CENTRALE

Planche 1
On admet que si u et v sont diagonalisables et commutent alors ils sont codiagonalisables.
Soit E un $\mathbb{K}$-ev de dimension finie n, $\mathcal{A}$ une sous algèbre de $\mathcal{L}(E)$ telle que tout u dans $\mathcal{A}$ est diagonalisable.
Soit $u \in \mathcal{A}$.

1. Soient $L_u : \left\{ \begin{array}{ccc} \mathcal{L}(E) & \to & \mathcal{L}(E) \\ v & \mapsto & u \circ v \end{array} \right.$ et $R_u : \left\{ \begin{array}{ccc} \mathcal{L}(E) & \to & \mathcal{L}(E) \\ v & \mapsto & v \circ u \end{array} \right.$
   Montrer que L_u et R_u sont diagonalisables.
   $\theta_u : \left\{ \begin{array}{ccc} \mathcal{L}(E) & \to & \mathcal{L}(E) \\ v & \mapsto & u \circ v - v \circ u \end{array} \right.$ est-t-il diagonalisable ?

2. Soit $\varphi_u : \left\{ \begin{array}{ccc} \mathcal{A} & \to & \mathcal{A} \\ v & \mapsto & u \circ v - v \circ u \end{array} \right.$, λ une valeur propre de φ_u et w vecteur propre associé.
   Montrer que $\forall k \in \mathbb{N},\ \varphi_u(w^k) = k\lambda w^k$. En déduire la valeur de λ.

3. Montrer que $\mathcal{A}$ est commutative et en déduire que sa dimension est majorée par n.

Indication 1 Pour la deuxième partie de la question 3., on pourra codiagonaliser une base de $\mathcal{A}$.

Solution 1

1. Une récurrence simple montre que
   $$\forall n \in \mathbb{N},\ \forall v,\ L_u^n(v) = u^n \circ v \ \text{ et } \ R_u^n(v) = v \circ u^n$$
   On en déduit par combinaisons linéaires que
   $$\forall P \in \mathbb{K}[X],\ \forall v,\ P(L_u)(v) = P(u) \circ v \ \text{ et } \ P(R_u)(v) = v \circ P(u)$$
   u étant diagonalisable, μ_u (polynôme minimal) est scindé simple. Il annule u et donc aussi L_u et R_u qui sont ainsi diagonalisables.
   On a $L_u \circ R_u(v) = L_u(v \circ u) = u \circ v \circ u = R_u(u \circ v) = R_u \circ L_u(v)$. Avec le résultat admis, R_u et L_u sont codiagonalisables et donc $\theta_u = L_u - R_u$ est diagonalisable.

2. On note que φ_u est bien définie de $\mathcal{A}$ dans lui même car $\mathcal{A}$ est une algèbre.
   On montre par récurrence que la propriété
   $$uw^k - w^k u = k\lambda w^k$$
   est vraie pour tout entier k.
   - Le résultat est vrai au rang 0 ($0 = 0$) et au rang 1 car w est propre pour φ_u associé à λ.
   - Supposons le résultat vrai à un rang $k \geq 2$. On a alors
     $$uw^{k+1} = (uw^k)w = (k\lambda w^k + w^k u)w = k\lambda w^{k+1} + w^k(wu + \lambda w)$$
     ce qui donne le résultat au rang $k + 1$.

Si $w^k \neq 0$ alors $k\lambda$ est propre pour φ_u associé à $k\lambda$. Ainsi, soit λ est nul, soit w est nilpotent (puisqu'il ne peut exister qu'un nombre fini de valeurs propres). Or $w \in \mathcal{A}$ est diagonalisable et donc nul si nilpotent. Finalement, $\lambda = 0$.

3. φ_u est diagonalisable comme restriction de θ_u (au sous-espace stable $\mathcal{A}$). Sa seule valeur propre est 0 et c'est donc l'endomorphisme nul. Ainsi,

$$\forall u, v \in \mathcal{A},\ u \circ v = v \circ u$$

$\mathcal{A}$ est donc une sous-algèbre commutative.
On généralise le résultat admis en : si un nombre fini d'endomorphismes diagonalisables commutent deux à deux alors ils sont codiagonalisables.
Ici, en notant $(M_1, \dots, M_p)$ une base de $\mathcal{A}$, il existe une matrice P telle que $P^{-1}M_kP$ est diagonale pour tout k. Ainsi, $P^{-1}MP$ est diagonale pour tout $M \in \mathcal{A}$. L'application $M \mapsto P^{-1}MP$ est injective de $\mathcal{A}$ dans l'ensemble des matrices diagonales et $\mathcal{A}$ est de dimension $\leq n$.

Planche 2
On note $P = X^n - X - 1$ où $n \geq 3$. On note R l'ensemble des racines complexes de P.

1. Montrer que P ne possède que des racines simples. Calculer

$$S(P) = \sum_{z \in R} \left(z - \frac{1}{z} \right)$$

2. On note $z = re^{i\theta}$ avec $r > 0$ et $\theta \in]0, 2\pi[$ une racine de P. Montrer que

$$2\mathrm{Re}\left(z - \frac{1}{z} \right) > \frac{1}{r^2} - 1$$

3. Montrer qu'il n'existe pas de polynômes A, B non constants à coefficients dans $\mathbb{Z}$ tels que $P = AB$.

Indication 2 Pour 2. exprimer $\cos(\theta)$ en fonction de r. Pour 3. on pourra raisonner par l'absurde et prouver (quitte à changer A en son opposé) que $S(A)$ est un entier supérieur ou égal à 1.

Solution 2

1. $P' = nX^{n-1} - 1$. Si z est racine multiple de P alors $P'(z) = 0$ et donc $z^{n-1} = 1/n$. Ainsi $P(z) = \frac{z}{n} - z - 1$ et donc $z = \frac{n}{1-n}$. On en déduit que $\left(\frac{n}{1-n}\right)^{n-1} = \frac{1}{n}$ ou encore que $n^n = (1-n)^{n-1}$ ce qui est faux ($|1-n|^n = (n-1)^n < n^n$). P n'a donc que des racines simples.
Notons $z_1, \dots, z_n$ les éléments de R. Par relations coefficients-racines, on a

$$\sum_{i=1}^{n} z_i = 0,\ \prod_{i=1}^{n} z_i = (-1)^{n+1},\ \sum_{i=1}^{n} \prod_{j \neq i} z_j = (-1)^n$$

En faisant le quotient des deux dernières égalité, on trouve que $\sum_{i=1}^{n} \frac{1}{z_i} = -1$. On en déduit que

$$\sum_{z \in R} \left(z - \frac{1}{z} \right) = 1$$

2. $re^{i\theta}$ étant racine de P, $P(re^{i\theta}) = 0$ et en passant aux parties réelle et imaginaire

$$r^n \cos(n\theta) = r\cos(\theta) + 1 \quad \text{et} \quad r^n \sin(n\theta) = r\sin(\theta)$$

