\|C\| = \max\{|\lambda_j|, j = 1,\dots,\ell\}$, les λ_j représentant les valeurs propres de C ou encore les racines du polynôme caractéristique de C. Or $B \in \mathcal{M}_{m,n}(\mathbb{Z})$ donc $C \in \mathcal{M}_\ell(\mathbb{Z})$ et $P_C \in \mathbb{Z}[X]$. On en conclut que soit $\|B\| \geq 2$, soit $\|B\| < 2$ auquel cas $\max\{|\lambda_j|, j = 1,\dots,\ell\} < 2$ et P_C vérifie les hypothèses de 1.e.(iii). On sait alors que

$$\max\{|\lambda_j|, j = 1,\dots,\ell\} = 2\cos(\frac{\pi}{q})$$

où $q \geq 2$.

IV. Indices d'inclusions

1. Comme $\rho(A) \subset B$ alors $\tau\circ\rho(A) \subset \tau(B)$ donc

$$\tau(B)' \subset (\tau\circ\rho(A))'.$$

On a vu au II.3.b. qu'il s'agissait d'algèbres de matrices.

On sait que $\tau : B \to C$ est un morphisme d'algèbres avec unité donc par le II.3.b.,

$$\dim C = \dim B\ \dim(\tau(B))'.$$

De même, $\tau\circ\rho : A \to C$ est un morphisme d'algèbres avec unité donc

$$\dim C = \dim A\ \dim(\tau\circ\rho(A))'.$$

On en conclut que

$$\begin{array}{rcl}[(\tau\circ\rho(A))' : (\tau(B))'] & = & \frac{\dim \tau\circ\rho(A)'}{\dim \tau(B)'} \\ & = & \frac{\dim B}{\dim A} = [B : A].\end{array}$$

2.a. On a vu au II.4. que $\{p_1, \ldots, p_s\}$ sont les idempotents centraux minimaux non nuls de S et comme $R \subset S$, on a pour tout $j = 1, \ldots, r$,

$$p_i q_j = q_j p_i \quad \text{et} \quad (p_i q_j)^2 = p_i^2 q_j^2 = p_i q_j.$$

On en conclut que $p_i q_j : S \to S$ définit en fait un endomorphisme de B_i et qu'il s'agit d'un idempotent de B_i.

b. Si $p_i q_j \neq 0$, d'après la relation précédente, on a

$$S_{ij} = p_i q_j B_i p_i q_j \text{ et } R_{ij} = p_i q_j A_j p_i q_j.$$

Or d'après le a. $p_i q_j$ est un idempotent de B_i. Il s'agit aussi d'un idempotent du centre de A_j. Il est non nul par hypothèse donc de la même manière qu'au II.6.a.(i) et II.6.b.(i), on démontre que

$$S_{ij} \simeq \mathcal{M}_{\mathrm{rg}(p_i q_j)}(\mathbb{C})$$

est une algèbre de matrices et que

$$\begin{array}{rcl} A_j & \to & R_{ij} \\ x & \mapsto & p_i x p_i \end{array}$$

est un isomorphisme d'algèbres avec unité (car pour tout $x \in A_j$, $q_j x q_j = x$).

c. Si une ligne de Λ_R^S est identiquement nulle alors il existe $i_0 \in \{1, \ldots, s\}$ tel que $\lambda_{i_0 j} = 0$ pour tout $j = 1, \ldots, r$. Ainsi, on a

$$\forall 1 \leq j \leq r,\ p_{i_0} q_j = 0.$$

Comme $\displaystyle\sum_{j=1}^{r} q_j = \mathrm{I}_S$ alors $p_{i_0} = 0$ ce qui est contradictoire.

Il en est de même si l'une des colonnes est nulle car $\displaystyle\sum_{i=1}^{s} p_i = \mathrm{I}_S$.

d. On vient de voir que la matrice Λ_R^S est non redondante. Ainsi, Λ_R^S est indécomposable si et seulement si elle n'est pas décomposable.

Montrons que si Λ_R^S est décomposable alors $Z(R) \cap Z(S)$ n'est pas réduit aux multiples de l'identité. Par le I.7. (voir la caractérisation (7.2)), on sait qu'il existe des partitions non triviales (I_1, I_2) de $\{1, \ldots, s\}$ et (J_1, J_2) de $\{1, \ldots, r\}$ telles que

$$\left\{ \begin{array}{l} \forall i \in I_1,\ \forall j \in J_2,\ p_i q_j = 0 \\ \forall i \in I_2,\ \forall j \in J_1,\ p_i q_j = 0. \end{array} \right.$$

Soit $P_1 = \displaystyle\sum_{i \in I_1} p_i$, $P_2 = \sum_{i \in I_2} p_i$, $Q_1 = \sum_{j \in J_1} q_j$, $Q_2 = \sum_{j \in J_2} q_j$. On a alors

$$P_1 + P_2 = Q_1 + Q_2 = \mathrm{I}_S \text{ et } P_1 Q_2 = P_2 Q_1 = 0.$$

D'après ces relations $P_1 = P_1(Q_1 + Q_2) = P_1Q_1$ et $Q_1 = (P_1 + P_2)Q_1 = P_1Q_1$ donc $P_1 = Q_1$. D'autre part, il est clair que $Q_1 \in Z(R)$ et $P_1 \in Z(S)$ car ce sont des combinaisons linéaires d'idempotents centraux. Comme les partitions ne sont pas triviales, $P_1 = Q_1 \in Z(R) \cap Z(S)$ n'est pas un multiple de l'identité.

Montrons que si $Z(R) \cap Z(S)$ n'est pas réduit aux multiples de l'identité alors Λ_R^S est décomposable. Soit $z \in Z(R) \cap Z(S)$ avec z non multiple de l'identité. Par le II.4.b., on trouve des complexes $\alpha_1, \ldots, \alpha_r$, $\beta_1, \ldots, \beta_s$ tels que

$$z = \sum_{j=1}^{r} \alpha_j q_j = \sum_{i=1}^{s} \beta_i p_i.$$

Quitte à multiplier z, on peut supposer que $\max |\alpha_j| = \alpha_{j_0} = 1$. Soit

$$J_1 = \{j \in \{1, \ldots, r\}; \alpha_j = 1\}.$$

On a $J_1 \neq \emptyset$ puisque $j_0 \in J_1$ et $J_1 \neq \{1, \ldots, r\}$ puisque z n'est pas un multiple de l'identité. Comme $\sum_{j=1}^{r} q_j = \mathrm{I}_S$ alors

$$\frac{z + \mathrm{I}_S}{2} = \sum_{j \in J_1} q_j + \sum_{j \notin J_1} \frac{\alpha_j + 1}{2} q_j.$$

Comme $Z(R)$ et $Z(S)$ sont des algèbres, on sait que pour tout $n \in \mathbb{N}$,

$$\left(\frac{z + \mathrm{I}_S}{2}\right)^n \in Z(R) \cap Z(S).$$

Or

$$\left(\frac{z + \mathrm{I}_S}{2}\right)^n = \sum_{j \in J_1} q_j + \sum_{j \notin J_1} \left(\frac{\alpha_j + 1}{2}\right)^n q_j$$

et comme pour tout $j \notin J_1$, $\alpha_j \neq 1$ et $|\alpha_j| \leq 1$ donc $|\frac{\alpha_j + 1}{2}| < 1$ et

$$\lim_{n \to \infty} \left(\frac{z + \mathrm{I}_S}{2}\right)^n = \sum_{j \in J_1} q_j \in Z(R) \cap Z(S).$$

Ainsi on a prouvé que $Q = \sum_{j \in J_1} q_j$ est un idempotent central de S donc par le II.4.c., Q s'écrit aussi

$$Q = \sum_{i \in I_1} p_i.$$

Comme $J_1 \neq \emptyset$ et $J_1 \neq \{1, \ldots, r\}$ alors nécessairement, $I_1 \neq \emptyset$ et $I_1 \neq \{1, \ldots, s\}$. D'autre part, $\forall i \in I_1, p_i Q = p_i$ et $\forall j \notin J_1, Q q_j = 0$ donc

$$\forall i \in I_1, \forall j \notin J_1, p_i q_j = 0.$$

De la même manière,

$$\forall i \notin I_1, \forall j \in J_1, p_i q_j = 0,$$

ce qui prouve que Λ_R^S est décomposable.

e. Soit $R \xrightarrow{\rho} S \xrightarrow{\tau} T$ avec $R = \bigoplus_{j=1}^{r} A_j$, $S = \bigoplus_{k=1}^{s} B_k$, $T = \bigoplus_{i=1}^{t} C_i$. On note $u_1, \ldots, u_t$ les idempotents centraux minimaux non nuls de T et on pose $\Lambda_R^T = (\lambda_{ij})_{\substack{1\le i\le t\\ 1\le j\le r}}$, $\Lambda_R^S = (\lambda'_{kj})_{\substack{1\le k\le s\\ 1\le j\le r}}$, $\Lambda_S^T = (\lambda''_{ik})_{\substack{1\le i\le t\\ 1\le k\le s}}$.

D'après le 2.b., on sait que lorsque $p_i q_j \neq 0$,

$$A_j \simeq R_{ij}$$

et S_{kj} est une algèbre de matrices donc en considérant le morphisme d'algèbres avec unité

$$\begin{array}{rl} \Phi_{kj} : & A_j \to S_{kj} \\ & x \mapsto p_k q_j x p_k q_j \end{array}$$

on sait par le II.2.c.(v) que la matrice de $\Phi_{kj}(x)$ est une matrice diagonale par blocs avec λ''_{kj} blocs diagonaux :

$$\begin{pmatrix} x & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & x \end{pmatrix}.$$

De la même manière on considère les morphismes d'algèbres avec unité

$$\begin{array}{rl} \Psi_{ij} : & A_j \to T_{ij} \\ & z \mapsto u_i q_j z u_i q_j \end{array}$$

et

$$\begin{array}{rl} \Theta_{ik} : & B_k \to U_{ik} \\ & y \mapsto u_i p_k y u_i p_k. \end{array}$$

On sait par le II.2.c.(v) que la matrice de $\Psi_{ij}(z)$ est une matrice diagonale par blocs avec λ_{ij} blocs diagonaux égaux à z et que la matrice de $\Theta_{ik}(y)$ est une matrice diagonale par blocs avec λ'_{ik} blocs diagonaux égaux à y.

Mais $S_{kj} \subset B_k$, $\sum_{k=1}^{s} p_k = \mathrm{I}_T$ et u_i, p_k, q_j commutent deux à deux donc

$$\sum_{k=1}^{s} \Theta_{ik} \circ \Phi_{kj}(z) = \sum_{k=1}^{s} u_i p_k q_j z p_k q_j u_i = \Psi_{ij}(z).$$

La matrice de $\Theta_{ik} \circ \Phi_{kj}(z)$ est une matrice diagonale par blocs avec $\lambda'_{ik}\lambda''_{kj}$ blocs diagonaux égaux à z. Comme $\{p_1, \ldots, p_s\}$ sont des idempotents orthogonaux de T, il est clair que la famille des algèbres $U_{ik}, 1 \le k \le s$ est en somme directe dans T donc la matrice de $\sum_{k=1}^{s} \Theta_{ik} \circ \Phi_{kj}(z)$ est une matrice diagonale par blocs avec

$$\sum_{k=1}^{s} \lambda'_{ik}\lambda''_{kj}$$

blocs diagonaux égaux à z. En égalant avec la matrice de $\Psi_{ij}(z)$, on trouve

$$\lambda_{ij} = \sum_{k=1}^{s} \lambda'_{ik}\lambda''_{kj}.$$

f. Comme $R \subset S$, il est clair que $C(S) \subset C(R)$ et que $C(S)$ est une sous-algèbre de $C(R)$. Ces sommes directes d'algèbres de matrices s'injectent dans une algèbre de matrices F donc on peut appliquer les résultats du II.5.. Par le II.5.d. et II.5.e., on a

$$C(R) = \bigoplus_{j=1}^{r} q_j C(R) q_j = \bigoplus_{j=1}^{r} A'_j$$

et

$$C(S) = \bigoplus_{i=1}^{s} p_i C(S) p_i = \bigoplus_{i=1}^{s} B'_i,$$

où A'_j est le commutant de A_j dans $q_j F q_j$, B'_i est le commutant de B_i dans $p_i F p_i$.

D'après le II.4., on déduit de ces écritures que $\{q_1, \ldots, q_r\}$ (respectivement $\{p_1, \ldots, p_s\}$) sont les idempotents centraux minimaux non nuls de $C(R)$ (respectivement $C(S)$).

Par définition de la matrice d'indice, on a $\Lambda_{C(S)}^{C(R)} = (\mu_{ji})_{\substack{1 \leq j \leq r \\ 1 \leq i \leq s}}$ avec

$$\mu_{ji}^2 = [q_j p_i C(R) q_j p_i : q_j p_i C(S) q_j p_i]$$

lorsque $q_j p_i \neq 0$ et 0 sinon.
Si $p_i q_j = 0$ alors $\mu_{ji} = \lambda_{ij}$.
Si $q_j p_i \neq 0$: on a évidemment $q_j p_i C(R) q_j p_i = p_i A'_j p_i$ et $q_j p_i C(S) q_j p_i = q_j B'_i q_j$ donc

$$\mu_{ji}^2 = \frac{\dim p_i A'_j p_i}{\dim q_j B'_i q_j}.$$

A ce stade, rappelons le résultat établi au II.3.b. : si A et B sont deux algèbres de matrices telles qu'il existe un morphisme d'algèbres avec unité de A dans B alors

$$[B : A] = \frac{\dim B}{\dim A} = \dim A'$$

où A' est le commutant de A dans B.

On a clairement l'injection $A_j \to q_j F q_j$ et A'_j est le commutant de A_j dans $q_j F q_j$. Comme $p_i \in Z(S)$ et $R \subset S$ alors $p_i \in C(R)$ donc $q_j p_i$ est un idempotent non nul de A'_j. D'après le II.6.b.(ii) le commutant de $p_i q_j A_j p_i q_j$ dans $p_i q_j F p_i q_j$ est égal à $p_i q_j A'_j p_i q_j$. Or $q_j A_j q_j = A_j$ et $q_j A'_j q_j = A'_j$ donc

$$\dim(p_i q_j F p_i q_j) = \dim(p_i A_j p_i) \dim(p_i A'_j p_i).$$

On a aussi l'injection $B_i \to p_i F p_i$ et B'_i est le commutant de B_i dans $p_i F p_i$. D'après le 2.b., $q_j p_i$ est un idempotent non nul de B_i donc d'après le II.6.a.(ii), le commutant de $q_j p_i B_i q_j p_i$ dans $q_j p_i F q_j p_i$ est égal à $q_j p_i B'_i q_j p_i$. Or $p_i B_i p_i = B_i$ et $p_i B'_i p_i = B'_i$ donc

$$\dim(p_i q_j F p_i q_j) = \dim(q_j B_i q_j) \dim(q_j B'_i q_j).$$

Comme $p_i A_j p_i = R_{ij}$ et $q_j B_i q_j = S_{ij}$, on a

$$\mu_{ji}^2 = \frac{\dim(p_i A'_j p_i)}{\dim(q_j B'_i q_j)} = \frac{\dim S_{ij}}{\dim R_{ij}} = \lambda_{ij}$$

ce qui permet de conclure que $\Lambda_{C(S)}^{C(R)} = {}^t\Lambda_R^S$.

3.a. On vérifie facilement que λ est un morphisme d'algèbres injectif avec unité, que ρ est un antihomomorphisme d'algèbres injectif avec unité et que

$$\forall x, z \in S,\ \lambda(x)\rho(z) = \rho(z)\lambda(x).$$

b. Par la relation vue au a., il est clair que $\lambda(S) \subset \mathrm{End}_R(S)$.
On définit un morphisme d'algèbres avec unité par

$$\begin{array}{rl} \tau : & S \to \mathrm{End}(S) \\ & x = \bigoplus_{i=1}^s x_i \mapsto \rho(\bigoplus_{i=1}^s {}^t x_i) \end{array}$$

Comme R est une somme directe d'algèbres de matrices, $\tau(R)$ est isomorphe à une somme directe d'algèbres de matrices. Comme $\tau(R) = \rho(R)$, $\mathrm{End}_R(S)$ est le commutant de $\tau(R)$ dans $\mathrm{End}(S)$ donc d'après le II.5.d., $\mathrm{End}_R(S)$ est isomorphe à une somme directe d'algèbres de matrices.

c. Montrons que $\lambda(S)$ est le commutant de $\tau(S)$ dans $\mathrm{End}(S)$. Tout d'abord, il est clair d'après la relation établie au a. que $\lambda(S) \subset (\tau(S))'$. Ensuite, si $f \in (\tau(S))'$ alors

$$\forall s \in S, f \circ \rho(s) = \rho(s) \circ f.$$

En appliquant cette égalité à l'élément I, on en déduit que pour tout $s \in S$, $f(s) = f(\mathrm{I})s$ ce qui prouve que $f = \lambda(x)$ avec $x = f(\mathrm{I})$ et que $f \in \lambda(S)$.

On a alors $R \longrightarrow S \longrightarrow \mathrm{End}(S)$. On vient de voir que $\lambda(S) = C(S)$ et on a vu au b. que $\mathrm{End}_R(S) = C(R)$ donc d'après le 2.f.,

$$\Lambda_{\lambda(S)}^{\mathrm{End}_R(S)} = {}^t\Lambda_R^S.$$

4.a. Par le 3.c., on a $\Lambda_{S_{2p}}^{S_{2p+1}} = \Lambda$ et $\Lambda_{S_{2p-1}}^{S_{2p}} = {}^t\Lambda$ et d'après la relation de transitivité des matrices d'indice pour l'inclusion établie au 2.e., on constate facilement que

$$\begin{array}{rcl} \Lambda_{S_0}^{S_{2k}} & = & \Lambda_{S_0}^{S_2} \cdots \Lambda_{S_{2k-2}}^{S_{2k}} \\ & = & (\Lambda\, {}^t\Lambda)^k, \end{array}$$

et que

$$\Lambda_{S_0}^{S_{2k+1}} = (\Lambda\, {}^t\Lambda)^k \Lambda.$$

b. Comme on suppose que $Z(R) \cap Z(S)$ est réduit aux multiples de l'identité alors d'après le 2.d., la matrice Λ est indécomposable. Par le I.7.b. on en conclut que les matrices $\Lambda\, {}^t\Lambda$ et ${}^t\Lambda\Lambda$ sont des matrices positives irréductibles et diagonalisables à valeurs propres positives ou nulles.

c. Comme A est diagonalisable à valeurs propres positives ou nulles alors pour tout vecteur y, on a

$$Ay = \sum \lambda_i P_i y$$

où P_i désigne le projecteur orthogonal sur le sous-espace propre associé à la valeur propre λ_i et λ_0 la valeur propre de module maximal. Comme A est

symétrique alors $\|A\| = \lambda_0$ et on a $A^k y = \sum \lambda_i^k P_i y$. Par le I.7.b., on sait que pour toute valeur propre α de A distincte de celle de module maximal, $|\alpha| < \lambda_0$, donc on en conclut que

$$\lim_{k\to\infty} \frac{A^k}{\|A^k\|} y = \lim_{k\to\infty} \frac{A^k}{\lambda_0^k} y = P_0 y.$$

d. On a vu au I.2.g que le sous-espace propre associé à la valeur propre de module maximal est de dimension 1 et que $\mathrm{im} P_0 = \mathrm{Vect} z$ où z est un vecteur strictement positif. Comme y est un vecteur positif non nul, $P_0 y = \langle z, y\rangle z$ est non nul.

D'après la question précédente, on a

$$\lim_{k\to\infty} \|(\Lambda\, {}^t\Lambda)^k y\|^{1/k} = \lim_{k\to\infty} \|({}^t\Lambda\Lambda)^k y\|^{1/k} = \|A\|.$$

D'après le b., A est irréductible et on a vu au III.2.a. que dans ce cas $\|A\| = \|\Lambda\|^2$ ce qui établit le résultat.

e. On a un morphisme injectif avec unité de $S_0 = R = \bigoplus_{j=1}^r \mathcal{M}_{a_j}(\mathbb{C})$ dans $S_k = S = \bigoplus_{i=1}^s \mathcal{M}_{b_i}(\mathbb{C})$ et la matrice d'indice pour cette inclusion est définie par

$$\begin{aligned} \alpha_{ij} &= 0 \quad \text{si } p_i q_j = 0 \\ \alpha_{ij} &= [S_{ij} : R_{ij}]^{\frac{1}{2}} \quad \text{si } p_i q_j \neq 0. \end{aligned}$$

On sait que par le 2.b. que lorsque $p_i q_j \neq 0$,

$$\mathcal{M}_{a_j}(\mathbb{C}) \simeq R_{ij} \text{ et } (\dim S_{ij})^{1/2} = \mathrm{rg}(p_i q_j).$$

Or $\{q_1, \ldots, q_r\}$ sont des idempotents orthogonaux dont la somme vaut l'identité donc

$$\sum_{j=1}^r \mathrm{rg}(p_i q_j) = \mathrm{rg}(p_i) = b_i.$$

Par la définition des α_{ij}, on en déduit que

$$\sum_{j=1}^r \alpha_{ij} a_j = b_i.$$

Soit $y = \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix}$.

Dans le cas pair : $k = 2p$. On a d'après le a.,

$$\dim(S_{2p}) = \sum_{i=1}^s b_i^2 = \|(\Lambda\, {}^t\Lambda)^p y\|^2$$

Dans le cas impair : $k = 2p+1$, on a

$$\dim(S_{2p+1}) = \sum_{i=1}^s b_i^2 = \|(\Lambda\, {}^t\Lambda)^p \Lambda y\|^2.$$

Or y et Λy sont des vecteurs positifs non nuls donc par le d., on en conclut que

$$\lim_{k\to\infty} (\dim(S_k))^{1/k} = \|\Lambda\|^2.$$

Comme Λ est une matrice à coefficients entiers, on peut appliquer les résultats du III.2.b.. Ainsi $\|\Lambda\|^2 \geq 4$ ou $\|\Lambda\|^2 = 4\cos^2(\frac{\pi}{q})$ avec q entier supérieur ou égal à 3 (car $\Lambda \neq 0$).

7.3 Commentaires

Comme l'indique clairement l'énoncé, les trois premières parties de cette épreuve sont indépendantes. Il est donc important le jour du concours que le candidat les lise et choisisse celle par laquelle il préfère commencer.

La première partie traite d'algèbre linéaire et de réduction de matrices à coefficients positifs autour du théorème de Perron-Froebenius. Les parties II et III, bien qu'indépendantes, établissent les premiers résultats de la théorie des représentations des algèbres associatives, la troisième partie demandant de maîtriser la notion de corps de rupture d'un polynôme. Enfin, la dernière partie traite d'indices d'inclusion des algèbres semi-simples et demande d'être prêt à utiliser tous les résultats établis dans les parties précédentes.

Chapitre 8

Session de 1996

8.1 Sujet

8.2 Correction

Partie 1. Partitions d'un entier

1. r' est le nombre de lignes du diagramme Λ' associé à λ', c'est-à-dire le nombre de colonnes du diagramme Λ associé à λ, on a donc $r' = \lambda_1$.
Soit $k \in \mathbb{N}^*$: r'_k est le nombre de lignes de Λ' qui contiennent k carrés, i.e le nombre de colonnes de Λ qui contiennent k carrés. Or, la j-ème colonne de Λ contient k carrés si et seulement si $\lambda_k \geq j > \lambda_{k+1}$: les k premières lignes de Λ contiennent au moins j carrés, donc la j-ème colonne contient au moins k carrés ; les lignes suivantes de Λ contiennent strictement moins de j carrés, donc la j-ème colonne de Λ contient exactement k carrés.
On a donc

$$r'_k = \lambda_k - \lambda_{k+1} \quad (k \in \mathbb{N}^*).$$

On en déduit que pour $i \in \mathbb{N}^*$:

$$\lambda_1 - \lambda_{i+1} = \sum_{k=1}^{i} (\lambda_k - \lambda_{k+1}) = \sum_{k=1}^{i} r'_k.$$

et tenant compte du fait que $\lambda_1 = r' = \sum_{k \geq 1} r'_k$, on obtient :

$$\lambda_i = \sum_{k \geq i} r'_k \quad (i \geq 1).$$

Comme $\left(\Lambda'\right)' = \Lambda$, on a aussi :

$$\lambda'_i = \sum_{k \geq i} r_k \quad (i \geq 1).$$

2. Il est clair que $\lambda \subset \mu$ si et seulement si le diagramme de λ est contenu dans celui de μ. Le diagramme de λ transposé est alors évidemment inclus dans celui de μ transposé et donc $\lambda' \subset \mu'$. De même, si $\lambda' \subset \mu'$, alors $\lambda = (\lambda')' \subset (\mu')' = \mu$.

3. Il est clair que :

$$(\lambda \oplus \mu)' = \lambda' + \mu'$$

et

$$(\lambda + \mu)' = \lambda' \oplus \mu' \ .$$

Partie 2. Quelques lemmes

4.a. On développe le produit et on regroupe suivant les puissances de T. Pour $k \geq 1$, le terme facteur de T^k est :

$$\sum_{0 \leq i_1 < \ldots < i_k \leq n-1} X^{i_1+\ldots+i_k}.$$

Or, si $(i_1, \ldots, i_k)$ est un k-uplet d'entiers tels que $0 \leq i_1 < \ldots < i_k \leq n-1$, on a :

$$i_1 + \ldots + i_k \geq 0 + 1 + \ldots + (k-1) = \frac{k\,(k-1)}{2}.$$

$X^{\frac{k\,(k-1)}{2}}$ est donc facteur de $X^{i_1+\ldots+i_k}$, donc de $\displaystyle\sum_{0 \leq i_1 < \ldots < i_k \leq n-1} X^{i_1+\ldots+i_k}$, et l'autre facteur est à coefficients entiers positifs (ses coefficients valent 0 ou 1). On peut donc bien écrire pour $k \geq 1$:

$$\sum_{0 \leq i_1 < \ldots < i_k \leq n-1} X^{i_1+\ldots+i_k} = X^{\frac{k\,(k-1)}{2}}\, P_{n,k}(X).$$

avec $P_{n,k}$ à coefficients entiers positifs.
Cette écriture est valide aussi pour $k = 0$ avec $P_{n,0} = 1$. D'où le résultat.

4.b. Soit $n \geq 1$. On écrit $\displaystyle\prod_{i=0}^{n}(1 + X^i T) = (1 + X^n T) \prod_{i=0}^{n-1}(1 + X^i T)$. On a donc :

$$\begin{aligned}
\prod_{i=0}^{n}(1 + X^i T) &= (1 + X^n T)\Big(\sum_{k=0}^{n} X^{\frac{k\,(k-1)}{2}} P_{n,k}(X) T^k\Big) \\
&= \sum_{k=0}^{n} X^{\frac{k\,(k-1)}{2}} P_{n,k}(X) T^k \\
&+ \sum_{k=0}^{n} X^{\frac{k\,(k-1)}{2}} P_{n,k}(X) X^n T^{k+1}.
\end{aligned}$$

Or, on a :

$$\begin{aligned}
\sum_{k=0}^{n} X^{\frac{k\,(k-1)}{2}} P_{n,k}(X) X^n T^{k+1} &= X^{\frac{n\,(n-1)}{2}} P_{n,n}(X) X^n T^{n+1} \\
&+ \sum_{j=1}^{n} X^{\frac{(j-1)\,(j-2)}{2}} P_{n,j-1}(X) X^n T^j.
\end{aligned}$$

et pour $1 \leq j \leq n$:

$$X^{\frac{(j-1)\,(j-2)}{2}} X^n = X^{\frac{j\,(j-1)}{2}} X^{n-j+1}.$$

Il en résulte que :

$$\begin{aligned}
\prod_{i=0}^{n}(1 + X^i T) &= \sum_{k=1}^{n} X^{\frac{k\,(k-1)}{2}} \big(P_{n,k}(X) + X^{n-k+1} P_{n,k-1}(X)\big) T^k \\
&+ P_{n,0}(X) + X^{\frac{n\,(n+1)}{2}} P_{n,n}(X) T^{n+1}.
\end{aligned}$$

On a donc par identification (la famille $\{T^k\}_{k\geq 0}$ est une base de $\big(\mathbb{Q}(X)\big)[T]$) :

$$\left\{\begin{array}{rcl} P_{n+1,0}(X) & = & P_{n,0}(X) \\ P_{n+1,k}(X) & = & P_{n,k}(X) + X^{n-k+1}P_{n,k-1}(X) \quad \text{si } 1\leq k\leq n \\ P_{n+1,n+1}(X) & = & P_{n,n}(X) \end{array}\right. .$$

On en déduit immédiatement que $\forall n\in\mathbb{N},\quad P_{n,0}(X)=P_{n,n}(X)=1$.

5.a. Si $n\in\mathbb{N}^*$, et si $1\leq k\leq n$, on a :

$$\begin{aligned} &F_{n,k}+X^{n-k+1}F_{n,k-1}\\ &=\frac{(1-X^{n-k+1})\dots(1-X^n)}{(1-X)\dots(1-X^k)}+X^{n-k+1}\frac{(1-X^{n-k+2})\dots(1-X^n)}{(1-X)\dots(1-X^{k-1})}\\ &=\frac{(1-X^{n-k+2})\dots(1-X^n)[(1-X^{n-k+1})+X^{n-k+1}(1-X^k)]}{(1-X)\dots(1-X^k)}\\ &=\frac{(1-X^{n-k+2})\dots(1-X^n)(1-X^{n+1})}{(1-X)\dots(1-X^k)}\\ &=F_{n+1,k}\end{aligned}$$

Il est d'autre part clair que $F_{n,n}(X)=1$, et l'énoncé pose $F_{n,0}(X)=1$. Donc les $F_{n,k}$ satisfont à toutes les conditions qui définissent en 4.b. les $P_{n,k}$ de manière unique dans $\mathbb{Q}[X]$, mais en fait aussi dans $\mathbb{Q}(X)$: les $F_{n,k}$ sont en réalité les $P_{n,k}$, donc d'après 4.a. des polynômes à coefficients entiers positifs.

5.b. Le degré sur $\mathbb{Q}(X)$ défini par $\deg U/V=\deg U-\deg V$ prolonge le degré sur $\mathbb{Q}[X]$ et possède des propriétés identiques. Il vient donc :

$$\begin{aligned}\deg F_{n,k} &= \deg\Big(\prod_{i=1}^{k}\frac{1-X^{n-k+i}}{1-X^i}\Big)\\ &= \sum_{i=1}^{k}\deg\frac{1-X^{n-k+i}}{1-X^i}\\ &= \sum_{i=1}^{k}(n-k)=k\,(n-k)\end{aligned}$$

5.c. Si $k=0$, il suffit de se rappeler que $F_{n,0}(X)=F_{n,n}(X)=1$.
Si $k\in\{1,\dots,n\}$, on multiplie numérateur et dénominateur de $F_{n,k}$ par le produit $(1-X)\dots(1-X^{n-k})$ pour obtenir

$$F_{n,k}(X)=\frac{(1-X)\dots(1-X^n)}{(1-X)\dots(1-X^{n-k})\,(1-X)\dots(1-X^k)}\ ,$$

expression sur laquelle il est évident que $F_{n,k}=F_{n,n-k}$.

