Devoir de Mathématiques n°3

Kévin Polisano
MP*

Jeudi 2 octobre 2009

Partie I

1. $f(x\varepsilon) = f(x)f(\varepsilon) \Rightarrow f(\varepsilon) = 1$ en prenant l'inverse à gauche de $f(x)$.

$$f(e_i) = f(e_i)^2 \Rightarrow f(e_i) = 1 \text{ ou } f(e_i) = 0$$

Si tous les $f(e_i) = 0$ alors $f = 0$. Sinon $\exists i, f(e_i) = 1$, or $j \neq i \Rightarrow e_i e_j = 0$ d'où :

$$0 = f(e_i e_j) = f(e_i)f(e_j) = f(e_j) \Rightarrow f(x) = x_i f(e_i) = x_i \Rightarrow f = c_i$$

2.1 f morphisme d'algèbre donc $\forall (x,y) \in E^2, f(xy) = f(x)f(y)$, d'où comme φ multiplicative :

$$\varphi \circ f(xy) = \varphi(f(x)f(y)) = \varphi \circ f(x) \varphi \circ f(y)$$

Ainsi $\varphi \circ f$ est également une forme multiplicative.

2.2 D'après la question 1. on a alors $\forall j \in [\![1,n]\!], \exists k \in [\![1,n]\!], c_j \circ f = c_k$.

$f(e_i) = \sum_{m=1}^{n} x_m e_m$, d'où d'après la remarque qui précède :

$$c_j \circ f(e_i) = x_j = c_k(e_i) = \delta_{i,k}$$

En balayant j de 1 à n on obtient pour chaque indice un c_k correspondant différent. En effet si $c_j \circ f = c_{j'} \circ f \Rightarrow c_j = c_{j'}$ par bijectivité de f. Ainsi comme il y a n forme k-alternée on les atteint toutes une fois et une seule fois seulement. Donc pour un certain j_0 on aura :

$$c_{j_0} \circ f(e_i) = x_{j_0} = c_i(e_i) = 1 \text{ et } x_j = 0 \text{ pour } j \neq j_0 \Rightarrow f(e_i) = e_{j_0}$$

Par conséquent f envoie chaque élément de la base sur un autre (uniquement déterminé car f bijective), donc f induit une permutation de la base. Réciproquement toute permutation de la base est un automorphisme de E. Les automorphismes de E sont donc exactement les permutations de la base, et sont donc au nombre de $n!$.

3. $a = (a_1, ..., a_n) \in E$. $m_a : x \mapsto ax$ est représenté dans la base B_0 par la matrice :

$$M_{B_0}(m_a) = \mathrm{Diag}(a_1, a_2, ..., a_n)$$

Donc son polynôme caractéristique est $\chi_{m_a}(X) = (-1)^n \prod_{i=1}^{n} (X - a_i)$.

On sait que le polynôme minimal μ_a divise le polynôme caractéristique χ_{m_a}.

Comme $K[a]$ contient a et K (tout comme E) il vient $K[a] \subset E$ et on sait aussi que :

$$\dim(K[a]) = \deg(\mu_a)$$

Si $\deg(\mu_a) = n = \dim(E)$ i.e tous les a_i distincts alors on a l'égalité $K[a] = E$.

Réciproquement si $K[a] = E$ c'est que $\deg(\mu_a) = n$ et donc nécessairement les a_i sont distincts.

4.1 Les d_i sont toutes non nulles car $\varepsilon \in A$ (car A sous-algèbre de E).

4.2 Pour $i, j \in \{1, ..., k\}$ $d_i \neq d_j$ donc $\exists x \in A$ tel que $d_i(x) = x_i \neq x_j = d_j(x)$.

Donc au moins un des 2 est non nul, si $x_i = 0$ alors $x_j^{-1}x$ convient, sinon :

$$x = (x_1, ..., x_i, ..., x_j, ..., x_n) \Rightarrow x_j^{-1}x = (..., x_j^{-1}x_i, ..., 1, ...) \Rightarrow x_j^{-1}x - 1 = (..., x_j^{-1}x_i - 1, ..., 0)$$

On multiplie ensuite par l'inverse de $x_j^{-1}x_i - 1$ qui est non nul et on obtient $u_{i,j}$.