En élevant au carré et en sommant, $r^{2n} = r^2 + 2r\cos(\theta) + 1$ et donc $\cos(\theta) = \frac{r^{2n}-r^2-1}{2r}$. On a ainsi

$$2\text{Re}\left(z - \frac{1}{z}\right) = 2\frac{r^2-1}{r}\cos(\theta) = 2\frac{r^2-1}{r}\frac{r^{2n}-r^2-1}{2r} = \frac{1}{r^2} - r^2 + r^{2n-2}(r^2-1)$$

L'inégalité à prouver est donc $r^{2n-2}(r^2-1) > r^2-1$ ou encore $(r^2-1)(r^{2n-2}-1) > 0$. Il nous suffit donc de justifier que $r \neq 1$.
Si $r = 1$ alors $z = e^{i\theta}$ et donc $e^{in\theta} = e^{i\theta} + 1 = 2\cos(\theta/2)e^{i\theta/2}$. Ainsi $|\cos(\theta/2)| = 1/2$ et $z = e^{\pm i\pi/3}$ dont on vérifie qu'il ne convient pas pour $n \geq 3$. On a donc justifié que

$$2\text{Re}\left(z - \frac{1}{z}\right) > \frac{1}{r^2} - 1$$

3. Supposons, par l'absurde, que $P = AB$ avec $A, B \in \mathbb{Z}[X]$ non constants. On a tout d'abord immédiatement $1 = S(P) = S(A) + S(B)$. De plus, quitte à changer les polynômes en leurs opposés, on peut les supposer unitaires (le produit des coefficients dominants de A et B vaut 1 et ces coefficients sont entiers).
En notant $x_1, \dots, x_q$ les racines complexes de A, les relations coefficients-racines (même calcul que plus haut) montre que $S(A)$ est rationnel et même entier si $A(0) = \pm 1$ ce qui est le cas puisque $A(0)B(0) = P(0) = -1$ et puisque $A(0), B(0) \in \mathbb{Z}$. Comme $S(A)$ est un réel, on a aussi

$$S(A) = \sum_{i=1}^{q} \text{Re}\left(x_i + \frac{1}{x_i}\right) > \frac{1}{2}\sum_{i=1}^{q}\left(\frac{1}{|x_i|^2} - 1\right) = \frac{q}{2}\left(\frac{1}{q}\sum_{i=1}^{q}\frac{1}{|x_i|^2} - 1\right)$$

La moyenne arithmétique étant plus grande que celle géométrique (pour des nombres positifs), on en conclut que

$$S(A) \geq \frac{q}{2}\left(\sqrt[q]{\prod_{i=1}^{q}\frac{1}{|x_i|^2}} - 1\right)$$

Or, le produit des racines de A vaut au signe près le coefficient constant et est donc de module 1. Ainsi $S(A) > 0$ et comme il est entier $S(A) \geq 1$.
On a de même $S(B) \geq 1$ et ainsi $1 = S(P) \geq 2$ ce qui donne une contradiction.

Planche 3

On considère la matrice $A = \begin{pmatrix} 0 & \dots & 0 & a_n \\ \vdots & \iddots & \iddots & 0 \\ 0 & \iddots & \iddots & \vdots \\ a_1 & 0 & \dots & 0 \end{pmatrix}$ où les a_i sont des complexes.

1. Rappeler la définition du polynôme minimal d'une matrice.

2. Calculer $\det(A)$ et A^2.

3. Donner une CNS sur les a_i pour que A soit diagonalisable.

Indication 3 Pour 3. on pourra distinguer les cas selon la parité de n.

Solution 3

1. $\{P \in \mathbb{C}[X] / \ P(A) = 0\}$ est un idéal de $\mathbb{C}[X]$ qui n'est pas réduit à $\{0\}$. Comme $\mathbb{C}[X]$ est principal, cet idéal est principal et possède un unique générateur unitaire. On l'appelle le polynôme minimal. C'est l'unique polynôme unitaire annulateur qui divise tous les polynômes annulateurs.

2. Pour calculer $\det(A)$, on peut faire des développements successifs selon la dernière colonne. On obtient
$$\det(A) = (-1)^{(n+1)+n+\cdots+3+2} a_1 \dots a_n = (-1)^{\frac{n(n+3)}{2}} \prod_{i=1}^{n} a_i$$
Une autre façon de raisonner est d'échanger les lignes 1 et n, puis 2 et $n-1$ etc. Chaque échange multiplie le déterminant par -1 et à la fin on a un déterminant diagonal. Ainsi
$$\det(A) = (-1)^{\lfloor n/2 \rfloor} \prod_{i=1}^{n} a_i$$
Le calcul de A^2 est immédiat :
$$A^2 = \operatorname{diag}(a_1 a_n, a_2 a_{n-1}, \dots, a_n a_1)$$

3. Le calcul précédente montre que l'on a envie de regrouper par deux les vecteurs de la base canonique. Selon que n est ou non pair, il restera ou non un vecteur "seul".
Cas $n = 2p$ **pair**.
Notons u l'endomorphisme canoniquement associé c'est à dire représenté par A dans la base canonique $(e_1, \dots, e_{2p})$ de $\mathbb{C}^{2p}$. Raisonnons par conditions nécessaires puis suffisantes.
   - Supposons A (et donc u) diagonalisable. Pour tout $i \in [1..p]$, $F_i = \operatorname{Vect}(e_i, e_{2p+1-i})$ est stable par u ($u(e_i) = a_i e_{2p+1-i}$) et u induit sur F_i un endomorphisme u_i qui est aussi diagonalisable. La matrice de u_i dans la base (e_1, e_{2p+1-i}) est donc diagonalisable. Elle vaut $M_i = \begin{pmatrix} 0 & a_{2p+1-i} \\ a_i & 0 \end{pmatrix}$ et son polynôme caractéristique est $X^2 - a_i a_{2p+1-i}$. La diagonalisablité de M_i entraîne que $a_i a_{2p+1-i} \neq 0$ (deux valeurs propres distinctes) ou $a_i = a_{2p+1-i} = 0$ (0 valeur propre double).
   - Réciproquement, on suppose que
$$\forall i \in [1..p], \ a_i a_{2p+1-i} \neq 0 \ \text{ ou } \ a_i = a_{2p+1-i} = 0$$
Chaque M_i et donc chaque F_i est diagonalisable. On peut ainsi trouver une base de F_i formée de vecteurs propres pour u. En concaténant ces bases, on obtient une base de E formée de vecteurs propres pour u et u est diagonalisable.

   Cas $n = 2p + 1$ **pair**.
La condition est de même $\forall i \in [1..p], \ a_i a_{2p+2-i} \neq 0 \ \text{ ou } \ a_i = a_{2p+2-i} = 0$ et il n'y a pas de condition sur a_{p+1}.

Planche 4
Soit $P = X^p + \sum\limits_{k=0}^{p-1} a_k X^k \in \mathbb{C}[X]$.