6.a. Comptons tout d'abord le nombre N_r de systèmes ordonnés libres $(e_1,\dots,e_r)$ de r vecteurs que l'on peut choisir dans E (qui compte p^n éléments). On a p^n-1choix possibles pour le premier vecteur e_1. Une fois que l'on a choisi $e_1,\dots,e_i$, e_{i+1} doit être choisi dans E privé de l'espace engendré par $e_1,\dots,e_i$, qui compte p^i éléments : on a donc p^n-p^i choix possibles pour e_{i+1}.
Il vient donc :

$$N_r=\prod_{i=1}^{r}(p^n-p^{i-1})=\prod_{i=1}^{r}(p^{n-i+1}-1)\prod_{i=1}^{r}p^{i-1}.$$

Si F désigne à présent un sous-espace vectoriel de E de dimension r, un calcul analogue au précédent montre que le nombre N'_r de bases ordonnées de F est

$$N'_r = \prod_{i=1}^{r}(p^r - p^{i-1}) = \prod_{i=1}^{r}(p^{r-i+1} - 1) \prod_{i=1}^{r} p^{i-1}.$$

Or, un sous-espace vectoriel de E de dimension r est déterminé par un système libre de r vecteurs, et deux tels systèmes engendrent le même sous-espace si et seulement si ils sont deux bases d'un même sous-espace : le nombre de sous-espaces de dimension r de E est donc

$$\frac{N_r}{N'_r} = \frac{\prod_{i=1}^{r}(p^{n-i+1} - 1)}{\prod_{i=1}^{r}(p^{r-i+1} - 1)} = F_{n,r}(p).$$

6.b. Les sous-espaces G de E, de dimension r et contenant F sont en bijection avec les sous-espaces $\overline{G}$ de E/F de dimension $r - l$ via la surjection canonique de E sur E/F. Mais E/F est à son tour un espace vectoriel de dimension $n - l$ sur $\mathbb{Z}/p\mathbb{Z}$, donc d'après a. :

$$c_{n,l,r} = F_{n-l,r-l}(p).$$

On a donc, en utilisant ce qui précède et 5.c.,

$$c_{n,l,n+r-l} = F_{n-l,n-r}(p) = F_{n-l,n-l-(n-r)}(p) = c_{n,l,r}.$$

6.c. Le cas $n = l$ est évident : la somme vaut $c_{l,l,l}$, c'est-à-dire 1.
Si $n > l$, on applique la formule du 4.a., avec X spécialisé en p, T en -1 et n remplacé par $n - l$. On obtient :

$$\prod_{i=0}^{n-l+1}(1 - p^i) = \sum_{k=0}^{n-l} p^{\frac{k(k-1)}{2}} P_{n-l,k}(p)(-1)^k.$$

Or, d'une part le produit est nul (son premier terme est nul), et d'autre part :

$$P_{n-l,k}(p) = F_{n-l,k}(p) = c_{n,l,l+k} \quad \text{d'après 5. et b.}$$

Donc on a bien

$$\sum_{k=0}^{n-l}(-1)^k p^{\frac{k(k-1)}{2}} c_{n,l,l+k} = 0\ .$$

6.d. Soit F un sous-espace vectoriel de E. Alors :

$$\begin{aligned}\sum_{G\subset F}(-1)^l p^{\frac{l(l-1)}{2}} f_G &= \sum_{G\subset F}(-1)^l p^{\frac{l(l-1)}{2}} \Big(\sum_{H\subset G} g_H\Big) \\ &= \sum_{H\subset G\subset F}(-1)^l p^{\frac{l(l-1)}{2}} g_H \\ &= \sum_{H\subset F}\Big(\sum_{H\subset G\subset F}(-1)^l p^{\frac{l(l-1)}{2}}\Big) g_H.\end{aligned}$$

Pour calculer la deuxième somme (où H est fixé et G varie), on regroupe les sous-espaces G de E tels que $H \subset G \subset F$ suivant leur dimension. On a donc :

$$\sum_{H\subset G\subset F} (-1)^l p^{\frac{l(l-1)}{2}} = \sum_{k=\dim H}^{\dim F} \Big(\sum_{H\subset G\subset F, \dim G=k} (-1)^l p^{\frac{l(l-1)}{2}} \Big).$$

Or le nombre $l = l_F(G)$ ne dépend que de la dimension de G, donc si $\dim H \leq k \leq \dim F$:

$$\sum_{H\subset G\subset F, \dim G=k} (-1)^l p^{\frac{l(l-1)}{2}} = (-1)^l p^{\frac{l(l-1)}{2}} N_k$$

où N_k est le nombre de sous-espaces G de E tels que $H \subset G \subset F$ de dimension k, c'est-à-dire que $N_k = c_{\dim F, \dim H, k}$. D'autre part, si G est un sous-espace de dimension k de E tels que $H \subset G \subset F$, on a $l = l_F(G) = \dim F - k$. La somme totale cherchée vaut donc :

$$\sum_{H\subset F} \Big(\sum_{k=\dim H}^{\dim F} (-1)^{(\dim F - k)} p^{\frac{(\dim F-k)(\dim F-k-1)}{2}} c_{\dim F, \dim H, k} \Big) g_H.$$

ou encore :

$$\sum_{H\subset F} \Big(\sum_{j=0}^{\dim F - \dim H} (-1)^{(j)} p^{\frac{j(j-1)}{2}} c_{\dim F, \dim H, \dim H + j} \Big) g_H.$$

D'après c., la somme $\sum_{j=0}^{\dim F - \dim H} (-1)^{(j)} p^{\frac{j(j-1)}{2}} c_{\dim F, \dim H, \dim H+j}$ est nulle si $\dim F > \dim H$, et vaut 1 si $\dim H = \dim F$. La somme précédente se réduit donc à g_F, ce qui est le résultat demandé.

7. Remarquons que puisque G est commutatif, tous les sous-groupes considérés ici sont distingués, et les quotients que l'on envisage sont bien munis d'une structure de groupe compatible avec la surjection canonique.

7.a. Soit π la surjection canonique de G sur G/K. On a bien sûr $H/K = \pi(H)$. Comme π est un homomorphisme de groupes, H/K est un sous-groupe de G/K. Considérons alors π' la surjection canonique de G/K sur $\dfrac{G/K}{H/K}$ ainsi que $\varphi = \pi' \circ \pi$. Le théorème d'isomorphisme nous dit que

$$\operatorname{im} \varphi \simeq G/\ker \varphi.$$

Comme π et π' sont surjectives, φ l'est aussi, i.e

$$\operatorname{im} \varphi = \frac{G/K}{H/K}.$$

On a $\ker \varphi = \{g \in G \ / \ \pi(g) \in H/K\}$. Il est alors clair que $H \subset \ker \varphi$.
Si $g \in G$ est tel que $\pi(g) \in H/K = \pi(H)$, alors il existe $h \in H$ tel que $\pi(g) = \pi(h)$, ce qui signifie que $g - h \in K$. Donc $g \in h + K \subset H$ car $K \subset H$. Donc $\ker \varphi = H$ et on a bien l'isomorphisme annoncé.

7.b. K est bien sûr un sous-groupe de $H + K$, et on peut considérer π la surjection canonique de $H + K$ sur $(H + K)/K$. Soit ψ la restriction de π à H.

On a $\ker\psi = H \cap \ker\pi = H \cap K$. ψ est d'autre part surjective : si g est dans $H+K$, g s'écrit $g = h + k$ avec $h \in H$ et $k \in K$ et on a

$$\pi(g) = \pi(h) + \pi(k) = \pi(h) = \psi(h) \in \operatorname{im}\psi.$$

Il suffit d'appliquer le théorème d'isomorphisme à ψ pour obtenir le résultat.

7.c. π est maintenant la surjection canonique de G sur G/H et on considère θ la restriction de π à qG.
On a $\ker\theta = \ker\pi \cap qG = H \cap qG$.
D'autre part, si $g \in G$, $\theta(qg) = \pi(qg) = q\pi(g) \in q\,(G/H)$. Réciproquement, si $x \in q\,(G/H)$, x s'écrit $x = q\pi(g)$ avec $g \in G$, i.e $x = \pi(qg) = \theta(qg) \in \operatorname{im}\theta$. Donc $\operatorname{im}\theta = q\,(G/H)$.
On applique alors le théorème d'isomorphisme à θ.

Partie 3. Les p-groupes commutatifs finis

8.a. Si G est de type λ, $G \simeq \mathbb{Z}/p^{\lambda_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\lambda_r}\mathbb{Z}$.
Si H est de type μ, $H \simeq \mathbb{Z}/p^{\mu_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\mu_l}\mathbb{Z}$.
$G \times H$ est alors isomorphe à

$$\mathbb{Z}/p^{\lambda_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\lambda_r}\mathbb{Z} \times \mathbb{Z}/p^{\mu_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\mu_l}\mathbb{Z}.$$

On peut réarranger le $(r+l)$-uplet $(\lambda_1, \ldots, \lambda_r, \mu_1, \ldots, \mu_l)$ en un $(r+l)$-uplet $(\nu_1, \ldots, \nu_{r+l})$ tel que $\nu_1 \geq \ldots \geq \nu_{r+l}$. Il est clair que ν est le type de $G \times H$.
Montrons qu'en fait $\nu = \lambda \oplus \mu$. On procède pour cela par récurrence sur $r+l$.
Si $r = l = 1$, c'est évident.
Supposons que $r + l > 2$ et que le résultat soit vrai pour $r + l - 1$. Il est clair que la première ligne de $\lambda \oplus \mu$ est $\max(\lambda_1, \mu_1) = \nu_1$. Pour fixer les idées, supposons que $\nu_1 = \lambda_1$ et considérons η qui est λ privée de λ_1. Il est clair que le réarrangé $(\xi_1, \ldots, \xi_{r+l-1})$ associé à la paire (η, μ) est $(\nu_2, \ldots, \nu_{r+l})$, donc il suffit d'appliquer l'hypothèse de récurrence pour obtenir que

$$(\nu_2, \ldots, \nu_{r+l}) = \eta \oplus \mu$$

et donc que $\nu = \lambda \oplus \mu$.

8.b. Puisque $\operatorname{Card}(G/H) = \dfrac{\operatorname{Card} G}{\operatorname{Card} H}$, on a $p^{l(G/H)} = p^{l(G)-l(H)}$.
D'où $l(G/H) = l(G) - l(H)$.

8.c. On a vu au 7.a. que $G/H \simeq \dfrac{G/K}{H/K}$: la définition du cotype entraine alors immédiatement le résultat.

9. Supposons $g^{\rho}_{\lambda\mu}(p) \neq 0$. Il existe alors H un sous-groupe de $G_\rho(p)$ tel que $H \simeq G_\lambda(p)$ et $G_\rho(p)/H \simeq G_\mu(p)$. Dans ce cas, on a d'une part

$$\operatorname{Card} H = \operatorname{Card} G_\lambda(p) = p^{|\lambda|}$$

et d'autre part

$$\operatorname{Card} H = \frac{\operatorname{Card} G_\rho(p)}{\operatorname{Card} G_\mu(p)} = p^{|\rho|-|\mu|}.$$

Donc $|\lambda| + |\mu| = |\rho|$. Ainsi, si $|\lambda| + |\mu| \neq |\rho|$, $g^{\rho}_{\lambda\mu}(p) = 0$.
Pour montrer que la multiplication sur $A(p)$ est bien définie, il suffit de voir que pour tous λ, μ, $g^{\rho}_{\lambda\mu}(p)$ est nul sauf pour un nombre fini de $\rho \in \Lambda$, ce qui est le cas puisqu'il n'existe qu'un nombre fini de ρ qui vérifient $|\rho| = |\lambda| + |\mu|$.

10. Fixons (λ, μ, ν) dans Λ^3 :

$$\begin{aligned}\Big(G_\lambda(p)G_\mu(p)\Big)G_\nu(p) &= \Big(\sum_{\rho\in\Lambda} g^{\rho}_{\lambda\mu}(p)G_\rho(p)\Big)G_\nu(p)\\ &= \sum_{\rho\in\Lambda} g^{\rho}_{\lambda\mu}(p)G_\rho(p)G_\nu(p)\\ &= \sum_{\rho\in\Lambda} g^{\rho}_{\lambda\mu}(p)\Big(\sum_{\rho'\in\Lambda} g^{\rho'}_{\rho\nu}(p)G_{\rho'}(p)\Big)\\ &= \sum_{\rho'\in\Lambda}\Big(\sum_{\rho\in\Lambda} g^{\rho}_{\lambda\mu}(p)g^{\rho'}_{\rho\nu}(p)\Big)G_{\rho'}(p).\end{aligned}$$

Par un calcul analogue, on obtient d'autre part :

$$G_\lambda(p)\Big(G_\mu(p)G_\nu(p)\Big) = \sum_{\rho'\in\Lambda}\Big(\sum_{\rho\in\Lambda} g^{\rho}_{\mu\nu}(p)g^{\rho'}_{\lambda\rho}(p)\Big)G_{\rho'}(p).$$

Comme pour vérifier l'associativité de la multiplication de $A(p)$, il suffit de le faire sur les éléments de la base des $G_\rho(p)$, il suffit de montrer que pour tout $(\lambda, \mu, \nu, \rho')$ dans Λ^4, on a :

$$\sum_{\rho\in\Lambda} g^{\rho}_{\lambda\mu}(p)g^{\rho'}_{\rho\nu}(p) = \sum_{\rho\in\Lambda} g^{\rho}_{\mu\nu}(p)g^{\rho'}_{\lambda\rho}(p).$$

Pour cela, calculons de deux manières différentes $g^{\rho'}_{\lambda\mu\nu}(p)$. Par définition, $g^{\rho'}_{\lambda\mu\nu}(p)$ est le nombre de couples (H_1, H_2) de sous-groupes de $G_{\rho'}(p)$ tels que $H_1 \subset H_2$, H_1 est de type λ, H_2/H_1 est de type μ et $G_{\rho'}(p)/H_2$ est de type ν.
D'une part, pour chaque $\rho \in \Lambda$, il y a $g^{\rho'}_{\rho\nu}(p)$ sous-groupes H_2 de $G_{\rho'}(p)$ de type ρ tels que $G_{\rho'}(p)/H_2$ est de type ν. Pour chacun de ces H_2, il y a par définition $g^{\rho}_{\lambda\mu}(p)$ sous-groupes H_1, de type λ et de cotype (dans H_2) μ.
Il vient donc

$$g^{\rho'}_{\lambda\mu\nu}(p) = \sum_{\rho\in\Lambda} g^{\rho}_{\lambda\mu}(p)g^{\rho'}_{\rho\nu}(p).$$

D'autre part, pour chaque $\rho \in \Lambda$, il y a $g^{\rho'}_{\lambda\rho}(p)$ sous-groupes H_1 de $G_{\rho'}(p)$ de type λ et de cotype ρ. Donnons-nous un de ces H_1 : $G_{\rho'}(p)/H_1$ est donc isomorphe à $G_\rho(p)$, donc le nombre de sous-groupes de $G_{\rho'}(p)/H_1$ de type μ et de cotype ν est $g^{\rho}_{\mu\nu}(p)$. Mais l'ensemble de ces sous-groupes est en bijection via la surjection canonique avec l'ensemble des sous-groupes H_2 de $G_{\rho'}(p)$ contenant H_1 et vérifiant H_2/H_1 de type μ et $G_{\rho'}(p)/H_2$ de type ν (d'après 8.c., le type de $G_{\rho'}(p)/H_2$ est aussi celui de $\dfrac{G_{\rho'}(p)/H_1}{H_2/H_1}$).
En conséquence,

$$g^{\rho'}_{\lambda\mu\nu}(p) = \sum_{\rho\in\Lambda} g^{\rho'}_{\lambda\rho}(p)g^{\rho}_{\mu\nu}(p).$$

D'où le résultat.

11.a. Tout d'abord, remarquons que si $G_1, \dots, G_n$ sont des groupes commutatifs, alors les groupes $\widehat{G_1 \times \dots \times G_n}$ et $\widehat{G_1} \times \dots \times \widehat{G_n}$ sont isomorphes : si $\phi \in \widehat{G_1 \times \dots \times G_n}$, on lui associe en effet $f_i(\phi) \in \widehat{G_i}$ défini par la relation $f_i(\phi)(x) = \phi(0, \dots, x, \dots, 0)$ (x est à la i-ème place).
L'application $\phi \to (f_1(\phi), \dots, f_n(\phi))$ est l'isomorphisme annoncé.
D'après cette remarque, il suffit donc de montrer le résultat pour chacun des facteurs cycliques de G : on peut supposer que G est cyclique. Soit n le cardinal de G et g un générateur. Considérons l'application

$$\begin{array}{rccc} \varphi & : & \widehat{G} & \to & \mathbb{C}^* \\ & & \phi & \mapsto & \phi(g) \end{array} .$$

Il est clair que φ est un homomorphisme de groupes. Comme g engendre G, il est injectif.
D'autre part, si $\phi \in \widehat{G}$, $\big(\phi(g)\big)^n = \phi(ng) = \phi(1) = 1$. Ceci montre que l'image de φ est contenue dans U_n, le groupe des racines n-ı‘emes de 1. Réciproquement, si $\zeta \in U_n$, en posant $\phi(pg) = \zeta^p$ on défini un élément de $\widehat{G}$ et $\zeta \in \operatorname{im} \varphi$. L'image de φ est ainsi U_n, et $\widehat{G}$ est isomorphe à U_n, donc à G (U_n et G sont deux groupes cycliques de même ordre).

11.b. Il suffit une fois encore de faire la démonstration dans le cas de $G_\lambda(p)$. Si $x \neq 0$ dans $G_\lambda(p)$, cela signifie en posant $x = (x_1, \dots, x_r)$ qu'il existe un i tel que x_i est non nul (dans $\mathbb{Z}/p^{\lambda_i}\mathbb{Z}$). Soit g un générateur de $\mathbb{Z}/p^{\lambda_i}\mathbb{Z}$, on peut écrire $x_i = j\,g$ avec $j \in \{0, \dots, p^{\lambda_i} - 1\}$. Soit ζ une racine primitive p^{λ_i}-ième de 1 et soit ϕ l'unique élément de $\widehat{\mathbb{Z}/p^{\lambda_i}\mathbb{Z}}$ tel que $\phi(g) = \zeta$. On définit alors $\theta \in \widehat{G_\lambda(p)}$ par $\theta(y_1, \dots, y_n) = \phi(y_i)$.
On a alors $\theta(x) = \phi(j\,g) = \zeta^j \neq 1$.
Intéressons-nous maintenant à Φ. Soit $x \in G$. Pour $\varphi, \phi \in \widehat{G}$, on a

$$\Phi(x)(\varphi\phi) = (\varphi\phi)(x) = \varphi(x)\phi(x) = \Phi(x)(\varphi)\Phi(x)(\phi)$$

donc $\Phi(x) \in \widehat{\widehat{G}}$.
Considérons ensuite $x, y \in G$. Pour $\phi \in \widehat{G}$, on a :

$$\Phi(x+y)(\phi) = \phi(x+y) = \phi(x)\phi(y) = \Phi(x)(\phi)\Phi(y)(\phi)$$

donc $\Phi(x+y) = \Phi(x)\Phi(y)$, ce qui prouve que Φ est un homomorphisme de groupes.
L'injectivité de Φ résulte de ce qui précède (si $x \neq 1$, il existe $\phi \in \widehat{G}$ tel que $\Phi(x)(\phi) \neq 1$, donc $\Phi(x) \neq 1$ et $x \notin \ker \Phi$).
Mais on sait que G et $\widehat{G}$ sont isomorphes, ainsi que $\widehat{G}$ et $\widehat{\widehat{G}}$: ces trois groupes ont mêmes cardinaux, et Φ est alors bijective.

11.c. Remarquons tout d'abord que $H^\circ = \bigcap_{x \in H} \ker \Phi(x)$, c'est donc un sous-groupe de G.
Soit π la surjection canonique de G sur G/H.
Soit $\phi \in H^\circ$. Si g et g' sont deux éléments de G tels que $g - g' \in H$, alors on a $\phi(g - g') = 1 = \phi(g)/\phi(g')$, i.e $\phi(g) = \phi(g')$. Ceci permet de définir sans équivoque une application $\theta(\phi)$ de G/H dans $\mathbb{C}^*$ en posant $\theta(\phi)(\pi(g)) = \phi(g)$.
De plus, si $g, g' \in G$, on a

$$\theta(\phi)(\pi(g)\pi(g')) = \theta(\phi)(\pi(gg')) = \phi(gg') = \phi(g)\phi(g') = \theta(\phi)(\pi(g))\theta(\phi)(\pi(g')).$$

Donc $\theta(\phi)$ est dans $\widehat{G/H}$.
On a donc défini une application θ de H° dans $\widehat{G/H}$. Montrons que c'est un isomorphisme de groupes.
Soient $\phi, \psi \in H^\circ$ et soit $g \in G$:

$$\theta(\phi\psi)(\pi(g)) = (\phi\psi)(g) = \phi(g)\psi(g) = [\theta(\phi)\theta(\psi)](\pi(g))$$

donc θ est un homomorphisme de groupes.
Si $\psi \in \ker\theta$, alors pour tout $g \in G$, $\psi(g) = \theta(\psi)(\pi(g)) = 1$, donc $\psi = 1$ et θ est injective.
Si $\varphi \in \widehat{G/H}$, posons pour $g \in G$, $\phi(g) = \varphi(\pi(g))$. Il est clair que $\phi \in H^\circ$ et on a $\theta(\phi) = \varphi$ et θ est bien surjective.

11.d. Considérons $\Gamma : \widehat{G} \to \widehat{H}$ définie par $\Gamma(\phi) = \phi_{|H}$. Il est clair que Γ est un morphisme de groupes et que $\ker\Gamma = H^\circ$. On a donc un isomorphisme entre $\widehat{G}/H^\circ$ et $\operatorname{im}\Gamma$. On a en particulier

$$\operatorname{Card}\operatorname{im}\Gamma = \frac{\operatorname{Card}(\widehat{G})}{\operatorname{Card} H^\circ} = \frac{\operatorname{Card} G}{\operatorname{Card} H^\circ}.$$

Or d'après c., on a

$$\operatorname{Card} H^\circ = \operatorname{Card}(\widehat{G/H}) = \operatorname{Card} G/H = \frac{\operatorname{Card} G}{\operatorname{Card} H}.$$

Donc $\operatorname{Card}\operatorname{im}\Gamma = \operatorname{Card} H = \operatorname{Card}\widehat{H}$, et $\operatorname{im}\Gamma = \widehat{H}$, ce qui répond à la question.

11.e. Montrons que pour tout sous-groupe H de G, $H = (H^\circ)^\perp$.
On a l'inclusion évidente $H \subset (H^\circ)^\perp$. Réciproquement, si $x \notin H$, alors dans G/H, on a $\pi(x) \neq 0$ (π désigne toujours la surjection canonique de G sur G/H). On peut donc considérer d'après b., $\chi \in \widehat{G/H}$ tel que $\chi(\pi(x)) \neq 1$. Il est clair que $\chi \circ \pi \in H^\circ$. Ainsi $x \notin (H^\circ)^\perp$, ce qui prouve ce que nous voulions.
Il en résulte que l'application proposée est injective car si $H_1^\circ = H_2^\circ$ alors

$$H_1 = (H_1^\circ)^\perp = (H_2^\circ)^\perp = H_2.$$

Mais comme on sait depuis le a. que G et $\widehat{G}$ sont isomorphes, ils ont même nombre de sous-groupes, et la surjectivité en découle. L'application réciproque est $K \to K^\perp$.

11.f. Soit $(\lambda, \mu, \rho) \in \Lambda^3$.
Considérons H un sous-groupe de $G = G_\rho(p)$ de type λ et de cotype μ. H° est isomorphe à $\widehat{G/H}$, lui-même isomorphe à G/H, donc H° est de type μ. $\widehat{G}/H^\circ$ est isomorphe à $\widehat{H}$, donc à H et H° est de cotype λ.
On en déduit grâce à e. que $g^\rho_{\lambda\mu}(p) \leq g^\rho_{\mu\lambda}(p)$ et il y a en fait égalité en échangeant les rôles de λ et μ. La commutativité de la multiplication dans $A(p)$ en découle.

12. On sait que $G \simeq \mathbb{Z}/p^{\lambda_1}\mathbb{Z} \times \ldots \mathbb{Z}/p^{\lambda_r}\mathbb{Z}$.
Il est alors évident que

$$\forall j \in \mathbb{N} \quad p^j G \simeq p^j\left(\mathbb{Z}/p^{\lambda_1}\right)\mathbb{Z} \times \ldots \times p^j\left(\mathbb{Z}/p^{\lambda_r}\mathbb{Z}\right).$$

Soit $j \in \mathbb{N}$ et $i \in \{1, \ldots, r\}$.
Il est clair que si $j \geq \lambda_i$ alors $p^j\Big(\mathbb{Z}/p^{\lambda_i}\mathbb{Z}\Big) = \{0\}$.
Si $j < \lambda_i$, on applique 7.c. avec $q = p^j$, $G = \mathbb{Z}$ et $H = p^{\lambda_i}\mathbb{Z}$. On obtient :

$$p^j\Big(\mathbb{Z}/p^{\lambda_i}\mathbb{Z}\Big) \simeq \big(p^j\mathbb{Z}\big)/\big(p^{\lambda_i}\mathbb{Z} \cap p^j\mathbb{Z}\big).$$

Comme $j < \lambda_i$, on a $\big(p^{\lambda_i}\mathbb{Z} \cap p^j\mathbb{Z}\big) = p^{\lambda_i}\mathbb{Z}$. Le cardinal de $p^j\Big(\mathbb{Z}/p^{\lambda_i}\mathbb{Z}\Big)$ est ainsi l'indice de $p^{\lambda_i}\mathbb{Z}$ dans $p^j\mathbb{Z}$, c'est-à-dire que

$$\operatorname{Card} p^j\Big(\mathbb{Z}/p^{\lambda_i}\mathbb{Z}\Big) = p^{\lambda_i - j}.$$

Finalement, on a pour $1 \leq i \leq r$,

$$\operatorname{Card} p^j\Big(\mathbb{Z}/p^{\lambda_i}\mathbb{Z}\Big) = p^{\max(\lambda_i - j, 0)}$$

et ainsi,

$$\operatorname{Card}\left(p^jG\right) = \prod_{i=1}^{r} p^{\max(\lambda_i - j, 0)} = p^{\left(\sum_{i=1}^{r} \max(\lambda_i - j, 0)\right)}.$$

On en déduit que

$$l(p^jG) = \sum_{i=1}^{r} \max(\lambda_i - j, 0).$$

D'après 8.b., on a $\mu_j = l(p^{j-1}G) - l(p^jG)$, d'où

$$\mu_j = \sum_{i=1}^{r} \big(\max(\lambda_i - j + 1, 0) - \max(\lambda_i - j, 0)\big)$$

Mais $\max(\lambda_i - j + 1, 0) - \max(\lambda_i - j, 0)$ vaut 1 si $\lambda_i \geq j$ et 0 sinon. On en déduit que

$$\mu_j = \operatorname{Card}\{i \ / \ \lambda_i \geq j\} = \lambda'_j.$$

Ainsi $\mu = \lambda'$.

13. G est un groupe de type ρ donc $\rho'_i = l\big(p^{i-1}G/p^iG\big)$ en appliquant le résultat de 12.
H est de cotype μ dans G donc $\mu'_i = l\big(p^{i-1}G_1/p^iG_1\big)$ où G_1 désigne le groupe G/H.
Notons π la surjection canonique de G sur G_1.
p^iG_1 est un sous-groupe de $p^{i-1}G_1$, on notera π_1 la surjection canonique de $p^{i-1}G_1$ sur $\big(p^{i-1}G_1\big)/\big(p^iG_1\big)$. On notera G_2 ce dernier groupe.
Remarquons que si g et g' sont deux éléments de G qui vérifient $p^{i-1}g = p^{i-1}g'$, alors on a $\pi_1(p^{i-1}\pi(g)) = \pi_1(p^{i-1}\pi(g'))$ et ceci permet de définir sans ambiguité l'application :

$$\begin{array}{rccc} \varphi & : & p^{i-1}G & \to & G_2 \\ & & p^{i-1}g & \mapsto & \pi_1(p^{i-1}\pi(g)) \end{array}.$$

Il est clair que φ est un homomorphisme de groupes surjectif. D'autre part, on a $p^iG \subset \ker\varphi$. il en résulte que

$$\operatorname{Card} G_2 = \frac{\operatorname{Card}\left(p^{i-1}G\right)}{\operatorname{Card}\,\ker\varphi} \leq \frac{\operatorname{Card}\left(p^{i-1}G\right)}{\operatorname{Card}\left(p^iG\right)} = \operatorname{Card}\left(p^{i-1}G/p^iG\right)$$

et par suite

$$l\big(p^{i-1}G/p^iG\big) \geq l(G_2).$$

On a donc $\rho'_i \geq \mu'_i$ pour tout i, i.e $\mu' \subset \rho'$ et ceci équivaut d'après 2. à $\mu \subset \rho$.
Enfin, H° est de cotype λ dans $\widehat{G}$ qui est toujours de type ρ car isomorphe à G, on a donc aussi $\lambda \subset \rho$.

Partie 4 Dénombrement de sous-groupes

14. Soit φ l'application de G dans G définie par $\varphi(x) = px$. Il est clair que φ est un morphisme de groupes. Si on note $S = \ker\varphi$, S est un sous-groupe élémentaire et comme tout sous-groupe élémentaire est contenu dans $\ker\varphi$, S est le socle de G.
G/S est isomorphe à $\operatorname{im}\varphi = pG$. $\tilde{\lambda}$ est ainsi le type de pG. Il est clair que

$$pG \simeq \prod_{i=1}^{r}\Big(\mathbb{Z}/p^{\max(\lambda_i-1,0)}\mathbb{Z}\Big).$$

On a donc $\tilde{\lambda}_i = \max(\lambda_i - 1, 0)$.

15. G est déjà muni d'une structure de groupe commutatif, il suffit donc de trouver une multiplication externe compatible avec cette structure. Il suffit de poser, si $\bar{q} \in \mathbb{Z}/p\mathbb{Z}$ et $x \in G$, $\bar{q}x = qx$ (cette définition est licite car si $\bar{q} = \bar{q'}$, $q - q'$ est un multiple de p et comme G est élémentaire, $(q-q')x = 0$). On vérifie aisément que G devient alors un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.

16. Comme G/H est fini et élémentaire, c'est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie (disons n). On a alors $\operatorname{Card}(G/H) = p^n$ et $n = l(G/H) = l(G) - l(H)$.
Rappelons que le nombre de familles libres $\{\bar{x}_1, \ldots, \bar{x}_l\}$ dans G/H est, comme on l'a expliqué au 6.a.,

$$\prod_{i=1}^{l}(p^n - p^{i-1}).$$

D'autre part, chaque élément de G/H admet $\operatorname{Card} H = p^{l(H)}$ antécédents dans G, le nombre cherché est donc

$$\prod_{i=1}^{l}(p^{l(G)} - p^{l(H)+i-1}).$$

17.a. Il est clair que $H' \subset G' \cap H$.
Réciproquement, soit $g \in G' \cap H$. Puisque $g \in G'$, on peut écrire $g = h' + \sum_{i=1}^{l} n_i x_i$ où $h' \in H'$ et $n_i \in \mathbb{Z}$ pour $1 \leq i \leq l$. Soit π la surjection canonique de G sur G/H. Alors $\pi(g) = 0$ car $g \in H$. Comme $H' \subset H$, on a aussi $\pi(h') = 0$, et par suite $\sum_{i=1}^{l} n_i\pi(x_i) = 0$, et $\sum_{i=1}^{l} \bar{n}_i\pi(x_i) = 0$ dans le $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel G/H. Par hypothèse, la famille $(\pi(x_1), \ldots, \pi(x_l))$ est libre dans cet espace vectoriel, donc tous les $\bar{n}_i$ sont nuls. Tous les n_i sont donc des multiples de p, et comme G est élémentaire, $\sum_{i=1}^{l} n_i x_i = 0$. Ainsi, $g = h' \in H'$. Donc $G' \cap H = H'$.

D'autre part, considérons π' la surjection canonique de G' sur G'/H', et posons $x'_i = \pi'(x_i)$ $(1 \leq i \leq l)$.
Puisque G/H' est élémentaire (quotient de groupe élémentaire), il en est de même de G'/H' qui en est un sous-groupe et la question 15. permet de le voir comme un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$. Montrons que $(x'_1, \ldots, x'_l)$ en est une base.
Soit $g' \in G'$. g' s'écrit $g' = h' + \sum_{i=1}^{l} n_i x_i$ où $h' \in H'$ et $n_i \in \mathbb{Z}$ pour $1 \leq i \leq l$.
Donc :

$$\pi'(g') = \pi'(h') + \sum_{i=1}^{l} n_i \pi'(x_i) = \sum_{i=1}^{l} n_i x'_i = \sum_{i=1}^{l} \bar{n_i} x'_i \ ,$$

ce qui prouve que la famille est génératrice.
Supposons maitenant que $\sum_{i=1}^{l} \bar{n_i} x'_i = 0$ dans G'/H'. On a donc $\sum_{i=1}^{l} n_i x'_i = 0$ dans G'/H', i.e $\sum_{i=1}^{l} n_i x_i \in H'$. Comme $H' \subset H$, on a $\pi(\sum_{i=1}^{l} n_i x_i) = 0$, puis $\sum_{i=1}^{l} \bar{n_i} \pi(x_i) = 0$ dans G/H. On en déduit comme plus haut que les $\bar{n_i}$ sont nuls, et la famille $(x'_1, \ldots, x'_l)$ est libre.
La dimension de G'/H' est donc l, et son cardinal est p^l. Ce cardinal est par ailleurs $p^{l(G'/H')}$, il en résulte que $l(G'/H') = l$.
On a montré que G' vérifie bien la condition (C).

17.b. On conserve les notations π et π' de la question précédente.
Supposons que G' vérifie la condition (C). De $l(G'/H') = l$, on déduit que G'/H' est de dimension l sur $\mathbb{Z}/p\mathbb{Z}$. Considérons-en une base $(x'_1, \ldots, x'_l)$, puis une famille $(x_1, \ldots, x_l)$ d'éléments de G' telle que pour tout i, $\pi'(x_i) = x'_i$.
On montre que la famille $(x_1, \ldots, x_l)$ est libre modulo H : si $\sum_{i=1}^{l} \bar{n_i} \pi(x_i) = 0$, cela signifie que $\sum_{i=1}^{l} n_i x_i \in H$. Comme par ailleurs $\sum_{i=1}^{l} n_i x_i \in G'$, on a $\sum_{i=1}^{l} n_i x_i \in H' = G' \cap H$. Donc $\pi'(\sum_{i=1}^{l} n_i x_i) = 0$, et $\sum_{i=1}^{l} \bar{n_i} x'_i = 0$ et tous les $\bar{n_i}$ sont nuls du fait de l'indépendance de la famille $(x'_1, \ldots, x'_l)$, ce que nous voulions.

Montrons ensuite que G' est engendré par H' et cette famille :
si $g' \in G'$, on peut écrire $\pi'(g') = \sum_{i=1}^{l} \bar{n_i} x'_i$ car la famille $(x'_1, \ldots, x'_l)$ engendre G'/H'. cela signifie que $\pi'(g' - \sum_{i=1}^{l} n_i x_i) = 0$, donc que $g' - \sum_{i=1}^{l} n_i x_i \in H'$, et le résultat en découle.

17.c. D'après les deux questions qui précèdent, se donner un sous-groupe G' de G vérifiant la condition (C), c'est exactement se donner une famille $(x_1, \ldots, x_l)$ d'éléments de G, libre modulo H.
Depuis 16., on sait que le nombre de telles familles est $\prod_{i=1}^{l} \left(p^{l(G)} - p^{l(H)+i-1}\right)$.
Cherchons à quelles conditions deux telles familles donnent naissance au même sous-groupe G'. Supposons donc que $(x_1, \ldots, x_l)$ et $(y_1, \ldots, y_l)$ sont deux familles libres modulo H donnant naissance aux sous-groupes G'_1 et G'_2 qui vérifient (C). Soit F_1 le sous-espace vectoriel de G/H' engendré par la famille $(\pi''(x_1), \ldots, \pi''(x_l))$ et F_2 celui engendré par $(\pi''(y_1), \ldots, \pi''(y_l))$ (ici, π'' désigne la surjection canonique de G sur G/H').
Si $G_1 = G_2$, alors pour tout j, $x_j \in G_2$ et x_j s'écrit $x_j = h' + \sum_{i=1}^{l} n_i y_i$ où $h' \in H'$ et $n_i \in \mathbb{Z}$. D'où $\pi''(x_j) = \sum_{i=1}^{l} \bar{n_i} \pi''(y_i)$, ce qui prouve que $F_1 \subset F_2$. On a de même $F_2 \subset F_1$, et $F_1 = F_2$.
Réciproquement, si $F_2 = F_1$, alors pour tout j de $\{1, \ldots, l\}$, $\pi''(x_j)$ s'écrit $\pi''(x_j) = \sum_{i=1}^{l} \bar{n_i} \pi''(y_i)$ et ainsi $\left(x_j - \sum_{i=1}^{l} n_i y_i\right) \in H'$, ce qui prouve que $x_j \in G'_2$, donc que $G'_1 \subset G'_2$, et par symétrie on a $G'_2 \subset G'_1$, puis $G'_1 = G'_2$.

