

DM 30

Partie I: la sous-algèbre de $\mathbb{K}[a]$

1) $\mathbb{K}[x]$ et A sont bien des \mathbb{K} -algèbres. Soit $P, Q \in \mathbb{K}[x]$, $\lambda \in \mathbb{K}$.

$$\varphi_a(1_{\mathbb{K}[x]}) = 1_{\mathbb{K}[x]}(a) = a^0 = 1_A$$

$$\varphi_a(P+Q) = (P+Q)(a) \stackrel{NP}{=} P(a) + Q(a) = \varphi_a(P) + \varphi_a(Q)$$

$$\varphi_a(P \cdot Q) = (P \cdot Q)(a) \stackrel{NP}{=} P(a) \cdot Q(a) = \varphi_a(P) \varphi_a(Q)$$

$$\varphi_a(\lambda P) = (\lambda P)(a) = \lambda P(a) = \lambda \varphi_a(P)$$

Donc φ_a est bien un morphisme d'algèbres

2) Soit $a \in \mathbb{K}[a] = \text{Im}(\varphi_a) = \{P(a) / P \in \mathbb{K}[x]\}$

Soit $x, y \in \mathbb{K}[a]$, $\lambda \in \mathbb{K}$. Il existe $P, Q \in \mathbb{K}[x]$ tq $P(a) = x$, $Q(a) = y$.

On a bien $1_{\mathbb{K}[x]}(a) = a^0 = 1_A \in \mathbb{K}[a]$

IC $\lambda x + y = \lambda P(a) + Q(a) = (\lambda P + Q)(a) \in \mathbb{K}[a]$ car $\lambda P + Q \in \mathbb{K}[x]$ car $\mathbb{K}[x]$ algèbre

$$xy = P(a)Q(a) = (PQ)(a) \in \mathbb{K}[a]$$
 car $\mathbb{K}[x]$ algèbre

Donc $\mathbb{K}[a]$ est une sous-algèbre de A .

De plus $xy = P(a)Q(a) = (PQ)(a) = (QP)(a) = Q(a)P(a) = yx$

Donc $\mathbb{K}[a]$ est une algèbre commutative.

Soit B une sous-algèbre de A contenant a .

Soit $x \in \mathbb{K}[a]$. Il existe $P \in \mathbb{K}[x]$ tq $P(a) = x$. Notons $P(x) = \sum_{n \in \mathbb{N}} b_n x^n$, $b_n \in \mathbb{K}$

$x = P(a) = \sum_{n \in \mathbb{N}} b_n a^n$. Or $a \in B$ et B algèbre donc $a^n \in B$. De plus $\forall n \in \mathbb{N}$, $b_n \in \mathbb{K}$

et (b_n) est une famille non nulle donc on fait une somme finie

Donc $x = \sum_{n \in \mathbb{N}} b_n a^n \in B$ car B algèbre

Donc $\mathbb{K}[a] \subset B$.

$\Rightarrow \mathbb{K}[a] = B$

Donc $\mathbb{K}[a]$ est la plus petite sous-algèbre contenant a .

3) Soit $x \in \mathbb{Q}[\sqrt{2}]$. Il existe $P \in \mathbb{Q}[x]$ tq $P(\sqrt{2}) = x$

Il existe $(b_n) \in \mathbb{Q}^{\mathbb{N}}$ tq $P(x) = \sum_{n \in \mathbb{N}} b_n x^n$. $\forall k \in \mathbb{N}, \sqrt{2}^{2k} = 2^k$

$$\text{et } \sqrt{2}^{2b_1} = 2^k \sqrt{2}.$$

$$\text{Donc } x = P(\sqrt{2}) = \sum_{n \in \mathbb{N}} b_n \sqrt{2}^n = \sum_{n \in \mathbb{N}} b_{2n} 2^n + \sum_{n \in \mathbb{N}} b_{2n+1} 2^n \sqrt{2}$$

$$= \sum_{n \in \mathbb{N}} b_{2n} 2^n + \sqrt{2} \left(\sum_{n \in \mathbb{N}} b_{2n+1} 2^n \right)$$

Or $b_{2n} 2^n \in \mathbb{Q}$ et $b_{2n+1} 2^n \in \mathbb{Q}$
donc $x \in \{a + b\sqrt{2} / a, b \in \mathbb{Q}\}$

Soit $y \in \{a + b\sqrt{2} / a, b \in \mathbb{Q}\}$. Il existe $a, b \in \mathbb{Q}$ tq $y = a + b\sqrt{2}$.

avec le polynôme $P(X) = a + bX$, on a bien $y = P(\sqrt{2})$ avec $a, b \in \mathbb{Q}$
donc $y \in \mathbb{Q}[\sqrt{2}]$.

