Algèbre linéaire avancée II
printemps 2024

Série 3 - Corrigé

L'exercice marqué d'un (+) sert d'introduction à la série, tandis que celui marqué d'une (*) est plus difficile. Tous les exercices sauf celui marqué d'une (*) seront corrigés. La correction sera postée sur Moodle 2 semaines après. Les solutions des exercices (*) et (+) seront discutées dans les séances d'exercices du mardi d'après et d'avant respectivement. Un des exercices (*) sera une question ouverte de l'examen final.

Exercice 1. Soit V un espace vectoriel réel et soit $B = \{v_1, \dots, v_4\}$ une base de V.

1. (+) Soit f l'endomorphisme défini par

$$f(v_1) = v_1 - v_2, f(v_2) = 2v_2 - 6v_3, f(v_3) = -2v_1 + 2v_2, f(v_4) = v_2 - 3v_3 + v_4.$$

   Écrivez la matrice A_B de l'application f dans la base $B = \{v_1, \dots, v_4\}$. Est-ce que f est inversible? Si oui, écrivez la matrice A_B^{-1} de l'application inverse $f^{-1} : V \longrightarrow V$.

2. Maintenant, soit g un autre endomorphisme défini par

$$g(v_1) = v_1 + 2v_2, g(v_2) = v_3 + v_4, g(v_3) = v_1 + v_2 + v_3, g(v_4) = 3v_2 - 2v_3.$$

   Écrivez la matrice C_B de l'application g dans la base $B = \{v_1, \dots, v_4\}$. Est-ce que g est inversible? Si oui, écrivez la matrice C_B^{-1} de l'application inverse $g^{-1} : V \longrightarrow V$.

3. Maintenant, soit $B' = \{w_1, \dots, w_4\}$ une autre base de V telle que

$$v_1 = w_1 + w_2, v_2 = w_3 + w_4, v_3 = w_1 + w_2 + w_3, v_4 = w_2 + w_4.$$

   Écrivez la matrice $P_{BB'}$ de changement de base, c'est-à-dire $[v]_{B'} = P_{BB'}[v]_B$. Écrivez la matrice $A_{B'}$ de l'application f dans la base B', et la matrice $C_{B'}$ de l'application g dans la base B'.

   Rappel:

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\phi_B"] & V \arrow[d, "\phi_B"] \\ K^n \arrow[r, "A"] & K^n \end{tikzcd}$$

Solution. *1.* $A_B = \begin{pmatrix} 1 & 0 & -2 & 0 \\ -1 & 2 & 2 & 1 \\ 0 & -6 & 0 & -3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, *les colonnes de cette matrice sont les images des vecteurs de la base B. Par exemple, la première colonne est l'image de v_1, ce qu'on peut voir si on calcule $A_B \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$. Le déterminant de la matrice A_B est nul, donc l'inverse n'existe pas.*

2. $C_B = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 0 & 1 & 3 \\ 0 & 1 & 1 & -2 \\ 0 & 1 & 0 & 0 \end{pmatrix}$, $C_B^{-1} = \begin{pmatrix} 5 & -2 & -3 & 3 \\ 0 & 0 & 0 & 1 \\ -4 & 2 & 3 & -3 \\ -2 & 1 & 1 & -1 \end{pmatrix}$.

3. On écrit la matrice de changement de base P de B a B'. On a que $P = P_{BB'} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, *alors* $P^{-1} = P_{B'B} = \begin{pmatrix} 2 & -1 & -1 & 1 \\ 1 & -1 & 0 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 0 & 0 \end{pmatrix}$. *Finalement, on a les relations* $A_{B'} = P_{BB'} A_B P_{B'B}$ *et* $C_{B'} = P_{BB'} C_B P_{B'B}$.

Exercice 2. Sachant que $\det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = 5$, calculer $\det \begin{pmatrix} 2a & 2b & 2c \\ g & h & i \\ 4d+3g & 4e+3h & 4f+3i \end{pmatrix}$.