Donc deux familles libres modulo H engendrent avec H' le même sous-groupe G' vérifiant (C) si et seulement si leurs images dans G/H' engendrent le même sous-espace vectoriel. En définitive, comme ces images sont évidemment libres dans G/H' (car $H' \subset H$), deux familles libres modulo H engendrent avec H' le même sous-groupe G' vérifiant (C) si et seulement si leurs images dans G/H' sont deux bases d'un même sous-espace vectoriel de dimension l. D'après un calcul déjà effectué au 6.a., il y a $(p^l-1)\dots(p^l-p^{l-1})$ bases pour un tel sous-espace. D'autre part une telle base provient via π'' d'exactement $(\operatorname{Card} H')^l$ familles d'éléments de G. Donc, le nombre de familles d'éléments de G qui donnent naissance au même sous-groupe G' est :

$$p^{l(H')\times l}\,(p^l-1)\dots(p^l-p^{l-1}).$$

Finalement, le nombre cherché est :

$$N=\frac{\prod_{i=1}^{l}\big(p^{l(G)}-p^{l(H)+i-1}\big)}{p^{l(H')\times l}\prod_{i=1}^{l}(p^l-p^{i-1})}.$$

Or, on a

$$\prod_{i=1}^{l}\big(p^{l(G)}-p^{l(H)+i-1}\big)=p^{l(H')\times l}\prod_{i=1}^{l}\big(p^{l(G)-l(H')}-p^{l(H)-l(H')+i-1}\big).$$

Dautre part,

$$\prod_{i=1}^{l}\big(p^{l(G)-l(H')}-p^{l(H)-l(H')+i-1}\big)=p^{l[l(H)-l(H')]}\prod_{i=1}^{l}p^{i-1}\big(p^{l(G)-l(H)-i+1}-1\big)$$

et

$$\prod_{i=1}^{l}(p^l-p^{i-1})=\prod_{i=1}^{l}p^{i-1}\big(p^{l-i+1}-1\big).$$

Il vient donc :

$$N=p^{l[l(H)-l(H')]}\times F_{l(G)-l(H),l}(p).$$

Ceci est une fonction polynomiale de p d'après 5.b. (le polynôme est même à coefficients entiers).

Partie 5. Précisions sur $g^{\rho}_{\lambda\mu}(p)$

18.a. On sait d'après le 7.c. que $\big(p^iG\big)/H_i\simeq p^i\big(G/H\big)$. En particulier, on a :

$$l\Big(p^i\big(G/H\big)\Big)=l\Big(\big(p^iG\big)/H_i\Big)=l\Big(p^iG\Big)-l\Big(H_i\Big)\ ,$$

et

$$l\Big(H_i\Big)=l\Big(p^iG\Big)-l\Big(p^i\big(G/H_i\big)\Big).$$

D'autre part, d'après 12., on sait que pour tout $j>i$, $l\big(p^{j-1}G\big)-l\big(p^jG\big)=\rho'_j$. Comme à partir d'un certain rang $p^jG=\{0\}$, on a

$$\sum_{j>i}\rho'_j=\sum_{j>i}l\big(p^{j-1}G\big)-l\big(p^jG\big)=l\big(p^iG\big).$$

Le type de G/H est α, donc de la même façon,

$$\sum_{j>i} \alpha'_j = l\big(p^i(G/H)\big).$$

On a donc bien

$$l(H_i) = \sum_{j>i} \big(\rho'_j - \alpha'_j\big).$$

18.b. Si K est de cotype β dans G, alors pour tout i, $l(K_i) = \sum_{j>i}\big(\rho'_j - \beta'_j\big)$ d'après a., et on a bien

$$l(K_{i-1}) - l(K_i) = \rho'_i - \beta'_i.$$

Réciproquement, supposons que pour tout i, $l(K_{i-1}) - l(K_i) = \rho'_i - \beta'_i$. Si γ est le cotype de K, on a d'après la partie directe $l(K_{i-1}) - l(K_i) = \rho'_i - \gamma'_i$. Il en résulte que pour tout i, $\gamma'_i = \beta'_i$, donc que $\gamma' = \beta'$, puis $\gamma = \beta$.

18.c. Montrons que l'application $K \mapsto \big(K_i = K \cap p^i G\big)_{i\geq 0}$ réalise une bijection de l'ensemble des sous-groupes de G contenus dans H et de cotype β dans G et l'ensemble $\mathcal{L}$ des chaînes décroissantes $(L_i)_{i\geq 1}$ de sous-groupes de H vérifiant pour $i \geq 1$:

$$L_{i-1} \cap H_i = L_i \quad \text{et} \quad l(L_{i-1}/L_i) = \rho'_i - \beta'_i.$$

Cette application est bien définie : si $K \subset H$ est de cotype β dans G, alors pour $i \geq 1$:

$$K_{i-1} \cap H_i = \big(K \cap H_{i-1}\big) \cap H_i = K \cap H_i = K_i$$

et $l(K_{i-1}/K_i) = \rho'_i - \beta'_i$ d'après a.(condition nécessaire).
Elle est injective car $K = K_0$.
Enfin, elle est surjective car si une chaîne (L_i) vérifie les conditions imposées, alors en posant $K = L_0$, K est un antécédent de (L_i) toujours grâce à a.(condition suffisante).
Le nombre cherché est donc Card $\mathcal{L}$.

Mais, pour tout $i \in \mathbb{N}^*$:

$$\begin{aligned} l(H) - l(H_i) &= \textstyle\sum_{k=1}^{i} \big(l(H_{k-1}) - l(H_k)\big) \\ &= \textstyle\sum_{k=1}^{i} \Big(\sum_{j>k-1}(\rho'_j - \alpha'_j) - \sum_{j>k}(\rho'_j - \alpha'_j)\Big) \\ &= \textstyle\sum_{k=1}^{i} (\rho'_k - \alpha'_k). \end{aligned}$$

Or $\alpha \subset \beta \subset \rho$ donc $\alpha' \subset \beta' \subset \rho'$, donc pour tout k, $\alpha'_k \leq \beta'_k \leq \rho'_k$.
En particulier, $\sum_{k=1}^{i}(\rho'_k - \alpha'_k) \geq \rho'_i - \beta'_i$, donc $l(H) - l(H_i) \geq \rho'_i - \beta'_i$ si K est de cotype β. Donc, puisque H est élémentaire, on peut appliquer 17.*c.* pour affirmer que si $L_i \subset H_i$ est donné, le nombre des sous-groupes L_{i-1} de H vérifiant

$$L_{i-1} \cap H_i = L_i \quad \text{et} \quad l(L_{i-1}/L_i) = \rho'_i - \beta'_i$$

est polynomial en p (le polynôme ne dépend que de α, β, ρ et i). D'autre part, si $i \geq \rho_1$, $p^i G = \{0\}$. Il en résulte immédiatement que si $(L_i)_{i\geq 1}$ appartient à $\mathcal{L}$, alors L_i est nul dès que $i \geq \rho_1$.
Pour compter le nombre de chaînes : on a un seul choix pour L_{ρ_1} et au-delà, et

si $L_i, \ldots, L_{\rho_1}$ sont fixés, le nombre de façons de choisir L_{i-1} est polynomial, et donc le nombre final cherché est un produit fini de polynômes en p (le processus s'arrête quand on atteint L_0). On obtient ainsi un polynôme en p qui ne dépend que de α, β, et ρ.

19. La première formule est immédiate : elle résulte du fait que l'ensemble des sous-groupes K de G de cotype α tels que $pK \subset L \subset H \subset K$ est l'union disjointe, lorsque T décrit les sous-groupes de L des ensembles des sous-groupes K de G de cotype α tels que $pK = T \subset H \subset K$.
Lorsque H est élémentaire, on peut considérer H comme un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel et ses sous-groupes comme des sous-espaces vectoriels : la seconde formule découle alors de 6.d.
Lorsque H est quelconque, on le "rend " élémentaire en quotientant G par pH. Plus précisément, soit π la surjection canonique de G sur G/pH. Il est clair que $\pi(H) = H/pH$ est un sous-groupe élémentaire de G/pH. D'autre part, π induit une bijection croissante au sens de l'inclusion entre les sous-groupes de G qui contiennent pH et les sous-groupes de G/pH. Soit L un sous-groupe de H. Soit K un sous-groupe de cotype α dans G tel que $pK \subset L \subset H \subset K$ (notons que pour qu'un tel sous-groupe K existe, il est nécessaire que $pH \subset L$ car $pH \subset pK$ puisque $H \subset K$). Alors le cotype de K/pH dans G/pH ne dépend que de α : nommons-le α_1. On a, par croissance de π :

$$\pi(pK) = p\pi(K) \subset \pi(L) \subset \pi(H) \subset \pi(K).$$

Réciproquement, si K' est un sous-groupe de G/pH de cotype α_1 tel que $pK' \subset \pi(L) \subset \pi(H) \subset K'$, alors $\pi^{-1}(K')$ est un sous-groupe de cotype α de G qui vérifie $pK \subset L \subset H \subset K$.
On a donc : $f(H, L) = f_1(\pi(H), \pi(L))$ et de même $g(H, L) = g_1(\pi(H), \pi(L))$ où $f_1(\pi(H), \pi(L))$ est le nombre de sous-groupes K' de G/pH de cotype α_1 tel que $pK' \subset \pi(L) \subset \pi(H) \subset K'$ et $g_1(\pi(H), \pi(L))$ le nombre de sous-groupes K' de G/pH de cotype α_1 tel que $pK' = \pi(L) \subset \pi(H) \subset K'$. Comme $\pi(H)$ est élémentaire, il vient

$$g_1(\pi(H), \pi(L)) = \sum_{T' \subset \pi(L)} (-1)^m p^{\frac{m(m-1)}{2}} f_1(\pi(H), T').$$

Dans cette formule, $m = l(\pi(L)/T') = l(L/T)$ où $T = \pi^{-1}(T')$. Le résultat en découle.

20.a. Soit $\overline{S}$ le socle de G/L. Considérons S_1 l'image réciproque de $\overline{S}$ par la surjection canonique π de G sur G/L. Alors $S_1/L = \overline{S}$ est le socle de G/L.
Si $S = S_1 + L$, on a également $\pi(S) = \overline{S}$ car $\pi(L) = 0$. D'autre part, puisque H est élémentaire, on a pour $h \in H$:

$$p\pi(h) = \pi(ph) = \pi(0) = 0.$$

Donc $\pi(h) \in \overline{S} = \pi(S_1)$ donc $h \in S_1 + L$ et S contient H.

20.b. On a : $K/H \subset S/H \iff K + H \subset S + H \iff K \subset S + H$.
Supposons que $K/H \subset S/H$, et considérons $k \in K$. On écrit $k = s + h$ où $s \in S$ et $h \in H$. Comme H est élémentaire, $pk = ps$. On a, avec les notations précédentes : $\pi(pk) = p\pi(s) = 0$ car $\pi(s) \in \overline{S}$. Ainsi, $pk \in L$ et $pK \subset L$.

Réciproquement, supposons que $pK \subset L$. Soit $k \in K$, alors $pk \in L$, donc $\pi(pk) = p\pi(k) = 0$ et $\pi(k) \in \overline{S} = \pi(S)$. Ainsi, $k \in S+L \subset S+H$ et $K \subset S+H$, ce que nous voulions.
Appelons $\mathcal{F}(H, L)$ l'ensemble des sous-groupes K de cotype α dans G tels que $pK \subset L \subset H \subset K$. Alors, d'après ce qui précède :

$$\begin{array}{rcl} K \in \mathcal{F}(H,L) & \iff & K \text{ est de cotype } \alpha \text{ dans } G \text{ et } K \subset S+H \\ & \iff & K \text{ est de cotype } \alpha \text{ dans } G \text{ et } K \subset S \text{ (car } H \subset S). \end{array}$$

Comme S est élémentaire, on peut appliquer le 18.c. avec $H = S$ pour évaluer le nombre de K vérifiant cette dernière propriété. Le cotype de S dans G est d'après 8.c. le cotype de S/L dans G/L. Le type de G/L est γ ; le cotype de S/L dans G/L est donc $\tilde{\gamma}$ d'après 14. car S/L est le socle de G/L.
On a donc $f(H, L) = \operatorname{Card} \mathcal{F}(H, L) = h_{\tilde{\gamma}\alpha\beta}(p)$.

20.c. Il est clair que le nombre cherché est

$$g(H, H) = \sum_{T \subset H} (-1)^m p^{\frac{m(m-1)}{2}} f(H, T).$$

D'après b., si $T \subset H$ est de cotype γ, alors $f(H, T) = h_{\tilde{\gamma}\alpha\beta}(p)$: c'est donc d'après 18.c. un polynôme en p à coefficients entiers, et il en est alors de même de $g(H, H)$.

21. Soit $(\rho^{(0)}, \ldots, \rho^{(r)})$ une RL-suite telle que $\rho^{(0)} = \mu$ et $\rho^{(r)} = \rho$: elle est obtenue à partir d'un groupe G de type ρ et d'un sous-groupe H de G de type λ et de cotype μ. On a les inclusions évidentes :

$$\{0\} = p^r H \subset p^{r-1} H \subset \ldots \subset H.$$

De plus, les inclusions précédentes sont strictes : supposons qu'il existe i dans $\{0, \ldots, r-1\}$ tel que $p^i H = p^{i+1} H$. On a $i \leq r-2$ par définition de r. Alors $p^{i+1} H = p^{i+2} H$. En effet, si $x \in p^{i+1} H$, on peut écrire $x = p^{i+1} y = p\, p^i y$. Alors $p^i y \in p^i H = p^{i+1} H$, donc $p^i y$ s'écrit $p^i y = p^{i+1} z$ et finalement $x = p^{i+2} z \in p^{i+2} H$. On montre alors facilement que pour $j \geq i$, $p^j H = p^i H$, et ceci entre en contradiction avec la définition de r.
On a donc en particulier pour $i \in \{0, \ldots, r-1\}$: $\operatorname{Card} p^{i+1} H < \operatorname{Card} p^i H$, et par voie de conséquence $l(p^{i+1} H) < l(p^i H)$, i.e $l(p^{i+1} H) + 1 \leq l(p^i H)$. On en déduit alors que

$$l(H) \geq l(p^r H) + r.$$

Donc $r \leq l(\lambda)$. Mais comme $\operatorname{Card} G = \operatorname{Card} H \operatorname{Card} G/H$, on a $l(\rho) = l(\lambda) + l(\mu)$ et on en déduit que $r \leq l(\rho) - l(\mu)$.
D'autre part, on note que $\rho^{(i)} \subset \rho^{(i+1)}$ pour $i \in \{0, \ldots, r-1\}$: en effet, d'après la question 8.c., le cotype de $p^i H$ dans G est le cotype de $p^i H / p^{i+1} H$ dans $G/p^{i+1} H$ et d'après la question 13., ce cotype est contenu dans le type de $G/p^{i+1} H$, qui est $\rho^{(i+1)}$ par définition.
L'entier r ne peut donc prendre qu'un nombre fini de valeurs, et lorsque r est fixé, il est clair qu'il n'y a qu'un nombre fini de partitions $\rho_1, \ldots, \rho_{r-1}$ telles que

$$\mu \subset \rho_1 \subset \ldots \subset \rho_{r-1} \subset \rho.$$

L'ensemble des RL-suites $(\rho^{(0)}, \ldots, \rho^{(r)})$ telles que $\rho^{(0)} = \mu$ et $\rho^{(r)} = \rho$ est bien fini.

22.a. Notons $\mathcal{A}$ l'ensemble des RL-suites $(\rho^{(0)}, \ldots, \rho^{(r)})$ telles que $\rho^{(0)} = \mu$ et $\rho^{(r)} = \rho$. Pour U dans $\mathcal{A}$, il y a $g_U(p)$ sous-groupes H de G de type λ et de cotype μ tel que $U(H) = U$. De plus, si H est un sous-groupe de G de type λ et de cotype μ , alors il est clair que $U(H) \in \mathcal{A}$. On obtient donc :

$$g^{\rho}_{\lambda\mu}(p) = \sum_{U \in \mathcal{A}} g_U(p).$$

Si chaque g_U est polynomiale, il en sera donc de même de $g^{\rho}_{\lambda\mu}(p)$.

22.b. On a tout de suite pour tout i, $p^i H' = p^{i+1} H$. Il en résulte immédiatement que

$$U(H') = (\rho^{(1)}, \ldots, \rho^{(r)}).$$

22.c. Suivons l'indication de l'énoncé et considérons π la surjection canonique de G sur G/pH'. On sait que π induit une bijection entre les sous-groupes de G qui contiennent pH' et les sous-groupes de G/pH'. Notons $\mathcal{U}$ l'ensemble des sous-groupes H de G tels que $U(H) = U$ et $pH = H'$. Notons que si $H \in \mathcal{U}$, alors $pH' = p^2 H \subset H$ et la restriction de π à $\mathcal{U}$ est une bijection entre $\mathcal{U}$ et $\pi(\mathcal{U})$.
Soit $H \in \mathcal{U}$ et soit $K' = \pi(H) = H/pH'$. Le cotype de K' dans G/pH' est (cf 8.c.) celui de H dans G, soit $\rho^{(0)}$. On a $pK' = \pi(pH) = \pi(H') = H'/pH'$.
Réciproquement, si K' est un sous-groupe de G/pH' de cotype $\rho^{(0)}$ tel que $pK' = H'/pH'$, alors $\pi^{-1}(K') \in \mathcal{U}$: en effet soit $H = \pi^{-1}(K')$. Le cotype de H dans G est celui de $\pi(H) = K'$ dans G/pH', i.e $\rho^{(0)}$. De plus, on a $\pi(pH) = pK' = \pi(H')$, donc $pH = H'$ (ce sont deux sous-groupes de G qui contiennent pH' et qui ont même image par π). Ceci entraîne évidemment que $U(H) = U$.
$\mathcal{U}$ est ainsi en bijection avec l'ensemble des sous-groupes K' de G/pH' de cotype $\rho^{(0)}$ tels que $pK' = H'/pH'$. Or H'/pH' est élémentaire de cotype le cotype de H' dans G, soit $\rho^{(1)}$ et G/pH' est un groupe de type $\rho^{(2)}$ puisque $U(H') = U'$. D'après 19.c., le nombre de sous-groupes K' de G/pH' de cotype $\rho^{(0)}$ tels que $pK' = H'/pH'$ est précisément $F_{\rho^{(0)}\rho^{(1)}\rho^{(2)}}(p)$: c'est donc le cardinal de $\mathcal{U}$.
Il y a $g_{U'}(p)$ sous-groupes de G tels que $U(H') = U'$. Pour chacun de ces H', on peut trouver $\mathrm{Card}\,\mathcal{U}$ sous-groupes H de G tels que $U(H) = U$ et $pH = H'$. De plus, si $U(H) = U$ alors $U(pH) = U'$. Il vient donc

$$g_U(p) = F_{\rho^{(0)}\rho^{(1)}\rho^{(2)}}(p)\, g_{U'}(p).$$

22.d. En itérant la méthode précédente, on obtient pour $r \geq 2$:

$$g_U(p) = F_{\rho^{(0)}\rho^{(1)}\rho^{(2)}}(p) F_{\rho^{(1)}\rho^{(2)}\rho^{(3)}}(p) \ldots F_{\rho^{(r-2)}\rho^{(r-1)}\rho^{(r)}}(p)\, g_V(p)$$

où $V = (\rho^{(r-1)}, \rho^{(r)})$. $g_V(p)$ est ainsi le nombre de sous-groupes H de G de cotype $\rho^{(r-1)}$ tels que $pH = \{0\}$, donc le nombre de sous-groupes élémentaires de G de cotype $\rho^{(r-1)}$ de G, donc le nombre de sous-groupes élémentaires de G contenus dans le socle de G (qui est élémentaire) de cotype $\rho^{(r-1)}$ dans G : d'après 18.c., ce nombre est une fonction polynomiale de p, et il en est de même de $g_U(p)$. Pour $r = 1$, $g_U(p)$ est le nombre de sous-groupes H de G tels que $U(H) = (\rho^{(0)}, \rho^{(1)})$ et on vient de voir que c'est un polynôme en p.
D'où le résultat.

8.3 Commentaires

Dénombrer : tel est le thème majeur du sujet de 1996. La première partie est assez facile, bien que déroutante. Les parties suivantes mélangent avec un certain bonheur groupes commutatifs finis et espaces vectoriels de dimension finie sur un corps fini. A ce sujet, les questions 6.a. et 6.b. sont des calculs classiques que tout candidat sérieux se doit de maîtriser. De même, il faut savoir résoudre la question 11., qui concerne des faits classiques sur les caractères des groupes commutatifs finis.

Une certaine familiarité avec les quotients de groupes est indispensable pour être à l'aise tout au long du sujet, notamment le fait capital que les sous-groupes de G/H sont en bijection via la surjection canonique avec les sous-groupes de G qui contiennent H. La plupart des questions sont abordables, mais certaines sont véritablement ardues du point de vue combinatoire, et il faut de la persévérance, voire de l'entêtement pour arriver au bout !

Bref, voilà un sujet assez long et pas toujours très facile qui testera à fond vos qualités de dénombreur, ainsi que votre volonté. Bon courage !

Chapitre 9

Session de 1997

9.1 Sujet

9.2 Correction

I. Fonctions polynômes à valeurs entières.

1. On va démontrer le résultat demandé par récurrence sur $p \in \mathbb{N}^*$:
Si $p = 1$ il s'agit juste de la définition de ∂f.
Considérons $p > 1$ et supposons que pour tout $n \in \mathbb{Z}$ on ait :

$$\partial^{p-1} f(n) = \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} f(n-k).$$

Alors pour tout $n \in \mathbb{Z}$ on a :

$$\begin{aligned}
\partial^p f(n) &= \partial(\partial^{p-1} f)(n) \\
&= \partial^{p-1} f(n) - \partial^{p-1} f(n-1) \\
&= \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} f(n-k) - \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} f(n-1-k) \\
&= \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} f(n-k) - \sum_{k'=1}^{p} (-1)^{k'-1} \binom{p-1}{k'-1} f(n-k') \\
&= \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} f(n-k) + \sum_{k=1}^{p} (-1)^k \binom{p-1}{k-1} f(n-k) \\
&= f(n) + \sum_{k=1}^{p-1} (-1)^k [\binom{p-1}{k} + \binom{p-1}{k-1}] + (-1)^p f(n-p).
\end{aligned}$$

Comme $\binom{p-1}{k} + \binom{p-1}{k-1} = \binom{p}{k}$ on obtient :

$$\partial^p f(n) = \sum_{k=0}^{p} (-1)^k \binom{p}{k} f(n-k).$$

Ceci achève la récurrence.

2.a.
$\mathcal{P}$ est un sous-ensemble non vide (prendre 0) de l'anneau $\mathbb{Q}[T]$; pour montrer qu'il en est un sous-anneau, il suffit de montrer qu'il est stable par addition, passage à l'opposé, multiplication. Comme $\mathbb{Z}$ est lui-même un sous-anneau de $\mathbb{Q}$, cela résulte immédiatement de la définition des opérations dans $\mathcal{P}$.

2.b. Il est évident que l'application en question est un homomorphisme d'anneaux (ceci est une conséquence évidente des structures d'anneaux de $\mathcal{P}$ et $\mathcal{F}(\mathbb{Z}, \mathbb{Z})$). Pour montrer qu'il s'agit d'un homomorphisme injectif, il suffit de considérer $P \in \mathcal{P}$ tel que pour tout $n \in \mathbb{Z}$, $P(n) = 0$ et de montrer qu'alors $P = 0$: ceci est vrai car un polynôme non nul n'admet qu'un nombre fini de racines.

3.a. Fixons $k > 0$ (pour P_0 il n' y a pas de problème).
Si $n \in [0, k-1]$, il est clair que $P_k(n) = 0$ donc $P_k(n) \in \mathbb{Z}$.

Si $n \geq k$, $P_k(n) = \dfrac{n(n-1)\dots(n-k+1)}{k!} = \dfrac{n!}{k!(n-k)!} = \binom{n}{k}$. En particulier $P_k(n) \in \mathbb{Z}$.
On montre de même que si $n \leq -1$, on a $P_k(n) = (-1)^k \binom{k-(n+1)}{k}$ et donc à nouveau $P_k(n) \in \mathbb{Z}$.

3.b. D'abord on a par définition pour tout $k \in \mathbb{N}$, $\partial^0 f_k = f_k$.
Ensuite fixons $k > 0$.

$$\begin{aligned}
\partial P_k(T) &= P_k(T) - P_k(T-1) \\
&= \frac{T(T-1)\dots(T-k+1)}{k!} - \frac{(T-1)(T-2)\dots(T-k)}{k!} \\
&= \frac{(T-1)\dots(T-k+1)}{k!}[T-(T-k)] \\
&= \frac{(T-1)\dots(T-k+1)}{(k-1)!} \\
&= P_{k-1}(T-1) \\
&= P_{k-1}(T) - [P_{k-1}(T) - P_{k-1}(T-1)] \\
&= P_{k-1}(T) - \partial P_{k-1}(T).
\end{aligned}$$

Donc pour tout $k > 0$, on a : $\partial f_k = f_{k-1} - \partial f_{k-1}$.
A l'aide de cette formule on va démontrer par récurrence sur $k \in \mathbb{N}$ que :

$$\partial f_k = \sum_{j=0}^{k-1} (-1)^{(k-1-j)} f_j.$$

(Par définition une somme sur un ensemble vide d'indices est nulle).
Il est bien évident que $\partial f_0 = 0$, ce qui prouve la formule pour $k = 0$.
Fixons $k > 0$ et supposons que : $\partial f_{k-1} = \sum_{j=0}^{k-2} (-1)^{(k-2-j)} f_j$.
Alors on a :

$$\begin{aligned}
\partial f_k &= f_{k-1} - \partial f_{k-1} \\
&= f_{k-1} - \sum_{j=0}^{k-2} (-1)^{(k-2-j)} f_j \\
&= f_{k-1} + \sum_{j=0}^{k-2} (-1)^{(k-1-j)} f_j \\
&= \sum_{j=0}^{k-1} (-1)^{(k-1-j)} f_j.
\end{aligned}$$

Ceci achève la récurrence.
Cette nouvelle formule nous permet de démontrer par récurrence sur $p \in \mathbb{N}^*$ que pour tout $k \in \mathbb{N}$:

$$\partial^p f_k = \sum_{l=0}^{k-p} (-1)^{p+k+l} \binom{k-1-l}{p-1} f_l.$$

(Par convention $\binom{n}{m} = 0$ si $m > n$.)
Pour $p = 1$ cette formule s'écrit :

$$\begin{aligned}\partial f_k &= \sum_{l=0}^{k-1}(-1)^{k+l+1}f_l \\ &= \sum_{l=0}^{k-1}(-1)^{k-l-1}f_l.\end{aligned}$$

C'est justement la formule précédemment démontrée.
Fixons maintenant $p > 1$ et supposons que :

$$\partial^{p-1}f_k = \sum_{l=0}^{k-p+1}(-1)^{p-1+k+l}\binom{k-1-l}{p-2}f_l.$$

Alors on a :

$$\begin{aligned}\partial^p f_k &= \partial(\partial^p f_k) \\ &= \partial(\sum_{l=0}^{k-p+1}(-1)^{p-1+k+l}\binom{k-1-l}{p-2}f_l) \\ &= \sum_{l=0}^{k-p+1}(-1)^{p-1+k+l}\binom{k-1-l}{p-2}\partial f_l \text{ (∂ est linéaire.)} \\ &= \sum_{l=0}^{k-p+1}(-1)^{p-1+k+l}\binom{k-1-l}{p-2}[\sum_{j=0}^{l-1}(-1)^{l-1-j}f_j] \\ &= \sum_{l=0}^{k-p+1}\sum_{j=0}^{l-1}(-1)^{p-1+k+l+l-1-j}\binom{k-1-l}{p-2}f_j \\ &= \sum_{l=0}^{k-p+1}\sum_{j=0}^{l-1}(-1)^{p+k+j}\binom{k-1-l}{p-2}f_j \\ &= \sum_{j=0}^{k-p}(-1)^{p+k+j}[\sum_{l=j+1}^{k-p+1}\binom{k-1-l}{p-2}]f_j \\ &= \sum_{j=0}^{k-p}(-1)^{p+k+j}[\sum_{l'=p-2}^{k-j-2}\binom{l'}{p-2}]f_j \\ &= \sum_{j=0}^{k-p}(-1)^{p+k+j}\binom{k-j-1}{p-1}f_j.\end{aligned}$$

On a utilisé pour finir la formule combinatoire suivante : $\sum_{q=n}^{m}\binom{q}{n} = \binom{m+1}{n+1}$.
Ceci termine cette récurrence et donc la démonstration de la formule générale annoncée. En particulier on note que $p > k$ implique $\partial^p f_k = 0$.

4.a. Si $f \in \mathcal{F}(\mathbb{Z},\mathbb{Z})$ provient du polynôme P, il est clair que ∂f provient du polynôme ∂P. Il est alors évident que $\partial f \in \mathcal{P}$, lorsque $f \in \mathcal{P}$. De plus pour tout $k \in \mathbb{N}$ on a :

$$\begin{aligned}\partial(T^k) &= T^k - (T-1)^k \\ &= T^k - \sum_{j=0}^{k}\binom{k}{j}(-1)^{k-j}T^j \\ &= \sum_{j=0}^{k-1}\binom{k}{j}(-1)^{k-j+1}T^j.\end{aligned}$$

En particulier $\deg(\partial(T^k)) = k-1$ ou $\partial(T^k) = 0$ si $k = 0$. On en déduit immédiatement que pour tout $P \in \mathbb{Q}[T]$ on a $\deg(\partial P) = \deg P - 1$, ou $\partial P = 0$ si $\deg P = 0$. Il est alors évident que $\deg(\partial f) = \deg f - 1$, ou $\partial f = 0$ si $\deg f = 0$.

4.b. Une récurrence évidente à partir du a. prouve que pour tout $f \in \mathcal{P}$ on a $\partial^{\deg f+1} f = 0$. Posons $p = \text{degf} + 1$: on a $\partial^p f = 0$ donc pour tout $n \in \mathbb{Z}$, $\partial^p f(n) = 0$. D'après 1. cela s'écrit exactement :

$$\text{Pour tout } n \in \mathbb{Z},\ \sum_{k=0}^{p} (-1)^k \binom{p}{k} f(n-k) = 0.$$

4.c. Puisque pour tout $k \in \mathbb{N}$, $\deg P_k = k$, la famille $\{P_k\}_{k\in\mathbb{N}}$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[T]$. Soit maintenant $P \in \mathbb{Q}[T]$ tel que $f = f_P$ et soit $p = \deg P$. Il existe $(a_0, \ldots, a_p) \in \mathbb{Q}^{p+1}$ tel que $P = \sum_{k=0}^{p} a_k P_k$. Il est alors clair que $f = \sum_{k=0}^{p} a_k f_k$. Supposons que l'on n'ait pas $(a_0, \ldots, a_p) \in \mathbb{Z}^{p+1}$ et considérons alors $k_0 = \max\{k \in [0, p] \text{ tel que } a_k \notin \mathbb{Z}\}$. Alors il est clair que $\sum_{k=k_0+1}^{p} a_k f_k \in \mathcal{P}$ d'après 3.a., donc que $\sum_{k=0}^{k_0} a_k f_k \in \mathcal{P}$. D'après a. (et une récurrence évidente) cela prouve que $\partial^{k_0}(\sum_{k=0}^{k_0} a_k f_k) \in \mathcal{P}$. Or en utilisant la conclusion mentionnée à la fin du 3.b. on obtient :

$$\partial^{k_0}(\sum_{k=0}^{k_0} a_k f_k) = \sum_{k=0}^{k_0} a_k \partial^{k_0}(f_k) = a_{k_0} f_0.$$

Donc en fait $a_{k_0} f_0 \in \mathcal{P}$ et $a_{k_0} \in \mathbb{Z}$. Ceci est absurde donc $(a_0, \ldots, a_p) \in \mathbb{Z}^{p+1}$: f admet bien une écriture de la forme demandée.
Supposons maintenant que $\sum_{k=0}^{p} n_k f_k = 0$. Alors d'après 2.b., $\sum_{k=0}^{p} n_k P_k = 0$ dans $\mathcal{P}$, donc à fortiori dans $\mathbb{Q}[T]$. Comme $\{P_k\}_{k\in\mathbb{N}}$ est une famille libre du $\mathbb{Q}$-ev $\mathbb{Q}[T]$, les n_k sont tous nuls : $\{f_k\}_{k\in\mathbb{N}}$ est une famille libre du $\mathbb{Z}$-module $\mathcal{P}$. Ceci prouve qu'une écriture sous la forme $f = \sum_{k=0}^{p} n_k f_k$ est nécessairement unique.