1. Montrer que $D : (u_n)_{n\in\mathbb{N}} \mapsto (u_{n+1})_{n\in\mathbb{N}}$ est un endomorphisme de $\mathbb{C}^{\mathbb{N}}$.
On pose
$$\forall n \in \mathbb{N}, \ v_n = u_{n+p} + \sum_{k=0}^{p-1} a_k u_{n+k}$$

2. (a) Montrer que $v = P(D)(u)$.
   (b) Montrer que la convergence de u entraine celle de v.
   (c) On note E l'ensemble des polynômes unitaires de $\mathbb{C}[X]$ tels que la convergence de $P(D)(u)$ entraine toujours celle de u. Montrer que, pour P et Q unitaires, $PQ \in E$ si et seulement si $P, Q \in E$.
   (d) En déduire que $P \in E$ si et seulement si toute racine de P est en module strictement inférieure à 1.

Indication 4 Pour 2.(d) on pourra d'abord étudier le cas où $P = X - a$.

Solution 4

1. $D(u + \lambda v) = D(u) + \lambda D(v)$ et D va de $\mathbb{C}^{\mathbb{N}}$ dans lui même. On a donc bien un endomorphisme de $\mathbb{C}^{\mathbb{N}}$.

2. (a) D^k est l'application qui à $(u_n)_{n\geq 0}$ associe $(u_{n+k})_{n\geq 0}$. Par combinaison linéaire, la suite $w = P(D)(u)$ vérifie
$$\forall n \in \mathbb{N},\ w_n = u_{n+p} + \sum_{k=0}^{p-1} a_k u_{n+k}$$
et c'est donc la suite v.
   (b) Si $u_n \to \ell$ alors $\forall k,\ u_{n+k} \to \ell$ et donc $v_n \to \ell.P(1)$.
   (c) On a $(PQ)(D) = P(D) \circ Q(D)$.
Supposons $P, Q \in E$ et considérons une suite u telle que $(PQ)(D)(u) = P(D)(Q(D)(u))$ converge. Comme $P \in E$, ceci entraine la convergence de $Q(D)(u)$. Et comme $Q \in E$, on en déduit la convergence de u. On a donc $PQ \in E$.
On suppose réciproquement que $PQ \in E$. Soit $u \in \mathbb{C}^{\mathbb{N}}$ telle que $Q(D)(u)$ converge. Avec 2(b) on a donc convergence de $P(D)(Q(D)(u)) = (PQ)(D)(u)$. Comme $PQ \in E$, on en déduit que u converge. ceci montre que $Q \in E$. Comme $PQ = QP$, on montre de même que $P \in E$.
   (d) Traitons d'abord le cas d'un polynôme unitaire de degré 1, c'est à dire le cas $P = X - a$.
Soit $u \in \mathbb{C}^{\mathbb{N}}$ et $v = P(D)(u)$ de sorte que pour tout $n \in \mathbb{N}$, $v_n = u_{n+1} - au_n$.
Ou bien $a = 0$ et alors u est clairement convergente si et seulement si v l'est (décalée).
On suppose donc dorénavant que $a \neq 0$. On a, pour tout $n \in \mathbb{N}^*$, $\frac{v_{n-1}}{a^n} = \frac{u_n}{a^n} - \frac{u_{n-1}}{a^{n-1}}$.
On suppose que $|a| < 1$ et que v converge vers ℓ. Montrons que u converge : ainsi $X - a \in E$.
On écrit $\frac{v_n}{a^n} = \frac{\ell}{a^n} + o\left(\frac{1}{a^n}\right)$. Par sommation des relations de comparaison, cas divergent, on a (après télescopage)
$$\frac{u_n}{a^n} - u_0 = \frac{\ell}{a}\frac{(1/a)^{n+1} - 1}{(1/a) - 1} + o((1/a)^n)$$
et donc
$$u_n = \frac{\ell}{a-1} + o(1).$$
u est bien convergente.
Réciproquement, supposons $P = X - a \in E$ et montrons que $|a| < 1$.
   - Supposons que $|a| \geq 1$ et $a \neq 1$. Posons $u_n = a^n$. On a alors $v_n = 0$. (v_n) converge mais pas (u_n) : contradiction.
   - Supposons $a = 1$ et posons $u_n = \sqrt{n}$. On a $v_n = \sqrt{n+1} - \sqrt{n} = \frac{1}{\sqrt{n+1}+\sqrt{n}} \to 0$. (v_n) converge mais pas (u_n) : contradiction.

On a montré que $X - a \in E$ si et seulement si $|a| < 1$.
Le résultat général s'en déduit en décomposant P en produit de facteurs unitaires de degré 1 (possible dans $\mathbb{C}$).

Planche 5
Soit p un entier premier impair. On note $F_p = \mathbb{Z}/p\mathbb{Z}$ et $C = \{x^2/\ x \in F_p \setminus \{0\}\}$.

1. (a) Quelle est la structure algébrique de F_p ? De $F_p \setminus \{0\}$?
   (b) Dans le cas $p = 11$, donner C.
2. Soit $P \in \mathbb{Z}[X]$ tel que $\deg(P) < d$ où $d \in \mathbb{N}^*$. Soient $a_1, \ldots, a_d \in [\![1, p-1]\!]$ distincts tels que $\forall i,\ p|P(a_i)$. Montrer que $\forall n \in \mathbb{Z},\ p|P(n)$.
3. Montrer que C est composé des racines dans F_p de $X^{\frac{p-1}{2}} - 1$ et est de cardinal $\frac{p-1}{2}$.

Indication 5

Solution 5

1. F_p est un corps et $F_p \setminus \{0\}$ est le groupe des inversibles de ce corps/anneau.
   Comme $(-x)^2 = x^2$, il suffit de chercher les carrés modulo 11 de $1, 2, 3, 4, 5$ et on trouve
   $$C = \{\overline{1}, \overline{4}, \overline{9}, \overline{5}, \overline{3}\}$$
2. Dire que $p|P(a_i)$, c'est dire que $\overline{a_i}$ est racine de P considéré comme polynôme à coefficients dans F_p, que l'on choisit de noter $\widetilde{P}$. Il est donc, dans F_p, factorisable par le produit des $(X - \overline{a_i})$. Pour des raisons de degré, $\widetilde{P} = 0$ et donc tous les coefficients de P sont multiples de p. Finalement, pour tout entier n, $P(n)$ est multiple de p.