Solution. *On sait que* det *est linéaire par rapport à chaque ligne et qu'il est invariant par ajout d'un multiple d'une ligne j à une ligne $i \neq j$. Ainsi*

$$\det \begin{pmatrix} 2a & 2b & 2c \\ g & h & i \\ 4d+3g & 4e+3h & 4f+3i \end{pmatrix} = 2 \det \begin{pmatrix} a & b & c \\ g & h & i \\ 4d+3g & 4e+3h & 4f+3i \end{pmatrix} =$$

$$= 2 \det \begin{pmatrix} a & b & c \\ g & h & i \\ 4d & 4e & 4f \end{pmatrix} = 8 \det \begin{pmatrix} a & b & c \\ g & h & i \\ d & e & f \end{pmatrix} = -8 \det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = -8 \cdot 5 = -40\,.$$

Exercice 3. Factoriser $f(x) \in K[x]$ en polynômes irréductibles.

a) $f(x) = 3x^4 + 2$, $K = \mathbb{Z}_5$.

b) $f(x) = 3x^4 + 2$, $K = \mathbb{Z}_{11}$.

c) $f(x) = x^3 + 2x^2 + 2x + 1$, $K = \mathbb{Z}_7$.

d) $f(x) = x^3 + 2x^2 + 2x + 1$, $K = \mathbb{Z}_3$.

e) $f(x) = x^4 - x^2 + x - 1$, $K = \mathbb{Z}_{13}$.

f) $f(x) = x^4 - x^2 + x - 1$, $K = \mathbb{Z}_{17}$.

Solution. *a) On vérifie si $f(x) = 3x^4 + 2$ a des racines en $\mathbb{Z}_5$. On commence avec 0: $f(0) = 2$ et donc 0 n'est pas racine. En suite, $f(1) = 5 = 0$ et donc 1 est racine. Alors on sait que $(x - 1)$ divise $f(x)$. On fait la division sur $\mathbb{Z}_5$ et on trouve que $f(x)/(x - 1) = 3x^3 + 3x^2 + 3x + 3$. On continue et on trouve que 2 est une racine du polynôme $3x^3 + 3x^2 + 3x + 3$. Alors on divise par $(x - 2)$. En continuant ainsi, on arrive à la factorisation finale de $f(x)$ qui est $f(x) = 3(x + 4)(x + 3)(x + 2)(x + 1)$.*

b) $f(x) = 3(x^2 + 5)(x + 4)(x + 7)$

c) $f(x) = (x + 5)(x + 3)(x + 1)$

d) $f(x) = (x + 1)(x + 2)^2$

e) $f(x) = (x + 12)(x + 11)(x^2 + 3x + 6)$

f) $f(x) = (x + 3)(x + 16)(x^2 + 15x + 6)$

Exercice 4. Calculer $\gcd(f, g)$ et $p, q \in K[x]$ tel que $\gcd(f, g) = p \cdot f + q \cdot g$:

1. $f(x) = x^2 + 2$, $g(x) = x^3 + 4x^2 + x + 1$, $K = \mathbb{Z}_5$
2. $f(x) = x^2 + 1$, $g(x) = x^5 + x^4 + x^3 + x^2 + x + 1$, $K = \mathbb{Z}_2$
3. $f(x) = x^2 - x - 2$, $g(x) = x^5 - 4x^3 - 2x^2 + 7x - 6$, $K = \mathbb{Q}$.

Solution. *1. On utilise l'algorithme d'Euclide pour calculer le $\gcd(f, g)$ et les coefficients p, q. On commence par diviser $g(x)$ par $f(x)$. On trouve que*

$$(x^3 + 4x^2 + x + 1) = (x^2 + 2)(x + 4) + (4x + 3).$$

En suite, on divise $x^2 + 2$ par le reste de la première division, c'est-à-dire par $(4x + 3)$. On trouve que

$$(x^2 + 2) = (4x + 3)(4x + 2) + 1.$$

Alors on a que $\gcd(f, g) = 1$ et que

$$(x + 3)(x^3 + 4x^2 + x + 1) + (x^2 + 2)(4x^2 + 3x + 4) = 1.$$

2. On trouve que $\gcd(f, g) = x + 1$ et que

$$(x^3 + x^2)(x^2 + 1) + (1)(x^5 + x^4 + x^3 + x^2 + x + 1) = x + 1.$$

3. On trouve que $\gcd(f,g) = x-2$ *et que*

$$(-1/4x^3 - 1/4x^2 + 1/4x + 1/4)(x^2 - x - 2) + (1/4)(x^5 - 4x^3 - 2x^2 + 7x - 6) = x - 2.$$

