Devoir de Mathématiques n°16

Kévin Polisano
MPSI 1

Vendredi 11 Avril 2008

Problème

Énoncé :

Dans tout ce problème, $\mathbb{R}$ désigne l'ensemble des réels.

Soit E un $\mathbb{R}$-espace vectoriel de dimension 4, et soit $B = (e_1, e_2, e_3, e_4)$ une base de E.

On considère les vecteurs :

$$\begin{aligned} f_1 &= e_1 + e_2 - e_3 + e_4 \\ f_2 &= e_1 + e_3 \\ f_3 &= -e_1 + e_2 + e_3 + e_4 \\ f_4 &= e_2 - e_4 \end{aligned}$$

Soit s l'endomorphisme de E ayant pour matrice dans la base B :

$$S = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$$

1. Commençons par montrer que la famille (f_1, f_2, f_3, f_4) est une base de E :

Soit $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in \mathbb{R}^4$ tels que :

$$\lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3 + \lambda_4 f_4 = 0$$

En remplaçant les f_i par leur expression on a :

$$(\lambda_1 + \lambda_2 - \lambda_3)e_1 + (\lambda_2 + \lambda_3 + \lambda_4)e_2 + (-\lambda_1 + \lambda_2 + \lambda_3)e_3 + (\lambda_1 + \lambda_3 - \lambda_4)e_4 = 0$$

Puisque la famille B est libre, on a à résoudre le système suivant :

$$\begin{cases} \lambda_1 + \lambda_2 - \lambda_3 = 0 \\ \lambda_2 + \lambda_3 + \lambda_4 = 0 \\ -\lambda_1 + \lambda_2 + \lambda_3 = 0 \\ \lambda_1 + \lambda_3 - \lambda_4 = 0 \end{cases}$$

En additionant la première et la troisième équation on a directement $\lambda_2 = 0$ et ensuite on trouve sans mal :

$$\boxed{\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = 0}$$

Posons $F = Vect(f_1, f_2)$ et $G = Vect(f_3, f_4)$.

Soit $x \in F \cap G$ alors $x = \lambda_1 f_1 + \lambda_2 f_2$ et $x = \lambda_3 f_3 + \lambda_4 f_4$ d'où :

$$\lambda_1 f_1 + \lambda_2 f_2 - \lambda_3 f_3 - \lambda_4 f_4 = 0$$

Ce qui nous amène à résoudre le système :

$$\begin{cases} \lambda_1 + \lambda_2 + \lambda_3 = 0 \\ \lambda_1 - \lambda_3 - \lambda_4 = 0 \\ -\lambda_1 + \lambda_2 - \lambda_3 = 0 \\ \lambda_1 - \lambda_3 + \lambda_4 = 0 \end{cases}$$

Et on trouve que tous les λ_i sont nuls donc $F \cap G = \{0\}$.

On peut alors écrire :

$$\boxed{E = F \bigoplus G}$$

On utilise alors la matrice S, on a :

$$\begin{array}{l} s(e_1) = \frac{1}{2}(e_1 + e_2 + e_3 + e_4) \\ s(e_2) = \frac{1}{2}(e_1 - e_2 - e_3 + e_4) \\ s(e_3) = \frac{1}{2}(e_1 - e_2 + e_3 - e_4) \\ s(e_4) = \frac{1}{2}(e_1 + e_2 - e_3 - e_4) \end{array}$$

Puisque s est un endomorphisme :

$$\begin{array}{rcl} s(f_1) & = & s(e_1 + e_2 - e_3 + e_4) \\ & = & s(e_1) + s(e_2) - s(e_3) + s(e_4) \\ & = & e_1 + e_2 - e_3 + e_4 \\ & = & f_1 \end{array}$$

On vérifie de même que $s(f_2) = f_2$, $s(f_3) = -f_3$ et $s(f_4) = -f_4$.

Ainsi si on prend $x_1 \in F$ et $x_2 \in G$ on a :

$$\begin{array}{rcl} s(x_1 + x_2) & = & s(x_1) + s(x_2) \\ & = & s(\lambda_1 f_1 + \lambda_2 f_2) + s(\lambda_3 f_3 + \lambda_4 f_4) \\ & = & \lambda_1 s(f_1) + \lambda_2 s(f_2) + \lambda_3 s(f_3) + \lambda_4 s(f_4) \\ & = & \lambda_1 f_1 + \lambda_2 f_2 - \lambda_3 f_3 - \lambda_4 f_4 \\ & = & x_1 - x_2 \end{array}$$

Par conséquent s est la symétrie par rapport au plan F parallèlement au plan G.