   On peut procéder autrement : posons
   $$\forall i \in [\![1, d]\!],\ L_i = \prod_{j \neq i} \frac{X - a_j}{a_i - a_j}$$
   On a alors (interpolation de Lagrange, P de degré $< d$ est caractérisé par les valeurs prises en d points)
   $$P = \sum_{i=1}^{d} P(a_i) L_i$$
   Posons c égal au produit de tous les $a_j - a_i$ pour $i < j$. On a alors
   $$cP(n) = \sum_{i=1}^{n} P(a_i) c L_i(n)$$
   Par choix de c, $cL_i(n)$ est entier et tous les termes de la somme sont des entiers multiples de p. On en déduit que $p|cP(n)$. Mais par choix de c, et comme p est premier, $c \wedge p = 1$. Par lemme de Gauss, $p|P(n)$.
3. D'après le théorème de Fermat, $\forall n \in \mathbb{N}$, si $n \wedge p = 1$ alors $n^{p-1} = 1[p]$, ce qui revient à dire que l'ordre d'un élément du groupe $F_p \setminus \{0\}$ divise le cardinal du groupe $(p-1)$. On en déduit que si $y \in C$, c'est à dire s'écrit $y = x^2$, alors $y^{\frac{p-1}{2}} = x^{p-1} = 1$ dans F_p. Tous les éléments de C sont racines de $X^{\frac{p-1}{2}} - 1$ dans F_p.
   Par ailleurs, $X^2 = k$ avec $k \in F_p \setminus \{0\}$ admet au plus deux solutions, ce qui signifie que seuls deux éléments peuvent donner le même carré. Il y a donc au moins $\frac{p-1}{2}$ carrés.
   Comme $X^{\frac{p-1}{2}} - 1$ a au plus $\frac{p-1}{2}$ racines, on a le résultat annoncé.

Planche 6
Soient $A, B \in \mathcal{M}_n(\mathbb{C})$.

1. On suppose que pour tout $M \in \mathcal{M}_n(\mathbb{C})$, $\chi_{AM+B} = \chi_{AM}$.
   (a) Montrer qu'il existe $p \in \mathbb{N}^*$ tel que $B^p = 0$.
   (b) Montrer que $BA = 0$.
2. On suppose que B est nilpotente et que $BA = 0$. Montrer que $\chi_{AM+B} = \chi_{AM}$ est vrai pour tout M.

Indication 6 Pour 2., on remarquera que pour $t \neq 0$, $tI_n - B$ est inversible.

Solution 6

1. (a) En prenant $M = 0$, on obtient $\chi_B = X^n$ et B est nilpotente par le théorème de Cayley-Hamilton.
   (b) Comme AM et $AM + B$ ont même polynôme caractéristique, elles ont mêmes valeurs propres avec mêmes multiplicités. Il en va de même pour les carrés de ces valeurs propres et donc $(AM)^2$ et $(AM + B)^2 = (AM)^2 + AMB + BAM + B^2$ ont même trace. Comme B^2 est de trace nulle,
   $$\mathrm{Tr}(AMB) + \mathrm{Tr}(BAM) = 0$$
   et donc $2\mathrm{Tr}(BAM) = 0$. Comme ceci est vrai pour tout M, $BA = 0$ (prendre pour M les $E_{i,j}$).
2. Pour la réciproque, comme B est nilpotente alors $tI_n - B$ est inversible si $t \neq 0$. Puisque $\det(tI_n - B) = t^n$, on a
   $$\det(tI_n - AM - B) = t^n \det(I_n - (tI_n - B)^{-1}AM) = \det(tI_n - t(tI_n - B)^{-1}AM)$$
   Comme $BA = 0$, $(tI_n - B)A = tA$ et donc $A = t(tI_n - B)^{-1}A$. Finalement
   $$\det(tI_n - AM - B) = \det(tI_n - AM).$$

Planche 7
Soit G un sous-groupe de $(\mathbb{C}^*, \times)$ tel que pour tout $g \in G$, il existe un voisinage V de g tel que $V \cap G = \{g\}$. On note $\mathbb{U}$ l'ensemble des complexes de module 1.

1. Soient $g_1, g_2 \in G$. Décrire le groupe G_1 engendré par g_1 et celui G_2 engendré par g_1 et g_2.
2. (a) Soit $K \subset \mathbb{C}^*$ un compact. Montrer que $K \cap G$ est fini.
   (b) Montrer que $G \cap \mathbb{U}$ est cyclique.
3. On suppose G non inclus dans $\mathbb{U}$ et on note G^* l'ensemble des éléments de G de module > 1. Montrer que G^* possède un élément g_2 de module minimal.

Indication 7 Pour $(z, z') \in G^2$, $|z - z'| = |zz'^{-1} - 1|\,|z'|$.

Solution 7

1. On a
$$G_1 = \{g_1^k / \ k \in \mathbb{Z}\}$$
Comme la multiplication est commutative dans $\mathbb{C}$, on a
$$G_2 = \{g_1^k g_2^\ell / \ k, \ell \in \mathbb{Z}\}$$
Dans les deux cas, l'inclusion réciproque est immédiate car G_i est un groupe et donc stable par multiplication ou passage à l'inverse. On prouve l'égalité en justifiant que les ensembles des membres de droite sont effectivement des sous-groupes (car ce sont alors les plus petits sous-groupes qui contiennent respectivement g_1 pour l'un, g_1 et g_2 pour l'autre).

2. (a) Supposons, par l'absurde, que $K \cap G$ soit infini. On peut alors construire une suite (z_n) d'éléments de $K \cap G$ constituée d'éléments deux à deux distincts. De cette suite d'éléments de K, on peut extraire une sous-suite $(z_{\varphi(n)})$ qui converge vers un élément $z \in K$ (Bolzano-Weierstrass). Quitte à travailler avec l'extraite, on suppose donc que $z_n \to z \in K$.
Pour tous $p, q \in \mathbb{N}$, $|z_p z_q^{-1} - 1| = |z_p - z_q|.|z_q^{-1}| \leq c|z_p - z_q|$ où $c > 0$ est tel que $\forall x \in K, \ |x| \geq c$ (un tel c existe puisque K est compact et donc $x \mapsto |x|$ atteint son minimum sur K et ce minimum est > 0 car $0 \notin K$). On en déduit que pour p, q arbitrairement grands, $|z_p z_q^{-1} - 1|$ est arbitrairement petit.
Or, $1 \in G$ (sous-groupe) et il existe donc $r > 0$ tel que $\forall y \in G \setminus \{1\}, \ |y - 1| \geq r$.
On en déduit que pour p, q assez grand $z_p z_q^{-1} = 1$, c'est à dire que la suite (z_n) est stationnaire à partir d'un certain rang et ceci contredit notre hypothèse initiale sur cette suite.
   (b) $\mathbb{U}$ étant un compact inclus dans $\mathbb{C}^*$, $G \cap \mathbb{U}$ est fini et comme c'est un groupe, c'est un groupe fini. On note n son cardinal. Pour tout $g \in G \cap \mathbb{U}$, $g^n = 1$. On en déduit que $G \cap \mathbb{U} \subset \mathbb{U}_n$. On a l'égalité par égalité des cardinaux.

