MPSI 1

Mathématiques
DS 07

Samedi 14 mars – 8h-12h

- Durée : 4 heures.
  - Prenez **10 minutes** pour lire le sujet en entier et décider de la stratégie que vous adopterez.
  - Prenez **10 minutes** au moins à la fin des 4 heures pour vous relire !
- Toute calculatrice ou appareil électronique est interdit.
- Le sujet est composé d'un seul problème.
- **Consignes de présentation.**
  - Les pages doivent être **numérotées.**
  - Les résultats doivent être **mis en valeur** (encadrés ou soulignés).
  - Les questions doivent être **numérotées**. Une question non numérotée, c'est une question potentiellement non corrigée.
  - Les questions doivent être **faites dans l'ordre** : si vous admettez une question, laissez de la place à l'endroit où elle est censée être pour y revenir ensuite. Changez de copie ou de page quand vous changez de grande partie.
- À tout moment, vous pouvez admettre le résultat d'une question pour pouvoir continuer : il suffit de le préciser clairement sur la copie.
- Si vous voyez ce qui semble être une erreur d'énoncé, indiquez-le sur la copie.
- Laissez de la place dans une marge à gauche pour pouvoir noter plus facilement le devoir.
- Une réponse fausse, si elle ne laisse pas paraître de calculs intermédiaires, compte 0 points ; avec calculs intermédiaires elle peut rapporter quelques points.

♫ Bon courage ! ♫

Polynômes annulateurs

Le but de ce problème est d'étudier une notion centrale en mathématiques : celle de « polynôme annulateur ».
La partie A. vous fait manipuler la notion d'idéal, qui est une structure algébrique qui sera utile durant tout le problème.
La partie B. manipule la notion de polynôme annulateur de matrices.
La partie C. fait étudier la notion de nombres algébriques : un peu d'algèbre linéaire (sans applications linéaires) sera nécessaire.
Enfin, la partie D. traite de polynômes annulateurs d'endomorphismes et aura besoin du cours d'algèbre linéaire jusqu'à mercredi.

A. Idéaux de $\mathbb{K}[X]$

Soit $\mathcal{I}$ une partie de $\mathbb{K}[X]$. On dit que $\mathcal{I}$ est un idéal de $\mathbb{K}[X]$ si :

- $0_{\mathbb{K}[X]} \in \mathcal{I}$,
- $\forall (P,Q) \in \mathcal{I}^2,\ P-Q \in \mathcal{I}$,
- $\forall P \in \mathcal{I},\ \forall Q \in \mathbb{K}[X],\ P \times Q \in \mathcal{I}$.

On remarquera que le dans le troisième point, P est dans $\mathcal{I}$ mais Q est **quelconque dans $\mathbb{K}[X]$.**

1. On note, si $P \in \mathbb{K}[X]$, $P.\mathbb{K}[X] = \{PQ, Q \in \mathbb{K}[X]\}$, l'ensemble des multiples de P. Montrer que $P.\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$.

Correction

Déjà, $0_{\mathbb{K}[X]} = P \times 0_{\mathbb{K}[X]}$, donc $0_{\mathbb{K}[X]} \in P.\mathbb{K}[X]$.
Ensuite, si (A,B) sont dans $P.\mathbb{K}[X]$, alors on dispose de (Q,R) dans $\mathbb{K}[X]$ tels que $A = PQ$ et $B = PR$. Ainsi, $A - B = P(Q-R) \in P.\mathbb{K}[X]$.
Enfin, si $A \in P.\mathbb{K}[X]$ et $B \in \mathbb{K}[X]$, alors on dispose de Q dans $\mathbb{K}[X]$ tel que $A = PQ$. Donc $AB = P(QB) \in P.\mathbb{K}[X]$.
Donc $P.\mathbb{K}[X]$ est bien un idéal de $\mathbb{K}[X]$.

On montre la réciproque : soit $\mathcal{I}$ un idéal de $\mathbb{K}[X]$, non réduit à $\{0_{\mathbb{K}[X]}\}$.

2. Démontrer qu'il existe un polynôme de $\mathcal{I}$, non nul, de degré minimal. On le note P. Vérifier que $P.\mathbb{K}[X] \subset \mathcal{I}$.

Correction

On considère $A = \{\deg(P),\ P \in \mathcal{I} \setminus \{0_{\mathbb{K}[X]}\}\}$. Alors A est une partie de $\mathbb{N}$, non vide car $\mathcal{I}$ n'est pas réduit à $\{0_{\mathbb{K}[X]}\}$, donc A possède un plus petit élément m. On dispose donc de $P \in A$ de degré m minimal.
Comme $\mathcal{I}$ est un idéal de $\mathbb{K}[X]$, alors pour tout Q dans $\mathbb{K}[X]$, $PQ \in \mathcal{I}$, donc $P.\mathbb{K}[X] \subset \mathcal{I}$.

3. Soit $Q \in \mathcal{I}$. Démontrer que P divise Q. On a donc démontré que $\mathcal{I} = P.\mathbb{K}[X]$.

Correction

On effectue la division euclidienne de Q par P : $Q = AP + R$. Alors $AP \in \mathcal{I}$, $Q \in \mathcal{I}$ donc $R = Q - AP \in \mathcal{I}$. Donc R est un élément de $\mathcal{I}$, de degré strictement inférieur à $\deg(P)$. Par minimalité de $\deg(P)$, on en déduit que $R = 0_{\mathbb{K}[X]}$. Ainsi, P divise Q.