Enfin étant donné qu'une symétrie est involutive on a $s \circ s = Id_E$ d'où :

$$\boxed{S^{-1} = S}$$

2. Pour tout entier i compris entre 1 et 4 on pose $e'_i = s(e_i)$.

Soit $B' = (e'_1, e'_2, e'_3, e'_4)$. B' est l'image de B par s qui est un automorphisme de E.

Donc B' est une base de E.

3. Soient a et b deux réels et $u_{a,b}$ l'endomorphisme de E ayant pour matrice dans la base B' :

$$D(a,b) = \begin{pmatrix} (a+b)^2 & 0 & 0 & 0 \\ 0 & (a-b)^2 & 0 & 0 \\ 0 & 0 & a^2-b^2 & 0 \\ 0 & 0 & 0 & a^2-b^2 \end{pmatrix}$$

a) $D(a,b)$ est une matrice carrée diagonale, ainsi si son inverse existe alors elle est égale à :

$$D(a,b)^{-1} = \begin{pmatrix} \frac{1}{(a+b)^2} & 0 & 0 & 0 \\ 0 & \frac{1}{(a-b)^2} & 0 & 0 \\ 0 & 0 & \frac{1}{a^2-b^2} & 0 \\ 0 & 0 & 0 & \frac{1}{a^2-b^2} \end{pmatrix}$$

Autrement dit l'inverse des éléments diagonaux doivent exister donc il faut et il suffit qu'ils soient non nuls. La condition nécessaire et suffisante d'inversibilité est donc :

$$\boxed{a - b \neq 0 \text{ et } a + b \neq 0}$$

b) Supposons cette condition remplie, et remarquons que :

$$\begin{aligned} D(a,b)D(a,-b) &= \begin{pmatrix} (a+b)^2 & 0 & 0 & 0 \\ 0 & (a-b)^2 & 0 & 0 \\ 0 & 0 & a^2-b^2 & 0 \\ 0 & 0 & 0 & a^2-b^2 \end{pmatrix} \begin{pmatrix} (a-b)^2 & 0 & 0 & 0 \\ 0 & (a+b)^2 & 0 & 0 \\ 0 & 0 & a^2-b^2 & 0 \\ 0 & 0 & 0 & a^2-b^2 \end{pmatrix} \\ &= \begin{pmatrix} (a^2-b^2)^2 & 0 & 0 & 0 \\ 0 & (a^2-b^2)^2 & 0 & 0 \\ 0 & 0 & (a^2-b^2)^2 & 0 \\ 0 & 0 & 0 & (a^2-b^2)^2 \end{pmatrix} \\ &= (a^2-b^2)^2 I_4 \end{aligned}$$

On en déduit :

$$\boxed{D(a,b)^{-1} = \frac{1}{(a^2-b^2)^2} D(a,-b)}$$

4. Soit $M(a,b)$ la matrice de $u_{a,b}$ dans la base B.

On remarque que la matrice de passage de B' à B est la matrice S donc :

$$M(a,b) = SD(a,b)S$$

Calculons ce produit matriciel :

$$\begin{aligned} SD(a,b) &= \tfrac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \begin{pmatrix} (a+b)^2 & 0 & 0 & 0 \\ 0 & (a-b)^2 & 0 & 0 \\ 0 & 0 & a^2-b^2 & 0 \\ 0 & 0 & 0 & a^2-b^2 \end{pmatrix} \\ &= \tfrac{1}{2}\begin{pmatrix} (a+b)^2 & (a-b)^2 & a^2-b^2 & a^2-b^2 \\ (a+b)^2 & -(a-b)^2 & -(a^2-b^2) & -(a^2-b^2) \\ (a+b)^2 & -(a-b)^2 & a^2-b^2 & -(a^2-b^2) \\ (a+b)^2 & (a-b)^2 & -(a^2-b^2) & -(a^2-b^2) \end{pmatrix} \end{aligned}$$