4.3 Notons pour $j \leqslant i$:

$$z_{i,j} = (0, ..., \overset{\overset{j}{\downarrow}}{1}, ..., \overset{\overset{i}{\downarrow}}{0}, *)$$

Nous voulons en fait construire $z_{k,j}$ pour tout $1 \leqslant j \leqslant k$.

On procède par récurrence forte :

Initialisation : les $z_{2,j}$ sont déjà construits d'après la question précédente.

Hérédité : supposons les $z_{i,j}$ construits pour tout $1 \leqslant j \leqslant i$.

Construisons tout d'abord $z_{i+1,i+1}$:

$$z_{i+1,i+1} = \left(1 - \sum_{k=1}^{i} z_{i,k}\right) \times \left[c_{i+1}\left(1 - \sum_{k=1}^{i} z_{i,k}\right)\right]^{-1}$$

On construit ensuite les $z_{i+1,j}$ pour $1 \leqslant j \leqslant i$ de la manière suivante :

$$z_{i+1,j} = z_{i,j} - z_{i+1,i+1} \times [c_{i+1}(z_{i,i})]^{-1}$$

Ce qui achève la récurrence.

remarque : si le $i+1$-ème coefficient est déjà nul on passe directement au rang suivant.

4.4 Considérons la l-ème composante des w_i $(l > k)$. Il existe $j \leqslant k$ tel que $d_l = d_j$.

Ainsi $d_l(w_i) = d_j(w_i) = \delta_{i,j}$. Donc la l-ème composante de la somme des w_i est :

$$\sum_{i=1}^{n} \delta_{i,j} = 1$$

En conséquence on a $\sum_{i=1}^{n} w_i = \varepsilon$.

Les vecteurs w_i engendrent le sous-espace vectoriel A de E. $\text{Vect}(w_i) = A$.

5. Une sous-algèbre de dimension k est engendrée par k vecteurs w_i tels que $\sum_{i=1}^{k} w_i = \varepsilon$. Plus généralement qu'en 4. les vecteurs w_i ne possèdent que des 0 et des 1 placés n'importe où sachant que si le vecteur w_1 possède un 1 en première composante, les autres w_i ont un 0 pour que la somme soit égale à ε. Autrement dit les "paquets" de 1 de chaque w_i forment une "partition" de ε, donc afin dénombrer le nombre de sous-algèbre de dimension k on compte le nombre de partitions de $[\![1, n]\!]$ en k ensembles.

• Pour $k = 2$ on cherche donc toutes les partitions possibles en 2 ensembles : on peut choisir un singleton avec les $n-1$ éléments restants ce qui fait $\binom{n}{1}$ choix pour le singleton, ou bien une paire avec les $n-2$ éléments restants ce qui donne $\binom{n}{2}$ choix pour la paire, et ainsi de suite. En procédant de cette façon on compte en fait 2 fois chaque disposition, puisque quand on choisit une paire donnée, les $n-2$ éléments restants forment le deuxième ensemble, mais quand on va choisir ensuite cet ensemble on va retrouver la paire, donc finalement le nombre de sous-algèbre de dimension 2 est :

$$\frac{1}{2}\sum_{k=1}^{n-1}\binom{n}{k} = \frac{1}{2}\left(\sum_{k=0}^{n}\binom{n}{k} - 2\right) = \frac{1}{2}(2^n - 2) = 2^{n-1} - 1$$

• Pour $k = n-1$ on cherche les partitions en $n-1$ ensembles. On est donc forcé de former une paire et $n-2$ singletons, notre choix porte donc sur celui de la paire, d'où le nombre de sous-algèbre de dimension $n-1$:

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

6.1 Supposons que μ_a ait un zéro multiple disons a_1 : $\mu_a(X) = (X - a_1)^2 \prod (X - a_i)$.

On construit le polynôme $Q \in E[X]$ tel que $Q(X) = (X - a_1\varepsilon) \prod (X - a_i\varepsilon)$ ainsi :

$$[Q(a)]^2 = 0$$

Ce qui impliquerait que $Q(a) = 0$ car 0 est le seul élément nilpotent.

Absurde car $Q(a) \neq 0$ (le polynôme minimal de a est μ_a).