4. Démontrer que le P trouvé précédemment est unique si on le suppose unitaire.

Correction

On sait que si R est dans $\mathcal{I}$ de degré $\deg(P)$, alors P divise R. Donc tous les polynômes de degré $\deg(P)$ sont associés à P. Ainsi, si on impose à P d'être unitaire, il est unique.

Ainsi, pour tout idéal $\mathcal{I}$ de $\mathbb{K}[X]$, il existe un unique polynôme unitaire P tel que $\mathcal{I} = P.\mathbb{K}[X]$.

B. Polynôme annulateur d'une matrice

Soit $M \in \mathscr{M}_n(\mathbb{C})$ une matrice à coefficients complexes. Si $P(X) = \sum_{k=0}^{d} a_k X^k$, on définit l'évaluation de P en M par

$$P(M) = \sum_{k=0}^{d} a_k M^k, \text{ avec la convention } M^0 = \mathrm{I}_n.$$

Ainsi, si $P(X) = 2X^2 + 3X - 4$, et $A \in \mathscr{M}_n(\mathbb{C})$, $P(A) = 2A^2 + 3A - 4\mathrm{I}_n$.
Un polynôme P est appelé polynôme annulateur de M si $P(M) = 0_n$ (matrice nulle).
On peut remarquer que si $M \in \mathscr{M}_n(\mathbb{C})$, si P et Q sont deux polynômes, alors

$$(P+Q)(M) = P(M) + Q(M) \text{ et } (PQ)(M) = P(M) \times Q(M).$$

On rappelle donc que si P est un polynôme et M est une matrice, $P(M)$ est **une matrice**.

B-I. Un exemple

On pose ici $A = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$.

5. Montrer que $P(X) = X^2 + X - 2$ est un polynôme annulateur de A. En déduire l'inversibilité et l'inverse de A.

Correction

Calculons $P(A)$:

$$\begin{aligned} P(A) &= A^2 + A - \mathrm{I}_3 \\ &= \begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix} + \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} - 2\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} - \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} = 0_3, \end{aligned}$$

donc P est bien un polynôme annulateur de A.

On sait que $A^2 + A - 2\mathrm{I}_3 = 0$, donc $A(A + \mathrm{I}_3) = 2\mathrm{I}_3$, donc $AB = \mathrm{I}_3$ où $B = \frac{1}{2}(A + \mathrm{I}_3)$, donc A est inversible d'inverse $B = \frac{1}{2}\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.

6. En étudiant la division euclidienne de X^n par P, déterminer une expression de A^n pour tout n dans $\mathbb{N}$.

Correction

Soit n dans $\mathbb{N}$. On sait que le reste de la division de X^n par P est de degré 1, il est donc de la forme $aX+b$. On a donc

$$X^n = Q(X)(X^2+X-2)+aX+b.$$

Or, $X^2+X-2=(X-1)(X+2)$. En évaluant l'égalité précédente en 1, on obtient $1=a+b$. En l'évaluant en -2, on obtient $(-2)^n=-2a+b$. D'où $a=\frac{1}{3}(1-(-2)^n)$ et $b=\frac{1}{3}(2+(-2)^n)$. Donc le reste de la division euclidienne de X^n par X^2+X-2 est $\frac{1}{3}(1-(-2)^n)X+\frac{1}{3}(2+(-2)^n)$. On sait donc que

$$X^n = Q(X)P(X)+\frac{1}{3}(1-(-2)^n)X+\frac{1}{3}(2+(-2)^n),$$

donc

$$A^n = Q(A)P(A)+\frac{1}{3}(1-(-2)^n)A+\frac{1}{3}(2+(-2)^n)\mathrm{I}_3,$$

donc, comme $P(A)=0$,

$$\begin{aligned}
&A^n\\
&=\frac{1}{3}(1-(-2)^n)A+\frac{1}{3}(2+(-2)^n)\mathrm{I}_3\\
&=\frac{1}{3}\begin{pmatrix}(-2)^n-1 & 1-(-2)^n & 1-(-2)^n\\ 1-(-2)^n & (-2)^n-1 & 1-(-2)^n\\ 1-(-2)^n & 1-(-2)^n & (-2)^n-1\end{pmatrix}-\frac{1}{3}\begin{pmatrix}2+(-2)^n & 0 & 0\\ 0 & 2+(-2)^n & 0\\ 0 & 0 & 2+(-2)^n\end{pmatrix}\\
&=\frac{1}{3}\begin{pmatrix}1-(-2)^{n+1} & 1-(-2)^n & 1-(-2)^n\\ 1-(-2)^n & 1-(-2)^{n+1} & 1-(-2)^n\\ 1-(-2)^n & 1-(-2)^n & 1-(-2)^{n+1}\end{pmatrix}
\end{aligned}$$

B-II. Matrice compagnon associée à un polynôme – théorème de Cayley-Hamilton

Si $P(X)=X^n+\sum_{k=0}^{n-1}a_kX^k$ est un polynôme **unitaire** (avec $(a_0,\dots,a_{n-1})$ des complexes), on définit la matrice compagnon associée à P par

$$C_P=\begin{pmatrix}0 & 0 & \cdots & 0 & -a_0\\ 1 & \ddots & & \vdots & -a_1\\ 0 & \ddots & \ddots & \vdots & \vdots\\ \vdots & \ddots & \ddots & 0 & \vdots\\ 0 & \cdots & 0 & 1 & -a_{n-1}\end{pmatrix}$$

7. Si P est un polynôme unitaire de degré n, si $\alpha_1,\dots,\alpha_r$ sont les racines complexes de P et $m_1,\dots,m_r$ leurs multiplicités, exprimer $\mathrm{Tr}(C_P)$ en fonction de $\alpha_1,\dots,\alpha_r$ et $m_1,\dots,m_r$.