4.d. On sait déjà depuis le a. que si $f \in \mathcal{P}$ alors $\partial f \in \mathcal{P}$.
Réciproquement considérons $f \in \mathcal{F}(\mathbb{Z}, \mathbb{Z})$ telle que $\partial f \in \mathcal{P}$. D'après c. il existe $(n_0, \ldots, n_p) \in \mathbb{Z}^{p+1}$ tel que $\partial f = \sum_{k=0}^{p} n_k f_k$. On a démontré au 3.b. que $f_k = \partial f_k + \partial f_{k+1}$ donc on a :

$$\partial f = \sum_{k=0}^{p} n_k(\partial f_k + \partial f_{k+1}) = \partial(\sum_{k=0}^{p} n_k(f_k + f_{k+1})).$$

On en déduit que :

$$\partial(f - \sum_{k=0}^{p} n_k(f_k + f_{k+1})) = 0.$$

Ceci prouve qu'il existe $m_0 \in \mathbb{Z}$ tel que pour tout $n \in \mathbb{Z}$ on ait :

$$f(n) - \sum_{k=0}^{p} n_k(f_k(n) + f_{k+1}(n)) = m_0.$$

Mais pour tout $n \in \mathbb{Z}$ on a $m_0 = m_0 f_0(n)$. Donc en fait :

$$f - \sum_{k=0}^{p} n_k(f_k + f_{k+1}) = m_0 f_0,$$

c'est-à-dire $f = m_0 f_0 + \sum_{k=0}^{p} n_k(f_k + f_{k+1})$. D'après 3.a. cela prouve que $f \in \mathcal{P}$, ce que nous voulions démontrer.

On a déjà démontré au b. que si $f \in \mathcal{P}$ alors il existe $p \in \mathbb{N}$ tel que $\partial^p f = 0$. Réciproquement supposons qu'il existe $p \in \mathbb{N}$ tel que $\partial^p f = 0$. En particulier $\partial^p f \in \mathcal{P}$. Comme on sait déjà que si $\partial g \in \mathcal{P}$ alors $g \in \mathcal{P}$, une récurrence finie triviale assure que $f \in \mathcal{P}$.

5. Il est évident que $\mathcal{P} \subset \mathcal{P}'$.
Appelons $\mathcal{F}(\mathbb{Z}, \mathbb{Q})$ l'ensemble des fonctions de $\mathbb{Z}$ dans $\mathbb{Q}$. L'opérateur ∂ est défini de la même manière sur $\mathcal{F}(\mathbb{Z}, \mathbb{Q})$. Si $f \in \mathcal{F}(\mathbb{Z}, \mathbb{Q})$ le résultat du 1. reste valide et on a pour tout $p \in \mathbb{N}^*$ et pour tout $n \in \mathbb{Z}$:

$$\partial^p f(n) = \sum_{k=0}^{p} (-1)^k \binom{p}{k} f(n-k).$$

D'autre part on montre comme au 4.a. que si $P \in \mathbb{Q}[T]$, $\partial^{\deg P+1} P = 0$. Soit $P \in \mathbb{Q}[T]$. On vient d'expliquer pourquoi il existe $p \in \mathbb{N}^*$ tel que pour tout $n \in \mathbb{Z}$ on ait :

$$\sum_{k=0}^{p} (-1)^k \binom{p}{k} P(n-k) = 0.$$

Supposons alors que $P \in \mathcal{P}'$ mais que $P \notin \mathcal{P}$. Puisque $P \in \mathcal{P}'$, il existe $n_0 \in \mathbb{Z}$ tel que pour tout $n \geq n_0$ on ait $P(n) \in \mathbb{Z}$. Donc $\{n \in \mathbb{Z},\ P(n) \notin \mathbb{Z}\}$ est majoré. De plus comme $P \notin \mathcal{P}$ cet ensemble n'est pas vide. Nous pouvons donc en considérer le plus grand élément, que nous notons n_1. Spécialisons la relation $\sum_{k=0}^{p} (-1)^k \binom{p}{k} P(n-k) = 0$ pour $n = n_1 + p$. Il vient :

$$\sum_{k=0}^{p} (-1)^k \binom{p}{k} P(n_1 + p - k) = 0.$$

Soit :

$$P(n_1) = \sum_{k=0}^{p} (-1)^{p+1+k} \binom{p}{k} P(n_1 + p - k).$$

Mais par définition de n_1 on a $P(n_1 + p - k) \in \mathbb{Z}$ pour tout $k \in [0, p-1]$. Donc cette relation assure que $P(n_1) \in \mathbb{Z}$ également. Ceci est absurde donc si $P \in \mathcal{P}'$ on a aussi $P \in \mathcal{P}$: $\mathcal{P}' \subset \mathcal{P}$. Finalement $\mathcal{P} = \mathcal{P}'$.

6.a. Si $f \in \mathcal{P}_\infty$, il existe $g \in \mathcal{P}$ et $n_0 \in \mathbb{Z}$ tels que $f(n) = g(n)$ si $n \geq n_0$. De cette égalité on déduit que $\partial f(n) = \partial g(n)$ si $n \geq n_0 + 1$. Comme d'après 4.a. on sait que $\partial g \in \mathcal{P}$ ceci prouve que $\partial f \in \mathcal{P}_\infty$.
Réciproquement supposons que $\partial f \in \mathcal{P}_\infty$: il existe $g \in \mathcal{P}$ et $n_0 \in \mathbb{Z}$ tels que $\partial f(n) = g(n)$ si $n \geq n_0$. Comme $g \in \mathcal{P}$ on sait d'après 4.c. qu'il existe $(m_0, \ldots, m_p) \in \mathbb{Z}^{p+1}$ tel que $g = \sum_{k=0}^{p} m_k f_k$. Puisque $f_k = \partial f_k + \partial f_{k+1}$, ceci peut se réécrire : $g = \partial(\sum_{k=0}^{p} m_k(f_k + f_{k+1}))$. Donc en fait on a l'identité suivante, valable dès que $n \geq n_0 + 1$:

$$\partial\left(f - \sum_{k=0}^{p} m_k(f_k + f_{k+1})\right)(n) = 0.$$

Ceci prouve qu'il existe $q_0 \in \mathbb{Z}$ tel que pour $n \geq n_0 + 1$ on ait :

$$\Big(f - \sum_{k=0}^{p} m_k(f_k + f_{k+1})\Big)(n) = q_0.$$

Puisque pour tout $n \in \mathbb{Z}$, $q_0 = q_0 f_0(n)$ on a en fait :

$$f(n) = [q_0 f_0 + \sum_{k=0}^{p} m_k(f_k + f_{k+1})](n),$$

et ceci dès que $n \geq n_0 + 1$. Comme $[q_0 f_0 + \sum_{k=0}^{p} m_k(f_k + f_{k+1})] \in \mathcal{P}$ (3.a.), on a montré que $f \in \mathcal{P}_\infty$.

6.b. Si $f \in \mathcal{P}_\infty$, il existe $g \in \mathcal{P}$ et $n_0 \in \mathbb{Z}$ tels que $f(n) = g(n)$ si $n \geq n_0$. Une récurrence évidente assure que pour tout $p \in \mathbb{N}$ on a $\partial^p f(n) = \partial^p g(n)$ si $n \geq n_0 + p$. Mais on sait (4.d.) qu'il existe $p_0 \in \mathbb{N}$ tel que $\partial^{p_0} g = 0$. On a alors $\partial^{p_0} f(n) = 0$ pour $n \geq n_0 + p_0$.
Réciproquement s'il existe $p \in \mathbb{N}$ et $n_0 \in \mathbb{Z}$ tels que $\partial^p f(n) = 0$ pour $n \geq n_0$, on a en particulier $\partial^p f \in \mathcal{P}_\infty$. Le résultat du a. et une récurrence finie triviale assurent alors que $f \in \mathcal{P}_\infty$.

7. On va montrer par récurrence sur $k \in \mathbb{N}$ que $\sum_{f_k}(t) = t^k[(1-t)^{k+1}]^{-1}$.
Pour $k = 0$: $\sum_{f_0}(t) = \sum_{n=0}^{\infty} t^n = (1-t)^{-1}$.
Soit $k > 0$ et supposons que $\sum_{f_{k-1}}(t) = t^{k-1}[(1-t)^k]^{-1}$.
Alors $(1-t)^k t \sum_{f_{k-1}}(t) = t^k$. Mais :

$$\begin{aligned}
t\sum_{f_{k-1}}(t) &= t\sum_{n\geq 0} f_{k-1}(n)t^n \\
&= t\sum_{n\geq k-1} \binom{n}{k-1} t^n \quad \text{(formules du 3.a.)} \\
&= t\sum_{n\geq k-1} [\binom{n+1}{k} - \binom{n}{k}]t^n \\
&= \sum_{n\geq k-1} \binom{n+1}{k} t^{n+1} - t\sum_{n\geq k-1} \binom{n}{k} t^n \\
&= \sum_{n'\geq k} \binom{n'}{k} t^{n'} - t\sum_{n\geq k} \binom{n}{k} t^n \\
&= \sum_{f_k}(t) - t\sum_{f_k}(t) \quad \text{(formules du 3.a.)} \\
&= (1-t)\sum_{f_k}(t).
\end{aligned}$$

Donc $(1-t)^{k+1}\sum_{f_k}(t) = t^k$, ce qui achève la récurrence.

II. Dimensions des composantes homogènes d'anneaux de polynômes.

1. Il est clair que S_n est un k-espace vectoriel : il suffit pour le voir de constater que c'est une partie du k-espace vectoriel S, stable par addition et par multiplication par un scalaire (car alors ce en sera un sous-espace vectoriel). Ceci est évident.

Il est également clair que $\{X_1^{\alpha_1}\dots X_r^{\alpha_r}, \sum_{i=1}^r \alpha_i a_i = n\}$ en est une base. Puisqu'il s'agit d'une partie finie, S_n est de dimension finie.

2.a. Dans ce cas on a, compte tenu de la question précédente, pour tout $n \in \mathbb{Z}$:

$$\dim S_n = \mathrm{card}(\{(\alpha_1,\dots,\alpha_r) \in \mathbb{N}^r, \sum_{i=1}^r \alpha_i = n\}).$$

On va montrer par récurrence sur $r \in \mathbb{N}^*$ que pour tout $n \in \mathbb{Z}$:

$$\mathrm{card}(\{(\alpha_1,\dots,\alpha_r) \in \mathbb{N}^r, \sum_{i=1}^r \alpha_i = n\}) = \binom{n+r-1}{r-1}.$$

Si $r = 1$, c'est évident : ce nombre vaut 1 si $n \geq 0$, et 0 sinon.
Soit $r > 1$, et supposons le résultat vrai pour $r-1$. Pour tout $n \in \mathbb{Z}$ on a en posant $N(n,r) = \mathrm{card}(\{(\alpha_1,\dots,\alpha_r) \in \mathbb{N}^r, \sum_{i=1}^r \alpha_i = n\})$:

$$\begin{aligned}
N(n,r) &= \mathrm{card}\Big(\bigcup_{\alpha_r\in[0,n]} \{(\alpha_1,\dots,\alpha_{r-1}) \in \mathbb{N}^{r-1}, \sum_{i=1}^{r-1} \alpha_i = n-\alpha_r\}\Big) \\
&= \sum_{\alpha_r=0}^{n} \mathrm{card}(\{(\alpha_1,\dots,\alpha_{r-1}) \in \mathbb{N}^{r-1}, \sum_{i=1}^{r-1} \alpha_i = n-\alpha_r\}) \\
&\quad \text{(car l'union est disjointe)} \\
&= \sum_{\alpha_r=0}^{n} \binom{n-\alpha_r+r-2}{r-2} \quad \text{(par hypothèse de récurrence)} \\
&= \sum_{k=0}^{n} \binom{k+r-2}{r-2} \\
&= \tbinom{n+r-1}{r-1} \quad \text{(formule combinatoire utilisée au I.3.b.).}
\end{aligned}$$

Ceci achève la récurrence donc pour tout $n \in \mathbb{Z}$, $h_S(n) = \binom{n+r-1}{r-1}$.

2.b. Dans ce cas il est clair que $h_S(n) = 1$ si a_1 divise n, et $h_S(n) = 0$ sinon.

3. En reprenant la base exhibée à la question 1. on obtient que l'on a pour tout $n \in \mathbb{Z}$:

$$\begin{aligned}
h_S(n) &= \mathrm{card}(\{(\alpha_1,\dots,\alpha_r) \in \mathbb{N}^r, \sum_{i=1}^r \alpha_i a_i = n\}) \\
&= \mathrm{card}\Big(\bigcup_{\substack{\alpha_r\in\mathbb{N}\\ 0\leq n-\alpha_r a_r}} \{(\alpha_1,\dots,\alpha_{r-1}) \in \mathbb{N}^{r-1}, \sum_{i=1}^{r-1} \alpha_i a_i = n-\alpha_r a_r\}\Big) \\
&= \sum_{\substack{\alpha_r\in\mathbb{N}\\ 0\leq n-\alpha_r a_r}} \mathrm{card}(\{(\alpha_1,\dots,\alpha_{r-1}) \in \mathbb{N}^{r-1}, \sum_{i=1}^{r-1} \alpha_i a_i = n-\alpha_r a_r\}).
\end{aligned}$$

Mais $\{X_1^{\alpha_1}\dots X_{r-1}^{\alpha_{r-1}}, \sum_{i=1}^{r-1} \alpha_i a_i = n-\alpha_r a_r\}$ est une base de $S'_{n-\alpha_r a_r}$ donc pour tout $n \in \mathbb{Z}$:

$$h_S(n) = \sum_{\alpha_r\in\mathbb{N}, 0\leq n-\alpha_r a_r} h_{S'}(n-\alpha_r a_r).$$

4. $\sum'(t) = \sum_{n'=0}^{\infty} h_{S'}(n')t^{n'}$ donc le terme général d'indice m du produit $\sum'(t) \times \sum_{n=0}^{\infty} t^{na_r}$ est donné par la formule :

$$\sum_{(n,n')\in\mathbb{N}^2, n'+na_r=m} (h_{S'}(n') \times 1).$$

Mais $\sum_{(n,n')\in\mathbb{N}^2, n'+na_r=m} h_{S'}(n')$ peut se réécrire sous la forme suivante :

$$\sum_{n\in\mathbb{N}, 0\leq m-na_r} h_{S'}(m-na_r).$$

On a justement montré à la question 3. que cette somme valait $h_S(m)$ donc le terme général en question est celui de $\sum$: on a $\sum' \times \sum_{n=0}^{\infty} t^{na_r} = \sum$. Multiplions les deux membres de cette égalité par $(1-t^{a_r})$ qui est la série formelle inverse de $\sum_{n=0}^{\infty} t^{na_r}$. Nous obtenons après simplification :

$$\sum{}' = \sum \times (1-t^{a_r}).$$

Une récurrence finie sur r, triviale, assure alors que :

$$1 = \sum \times \prod_{i=1}^{r} (1-t^{a_i}).$$

Ceci signifie que :

$$\begin{aligned} \sum &= (\prod_{i=1}^{r}(1-t^{a_i}))^{-1} \\ &= \prod_{i=1}^{r}(1-t^{a_i})^{-1}. \end{aligned}$$

III. Idéaux homogènes et relations.

1.a. Débutons par une remarque générale dont nous ferons par la suite un usage constant sans plus de commentaire. Pour tout $n \in \mathbb{Z}$, π_n est un opérateur linéaire, et vérifie la propriété suivante : si P est homogène alors $\pi_n(PQ) = P\pi_{n-\deg P}(Q)$.

Supposons que toutes les composantes homogènes de P appartiennent à I. Alors P, qui est la somme de toutes ses composantes homogènes, appartient aussi à I car une somme d'éléments d'un idéal est encore dans cet idéal.

Réciproquement supposons que $P \in I$:
Puisque I est homogène, il admet un système fini de générateurs homogènes, que nous notons $(P_1, \ldots, P_s)$. Il existe $(F_1, \ldots, F_s) \in S^s$ tel que $P = \sum_{i=1}^{s} F_i P_i$. Soit maintenant $n \in \mathbb{N}$. On a :

$$\begin{aligned} \pi_n(P) &= \sum_{i=1}^{s} \pi_n(F_i P_i) \ (\pi_n \quad \text{est linéaire}) \\ &= \sum_{i=1}^{s} \pi_{n-\deg P_i}(F_i)P_i \ (\text{les } P_i \quad \text{sont homogènes}). \end{aligned}$$

Pour tout $i \in [1,s]$, $\pi_{n-degP_i}(F_i)P_i \in I$ puisque $P_i \in I$, donc $\pi_n(P) \in I$. Ceci est vrai pour tout $n \in \mathbb{N}$, donc toutes les composantes homogènes de P appartiennent à I.

1.b. Soit $(P_1, \ldots, P_s)$ un système fini de générateurs de I. Par hypothèse les composantes homogènes des P_i sont des éléments de I, et il est clair qu'en les regroupant toutes on obtient un nouveau système fini de générateurs de I. Mais celui-ci est composé d'éléments homogènes, donc I est homogène.

1.c. Il est clair que $X_1 + X_2$ et $X_1^2 + X_2(X_1 - 1)$ sont des éléments de $< X_1, X_2 >$ donc :

$$< X_1 + X_2, X_1^2 + X_2(X_1 - 1) > \subset < X_1, X_2 > .$$

Réciproquement

$$\begin{array}{rcl} X_2 & = & X_1(X_1 + X_2) - (X_1^2 + X_2(X_1 - 1)) \\ \text{et } X_1 & = & (1 - X_1)(X_1 + X_2) + (X_1^2 + X_2(X_1 - 1)) \end{array}$$

donc en fait :

$$< X_1, X_2 > \subset < X_1 + X_2, X_1^2 + X_2(X_1 - 1) > .$$

Ceci prouve que $< X_1 + X_2, X_1^2 + X_2(X_1 - 1) > = < X_1, X_2 >$, qui est un idéal homogène par définition, car X_1 et X_2 sont bien évidemment homogènes.

2.a. S_n est un sous-espace vectoriel de S. (II.1.)
I est un idéal de S, donc en particulier un sous-espace vectoriel de S.
Donc $I_n = I \cap S_n$ est encore un sous-espace vectoriel de S. Il est dans le sous-espace vectoriel S_n, donc on peut le voir comme un sous-espace vectoriel de S_n.

2.b. Soit I un idéal homogène de S et $(P_1, \ldots, P_s)$ un système fini de générateurs homogènes de I. Un polynôme homogène en une variable est un monôme donc pour tout $i \in [1,s]$, il existe $p_i \in \mathbb{N}$ tel que $P_i = X^{p_i}$. Soit alors $p = \min\{p_i, i \in [1,s]\}$. On a pour tout $i \in [1,s]$, $P_i = X^{p_i - p}X^p$ donc $P_i \in < X^p >$. Ceci prouve que $I \subset < X^p >$. X^p étant l'un des P_i l'inclusion réciproque est évidente d'où $I = < X^p >$. Comme par ailleurs il est clair que pour tout $p \in \mathbb{N}$, $< X^p >$ est un idéal homogène de S, les idéaux homogènes de S sont tous les $< X^p >$, $p \in \mathbb{N}$.

2.c. Soit $I = < X^p >$ (voir b.).
Si $0 \leq n < p$, $I_n = \{0\}$, donc $h_{S/I}(n) = \dim S_n/I_n = \dim S_n = 1$.
Si $n \geq p$:

$$\begin{array}{rcl} I_n & = & \{X^p P,\ P \in S_{n-p}\} \\ & = & \{X^p(\lambda X^{n-p}),\ \lambda \in k\} \\ & = & \{\lambda X^n,\ \lambda \in k\} \\ & = & S_n. \end{array}$$

Donc $h_{S/I}(n) = \dim S_n/I_n = \dim\{0\} = 0$.

3. $\underline{A}$ appartient au sous-module de relations engendré par $\underline{A}_1, \ldots, \underline{A}_M$, donc il existe $(P_1, \ldots, P_M) \in S^M$ tel que $\underline{A} = \sum_{j=1}^{M} P_j \underline{A}_j$. De même on sait qu'il

existe $(Q_1, \ldots, Q_M) \in S^M$ tel que $\underline{B} = \sum_{j=1}^{M} Q_j \underline{A}_j$. Il est alors évident que :

$$\underline{A} + \underline{B} = \sum_{j=1}^{M} (P_j + Q_j)\underline{A}_j$$

et que :

$$P\underline{A} = \sum_{j=1}^{M} (PP_j)\underline{A}_j.$$

Ceci prouve le résultat demandé et justifie donc la terminologie employée (i.e. le terme de "sous-module", l'anneau de base étant S.)

4. Soit $\underline{A} = (A_1, \ldots, A_N)$ une relation quelconque entre $F_1, \ldots, F_N$. Notons pour tout $j \in \mathbb{Z}$:

$$\underline{A}_j = (\pi_{j-\deg F_1}(A_1), \ldots, \pi_{j-\deg F_N}(A_N)).$$

Il est clair que seul un nombre fini des $\underline{A}_j$ sont non nulles.
Montrons d'abord que pour tout $j \in \mathbb{Z}$, $\underline{A}_j$ est une relation :

$$\begin{aligned}
\sum_{i=1}^{N} \pi_{j-\deg F_i}(A_i)F_i &= \sum_{i=1}^{N} \pi_j(A_i F_i) \text{ (les } F_i \text{ sont homogènes)} \\
&= \pi_j(\sum_{i=1}^{N} A_i F_i) \\
&= \pi_j(0) \text{ (} \underline{A} \text{ est une relation)} \\
&= 0.
\end{aligned}$$

Il est ensuite évident que pour tout $i \in [1, N]$, $\pi_{j-\deg F_i}(A_i)$ est homogène avec $\deg(\pi_{j-\deg F_i}(A_i)F_i) = j$, qui est indépendant de i, ce qui prouve que $\underline{A}_j$ est une relation homogène.
Enfin on a :

$$\begin{aligned}
\sum_{j\in\mathbb{Z}} \underline{A}_j &= \left(\sum_{j\in\mathbb{Z}} \pi_{j-\deg F_1}(A_1), \ldots, \sum_{j\in\mathbb{Z}} \pi_{j-\deg F_N}(A_N) \right) \\
&= \left(\sum_{j_1\in\mathbb{Z}} \pi_{j_1}(A_1), \ldots, \sum_{j_N\in\mathbb{Z}} \pi_{j_N}(A_N) \right) \\
&= (A_1, \ldots, A_n) \\
&= \underline{A}.
\end{aligned}$$

Donc $\underline{A}$ est la somme des $\underline{A}_j$, (toutes les sommes en jeu dans ce calcul sont bien sûr en réalité finies), ce qui prouve que $\underline{A}$ est somme de relations homogènes.

5.a. Soient A_1 et B_1 deux éléments de $p_1(\mathcal{R}_F)$ et P un élément de S. Il existe $(A_2, \ldots, A_N) \in S^{N-1}$ et $(B_2, \ldots, B_N) \in S^{N-1}$ tels que $\underline{A} = (A_1, \ldots, A_N)$ et $\underline{B} = (B_1, \ldots, B_N)$ soient des éléments de $\mathcal{R}_F$. Il est clair qu'alors $\underline{A}+\underline{B} \in \mathcal{R}_F$ et que $P\underline{A} \in \mathcal{R}_F$ (ce que l'énoncé admet implicitement en parlant de "la relation $\underline{A} + \underline{B}$" ou de "la relation $P\underline{A}$" et en employant le terme de module). Donc $p_1(\underline{A} + \underline{B}) \in p_1(\mathcal{R}_F)$ et $p_1(P\underline{A}) \in p_1(\mathcal{R}_F)$. Comme $p_1(\underline{A} + \underline{B}) = A_1 + A_2$ et $p_1(P\underline{A}) = PA_1$, cela prouve que $p_1(\mathcal{R}_F)$ est un idéal de S. Supposons de plus les F_i homogènes. Alors d'après 4., on peut écrire $\underline{A}$ comme une somme de relations

homogènes $\underline{A}_j = (A_{j,1}, \ldots, A_{j,N})$ pour $j \in J$ (J ensemble fini d'indices.) Pour tout $j \in J$, $A_{j,1} = p_1(\underline{A}_j) \in p_1(\mathcal{R}_F)$. D'autre part $A_1 = \sum_{j\in J} A_{j,1}$. Puisque les $\underline{A}_j$ sont homogènes, les $A_{j,1}$ également, donc les composantes homogènes de A_1 sont chacune des sommes de certains des $A_{j,1}$. En particulier les composantes homogènes de A_1 sont dans $p_1(\mathcal{R}_F)$ puisque c'est un idéal. D'après 1.b. cela prouve que $p_1(\mathcal{R}_F)$ est un idéal homogène.

5.b. D'après a., $p_1(\mathcal{R}_F)$ est un idéal de S. Notons-en $(A_{1,1}, \ldots, A_{M,1})$ un système fini de générateurs. Puisque les $A_{j,1}$ sont des éléments de $p_1(\mathcal{R}_F)$ on peut trouver $\{A_{j,i}\}_{(j,i)\in[1,M]\times[2,N]}$ tels que pour tout $j \in [1, M]$, $(A_{j,1}, \ldots, A_{j,N})$ soit une relation que l'on notera $\underline{A}_j$. Soit également $\mathcal{R}_1$ le sous-module de relations qu'elles engendrent. Considérons alors $\underline{A} = (A_1, \ldots, A_N)$ un élément de $\mathcal{R}_F$ quelconque. $A_1 \in p_1(\mathcal{R}_F)$, donc il existe $(P_1, \ldots, P_M) \in S^M$ tel que $A_1 = \sum_{j=1}^M P_j A_{j,1}$ ou encore $A_1 - \sum_{j=1}^M P_j A_{j,1} = 0$. Cela prouve que $\underline{A} - \sum_{j=1}^M P_j \underline{A}_j$ est une relation dont l'image par p_1 est nulle. De plus $\sum_{j=1}^M P_j \underline{A}_j$ est un élément de $\mathcal{R}_1$. Comme $\underline{A} = \sum_{j=1}^M P_j \underline{A}_j + (\underline{A} - \sum_{j=1}^M P_j \underline{A}_j)$, les relations $\underline{A}_1, \ldots, \underline{A}_M$ répondent à la question posée.

5.c. Montrons par récurrence sur $N \in \mathbb{N}^*$ que $\mathcal{R}_F$ peut être engendré par un nombre fini de relations :

Si $N = 1$ et si $\underline{A} = (A_1) \in \mathcal{R}_F$, alors $A_1 F_1 = 0$. Comme F_1 est non nul l'intégrité de S assure que $A_1 = 0$ et $\mathcal{R}_F$ est constitué uniquement de la relation nulle : celle-ci engendre donc $\mathcal{R}_F$.

Si $N > 1$, et si le résultat est vrai pour $N - 1$:

Appelons $\mathcal{R}'_F$ le module des relations entre $F_2, \ldots, F_N$. Par hypothèse de récurrence on peut l'engendrer avec un nombre fini de relations, par exemple $\underline{B}'_1, \ldots, \underline{B}'_P$. On pose pour tout $k \in [1, P]$, $\underline{B}'_k = (B_{k,2}, \ldots, B_{k,N})$. Il est alors clair qu'en posant pour tout $k \in [1, P]$, $\underline{B}_k = (0, B_{k,2}, \ldots, B_{k,N})$ on définit P éléments de $\mathcal{R}_F$. Soit maintenant $\underline{A}$ un élément de $\mathcal{R}_F$ dont l'image par p_1 est nulle : $\underline{A} = (0, A_2, \ldots, A_N)$. Il est clair que $(A_2, \ldots, A_N) \in \mathcal{R}'_F$ donc il existe $(P_1, \ldots, P_P) \in S^P$ tel que $(A_2, \ldots, A_N) = \sum_{k=1}^P P_k \underline{B}'_k$. On en déduit que : $\underline{A} = \sum_{k=1}^P P_k \underline{B}_k$. En invoquant le b. (dont on reprend également les notations), on a obtenu un système fini de générateurs pour $\mathcal{R}_F$: c'est $\underline{A}_1, \ldots, \underline{A}_M, \underline{B}_1, \ldots, \underline{B}_P$. Ceci achève la récurrence.

5.d. Il suffit d'utiliser c. pour exhiber un nombre fini de relations génératrices, puis d'invoquer 4. pour décomposer chacun de ces générateurs en une somme finie de relations homogènes : on obtient ainsi un système générateur de $\mathcal{R}_F$, fini, composé de relations homogènes.

IV. Etude des relations dans le cas $r = 2$.

1.a. D'abord par définition $\mathcal{R}_F \subset S^N$. Ensuite si $(A_1, \ldots, A_N) \in S^N$ on a :

$$\begin{aligned}
(A_1,\dots,A_N)\in\mathcal{R}_F &\iff \sum_{i=1}^{N} A_iF_i = 0\\
&\iff \sum_{i=1}^{N} A_i\varphi(e_i) = 0\\
&\iff \varphi(\sum_{i=1}^{N} A_ie_i) = 0 \ (\varphi \text{ est } K-\text{linéaire})\\
&\iff \varphi((A_1,\dots,A_N)) = 0\\
&\iff (A_1,\dots,A_N)\in\ker\varphi.
\end{aligned}$$

Donc $\mathcal{R}_F = S^N \cap \ker\varphi$.

1.b. D'après a., $\{\underline{A}_1,\dots,\underline{A}_M\}\subset\ker\varphi$.
Considérons réciproquement $(A_1,\dots,A_N)\in\ker\varphi$: d'après a., $(A_1,\dots,A_N)$ est un élément de $\mathcal{R}_F$ que l'on note $\underline{A}$. Par hypothèse il existe $(P_1,\dots,P_M)$, un élément de S^M tel que $\underline{A}=\sum_{j=1}^{M}P_j\underline{A}_j$. Les éléments de S sont à fortiori dans K, donc $\underline{A}$ est combinaison K-linéaire des $\underline{A}_j$, pour $j\in[1,M]$.
Ceci prouve que $\{\underline{A}_1,\dots,\underline{A}_M\}$ est un système générateur de $\ker\varphi$ (dans l'espace vectoriel K^N). En particulier $\text{card}(\{\underline{A}_1,\dots,\underline{A}_M\})\geq \dim\ker\varphi$. Mais d'une part évidemment $\text{card}(\{\underline{A}_1,\dots,\underline{A}_M\}) = M$ et d'autre part $\dim\ker\varphi = \dim K^N - 1 = N-1$ d'après le théorème du rang. Donc finalement $M\geq N-1$.

2.a. Fixons $j\in[1,M]$. Considérons les polynômes $A_{1j},\dots,A_{Nj}$. Comme $\underline{A}_j$ est une relation homogène, ils sont tous homogènes et les polynômes $A_{1j}F_1,\dots,A_{Nj}F_N$ sont également homogènes, qui plus est de même degré que l'on note δ_j. Puisque pour tout $i\in[1,N]$, $\deg A_{ij}F_i = \deg A_{ij}+\deg F_i$ on a $\delta_j = \deg A_{ij}+d_i$ soit $\deg A_{ij} = \delta_j - d_i$.

2.b. Soit $\underline{A}$ une relation homogène. $\underline{A}=(A_1,\dots,A_N)$ avec pour tout $i\in[1,N]$, A_i homogène. Notons Δ_i son degré ; il existe $d\in\mathbb{N}$ tel que pour tout $i\in[1,N]$, $\Delta_i+d_i=d$, car les A_iF_i sont tous de même degré (justement ce d). Il existe $(Q_1,\dots,Q_M)\in S^M$ tel que $\underline{A}=\sum_{j=1}^{M}Q_j\underline{A}_j$. De cette égalité on déduit que pour tout $i\in[1,N]$ on a : $A_i=\sum_{j=1}^{M}Q_jA_{ij}$. En particulier pour tout $n\in\mathbb{N}$ on a :

$$\begin{aligned}
\pi_n(A_i) &= \pi_n(\sum_{j=1}^{M}Q_jA_{ij})\\
&= \sum_{j=1}^{M}\pi_n(Q_jA_{ij})\\
&= \sum_{j=1}^{M}\pi_{n-(\delta_j-d_i)}(Q_j)A_{ij}
\end{aligned}$$

car les A_{ij} sont homogènes de degrés δ_j-d_i d'après a.. Donc si $n=\Delta_i$, cela donne $A_i=\sum_{j=1}^{M}\pi_{\Delta_i-(\delta_j-d_i)}(Q_j)A_{ij}=\sum_{j=1}^{M}\pi_{d-\delta_j}(Q_j)A_{ij}$. Posons donc pour tout $j\in[1,M]$, $P_j=\pi_{d-\delta_j}(Q_j)$. En particulier les P_j sont homogènes. La formule précédente assure que pour tout $i\in[1,N]$, $A_i=\sum_{j=1}^{M}P_jA_{ij}$ c'est-à-dire que $\underline{A}=\sum_{j=1}^{M}P_j\underline{A}_j$.

3.a. Notons pour tout $j \in [1,M]$, $A_{1j} = \sum_{k=0}^{\delta_j - d_1} a_{j,k} Y^k X^{(\delta_j - d_1)-k}$ ce qui est possible car d'après 2.a., A_{1j} est homogène de degré $\delta_j - d_1$. Choisissons alors $j_0 \in [1,M]$ tel que $\delta_{j_0} = \inf\{\delta_j, j \in [1,M] \text{ tel que } a_{j,(\delta_j - d_1)} \neq 0\}$. Posons ensuite pour tout $j \in [1,M]$ différent de j_0, $\lambda_j = -(a_{j_0,(\delta_{j_0}-d_1)})^{-1} a_{j,(\delta_j - d_1)}$. On a la relation :

$$a_{j,(\delta_j - d_1)} + \lambda_j a_{j_0,(\delta_{j_0} - d_1)} = 0.$$

Posons également $\underline{A}'_j = \underline{A}_j + \lambda_j Y^{(\delta_j - \delta_{j_0})} \underline{A}_{j_0}$. (Ceci est licite car par définition de δ_{j_0}, $Y^{(\delta_j - \delta_{j_0})}$ est bien un élément de S.) Posons enfin $\underline{A}'_{j_0} = \underline{A}_{j_0}$.