Exercice 5. Soient E, F deux corps tels que $F \subseteq E$.

i) Montrer que E est un espace vectoriel sur F avec multiplication externe $e \cdot f$, $e \in E$, $f \in F$ étant la multiplication sur E en vérifiant l'associativité, la distributivité et la neutralité de $1_E = 1_F$.

ii) Maintenant, soit E vu comme espace vectoriel sur F de dimension finie et soit $e \in E \setminus \{0\}$. Montrer qu'il existe un polynôme $f(x) \in F[x] \setminus \{0\}$ tel que $f(e) = 0$.

iii) Montrer qu'il y a un seul tel polynome $p_e(x) \neq 0$ de degré minimal et de coefficient dominant égal à 1.

iv) Montrer que ce polynôme $p_e(x)$ est irréductible.

Solution. *i) Simple à vérifier.*

ii) Soit n la dimension de E sur F, alors $1, e, e^2, \ldots, e^{n+1}$ sont $n+1$ éléments de E. Il existe donc une combinaison linéaire non-triviale de ces éléments avec des coefficients dans F qui est égal à zéro:

$$\sum_{i=0}^{n} f_i e^i = 0$$

avec $f_i \in F$ pour tout $i \in \{0, 1, \ldots, n\}$. Le polynôme à définir est $f(x) = \sum_{i=0}^{n} f_i x^i$.

iii) On suppose l'existence de deux polynômes $g(x), h(x) \in F[x]$ qui satisfont les conditions de l'énoncé. Considérons le polynôme $g-h$ qui est de degré strictement inférieur au degré de g et de h et qui s'annule en e. Par la minimalité des polynômes g et h on obtient que $g-h$ doit être le polynôme identiquement nul et on a donc $g = h$.

iv) On suppose que $p_e(x) \in F[x]$ est un polynôme réductible. Ainsi $p_e = g \cdot h$ avec $g(x), h(x) \in F[x]$ des polynômes non-constants. On a bien $g(e) = 0$ ou $h(e) = 0$ car un corps est intègre. Comme $\deg(g), \deg(h) < \deg(p_e)$ on a une contradiction avec la minimalité de p_e. On a donc montré que p_e est irréductible sur F.

Exercice 6. Soit K un corps. On écrit $\frac{\partial}{\partial x} : K[x] \to K[x]$ pour l'application K-linéaire tel que $\frac{\partial}{\partial x} x^n = n x^{n-1}$ pour chaque $n \geq 0$ (où n est regardé en tant qu'élément de K à travers l'homomorphisme canonique $\mathbb{Z} \to K$).
Soient $f, g \in K[x]$, montrer que $\frac{\partial}{\partial x}(f \cdot g) = f \cdot \frac{\partial}{\partial x}(g) + \frac{\partial}{\partial x}(f) \cdot g$.
Soient $h \in K[x]$ et $\alpha \in K$. Montrer que α est racine multiple de h si et seulement si $h(\alpha) = 0$ et $\frac{\partial}{\partial x}(h)(\alpha) = 0$.