Correction

D'après la définition, $\mathrm{Tr}(C_P)=-a_{d-1}$. Or, d'après les relations coefficients racines, $-a_{d-1}$ est la somme des racines de P, donc $\mathrm{Tr}(C_P)=m_1\alpha_1+\cdots+m_r\alpha_r$.

8. Dans cette question seulement, $P(X)=X^3-X^2+X-2$. Donner l'expression de $A=C_P$ et vérifier

que $P(A) = 0$.

Correction

La matrice compagnon de P est $A = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}$.

On calcule alors

$$A^2 = \begin{pmatrix} 0 & 2 & 2 \\ 0 & -1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \ A^3 = \begin{pmatrix} 2 & 2 & 0 \\ -1 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix},$$

d'où

$$A^3 - A^2 + A - 2 = \begin{pmatrix} 2 & 2 & 0 \\ -1 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 2 & 2 \\ 0 & -1 & 1 \\ 1 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix} - 2\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 0$$

Le but de la suite de la partie est de généraliser ce résultat, qui est un cas particulier du **théorème de Cayley-Hamilton** : pour tout polynôme P unitaire, $P(C_P) = 0_n$.

Soit P un polynôme unitaire, $P(X) = X^n + \sum_{k=0}^{n-1} a_k X^k$. On pose $A = C_P$. On note $(e_1, \dots, e_n)$ la base canonique de $\mathscr{M}_{n,1}(\mathbb{C})$.

9. Donner la valeur de $A^k e_1$ pour tout k dans $[\![0, n]\!]$, et en déduire que $P(A)e_1 = 0_{n,1}$.

Correction

On fait le calcul directement avec les matrices $n \times n$

$$Ae_1 = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{d-1} \end{pmatrix} \times \begin{pmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = e_2.$$

On remarque que de même, $A^2 e_1 = Ae_2 = e_3$ et que pour tout k dans $[\![0, n-1]\!]$, $A^k e_1 = e_{k+1}$. Ensuite,

$$A^n e_1 = Ae_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{d-1} \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -a_0 \\ -a_1 \\ -a_2 \\ \vdots \\ -a_{n-1} \end{pmatrix}$$

On calcule

$$\left(A^n+\sum_{k=0}^{n-1}a_kA^k\right)e_1 = A^ne_1+\sum_{k=0}^{n-1}a_kA^ke_1$$

$$= \begin{pmatrix}-a_0\\-a_1\\-a_2\\\vdots\\-a_{n-1}\end{pmatrix} + a_0\begin{pmatrix}1\\0\\\vdots\\\vdots\\0\end{pmatrix} + a_1\begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix} + \cdots + a_{n-1}\begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix}$$

$$= \begin{pmatrix}-a_0\\-a_1\\-a_2\\\vdots\\-a_{n-1}\end{pmatrix} + \begin{pmatrix}a_0\\0\\\vdots\\\vdots\\0\end{pmatrix} + \begin{pmatrix}0\\a_1\\0\\\vdots\\0\end{pmatrix} + \cdots + \begin{pmatrix}0\\0\\\vdots\\0\\a_{n-1}\end{pmatrix} = \begin{pmatrix}0\\0\\\vdots\\0\\0\end{pmatrix}$$

10. Calculer, pour tout j dans $[\![1,n]\!]$, $P(A)e_j$, puis montrer que $P(A)=0_n$.

Correction

Si $j\in[\![1,n]\!]$, $e_j = A^j\times e_1$. Donc

$$\begin{aligned}P(A)e_j &= \left(A^n+\sum_{k=0}^{n-1}a_kA^k\right)e_j\\ &= \left(A^n+\sum_{k=0}^{n-1}a_kA^k\right)A^je_1\\ &= \left(A^{n+j}+\sum_{k=0}^{n-1}a_kA^{k+j}\right)e_1\\ &= A^j\left(A^n+\sum_{k=0}^{n-1}a_kA^k\right)e_1 = A^jP(A)e_1 = 0.\end{aligned}$$

D'où le résultat ! (c'était infiniment plus simple que de refaire tous les calculs !)
On remarque que la matrice I_n est la matrice $(e_1\ e_2\ \cdots\ e_n)$ (avec les vecteurs e_k accollés), donc $P(A)\mathrm{I}_n = (P(A)e_1\ P(A)e_2\ \cdots\ P(A)e_n) = (0\ 0\ \cdots\ 0)$. Donc $A = A\mathrm{I}_n = 0_n$, donc $A = 0_n$.

B-III. Idéal annulateur d'une matrice

Soit A dans $\mathscr{M}_n(\mathbb{C})$, on note $\mathrm{Ann}(A)$ l'ensemble des polynômes annulateurs de A :

$$\mathrm{Ann}(A) = \{P\in\mathbb{C}[X],\ P(A)=0_n\}.$$

11. Démontrer que $\mathrm{Ann}(A)$ est un idéal de $\mathbb{C}[X]$. En déduire qu'il existe un unique polynôme unitaire $\pi_A\in\mathbb{C}[X]$ tel que $\mathrm{Ann}(A) = \pi_A.\mathbb{C}[X]$.