3. Si G n'est pas inclus dans $\mathbb{U}$, il possède un élément g de module différent de 1 et comme $g^{-1} \in G$, il possède un élément de module > 1. L'ensemble $\{|g| / \ g \in G^*\}$ est ainsi non vide. Comme il est minoré par 1, il possède une borne inférieure.
Si cette borne inférieure α n'est pas un minimum, on construit facilement (par récurrence) une suite (z_n) d'éléments de G^*, telle que $(|z_n|)$ décroît strictement vers α. En notant $K = \{z \in \mathbb{C} / \ 1 \leq |z| \leq |z_0|\}$, qui est un compact, on a ainsi une suite (z_n) d'éléments de $K \cap G$. Comme plus haut, on peut, quitte à extraire, la supposer convergente et obtenir une contradiction.

Planche 8
Soit $M \in \mathcal{M}_n(\mathbb{C})$ une matrice nilpotente.

1. Justifier l'existence de $p = \min\{d \in \mathbb{N} / \ M^d = 0\}$. Montrer que $p \leq n$.
2. Montrer que $M^2 - I_n$ est inversible et trouver son inverse.
3. Etudier l'inversibilité de $M^4 + M^3 + M^2 + M + I_n$. *Enoncé incomplet.*

Indication 8

Solution 8

1. $\{d \in \mathbb{N} / \ M^d = 0\}$ est non vide par définition d'une matrice nilpotente. Cet ensemble étant inclus dans $\mathbb{N}$, il admet un minimum p.
M possède un annulateur du type X^k et 0 est donc son unique valeur propre complexe. Son polynôme caractéristique (dans $\mathbb{C}$, tout polynôme est scindé) est alors X^n et comme il annule M, on a $p \leq n$.

2. M^2 est aussi nilpotente et donc 0 est son unique valeur propre. 1 n'est donc pas dans le spectre de M^2 et $M^2 - I_n$ est inversible.
   On vérifie que
   $$(M^2 - I_n)\sum_{k=0}^{n} M^{2k} = \sum_{k=0}^{n} M^{2(k+1)} - \sum_{k=0}^{n} M^{2k} = M^{2(n+1)} - I_n = -I_n$$
   On en déduit que
   $$(M^2 - I_n)^{-1} = -\sum_{k=0}^{n} M^{2k}$$
   On peut sommer uniquement jusqu'à $\lfloor n/2 \rfloor$, les itérées suivantes étant nulles.

3. $N = M^4 + M^3 + M^2 + M = M(M^3 + M + M + I_n)$ est nilpotente (car M l'est) et -1 n'en est pas valeur propre. Ainsi, $N + I_n$ est inversible.
   On a, de même que précédemment,
   $$(N + I_n)\sum_{k=0}^{n-1}(-1)^k N^k = I_n.$$
   Donc,
   $$(I_n + M + M^2 + M^3 + M^4)^{-1} = \sum_{k=0}^{n-1}(-1)^k(M + M^2 + M^3 + M^4)^k.$$

Planche 9
On cherche les morphismes continus de $\mathbb{U}$ dans $GL_n(\mathbb{C})$. On se donne un tel morphisme et on note $\tilde{\varphi}(t) = \varphi(e^{it})$.

1. Soit $\|.\|$ une norme sur $\mathcal{M}_n(\mathbb{C})$. Soit $\varepsilon > 0$. Montrer qu'il existe $\alpha > 0$ tel que
   $$\left\| I_n - \frac{1}{\alpha}\int_0^{\alpha} \tilde{\varphi}(t)\, dt \right\| \leq \varepsilon$$

2. Justifier que $\tilde{\varphi}$ est dérivable. Justifier alors qu'il existe une matrice A telle que $\tilde{\varphi}(t) = \exp(tA)$.

3. Conclure.

Indication 9 Pour 2., on pourra poser $F : x \mapsto \int_0^x \tilde{\varphi}(t)\, dt$. Pour la dernière question, on pourra admettre, quitte à le démontrer ensuite (penser alors à Dunford), que si $\exp(M)$ est diagonalisable alors M l'est aussi.

Solution 9

1. φ étant continu, $\tilde{\varphi}$ l'est aussi. Pour tout $\varepsilon > 0$, il existe donc $\alpha > 0$ tel que $\|\tilde{\varphi}(t) - \tilde{\varphi}(0)\| \leq \varepsilon$ pour tout $|t| \leq \alpha$. On notera que $\tilde{\varphi}(0) = \varphi(1) = I_n$ (car φ est un morphisme multiplicatif). Ainsi,
   $$\left\| I_n - \frac{1}{\alpha}\int_0^{\alpha} \tilde{\varphi}(t)\, dt \right\| = \left\| \frac{1}{\alpha}\int_0^{\alpha} (\tilde{\varphi}(0) - \tilde{\varphi}(t))\, dt \right\| \leq \frac{1}{\alpha}\int_0^{\alpha} \|\tilde{\varphi}(0) - \tilde{\varphi}(t)\|\, dt \leq \varepsilon$$

2. Posons $F(x) = \int_0^x \tilde\varphi(t)\ dt$. Comme $GL_n(\mathbb{C})$ est un ouvert et comme I_n est inversible, avec la question précédente $F(\alpha)/\alpha$ et donc $F(\alpha)$ est inversible pour $\alpha > 0$ petit. On se donne un tel α et on écrit que
$$\int_0^\alpha \tilde\varphi(x+t)\ dt = \int_0^\alpha \tilde\varphi(x)\tilde\varphi(t)\ dt = \tilde\varphi(x)F(\alpha)$$
ce que l'on peut écrire
$$\tilde\varphi(x) = \left(\int_0^\alpha \tilde\varphi(x+t)\ dt\right).(F(\alpha))^{-1} = (F(x+\alpha) - F(x)).(F(\alpha))^{-1}$$
Comme $\tilde\varphi$ est continue, F est de classe C^1 et $\tilde\varphi$ l'est donc aussi.
On a $\tilde\varphi(t+s) = \tilde\varphi(t)\tilde\varphi(s)$. En dérivant par rapport à t et en donnant à t la valeur 0, on obtient
$$\tilde\varphi'(s) = \tilde\varphi'(0)\tilde\varphi(s)$$
et d'après le cours
$$\tilde\varphi(s) = \exp(sA)\tilde\varphi(0) \ \text{ avec } \ A = \tilde\varphi'(0)$$
Comme $\tilde\varphi(0) = I_n$, on a le résultat voulu.