Il est clair que les $\underline{A}'_j$ pour $j \in [1,M]$, sont des éléments de $\mathcal{R}_F$ car c'est un S-module comme il l'a été remarqué au III.

On a d'après 2.a., $\deg A_{ij} = \delta_j - d_i$ et :

$$\deg(\lambda_j Y^{(\delta_j - \delta_{j_0})} A_{ij_0}) = (\delta_j - \delta_{j_0}) + (\delta_{j_0} - d_i) = \delta_j - d_i.$$

Donc A'_{ij} est homogène de degré $\delta_j - d_i$ et les $A'_{ij} F_i$ (pour $i \in [1,N]$) sont tous homogènes de même degré δ_j, ce qui prouve que chacune des $\underline{A}'_j$ est en fait une relation homogène.

Si $j \neq j_0$ on a :

$$\begin{aligned}
A'_{1j} &= A_{1j} + \lambda_j Y^{(\delta_j - \delta_{j_0})} A_{1j_0} \\
&= \sum_{k=0}^{(\delta_j - d_1)} a_{j,k} Y^k X^{(\delta_j - d_1)-k} \\
&\quad + \sum_{k'=0}^{(\delta_{j_0} - d_1)} [-(a_{j_0,(\delta_{j_0}-d_1)})^{-1} a_{j,(\delta_j - d_1)}] a_{j_0,k'} Y^{k' + (\delta_j - \delta_{j_0})} X^{(\delta_{j_0} - d_1) - k'} \\
&= \sum_{k=0}^{(\delta_j - d_1)} a_{j,k} Y^k X^{(\delta_j - d_1)-k} \;-\; a_{j,(\delta_j - d_1)} Y^{(\delta_j - d_1)} \\
&\quad + \sum_{k'=0}^{(\delta_{j_0} - d_1)-1} [-(a_{j_0,(\delta_{j_0}-d_1)})^{-1} a_{j,(\delta_j - d_1)}] a_{j_0,k'} Y^{k' + (\delta_j - \delta_{j_0})} X^{(\delta_{j_0} - d_1) - k'} \\
&= \sum_{k=0}^{(\delta_j - d_1)-1} a_{j,k} Y^k X^{(\delta_j - d_1)-k} \\
&\quad + \sum_{k'=0}^{(\delta_{j_0} - d_1)-1} [-(a_{j_0,(\delta_{j_0}-d_1)})^{-1} a_{j,(\delta_j - d_1)}] a_{j_0,k'} Y^{k' + (\delta_j - \delta_{j_0})} X^{(\delta_{j_0} - d_1) - k'}.
\end{aligned}$$

Ceci prouve que $A'_{1j} \in < X >$, donc est divisible par X.

Enfin si $\underline{A}$ est un élément quelconque de $\mathcal{R}_F$: il existe $(P_1, \ldots, P_M) \in S^M$ tel que $\underline{A} = \sum_{j=1}^{M} P_j \underline{A}_j$. Posons si $j \neq j_0$, $Q_j = P_j$ et $Q_{j_0} = P_{j_0} - \sum_{j \neq j_0} \lambda_j Y^{(\delta_j - \delta_{j_0})} P_j$.

Alors :

$$\begin{aligned}\sum_{j=1}^{M} Q_j \underline{A}'_j &= \sum_{j\neq j_0} P_j(\underline{A}_j + \lambda_j Y^{(\delta_j-\delta_{j_0})}\underline{A}_{j_0}) \\ &\quad +(P_{j_0} - \sum_{j\neq j_0} \lambda_j Y^{(\delta_j-\delta_{j_0})}P_j)\underline{A}_{j_0} \\ &= \sum_{j\neq j_0} P_j\underline{A}_j + (\sum_{j\neq j_0} \lambda_j Y^{(\delta_j-\delta_{j_0})}P_j)\underline{A}_{j_0} \\ &\quad +P_{j_0}\underline{A}_{j_0} - (\sum_{j\neq j_0} \lambda_j Y^{(\delta_j-\delta_{j_0})}P_j)\underline{A}_{j_0} \\ &= \sum_{j=1}^{M} P_j\underline{A}_j \\ &= \underline{A}.\end{aligned}$$

Cela prouve que les $\underline{A}'_j$ sont bien encore des générateurs de $\mathcal{R}_F$.

3.b. Soit $i_0 \in [1, N]$ et appelons P_{i_0} la propriété suivante : $\mathcal{R}_F$ peut être engendré par des relations homogènes $\underline{B}_1, \ldots, \underline{B}_M$ telles que pour tout $i \leq i_0$ et pour tout $j > i$, la i-ème composante B_{ij} de $\underline{B}_j$ soit divisible par X. Il faut ici démontrer P_N, ce que nous allons faire en procédant par récurrence sur i_0 pour montrer qu'en fait P_{i_0} est vraie pour tout $i_0 \in [1, N]$.
Si $i_0 = 1$: il suffit de considérer la famille $\{\underline{A}'_1, \ldots, \underline{A}'_M\}$ construite au a. et de la réordonner pour placer $\underline{A}'_{j_0}$ en première position.
Si $i_0 \in [1, N-1]$ et si P_{i_0} est vérifiée : alors $\mathcal{R}_F$ est engendré par des relations homogènes $\underline{B}_1, \ldots, \underline{B}_M$ telles que pour tout $i \leq i_0$ et pour tout $j > i$, la i-ème composante B_{ij} de $\underline{B}_j$ soit divisible par X. Si $i_0 \geq M-1$, il est clair que P_{i_0+1} est aussi vérifiée (en prenant la même famille de relations car en réalité on n'ajoute pas de conditions supplémentaires). On peut donc supposer que $i_0+1 < M$. Intéressons-nous au sous-module de $\mathcal{R}_F$ des relations engendrées par $\underline{B}_{i_0+1}, \ldots, \underline{B}_M$ et notons le $\mathcal{R}$. En appliquant la même technique qu'à la question a., il est clair que l'on peut trouver $\underline{B}'_{i_0+1}, \ldots, \underline{B}'_M$, générateurs homogènes de $\mathcal{R}$, et possédant de plus la propriété suivante : la (i_0+1)-ème composante de $\underline{B}'_j$ est divisible par X, pour tout $j \in [i_0+2, M]$. De plus si $j \geq i_0+1$ et $i \leq i_0$ alors la i-ème composante B'_{ij} de $\underline{B}'_j$ "reste" divisible par X car c'est une combinaison S-linéaire de polynômes divisibles par X (car la technique de construction est celle du a.). La famille $\{\underline{B}_1, \ldots, \underline{B}_{i_0}, \underline{B}'_{i_0+1}, \ldots, \underline{B}'_M\}$ possède donc les propriétés requises pour pouvoir affirmer que P_{i_0+1} est vraie.

3.c. Il y a ici une erreur dans l'énoncé :
considérons en effet $F_1 = Y$ et $F_2 = X$. (Cas $N = 2$). Soit alors $(P, Q) \in \mathcal{R}_F$. On a $PY + QX = 0$. D'où $QX = -PY$ et en particulier Y divise QX. Du théorème de Gauss on déduit que Y divise Q : $Q = YS$. On montre de même que $P = XR$. On a alors $(R+S)XY = 0$ donc $S = -R$: $(P, Q) = (RX, -RY) = R(X, -Y)$. Ceci prouve que $(X, -Y)$ est un générateur (homogène) de $\mathcal{R}_F$. Donc en posant $\underline{B}_1 = \underline{B}_2 = (X, -Y)$ on obtient un système générateur de relations homogènes de $\mathcal{R}_F$ ($M = 2$). Ce système vérifie les conditions du b. car $B_{12} = X$ est divisible par X. Pourtant $B_{22} = -Y$ n'est pas divisible par X, donc $\underline{B}_2 \notin X\mathcal{R}_F$.
Cependant on peut corriger l'énoncé, au prix d'accepter éventuellement une permutation préalable dans le système $\{F_1, \ldots, F_N\}$ (ce qui ne modifie pas la nature des relations de $\mathcal{R}_F$, mais juste l'ordre des facteurs dans une relation) : en effet posons $k = \max\{p \in \mathbb{N} \text{ tel que pour tout } i \in [1, N],\ X^p | F_i\}$. Alors il

existe $i_0 \in [1,N]$ tel que X^{k+1} ne divise pas F_{i_0}, et pour tout $i \in [1,N]$, X^k divise F_i. Réordonnons le système $\{F_1,\dots,F_N\}$ de sorte que F_{i_0} devienne le dernier. C'est à présent ce nouveau système que nous appelons $\{F_1,\dots,F_N\}$ (nous supposerons que ce choix a été opéré au début de cette partie, ce qui ne pose aucun problème comme pourra très aisément le vérifier un lecteur pointilleux). Intoduisons à présent le système $\{F'_1,\dots,F'_N\}$ où pour tout $i \in [1,N]$, F'_i désigne le quotient de F_i par X^k. Par choix de k, $\{F'_1,\dots,F'_N\} \subset S^N$ et X ne divise pas F'_N. Il est clair que $\mathcal{R}_F = \mathcal{R}'_F$:

$$\begin{aligned}\sum_{i=1}^{N} P_i F_i = 0 \quad &\text{ssi} \quad \sum_{i=1}^{N} P_i (F'_i X^k) = 0\\ &\iff \quad (\sum_{i=1}^{N} P_i F'_i) X^k = 0\\ &\iff \quad \sum_{i=1}^{N} P_i F'_i = 0.\end{aligned}$$

Montrons que pour tout $j \in [N,M]$, on a $\underline{B}_j \in X\mathcal{R}_F$:
Si $j > N$, c'est facile : d'après b. pour tout $i \in [1,N]$, B_{ij} est divisible par X : $B_{ij} = XB'_{ij}$ avec $B'_{ij} \in S$. On a $X(\sum_{i=1}^{N} B'_{ij}F_i) = \sum_{i=1}^{N} XB'_{ij}F_i = \sum_{i=1}^{N} B_{ij}F_i = 0$ car $\underline{B}_j \in \mathcal{R}_F$. Comme S est intègre, $\sum_{i=1}^{N} B'_{ij}F_i = 0$ ce qui prouve que $(B'_{1j},\dots,B'_{Nj}) \in \mathcal{R}_F$. Or $\underline{B}_j = X(B'_{1j},\dots,B'_{Nj})$ donc $\underline{B}_j \in X\mathcal{R}_F$.
Si $j = N$: toujours d'après b. pour tout $i \in [1,N-1]$, B_{iN} est divisible par X. Il suffit alors de prouver que B_{NN} est également divisible par X pour conclure comme dans le cas $j > N$. Comme $\underline{B}_N \in \mathcal{R}_F$, $\underline{B}_N \in \mathcal{R}'_F$: $\sum_{i=1}^{N} B_{iN}F'_i = 0$, soit $B_{NN}F'_N = -\sum_{i=1}^{N-1} B_{iN}F'_i$. Puisque pour tout $i \in [1,N-1]$, B_{iN} est divisible par X, on en déduit que X divise $B_{NN}F'_N$. Comme X ne divise pas F'_N, X est premier avec F'_N, donc X divise B_{NN} par le théorème de Gauss (S est factoriel). CQFD.

4.a. On va montrer ce résultat par récurrence sur $n \in \mathbb{N}^*$:
Si $n = 1$: $\underline{A} \in \mathcal{R}_F$ donc il existe $(P_1,\dots,P_M) \in S^M$ tel que :

$$\underline{A} = \sum_{j=1}^{M} P_j \underline{B}_j = \sum_{j=1}^{N-1} P_j \underline{B}_j + \sum_{j=N}^{M} P_j \underline{B}_j.$$

Par définition de $\mathcal{R}'$, $\sum_{j=1}^{N-1} P_j \underline{B}_j \in \mathcal{R}'$. D'après le 3.c., pour tout $j \in [N,M]$, il existe $\underline{B}'_j \in \mathcal{R}_F$ tel que $\underline{B}_j = X\underline{B}'_j$. On a :

$$\sum_{j=N}^{M} P_j \underline{B}_j = \sum_{j=N}^{M} P_j X \underline{B}'_j = X(\sum_{j=N}^{M} P_j \underline{B}'_j).$$

Or $\sum_{j=N}^{M} P_j \underline{B}'_j \in \mathcal{R}_F$ puisque $\underline{B}'_j \in \mathcal{R}_F$, donc $\sum_{j=N}^{M} P_j \underline{B}_j \in X\mathcal{R}_F$.
Si $n \geq 1$ et si le résultat est vrai pour n alors $\underline{A} = \underline{A}' + X^n \underline{B}$ où $\underline{A}' \in \mathcal{R}'$ et $\underline{B} \in \mathcal{R}_F$. Puisque $\underline{B} \in \mathcal{R}_F$ le cas $n = 1$ permet d'affirmer qu'il existe $\underline{B}' \in \mathcal{R}'$ et $\underline{C} \in \mathcal{R}_F$ tels que $\underline{B} = \underline{B}' + X\underline{C}$. Alors :

$$\underline{A} = \underline{A}' + X^n(\underline{B}' + X\underline{C}) = (\underline{A}' + X^n\underline{B}') + X^{n+1}\underline{C}.$$

Comme $\underline{B}' \in \mathcal{R}'$, $X^n\underline{B}' \in \mathcal{R}'$ d'où $\underline{A}' + X^n\underline{B}' \in \mathcal{R}'$: le résultat est vrai pour $n+1$, ce qui achève la récurrence.

4.b. On va démontrer que $\mathcal{R}_F \subset \mathcal{R}'$ (ce qui est suffisant car l'inclusion réciproque est évidente, et alors $\underline{B}_1, \ldots, \underline{B}_{N-1}$ engendrent $\mathcal{R}_F$). Pour cela considérons $\underline{A}$ dans $\mathcal{R}_F$ quelconque et montrons que $\underline{A} \in \mathcal{R}'$. D'après III.4., $\underline{A}$ est somme de relations homogènes : $\underline{A} = \sum_{k=1}^{K} \underline{A}_k$ où $\underline{A}_k$ est une relation homogène. Comme $\mathcal{R}'$ est un sous-module, il suffit de vérifier que chaque $\underline{A}_k \in \mathcal{R}'$. Fixons donc $k \in [1, K]$ et étudions $\underline{A}_k = (A_{1k}, \ldots, A_{Nk})$. Puisque $\underline{A}_k$ est une relation homogène les A_{ik} sont tous homogènes et il existe $D_k \in \mathbb{N}$ tel que pour tout $i \in [1, N]$, $A_{ik}F_i$ soit homogène de degré D_k. On a alors $\deg A_{ik} = D_k - d_i$. D'autre part en utilisant 2.a. il existe $(\delta'_1, \ldots, \delta'_M)$ tel que pour tout $(i, j) \in [1, N]\times[1, M]$, $\deg B_{ij} = \delta'_j - d_i$. Alors $\deg A_{ik} - \deg B_{ij} = (D_k - d_i) - (\delta'_j - d_i) = D_k - \delta'_j$. Posons $n = \max\{\deg(A_{ik}) + 1, i \in [1, N]\}$. D'après a. il existe $\underline{A}'_k \in \mathcal{R}'$ et $\underline{B} \in \mathcal{R}_F$ tels que $\underline{A}_k = \underline{A}'_k + X^n\underline{B}$. On pose $\underline{A}'_k = \sum_{j=1}^{N-1} P_j\underline{B}_j$ et $\underline{B} = \sum_{j=1}^{M} Q_j\underline{B}_j$. Alors pour tout $i \in [1, N]$ on a :

$$A_{ik} = \sum_{j=1}^{N-1} P_j B_{ij} + \sum_{j=1}^{M} X^n Q_j B_{ij}.$$

Comme A_{ik} est homogène on a :

$$\begin{aligned} A_{ik} &= \pi_{\deg A_{ik}}(A_{ik}) \\ &= \sum_{j=1}^{N-1} \pi_{\deg A_{ik}}(P_j B_{ij}) + \sum_{j=1}^{M} \pi_{\deg A_{ik}}(X^n Q_j B_{ij}). \end{aligned}$$

Chaque terme de la seconde somme est nulle par choix de n donc en fait :

$$\begin{aligned} A_{ik} &= \sum_{j=1}^{N-1} \pi_{\deg A_{ik}}(P_j B_{ij}) \\ &= \sum_{j=1}^{N-1} \pi_{\deg A_{ik} - \deg B_{ij}}(P_j) B_{ij} \\ &\quad \text{car les } B_{ij} \text{ sont homogènes.} \\ &= \sum_{j=1}^{N-1} \pi_{D_k - \delta'_j}(P_j) B_{ij}. \end{aligned}$$

Posons alors pour tout $j \in [1, N-1]$, $R_j = \pi_{D_k - \delta'_j}(P_j)$. Le calcul précédent prouve que pour tout $i \in [1, N]$, $A_{ik} = \sum_{j=1}^{N-1} R_j B_{ij}$. Cela signifie exactement que $\underline{A}_k = \sum_{j=1}^{N-1} R_j\underline{B}_j$, donc $\underline{A}_k \in \mathcal{R}'$.

5.a. Considérons l'espace vectoriel $\bigoplus_{i=1}^{N} S_{n-d_i}$ (somme directe "externe" d'espaces vectoriels). Considérons également l'application φ suivante :

$$\begin{aligned} \bigoplus_{i=1}^{N} S_{n-d_i} &\to S \\ (P_1, \ldots, P_N) &\mapsto \sum_{i=1}^{N} P_i F_i. \end{aligned}$$

Il est clair que φ est une application linéaire.

Puisque les F_i sont des éléments de I, on a forcément $\mathrm{im}\varphi \subset I$. De plus si $P_i \in S_{n-d_i}$, $P_iF_i \in S_n$ donc $\mathrm{im}\varphi \subset S_n$; Ceci force $\mathrm{im}\varphi \subset I \cap S_n = I_n$.
Réciproquement si $F \in I_n$, alors en particulier $F \in I$. Comme les F_i en forment un système générateur il existe $(P_1, \ldots, P_N) \in S^N$ tel que $F = \sum_{i=1}^N P_iF_i$. F appartient également à S_n donc $F = \pi_n(F)$. Cela donne :

$$\begin{aligned} F &= \pi_n(\sum_{i=1}^N P_iF_i) \\ &= \sum_{i=1}^N \pi_n(P_iF_i) \\ &= \sum_{i=1}^N \pi_{n-d_i}(P_i)F_i \end{aligned}$$

car les F_i sont homogènes de degrés d_i.
Posons alors pour tout $i \in [1, N]$, $Q_i = \pi_{n-d_i}(P_i) : Q_i \in S_{n-d_i}$. De plus $F = \sum_{i=1}^N Q_iF_i$. Donc $F = \varphi(Q_1, \ldots, Q_N)$ ce qui prouve que $I_n \subset \mathrm{im}\varphi$. Finalement $\mathrm{im}\varphi = I_n$.

Appliquons le théorème d'isomorphisme à $\varphi : \mathrm{im}\varphi \simeq (\bigoplus_{i=1}^N S_{n-d_i})/\ker\varphi$ c'est-à-dire $I_n \simeq (\bigoplus_{i=1}^N S_{n-d_i})/\ker\varphi$. Intéressons-nous donc maintenant au noyau de φ. Pour cela considérons les espaces vectoriels $\bigoplus_{j=1}^{N-1} S_{n-\varepsilon_j}$ et $\bigoplus_{i=1}^N S$ (toujours des sommes directes "externes") et l'application ψ suivante :

$$\begin{aligned} \bigoplus_{j=1}^{N-1} S_{n-\varepsilon_j} &\to \bigoplus_{i=1}^N S \\ (P_1, \ldots, P_{N-1}) &\mapsto (\sum_{j=1}^{N-1} P_jC_{1j}, \ldots, \sum_{j=1}^{N-1} P_jC_{Nj}). \end{aligned}$$

Il est clair que ψ est une application linéaire.

Soit $(P_1, \ldots, P_{N-1}) \in \bigoplus_{j=1}^{N-1} S_{n-\varepsilon_j}$. Si $(i, j) \in [1, N] \times [1, N-1]$, P_jC_{ij} est homogène avec $\deg P_jC_{ij} = \deg P_j + \deg C_{ij} = (n - \varepsilon_j) + (\varepsilon_j - d_i) = n - d_i$. Donc en fait $\mathrm{im}\psi \subset \bigoplus_{i=1}^N S_{n-d_i}$.
De plus :

$$\begin{aligned} \varphi(\psi(P_1, \ldots, P_{N-1})) &= \sum_{i=1}^N (\sum_{j=1}^{N-1} P_jC_{ij})F_i \\ &= \sum_{j=1}^{N-1} P_j(\sum_{i=1}^N C_{ij}F_i) \\ &= \sum_{j=1}^{N-1} P_j 0 \text{ (car } \underline{C}_j \in \mathcal{R}_F) \\ &= 0. \end{aligned}$$

Donc $\mathrm{im}\psi \subset \ker\varphi$.
Réciproquement soit $(Q_1, \ldots, Q_N) \in \ker\varphi : (Q_1, \ldots, Q_N)$ définit donc un élément de $\mathcal{R}_F$ que l'on peut noter $\underline{Q}$. Puisque les $\underline{C}_j$ forment un système de générateurs de $\mathcal{R}_F$ on peut trouver des polynômes $R_1, \ldots, R_{N-1}$ tels que $\underline{Q} = \sum_{j=1}^{N-1} R_j\underline{C}_j$.

En particulier pour tout $i \in [1,N]$, $Q_i = \sum_{j=1}^{N-1} R_j C_{ij}$. Puisque $(Q_1,\dots,Q_N) \in \ker\varphi$, on voit que pour tout $i \in [1,N]$, Q_i est homogène de degré $n-d_i$ ce qui s'écrit $Q_i = \pi_{n-d_i}(Q_i)$. On en déduit que :

$$\begin{aligned} Q_i &= \pi_{n-d_i}(\sum_{j=1}^{N-1} R_j C_{ij}) \\ &= \sum_{j=1}^{N-1} \pi_{n-d_i}(R_j C_{ij}) \\ &= \sum_{j=1}^{N-1} \pi_{n-d_i-(\varepsilon_j-d_i)}(R_j) C_{ij} \end{aligned}$$

car les C_{ij} sont homogènes de degrés $\varepsilon_j - d_i$.
Mais $n-d_i-(\varepsilon_j-d_i) = n-\varepsilon_j$ est indépendant de i donc on peut poser pour tout $j \in [1,N-1]$: $P_j = \pi_{n-d_i-(\varepsilon_j-d_i)}(R_j)$. On note d'abord que $P_j \in S_{n-\varepsilon_j}$. Ensuite le calcul précédent donne pour tout $i \in [1,N]$, $Q_i = \sum_{j=1}^{N-1} P_j C_{ij}$. Cela prouve que $(Q_1,\dots,Q_N) = \psi(P_1,\dots,P_{N-1})$ donc que $(Q_1,\dots,Q_N) \in \mathrm{im}\psi$: $\ker\varphi \subset \mathrm{im}\psi$ d'où finalement $\ker\varphi = \mathrm{im}\psi$.

Appliquons le théorème d'isomorphisme à ψ : $\mathrm{im}\psi \simeq (\bigoplus_{j=1}^{N-1} S_{n-\varepsilon_j})/\ker\psi$ donc en fait $\ker\varphi \simeq (\bigoplus_{j=1}^{N-1} S_{n-\varepsilon_j})/\ker\psi$.

Il suffit donc maintenant d'établir que $\ker\psi = \{0\}$ pour répondre à la question posée. Soit alors $(P_1,\dots,P_N) \in \ker\psi$. On obtient immédiatement que $\sum_{j=1}^{N-1} P_j \underline{C}_j = 0$ dans K^N. Mais comme $\underline{C}_1,\dots,\underline{C}_{N-1}$ engendrent $\mathcal{R}_F$, ils forment un système générateur (dans le K-espace vectoriel K^N) du noyau de la forme linéaire considérée au 1.. Ce noyau était de dimension $N-1$, donc cette famille en est en fait une base. En particulier c'est une famille libre sur K, ce qui force la nullité de tous les P_j : effectivement $\ker\psi = \{0\}$.

5.b. On sait que $\dim E/F = \dim E - \dim F$ donc d'après a. :

$$\begin{aligned} \dim I_n &= \dim(\bigoplus_{i=1}^{N} S_{n-d_i}) - \dim(\bigoplus_{j=1}^{N-1} S_{n-\varepsilon_j}) \\ &= \sum_{i=1}^{N} \dim(S_{n-d_i}) - \sum_{j=1}^{N-1} \dim(S_{n-\varepsilon_j}) \\ &= \sum_{i=1}^{N} \binom{n-d_i+1}{1} - \sum_{j=1}^{N-1} \binom{n-\varepsilon_j+1}{1} \end{aligned}$$

d'après II.2.a..
Or $h_{S/I}(n) = \dim S_n/I_n = \dim S_n - \dim I_n = \binom{n+1}{1} - \dim I_n$. Donc on a :

$$h_{S/I}(n) = \binom{n+1}{1} - \sum_{i=1}^{N} \binom{n-d_i+1}{1} + \sum_{j=1}^{N-1} \binom{n-\varepsilon_j+1}{1}.$$

5.c. Posons $n_0 = \max\{\max\{d_i-1, i \in [1,N]\}, \max\{\varepsilon_j - 1, j \in [1,N-1]\}\}$.
Alors pour tout $n \geq n_0$, on a :
pour tout $i \in [1,N]$, $\binom{n-d_i+1}{1} = n-d_i+1$;
pour tout $j \in [1,N-1]$, $\binom{n-\varepsilon_j+1}{1} = n-\varepsilon_j+1$.

Donc si $n \geq n_0$:

$$\begin{aligned} h_{S/I}(n) &= (n+1) - \sum_{i=1}^{N}(n - d_i + 1) + \sum_{j=1}^{N-1}(n - \varepsilon_j + 1) \\ &= n + 1 - Nn + \sum_{i=1}^{N} d_i - N + (N-1)n - \sum_{j=1}^{N-1} \varepsilon_j + (N-1) \\ &= \sum_{i=1}^{N} d_i - \sum_{j=1}^{N-1} \varepsilon_j. \end{aligned}$$

C'est une constante (i.e. c'est indépendant de n). Il est donc clair que $h_{S/I} \in \mathcal{P}_\infty$ car il suffit de prendre pour g cette constante, dans la définition de $\mathcal{P}_\infty$ donnée au I..

V. Idéaux monômiaux.

1.a. Précisons tout de suite que l'ensemble des monômes de S forme une base de S. Ce fait revêt une importance capitale dans cette partie.
Si m est divisible par l'un des monômes $m_1, \ldots, m_s$, il est clair que $m \in I$ car I est un idéal.
Réciproquement supposons que $m \in I$: il existe $(P_1, \ldots, P_s) \in S^s$ tel que $m = \sum_{i=1}^{s} P_i m_i$. Fixons $i \in [1, s]$ et écrivons $P_i = \sum_{t_i \in T_i} \lambda_t p_{it_i}$ la décomposition de P_i en somme de ses termes (i.e. on décompose P_i suivant la base des monômes). Puisque m_i est un monôme, il est immédiat que $\sum_{t_i \in T_i} \lambda_{t_i}(p_{it_i} m_i)$ est la décomposition de $P_i m_i$ en somme de ses termes. On a :

$$m - \sum_{i=1}^{s} \sum_{t_i \in T_i} \lambda_{t_i}(p_{it_i} m_i) = 0.$$

Mais pour tout $i \in [1, s]$, pour tout $t_i \in T_i$, $p_{it_i} m_i$ est un monôme, donc cette relation est en fait une combinaison linéaire nulle de monômes. Supposons que pour tout $i \in [1, s]$, pour tout $t_i \in T_i$, $p_{it_i} m_i \neq m$. Alors cette combinaison linéaire est non triviale (le coefficient affecté à m vaut 1) : c'est absurde car puisque la famille des monômes est une base de S, elle est en particulier libre. Donc il existe $i_0 \in [1, s]$ et $t_{i_0} \in T_{i_0}$ tels que $p_{i_0 t_{i_0}} m_{i_0} = m$. En particulier m est divisible par le monôme m_{i_0}.

1.b. Si chacun des termes de P appartient à I, alors il est clair que $P \in I$ car I est un idéal.
Réciproquement supposons que $P \in I$: il existe $(P_1, \ldots, P_s) \in S^s$ tel que $P = \sum_{i=1}^{s} P_i m_i$. Ecrivons encore que $P_i = \sum_{t_i \in T_i} \lambda_{t_i} p_{it_i}$ comme au a.. Alors $P = \sum_{i=1}^{s} \sum_{t_i \in T_i} \lambda_{t_i}(p_{it_i} m_i)$ est une écriture de P comme combinaison linéaire de termes (mais pas forcément les "siens") car les m_i sont des monômes. Si dans cette somme on regroupe les termes qui ont même monôme associé, alors on obtient la décomposition de P comme somme de ses termes. On voit donc que chacun des termes de P est une combinaison S-linéaire des monômes $m_1, \ldots, m_s$, et est donc un élément de I.

1.c. D'abord puisque I est un idéal, il est clair que J est également un idéal. En effet si $(P,Q) \in J^2$ alors $(P+Q)m = Pm + Qm \in I$ car $(Pm, Qm) \in I^2$ et si $(P,Q) \in S \times J$ alors $(PQ)m = P(Qm) \in I$ car $Qm \in I$.
Ensuite posons $\mathcal{M}_I = \{p \text{ tel que } p \text{ est un monôme avec } pm \in I\}$, et soit J' l'idéal engendré par les éléments de $\mathcal{M}_I$. C'est un idéal monômial car il admet le système de générateurs $\mathcal{M}_I$, qui est formé de monômes. (Le lecteur s'inquiète peut-être du fait que ce système soit infini ; mais la définition donnée ici d'un idéal monômial ne suppose pas qu'il doive s'agir d'un système fini, et de toute manière il peut toujours en être ainsi car S est noethérien.) Par définition $\mathcal{M}_I \subset J$ donc $J' \subset J$.
Réciproquement soit $P \in J$ et écrivons sa décomposition comme somme de ses termes : $P = \sum_{t\in T} \lambda_t p_t$. Alors puisque m est un monôme, $P = \sum_{t\in T} \lambda_t (p_t m)$ est la décomposition de Pm comme somme de ses termes. Comme $P \in J$, $Pm \in I$ et donc d'après b., $\lambda_t(p_t m) \in I$ pour tout $t \in T$. Cela signifie que pour tout $t \in T$, $p_t m \in I$, et donc que $p_t \in \mathcal{M}_I$. Ceci prouve que $P \in J'$, donc $J \subset J'$.
Finalement $J = J'$ donc J est monômial.

2. D'abord il est clair que $I \cap I'$ est un idéal.
Posons ensuite pour tout $(i,j) \in [1,s] \times [1,t]$, $m_{ij} = \text{ppcm}(m_i, m'_j)$ et soit J l'idéal engendré par tous les monômes m_{ij}. C'est bien sûr un idéal monômial.
Soit m un monôme de J. Il est divisible par un $m_{i_0 j_0}$ d'après 1.a.. Donc il est divisible par m_{i_0} et par m'_{j_0} puisque $m_{i_0 j_0}$ en est un multiple commun ; on en déduit qu'il appartient à I et à I' : $m \in I \cap I'$. Mais puisque J est monômial, il est engendré par les monômes qu'il contient. On vient donc de montrer que $I \cap I'$ contient un système générateur de J, ce qui assure l'inclusion $J \subset I \cap I'$.
Réciproquement soit $P \in I \cap I'$ et $P = \sum_{t\in T} \lambda_t p_t$ sa décomposition en somme de ses termes. En particulier $P \in I$ qui est monômial, donc d'après 1.b. pour tout $t \in T$, $p_t \in I$. Fixons $t_0 \in T$: $p_{t_0} \in I$. Alors d'après 1.a. il existe $i_0 \in [1,s]$ tel que m_{i_0} divise p_{t_0}. De même puisque $P \in I'$, $p_{t_0} \in I'$ et il existe $j_0 \in [1,t]$ tel que m'_{j_0} divise p_{t_0}. Donc p_{t_0} est un multiple commun à m_{i_0} et m'_{j_0}. Or $m_{i_0 j_0}$ est leur ppcm donc p_{t_0} est également un multiple de $m_{i_0 j_0}$: $p_{t_0} \in J$. Comme t_0 est quelconque, ceci prouve que $P \in J$, donc $I \cap I' \subset J$.
Finalement $I \cap I' = J$, donc $I \cap I'$ est bien monômial.