Correction

On vérifie que $\mathrm{Ann}(A)$ est un idéal de $\mathbb{C}[X]$:

- Déjà, $0_{\mathbb{C}[X]}(A) = 0_n$, donc $0_{\mathbb{C}[X]} \in \mathrm{Ann}(A)$.
- Ensuite, si $(P, Q) \in \mathrm{Ann}(A)^2$, $(P - Q)(A) = P(A) - Q(A) = 0_n$, donc $P - Q \in \mathrm{Ann}(A)$.
- Enfin, si $P \in \mathrm{Ann}(A)$ et $Q \in \mathbb{C}[X]$, $(P \times Q)(A) = P(A) \times Q(A) = 0_n \times Q(A) = 0_n$, donc $PQ \in \mathrm{Ann}(A)$.

Donc $\mathrm{Ann}(A)$ est un idéal de $\mathbb{C}[X]$. Par la partie A, on dispose donc de π_A unitaire dans $\mathbb{C}[X]$ tel que $\mathrm{Ann}(A) = \pi_A.\mathbb{C}[X]$.

On appelle ce polynôme π_A le polynôme minimal de A.
Dans cette fin de partie, on suppose que A est une matrice compagnon. On dispose alors de P un polynôme unitaire de degré n vérifiant $A = C_P$.

12. Démontrer que π_A divise P.

Correction

On a vu que $P(A) = 0_n$ donc $P \in \mathrm{Ann}(A)$, ce qui signifie que π_A divise P.

Soit $Q \in \mathbb{C}_{n-1}[X]$, notons $Q(X) = \sum_{k=0}^{n-1} b_k X^k$. On suppose que $Q(A) = 0_n$.

13. Calculer $Q(A)e_1$, et en déduire que $Q = 0_{\mathbb{C}[X]}$.

Correction

On remarque que

$$Q(A)e_1 = \sum_{k=0}^{n-1} b_k A^k e_1 = \sum_{k=0}^{n-1} b_k e_{k+1} = \begin{pmatrix} b_0 \\ \vdots \\ b_{n-1} \end{pmatrix}.$$

Comme $Q(A) = 0_n$, $Q(A)e_1 = 0_{n,1}$, donc $\begin{pmatrix} b_0 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$, donc $b_0 = \cdots = b_{n-1} = 0_{\mathbb{C}}$, donc $Q = 0_{\mathbb{C}[X]}$.

14. Conclure enfin $\pi_A = P$.

Correction

Il suffit, au vu de la partie A, de démontrer que P est un polynôme non nul de degré minimal annulateur de A. Or, on a vu que si $\deg(Q) < \deg(P)$ et Q annule A, alors $Q = 0_{\mathbb{C}[X]}$. Donc P est bien un polynôme non nul de degré minimal annulateur de A. Comme P est unitaire, on a bien $\mathrm{Ann}(A) = P.\mathbb{C}[X]$, donc, $P = \pi_A$.

C. Polynômes annulateurs de nombres complexes

Dans cette partie seulement, tous les espaces vectoriels considérés seront des $\mathbb{Q}$-espaces vectoriels.
On considère donc que $\mathbb{C}$ est bien un $\mathbb{Q}$-espace vectoriel : les vecteurs sont dans $\mathbb{C}$ et les scalaires sont dans $\mathbb{Q}$.
Ainsi, $j = \mathrm{e}^{\frac{2i\pi}{3}}$ est une combinaison linéaire de 1 et de $i\sqrt{3}$ car $j = \underbrace{-\frac{1}{2}}_{\in\mathbb{Q}}.1 + \underbrace{\left(-\frac{1}{2}\right)}_{\in\mathbb{Q}}.i\sqrt{3}$.
On a aussi, à titre d'exemple, $\mathrm{Vect}(1, i\sqrt{3}) = \{a + bi\sqrt{3},\ (a,b) \in \mathbb{Q}^2\}$.
Bref, **les scalaires sont des rationnels.**

C-I. Nombres algébriques

Soit $\alpha \in \mathbb{C}$. On dit que α est algébrique s'il existe un polynôme $P \in \mathbb{Q}[X]$ non nul tel que $P(\alpha) = 0$. Un nombre complexe qui n'est pas algébrique est transcendant.

15. Montrer que α est algébrique si et seulement si il existe un entier p tel que la famille $(1, \alpha, \cdots, \alpha^p)$ est liée.

Correction

On raisonne par équivalences (mais c'est très bien par double implications) :

$$\begin{aligned}\alpha \text{ est algébrique} &\Leftrightarrow \exists P \in \mathbb{Q}[X] \setminus \{0_{\mathbb{Q}[X]}\},\ P(\alpha) = 0\\ &\Leftrightarrow \exists p \in \mathbb{N},\ \exists (a_0, \ldots, a_p) \in \mathbb{Q}^{p+1} \setminus \{(0,\ldots,0)\},\ \sum_{k=0}^{p} a_k \alpha^k = 0\\ &\Leftrightarrow \exists p \in \mathbb{N},\ (1, \alpha, \ldots, \alpha^p) \text{ est liée.}\end{aligned}$$

Soit α algébrique et d le plus petit des entiers p tels que la famille $(1, \alpha, \cdots, \alpha^p)$ soit liée. On dira que d est le **degré** de α. On note

$$\mathbb{Q}[\alpha] = \mathrm{Vect}\left(1, \alpha, \cdots \alpha^{d-1}\right).$$