3. $\tilde\varphi$ étant 2π-périodique, $\exp(tA) = \exp((t+2\pi)A) = \exp(tA)\exp(2\pi A)$ et ainsi $\exp(2\pi A) = I_n$.
Admettons provisoirement le résultat suivant : si $\exp(M)$ est diagonalisable alors M est diagonalisable.
Ici, on en déduit que $2\pi A$ est diagonalisable et que donc A l'est aussi. Il existe une matrice inversible P telle que $P^{-1}AP = \text{diag}(\lambda_1, \dots, \lambda_n)$. On a alors
$$I_n = \exp(2\pi A) = P\text{diag}(e^{2\pi\lambda_1}, \dots, e^{2\pi\lambda_n})P^{-1}$$
On peut en conclure que $e^{2\pi\lambda_k} = 1$ et donc que $\lambda_k \in i\mathbb{Z}$. Finalement, il existe des entiers $p_1, \dots, p_n$ tels que
$$\varphi(e^{it}) = \tilde\varphi(t) = P\text{diag}(e^{ip_1t}, \dots, e^{ip_nt})P^{-1}$$
On a montré que les seules applications envisageables sont du type
$$z \mapsto P\text{diag}(z^{p_1}, \dots, z^{p_n})P^{-1}$$
avec $P \in GL_n(\mathbb{C})$ et $p_1, \dots, p_n \in \mathbb{Z}$.
Il reste à vérifier que ces fonctions conviennent (ce sont des morphismes continus de $\mathbb{U}$ dans $GL_n(\mathbb{C})$).

Pour la preuve du résultat admis, on utilise la décomposition de Dunford. On suppose que $\exp(M)$ est diagonalisable et on écrit $M = D + N$ où D est une matrice diagonalisable et N une matrice nilpotente qui commutent. On a ainsi $\exp(M) = \exp(D)\exp(N)$ ou encore $\exp(N) = \exp(-D)\exp(M)$. Comme $MD = DM$ (car N et D commutent), $\exp(M)$ et $\exp(D)$ commutent. Or, ces matrices sont diagonalisables et elles sont donc co-diagonalisables ce qui permet de montrer que $\exp(N)$ est diagonalisable. Or,
$$\exp(N) = I_n + N + \frac{N^2}{2!} + \dots + \frac{N^{n-1}}{(n-1)!}$$
permet de montrer que $\exp(N) - I_n$ est nilpotente (car N l'est) et donc que 0 est sa seule valeur propre. Ainsi (par diagonalisabiité de $\exp(N) - I_n$) $\exp(N) = I_n$ et avec l'identité ci-dessus, $N + \frac{N^2}{2!} + \frac{N^{n-1}}{(n-1)!} = 0$. On a un polynôme annulateur Q de N qui est multiple du polynôme minimal de N qui est du type X^k et comme $Q = XR$ avec $R(0) = 1 \neq 1$, il faut que $k = 1$ c'est à dire $N = 0$. M est ainsi diagonalisable.

Planche 10

On considère $A \in \mathcal{M}_n(\mathbb{R})$ symétrique que l'on note par blocs : $A = \begin{pmatrix} B_p & C_p \\ {}^tC_p & D_p \end{pmatrix}$ où $p \in \{1, \dots, n-1\}$ et $B_p \in \mathcal{M}_p(\mathbb{R})$ et $D_p \in \mathcal{M}_{n-p}(\mathbb{R})$.

1. On dit que A est *définie positive* si et seulement si : $\forall X \in \mathbb{R}^n \setminus \{0\},\ {}^tX\ AX > 0$ (on identifie $\mathbb{R}^n$ et les matrices unicolonnes).

   Montrer que A est définie positive si et seulement si $\mathrm{Sp}(A) \subset]0, +\infty[$.

On suppose désormais que A est définie positive.

2. Montrer que $\det(B_p) > 0$.
3. Montrer que $\det(A) \leq \det(B_p)\det(D_p)$ puis en déduire que $\det(A) \leq a_1 a_2 \cdots a_n$ où $a_1, a_2, \dots, a_n$ sont les coefficients diagonaux de A.

Indication 10 En notant $q = n - p$, on pourra remarquer que :

$$A = \begin{pmatrix} I_p & C_p D_p^{-1} \\ 0 & I_q \end{pmatrix} \begin{pmatrix} B_p - C_p D_p^{-1t} C_p & 0 \\ 0 & D_p \end{pmatrix} \begin{pmatrix} I_p & 0 \\ D_p^{-1t} C_p & I_q \end{pmatrix}$$

Par ailleurs, si B_p est définie positive, elle possède une racine carrée définie positive.
On pourra enfin montrer que $B_p - C_p D_p^{-1t} C_p$ est symétrique positive.

Solution 10

1. Cours.
2. B_p est symétrique. Soit $Y \in \mathbb{R}^p$. On le complète en $X \in \mathbb{R}^n$ en ajoutant des 0. On a alors

   $${}^tXAX = {}^tYBY$$

   Si $Y \neq 0$ alors $X \neq 0$ et la quantité précédente est > 0, ce qui montre que B_p est définie positive.
   B_p a donc des valeurs propres > 0 et comme elle est diagonalisable, son déterminant est le produit des valeurs propres (avec multiplicités). Ainsi $\det(B_p) > 0$.

3. On prouve exactement comme ci-dessus que D_p est définie positive et donc à spectre inclus dans $\mathbb{R}^{+*}$. En particulier, 0 n'est pas valeur propre et D_p est inversible.
   On vérifie ensuite sans peine l'égalité proposée grace à un calcul matriciel par blocs et on en déduit, en passant au déterminant, que

   $$\det(A) = \det(B_p - C_p D_p^{-1t} C_p)\det(D_p)$$

   Il s'agit désormais de prouver que $\det(B_p - C_p D_p^{-1t} C_p) \leq \det(B_p)$ et on s'intéresse tout d'abord à la matrice dans le déterminant de gauche.
   Montrons que $M = B_p - C_p D_p^{-1t} C_p$ (qui est symétrique) est positive. Pour cela, on remarque avec l'expression de A par blocs que pour X définie par blocs avec Y et Z on a

   $${}^tXAX = {}^tY(B_p - C_p D_p^{-1t} C_p)Y + {}^t(Z + D_p^{-1t} C_p Y) D_p (Z + D_p^{-1t} C_p Y)$$

   Pour $Y \in \mathbb{R}^p$ quelconque et en prenant $Z = -D_p^{-1t} C_p Y$ on obtient ${}^tY(B_p - C_p D_p^{-1t} C_p)Y \geq 0$, ce que l'on voulait.

Comme B_p est symétrique définie positive, elle s'écrit $Q^{-1}\Delta Q$ avec Q orthogonale et Δ diagonale à coefficients diagonaux > 0. En notant Δ_1 la matrice diagonale dont les coefficients sont les racines carrées de ceux de Δ, on a alors $B_p = S^2$ avec $S = Q^{-1}\Delta_1 Q$ et S est encore symétrique définie positive.

On peut alors écrire que $B_p - C_p D_p^{-1t}C_p = S(I_p - S^{-1}C_p D_p^{-1t}C_p S^{-1})S = S(I_p - S_1)S$.

- S_1 est symétrique de taille p.
- Soit $Z \in \mathbb{R}^p$. ${}^tZS_1Z = {}^tYD_p^{-1}Y$ avec $Y = {}^tC_pS^{-1}X$ et ainsi ${}^tZS_1Z \geq 0$ car D_p^{-1} est symétrique positive.

