DM 21 : Polynôme minimal

Partie I : La sous-algèbre $\mathbb{K}[a]$.

Dans toute cette partie, $\mathbb{K}$ désigne un corps quelconque, A est une $\mathbb{K}$-algèbre et a est un élément de A.
Si $P = \sum_{n\in\mathbb{N}} b_n X^n \in \mathbb{K}[X]$, on notera $P(a) = \sum_{n\in\mathbb{N}} b_n a^n$: $P(a)$ est un élément de A.

1°) Montrer que l'application $\begin{array}{cccc} \varphi_a : & \mathbb{K}[X] & \longrightarrow & A \\ & P & \longmapsto & P(a) \end{array}$ est un morphisme d'algèbres.

2°) L'image de φ_a sera notée $\mathbb{K}[a]$.
Montrer que $\mathbb{K}[a]$ est une algèbre commutative et que $\mathbb{K}[a]$ est la plus petite sous-algèbre de A contenant a.

3°) Dans la $\mathbb{Q}$-algèbre $\mathbb{R}$, montrer que $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}/(a,b) \in \mathbb{Q}^2\}$.

4°) Pour toute la suite de cette partie, on suppose que $\mathrm{Ker}(\varphi_a) \neq \{0\}$.
Montrer qu'il existe un unique polynôme unitaire π_a dans $\mathbb{K}[X]$ tel que
$Ker(\varphi_a) = \pi_a\mathbb{K}[X]$. π_a est appelé le ***polynôme minimal*** de a.

5°) Dans la $\mathbb{Q}$-algèbre $\mathbb{R}$,
montrer que $\sqrt{2}$ possède un polynôme minimal puis déterminer $\pi_{\sqrt{2}}$.

6°) On note n le degré de π_a. Montrer que $(a^k)_{0\leq k\leq n-1}$ est une base de $\mathbb{K}[a]$.

7°) Montrer qu'un élément $P(a)$ de $\mathbb{K}[a]$ est inversible dans l'algèbre A si et seulement si P et π_a sont premiers entre eux et que dans ce cas, $P(a)$ est inversible dans l'algèbre $\mathbb{K}[a]$.

8°) Lorsque A est intègre, montrer que $\mathbb{K}[a]$ est un corps.

9°) Montrer que $\{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2/(a,b,c) \in \mathbb{Q}^3\}$ est un sous-corps de $\mathbb{R}$ et un $\mathbb{Q}$-espace vectoriel de dimension 3.

Partie II : Les matrices de Toeplitz

Dans $\mathcal{M}_n(\mathbb{C})$, on considère les deux matrices suivantes :

$$S = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{pmatrix} \quad \text{et} \quad Z = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ -1 & 0 & \cdots & \cdots & 0 \end{pmatrix}.$$

10°) Montrer que $\mathbb{C}[S]$ est l'ensemble des matrices $M = (m_{i,j})_{1 \leq i,j \leq n}$ telles que, pour tout $i, j, k, h \in \{1, \ldots, n\}$, $[i - j \equiv k - h \text{ modulo } n \Longrightarrow m_{i,j} = m_{k,h}]$.

11°) Montrer que $\mathbb{C}[S]$ est une algèbre commutative de dimension n.
Lorsque $M \in \mathbb{C}[S]$, donner une CNS portant sur les coefficients de M pour qu'elle soit inversible et montrer que dans ce cas, $M^{-1} \in \mathbb{C}[S]$.

12°) De manière analogue, décrire les matrices de $\mathbb{C}[Z]$ puis montrer que $\mathbb{C}[Z]$ est une algèbre commutative de dimension n et donner une CNS portant sur les coefficients de $M \in \mathbb{C}[Z]$ pour qu'elle soit inversible.

13°) On dit qu'une matrice $M = (m_{i,j})_{1 \leq i,j \leq n}$ de $\mathcal{M}_n(\mathbb{C})$ est une matrice de Toeplitz si et seulement si pour tout $i, j, k, h \in \{1, \ldots, n\}$, $i - j = k - h \Longrightarrow m_{i,j} = m_{k,h}$.
En notant T l'ensemble des matrices de Toeplitz, montrer que $T = \mathbb{C}[S] + \mathbb{C}[Z]$.

14°) Soit $M \in \mathcal{M}_n(\mathbb{C})$ et $\lambda \in \mathbb{C}$. On dit que λ est une valeur propre de M si et seulement si il existe $X \in \mathbb{C}^n$ avec $X \neq 0$ tel que $MX = \lambda X$. Dans ce cas, on dit que X est un vecteur propre de M pour la valeur propre λ.
Si X est un vecteur propre de M pour la valeur propre λ, montrer que, pour tout $P \in \mathbb{C}[X]$, X est un vecteur propre de $P(M)$ pour la valeur propre $P(\lambda)$.
Soit $P \in \mathbb{C}[X]$ tel que $P(M) = 0$. Montrer que les valeurs propres de M sont nécessairement des racines de P.

15°) Déterminer les valeurs propres et les vecteurs propres de S.

16°) On note P la matrice suivante de $\mathcal{M}_n(\mathbb{C})$: $P = \left(e^{2i\pi\frac{hk}{n}}\right)_{0 \leq h,k \leq n-1}$. On s'est permis de faire varier les indices de lignes et de colonnes de 0 à $n - 1$.
Montrer que $SP = PD$, où D est une matrice diagonale que l'on précisera.

17°) Montrer que P est une matrice inversible et que $P^{-1} = \frac{1}{n}\overline{P}$, où $\overline{P} = \left(e^{-2i\pi\frac{hk}{n}}\right)_{0 \leq h,k \leq n-1}$.