16. Montrer que si $\alpha \neq 0$, $\alpha \in \mathbb{Q}$ si et seulement si $d = 1$.

Correction

Si $\alpha \in \mathbb{Q}$, on a $\alpha.1 - 1.\alpha = 0$ et $(\alpha, 1) \in \mathbb{Q}^2$, donc $(1, \alpha)$ est liée, donc $d = 1$.
Si $d = 1$, $(1, \alpha)$ est liée, donc on dispose de $(a,b) \in \mathbb{Q}^2$ vérifiant $(a,b) \neq (0,0)$ et tels que $a + b\alpha = 0$. Déjà, $b \neq 0$ car sinon $a = 0$, donc $\alpha = -\frac{a}{b} \in \mathbb{Q}$.

17. Démontrer que $\sqrt{2}$ et j sont algébriques et déterminer leurs degrés.

Correction

On remarque que $\sqrt{2} \notin \mathbb{Q}$, donc $(1, \sqrt{2})$ est libre. Mais $\sqrt{2}^2 - 2 = 0$, donc $(1, \sqrt{2}, \sqrt{2}^2)$ est liée, ce qui assure que $\sqrt{2}$ est algébrique de degré 2.
Ensuite, $j \notin \mathbb{Q}$ donc $(1, j)$ est libre. Mais $1 + j + j^2 = 0$ donc $(1, j, j^2)$ est liée, donc j est algébrique de degré 2.

On suppose désormais α irrationnel.

18. Montrer que $\left(1, \alpha, \cdots, \alpha^{d-1}\right)$ est une base de $\mathbb{Q}[\alpha]$.

Correction

On sait que $\left(1, \alpha, \cdots, \alpha^{d-1}\right)$ est génératrice de $\mathbb{Q}[\alpha]$. Ensuite, comme d est le plus petit entier tel que $(1, \alpha, \ldots, \alpha^{d-1})$ est liée, cela signifie que $(1, \alpha, \ldots, \alpha^{d-1})$ est libre.
Libre et génératrice, cette famille est une base de $\mathbb{Q}[\alpha]$.

19. Montrer que $\alpha^n \in \mathbb{Q}[\alpha]$ pour tout entier naturel n.

Correction

Plusieurs manières de faire cela : par récurrence ou comme suit. Soit P un polynôme de degré d tel que $P(\alpha) = 0$ (c'est la relation de liaison de $(1, \alpha, \ldots, \alpha^d)$. Effectuons la division euclidienne de X^n par P. Alors on dispose de Q, R dans $\mathbb{C}[X]$ tel que $X^n = PQ + R$, et $\deg(R) < d$.
Alors $\alpha^n = P(\alpha)Q(\alpha) + R(\alpha) = R(\alpha) \in \mathbb{Q}[\alpha]$.

20. Montrer que $\alpha^{-1} \in \mathbb{Q}[\alpha]$.

Correction

On note

$$p_0 + p_1\alpha + \cdots + p_{d-1}\alpha^{d-1} = 0$$

une relation de liaison entre $(1, \alpha, \ldots, \alpha^{d-1})$. On remarque que $p_0 \neq 0$ car, sinon, en divisant par α, on aurait une relation de liaison entre $(1, \alpha, \ldots, \alpha^{d-2})$. On a donc

$$-\sum_{i=1}^{d-1} \frac{p_i}{p_0}\alpha^i = 1,$$

d'où

$$\alpha \times \left(-\sum_{i=1}^{d-1} \frac{p_i}{p_0}\alpha^{i-1}\right) = 1,$$

donc

$$\frac{1}{\alpha} = -\sum_{i=1}^{d-1} \frac{p_i}{p_0}\alpha^{i-1} \in \mathbb{Q}[\alpha].$$

21. Montrer qu'il existe un unique $P \in \mathbb{Q}[X]$ unitaire et irréductible sur $\mathbb{Q}$ tel que $P(\alpha) = 0$. Quel est son degré ? On le note π_α.

Correction

On considère $\mathrm{Ann}(\alpha) = \{P \in \mathbb{Q}[X],\ P(\alpha) = 0\}$. On montre, de même que dans la partie précédente, que $\mathrm{Ann}(\alpha)$ est un idéal de $\mathbb{Q}[X]$, donc que l'on dispose d'un unique π_α unitaire et de degré minimal vérifiant $\pi_\alpha(\alpha) = 0$.
Si π_α n'était pas irréductible, on disposerait de (A, B) dans $\mathbb{Q}[X]$, de degrés $< \deg(\pi_\alpha)$, tels que $\pi_\alpha = AB$. Ainsi, on aurait $A(\alpha)B(\alpha) = 0$, donc on aurait $A(\alpha) = 0$ ou $B(\alpha) = 0$, ce qui entre en contradiction avec la minimalité du degré de π_α.
Enfin, $\deg(\pi_\alpha) = d$ car, par définition du degré, pour tout A dans $\mathbb{C}_{d-1}[X]$ non nul, $A(\alpha) \neq 0$.

22. Démontrer que $\mathbb{Q}[\alpha]$ est un corps.
Indication. On pourra vérifier que tout polynôme non nul de $\mathbb{Q}_{d-1}[X]$ est premier avec π_A.