On a donc S_1 qui est symétrique positive. $\det(I_p - S_1)$ est le produit des $1-\lambda$ où les λ sont les valeurs propres de S_1. Comme $1 - \lambda \leq 1$ (positivité de S_1), il suffit de prouver que $1 - \lambda \geq 0$ pour conclure que le déterminant de $I_p - S_1$ est ≤ 1. Il nous reste donc à montrer que $I_p - S_1$ est positive. Et pour cela on écrit que $I - S_1 = S^{-1}MS^{-1}$ et on utilise le fait que M est symétrique positive (montré plus haut).

On a finalement montré que

$$\det(A) \leq \det(B_p)\det(D_p)$$

Le dernier résultat en découle par récurrence (travailler avec $p = n-1$ pour faire apparaître a_n et utiliser la récurrence avec B_{n-1}) :

$$\det(A) \leq \prod_{i=1}^{n} a_i$$

Planche 11

Soit $(E, \|\cdot\|)$ un $\mathbb{R}-$ev normé.

Pour $A \subset E$ non vide et $x \in E$, on rappelle que la distance entre A et x est définie par :

$$d(x, A) = \inf_{a\in A} \|x - a\|$$

et pour $r > 0$, on pose $A(r) = \{x \in E/\ d(x, A) \leq r\}$.

1. Montrer que la distance à une partie X non vide est en fait un minimum lorsque X est une partie compacte.
2. Soit A et B deux parties bornées non vides.

   On pose : $\delta(A, B) = \min\{r \geq 0/\ A \subset B(r) \text{ et } B \subset A(r)\}$.

   Montrer l'existence de $\delta(A, B)$.
3. Application : pour $E = \mathbb{R}^2$, $A = [-1, 1]^2$ et B la boule ouverte unité pour la norme 2, calculer $\delta(A, B)$.
4. Soit A, B et C des bornés non vides de E.

   (a) A quelle condition nécessaire et suffisante a-t-on $\delta(A, B) = 0$?

   (b) Etablir que : $\delta(A, C) \leq \delta(A, B) + \delta(B, C)$.

Indication 11 Pour 4.b. montrer que $A \subset C(\delta(A, B) + \delta(B, C))$.

Solution 11

1. Par caractérisation de la borne inférieure, il existe une suite (a_n) d'éléments de X telle que $\|x - a_n\| \to d(x, X)$.
   Comme X est supposé compact, on peut trouver une extractrice φ telle que $(a_{\varphi(n)})$ converge vers un élément $a \in X$.
   Par continuité du passage à la norme, $d(x, X) = \|x - a\|$ et comme $a \in X$, la distance est atteinte et est un minimum.

2. A et B étant non vides, on peut trouver $a \in A$ et $b \in B$. Et comme ils sont bornés et il existe R_A, R_B tels que $A \subset \overline{B}(0, R_A)$ et $B \subset \overline{B}(0, R_B)$.
   Posons $r = \|b\| + R_A$. Soit $x \in A$ alors $\|x\| \leq R_A$ donc $\|x - b\| \leq \|x\| + \|b\| \leq r$ et $d(x, B) \leq r$ i.e. $x \in B(r)$. Ainsi $A \subset B(r)$.
   On procède de même pour montrer que $B \subset A(r')$ avec $r' = \|a\| + R_B$.
   $\max(r, r')$ est alors un élement de $\{r \geq 0/\ A \subset B(r) \text{ et } B \subset A(r)\}$ et cet ensemble est non vide.
   Comme il est minoré (par 0), il admet une borne inférieure α.
   Il est clair que $]\alpha, +\infty[\subset \{r \geq 0/\ A \subset B(r) \text{ et } B \subset A(r)\} \subset [\alpha, +\infty[$
   Soit $x \in A$. On a $\forall r > \alpha,\ x \in B(r)$ et donc $d(x, B) \leq r$. On en déduit que $d(x, B) \leq \alpha$ et donc $x \in B(\alpha)$. Ainsi $A \subset B(\alpha)$. De même $B \subset A(\alpha)$. α est donc en réalité un minimum.

3. Il faut bien sûr commencer par faire un dessin. On note aussi que A et B sont bornées et non vides.
   Ici, $B \subset A(r)$ est vrai pour tout $r > 0$. On cherche donc le minimum des r tels que $A \subset B(r)$. Or, $B(r)$ est la boule fermée de centre l'origine et de rayon $r + 1$. Les r convenables sont donc ceux tels que $r + 1 \geq \sqrt{2}$. Ainsi
   $$\delta(A, B) = \sqrt{2} - 1$$

4.
   (a) Soit C une partie bornée non vide de E. Si $y \in C(0)$ alors $d(y, C) = 0$ et il existe une suite (x_n) d'éléments de C telle que $\|y - x_n\| \to 0$. On a donc $y \in \overline{C}$. Réciproquement, $\overline{C} \subset C(0)$. Ainsi, $C(0) = \overline{C}$.

   Si $\overline{A} = \overline{B}$ alors $A \subset \overline{B} = B(0)$ et de même $B \subset A(0)$. Ainsi $\Delta(A, B) = 0$.

   Réciproquement, on suppose que $\delta(A, B) = 0$. On a alors $A \subset \overline{B}$ et $B \subset \overline{A}$. On en déduit aisément que A et B ont même adhérence.
   $$\delta(A, B) = 0 \iff \overline{A} = \overline{B}$$

   (b) Soit $x \in A$. Comme $A \subset B(\delta(A, B))$, $d(x, B) \leq \delta(A, B)$.
   Ainsi, pour tout $n \in \mathbb{N}$, il existe $y_n \in B$ tel que $\|x - y_n\| \leq \delta(A, B) + \frac{1}{2^n}$.
   Soit $n \in \mathbb{N}$, comme $B \subset C(\delta(B, C))$, $d(y_n, C) \leq \delta(B, C)$.
   Ainsi il existe $z_n \in C$ tel que $\|y_n - z_n\| \leq \delta(B, C) + \frac{1}{2^n}$.
   On a donc $\|x - z_n\| \leq \|x - y_n\| + \|y_n - z_n\| \leq \delta(A, B) + \delta(B, C) + \frac{2}{2^n}$.
   Comme $z_n \in C$, on conclut que $d(x, C) \leq \delta(A, B) + \delta(B, C) + \frac{2}{2^n}$.
   Ceci étant vrai pour tout $n \in \mathbb{N}$, alors $d(x, C) \leq \delta(A, B) + \delta(B, C)$.
   Ceci est vrai pour tout $x \in A$ et donc $A \subset C(\delta(A, B) + \delta(B, C))$.
   De même $C \subset A(\delta(A, B) + \delta(B, C))$ et ainsi
   $$\delta(A, C) \leq \delta(A, B) + \delta(B, C).$$

Planche 12

Soit $A \in \mathcal{M}_n(\mathbb{C})$. On note $\mathrm{Com}(A)$ la comatrice de A. On suppose qu'il existe $k \in \mathbb{C}$ tel que
$$A + {}^t\mathrm{Com}(A) = kI_n$$

1. Montrer que $|\mathrm{Sp}(A)| \leq 2$.
   On suppose maintenant que $|\mathrm{Sp}(A)| = 2$ et on note a, b les valeurs propres. Montrer que A est diagonalisable.