Donc :

$$SD(a,b)S = \frac{1}{4}\begin{pmatrix} (a+b)^2 & (a-b)^2 & a^2-b^2 & a^2-b^2 \\ (a+b)^2 & -(a-b)^2 & -(a^2-b^2) & -(a^2-b^2) \\ (a+b)^2 & -(a-b)^2 & a^2-b^2 & -(a^2-b^2) \\ (a+b)^2 & (a-b)^2 & -(a^2-b^2) & -(a^2-b^2) \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$$

Notons a_{ij} les coefficients de la matrice $4SD(a,b)S$, ainsi :

$$\begin{aligned} a_{11} &= (a+b)^2 + (a-b)^2 + (a^2-b^2) + (a^2-b^2) = 4a^2 \\ a_{12} &= (a+b)^2 - (a-b)^2 - (a^2-b^2) + (a^2-b^2) = 4ab \\ a_{13} &= (a+b)^2 - (a-b)^2 + (a^2-b^2) - (a^2-b^2) = 4ab \\ a_{14} &= (a+b)^2 + (a-b)^2 - (a^2-b^2) - (a^2-b^2) = 4b^2 \end{aligned}$$

En faisant de même pour les trois autres lignes on obtient :

$$\boxed{M(a,b) = \begin{pmatrix} a^2 & ab & ab & b^2 \\ ab & a^2 & b^2 & ab \\ ab & b^2 & a^2 & ab \\ b^2 & ab & ab & a^2 \end{pmatrix}}$$

5. a) Sous les mêmes conditions qu'à la question 3, $M(a,b)$ est inversible et :

$$M(a,b)^{-1} = (SD(a,b)S)^{-1} = S^{-1}D(a,b)^{-1}S^{-1} = \frac{1}{(a^2-b^2)^2}SD(a,-b)S$$

On trouve alors d'après ce qui précède :

$$M(a,b)^{-1} = \frac{1}{(a^2-b^2)^2}\begin{pmatrix} a^2 & -ab & -ab & b^2 \\ -ab & a^2 & b^2 & -ab \\ -ab & b^2 & a^2 & -ab \\ b^2 & -ab & -ab & a^2 \end{pmatrix}$$

En posant $A = \frac{a}{a^2-b^2}$ et $B = -\frac{b}{a^2-b^2}$, on a $(A,B) \in \mathbb{R}^2$ et :

$$M(a,b) = \begin{pmatrix} A^2 & AB & AB & B^2 \\ AB & A^2 & B^2 & AB \\ AB & B^2 & A^2 & AB \\ B^2 & AB & AB & A^2 \end{pmatrix}$$

Ce qui montre que $M(a,b)^{-1} \in L$.

b) Si on effectue le produit $M(a,b) \times M(a',b')$ en simplifiant on obtient :

$$\begin{pmatrix} (aa'+bb')^2 & (aa'+bb')(ab'+a'b) & (aa'+bb')(ab'+a'b) & (ab'+a'b)^2 \\ (aa'+bb')(ab'+a'b) & (aa'+bb')^2 & (ab'+a'b)^2 & (aa'+bb')(ab'+a'b) \\ (aa'+bb')(ab'+a'b) & (ab'+a'b)^2 & (aa'+bb')^2 & (aa'+bb')(ab'+a'b) \\ (ab'+a'b)^2 & (aa'+bb')(ab'+a'b) & (aa'+bb')(ab'+a'b) & (aa'+bb')^2 \end{pmatrix}$$

Si on pose $a'' = aa' + bb'$ et $b'' = ab' + a'b$ on voit alors que :

$$\boxed{M(a,b) \times M(a',b') = M(a'',b'')}$$

6. On pose $N(t) = M(ch(t), sh(t))$ et on note L' l'ensemble des matrices $N(t)$ quand t décrit $\mathbb{R}$.

Signalons que les matrices $N(t)$ sont inversibles puisque :

$$\forall t \in \mathbb{R}, ch(t) - sh(t) \neq 0 \text{ et } ch(t) + sh(t) \neq 0$$

(Les fonctions $t \mapsto ch(t) - sh(t)$ et $t \mapsto ch(t) + sh(t)$ ne s'annulent en aucun point).