Correction

On montre que $\mathbb{Q}[\alpha]$ est un sous-corps de $\mathbb{C}$.
En effet, $1 \in \mathbb{Q}[\alpha]$ et, si $(x, y) \in \mathbb{Q}[\alpha]^2$, on dispose de (P, Q) deux polynômes à coefficients dans $\mathbb{Q}$, de degré inférieur ou égal à d tels que $x = P(\alpha)$ et $y = Q(\alpha)$. Cela signifie donc que

$$x - y = P(\alpha) - Q(\alpha) = (P - Q)(\alpha),$$

et $P - Q$ est de degré inférieur ou égal à d. Donc $x - y \in \mathbb{Q}[\alpha]$.
De plus, si $P(X) = \sum_{i=0}^{d} p_i X^i$ et $Q(X) = \sum_{i=0}^{d} q_i X^i$, on a

$$xy = \sum_{i=0}^{2d} r_i \alpha^i,$$

avec $r_i \in \mathbb{Q}$ (par produit de Cauchy). Mais, pour tout i dans $[\![0, 2d]\!]$, $\alpha^i \in \mathbb{Q}[\alpha]$, donc $r_i \alpha^i$ aussi, donc $xy \in \mathbb{Q}[\alpha]$.
Enfin, pour l'inverse, c'est un peu plus compliqué.
On sait que $P \in \mathbb{Q}_{d-1}[X]$, non nul. On note $A = P \wedge \pi_\alpha$. Alors A est un polynôme de $\mathbb{Q}[X]$ qui divise π_α. Par irréductibilité de π_α, $A = \pi_\alpha$ ou $A = 1$. Mais comme $\deg(A) \leqslant \deg(P)$, $A = 1$. Donc $P \wedge \pi_\alpha = 1$, ce qui signifie que l'on dispose de (U, V) dans $\mathbb{Q}[X]^2$ tels que $UP + V\pi_\alpha = 1$. En évaluant en α, on a $U(\alpha)P(\alpha) = 1$. Ainsi, $\dfrac{1}{P(\alpha)} = U(\alpha) \in \mathbb{Q}[\alpha]$ (car toutes les puissances de α sont dans $\mathbb{Q}[\alpha]$).
Donc $\mathbb{Q}[\alpha]$ est un corps.

C-II. Stabilité par somme

Soit P et Q deux polynômes à coefficients rationnels. Pour $s \in \mathbb{C}$, on note par $Q_s(X) = Q(s - X)$.

23. Soient $P = X^2+X+1$ et $Q = X^2-2$. Soit $s \in \mathbb{C}$. En calculant le pgcd de P et Q_s à l'aide de l'algorithme d'Euclide, démontrer que P et Q_s sont premiers entre eux si et seulement si $s^4 + 2s^3 - s^2 - 2s + 7 \neq 0$.

Correction

On écrit que $Q_s(X) = (s - X)^2 - 2 = X^2 - 2sX + s^2 - 2$. On applique l'algorithme d'Euclide à P et à Q :

$$P(X) = Q_s(X) + (1 + 2s)X + 3 - s^2.$$

Si $s = -\dfrac{1}{2}$, alors P et Q_s sont automatiquement premiers entre eux.
Sinon, $R(X) \neq 0$ et on poursuit l'algorithme, en notant $R(X) = (1 + 2s)X + 3 - s^2$. On a alors

$$Q_s(X) = R(X)T(X) + C,$$

où C est une constante, égale à

$$\begin{aligned} Q_s\left(\frac{s^2-3}{1+2s}\right) &= \left(s-\frac{s^2-3}{1+2s}\right)^2 - 2 \\ &= \frac{(s+2s^2-s^2+3)^2}{(1+2s)^2} - 2 \\ &= \frac{(s^2+s+3)^2}{(1+2s)^2} - \frac{2+8s+8s^2}{(1+2s)^2} \\ &= \frac{s^4+s^2+9+2s^3+6s^2+6s-2-8s-8s^2}{(1+2s)^2} \\ &= \frac{s^4+2s^3-s^2-2s+7}{(1+2s)^2}. \end{aligned}$$

Ainsi, si $s^4+2s^3-s^2-2s+7 \neq 0$, P et Q_s sont premiers entre eux ; sinon, ils ne le sont pas.
On a donc P et Q_s sont premiers entre eux si et seulement si $s^4+2s^3-s^2-2s+7 \neq 0$.

24. Factoriser P et Q_s sur $\mathbb{C}$ puis, en étudiant une condition nécessaire et suffisante pour que P et Q_s aient une racine en commun, déterminer un polynôme annulateur de $j+\sqrt{2}$.

Correction

On sait que $P(X) = (X-j)(X-\bar{j})$ et $Q(X) = (X-\sqrt{2})(X+\sqrt{2})$, donc $Q_s(X) = (s-\sqrt{2}-X)(s+\sqrt{2}-X) = (X-(s-\sqrt{2}))(X-(s+\sqrt{2}))$.
On sait ensuite que P et Q_s ont une racine en commun si et seulement si $P \wedge Q_s \neq 1$, i.e. si et seulement si $s^4+2s^3-s^2-2s+7=0$.
Enfin, on a les équivalences

$$\begin{aligned} s^4+2s^3-s^2-2s+7=0 \Leftrightarrow\ & P \text{ et } Q_s \text{ ont une racine en commun} \\ \Leftrightarrow\ & s-\sqrt{2}=j \text{ ou } s-\sqrt{2}=j^2 \text{ ou } s+\sqrt{2}=j \text{ ou } s-\sqrt{2}=j^2 \\ \Leftrightarrow\ & s \in \{j\pm\sqrt{2}, j^2\pm\sqrt{2}\}. \end{aligned}$$

On en déduit que $X^4+2X^3-X^2-2X+7$ est un polynôme annulateur de $j+\sqrt{2}$.