Solution. *Comme l'application* $\frac{\partial}{\partial x}$ *est* K*-linéaire, il suffit de vérifier l'identité sur les monômes:*

$$x^r \cdot \frac{\partial}{\partial x}(x^s) + \frac{\partial}{\partial x}(x^r) \cdot x^s = x^r \cdot sx^{s-1} + rx^{r-1} \cdot x^s = (r+s)x^{r+s-1} = \frac{\partial}{\partial x}(x^{r+s})$$

Pour la deuxième partie de l'exercice on peut supposer que α *est une racine de* h *et il suffit de montrer l'équivalence suivante:*

$$x - \alpha | \tfrac{\partial}{\partial x}(h) \text{ si et seulement si } \alpha \text{ est une racine multiple de } h$$

On écrit $h(x) = (x-\alpha)^m \tilde{h}(x)$ *tel que* $(x-\alpha)$ *ne divise pas* $\tilde{h}(x)$*. Puisque on a supposé que* $h(\alpha) = 0$*, on obtient* $m \geq 1$ *et*

$$\frac{\partial}{\partial x}(h) = (x-\alpha)^m \cdot \frac{\partial}{\partial x}(\tilde{h}) + \frac{\partial}{\partial x}((x-\alpha)^m) \cdot \tilde{h} = (x-\alpha)^m \cdot \frac{\partial}{\partial x}(\tilde{h}) + m(x-\alpha)^{m-1} \cdot \tilde{h}$$

Comme $m \geq 1$*, on a*

$$x - \alpha | \frac{\partial}{\partial x}(h) \iff (x-\alpha) | m(x-\alpha)^{m-1}\tilde{h} \iff m \geq 2$$

On note que pour la dernière équivalence on a soit $m \geq 2$ *soit* $m = 0$ *et dans ce dernier cas on a* $0 < car(K) | m$ *où la caractéristique* $car(K)$ *est un nombre premier, ce qui implique* $m \geq 2$*.*

Exercice 7. Le but de cet exercice est la construction du corps des nombres rationnels $\mathbb{Q}$ à partir de l'anneau des nombres entiers $\mathbb{Z}$.

1. On définit sur l'ensemble $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ la relation: $(a,b) \sim (a',b')$ si et seulement si $ab' = a'b$. Montrer qu'il s'agit d'une relation d'équivalence.

2. Maintenant, on désigne $\frac{a}{b}$ la classe (a,b) et on définit $\mathbb{Q}$ comme l'ensemble des classes d'équivalence de $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ par $\sim$.

   Soient $a, a' \in \mathbb{Z}$ et $b, b' \in \mathbb{Z} \setminus \{0\}$ alors on munit $\mathbb{Q}$ des opérations suivantes:

   i) somme: $\frac{a}{b} + \frac{a'}{b'} = \frac{ab'+a'b}{bb'}$,

   ii) produit: $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$.

   Montrer que ces opérations sont bien définies.

3. Montrer que $\mathbb{Q}$ est un corps qui contient $\mathbb{Z}$ sous la forme d'un sous-anneau via l'homomorphisme d'inclusion

$$\iota : \mathbb{Z} \to \mathbb{Q} : n \mapsto \iota(n) = \frac{n}{1}.$$

   En particulier montrer que $\frac{0}{1}$ et $\frac{1}{1}$ sont le zéro et l'unité de $\mathbb{Q}$.

Solution. *1. La réflexivité ($(a,b) \sim (a,b)$) et la symétrie ($(a,b) \sim (a',b') \Rightarrow (a',b') \sim (a,b)$) sont évidentes. Pour la transitivité on suppose que $(a,b) \sim (a',b')$ et $(a',b') \sim (a'',b'')$. Ceci est équivalent aux égalités $ab' = a'b$ et $a'b'' = a''b'$ et notre but est de montrer $ab'' = a''b$. On a d'abord*

$$ab''b' = ab'b'' = a'bb'' = a'b''b = b'a''b$$

ce qui nous donne ensuite

$$(ab'' - ba'')b' = 0$$

et par intégrité de $\mathbb{Z}$ comme $b' \neq 0$ on a finalement $a''b = ab''$.

Ainsi $\sim$ est bien une relation d'équivalence.