3. Si $n \leq 0$, il est clair que $I_n = \{0\}$ donc $h_{S/I}(n) = 0$ si $n < 0$ et $h_{S/I}(0) = 1$.
Si $n > 0$, étudions l'espace vectoriel I_n : la famille des $X_1^{\alpha_1} \dots X_r^{\alpha_r}$ où les $(\alpha_1, \dots, \alpha_r)$ sont les éléments de $\mathbb{N}^r$ qui vérifient $\sum_{i=1}^r \alpha_i = n$ et il existe $i_0 \in [1,s]$ tel que $\alpha_{i_0} > 0$, en est une base. Pourquoi ?
D'abord cette famille est évidemment incluse dans I_n.
Ensuite c'est une famille de monômes distincts donc elle est libre.
Enfin considérons $P \in I_n$, et écrivons $P = \sum_{t\in T} \lambda_t p_t$ sa décomposition en somme de ses termes. I est monômial par définition donc d'après 1.b. on a pour tout $t \in T$, $\lambda_t p_t \in I$, donc $p_t \in I$. Comme pour tout $t \in T$, p_t est un monôme on a d'après 1.a. : pour tout $t \in T$, il existe $i(t) \in [1,s]$ tel que $X_{i(t)} | p_t$. Donc p_t s'écrit $X_1^{\alpha_1} \dots X_r^{\alpha_r}$ où $(\alpha_1, \dots, \alpha_r) \in \mathbb{N}^r$ et il existe $i_0 \in [1,s]$ tel que $\alpha_{i_0} > 0$ (prendre $i_0 = i(t)$). De plus $\lambda_t p_t$ est un terme de P qui est un polynôme homogène de degré n, donc le degré du monôme p_t est n : $\sum_{i=1}^r \alpha_i = n$. Donc notre famille est aussi génératrice de I_n.
Comme par ailleurs la famille $\{X_1^{\alpha_1} \dots X_r^{\alpha_r}\}$ où $(\alpha_1, \dots, \alpha_r)$ est un élément de $\mathbb{N}^r$ qui vérifie $\sum_{i=1}^r \alpha_i = n$, est une base de S_n, alors en prenant le complémentai-

re de notre base de I_n dans cette famille on obtient une base d'un supplémentaire de I_n dans S_n : la famille $\{X_1^{\alpha_1}\dots X_r^{\alpha_r}\}$ où $(\alpha_1,\dots,\alpha_r)\in\mathbb{N}^r$ vérifie $\sum_{i=1}^r\alpha_i = n$ et pour tout $i\in[1,s]$, $\alpha_i = 0$ est une base d'un supplémentaire de I_n dans S_n. Ce supplémentaire étant isomorphe à S_n/I_n, la dimension de S_n/I_n est le cardinal de cette dernière base. Mettant à part le cas $s = r$ qui est évident $(h_{S/I}(n) = 0)$, on constate donc qu'en posant $S' = k[X_{s+1}^{\alpha_{s+1}},\dots,X_r^{\alpha_r}]$ on a $h_{S/I}(n) = h_{S'}(n)$. Or d'après II.2.a., $h_{S'}(n) = \binom{n+r-s-1}{r-s-1}$. Donc $h_{S/I}(n) = \binom{n+r-s-1}{r-s-1}$. En utilisant les formules établies au I.3.a., ceci prouve que si $n\geq 1$, $h_{S/I}(n) = f_{r-s-1}(n+r-s-1)$. Toujours d'après I.3.a., $f_{r-s-1}\in\mathcal{P}$ donc $h_{S/I}\in\mathcal{P}_\infty$.

4.a. Considérons $P\in S_{n-d}$. Comme m est un monôme, donc homogène, de degré d, $Pm\in S_n$. Cela a donc un sens de considérer l'application φ suivante :

$$\begin{array}{ccc} S_{n-d} & \to & S_n/I_n \\ P & \mapsto & \overline{Pm}. \end{array}$$

Il est clair qu'il s'agit d'une application linéaire.
Si $P\in J_{n-d}$ (donc $P\in J$) on a immédiatement $Pm\in I$ par définition de J, donc $\varphi(P) = 0 : J_{n-d}\subset\ker\varphi$.
Réciproquement si $P\in\ker\varphi$ alors $\overline{Pm} = 0$ donc $Pm\in I$: cela prouve que $P\in J$, donc $\ker\varphi\subset J_{n-d}$ et en définitive $\ker\varphi = J_{n-d}$.
Si $P\in S_{n-d}$, alors $Pm\in <m>\cap S_n\subset I'_n$, donc $\varphi(P)\in I'_n/I_n$: $\mathrm{im}\varphi\subset I'_n/I_n$.
Réciproquement soit $\overline{Q}\in I'_n/I_n$, $(Q\in I'_n)$. Puisque $Q\in I'$ il existe $(Q'',P')\in I\times S$ tel que $Q = Q''+P'm$. On a $Q = \pi_n(Q) = \pi_n(Q'')+\pi_{n-d}(P')m$ puisque Q et m sont homogènes de degrés n et d. Posons $Q' = \pi_n(Q'')$ et $P = \pi_{n-d}(P')$. Comme I est un idéal homogène, $Q'\in I_n$, et il est de plus évident que $P\in S_{n-d}$. La première remarque prouve que $\overline{Q'} = 0$ et la seconde que cela a un sens de considérer $\varphi(P)$; $\varphi(P) = \overline{Pm} = \overline{Pm}+\overline{Q'} = \overline{Pm+Q'} = \overline{Q}$. D'où $I'_n/I_n\subset\mathrm{im}\varphi$ et en définitive $\mathrm{im}\varphi = I'_n/I_n$.
Appliquons à présent le théorème du rang à φ :

$$\begin{array}{rcl} \dim S_{n-d} & = & \dim\ker\varphi+\mathrm{rg}\varphi \\ & = & \dim J_{n-d}+\dim I'_n/I_n. \end{array}$$

On a donc :

$$\begin{array}{rcl} \dim S_{n-d}-\dim J_{n-d} & = & \dim I'_n-\dim I_n \\ & = & (\dim I'_n-\dim S_n)+(\dim S_n-\dim I_n). \end{array}$$

Ceci peut se réécrire de la manière suivante :

$$\dim(S_{n-d}/J_{n-d}) = -\dim(S_n/I'_n)+\dim(S_n/I_n).$$

C'est-à-dire :

$$h_{S/J}(n-d) = -h_{S/I'}(n)+h_{S/I}(n).$$

4.b. Appelons $\mathcal{I}_N$ l'ensemble des idéaux monômiaux L qui peuvent s'écrire $L = <m'_1,\dots,m'_t>$ avec $\sum_{i=1}^t\deg m'_i\leq N$. En particulier $I\in\mathcal{I}_{\sum_{i=1}^s\deg m_s}$. On va démontrer par récurrence sur $N\in\mathbb{N}$, que pour tout $N\in\mathbb{N}$ et pour tout $L\in\mathcal{I}_N$, $h_{S/L}\in\mathcal{P}_\infty$ ce qui prouvera le résultat.

Si $N = 0$: si $L \in \mathcal{I}_0$, alors forcément $L =< 1 >$ donc $L = S$ et $h_{S/L} = 0 \in \mathcal{P}_\infty$.
Si $N \geq 0$ et si pour tout $L \in \mathcal{I}_N$, $h_{S/L} \in \mathcal{P}_\infty$: considérons $L \in \mathcal{I}_{N+1}$; $L =< m'_1, \ldots, m'_t >$ avec $\sum_{i=1}^t \deg m'_i \leq N+1$. Deux cas peuvent se présenter :
dans le premier on a $\deg m'_i \leq 1$ pour tout $i \in [1,t]$. Il suffit alors d'invoquer le 3. pour conclure que $h_{S/L} \in \mathcal{P}_\infty$.
Dans le second il existe $i_0 \in [1,t]$ tel que $\deg m'_{i_0} > 1$. Quitte à réordonner les m'_i, on peut supposer que $i_0 = 1$: $\deg m'_1 > 1$. En particulier il existe $j \in [1,r]$ tel que $X_j | m'_1$. Posons $J_L = (L : X_j)$ et $I'_L = L + < X_j >$. On est donc dans la situation du a. avec : I remplacé par L, m par X_j (ici $d = 1$), J par J_L, et I' par I'_L. Donc en appliquant ici le résultat de cette question on obtient la relation :

$$(*) \qquad h_{S/L}(n) = h_{S/J_L}(n-1) + h_{S/I'_L}(n).$$

Puisque $X_j | m'_1$ il est clair que $I'_L =< X_j, m'_2, \ldots, m'_t >$. De plus on a en fait : $\deg X_j = 1 < \deg m'_1$, donc :

$$\deg X_j + \sum_{i=2}^t \deg m'_i < \sum_{i=1}^t \deg m'_i \leq N+1,$$

soit :

$$\deg X_j + \sum_{i=2}^t \deg m'_i \leq N.$$

Il suffit donc d'appliquer l'hypothèse de récurrence pour prouver que $h_{S/I'_L} \in \mathcal{P}_\infty$.
Pour tout $i \in [1,t]$ on pose $m''_i = \frac{m'_i}{X_j}$ si $X_j | m'_i$ et $m''_i = m'_i$ sinon. On considère ensuite $J' =< m''_1, \ldots, m''_t >$. Il est clair que $J' \subset (L : X_j) = J_L$. Réciproquement considérons $P \in J_L$ et $\sum_{t \in T} \lambda_t p_t$ sa décomposition comme somme de ses termes. D'après 1.c., J_L est monômial donc pour tout $t \in T$, $p_t \in J_L : X_j p_t \in L$. Fixons $t_0 \in T$. D'après 1.a. il existe $i_1 \in [1,t]$ tel que $m'_{i_1} | X_j p_{t_0}$. Si $X_j | m'_{i_1}$ alors cela signifie exactement que $X_j m''_{i_1} | X_j p_{t_0}$ donc $m''_{i_1} | p_{t_0}$. Sinon X_j et m'_{i_1} sont premiers entre eux donc $m'_{i_1} | p_{t_0}$ (théorème de Gauss) c'est-à-dire exactement (dans ce cas) $m''_{i_1} | p_{t_0}$. Quelle que soit la situation on a donc montré que $p_{t_0} \in J'$. Puisque t_0 était quelconque cela assure que $P \in J'$ ce qui prouve que $J_L \subset J'$ et finalement $J_L = J'$.
Mais pour tout $i \in [1,t]$, $\deg m''_i \leq \deg m'_i$ et même $\deg m''_1 < \deg m'_1$ car $X_j | m'_1$. Donc $\sum_{i=1}^t \deg m''_i < \sum_{i=1}^t \deg m'_i \leq N+1$. Il suffit d'appliquer à nouveau l'hypothèse de récurrence pour obtenir que $h_{S/J'} \in \mathcal{P}_\infty$ c'est-à-dire $h_{S/J_L} \in \mathcal{P}_\infty$. Il est clair que $n \mapsto h_{S/J_L}(n-1)$ est alors aussi dans $\mathcal{P}_\infty$.
De la définition de $\mathcal{P}_\infty$ donnée au I. et de I.2.a. on tire facilement que $\mathcal{P}_\infty$ est un sous-anneau de $\mathcal{F}(\mathbb{Z}, \mathbb{Z})$ donc $(*)$ prouve que $h_{S/L} \in \mathcal{P}_\infty$, ce qui achève la récurrence.

5.a. On va d'abord montrer le lemme suivant : si I et J sont deux idéaux homogènes alors :

$$h_{S/I} + h_{S/J} = h_{S/(I \cap J)} + h_{S/(I+J)}.$$

En voici la preuve : si $n \in \mathbb{Z}$ on considère l'application linéaire φ ainsi définie

$$\begin{array}{rcl} I_n \bigoplus J_n & \to & S_n \\ (P,Q) & \mapsto & P+Q. \end{array}$$

Il est clair que $\mathrm{im}\varphi \subset (I+J)_n$ et réciproquement si $R \in (I+J)_n$ alors $R = \pi_n(R)$ car $R \in S_n$ et $R = P+Q$ avec $(P,Q) \in I \times J$ car $R \in I+J$. On a $R = \pi_n(P+Q) = \pi_n(P)+\pi_n(Q)$. Comme I et J sont homogènes, $\pi_n(P) \in I_n$ et $\pi_n(Q) \in J_n$. Ceci prouve que $R \in \mathrm{im}\varphi : (I+J)_n \subset \mathrm{im}\varphi$. Finalement $\mathrm{im}\varphi = (I+J)_n$ donc $\dim(\mathrm{im}(\varphi)) = \dim(I+J)_n$. Soit également l'application ψ :

$$\begin{array}{rcl} (I \cap J)_n & \to & I_n \bigoplus J_n \\ P & \mapsto & (P,-P). \end{array}$$

Il est évident que ψ est linéaire, que $\ker\psi = \{0\}$ et que $\mathrm{im}\psi \subset \ker\varphi$. Prenons donc (P,Q) dans $\ker\varphi$; $P+Q = 0$ donc il existe $R \in S$ tel que $(P,Q) = (R,-R)$. Puisque P et Q sont homogènes de degré n, $R \in S_n$. Puisque $(P,Q) \in I \times J$, $R \in I \cap J$. Donc $R \in (I \cap J)_n$. Enfin puisque $(P,Q) = (R,-R)$, $(P,Q) = \psi(R)$, ce qui prouve $\ker\varphi \subset \mathrm{im}\psi$ et donc $\mathrm{im}\psi = \ker\varphi$. Finalement ψ réalise un isomorphisme de $(I \cap J)_n$ sur $\ker\varphi$ donc $\dim\ker\varphi = \dim(I \cap J)_n$.
Comme $\dim(I_n \bigoplus J_n) = \dim I_n + \dim J_n$, l'application du théorème du rang à φ donne :

$$\dim I_n + \dim J_n = \dim(I \cap J)_n + \dim(I+J)_n.$$

On en déduit immédiatement que $(\dim S_n - \dim I_n) + (\dim S_n - \dim J_n)$ vaut :

$$(\dim S_n - \dim(I \cap J)_n) + (\dim S_n - \dim(I+J)_n).$$

Cela est exactement l'égalité que nous avons annoncée, spécialisée en n. Le lemme est donc démontré.
Posons à présent :

$$\begin{array}{rcl} I_0 & = & < X_1, \ldots, X_r >, \\ I_1 & = & < X_1, \ldots, X_s > \text{ et} \\ I_2 & = & < X_{s+1}, \ldots, X_r > . \end{array}$$

D'une part il est clair que $I_1 + I_2 = I_0$ et d'autre part si $(i,j) \in [1,s] \times [s+1,r]$, on a $\mathrm{ppcm}(X_i, X_j) = X_i X_j$ donc en reprenant la démonstration effectuée au 2. on constate que $I = I_1 \cap I_2$.
Notre lemme appliqué à I_1 et I_2 nous permet donc d'écrire que :

$$h_{S/I_1} + h_{S/I_2} = h_{S/I} + h_{S/I_0},$$

soit :

$$h_{S/I} = h_{S/I_1} + h_{S/I_2} - h_{S/I_0}.$$

On utilise le résultat de 3. pour estimer les trois termes de cette expression de $h_{S/I}$; si $n \in \mathbb{N}^*$, on a :

$$\begin{array}{rcl} h_{S/I_1}(n) & = & \binom{n+r+s-1}{r-s-1}, \\ h_{S/I_2}(n) & = & \binom{n+r-(r-s)-1}{r-(r-s)-1} \text{ et} \\ h_{S/I_0}(n) & = & 0. \end{array}$$

On obtient donc, avec les notations du I.3.a. :

$$h_{S/I}(n) = f_{r-s-1}(n+r-s-1) + f_{s-1}(n+s-1).$$

5.b. Introduisons $r = \sum_{j=1}^{p}(k_j+1)$ et pour tout $j \in [1,p]$, posons :

$$\mathcal{I}_j = [(\sum_{l=1}^{j-1}(k_l+1))+1, (\sum_{l=1}^{j}(k_l+1))].$$

On considère alors l'anneau de polynômes $S' = k[X_1,\ldots,X_r]$ et pour tout $j \in [1,p]$, l'idéal monômial I_j engendré par les monômes X_i pour $i \notin \mathcal{I}_j$. On définit enfin pour tout $j \in [1,p]$, l'idéal $I'_j = \cap_{l=1}^{j} I_j$. Alors on a pour tout $j \in [1,p]$ et pour tout $n \geq 1$:

$$\sum_{l=1}^{j} h_{S/I_l}(n) = h_{S/I'_j}(n).$$

Montrons le par récurrence sur j :
Si $j = 1$ il n'y a rien à démontrer.
Soit $j \in [1, p-1]$ et supposons que pour tout $n \geq 1$:

$$\sum_{l=1}^{j} h_{S/I_l}(n) = h_{S/I'_j}(n).$$

Appliquons le lemme démontré au a. aux idéaux I'_j et I_{j+1}. On obtient :

$$h_{S/I'_j} + h_{S/I_{j+1}} = h_{S/(I'_j \cap I_{j+1})} + h_{S/(I'_j + I_{j+1})}.$$

En utilisant l'hypothèse de récurrence et en remarquant que par définition on a $I'_j \cap I_{j+1} = I'_{j+1}$, il vient pour tout $n \geq 1$:

$$\sum_{l=1}^{j+1} h_{S/I_l}(n) = h_{S/I'_{j+1}}(n) + h_{S/(I'_j+I_{j+1})}(n).$$

Pour obtenir la propriété au rang $j+1$ il suffit d'avoir $h_{S/(I'_j+I_{j+1})}(n) = 0$ c'est-à-dire $(I'_j + I_{j+1})_n = S_n$ pour tout $n \geq 1$. C'est le cas car clairement $< \{X_i, i \in \mathcal{I}_{j+1}\} > \subset I'_j$ donc $< \{X_i, i \in [1,r]\} > \subset I'_j + I_{j+1}$. La récurrence est achevée.
Posons maintenant en particulier $I' = I'_p$. Ce qui précède prouve que pour tout $n \geq 1$:

$$h_{S/I'}(n) = \sum_{j=1}^{p} h_{S/I_j}(n).$$

Mais en utilisant 3. on peut calculer $h_{S/I_j}(n)$; si $n \geq 1$:

$$\begin{aligned} h_{S/I_j}(n) &= f_{r-(r-\mathrm{card}(\mathcal{I}_j))-1}(n+r-(r-\mathrm{card}(\mathcal{I}_j))-1) \\ &= f_{\mathrm{card}(\mathcal{I}_j)-1}(n+\mathrm{card}(\mathcal{I}_j)-1). \end{aligned}$$

Comme $\mathrm{card}(\mathcal{I}_j) = k_j+1$ ce nombre est $f_{k_j}(n+k_j)$. L'identité souhaitée ici sera donc vérifiée : il ne reste plus qu'à montrer que I' est monômial. Pour cela on constate d'abord que par définition I_j est monômial pour tout $j \in [1,p]$. On en déduit par une récurrence finie évidente basée sur le résultat de la question 2. que $\cap_{j=1}^{p} I_j$ est encore monômial. Mais cet idéal n'est autre que I' par définition, donc on a le résultat.

Le sens du mot "construire" n'est pas forcément tout à fait clair et peut-être attendait-on un système explicite de générateurs monômiaux pour I'. Le lecteur se convaincra facilement qu'un tel système est (par exemple) l'ensemble des $X_i X_{i'}$ vérifiant cette propriété : si j est tel que $i \in \mathcal{I}_j$, alors $i' \notin \mathcal{I}_j$.

6.a. Remarque : on suppose dans toute cette question que l'ordre lexicographique est en effet un ordre, ce que semble admettre implicitement l'énoncé par le choix de cette terminologie.
Puisque $m = m$ on a $m \geq m$, et donc $\geq$ est une relation réflexive.
Soient m et m' tels que $m \geq m'$ et $m' \geq m$. De $m \geq m'$ on tire $\deg m \geq \deg m'$, et de $m' \geq m$ on tire $\deg m' \geq \deg m$, donc $\deg m = \deg m'$. On obtient alors $(\alpha_1, \ldots, \alpha_r) \geq (\alpha'_1, \ldots, \alpha'_r)$ et $(\alpha'_1, \ldots, \alpha'_r) \geq (\alpha_1, \ldots, \alpha_r)$ pour l'ordre lexicographique. L'antisymétrie de cet ordre prouve alors que $(\alpha_1, \ldots, \alpha_r) = (\alpha'_1, \ldots, \alpha'_r)$ d'où $m = m'$ ce qui prouve que $\geq$ est une relation antisymétrique.
Soient m, m', et m'' tels que $m \geq m'$ et $m' \geq m''$. Si $\deg m > \deg m''$ alors on a bien $m \geq m''$. Sinon $\deg m \leq \deg m''$. Mais on sait que $\deg m \geq \deg m'$ (car $m \geq m'$) et de même $\deg m' \geq \deg m''$. Donc dans ce cas $\deg m = \deg m' = \deg m''$. Il suffit alors d'invoquer la transitivité de l'ordre lexicographique pour obtenir celle de $\geq$.
Tout ceci prouve que $\geq$ est une relation d'ordre.
Pour montrer que cet un ordre total, on prend deux monômes m et m' et il s'agit de montrer qu'ils sont comparables :
Si $m = m'$ alors $m \geq m'$ (par exemple). Donc on peut supposer $m \neq m'$.
Si $\deg m \neq \deg m'$, alors $\deg m > \deg m'$ ou $\deg m' > \deg m$. Dans le premier cas $m \geq m'$, et dans le second $m' \geq m$. On peut donc supposer que $\deg m = \deg m'$.
Puisque $m \neq m'$, $\{i \in [1, r], \alpha_i \neq \alpha'_i\}$ est non vide. On peut donc en considérer le plus petit élément i_0. On a alors $\alpha_{i_0} > \alpha'_{i_0}$ ou $\alpha'_{i_0} > \alpha_{i_0}$. Dans le premier cas $m \geq m'$, et dans le second $m' \geq m$. (On vient juste de réexpliquer pourquoi l'ordre lexicographique est total.)

6.b. Supposons que $mm'' = m'm''$. Alors $(m - m')m'' = 0$. Comme $m'' \neq 0$, $m = m'$. Absurde car $m > m'$. Donc $mm'' \neq m'm''$. Supposons que $m'm'' = m'$. Alors $m'(m'' - 1) = 0$. Comme $m' \neq 0$ et $m'' \neq 1$, ceci aussi est absurde, et $m'm'' \neq m'$. Il suffit donc de montrer que $mm'' \geq m'm'' \geq m'$:

(i) Comme $m'' \neq 1$, $\deg m'' \geq 1$ d'où $\deg(m'm'') = \deg m' + \deg m'' > \deg m'$. Cela prouve que $m'm'' \geq m'$.

(ii) On a $m > m'$, donc deux cas peuvent se présenter : soit on a $\deg m > \deg m'$, soit on a $\deg m = \deg m'$ et si $i_0 = \min\{i \in [1, r], \alpha_i \neq \alpha'_i\}$ (qui existe car $m \neq m'$), $\alpha_{i_0} > \alpha'_{i_0}$. Dans le premier cas $\deg(mm'') = \deg m + \deg m'' > \deg m' + \deg m'' = \deg(m'm'')$, donc $mm'' \geq m'm''$. Dans le second on écrit $mm'' = X_1^{\alpha_1 + \alpha''_1} \ldots X_r^{\alpha_r + \alpha''_r}$ et $m'm'' = X_1^{\alpha'_1 + \alpha''_1} \ldots X_r^{\alpha'_r + \alpha''_r}$. On a $\deg(mm'') = \deg(m'm'')$ et :

$$i_0 = \min\{i \in [1, r], \alpha_i + \alpha''_i \neq \alpha'_i + \alpha''_i\},$$

avec $\alpha_{i_0} + \alpha''_{i_0} > \alpha'_{i_0} + \alpha''_{i_0}$. Donc $mm'' \geq m'm''$.

6.c. Soit M un ensemble non vide de monômes. Considérons l'ensemble suivant :

$$D_M = \{\deg m,\ m \in M\}.$$

D_M est un ensemble non vide d'entiers naturels donc on peut en considérer le plus petit élément d_M : pour tout $m \in M$, deg$m \geq d_M$ et $M' = \{m \in M,\ \text{deg}m = d_M\}$ est non vide. On définit ensuite récursivement $M_0, \ldots, M_r$ de la manière suivante : $M_0 = M'$ et :

$$M_{i+1} = \{m \in M_i,\ \alpha_{i+1} = \min\{\alpha'_{i+1},\ m' \in M_i\}\}.$$

Il est facile de vérifier (récursivement) que l'on a ainsi construit une suite décroissante d'ensembles non vides. Soit $m_r \in M_r$. On note :

$$m_r = X_1^{(\alpha_r)_1} \ldots X_r^{(\alpha_r)_r}.$$

Alors m_r est un (donc le) plus petit élément de M. En effet si $m \in M$, il suffit de montrer que $m \geq m_r$. Deux cas peuvent se présenter : soit $m \notin M'$, et donc deg$m >$ degm_r, d'où $m \geq m_r$, soit $m \in M'$. Si dans ce cas $m = m_r$, il n'y a rien à montrer, donc on peut supposer que $m \neq m_r$. Alors il existe $i_0 = \min \{i \in [1, r], \alpha_i \neq (\alpha_r)_i\}$. Puisque deg$m =$ degm_r, il suffit de vérifier que $\alpha_{i_0} > (\alpha_r)_{i_0}$. Pour cela on montre (récursivement) que $m \in M_{i_0-1}$. ($m \in M' = M_0$, puis si $m \in M_i$ avec $i \in [1, i_0 - 2]$ alors $i + 1 \leq i_0 - 1$ donc $\alpha_{i+1} = (\alpha_r)_{i+1}$. Comme $m_r \in M_{i+1}$, cela prouve que $m \in M_{i+1}$ également.) Maintenant comme $m_r \in M_{i_0}$, $m \in M_{i_0-1}$ force $\alpha_{i_0} \geq (\alpha_r)_{i_0}$. Puisque $\alpha_{i_0} \neq (\alpha_r)_{i_0}$, $\alpha_{i_0} > (\alpha_r)_{i_0}$.

6.d. Fixons un monôme m. Alors $m > m'$ entraîne deg$m \geq$ degm' donc $\{m',\ m > m'\} \subset \{m',\ \text{deg}m' \leq \text{deg}m\}$. Mais il est clair qu'il n'y a qu'un nombre fini de monômes qui ont un degré n donné (ce nombre vaut dimS_n), donc seul un nombre fini de monômes ont un degré inférieur à celui de m, ce qui assure le résultat demandé.

8.a. Soit $m \in J$ un monôme. Puisque $m \in J$, il existe $(P_1, \ldots, P_s) \in S^s$ et $(Q_1, \ldots, Q_s) \in I^s$ tels que $m = \sum_{i=1}^s P_i \text{in}Q_i$. Quitte à multiplier les P_i par des constantes on peut supposer que les inQ_i sont des monômes. Posons donc $m_i = \text{in}Q_i$. Alors $m \in < m_1, \ldots, m_s >$. D'après 1.a., il existe i_0 tel que $m_{i_0} | m$. Posons $m'_{i_0} = \frac{m}{m_{i_0}}$ et considérons $Q'_{i_0} = m'_{i_0} Q_{i_0}$. Puisque $Q_{i_0} \in I$, $Q'_{i_0} \in I$. Montrons que son terme initial est m (ce qui prouvera le résultat demandé) : soit m' un monôme de Q_{i_0} différent de m_{i_0} : alors $m_{i_0} > m'$. Si $m'_{i_0} \neq 1$, on tire de 6.b. que $m'_{i_0} m_{i_0} > m'_{i_0} m'$. Comme l'ensemble des monômes associés aux termes de Q'_{i_0} est $\{m'_{i_0} m', m'$ monôme associé à un terme de $Q_{i_0}\}$, on en déduit que $m'_{i_0} m_{i_0}$ est le terme initial de Q'_{i_0}. Il est clair que ce résultat est encore vrai si $m'_{i_0} = 1$. Enfin $m'_{i_0} m_{i_0} = m$, donc on a le résultat.

8.b. Remarque : en notant in$(P - \text{in}P) <$ in$P$, l'auteur du problème confond abusivement termes et monômes associés. Il a raison de le faire, et à partir de maintenant nous ferons de même le cas échéant ! Ceci dit cette question est facile : en effet $(P - \text{in}P)$ est non nul ; si m est un terme quelconque de $(P - \text{in}P)$ c'est aussi un terme de P, donc on a in$P \geq m$. De plus in$P$ n'est pas un terme de $(P - \text{in}P)$ donc in$P \neq m$. Ceci prouve que in$P > m$. Il suffit alors de considérer $m = \text{in}(P - \text{in}P)$, qui est en particulier un terme de $(P - \text{in}P)$.

8.c. Supposons que $\mathcal{M}'$ ne soit pas un système libre du k-espace vectoriel S/I. On peut donc trouver une combinaison linéaire nulle mais non triviale entre éléments de $\mathcal{M}'$: il existe $(\lambda_1, \ldots, \lambda_s) \in (k^*)^s$, $(m'_1, \ldots, m'_s) \in \mathcal{M}'^s$ (tous distincts) tels que $\sum_{i=1}^s \lambda_i m'_i = 0_{S/I}$. Soit $(m_1, \ldots, m_s) \in \mathcal{M}^s$ tel que pour tout $i \in [1, s]$, $m'_i = \overline{m_i}$ où $\overline{P}$ désigne la classe de $P \in S$, dans S/I. On a alors

$\sum_{i=1}^{s} \lambda_i m'_i = \sum_{i=1}^{s} \lambda_i \overline{m_i} = \overline{\sum_{i=1}^{s} \lambda_i m_i}$ donc $\overline{\sum_{i=1}^{s} \lambda_i m_i} = 0_{S/I}$. Ceci prouve que $P = \sum_{i=1}^{s} \lambda_i m_i \in I$. Il est facile de montrer récursivement, en utilisant 6.c., que l'on peut réindexer les m_i de manière à avoir $m_s \geq m_{s-1} \geq \dots m_1$ (on commence par choisir le plus petit d'entre eux, qui deviendra m_1, puis à chaque étape on choisit le plus petit de ceux qui restent). De plus puisque les m'_i sont distincts, les m_i le sont également. Donc en fait $m_s > m_{s-1} > \dots > m_1$. Ceci prouve que $\lambda_s m_s = \text{in}P$. Or puisque les m_i (qui sont libres dans S) sont distincts et les λ_i non nuls, $P \neq 0$. Donc $\lambda_s m_s \in J$, d'où $m_s \in J$. Mais $m_s \in \mathcal{M}$ donc $m_s \notin J$. C'est absurde donc $\mathcal{M}'$ est un système libre de S/I.

8.d. Montrons par l'absurde le résultat suivant : pour tout monôme $m \in S$, il existe $(m_1, \dots, m_s) \in \mathcal{M}^s$, $(\lambda_1, \dots, \lambda_s) \in (k)^s$ et $P \in I$ tels que :

$$m = \sum_{i=1}^{s} \lambda_i m_i + P.$$

Si c'est faux on considère le plus petit élément m_0, de ceux qui ne vérifient pas cette propriété (ce que l'on peut faire grâce au 6.c.). On ne peut pas avoir $m_0 \in \mathcal{M}$ sinon il suffirait d'écrire $m_0 = m_0$ pour obtenir une décomposition de m_0 de la forme voulue. Donc $m_0 \in J$. D'après a., il existe $Q \in I$ tel que $m_0 = \text{in}Q$. On peut encore écrire que $m_0 = -(Q - \text{in}Q) + Q$. Si $Q = \text{in}Q$ alors $m_0 = Q$ ce qui est absurde car c'est une décomposition de la forme voulue. Donc $Q \neq \text{in}Q$ et d'après b., $\text{in}(Q - \text{in}Q) < \text{in}Q$. Donc $\text{in}(Q - \text{in}Q) < m_0$. Par définition de m_0 cela prouve que tout monôme associé à un terme de $\text{in}(Q - \text{in}Q)$ admet une décomposition de la forme voulue. Il suffit alors de reporter ces décompositions dans l'expression $-(Q - \text{in}Q) + Q$ pour en obtenir une de m_0 ce qui est absurde. Donc pour tout monôme m de S, on peut écrire $m = \sum_{i=1}^{s} \lambda_i m_i + P$ où pour tout $i \in [\![1, s]\!]$, $m_i \in \mathcal{M}$ et $P \in I$. On en déduit que $\overline{m} = \sum_{i=1}^{s} \lambda_i \overline{m_i} + \overline{P} = \sum_{i=1}^{s} \lambda_i \overline{m_i}$ car $\overline{P} = 0$. Ceci prouve que le système $\mathcal{M}'$ engendre la famille suivante :

$$\{\overline{m},\ m \text{ monôme de } S\}.$$

Or la famille $\{m,\ m \text{ monôme de } S\}$ est une base de S donc $\{\overline{m},\ m \text{ monôme de } S\}$ est une famille génératrice de S/I. Donc le système $\mathcal{M}'$ est à son tour générateur de S/I. En joignant ce résultat à celui du c., on obtient que $\mathcal{M}'$ est une base de S/I.

8.e. Fixons $n \in \mathbb{Z}$ et introduisons les notations suivantes :
$\mathcal{M}_n = \{m \in \mathcal{M} \text{ tel que } \deg m = n\}$, $\overline{P}^n$ désigne la projection de $P \in S_n$ sur I_n, et $\mathcal{M}'_n = \{\overline{m}^n,\ m \in \mathcal{M}_n\}$. Montrons que $\mathcal{M}'_n$ est une base de S_n/I_n.
C'est une famille libre : si $\overline{m_1}^n, \dots, \overline{m_s}^n$ sont des éléments distincts de $\mathcal{M}'_n$ et si $(\lambda_1, \dots, \lambda_s) \in (k)^s$ vérifie $\sum_{i=1}^{s} \lambda_i \overline{m_i}^n = 0_{(S_n/I_n)}$ alors $\sum_{i=1}^{s} \lambda_i m_i \in I_n \subset I$ donc $\sum_{i=1}^{s} \lambda_i \overline{m_i} = 0_{S/I}$. Mais les $\overline{m_i}$ sont distincts dans $\mathcal{M}'$: sinon il existe $i \neq j$ avec $\overline{m_i} = \overline{m_j}$, donc $m_i - m_j \in I$. Puisque $m_i \neq m_j$ (car $\overline{m_i}^n \neq \overline{m_j}^n$) $\text{in}(m_i - m_j)$ est m_i ou $-m_j$, et appartient à J. Donc $m_i \in J$ ou $m_j \in J$. Ceci est absurde car ce sont des éléments de $\mathcal{M}$. On est donc en position d'appliquer le résultat de c. pour obtenir la nullité de tous les λ_i.
C'est une famille génératrice ; pour le montrer nous partons d'un élément quelconque de S_n/I_n. Il peut s'écrire $\overline{P}^n$ avec $P \in S_n$. Nous considèrons $\overline{P} \in S/I$. On sait que $P = \sum_{i=1}^{s} \lambda_i \overline{m_i}$ où les $\overline{m_i} \in \mathcal{M}$, car d'après d. $\mathcal{M}$ est génératrice

de S/I. Cela signifie que $P = \sum_{i=1}^{s} \lambda_i m_i + Q$ avec $Q \in I$. Donc :

$$\pi_n(P) = \sum_{i=1}^{s} \lambda_i \pi_n(m_i) + \pi_n(Q).$$

Comme $P \in S_n$ on a en fait $P = \sum_{i=1}^{s} \lambda_i \pi_n(m_i) + \pi_n(Q)$. De plus I est un idéal homogène donc d'après III.1.a., $\pi_n(Q) \in I_n$. Notre égalité passe donc au quotient de la manière suivante :

$$\overline{P}^n = \sum_{i=1}^{s} \lambda_i \overline{\pi_n(m_i)}^n.$$

Or pour tout i dans $[1, s]$, $\pi_n(m_i) = 0$ ou m_i. Donc les $\overline{\pi_n(m_i)}^n$ sont soit nuls, soit des éléments de $\mathcal{M}'_n$ ce qui prouve la propriété annoncée.
On déduit de tout ceci que $\dim(S_n/I_n) = \text{card}\ \mathcal{M}'_n$, donc $h_{S/I}(n) = \text{card}(\mathcal{M}'_n)$.
Considérons maintenant $(m, m') \in (\mathcal{M}_n)^2$ tel que $\overline{m}^n = \overline{m'}^n$. Alors $m - m' \in I_n \subset I$. Si $m \neq m'$ on a déjà expliqué qu'on obtient une absurdité, donc $m = m'$. Ceci prouve que $\text{card}(\mathcal{M}_n) = \text{card}(\mathcal{M}'_n)$, dont on tire qu'en fait $h_{S/I}(n) = \text{card}(\mathcal{M}_n)$.
$\mathcal{M}_n$ est l'ensemble des monômes de degré n qui n'appartiennent pas à J. Nous appelons alors $\mathcal{M}''_n$ l'ensemble des monômes de degré n qui appartiennent à J. Il est clair que $\mathcal{M}_n \cup \mathcal{M}''_n$ est une base de S_n, et qu'il s'agit d'une union disjointe. Donc $\text{card}(\mathcal{M}_n) + \text{card}(\mathcal{M}''_n) = \dim S_n$, c'est-à-dire qu'en fait on dispose de l'égalité : $\text{card}(\mathcal{M}_n) = \dim S_n - \text{card}(\mathcal{M}''_n)$.
Montrons que $\mathcal{M}''_n$ est une base de J_n.