25. Expliquer comment, de manière générale, si α et β sont algébriques, on peut trouver un polynôme annulateur de $\alpha+\beta$ à coefficients dans $\mathbb{Q}$.

Correction

On considère P un polynôme annulateur de α, Q de β et on note $Q_s = Q(s-X)$.
On fait un algorithme d'Euclide pour trouver une condition polynomiale sur s pour que P et Q_s ne soient pas premiers entre eux, i.e. aient une racine en commun.
Or, P et Q_s ont une racine en commun ssi s est la somme d'une racine de P et d'une racine de Q. La condition polynomiale en s donne donc un polynôme annulateur de $\alpha+\beta$.

D. Polynôme annulateur d'un endomorphisme

Soit E un $\mathbb{K}$-espace vectoriel. Si $P(X)=\sum_{k=0}^{n} a_k X^k$, et u est un endomorphisme de E, on définit $P(u)=\sum_{k=0}^{n} a_k u^k$, en posant $u^0=\mathrm{Id}_E$.
On dit que P est **annulateur** de u si $P(u)=0_{\mathscr{L}(E)}$. On note $\mathrm{Ann}(u)=\{P\in\mathbb{K}[X],\ P(u)=0_{\mathscr{L}(E)}\}$.

D-I. Un exemple

On fixe un entier naturel n. Dans cette partie seulement, on considère $E=\mathbb{K}_n[X]$ et u : $\left|\begin{array}{l}\mathbb{K}_n[X]\to\mathbb{K}_n[X]\\ P\mapsto P(X+1)-P(X)\end{array}\right.$.

26. Démontrer que $u\in\mathscr{L}(E)$.

Correction

Déjà, u est bien à valeurs dans E. Ensuite, si (P,Q) sont dans $\mathbb{K}_n[X]$ et (λ,μ) sont dans $\mathbb{K}$,

$u(\lambda P+\mu Q)=(\lambda P+\mu Q)(X+1)-(\lambda P+\mu Q)(X)=\lambda(P(X+1)-P(X))+\mu(Q(X+1)-Q(X))=\lambda u(P)+\mu u(Q)$,

donc $u\in\mathscr{L}(E)$.

27. Déterminer $\ker(u)$.

Correction

Déjà, $\mathbb{K}_0[X]\subset\ker(u)$ car si P est constant, égal à λ, $P(X+1)-P(X)=\lambda-\lambda=0_{\mathbb{K}[X]}$.
Réciproquement, si $P\in\ker(u)$, alors $P(X+1)=P(X)$. Donc, par récurrence immédiate, pour tout n dans $\mathbb{N}$, $P(n)=P(0)$, donc $Q=P-P(0)$ s'annule une infinité de fois, donc $P=P(0)\in\mathbb{K}_0[X]$.
Ainsi, $\boxed{\ker(u)=\mathbb{K}_0[X]}$.

28. Démontrer que pour tout P dans $\mathbb{K}_n[X]$ non constant, $\deg(u(P))=\deg(P)-1$.

Correction

Soit $P\in\mathbb{K}_n[X]$ non constant, $P(X)=\sum_{k=0}^{d} a_k X^k$, et $a_d\neq 0$. Alors

$$\begin{aligned}P(X+1)-P(X)&=\sum_{k=0}^{d} a_k\left((X+1)^k-X^k\right)\\&=\sum_{k=0}^{d} a_k\sum_{i=0}^{k-1}\binom{k}{i}X^i\\&=\sum_{i=0}^{d-1}\sum_{k=i+1}^{d} a_k\binom{k}{i}X^i,\end{aligned}$$

donc $\deg(u(P))\leqslant d-1$, et le coefficient devant X^{d-1} est $da_d\neq 0$, donc $\deg(u(P))=d-1$.

29. En déduire que X^{n+1} est annulateur de u, puis que $\mathrm{Ann}(u)=\{X^{n+1}Q(X),\ Q\in\mathbb{K}[X]\}$.

Correction

Par récurrence immédiate, pour tout P dans $\mathbb{K}_n[X]$, pour tout k dans $\mathbb{N}$,

$$\deg(u^k(P)) = \begin{cases} \deg(P) - k \text{ si } k \leqslant \deg(P) \\ -\infty \text{ sinon.} \end{cases}$$

Ainsi, $u^{n+1}(P) = 0$ pour tout P dans $\mathbb{K}_n[X]$, donc X^{n+1} est annulateur de u.
On montre facilement que $\mathrm{Ann}(u)$ est un idéal de $\mathbb{K}[X]$, donc on dispose de π_u de degré minimal, unitaire, annulant u et $\mathrm{Ann}(u) = \pi_u.\mathbb{K}[X]$. Comme X^{n+1} annule u, π_u divise X^{n+1} donc on dispose de p tel que $\pi_u = X^p$.
Mais, si $p \leqslant n$, $u^p(X^p)$ est de degré 0, donc $u^p(X^p)$ n'est pas nul. Donc X^p n'annule pas u.
Donc X^{n+1} est le polynôme annulateur de u de degré minimal, donc $\pi_u = X^{n+1}$. D'où le résultat !