2. On doit montrer que la somme et le produit dans $\mathbb{Q}$ ne dépendent pas du choix des représentants pour les classes d'équivalence. Si $\frac{a}{b} = \frac{c}{d}$ et $\frac{a'}{b'} = \frac{c'}{d'}$ on a les relations

$$ad = cb \quad \text{et} \quad a'd' = c'b'. \tag{1}$$

On voudrait montrer que

$$\frac{ab' + a'b}{bb'} = \frac{cd' + c'd}{dd'}$$

ce qui est équivalent à

$$\begin{gathered}(ab' + a'b)dd' = (cd' + c'd)bb' \\ \Updownarrow \\ ab'dd' + a'bdd' = cd'bb' + c'dbb' \\ \Updownarrow \\ adb'd' + a'd'bd = cbb'd' + c'b'bd\end{gathered}$$

où la dernière équation est satisfaite grâce à (1).

Le produit se montre de la même manière.

3. On prouve d'abord que $(\mathbb{Q}, +)$ est un groupe abélien:

i) $\frac{0}{1}$ est l'élément neutre car pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$ on a

$$\frac{0}{1} + \frac{a}{b} = \frac{0 \cdot b + 1 \cdot a}{1 \cdot b} = \frac{a}{b}.$$

ii) L'inverse additif de $\frac{a}{b}$ est donné par $\frac{-a}{b}$.

iii) L'opération $+$ est associative car si on prend $\frac{a}{b}, \frac{a'}{b'}, \frac{a''}{b''} \in \mathbb{Q}$ alors on a

$$\begin{aligned}\left(\frac{a}{b} + \frac{a'}{b'}\right) + \frac{a''}{b''} &= \frac{ab' + a'b}{bb'} + \frac{a''}{b''} \\ &= \frac{ab'b'' + a'bb'' + a''bb'}{bb'b''} \\ &= \frac{a}{b} + \frac{a'b'' + a''b'}{b'b''} \\ &= \frac{a}{b} + \left(\frac{a'}{b'} + \frac{a''}{b''}\right).\end{aligned}$$

iv) La commutativité de l'opération $+$ est une conséquence immédiate de la commutativité de $\mathbb{Z}$ et de la définition de la somme dans $\mathbb{Q}$.

Ensuite on montre que $(\mathbb{Q}, \cdot)$ est un monoïde avec $\frac{1}{1}$ comme élément neutre et les opérations $+$ et $\cdot$ dans $\mathbb{Q}$ sont distributives. La preuve de ces faits et similaire à la preuve que $(\mathbb{Q}, +)$ est un groupe abélien et sera donc omise.

Il reste à montrer que ι est un homomorphisme d'anneau injectif. Pour tout $a, b \in \mathbb{Z}$ on a

$$\iota(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \iota(a) + \iota(b)$$

et

$$\iota(a \cdot b) = \frac{a \cdot b}{1} = \frac{a}{1} \cdot \frac{b}{1} = \iota(a) \cdot \iota(b)$$

ainsi que $\iota(1) = \frac{1}{1}$ qui est bien l'unité de $\mathbb{Q}$. L'injectivité de ι découle des équivalences suivantes:

$$\iota(a) = \iota(b) \Leftrightarrow \frac{a}{1} = \frac{b}{1} \Leftrightarrow a \cdot 1 = b \cdot 1 \Leftrightarrow a = b.$$

Ceci termine la construction du corps des nombres rationnels $\mathbb{Q}$ à partir de l'anneau des nombres entiers $\mathbb{Z}$.

Il est intéressant de noter que cette construction ne fonctionne pas seulement dans le cas de $\mathbb{Z}$, mais qu'elle fournit pour chaque anneau intègre R un corps dans lequel on peut inclure l'anneau R de manière injective. Ce corps est appelé corps des fractions et on le dénote $Frac(R)$. Peux-tu construire le corps des fractions de l'anneau polynomial $K[x]$ pour n'importe quel corps K en utilisant la même construction ?

Exercice 8. (*) Soit K un corps, et $f, g \in K[x]$ deux polynômes pas tous les deux nuls. Considérons l'ensemble des diviseurs communs à f et g :

$$\mathcal{D}_{f,g} = \{d \in K[x] \ : \ d|f, d|g\}.$$

1. Montrer qu'il existe un unique polynôme $d \in \mathcal{D}_{f,g}$ unitaire et de degré maximal.
2. Montrer que $d = \gcd(f, g)$.

Solution.