Ainsi $L' \subset GL_4(\mathbb{R})$ montrons alors que $(L', \times)$ est un sous-groupe de $GL_4(\mathbb{R})$:

D'après 5)b on a $M(ch(t), sh(t)) \times M(ch(t'), sh(t')) = M(a'', b'')$ avec :

$$\begin{aligned} a'' &= ch(t)ch(t') + sh(t)sh(t') = ch(t+t') \\ b'' &= ch(t)sh(t') + ch(t')sh(t) = sh(t+t') \end{aligned}$$

On pose $t'' = t + t' \in \mathbb{R}$ et on a alors :

$$\boxed{M(ch(t), sh(t)) \times M(ch(t'), sh(t')) = M(ch(t''), sh(t'')) \in L'}$$

Donc les éléments de L' sont stables par multiplication.

Par ailleurs on a vu que $M(a,b)^{-1} = M(A,B)$ avec $A = \frac{a}{a^2-b^2}$ et $B = -\frac{b}{a^2-b^2}$.

Puisque $ch^2(t) - sh^2(t) = 1$ et que ces fonctions sont respectivement paire et impaire :

$$\boxed{M(ch(t), sh(t))^{-1} = M(ch(-t), sh(-t)) \in L'}$$

On a donc démontré que L' est un sous-groupe de $GL_4(\mathbb{R})$ qui est clairement commutatif.

Au passage on a également démontré que :

$$\boxed{(\forall t, t') \in \mathbb{R}^2, N(t+t') = N(t) \times N(t')}$$

Donc l'application N de $\mathbb{R}$ dans L' qui à t associe $N(t)$ est un homomorphisme.

De surcroît elle est clairement surjective, montrons qu'elle est injective, soit :

$$N(t) = N(t') \Leftrightarrow M(ch(t), sh(t)) = M(ch(t'), sh(t'))$$

En l'écrivant sous forme matricielle on doit avoir :

Soit l'égalité $ch(t) = ch(t')$ et $sh(t) = sh(t')$ soit $ch(t) = -ch(t')$ et $sh(t) = -sh(t')$.

Ce deuxième cas étant exclu car le cosinus hyperbolique est strictement positif.

Du premier cas on en tire $t = t'$ car le sinus hyperbolique est bijectif.

Ainsi l'application est un isomorphisme de groupe.

7. L'ensemble $GL_4(\mathbb{R}) \cap L$ possède une structure de groupe non commutatif.

Exercice

Énoncé :

On se propose d'étudier une méthode de calcul de l'inverse d'un élément a d'un groupe multiplicatif G de cardinal fini $N \in \mathbb{N}^{\star}$. L'élément neutre de G est noté 1.

Nous allons donc écrire un algorithme et écrire son coût, c'est-à-dire le nombre de multiplications dans le groupe G que nécessite son éxecution. On ne tiendra pas compte des autres opérations (en particulier celles dans $\mathbb{N}$).

1) Soit $\{a, a^2, ..., a^{p-1}\}$ le sous-groupe engendré par a d'ordre p.

D'après le théorème de Lagrange :

$$p|N \Leftrightarrow \exists k \in \mathbb{N}, N = pk$$

D'où :

$$a^N = a^{pk} = (a^p)^k = 1^k = 1$$

Donc a^{N-1} est l'inverse de a^N car :

$$\boxed{a^{N-1}.a = a.a^{N-1} = 1}$$

2) On écrit la décomposition en base 2 de $N-1$ sous la forme :

$$N-1 = \sum_{i=0}^{k} x_i 2^i \text{ avec } k \in \mathbb{N}, x_i \in \{0,1\} \text{ pour } i \in [0,k] \cap \mathbb{N} \text{ et } x_k \neq 0$$

On considère les suites finies $(a_i)_{0 \leq i \leq k+1}$ et $(b_i)_{0 \leq i \leq k+1}$ définies par :

$$a_0 = 1, b_0 = a \text{ et pour } i \in [0,k] \cap \mathbb{N}, a_{i+1} = a_i b_i^{x_i}, b_{i+1} = b_i^2$$

a) On a $b_1 = b_0^2$ puis $b_2 = b_1^2 = (b_0^2)^2 = b_0^{2^2}$, $b_3 = b_2^2 = (b_0^{2^2})^2 = b_0^{2^3}$.