D'abord c'est une famille libre car elle est composée de monômes.

Ensuite c'est une famille génératrice : soit $P \in J_n$ et $\sum_{t \in T} \lambda_t p_t$ sa décomposition en somme de ses termes. Pour tout $t \in T$, $\deg p_t = n$ car $P \in S_n$. De plus $P \in J$ donc pour tout $t \in T$, $p_t \in J$ d'après 1.b. car J est monômial. (Remarque : en toute rigueur pour appliquer les résultats de 1. ou 4., il faudrait que J soit engendré par un nombre fini de monômes, mais on sait qu'en fait c'est le cas car S est noethérien.) Donc pour tout $t \in T$, $p_t \in J_n$, d'où $p_t \in \mathcal{M}''_n$. En particulier on en déduit que $\text{card}(\mathcal{M}''_n) = \dim J_n$.
Donc en fait $\text{card}(\mathcal{M}_n) = \dim S_n - \dim J_n = \dim(S_n/J_n) = h_{S/J}(n)$.
Finalement on a obtenu que $h_{S/I}(n) = h_{S/J}(n)$. Comme cette relation est vraie pour tout n, $h_{S/I} = h_{S/J}$. On conclut en remarquant que puisque J est monômial on a d'après 4.b. (cf remarque précédente), $h_{S/J} \in \mathcal{P}_\infty$.

9.3 Commentaires

Ce problème se fixe l'objectif de démontrer un célèbre théorème de Hilbert après avoir familiarisé le candidat avec les notions relatives à son énoncé et à sa signification :

Si I est un idéal homogène de $\mathbb{K}[X_1, \ldots, X_r]$ et si pour tout entier n, $h_I(n)$ désigne la codimension de I_n (i.e. les éléments homogènes de degré n de I) dans $(\mathbb{K}[X_1, \ldots, X_r])_n$ (i.e. les éléments homogènes de degré n dans $\mathbb{K}[X_1, \ldots, X_r]$) alors la fonction h_I est polynomiale pour n grand.

Précisons que le polynôme en question est appelé traditionnellement polynôme de Hilbert de l'idéal I par les géomètres algébristes.

En conséquence, cette épreuve est à la fois longue et difficile. Si dans un premier temps une certaine aisance dans les calculs et le raisonnement par récurrence peut suffire face à des polynômes en une variable et à valeurs entières (première partie), très vite (surtout à partir de la troisième partie) une bonne familiarité avec les anneaux de polynômes à plusieurs variables devient nécessaire. Le maniement des idéaux et des "relations" dans de tels anneaux est mis en jeu à chaque question, parfois de façon assez technique. On notera aussi une utilisation intéressante et variée des outils d'algèbre linéaire autour de la notion de dimension (base, théorème du rang,...). En résumé, il s'agit d'un beau sujet d'algèbre (commutative) qui ravira les amateurs en testant leurs connaissances, les poussant à plusieurs reprises à une véritable recherche et vraisemblablement en les instruisant, spécialement dans les deux dernières parties. Un petit regret tout de même en forme d'avertissement pour le lecteur : une erreur subtile (déstabilisante le jour du concours) s'est glissée dans l'avant-dernière partie du sujet.

Chapitre 10

Session de 1998

10.1 Sujet

10.2 Correction

I.

1. Construisons la suite $(i_n)_{n\in\mathbb{N}}$ par récurrence.
On prend i_0 quelconque dans I.
Supposons avoir construit $i_0, \ldots, i_n$: soit O le centre de C_{i_n}. Comme $(C_i)_{i\in I}$ est une partition de $\mathcal{E}$, il existe un unique $j \in I$ tel que $O \in C_j$. On a alors $C_j \subset D_{i_n}$. En effet $C_j \cap C_{i_n} = \emptyset$ c'est à dire $C_j \subset \mathcal{E} - C_{i_n}$ et comme C_j est connexe, C_j est inclus dans l'une des deux composantes connexes de $\mathcal{E} - C_{i_n}$. Puisque $O \in C_j$, on a $C_j \subset D_{i_n}$ ce qui entraîne $D_j \subset D_{i_n}$. Soit O' le point de C_j diamétralement opposé à O : $\|O - O'\| = 2r_j < r_{i_n}$ car $O' \in D_{i_n}$. On prend alors $i_{n+1} = j$.

2. Il s'agit d'une intersection décroissante de fermés non vides dont le diamètre tend vers 0 (on montre facilement par récurrence que pour tout $n \geq 0$, $r_{i_n} \leq 2^{-n} r_{i_0}$) dans un espace complet. D'après le théorème des fermés emboîtés, on sait que $\cap_{n\in\mathbb{N}} D_{i_n}$ est un singleton $\{P\}$.

Remarque : on utilisera dans la suite le résultat élémentaire suivant : soient deux cercles distincts C et C', de centres respectifs O et O' et de rayons respectifs R et R'. Ils sont d'intersection non vide si et seulement si

$$|R - R'| \leq \|O - O'\| \leq R + R'.$$

Dans le cas où $C \cap C' \neq \emptyset$, cette intersection est réduite à un point si une des deux inégalités précédentes est une égalité et cette intersection est réduite à deux points si les deux inégalités sont strictes.

3. Soit j l'unique élément de I tel que $P \in C_j$. On peut considérer $n \in \mathbb{N}$ tel que $r_{i_n} < r_j$. Soit O_j le centre de C_j et O_{i_n} le centre de C_{i_n}. On a $\|O_j - O_{i_n}\| = \|O_j - P + P - O_{i_n}\|$ et comme $\|P - O_{i_n}\| \leq r_{i_n} < r_j$ (on se souvient que $P \in D_{i_n}$) alors

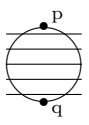
$$r_j - r_{i_n} \leq \|O_j - O_{i_n}\| \leq r_j + r_{i_n}.$$

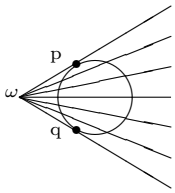
D'après la remarque, $C_j \cap C_{i_n} \neq \emptyset$, ce qui est absurde car $j \neq i_n$.

Finalement, on conclut qu'on ne peut pas recouvrir $\mathcal{E}$ par une famille de cercles disjoints.

II.

1.





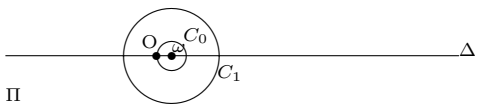
Distinguons deux cas.

Si p et q sont diamétralement opposés, on considère les cordes de longueur non nulles de D perpendiculaires à la droite (p,q). Tout point M de $D-\{p,q\}$ est dans une telle corde (il suffit de considérer la droite passant par M perpendiculaire à (p,q)). De plus, deux telles cordes distinctes sont strictement parallèles donc disjointes d'où le résultat.
Si p et q ne sont pas diamétralement opposés, les tangentes en p et q à C sont sécantes en un point ω. Considérons l'ensemble $\mathcal{L}$ des cordes de D non réduites à un point supportées par des droites passant par ω. Cet ensemble est une partition de $D-\{p,q\}$ car :

- il ne contient ni p ni q car (ωp) et (ωq) sont tangentes au cercle C,
- si $m \in D-\{p,q\}$, la droite (ωm) coupe C en deux points distincts donc la corde $D \cap (\omega m)$ appartient à $\mathcal{L}$,
- deux éléments distincts de $\mathcal{L}$ sont disjoints car supportés par des droites distinctes sécantes en $\omega \notin D$.

2. Considérons Π un plan contenant le centre de S, p et q (ce plan est unique lorsque p et q ne sont pas diamétralement opposés). On projette orthogonalement $S-\{p,q\}$ sur Π : on obtient un disque D de centre O de diamètre le diamètre de S, privé des points p et q. Grâce à 1., on trouve une partition de D en segments de droite de longueur non nulle (contenus dans Π). Les images réciproques de ces segments par la projection orthogonale tracent sur la sphère des cercles et il est clair que la famille formée par ces cercles convient.

3. L'énoncé suggérait de choisir une famille indexée par $\mathbb{Z}$, comme, par exemple la famille de cercles de rayon 1 centrés en $1+4n$ où $n \in \mathbb{Z}$. Nous proposons une autre solution, nécessitant également un nombre dénombrable de cercles.



Soit Π un plan qui contient Δ et ω un point de Δ tel que $\|\omega - O\| = 1$. Considérons la famille $(C_n)_{n\in\mathbb{N}}$ suivante : C_n est le cercle de centre ω, de rayon $r_n = 1+2n$, inclus dans Π.

Soit $r > 0$. Il existe un et un seul $n \in \mathbb{N}$ tel que $2n < r \leq 2(n+1)$. Distinguons deux cas.
Si $2n < r < 2(n+1)$: si $i < n$ ou si $i \geq n+1$, il est clair que $|r-r_i| > 1 = \|\omega - O\|$ donc $S(O,r) \cap C_i = \emptyset$. Si $i = n$, $|r-r_n| < 1$ donc $S(O,r) \cap C_n$ est un doubleton.
Si $r = 2(n+1)$: si $i < n$ ou si $i > n+1$, il est clair que $|r-r_i| > 1 = \|\omega - O\|$ donc $S(O,r) \cap C_i = \emptyset$. Sinon $|r-r_n| = 1$ et $|r-r_{n+1}| = 1$ donc $S(O,r) \cap C_n$ est réduit à un point appartenant à C_n et $S(O,r) \cap C_{n+1}$ est réduit à un point appartenant à C_{n+1}.

Dans tous les cas, on en conclut que $S(O,r) \bigcap \big(\bigcup_{n\in\mathbb{N}} C_n \big)$ est un doubleton.

4. Conservons les notations de la question 3. Pour tout $r > 0$,

$$S(O,r) \bigcap \big(\bigcup_{n\in\mathbb{N}} C_n \big) = \{p_r, q_r\}.$$

D'après 2., on peut recouvrir $S(O,r) - \{p_r, q_r\}$ par une famille $\hat{\mathcal{C}}_r$ de cercles disjoints. Les cercles de $\hat{\mathcal{C}}_r$ sont disjoints des C_m ($m \geq 0$) car p_r et q_r sont les deux seuls points d'intersection de $S(O,r)$ et de $\cup_{n\in\mathbb{N}} C_n$. De plus, pour $r \neq r'$, $\hat{\mathcal{C}}_r$ et $\hat{\mathcal{C}}_{r'}$ sont disjointes car $S(O,r) \cap S(O,r') = \emptyset$. Enfin, on note que $O \in C_0$ et que $\mathcal{E} - \{O\} = \bigcup_{r>0} S(O,r)$ donc $\mathcal{E}$ est recouvert par la famille de cercles disjoints

$$\bigcup_{r>0} \hat{\mathcal{C}}_r \cup \Big(\bigcup_{n\in\mathbb{N}} C_n\Big).$$

III.

On notera $\mathcal{E} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$; $\mathrm{Mat}_\beta(x_1, \ldots, x_n)$ la matrice dont les vecteurs colonnes sont les coordonnées des vecteurs $x_1, \ldots, x_n$ dans la base β ; $\mathrm{Mat}(f, \beta, \beta')$ la matrice représentative de l'applicaton linéaire f dans les bases β et β'.

1. Pour $1 \leq i \leq n$, notons $Me_i = e'_i$. Comme $M \in \mathrm{GL}_n(\mathbb{R})$, $\mathcal{E}' = (e'_1, \ldots, e'_n)$ est une base de $\mathbb{R}^n$. Orthonormalisons cette base pour le produit scalaire usuel sur $\mathbb{R}^n$: on obtient une base orthonormée $\mathcal{E}'' = (e''_1, \ldots, e''_n)$ et on a immédiatement par récurrence $\mathrm{Vect}(e''_1, \ldots, e''_i) = \mathrm{Vect}(e'_1, \ldots, e'_i)$ pour tout $i = 1, \ldots, n$. Il en résulte que $T_1 = \mathrm{Mat}_{\mathcal{E}''}(e'_1, \ldots, e'_n)$ est triangulaire supérieure. Comme $\mathcal{E}''$ est orthonormée, les coefficients diagonaux de T_1 sont égaux à $\langle e'_i, e''_i \rangle > 0$. On a alors

$$\begin{aligned} M = \mathrm{Mat}(\mathrm{I}, \mathcal{E}', \mathcal{E}) &= \mathrm{Mat}(\mathrm{I}, \mathcal{E}'', \mathcal{E})\,\mathrm{Mat}(\mathrm{I}, \mathcal{E}', \mathcal{E}'') \\ &= \mathrm{Mat}(\mathrm{I}, \mathcal{E}'', \mathcal{E})\,T_1. \end{aligned}$$

Soit $K = \mathrm{Mat}(\mathrm{I}, \mathcal{E}'', \mathcal{E})$: K est la matrice de passage d'une base orthonormée de $\mathbb{R}^n$ vers une autre base orthonormée donc K est orthogonale. D'autre part, si les t_{ii} désignent les coefficients diagonaux de T_1 et $D = \mathrm{diag}(t_{11}, \ldots, t_{nn})$ alors on peut écrire $T_1 = DT$ donc (la ligne i de T est $\frac{1}{t_{ii}}$ fois la ligne i de T_1) $M = KDT$ où T est triangulaire supérieure avec des 1 sur la diagonale.
Montrons l'unicité d'une telle décomposition. Supposons disposer de K_1, $K_2 \in O_n(\mathbb{R})$, D_1, D_2 diagonales à éléments diagonaux strictement positifs (en particulier inversibles) et T_1, T_2 triangulaires supérieures avec des 1 sur la diagonale telles que $K_1 D_1 T_1 = K_2 D_2 T_2$ alors on a

$$K_2^{-1} K_1 = D_2 T_2 T_1^{-1} D_1^{-1},$$

avec $K_2^{-1} K_1$ orthogonale, et on remarque que $D_2 T_2 T_1^{-1} D_1^{-1}$ est triangulaire supérieure à éléments diagonaux positifs. Comme la seule matrice orthogonale et triangulaire supérieure à éléments diagonaux positifs est l'identité, $K_2^{-1} K_1 = D_2 T_2 T_1^{-1} D_1^{-1} = \mathrm{I}$ ce qui prouve que $K_1 = K_2$ et $D_1 T_1 = D_2 T_2$. Les coefficients diagonaux de $D_1 T_1$ sont ceux de D_1, les coefficients diagonaux de $D_2 T_2$ sont ceux de D_2 donc $D_1 = D_2$. Comme D_1 est inversible, on a $T_1 = T_2$.

2. Si $M \in \mathrm{GL}_n(\mathbb{Z})$ alors $\det M \in \mathbb{Z}$ et $\det M^{-1} \in \mathbb{Z}$ car M et M^{-1} sont à coefficients entiers. Or $\det M \det M^{-1} = 1$ donc $\det M$ est inversible dans $\mathbb{Z}$ et nécessairement, $\det M \in \{-1, 1\}$.

Réciproquement, si $M \in M_n(\mathbb{Z})$ et $\det M \in \{-1, 1\}$ alors les cofacteurs de M sont entiers et comme $\det M$ est inversible dans $\mathbb{Z}$, la matrice $M^{-1} = \dfrac{1}{\det M}\, {}^t\mathrm{com}M$ est à coefficients entiers et $M \in \mathrm{GL}_n(\mathbb{Z})$.

3. Il existe une structure de groupe sur $\mathcal{H}_n$ faisant de π_n un homomorphisme de groupes si et seulement si $\mathrm{GL}_n(\mathbb{Z})$ est distingué dans $\mathrm{GL}_n(\mathbb{R})$. C'est clairement le cas si $n = 1$ mais ce n'est plus vrai pour $n \geq 2$ comme le montre l'exemple suivant : pour $n = 2$, on a

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1/2 \\ 2 & 0 \end{pmatrix} \notin \mathrm{GL}_2(\mathbb{Z}).$$

Pour $n \geq 3$, il suffit de considérer les matrices définies par bloc :

$$\begin{pmatrix} 2 & 0 & \\ 0 & 1 & 0 \\ & 0 & I_{n-2} \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 & \\ 1 & 0 & 0 \\ & 0 & I_{n-2} \end{pmatrix}.$$

4. Appelons ψ cette application. Pour $M \in \mathrm{GL}_n(\mathbb{R})$, il est clair que $M(\mathbb{Z}^n)$ est le réseau dont une base est $(Me_1, \ldots, Me_n)$ car

$$M(a_1, \ldots, a_n) = M(\sum_{i=1}^{n} a_i e_i) = \sum_{i=1}^{n} a_i M(e_i).$$

Si Γ est un réseau de base $(f_1, \ldots, f_n)$, il suffit de considérer la matrice M dont les colonnes sont les f_i pour obtenir $\psi(M) = \Gamma$: ψ est surjective.

On sait aussi qu'en définissant la relation $\mathcal{R}$ sur $\mathrm{GL}_n(\mathbb{R})$ de la façon suivante :

$$M\mathcal{R}M' \text{ si et seulement si } M(\mathbb{Z}^n) = M'(\mathbb{Z}^n),$$

on peut factoriser ψ en une injection $\overline{\psi}$ de $\mathrm{GL}_n(\mathbb{R})/\mathcal{R}$ qui a même image que ψ définie par $\overline{\psi}([M]_{\mathcal{R}}) = \psi(M)$.
Il suffit donc de montrer que $\mathrm{GL}_n(\mathbb{R})/\mathcal{R} = \mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z})$, c'est à dire

$$M(\mathbb{Z}^n) = M'(\mathbb{Z}^n) \Longleftrightarrow \exists A \in \mathrm{GL}_n(\mathbb{Z}), M = M'A.$$

Mais $M(\mathbb{Z}^n) = M'(\mathbb{Z}^n)$ si et seulement si $M'^{-1}M(\mathbb{Z}^n) = \mathbb{Z}^n$ car M' est bijective. Il suffit alors de prouver que si $A \in \mathrm{GL}_n(\mathbb{R})$, $A(\mathbb{Z}^n) = \mathbb{Z}^n$ si et seulement si $A \in \mathrm{GL}_n(\mathbb{Z})$.
Supposons que $A(\mathbb{Z}^n) = \mathbb{Z}^n$ avec $A \in \mathrm{GL}_n(\mathbb{R})$. Alors il est clair que $A \in M_n(\mathbb{Z})$: en effet, les vecteurs colonnes de A sont les images de vecteurs de $\mathbb{Z}^n$ donc sont dans $\mathbb{Z}^n$. D'autre part, on a aussi $\mathbb{Z}^n = A^{-1}(\mathbb{Z}^n)$ donc $A^{-1} \in M_n(\mathbb{Z})$ et $A \in \mathrm{GL}_n(\mathbb{Z})$.
Réciproquement si $A \in \mathrm{GL}_n(\mathbb{Z})$, il est clair que $A(\mathbb{Z}^n) \subset \mathbb{Z}^n$. De même, $A^{-1} \in \mathrm{GL}_n(\mathbb{Z})$ donc $A^{-1}(\mathbb{Z}^n) \subset \mathbb{Z}^n$ d'où $\mathbb{Z}^n \subset A(\mathbb{Z}^n)$.

5. Pour tout $M \in \mathrm{GL}_n(\mathbb{R})$, pour tout $A \in \mathrm{GL}_n(\mathbb{Z})$,

$$|\det MA| = |\det M|\,|\det A| = |\det M|$$

car d'après 2., $\det A \in \{-1, 1\}$. On peut donc définir

$$\begin{array}{rcl} f : \mathcal{H}_n & \to & \mathbb{R} \\ [M] & \mapsto & |\det M|. \end{array}$$

Comme $\mathcal{H}_n$ est en bijection avec $\mathcal{R}_n$ d'après 4., on en déduit une application $\nu = f \circ \overline{\psi}^{-1}$:

$$\begin{array}{rcl} \nu : \mathcal{R}_n & \to & \mathbb{R} \\ \Gamma = M(\mathbb{Z}^n) & \mapsto & |\det M|. \end{array}$$

Si $u_1, \ldots, u_n$ est une base du réseau Γ, on a $u_i = Me_i$ donc

$$\nu(\Gamma) = |\det_{\mathcal{B}}(u_1, \ldots, u_n)|.$$

C'est donc le volume du parallélotope défini par les vecteurs $u_1, \ldots, u_n$ (ce volume ne dépend pas de la base choisie).

6. Soit $B(c,r)$ une boule de $\mathbb{R}^n$ et $M \in \mathrm{GL}_n(\mathbb{R})$ telle que $\Gamma = M(\mathbb{Z}^n)$. On a

$$\begin{array}{rcll} \#\{x \in \Gamma; x \in B(c,r)\} & = & \#\{x \in M(\mathbb{Z}^n); x \in B(c,r)\} & \\ & = & \#\{y \in \mathbb{Z}^n; y \in M^{-1}(B(c,r))\}. & \end{array}$$

L'application M^{-1} est linéaire et continue (nous sommes en dimension finie) donc $M^{-1}(B(c,r))$ est une partie bornée de $\mathbb{R}^n$ incluse dans un cube de la forme $[-a,a]^n$ avec $a \in \mathbb{N}$. Un tel cube contient au plus $(2a+1)^n$ éléments de $\mathbb{Z}^n$ ce qui entraîne le résultat.

7. Soit $\Lambda = M(\mathbb{Z}^n)$ le réseau défini par la classe $\mathcal{M}$ (cf. 4.). Pour $M \in \mathcal{M}$, Me est un élément de Λ donc $\varphi(M)$ est la norme d'un élément de Λ pour $M \in \mathcal{M}$. Soit $M_0 \in \mathcal{M}$. D'après la question 6., il n'y a qu'un nombre fini de points de Λ de norme inférieure à $\varphi(M_0)$. En particulier, $\varphi(\mathcal{M}) \cap B(0, \varphi(M_0))$ est fini dans $\mathbb{R}$ donc φ atteint son minimum sur $\mathcal{M}$.

8. On a clairement

$$\begin{array}{rcll} \varphi(M) & = & \|Me\| = \|KDTe\| = \|DTe\| & \text{car } K \text{ est isométrique} \\ & = & \|De\| = \|d_1(M)e\| = |d_1(M)| = d_1(M) & \text{via } Te = e. \end{array}$$

9. Posons $t = t_{1,2}(M)$ et choisissons $p \in \mathbb{Z}$ tel que $-1/2 \leq p + t \leq 1/2$. On a $(p+t)^2 \leq 1/4$. Posons

$$A = \begin{pmatrix} \begin{pmatrix} p & -1 \\ 1 & 0 \end{pmatrix} & & 0 & \\ & 1 & & \\ 0 & & \ddots & \\ & & & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z}) \text{ (cf 2.).}$$

On a alors $Ae = pe + e_2$, $TAe = pe + te + e_2$ et $DTAe = d_1(M)(p+t)e + d_2(M)e_2$ d'où

$$\varphi(MA)^2 = \|KDTAe\|^2 = \|DTAe\|^2 = d_1(M)^2(p+t)^2 + d_2(M)^2$$

car la base canonique est orthonormale.

Comme M est minimale, $\varphi(M)^2 \leq \varphi(MA)^2$ ce qui donne, d'après la question 8., $d_1(M)^2 \leq \varphi(MA)^2$. On obtient

$$d_1(M)^2(1 - (p+t)^2) \leq d_2(M)^2$$

et comme $1-(p+t)^2 \geq 3/4$, on a

$$d_1(M) \leq \frac{2}{\sqrt{3}} d_2(M).$$

10.a. La matrice DT est triangulaire supérieure et ses coefficients diagonaux sont les $d_i(M)$. Elle peut s'écrire par blocs sous la forme suivante :

$$DT = \begin{pmatrix} d_1(M) & L \\ 0 & \\ \vdots & T' \\ 0 & \end{pmatrix},$$

où T' est une matrice triangulaire supérieure inversible d'ordre $n-1$ et L une matrice ligne de taille $(n-1)$. Puisque $\pi_{n-1}(\mathcal{T}_{n-1}) = \mathcal{H}_{n-1}$, on peut trouver $A' \in \mathrm{GL}_{n-1}(\mathbb{Z})$ telle que $T'A' \in \mathcal{T}_{n-1}$. Posons

$$A = \begin{pmatrix} 1 & 0 \dots 0 \\ 0 & \\ \vdots & A' \\ 0 & \end{pmatrix}.$$

Il est clair qu'on a aussi $A \in \mathrm{GL}_n(\mathbb{Z})$ car $\det A = \det A'$ (cf 2.). On a

$$DTA = \begin{pmatrix} d_1(M) & b_2 \dots b_n \\ 0 & \\ \vdots & T'A' \\ 0 & \end{pmatrix},$$

donc A répond à la question posée.

b. Soit (K', D', T') la décomposition d'Iwasawa de M'. Posons

$$\tilde{K} = K \cdot \begin{pmatrix} 1 & 0 \dots 0 \\ 0 & \\ \vdots & K' \\ 0 & \end{pmatrix}, \tilde{D} = \begin{pmatrix} d_1(M) & 0 \dots 0 \\ 0 & \\ \vdots & D' \\ 0 & \end{pmatrix},$$

$$\text{et } \tilde{T} = \begin{pmatrix} 1 & b_2/d_1(M) \dots b_n/d_1(M) \\ 0 & \\ \vdots & T' \\ 0 & \end{pmatrix}.$$

Il est clair que $\tilde{K} \in O_n(\mathbb{R})$, que $\tilde{D}$ est diagonale à coefficients strictement positifs et $\tilde{T}$ est triangulaire supérieure à coefficients diagonaux égaux à 1. De plus,

$$\tilde{K}\tilde{D}\tilde{T} = K(DTA) = (KDT)A = MA.$$

Par unicité (cf 1), la décomposition d'Iwasawa de MA est donc $(\tilde{K}, \tilde{D}, \tilde{T})$.

11. On procède par récurrence sur $n \in \mathbb{N}^\star$.
Si $n = 1$, c'est évident car $\mathcal{T}_1 = \mathrm{GL}_1(\mathbb{R})$.
Supposons que $\pi_{n-1}(\mathcal{T}_{n-1}) = \mathcal{H}_{n-1}$ ce qui nous permet d'appliquer 10. Soit $\mathcal{M} \in \mathcal{H}_n$. D'après 7., on peut trouver $M \in \mathcal{M}$ minimale. D'après 10.a., il existe $A \in \mathrm{GL}_n(\mathbb{Z})$ et $M' \in \mathcal{T}_{n-1}$ telles que

$$DTA = \begin{pmatrix} d_1(M) & b_2 \dots b_n \\ 0 & \\ \vdots & M' \\ 0 & \end{pmatrix}.$$

On a bien sûr $MA \in \mathcal{M}$. Le 10.b. prouve que $d_1(MA) = d_1(M)$ et $d_i(MA) = d_{i-1}(M')$ dès que $i \geq 2$. En particulier, d'après 8., $\varphi(MA) = \varphi(M)$ donc MA est minimale et d'après 9.,

$$d_1(MA) \leq \frac{2}{\sqrt{3}}\, d_2(MA).$$

D'autre part, puisque $M' \in \mathcal{T}_{n-1}$, dès que $i \geq 2$,

$$d_i(MA) = d_{i-1}(M') \leq \frac{2}{\sqrt{3}}\, d_i(M') = \frac{2}{\sqrt{3}}\, d_{i+1}(MA).$$

Ceci prouve que $MA \in \mathcal{T}_n$ et achève la récurrence.

12. D'après 4., tout réseau Γ s'identifie à un élément $\mathcal{M}$ de $\mathcal{H}_n$. D'après 11., on peut considérer $M \in \mathcal{M} \cap \mathcal{T}_n$.
Remarquons que $\varphi(M) = \|Me\| \geq m(\Gamma)$ car $Me \in \Gamma - \{0\}$. On a ainsi $m(\Gamma)^2 \leq d_1(M)^2$.
D'autre part, comme $M \in \mathcal{T}_n$, pour tout $i = 1, \dots, n$,

$$d_i(M) \geq \big(\frac{\sqrt{3}}{2}\big)^{i-1} d_1(M).$$

Comme $\nu(\Gamma) = |\det M| = |\det(KDT)| = |\det D|$ car $|\det K| = |\det T| = 1$, on en déduit que

$$\nu(\Gamma) = \prod_{i=1}^{n} d_i(M) \geq d_1(M)^n \prod_{i=1}^{n} \big(\frac{\sqrt{3}}{2}\big)^{i-1} = \big(\frac{\sqrt{3}}{2}\big)^{n(n-1)/2} d_1(M)^n.$$

On obtient donc

$$\gamma(\Gamma) \leq \frac{d_1(M)^2}{d_1(M)^2 \big(\frac{\sqrt{3}}{2}\big)^{n-1}} = \big(\frac{2}{\sqrt{3}}\big)^{n-1}.$$

Pour montrer que $\gamma(\Gamma) > 0$, il suffit de montrer que $m(\Gamma) > 0$. Pour cela, nous allons montrer que la borne inférieure définissant $m(\Gamma)$ est atteint en $a \in \Gamma - \{0\}$. Si ce n'est pas le cas, pour tout $a \in \Gamma - \{0\}$, il existe $a' \in \Gamma - \{0\}$ tel que $\|a'\| < \|a\|$. On peut donc trouver une suite $(a_n)_{n\in\mathbb{N}}$ bornée d'éléments tous distincts de Γ ce qui contredit le résultat de 6.

13. Si $(p_1, \dots, p_n) \in \mathbb{Z}^n - \{0\}$, $\|(p_1, \dots, p_n)\|^2 = \sum_{i=1}^{n} p_i^2 \geq 1$ et $\|e\| = 1$ donc $m(\mathbb{Z}^n) = 1$. D'autre part, il est clair que I_n est dans l'élément de $\mathcal{H}_n$

correspondant à $\mathbb{Z}^n$ (I_n correspond à la base $(e_1, \ldots, e_n)$ de $\mathbb{Z}^n$). Ainsi $\nu(\mathbb{Z}^n) = |\det \mathrm{I}_n| = 1$ et on en déduit immédiatement que $\gamma(\mathbb{Z}^n) = 1$.

On appelle Γ le réseau

$$\mathbb{Z}(1,0) \oplus \mathbb{Z}\big(\frac{1}{2}, \frac{\sqrt{3}}{2}\big)$$

Soit $a = p(1,0) + q(1/2, \sqrt{3}/2) \in \Gamma - \{0\}$. On calcule

$$\|a\|^2 = (p + \frac{q}{2})^2 + \frac{3}{4}q^2 = \frac{1}{4}(2p+q)^2 + \frac{3}{4}q^2.$$

Si $q = 0$, clairement $\|a\|^2 \geq 1$.

Si $q \neq 0$, on a $\|a\|^2 \geq \frac{1}{4} + \frac{3}{4}$. En effet, si $2p + q$ est non nul, c'est trivial. Si $2p + q$ est nul, p est alors non nul (car $q \neq 0$), q est pair donc $\|a\|^2 \geq 3$.

Dans tous les cas, $\|a\| \geq 1$ et le minimum est atteint en $(1,0)$ et en $(\frac{1}{2}, \frac{\sqrt{3}}{2})$. Ainsi, $m(\Gamma) = 1$.

D'autre part, si $\mathcal{M}$ est l'élément de $\mathcal{H}_n$ correspondant à Γ,

$$M = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix} \in \mathcal{M}$$

donc $\nu(\Gamma) = |\det M| = \sqrt{3}/2$.
Finalement, $\gamma(\Gamma) = 2/\sqrt{3}$ et l'on constate que l'inégalité obtenue en 12. est optimale dans le cas des réseaux de dimension 2.