Donc $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} / a, b \in \mathbb{Q}\}$.

4) Soit $a \in I$. $\text{Id}_{\mathbb{K}}(\mathbb{Q}_a)$ est un idéal de l'anneau principal $\mathbb{K}[X]$

donc $\text{Id}_{\mathbb{K}}(\mathbb{Q}_a)$ est principal donc c'est l'idéal engendré par un polynôme Π

Il reste à montrer que tous les éléments qui engendrent $\text{Id}_{\mathbb{K}}(\mathbb{Q}_a)$ sont de la forme $\lambda \Pi_a$
avec $\lambda \in \mathbb{K}^*$, Π_a un polynôme unitaire

Soit $I = \{\Pi \in \mathbb{K}[X] / \Pi | \mathbb{K}[X] = \text{Id}_{\mathbb{K}}(\mathbb{Q}_a)\}, \Pi \in I$.

Soit $\lambda \in \mathbb{K}^*$. $\Pi_1 = \lambda \Pi \in I$ aussi

Réciprocement Soit $\Pi_1 \in I$. $\Pi_1 | \mathbb{K}[X] = \Pi | \mathbb{K}[X]$ donc il existe $\lambda \in \mathbb{K}^*$ tq
 $\Pi_1 = \lambda \Pi$. De fait les éléments de I se trouvent en les multipliant
par une constante non nulle. Donc s'ils sont unitaires, ils sont égaux.

Donc $\Pi_a \in I$ unitaire existe et est unique.

5) $\text{N}(a\mathbb{Q}_a \Pi = X^2 - 2 \in \mathbb{Q}[X])$. $\Pi | (\sqrt{2}) = 0$ donc $\Pi \in \text{Id}_{\mathbb{K}}(\mathbb{Q}_{\sqrt{2}})$ donc $\text{Id}_{\mathbb{K}}(\mathbb{Q}_{\sqrt{2}}) \neq \{0\}$.

Donc d'après 4) le polynôme minimal $\Pi_{\sqrt{2}}$ existe et est unique.

Montrons que $\Pi_{\sqrt{2}} = \Pi$ i.e. Π engendre $\text{Id}_{\mathbb{K}}(\mathbb{Q}_{\sqrt{2}})$ i.e. $\forall P \in \text{Id}_{\mathbb{K}}(\mathbb{Q}_{\sqrt{2}})$, il existe $Q \in \mathbb{K}[X]$
tq $P = \Pi Q$

Soit $P \in \text{Id}_{\mathbb{K}}(\mathbb{Q}_{\sqrt{2}})$. D'après la division euclidienne de P par Π , il
existe $Q, R \in \mathbb{K}[X]$, $d^o R < d^o \Pi$ tq $P = \Pi Q + R$. donc $d^o R < 2$

Si $d^o R = 0$, alors $R(\sqrt{2}) = P(\sqrt{2}) - (\Pi Q)(\sqrt{2}) = 0$ \exists

Si $d^o R = 1$, alors il existe $(a, b) \in \mathbb{Q}^* \times \mathbb{Q}$ tq $R = ax + b$. Donc

or $R(\sqrt{2}) = P(\sqrt{2}) - \Pi(\sqrt{2})Q(\sqrt{2}) = 0$ donc $a\sqrt{2} + b = 0$ donc $\sqrt{2} = -\frac{b}{a} \in \mathbb{Q}$

Donc $d^o R = 0$ donc $R = 0$, cqfd

Donc $\text{Id}_{\mathbb{K}}(\mathbb{Q}_{\sqrt{2}}) = (X^2 - 2)\mathbb{Q}[X]$ et $X^2 - 2$ unitaire, donc $\Pi_{\sqrt{2}} = (X^2 - 2)$.