Par récurrence sur $\mathbb{N}$ on obtient puisque $b_0 = a$:

$$\forall i \in [1,k] \cap \mathbb{N}, b_i = a^{2^i}$$

Or

$$a_{i+1} = a_i b_i^{x_i} = (a_{i-1} b_{i-1}^{x_{i-1}}) b_i^{x_i} = a_{i-1} a^{2^{i-1} x_{i-1}} a^{2^i x_i} = a_{i-1} a^{2^{i-1} x_{i-1} + 2^i x_i}$$

En itérant et sachant que $a_0 = 1$ il vient :

$$\forall i \in [1,k] \cap \mathbb{N}, a_{i+1} = a^{\left(\sum_{m=0}^{i} 2^m x_m\right)}$$

Pour $i = k$ on a puisque $N-1 = \sum_{m=0}^{k} x_m 2^m$:

$$\boxed{a_{k+1} = a^{\left(\sum_{m=0}^{i} 2^m x_m\right)} = a^{N-1}}$$

Et donc d'après la question précédente a_{k+1} est l'inverse de a dans G.

b) On peut donc écrire un algorithme calculant le terme a_{k+1} :

On se donne des variables initialisées à $x = 1$, $y = a$ et $z = N-1$ et on effectue la boucle :

Tant que z est non nul on effectue la division de z par 2 et on s'intéresse au reste r :

Toujours dans la boucle on fait un test logique :

Si $r = 1$ alors x reçoit $x.y$ sinon si $r = 0$ alors x reçoit x. (*Calcul du terme a_{i+1}*)

Et y reçoit y^2. (*Calcul du terme b_{i+1}*)

En fin de boucle on demande alors au programme de retourner la valeur de x.

Le nombre de fois qu'on exécute la boucle correspond au nombre de bit calculés dans l'écriture binaire de $N-1$ à savoir $k+1$.

De plus à l'intérieure de la boucle on effectue au maximum 2 multiplications donc le coût est :

$$\boxed{\text{Coût} = 2(k+1)}$$

3) Dans cette question, G est le groupe des éléments inversibles de $\mathbb{Z}/148\mathbb{Z}$.

a) Les éléments inversibles sont ceux qui sont premiers avec 148, il y en a donc :

$$\boxed{\varphi(148) = \varphi(4 \times 37) = \varphi(4) \times \varphi(37) = 2 \times 36 = 72}$$

En effet pour u et v premiers entre eux $\varphi(uv) = \varphi(u)\varphi(v)$ ce qui est le cas pour 4 et 37.

Il y a donc $N = 72$ éléments inversibles dans $\mathbb{Z}/148\mathbb{Z}$.

b) Puisque $148 \wedge 5 = 1$ alors 5 est inversible dans $\mathbb{Z}/148\mathbb{Z}$ donc $5 \in G$.

En se reportant à la question 2) on a :

$$N-1 = 71 = 1 \times 2^0 + 1 \times 2^1 + 1 \times 2^2 + 0 \times 2^3 + 0 \times 2^4 + 0 \times 2^5 + 1 \times 2^6$$

Calculons les termes en b_i :

$$\boxed{\begin{array}{l} b_0 = 5 \\ b_1 = b_0^2 = 25 \\ b_2 = 25^2 = 625 = 4 \times 148 + 33 = 33 \\ b_3 = 33^2 = 1089 = 7 \times 1048 + 53 = 53 \\ b_4 = 53^2 = 2809 = 17 \times 148 + 145 = 145 = -3 \\ b_5 = (-3)^2 = 9 \\ b_6 = 9^2 = 81 \end{array}}$$

Calculons les termes en a_i :

$$\boxed{\begin{array}{l} a_0 = 1 \\ a_1 = 5 \\ a_2 = 5 \times 25^1 = 125 = -23 \\ a_3 = -23 \times 33 = -(5 \times 148 + 19) = -19 \\ a_4 = -19 \\ a_5 = -19 \\ a_6 = -19 \\ a_7 = -19 \times 81 = -(10 \times 148 + 59) = -59 \end{array}}$$

On en conclut que l'inverse de 5 dans $\mathbb{Z}/148\mathbb{Z}$ est -59.

c) Une autre méthode consiste à utiliser l'algorithme d'Euclide :

$$\begin{aligned}&148 = 29 \times 5 + 3\\&5 = 1 \times 3 + 2\\&3 = 1 \times 2 + 1\end{aligned}$$

On retrouve que 148 et 5 sont premiers entre eux, en remontant l'algorithme on a :

$$1 = 2 \times 148 - 5 \times 59$$

On a donc bien -59 qui est l'inverse de 5 dans $\mathbb{Z}/148\mathbb{Z}$.