6.2 D'après le cours puisque μ_a est séparablement scindé alors m_a est diagonalisable.

Partie II

1. D'après la question I.3 on trouve donc $\tau(a) = \sum_{i=1}^{n} a_i$.

2. Puisque f est bijective elle envoie une base sur une base, donc $f(B)$ est une base, et de plus $f(v_k) = f(v_i v_j) = f(v_i) f(v_j)$ car morphisme d'algèbre, donc $f(B)$ est une m-base.

3. Permuter les colonnes de $M(B)$ revient à changer la place des éléments dans la famille B ce qui conserve la stabilité de la base par le produit interne. Quant aux lignes, la permutation

revient à multiplier par une matrice de permutation M_p à gauche de $M(B)$. Or comme nous avons $B = M(B)B_0$ cela donne :

$$(M_pB) = (M_pM(B))B_0$$

M_pB est une m-base (permutation de B). Ainsi $M_pM(B)$ (déduite de $M(B)$ par permutation de lignes) est aussi une matrice de passage vers une m-base.

4. $\varphi(v_iv_j) = \varphi(v_k) = 1$ et $\varphi(v_i)\varphi(v_j) = 1.1 = 1$ donc $\varphi(v_iv_j) = \varphi(v_i)\varphi(v_j)$ forme multiplicative.

5. Notons $\varphi = c_j$ ainsi $\forall 1 \leqslant 1 \leqslant n, c_j(v_i) = 1$ donc la j-ième ligne ne possède que des 1.

Il ne peut y en avoir qu'une seule car sinon $\text{rg}(M(B)) \leqslant n-1$ et $M(B)$ non inversible.

On en déduit les 4 m-bases de $\mathbb{K}^2$:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

les 2 autres étant obtenues par permutation des lignes.

6. Prenons $a = v_1$ et quitte à réordonner la base supposons que les puissances de a prennent la valeur des v_i dans l'ordre croissant. Si $v_1^2 = v_1$ c'est gagné, sinon $v_1^2 = v_2$. On recommence, si $v_1^3 = v_2v_1 = v_1$ c'est gagné. Si $v_1^3 = v_2v_1 = v_2 = v_1^2$ alors $v_1^2 = v_1$ (on multiplie par v où $c_i(v) = (c_i(v_1))^{-1}$ si $c_i(v_1) \neq 0$ et 0 sinon). Sinon c'est que $v_1^3 = v_3$.

Plus généralement $v_1^i = v_i$. Si $v_1^{i+1} = v_iv_1 = v_1$ c'est gagné, si $v_1^{i+1} = v_k$ avec $k \leqslant i$ c'est que $v_1^{i+1} = v_1^k \Rightarrow v_1^{i+1-(k-1)} = v_1$ en procédant comme ci-dessus, et sinon $v_1^{i+1} = v_{i+1}$.

Mais comme il n'y a que n vecteurs on tombera bien à un moment donné sur v_1.

Ainsi $p(a)$ existe et on a $p(a) \leqslant n$.

6.2 Les coefficients de a sont racines de $X^{p(a)+1} - X$ qui en possède au plus $p(a)+1$. Comme $p(a) \leqslant n$, il y a au plus $n+1$ valeurs possibles pour chaque coefficient, et comme il y en a n, on a au plus $(n+1)^n$ candidats pour a. Reste à choisir n vecteurs parmi ceux-ci, ce qui nous donne au plus $\binom{(n+1)^n}{n}$ m-bases. (majoration très grossière, notamment car on ne prend pas en compte le caractère stable de la base).

6.3 Les coefficients de a sont racines de $X^{p(a)+1} - X = X(X^{p(a)} - 1)$, dans $\mathbb{K} = \mathbb{R}$ ils ne peuvent valoir que 0, 1 ou -1, qui sont tous trois racines de $X^3 - X$, donc dans ce cas particulier $p(a) = 2$. On améliore la majoration trouvée par $\binom{3^n}{n}$.

7. $a \in B$, la matrice de m_a représentée dans la base B possède un seul 1 par colonne et des 0 partout ailleurs, car par stabilité $m_a(v_i) = av_i = v_j$. Donc puisqu'il n'y a que des 0 et/ou des 1 sur la diagonale, la trace $\tau(a)$ de m_a est un entier compris entre 0 (que des 0 sur la diagonale) et n (que des 1 sur la diagonale). $\tau(a) = n \Leftrightarrow a = \varepsilon$. En effet, il existe toujours un vecteur v_k tel que sa composante j soit non nulle (car B génératrice de E) on a alors $a_jx_j = x_j \Rightarrow a_j = 1$, donc $a_j = 1$ pour tout j.