2. On note m_1, m_2 les multiplicité de a, b et on suppose $ab \neq 0$. Montrer que $a^{m_1-1}b^{m_2-1} = 1$.

3. On suppose $a = 0$. Montrer que $m_1 = 1$ et $b^{n-2} = 1$.

Indication 12 Pour 3. on pourra montrer que $\mathrm{Com}(MN) = \mathrm{Com}(M)\mathrm{Com}(N)$ pour toutes matrices M et N.

Solution 12
On rappelle que

$$A.{}^t\mathrm{Com}(A) = {}^t\mathrm{Com}(A).A = \det(A)I_n$$

1. En multipliant l'égalité par A, on obtient que $X^2 - kX + \det(A)$ annule A. Les valeurs propres de A, qui sont racines de tout polynôme annulateur, sont donc en nombre ≤ 2.
   Si on suppose qu'il y a deux valeurs propres distinctes, alors le polynôme minimal de A est au moins de degré 2. Comme il divise tout polynôme annulateur et qu'on a un annulateur de degré 2, il est de degré 2 et vaut $(X - a)(X - b) = X^2 - kX + \det(A)$. Il est scindé simple et A est diagonalisable.

2. A étant diagonalisable (en fait, la trigonalisabilité dans $\mathbb{C}$ suffit), on a $\det(A) = a^{m_1}b^{m_2}$. Mais les deux formes du polynôme minimal donnent aussi $\det(A) = ab$. Ainsi $a^{m_1}b^{m_2} = ab$ et comme $ab \neq 0$, on peut diviser par ab pour obtenir le résultat demandé.

3. Si A est de rang $\leq n-2$ alors tout déterminant extrait de taille $n-1$ de A est nul et la comatrice de A est nulle. $A = kI_n$ est alors scalaire et ceci contredit l'hypothèse de deux valeurs propres.
   Si $a = 0$, A est non inversible et de rang $\geq n - 1$. Elle est donc de rang $n - 1$. Son noyau est de dimension 1 et comme A est diagonalisable, la multiplicité de la valeur propre $a = 0$ vaut 1. Ainsi $m_1 = 1$. Comme $m_1 + m_2 = n$, $m_2 = n - 1$.
   A est semblable à $D = \mathrm{diag}(b, \dots, b, 0)$ et il existe P inversible telle que $A = PDP^{-1}$. On a alors

   $$\mathrm{Com}(A) = \mathrm{Com}(PDP^{-1})$$

   Admettons provisoirementle résultat suivant : $\mathrm{Com}(MN) = \mathrm{Com}(M)\mathrm{Com}(N)$. On a alors

   $$\mathrm{Com}(A) = \mathrm{Com}(P)\mathrm{Com}(D)\mathrm{Com}(P^{-1})$$

   Or, $\mathrm{Com}(P) = \det(P)({}^tP)^{-1}$ et $\mathrm{Com}(P^{-1}) = \det(P^{-1})({}^t(P^{-1}))^{-1} = \frac{1}{\det(P)}{}^tP$ et donc

   $$\mathrm{Com}(A) = ({}^tP)^{-1}\mathrm{Com}(D){}^tP \quad \text{et} \quad {}^t\mathrm{Com}(A) = P{}^t\mathrm{Com}(D)P^{-1}$$

   La relation de départ donne ainsi

   $$D + {}^t\mathrm{Com}(D) = kI_n$$

   On a ${}^t\mathrm{Com}(D) = \mathrm{diag}(0, \dots, 0, b^{n-1})$ et comme le polynôme minimal vaut $X(X - b) = X^2 - kX$ on a $k = b$. L'identité ci-dessus s'écrit donc

   $$\mathrm{diag}(b, \dots, b, b^{n-1}) = bI_n$$

   et comme $b \neq 0$, on a $b^{n-2} = 1$.

   Il reste à justifier le résultat admis. Il est facile quand M et N sont inversibles avec la relation rappelée initialement. Dans le cas général, on utilise la relation avec $N - \lambda I_n$ et $M - \lambda I_n$ qui sont inversibles pour λ petit et on fait tendre λ vers 0. Ainsi, le passage à la comatrice étant continu, on en déduit le résultat dans le cas général.

Planche 13

1. Pour $U \in M_n(\mathbb{C})$, on pose $J_U = \{AU; A \in M_n(\mathbb{C})\}$. Montrer que J_U est un sous-groupe additif de $M_n(\mathbb{C})$, et que pour P une matrice de projection, J_P et J_{I_n-P} sont deux sous-espaces vectoriels supplémentaires dans $M_n(\mathbb{C})$.

2. Soit J un sous-groupe additif de $M_n(\mathbb{C})$ stable par multiplication à gauche (pour tout $A \in J$, pour tout $B \in M_n(\mathbb{C})$, $BA \in J$). Soit $A \in J$, montrer qu'il existe $P \in J$ matrice de projection telle que $\text{rg}(P) = \text{rg}(A)$.

Indication 13

Solution 13

1. $A \mapsto AU$ est une application linéaire dont J_U est l'image. J_U est ainsi un sous-espace vectoriel de $M_n(\mathbb{C})$ et a fortiori un sous-groupe additif.

   Soit P une matrice de projection ($P^2 = P$). $F = J_P$ et $G = J_{I_n-P}$ sont des sous-espaces vectoriels de $M_n(\mathbb{C})$.

   - Soit $M \in F \cap G$. Il existe des matrices A et B telles que $M = AP = B(I - P)$. On en déduit que $AP = AP^2 = B(P - P^2) = 0$ et donc que $M = 0$. Ceci montre que F et G sont en somme directe.
   - Soit $M \in M_n(\mathbb{C})$. On a $M = MP + M(I_n - P) \in F + G$. On a donc $F + G = M_n(\mathbb{C})$ (inclusion directe évidente et on vient de voir la réciproque).

   On a donc montré que
   $$J_P \oplus J_{I_n-P} = M_n(\mathbb{C})$$

2. Soit $A \in J$ une matrice de rang r. On sait qu'il existe des matrices inversibles Q_1, Q_2 telles que $Q_1AQ_2 = J_r$ (matrice nulle sauf les r premiers coefficients de la diagonale qui valent 1). On a alors $Q_1A = J_rQ_2^{-1}$ et ainsi
   $$Q_2Q_1A = Q_2J_rQ_2^{-1}$$
   Comme $J_r^2 = J_r$, Q_2Q_1A est une matrice de projection et c'est aussi un élément de J. Le rang étant invariant par similitude, on a enfin Q_2Q_1A de rang r (égal à celui de J_r).