14. Soit $\mathcal{M}$ un élément quelconque de $\mathcal{H}_n$. D'après 11., on sait qu'il existe $M \in \mathcal{T}_n$ telle que $\pi_n(M) = \mathcal{M}$. Soit (K, D, T) la décomposition d'Iwasawa de M et A une matrice triangulaire supérieure à coefficients entiers dont les coefficients diagonaux valent 1 : il est clair que $A \in \mathrm{GL}_n(\mathbb{Z})$ donc $\pi_n(MA) = \mathcal{M}$. D'autre part, TA est triangulaire supérieure dont les coefficients diagonaux valent 1 donc (K, D, TA) est la décomposition d'Iwasawa de MA. En particulier, $D_{MA} = D_A = D$ donc on a encore $MA \in \mathcal{T}_n$.
Il suffit donc de montrer que l'on peut ajuster les coefficients hors diagonale de A de façon à ce que ceux de TA soient de valeur absolue inférieure à $1/2$.

On a : $(TA)_{ij} = \sum_{k=i}^{j} t_{ik} a_{kj}$. Si $j > i$, $(TA)_{ij} = a_{ij} + \sum_{k=i+1}^{j} t_{ik} a_{kj}$.

Fixons $j \geq 2$. Supposons choisis $a_{i+1,j}; \ldots; a_{j,j}$ donc le réel $\sum_{k=i+1}^{j} t_{ik} a_{k,j}$ est fixé. On choisit alors $a_{i,j} \in \mathbb{Z}$ tel que

$$-1/2 \leq a_{i,j} + \sum_{k=i+1}^{j} t_{ik} a_{k,j} \leq 1/2.$$

Comme $a_{j,j} = 1$, cela définit par une récurrence décroissante les coefficients de la j-ième colonne de A qui permettent de satisfaire aux conditions posées pour la j-ième colonne de TA. On fait bien sûr ce travail pour tout $j = 2, \ldots, n$. Pour la matrice A obtenue, $MA \in \mathcal{S}_n$ et $\pi_n(MA) = \mathcal{M}$.

IV.

1. Soit V un ouvert de $\mathcal{R}_n$. Il existe U un ouvert de $\mathrm{GL}_n(\mathbb{R})$, tel que $V = \pi_n(U)$. On a

$$\begin{aligned}\pi_n^{-1}(V) &= \{M \in \mathrm{GL}_n(\mathbb{R});\ \pi_n(M) \in \pi_n(U)\} \\ &= \{M \in \mathrm{GL}_n(\mathbb{R});\ MA = vB,\ \text{où } A, B \in \mathrm{GL}_n(\mathbb{Z}),\ v \in U\} \\ &= \bigcup_{A \in \mathrm{GL}_n(\mathbb{Z})} UA.\end{aligned}$$

On remarque que pour tout $A \in \mathrm{GL}_n(\mathbb{Z})$, UA est un ouvert de $\mathrm{GL}_n(\mathbb{R})$ car c'est un translaté de l'ouvert U. L'ensemble $\pi_n^{-1}(V)$ est donc une intersection d'ouvert donc c'est un ouvert de $\mathrm{GL}_n(\mathbb{R})$. Ceci est valable pour tout ouvert V donc π_n est continue.

Supposons $\mathcal{R}_n$ non séparée. Il existe $\Gamma, \Gamma' \in \mathcal{R}_n$ tels que $\Gamma \neq \Gamma'$ et pour tous ouverts U, V de $\mathrm{GL}_n(\mathbb{R})$ tels que $\Gamma \subset \pi_n(U)$ et $\Gamma' \subset \pi_n(V)$, on a

$$\pi_n(U) \cap \pi_n(V) \neq \emptyset.$$

Soient M, $M' \in \mathrm{GL}_n(\mathbb{R})$ telles que $\pi_n(M) = \Gamma$ et $\pi_n(M') = \Gamma'$. Pour tout $p \in \mathbb{N}^\star$, on a donc

$$\pi_n(B(M, 1/p)) \cap \pi_n(B(M', 1/p)) \neq \emptyset,$$

où $B(M, 1/p)$ est la boule ouverte de centre M et de rayon $1/p$ dans $\mathrm{GL}_n(\mathbb{R})$. On peut donc trouver $M_p \in B(M, 1/p)$ et $M'_p \in B(M', 1/p)$ telles que $\pi_n(M_p) = \pi_n(M'_p)$. On a donc $M_p^{-1} M'_p \in \mathrm{GL}_n(\mathbb{Z})$. Il est clair que M_p converge vers M et que M'_p converge vers M' dans $\mathrm{GL}_n(\mathbb{R})$. Comme l'application $(A, A') \mapsto A^{-1}A'$ est continue donc $M_p^{-1}M'_p$ converge vers $M^{-1}M'$. Or $\mathrm{GL}_n(\mathbb{Z})$ est fermé dans $\mathrm{GL}_n(\mathbb{R})$ car on peut le voir comme $\mathbb{Z}^{n^2}$ (fermé dans $\mathbb{R}^{n^2}$) intersecté avec $\det^{-1}(\{-1, 1\})$ (fermé dans $\mathrm{GL}_n(\mathbb{R})$ car det est continue). On a donc $M^{-1}M' \in \mathrm{GL}_n(\mathbb{Z})$ c'est à dire $\pi_n(M) = \pi_n(M')$ ce qui est absurde.

2. Soit O un ouvert de $\mathbb{R}$. Supposons avoir montré que

$$\nu^{-1}(O) = \pi_n(|\det|^{-1}(O)).$$

Comme $|\det|$ est continue sur $\mathrm{GL}_n(\mathbb{R})$, $|\det|^{-1}(O)$ est ouvert dans $\mathrm{GL}_n(\mathbb{R})$. Puisque π_n est ouverte, $\pi_n(|\det|^{-1}(O))$ est ouvert dans $\mathcal{R}_n$. Ceci prouve que $\nu^{-1}(O)$ est ouvert d'où la continuité de ν.
Montrons l'égalité annoncée.
Considérons $\Gamma \in \nu^{-1}(O)$ et soit $M \in \mathrm{GL}_n(\mathbb{R})$ telle que $\Gamma = \pi_n(M)$. Par définition de ν (voir 5.), $|\det M| = \nu(\Gamma) \in O$ donc $M \in |\det|^{-1}(O)$ et $\Gamma \in \pi_n(|\det|^{-1}(O))$.
Considérons $\Gamma \in \pi_n(|\det|^{-1}(O))$, il existe $M \in |\det|^{-1}(O)$ telle que $\Gamma = \pi_n(M)$. Or $\nu(\Gamma) = |\det M| \in O$ donc $\Gamma \in \nu^{-1}(O)$.

3. L'application

$$\begin{aligned}\mathrm{GL}_n(\mathbb{R}) &\to \mathbb{R}_+^\star \\ M &\mapsto \|M^{-1}\|\end{aligned}$$

est continue comme composée d'applications continues. Comme U est compact, son image par cette application est bornée :

$$\exists \alpha > 0, \forall M \in U, \|M^{-1}\| \leq \alpha.$$

Ainsi pour tout $x \in \mathbb{R}^n$, pour tout $M \in U$,

$$\|x\| = \|M^{-1}Mx\| \leq \|M^{-1}\|\|Mx\| \leq \alpha\|Mx\|.$$

Il suffit de choisir $c = 1/\alpha$.

4. Soit $\Gamma \in \mathcal{R}_n$ et $M \in \mathrm{GL}_n(\mathbb{R})$ tel que $\pi_n(M) = \Gamma$. Par continuité du déterminant, on trouve $\alpha > 0$ tel que $\|M - P\| \leq \alpha$ entraîne $|\det M - \det P| \leq \frac{1}{2}|\det M|$, ce qui assure que $P \in \mathrm{GL}_n(\mathbb{R})$. L'ensemble

$$U = \{P \in M_n(\mathbb{R}), \|M - P\| \leq \alpha\}.$$

est inclus dans $\mathrm{GL}_n(\mathbb{R})$ et c'est un compact de $M_n(\mathbb{R})$ en tant que fermé borné donc U est un compact pour la topologie induite sur $\mathrm{GL}_n(\mathbb{R})$. Par la question précédente, il existe $c > 0$ tel que

$$\forall P \in U, \forall x \in \mathbb{R}^n, \|Px\| \geq c\|x\|.$$

Soit $\varepsilon > 0$, $O = \{M' \in \mathrm{GL}_n(\mathbb{R}), \|M' - M\| < \varepsilon\}$. L'ouvert $\pi_n(O)$ est un voisinage de Γ et pour tout $\Gamma' \in \pi_n(O)$, il existe $M' \in O$ telle que $\pi_n(M') = \Gamma'$. On a vu au III.12. que $m(\Gamma)$ et $m(\Gamma')$ sont atteints donc il existe $z \in \mathbb{Z}^n$, $z' \in \mathbb{Z}^n$ tels que

$$m(\Gamma) = \|Mz\| \text{ et } m(\Gamma') = \|M'z'\|.$$

Par définition de l'application m,

$$m(\Gamma) \leq \|Mz'\| \text{ et } m(\Gamma') \leq \|M'z\|$$

Or

$$\|Mz'\| = \|M'z' + (M - M')z'\| \leq m(\Gamma') + \varepsilon\|z'\|$$

et de même $\|M'\,z\| \leq m(\Gamma) + \varepsilon\|z\|$.

Il vient : $m(\Gamma') - m(\Gamma) \leq \varepsilon\|z\|$. De même, $m(\Gamma) - m(\Gamma') \leq \varepsilon\|z'\|$. En choisissant ε suffisamment petit, M' est un élément de U. On a alors $\|z'\| \leq \frac{1}{c}\|M'z'\|$. Puis

$$m(\Gamma) - m(\Gamma') \leq \frac{\varepsilon}{c}\|M'z'\| \leq \frac{\varepsilon}{c}m(\Gamma').$$

Ainsi, $m(\Gamma) - m(\Gamma') \leq \frac{\varepsilon}{\varepsilon+c}m(\Gamma)$.

La fonction m est donc continue au point Γ.

D'après 2., ν est continue. Comme elle ne s'annule pas sur $\mathcal{R}_n$, il en résulte immédiatement que γ est continue.

5. Soit $\mathcal{Y}$ une partie fermée de $\mathcal{S}_n$.

Supposons qu'il existe $\alpha > 0$ et $\beta > 0$ tels que

$$\forall M \in \mathcal{Y}, d_1(M) \geq \alpha \text{ et } d_n(M) \leq \beta.$$

Soit $(M_p)_{p\in\mathbb{N}}$ une suite d'éléments de $\mathcal{Y}$. Pour tout $p \in \mathbb{N}$, (K_p, D_p, T_p) est la décomposition d'Iwasawa de M_p. Puisque $O_n(\mathbb{R})$ est compact, il existe $K \in O_n(\mathbb{R})$ et ϕ strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$ telle que $K_{\phi(p)} \to K$. L'ensemble des matrices triangulaires supérieures à coefficients diagonaux égaux à 1 et à coefficients hors-diagonaux de valeur absolue inférieure ou égale à $1/2$ est compact car homéomorphe à $[-1/2, 1/2]^{n(n-1)/2}$ donc il existe T de ce type et

ψ telles que $T_{\phi\circ\psi(p)} \to T$. Enfin, comme $M \in \mathcal{S}_n \subset \mathcal{T}_n$, la condition sur $d_1(M)$ et $d_n(M)$ assure que pour tout $i = 1, \ldots, n$, pour tout $p \in \mathbb{N}$,

$$\big(\frac{\sqrt{3}}{2}\big)^{n-1}\alpha \leq d_i(M_p) \leq \big(\frac{2}{\sqrt{3}}\big)^{n-1}\beta,$$

donc D_p est à valeurs dans un compact de $\mathbb{R}^{+*}$ et il existe D diagonale à coefficients diagonaux strictement positifs et θ telles que $D_{\phi\circ\psi\circ\theta(p)} \to D$. Il est alors clair que $M_{\phi\circ\psi\circ\theta(p)} \to KDT$ et comme $\mathcal{Y}$ est fermé, $KDT \in \mathcal{Y}$ ce qui prouve la compacité de $\mathcal{Y}$.

Réciproquement, supposons que $\mathcal{Y}$ soit compacte. L'application

$$\begin{array}{rcl} \mathrm{GL}_n(\mathbb{R}) & \to & \mathbb{R}_+^\star \\ M & \mapsto & d_1(M) \end{array}$$

est continue car d'après 8., $d_1(M) = \varphi(M) = \|Me\|$ donc l'image de $\mathcal{Y}$ par cette application est un compact de $\mathbb{R}_+^\star$. En particulier, il existe $\alpha > 0$ tel que

$$\forall M \in \mathcal{Y}, d_1(M) \geq \alpha.$$

L'application

$$\begin{array}{rcl} \mathrm{GL}_n(\mathbb{R}) & \to & \mathbb{R}_+^\star \\ M & \mapsto & |\det M| \end{array}$$

est continue donc l'image de $\mathcal{Y}$ par cette application est un compact de $\mathbb{R}_+^\star$. En particulier, il existe $\beta > 0$ tel que

$$\forall M \in \mathcal{Y}, |\det M| \leq \beta.$$

Mais $M \in \mathcal{S}_n \subset \mathcal{T}_n$ donc pour tout $i = 1, \ldots, n$

$$d_i(M) \geq \big(\frac{\sqrt{3}}{2}\big)^{i-1} d_1(M)$$

Finalement,

$$\beta \geq |\det M| = \prod_{i=1}^{n} d_i(M) \geq d_n(M) d_1(M)^{n-1} \big(\frac{\sqrt{3}}{2}\big)^{(n-1)(n-2)/2},$$

et comme $d_1(M) \geq \alpha$, on en conclut que

$$d_n(M) \leq \frac{\beta}{\alpha^{n-1}} \big(\frac{2}{\sqrt{3}}\big)^{(n-1)(n-2)/2}.$$

Les conditions posées sur d_1 et d_n sont donc satisfaites sur $\mathcal{Y}$.

6. Supposons que $\mathcal{P}$ soit compacte. On a montré au 2. que ν est continue de $\mathcal{R}_n$ dans $\mathbb{R}$ donc $\nu(P)$ est une partie compacte de $\mathbb{R}$ qui est en particulier majorée : (i) est vérifiée. On a montré au 4. que m est continue de $\mathcal{R}_n$ dans $\mathbb{R}_+^\star$ donc $m(\mathcal{P})$ est une partie compacte de $\mathbb{R}_+^\star$ et en particulier, il existe $a > 0$ tel que pour tout $\Gamma \in \mathcal{P}$, $m(\Gamma) \geq a$. Il suffit alors de poser $U = B(0, a/2)$ pour vérifier (ii).

Réciproquement, supposons que (i) et (ii) soient vérifiées. Posons

$$\mathcal{Y} = \pi_n^{-1}(\mathcal{P}) \cap \mathcal{S}_n.$$

D'après II.14., $\pi_n(\mathcal{Y}) = \mathcal{P}$. Il suffit de montrer que $\mathcal{Y}$ est compacte car $\mathcal{P}$ sera également compacte comme image dans un espace séparé (par 1.) d'un compact par une application continue.
Puisque π_n est continue et $\mathcal{P}$ fermé dans $\mathcal{R}_n$, $\mathcal{Y}$ est fermé dans $\mathcal{S}_n$. Pour obtenir la compacité de $\mathcal{Y}$, il suffit de vérifier les deux conditions sur d_1 et d_n de la question précédente.
D'après (ii), on peut considérer $\alpha > 0$ tel que pour tout $\Gamma \in \mathcal{P}$, $\Gamma \cap B(0,\alpha) = \{0\}$. Ceci entraîne évidemment que pour tout $\Gamma \in \mathcal{P}$, $m(\Gamma) \geq \alpha$. Si $M \in \mathcal{Y}$,

$$d_1(M) = \varphi(M) = \|Me\| \geq m(\pi_n(M)) \geq \alpha$$

donc la condition sur d_1 est vérifiée.
D'après (i), on peut considérer $\beta > 0$ tel que pour tout $\Gamma \in \mathcal{P}$, $\nu(\Gamma) \leq \beta$. Ceci entraîne évidemment que pour tout $M \in \mathcal{Y}$, $|\det M| \leq \beta$. On conclut exactement comme dans 5. à l'existence d'un β_1 tel que pour tout $M \in \mathcal{Y}$, $d_n(M) \leq \beta_1$: la condition sur d_n est également vérifiée.

7. Il est évident que l'image de γ' est incluse dans l'image de γ. Considérons a dans l'image de γ : il existe $\Gamma \in \mathcal{R}_n$ tel que $\gamma(\Gamma) = a$. Soit $\lambda = 1/\nu(\Gamma)^{1/n}$ et considérons $\Gamma' = \lambda\Gamma = \{\lambda x,\, x \in \Gamma\}$.
Il est clair que Γ' est un réseau : si $(f_1, \ldots, f_n)$ est une base de Γ, Γ' est le réseau de base $(\lambda f_1, \ldots, \lambda f_n)$.
Il est également clair que $\nu(\Gamma') = \lambda^n \nu(\Gamma) = 1$ donc $\Gamma' \in \mathcal{R}'_n$.
Enfin, comme $m(\Gamma') = \lambda m(\Gamma)$ on a

$$\gamma'(\Gamma') = \frac{m(\Gamma')^2}{\nu(\Gamma')^{2/n}} = \frac{(\lambda m(\Gamma))^2}{(\lambda^n \nu(\Gamma))^{2/n}} = \gamma(\Gamma) = a$$

donc a est dans l'image de γ'.

8. D'après 4., γ et donc γ' sont continues. Considérons K un compact de $]0, +\infty[$: K est fermé donc $\gamma'^{-1}(K)$ est fermée dans $\mathcal{R}'_n$ donc dans $\mathcal{R}_n$ car $\mathcal{R}'_n$ est fermée dans $\mathcal{R}_n$. Pour montrer sa compacité, on peut donc appliquer la question 6. et il suffit de vérifier les conditions (i) et (ii).
Par définition de $\mathcal{R}'_n$, (i) est vérifiée.
D'autre part, il existe $\alpha > 0$ tel que $K \subset [\alpha, +\infty[$ donc pour tout $\Gamma \in \gamma'^{-1}(K)$, $\gamma'(\Gamma) \geq \alpha$. Mais

$$\gamma'(\Gamma) = \frac{m(\Gamma)^2}{\nu(\Gamma)^{2/n}} = m(\Gamma)^2$$

donc pour tout $\Gamma \in \gamma'^{-1}(K)$, $m(\Gamma) \geq \sqrt{\alpha}$. Si $U = B(0, \sqrt{\alpha}/2)$, la propriété (ii) est vérifiée.

9. D'après 7., $\sup_{\Gamma \in \mathcal{R}_n} \gamma(\Gamma) = \sup_{\Gamma' \in \mathcal{R}'_n} \gamma'(\Gamma')$. Considérons $\Gamma'_1 \in \mathcal{R}'_n$ alors par le III.12.,

$$\sup_{\Gamma' \in \mathcal{R}'_n} \gamma'(\Gamma') \subset \big[\gamma'(\Gamma'_1), \big(\frac{2}{\sqrt{3}}\big)^{n-1}\big].$$

On pose $K = \gamma'^{-1}([\gamma'(\Gamma'_1), \big(\frac{2}{\sqrt{3}}\big)^{n-1}])$: d'après 8., K est compact et $\gamma'_{|K}$ est continue et atteint son maximum en Γ'_0. Il est clair que

$$\gamma'(\Gamma'_0) = \sup_{\Gamma' \in \mathcal{R}'_n} \gamma'(\Gamma'),$$

donc Γ_0' convient.

V.

Remarquons tout d'abord que :

- $S(\Gamma)$ est non vide par III.6. et 12.
- $S(\Gamma)$ est fini en utilisant III.6.
- $S(\Gamma)$ est de cardinal pair car si $a \in S(\Gamma)$, $-a \in S(\Gamma)$ et $a \neq -a$.

1. Il suffit de poser $B(x,y) = \dfrac{1}{m(\Gamma)^2}\langle x, y\rangle$.

2. Soit y_0 non nul dans $\Gamma - S(\Gamma)$. D'après III.6., la boule $\overline{B(0, \|y_0\|)}$ ne contient qu'un nombre fini d'éléments de Γ donc qu'un nombre fini d'éléments non nuls de $\Gamma - S(\Gamma)$. Soit y_1 de norme minimale dans cet ensemble. Il est clair qu'en posant

$$c(\Gamma) = \frac{\|y_1\|}{m(\Gamma)},$$

on a bien $c(\Gamma) > 1$ (car $y_1 \notin S(\Gamma)$) et pour tout $y \in \Gamma - S(\Gamma)$ non nul,

$$\|y\| \geq \|y_1\| = c(\Gamma)m(\Gamma).$$

Soit y non nul dans $\Gamma - S(\Gamma)$ et $M \in \mathrm{GL}_n(\mathbb{R})$ alors

$$c(\Gamma)m(\Gamma) \leq \|y\| = \|M^{-1}My\| \leq \|M^{-1}\|\,\|My\|,$$

ce qui est le résultat.

3. L'application $M \mapsto \|M\|\,\|M^{-1}\|$ est continue sur $\mathrm{GL}_n(\mathbb{R})$ et vaut 1 en I_n. On peut donc trouver un voisinage U de I_n dans $\mathrm{GL}_n(\mathbb{R})$ tel que

$$\forall M \in U,\ \|M\|\,\|M^{-1}\| < c(\Gamma).$$

Prenons $b \in S(M(\Gamma))$ et $a \in \Gamma$ tel que $b = Ma$. Pour tout $u \in \Gamma - \{0\}$, $m(\Gamma) = \|Ma\| \leq \|Mu\|$. Montrons que $a \in S(\Gamma)$. On a $\|a\| = \|M^{-1}Ma\| \leq \|M^{-1}\|\|Ma\|$ mais $\|Ma\| \leq \|Mu\|$ donc

$$\|a\| \leq \|M^{-1}\|\|Mu\| \leq \|M^{-1}\|\|M\|\|u\| < c(\Gamma)\|u\|.$$

En particulier, si $u \in S(\Gamma)$, $\|a\| < c(\Gamma)m(\Gamma)$. Mais d'après 2., si $a \notin S(\Gamma)$, on a avec $M = \mathrm{I}_n$, $\|a\| \geq c(\Gamma)m(\Gamma)$ ce qui est contradictoire. On en conclut que $a \in S(\Gamma)$ donc $b = Ma \in M(S(\Gamma))$.

4. Puisque $\lim\limits_{\alpha \to 0} M_\alpha = \mathrm{I}_n$, on peut trouver $\varepsilon > 0$ tel que si $|\alpha| < \varepsilon$ alors $M_\alpha \in U$. On a donc pour tout $|\alpha| < \varepsilon$,

$$S(M_\alpha(\Gamma) \subset M_\alpha(S(\Gamma)).$$

Considérons $b \in S(M_\alpha(\Gamma)) : \|b\| = m(M_\alpha(\Gamma))$. D'autre part, b s'écrit $M_\alpha a$ où $a \in S(\Gamma)$. Comme M_α est symétrique,

$$\|b\|^2 = \|M_\alpha a\|^2 = \langle a, M_\alpha^2 a\rangle$$

et $M_\alpha^2 = \mathrm{I}_n + \alpha M$ donc

$$\|b\|^2 = \|a\|^2 + \alpha\langle a, Ma\rangle.$$

Par définition de M, on a $\langle a, Ma\rangle = (B - B')(a, a) = 1 - 1 = 0$, donc $\|b\| = \|a\| = m(\Gamma)$ ce qui prouve que $m(M_\alpha(\Gamma)) = m(\Gamma)$.

5. La matrice M est symétrique donc diagonalisable dans une base orthonormée de $\mathbb{R}^n$ ainsi que $\mathrm{I}_n + \alpha M$. Si $\lambda_1, \ldots, \lambda_n$ désignent les valeurs propres de M alors les valeurs propres de $\mathrm{I}_n + \alpha M$ sont $1 + \alpha\lambda_1, \ldots, 1 + \alpha\lambda_n$. Soit $f : \alpha \mapsto \det M_\alpha$ alors

$$\begin{aligned} f^2(\alpha) &= \det M_\alpha^2 = \det(\mathrm{I}_n + \alpha M) \\ &= \prod_{i=1}^{n}(1 + \alpha\lambda_i) = 1 + \alpha\sum_{i=1}^{n}\lambda_i + \alpha^2\Big(\sum_{1\le i<j\le n}\lambda_i\lambda_j\Big) + o(\alpha^2). \end{aligned}$$

On pose $\sigma_1 = \displaystyle\sum_{i=1}^{n}\lambda_i$ et $\sigma_2 = \sum_{1\le i<j\le n}\lambda_i\lambda_j$. On a alors ($f(\alpha)$ étant positif pour α assez petit)

$$\begin{aligned} f(\alpha) = \sqrt{f^2(\alpha)} &= (1 + \alpha\sigma_1 + \alpha^2\sigma_2 + o(\alpha^2))^{1/2} \\ &= 1 + \alpha\frac{\sigma_1}{2} + \alpha^2\Big(\frac{\sigma_2}{2} - \frac{\sigma_1^2}{8}\Big) + o(\alpha^2). \end{aligned}$$

Supposons maintenant $\gamma(\Gamma) = \sup_{\Gamma' \in \mathcal{R}_n}\gamma(\Gamma')$ alors $\gamma(M_\alpha(\Gamma)) \le \gamma(\Gamma)$. D'après 4., on a pour α assez petit, $m(M_\alpha(\Gamma)) = m(\Gamma)$ donc

$$\gamma(M_\alpha(\Gamma)) = \frac{m(\Gamma)^2}{\nu(M_\alpha(\Gamma))^{2/n}},$$

et on en déduit que $\nu(M_\alpha(\Gamma)) \ge \nu(\Gamma)$. Or $\nu(M_\alpha(\Gamma)) = |\det(M_\alpha\tilde{M})|$ où $\Gamma = \pi_n(\tilde{M})$ donc (comme M_α est définie positive) $\nu(M_\alpha(\Gamma)) = \det(M_\alpha)|\det(\tilde{M})| = (\det M_\alpha)\,\nu(\Gamma)$ puis pour α assez petit, on a

$$\det M_\alpha \ge 1 = \det M_0.$$

Ceci entraîne d'abord $\sigma_1 = 0$ sinon le développement limité précédent assurerait que $\det M_\alpha$ prend des valeurs strictement plus petites que 1 au voisinage de 0 à gauche. Pour la même raison, $\dfrac{\sigma_2}{2} - \dfrac{\sigma_1^2}{8} = \dfrac{\sigma_2}{2} \ge 0$ donc

$$\sum_{i=1}^{n}\lambda_i^2 = \sigma_1^2 - 2\sigma_2 = -2\sigma_2 \le 0.$$

Ceci entraîne la nullité de tous les λ_i donc de la matrice M. Ainsi, $B = B'$ et B_Γ n'a qu'un seul élément.

6.a. Soient $b_1, \ldots, b_n$ les éléments de $\mathcal{B}$. Ecrivons pour $a \in S(\Gamma)$,

$$a = \sum_{i=1}^{n} \alpha_i(a) b_i$$

avec $\alpha_i(a) \in \mathbb{Z}$. On a alors

$$\begin{aligned} B \in B_\Gamma &\iff \forall a \in S(\Gamma), B(a,a) = 1 \\ &\iff \forall a \in S(\Gamma), \sum_{i,j} \alpha_i(a)\alpha_j(a) B(b_i, b_j) = 1. \end{aligned}$$

On obtient donc un système à coefficients entiers de $\#S(\Gamma)$ équations. Or a et $-a$ donnent naissance à la même équation donc on obtient en fait un système linéaire à $\#S(\Gamma)/2$ équations.

b. Comme B est symétrique, le système précédent comporte $n(n+1)/2$ inconnues. Il doit avoir une unique solution car B_Γ a un seul élément. Il possède donc plus d'équations que d'inconnues donc

$$\frac{\#S(\Gamma)}{2} \geq \frac{n(n+1)}{2}$$

d'où le résultat.

c. Soit q la forme bilinéaire $q(x,y) = \langle x, y \rangle$ alors

$$(\langle b, b' \rangle)_{b,b' \in \mathcal{B}} = \mathrm{Mat}(q, \mathcal{B}).$$

Si P désigne la matrice de passage de la base canonique $\mathcal{E}$ vers $\mathcal{B}$, on a

$$\mathrm{Mat}(q, \mathcal{B}) = {}^tP \mathrm{Mat}(q, \mathcal{E}) P$$

ce qui donne $(\langle b, b' \rangle)_{b,b' \in \mathcal{B}} = {}^tPP$. Or $|\det P| = \nu(\Gamma)$ car P est la matrice des vecteurs de $\mathcal{B}$ dans la base canonique. Le déterminant cherché est donc $(\nu(\Gamma))^2$.

d. Comme B_Γ a un seul élément, cet élément de B_Γ est celui déterminé au 1., c'est à dire

$$B(x,y) = \frac{\langle x, y \rangle}{m(\Gamma)^2}.$$

D'autre part les $B(b,b')$ sont rationnels car solution d'un système linéaire à coefficients dans $\mathbb{Z}$ donc

$$\det\left(\left[B(b,b')\right]_{b,b' \in \mathcal{B}}\right) \in \mathbb{Q}.$$

Or ce déterminant vaut

$$\frac{1}{m(\Gamma)^{2n}} \det\left([\langle b, b' \rangle]_{b,b' \in \mathcal{B}}\right) = \frac{\nu(\Gamma)^2}{m(\Gamma)^{2n}} = \frac{1}{\gamma(\Gamma)^n}$$

donc $\gamma(\Gamma)^n \in \mathbb{Q}$.

Remarque : d'après 5., cette dernière propriété de rationnalité est en particulier vérifiée si Γ maximise γ.

10.3 Commentaires

On étudie dans un premier temps un problème de recouvrement dans le cas du plan puis de l'espace. Aucune connaissance particulière n'est requise. Le reste du sujet concerne la géométrie des réseaux. Le problème utilise principalement des techniques d'algèbre linéaire, d'optimisation et d'estimations volumiques. La partie IV permettra aux candidats de manipuler des notions topologiques standards sur l'ensemble des réseaux.

La topologie quotient. Identifier $\mathcal{R}_n$ et $\mathcal{H}_n$, c'est par définition dire que $\mathcal{R}_n$ est l'ensemble quotient $\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z})$. Expliquons pourquoi la topologie dont on munit $\mathcal{R}_n$ dans la partie IV est en fait la topologie quotient associée. En effet, la définition donnée ici n'est pas la définition générale de la topologie quotient.

Posons

$$\mathcal{T} = \{\pi_n(U) \text{ où } U \text{ ouvert de } \mathrm{GL}_n(\mathbb{R})\}$$

et

$$\mathcal{T}' = \{V \in \mathcal{R}_n \text{ tel que } \pi_n^{-1}(V) \text{ ouvert de } \mathrm{GL}_n(\mathbb{R})\}.$$

Il est facile de vérifier que $\mathcal{T}'$ est une topologie sur $\mathcal{R}_n$: c'est une conséquence immédiate des relations

$$\pi_n^{-1}\left(\bigcup_{i\in I} V_i\right) = \bigcup_{i\in I} \pi_n^{-1}(V_i) \quad \text{et} \quad \pi_n^{-1}\left(\bigcap_{i\in I} V_i\right) = \bigcap_{i\in I} \pi_n^{-1}(V_i).$$

Par définition, $\mathcal{T}'$ rend π_n continue et si $\mathcal{T}''$ est une autre topologie rendant π_n continue alors un ouvert V pour $\mathcal{T}''$ vérifie $\pi_n^{-1}(V)$ ouvert de $\mathrm{GL}_n(\mathbb{R})$, et donc est un ouvert de $\mathcal{T}'$. Ainsi $\mathcal{T}'' \subset \mathcal{T}'$ ce qui prouve que $\mathcal{T}'$ est la topologie la plus fine sur $\mathcal{R}_n$ rendant π_n continue. C'est elle que par définition on appelle la topologie quotient.

D'autre part si $V \in \mathcal{T}'$ alors, comme $V = \pi_n(\pi_n^{-1}(V))$ puisque π_n est surjective, on a $V \in \mathcal{T}$ donc $\mathcal{T}' \subset \mathcal{T}$. Mais également si $V \in \mathcal{T}$, V s'écrit $\pi_n(U)$ et

$$\begin{aligned} \pi_n^{-1}(V) &= \{M \in \mathrm{GL}_n(\mathbb{R}) \ / \ \pi_n(M) \in \pi_n(U)\} \\ &= \{M \in \mathrm{GL}_n(\mathbb{R}) \ / \ M \in U\mathrm{GL}_n(\mathbb{Z})\} \\ &= \bigcup_{A\in \mathrm{GL}_n(\mathbb{Z})} UA. \end{aligned}$$

L'application $M \mapsto MA$ définit un homéomorphisme de U sur UA donc $\pi_n^{-1}(V)$ est un ouvert de $\mathrm{GL}_n(\mathbb{R})$, comme union d'ouverts de $\mathrm{GL}_n(\mathbb{R})$. Ceci prouve que $V \in \mathcal{T}'$ donc que $\mathcal{T}' = \mathcal{T}$, ce qui fournit dans le cas particulier de classe d'équivalence modulo un sous-groupe, une description alternative commode de la topologie quotient. Une conséquence immédiate est le caractère d'application ouverte de la surjection canonique.

Mettons également en garde le lecteur contre la dangereuse tentation de simplifier la démonstration du fait que cette topologie est séparée de la façon suivante (question IV.1.) : $\pi_n(M_p) \underset{p\to\infty}{\longrightarrow} \pi_n(M)$ et $\pi_n(M'_p) \underset{p\to\infty}{\longrightarrow} \pi_n(M')$ car π_n est continue. De $\pi_n(M_p) = \pi_n(M'_p)$ on peut déduire que $\pi_n(M) = \pi_n(M')$ ce qui était la contradiction cherchée. Cette déduction est injustifiée tant que l'on ne peut assurer l'unicité de la limite d'une suite convergente. Or c'est justement la

séparation de $\mathcal{T}$ (que nous cherchons à établir dans cette question) qui permet d'obtenir cette unicité.

Le lecteur devra de toute façon se convaincre que le caractère fermé de $\mathrm{GL}_n(\mathbb{Z})$ est ici l'hypothèse nécessaire au résultat.