8. La matrice $M(B)$ possède déjà une ligne de 1 d'après 5., il nous reste à placer $n-1$ coefficients dans $n-1$ lignes. Il est clair qu'on est forcé d'en placer exactement un à chaque ligne, sinon on aurait une ligne de 0 et le déterminant serait nul. Comme il y a n colonnes, il y en aura une qui sera un vecteur e_i. Par ailleurs vu les restrictions précédentes on a $C_i^2 = C_i$ donc les $2n-1$ coefficients sont tous des 1. On traduit une combinaison linéaire des colonnes par un système très simple qui confirme que cette famille est libre donc que $M(B)$ est inversible et B est une base. De plus pour $i \neq j$ on a $C_iC_j = C_0$ la colonne correspondant au vecteur e_i sus-cité. Donc B ainsi construite est bien une m-base.

On peut les dénombrer : on a n choix pour la ligne de 1, n choix pour la colonne C_0 et $(n-1)!$ choix pour placer les 1 restants, soit au total $n^2(n-1)!$ m-bases répondants aux hypothèses.

Partie III

1. $a^{p(a)+1} = a$ on multiplie par l'inverse : $a^{p(a)} = \varepsilon$ soit encore :

$$a \times a^{p(a)-1} = a^{p(a)-1} \times a = \varepsilon \ (*)$$

Comme $a^{p(a)-1} \in B$ par stabilité il vient que $\varepsilon \in B$.

2. En utilisant de nouveau la matrice de m_a dans la base B : on a pour tout i, $av_i \neq v_i$ sinon on aurait $a = \varepsilon$ en multipliant par l'inverse de v_i. Donc que des zéros sur la diagonale $\Rightarrow \tau(a) = 0$.

3. Par linéarité de la trace (et sachant que $\tau(v_i) = 0$ si $v_i \neq \varepsilon$ et $\tau(\varepsilon) = n$) :

$$\tau(s) = n + 0 + \cdots + 0 = n$$

L'application $x \mapsto xv_i$ laisse stable B car c'est une m-base, mais en outre comme v_i est inversible elle induit une permutation de B (car si $xv_i = yv_i$ alors $x = y$). Par conséquent $sv_i = s$. On distribue alors :

$$s^2 = (v_1 + v_2 + \cdots + v_n)s = v_1 s + v_2 + \cdots + v_n s = s + s + \cdots + s = ns$$

En divisant par n^2 il vient $\left(\frac{s}{n}\right)^2 = \frac{s}{n}$ donc les coefficients sont racines de $X^2 - X = X(X-1)$ donc valent 0 ou 1. Mais $\tau\left(\frac{s}{n}\right) = 1$ car $\tau(s) = n$ donc un et un seul coefficient vaut 1, les autres 0. D'où :

$$\frac{s}{n} \in B_0$$

4. En effectuant le produit lignes par colonnes (au sens du produit interne) on trouve comme coefficients de $\overline{{}^tM}M$: $a_{i,j} = \tau(\overline{v_i}v_j)$. Les composantes de v_i sont racines de $X(X^{p(a)}-1)$ donc sont des racines $p(a)$-ième de l'unité (0 exclu car les v_i inversibles) donc de la forme $e^{2ik\pi/n}$. Donc les composantes de $\overline{v_i}$ sont $e^{-2ik\pi/n}$, ainsi $\overline{v_i}$ est l'inverse de v_i qui appartient à B d'après $(*)$. Par conséquent pour tout j il existe k (unique car inversibilité) tel que $\overline{v_i}v_j = v_k$. Puisque $\tau(v_k) = 0$ si $v_k \neq \varepsilon$ et $\tau(\varepsilon) = n$ on a exactement un n par colonne et des 0 ailleurs. On permute les colonnes de $\overline{{}^tM}M$ de façon à avoir (au signe près, mais on prendra le module) le déterminant de nI_n soit n^n. Enfin comme $\det(\overline{{}^tM}M) = |\det(M)|^2$ on obtient :

$$|\det(M)| = \sqrt{n^n}$$

5.1 Le neutre est ε, l'existence de l'inverse est garantie par $(*)$, enfin l'associativité du produit interne découle de celle du produit externe dans $\mathbb{K} = \mathbb{R}$ qui est commutatif. (Ceci ne serait pas vrai dans le corps des quaternions par exemple).