18°) Montrer que, pour tout $M \in \mathbb{C}[S]$, $P^{-1}MP$ est diagonale : on dit que les matrices de $\mathbb{C}[S]$ sont simultanément diagonalisables.

19°) On note R la matrice diagonale de $\mathcal{M}_n(\mathbb{C})$ suivante : $R = \left(e^{-i\pi\frac{h}{n}}\delta_{h,k}\right)_{0 \leq h,k \leq n-1}$.
Montrer que R est inversible et calculer RZR^{-1}.

20°) En déduire que les matrices de $\mathbb{C}[Z]$ sont simultanément diagonalisables.

Partie III : Irréductibilité dans $\mathbb{Q}[X]$

21°) Soit p un nombre premier. Pour tout $Q = \sum_{n\in\mathbb{N}} a_n X^n \in \mathbb{Z}[X]$, on pose $\overline{Q} = \sum_{n\in\mathbb{N}} \overline{a_n} X^n \in \mathbb{F}_p[X]$, où $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
Montrer que l'application $Q \longmapsto \overline{Q}$ est un morphisme d'anneaux.

22°) Lorsque $Q = \sum_{n\in\mathbb{N}} a_n X^n \in \mathbb{Z}[X]$, on note $c(Q)$ le pgcd de la famille $(a_n)_{n\in\mathbb{N}}$ des coefficients de Q. $c(Q)$ s'appelle le contenu du polynôme Q.
On dit que Q est primitif si et seulement si $c(Q) = 1$.
En utilisant le morphisme de la question précédente, montrer que le produit de deux polynômes primitifs de $\mathbb{Z}[X]$ est aussi un polynôme primitif. Il s'agit du lemme de Gauss.
En déduire le théorème de Gauss : pour tout $P, Q \in \mathbb{Z}[X]$, $c(PQ) = c(P)c(Q)$.

23°) Soit $P \in \mathbb{Z}[X]$ un polynôme de degré supérieur à 2 que l'on suppose réductible dans $\mathbb{Q}[X]$. Montrer qu'il existe $A, B \in \mathbb{Z}[X]$ tels que $P = AB$ avec $\deg(A) \geq 1$ et $\deg(B) \geq 1$.

24°) *Critère d'Eisenstein :* Soit $P \in \mathbb{Z}[X]$ un polynôme de degré $n \geq 1$. En notant $P = \sum_{k=0}^{n} a_k X^k$, on suppose qu'il existe un nombre premier p tel que p ne divise pas a_n, p divise $a_0, \ldots, a_{n-1}$ et p^2 ne divise pas a_0. Montrer que P est irréductible dans $\mathbb{Q}[X]$.
En déduire que, pour tout $n \in \mathbb{N}^*$, $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$.

25°) Soit $P \in \mathbb{Z}[X]$ un polynôme non nul et unitaire. Soit $A, B \in \mathbb{Q}[X]$ tels que $AB = P$ et A unitaire. Montrer que $A, B \in \mathbb{Z}[X]$.

26°) Pour tout $n \in \mathbb{N}^*$, on pose $\Phi_n = \prod_{\substack{1\leq k\leq n \\ k\wedge n=1}} (X - e^{2i\pi\frac{k}{n}})$: c'est le n-ième polynôme cyclotomique. Montrer que, pour tout $n \in \mathbb{N}^*$, $X^n - 1 = \prod_{\substack{1\leq d\leq n \\ d \mid n}} \Phi_d$.

27°) Montrer que pour tout $n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.

28°) Soit p un nombre premier. Montrer que l'application f_p, définie de $\mathbb{F}_p[X]$ dans lui-même par $f_p(A) = A^p$, est un endomorphisme d'algèbre (que l'on appelle l'endomorphisme de Frobenius). En déduire que, pour tout $h \in \mathbb{Z}[X]$, selon les notations de la question 21, $(\overline{h}(X))^p = \overline{h(X^p)}$.

29°) Jusqu'à la fin du problème, on fixe $n \in \mathbb{N}^*$ et on pose $\omega = e^{2i\frac{\pi}{n}}$.
Dans la $\mathbb{Q}$-algèbre $\mathbb{C}$, montrer que ω possède un polynôme minimal.
Montrer que $\pi_\omega \in \mathbb{Z}[X]$ et qu'il existe $h \in \mathbb{Z}[X]$ tel que $X^n - 1 = \pi_\omega(X)h(X)$.

30°) Soit p un nombre premier qui ne divise pas n et soit u une racine complexe de π_ω. On souhaite montrer que $\pi_\omega(u^p) = 0$. On raisonne par l'absurde en supposant que $\pi_\omega(u^p) \neq 0$.

a) Montrer que $h(u^p) = 0$ et en déduire l'existence de $g \in \mathbb{Z}[X]$ tel que $h(X^p) = \pi_\omega(X)g(X)$.

b) Dans $\mathbb{F}_p[X]$, considérons un facteur irréductible $P(X)$ de $\overline{\pi_\omega}$. Montrer qu'il existe $Q \in \mathbb{F}_p[X]$ tel que $\overline{X^n - 1} = P^2\, Q$.

c) En déduire que P est un polynôme constant et conclure.

31°) Montrer que, pour tout $k \in \{1, \dots, n\}$ tel que $k \wedge n = 1$, $\pi_\omega(\omega^k) = 0$.

32°) Montrer que Φ_n est irréductible dans $\mathbb{Q}[X]$.