6) Notons $f = (x_b)_{0 \leq b \leq n-1}$.

Soit $(x_b)_{0 \leq b \leq n-1}$. $\text{If } \sum_{b=0}^n x_b a^b = 0$, alors $P = \sum_{b=0}^{n-1} x_b a^b \in \ker \pi_a$

Or $d^\circ P = n-1 < d^\circ \pi_a$ donc $P = 0$ donc $(x_b)_{0 \leq b \leq n-1} = 0$. Donc f est libre.

Soit $x \in \mathbb{K}[a]$. Il existe $P \in \mathbb{K}[X]$ tq $P(a) = x$.

D'après la division euclidienne de P par π_a , il existe $Q, R \in \mathbb{K}[X]$,

$$d^\circ R < d^\circ \pi_a = n, \text{ tq } P = \pi_a Q + R$$

donc $P(a) = R(a) = x$, or $d^\circ R \leq n-1$ donc il existe $(x_b)_{0 \leq b \leq n-1}$

$$\text{tq } x = R(a) = \sum_{b=0}^{n-1} x_b a^b$$

Donc f est génératrice.

Donc f est une base.

libre?

7) Soit $P \in \mathbb{K}[X]$ tq $P(a)$ inversible dans A .

$$\text{Soit } R = P_1 \pi_a. \text{ If } d^\circ R \geq 1$$

Il existe $Q, Q' \in \mathbb{K}[X] \setminus \{0\}$ tq $P = QR, \pi_a = Q' R$

$$P(a) Q'(a) = (PQ')(a) = (QRQ')(a) = (Q \pi_a)(a) = Q(a) \pi_a(a) = 0 \text{ donc } Q'(a) = 0$$

et $P(a)$ inversible donc $Q'(a) = P(a)^{-1} Q(a) \pi_a(a) = 0$ donc $Q(a) = 0$

Or $d^\circ Q' < d^\circ \pi_a$ $d^\circ Q' \neq 0$ donc c'est impossible par définition de π_a

\rightarrow Réciproquement, $\text{If } d^\circ(P_1 \pi_a) \leq 0$. D'après Bezout il existe $U, V \in \mathbb{K}[X]$

$$\text{tq } UP + V \pi_a = 1 \text{ donc } U(a)P(a) + V(a)\pi_a(a) = 1 \text{ donc } U(a)P(a) = 1, \text{ or } U(a) \in \mathbb{K}[a]$$

donc $P(a)$ inversible dans $\mathbb{K}[a] \subset A$

8) $\text{If } A$ intègre

$\text{If } \pi_a$ irréductible. $\text{If } \pi_a$ réductible il existe $P, Q \in \mathbb{K}[X]$ tq $\pi_a = PQ$ et $d^\circ P < d^\circ \pi_a$

Alors $0 = \pi_a(a) = P(a)Q(a)$ et tant que $P(a)$ ou $Q(a)$ soit nul ce qui contredit la définition de π_a : suppose SPPG que $P(a) = 0$.

On a $d^\circ P < d^\circ \pi_a$ alors cela contredit la définition de π_a .

De plus $\mathbb{K}[a]$ est un anneau commutatif, non réduit à $\{0\}$ (question 2), donc $P(a) \in \mathbb{K}[a]$, vrai

alors $P \notin \pi_a(\mathbb{K}[X])$ de sorte que π_a irréductible de $P_1 \pi_a = 1$. D'après 7,

π_a inversible dans $\mathbb{K}[a]$

Donc $\mathbb{K}[a]$ est un corps

9) Soit $\alpha = \sqrt[3]{2}$. $\Pi = X^3 - 2$ annule α . $\text{D}\overset{\circ}{\text{m}} \Pi_\alpha = \Pi$.

On sait que $\Pi_\alpha \mid \Pi$. De $d(\Pi_\alpha)$ est $\{1, 2, 3\}$

$\text{D}\overset{\circ}{\text{m}} \Pi_\alpha < 3$. Alors il existe $P \in \mathbb{P}_q$ tel que $\Pi = P\Pi_\alpha$. Pour Π_α est de degré 1 donc

Il existe $\lambda \in \mathbb{Q}$. Donc $P(\lambda) = 0$. $\text{D}\overset{\circ}{\text{m}}$ P n'a pas de racines rationnelles

On a donc $P = (X-\alpha)(X-\bar{\alpha})(X-\bar{\alpha}^2)$. Or $\alpha \in \mathbb{Q}$.