5.2 D'après II.6.3 $a^3 = a$ et comme B est une m-base inversible : $a^2 = \varepsilon$.

On construit la loi externe de $\mathbb{Z}/2\mathbb{Z}$ sur B en posant :

$$\forall a \in B, 0a = 0 \quad \text{et} \quad 1a = a$$

On vérifie les axiomes d'espace vectoriel :

$1(u+v) = u+v = 1u+1v$ et $0(u+v) = 0 = 0u+0v$ donc distributive à gauche. $(0\times1)u = 0u = 0(1u)$, $(1 \times 0)u = 0u = 1(u0)$, $(1 \times 1)u = 1u = 1(1u)$, $(0 \times 0)u = 0u = 0(0u)$, d'où l'associativité. $(0+1)u = 1u = 0u+1u$, $(1+0)u = 1u = 1u+0u$, $(1+1)u = 0u = 0$ et $1u+1u = u+u = 0$ donc $(1+1)u = 1u+1u$ ainsi on obtient le dernier axiome de distributivité à droite.

B est donc un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. Comme B est fini, l'espace vectoriel que l'on vient de construire est de dimension d donc est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^d$. On en déduit que le cardinal de B est 2^d donc une condition nécessaire pour avoir une m-base inversible est que n soit une puissance de 2.

remarque : on utilise la même méthode pour démontrer que le cardinal d'un corps fini est de la forme p^d où p est sa caractéristique.

6. On va prendre simplement pour vecteurs de $\tilde{B}$ les vecteurs colonnes de $\tilde{M}$.

Vérifions que $\tilde{B}$ est bien une m-base inversible de $\mathbb{R}^{2n}$:

• J'utilise le résultat suivant vu l'an passé $(A, B, C, C \in \mathcal{M}_n(\mathbb{R}))$:

$$N = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \ A \text{ inversible et } AC = CA \Rightarrow \det(N) = \det(AD - CB)$$

démo : On passe au déterminant (en utilisant les matrices triangulaires par blocs)

$$\begin{pmatrix} I_n & 0 \\ -A^{-1}C & I_n \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ 0 & -A^{-1}CB + D \end{pmatrix}$$

Dans notre cas $\tilde{M}$ vérifie ces hypothèses et donc $\det(\tilde{M}) = -(\det M)^2 < 0$.

Donc $\tilde{M}$ est inversible et $\tilde{B}$ est bien une base.

• Chaque vecteur de base est inversible car $\binom{V_i}{\pm V_i}$ a pour inverse $\binom{V_i^{-1}}{\pm V_i^{-1}}$.

• Dernier point enfin : la stabilité de la base $\tilde{B}$.

En utilisant la stabilité des v_i on obtient par produit de colonnes :
$(i,j) \in [\![1,n]\!]^2, V_iV_j = V_k$ où $k \in [\![1,n]\!]$.
$(i,j) \in [\![n+1,2n]\!]^2, V_iV_j = V_k$ où $k \in [\![1,n]\!]$.
$(i,j) \in [\![1,n]\!] \times [\![n+1,2n]\!] V_iV_j = V_k$ où $k \in [\![n+1,2n]\!]$.

Donc la base $\tilde{B}$ est bien stable. Ce qui clos la démonstration.

7. $v_1 = \binom{1}{1}, v_2 = \binom{-1}{1} \in \mathbb{R}^2$ sont inversibles (leur propre inverse) et la matrice :

$$M(B) = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

est inversible ($\det(M(B)) = 2$ par exemple) donc $B = (v_1, v_2)$ est une base, stable de surcroît.

Donc B est une m-base inversible de $\mathbb{R}^2$.

On a vu en 5. que pour qu'il existe une m-base inversible de $\mathbb{R}^n$ il faut que n soit une puissance de 2. Mais cette condition est aussi suffisante car on a exhibé une telle base pour $n = 2^1$ et on sait d'après 6. construire à partir de celle-ci une m-base inversible pour $\mathbb{R}^{2n}$ donc finalement pour toutes les puissances de 2. On en conclut que pour toute valeur de n qui est une puissance de 2 il existe des m-bases inversibles.