D-II. Deux questions préliminaires

On revient au cas d'un espace vectoriel quelconque E.
On considère $u \in \mathscr{L}(E)$.

30. Montrer que $E = \ker(u) + \mathrm{Im}(u) \Leftrightarrow \mathrm{Im}(u) = \mathrm{Im}\left(u^2\right)$.

Correction

Cf TD

31. Montrer que $\ker(u) \cap \mathrm{Im}(u) = \{0\} \Leftrightarrow \ker(u) = \ker\left(u^2\right)$.

Correction

Cf TD

D-III. Cœur et nilespace – décomposition de Fitting

Pour tout entier $n \in \mathbb{N}$, on définit $K_n = \ker\left(u^n\right)$ et $\mathrm{I}_n = \mathrm{Im}\left(u^n\right)$.

32. Montrer que pour tout n dans $\mathbb{N}$, $K_n \subset K_{n+1}$ et $\mathrm{I}_{n+1} \subset \mathrm{I}_n$.

Correction

Soit $n \in \mathbb{N}$. Soit $x \in \mathbb{K}_n$. Alors $u^n(x) = 0_E$. Donc $u^{n+1}(x) = 0_E$, donc $x \in \mathbb{K}_{n+1}$. Donc $K_n \subset K_{n+1}$.
Soit $z \in \mathrm{I}_{n+1}$. Alors on dispose de $y \in E$ tel que $z = u^{n+1}(y) = u^n(u(y)) \in \mathrm{I}_n$. Donc $\mathrm{I}_{n+1} \subset \mathrm{I}_n$.

On note $F = \bigcup_{n\in\mathbb{N}} K_n$ et $G = \bigcap_{n\in\mathbb{N}} \mathrm{I}_n$.

33. Démontrer que F et G sont deux sous-espaces vectoriels de E, stables par u (c'est-à-dire que $u(F) \subset F$ et $u(G) \subset G$).

Correction

Déjà, G étant une intersection de sous-espaces vectoriels de E, G est un sous-espace vectoriel de E. De plus, soit $x \in G$. Soit $n \in \mathbb{N}$. $x \in \mathrm{I}_n$ donc on dispose de w dans E tel que $x = u^n(w)$. Donc $u(x) = u^n(u(w)) \in \mathrm{I}_n$. Donc, pour tout n dans $\mathbb{N}$, $u(x) \in \mathrm{I}_n$, donc $u(x) \in G$, donc G est stable par u.
Ensuite, on montre que F est un sous-espace vectoriel.

$0_E \in K_0$ donc $0_E \in F$.
Ensuite, soient x et y dans F, $(\lambda, \mu) \in \mathbb{K}^2$. Alors on dispose de $(n, m) \in \mathbb{N}^2$ tels que $u^n(x) = 0_E$ et $u^m(y) = 0_E$.
Donc $u^{n+m}(\lambda x + \mu y) = \lambda u^m(u^n(x)) + \mu u^m(u^n(y)) = 0_E$, donc $\lambda x + \mu y \in K_{n+m} \subset F$, donc F est un sous-espace vectoriel de E.
Enfin, si $u^n(u(x)) = 0$, donc $u(x) \in F$, donc F est stable par u.

On suppose désormais qu'il existe r dans $\mathbb{N}$ tel que $K_r = K_{r+1}$ et s dans $\mathbb{N}$ tel que $\mathrm{I}_s = \mathrm{I}_{s+1}$.

34. Démontrer que pour tout $n \geqslant r$, $K_n = K_r$. On admettra que pour tout $n \geqslant s$, $\mathrm{I}_n = \mathrm{I}_s$.

Correction

On montre le résultat par récurrence sur n.
L'**initialisation** est évidente.
Ensuite, si $n \geqslant r$ est tel que $K_n = K_r$, on montre que $K_{n+1} = K_r$. On a déjà $K_n \subset K_{n+1}$, on montre donc que $K_{n+1} \subset K_n$.
Soit $x \in K_{n+1}$. Alors $u^{n+1}(x) = 0_E$ donc $u^{r+1}(u^{n-r}(x)) = 0_E$, donc $u^{n-r}(x) \in K_{r+1} = K_r$, donc $u^r(u^{n-r}(x)) = 0_E$, donc $u^n(x) = 0_E$, donc $x \in K_n$. Donc $K_{n+1} = K_n = K_r$.
D'où l'hérédité et le résultat.

35. En déduire, en notant $q = \max(r, s)$, que $K_q \oplus \mathrm{I}_q = E$, puis que $F \oplus G = E$.

Correction

Pfiouuu, c'était long comme DS.
Mais là, c'est facile. On sait que $K_q = K_{2q}$ donc $\ker(u^q) = \ker(u^{2q})$, donc, par les questions préliminaires, $\ker(u^q) \cap \mathrm{Im}(u^q) = \{0_E\}$.
Ensuite, on sait que $\mathrm{I}_q = \mathrm{I}_{2q}$ donc, par les questions préliminaires, $\ker(u^q) + \mathrm{Im}(u^q) = E$. D'où la supplémentarité.
Enfin, comme $(K_n)_{n\in\mathbb{N}}$ est croissante stationnaire à partir de q et $(\mathrm{I}_n)_{n\in\mathbb{N}}$ est décroissante stationnaire à partir de q, on a $F = K_q$ et $G = \mathrm{I}_q$, d'où le résultat final !