Donc $\alpha = \frac{p}{q}$ irréductible. $\sqrt[3]{2} = \frac{p}{q}$, donc $q^3 \cdot 2 = p^3$ donc $q \mid p^3$ ou $q \nmid p$. donc

d'après Gauss $q \mid 1$ donc $p^3 = 2$ \Rightarrow

Donc $\Pi_\alpha = X^3 - 2$

Donc $(\mathbb{Q}[\alpha])$ est un corps de degré 3, \mathbb{Q} -engendré par $(1, \alpha, \alpha^2)$.

Donc $(\mathbb{Q}[\alpha]) = \{x + y\alpha + z\alpha^2 / x, y, z \in \mathbb{Q}\}$

Partie II : Les matrices de Toeplitz

Partie III : Réductibilité dans $\mathbb{Q}[x]$

21) Notons φ cette application

$$\varphi(1) = T = \mathbf{1}_{\mathbb{F}_p[x]}$$

Soient $P, Q \in \mathbb{Z}[x]$. Notons $P = \sum_{n \in \mathbb{N}} a_n x^n$, $Q = \sum_{n \in \mathbb{N}} b_n x^n$

$$\varphi(P+Q) = \varphi\left(\left(\sum_{n \in \mathbb{N}} (a_n + b_n)x^n\right)\right) = \overline{\left(\sum_{n \in \mathbb{N}} (a_n + b_n)\right)} X^n = \sum_{n \in \mathbb{N}} \overline{a_n} X^n + \sum_{n \in \mathbb{N}} \overline{b_n} X^n = \varphi(P) + \varphi(Q)$$

$$\begin{aligned} \varphi(PQ) &= \varphi\left(\left(\sum_{n \in \mathbb{N}} \left(\sum_{k=0}^n a_{n-k} b_k\right) x^n\right)\right) = \overline{\left(\sum_{n \in \mathbb{N}} \left(\sum_{k=0}^n a_{n-k} b_k\right)\right)} X^n = \sum_{n \in \mathbb{N}} \overline{\left(\sum_{k=0}^n a_{n-k} b_k\right)} X^n \\ &= \varphi(P) \varphi(Q) \end{aligned}$$

Donc φ est bien un morphisme d'algèbres

22) Soient P, Q 2 polynômes premiers de $\mathbb{Z}[x]$

$\text{D}\overset{\circ}{\text{m}} P \text{ et } Q \text{ n'est pas premier}$.

Il existe donc $p \in \mathbb{P}$ tq p divise les coeffs de P et Q

Donc $\text{D}\overset{\circ}{\text{m}} P \text{ et } Q = \overline{PQ} = \overline{P}\overline{Q}$ et $\overline{\mathbb{F}_p[x]}$ intègre donc \overline{P} et \overline{Q} est nul.

Donc p divise soit les coeffs de P soit Q donc au moins 1 des 2 n'est pas premier \Leftrightarrow

Soit $P, Q \in \mathbb{Z}[x]$

Il existe $P' \in \mathbb{Z}[x]$ tq $P = c(P)P'$ avec P' un polynôme premier de $\mathbb{Z}[x]$

$P=0$ ou $Q=0$?

Il existe $Q' \in \mathbb{Z}[x]$ tq $Q = c(Q)Q'$ avec Q' premier de $\mathbb{Z}[x]$

$$c(PQ) = c(c(P)P' c(Q)Q') = c(P)c(Q)c(P'Q')$$
 car le produit est distributif par rapport au pgcd. De plus $P'Q'$ premier donc $c(PQ) = c(P)c(Q)$

23) Soit $P \in \mathbb{Z}[x]$ tq $d \circ P \geq 2$ et P réductible dans $\mathbb{Q}[x]$

Il existe donc $A, B \in \mathbb{Q}[x]$ tq $P = AB$ et $d \circ A \geq 1$, $d \circ B \geq 1$

notons a le ppcm des coeffs de A . Il existe A' tq $A = \frac{1}{a}A'$.