

## DM 30 : corrigé.

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

1°) •  $\varphi_a(1) = \varphi_a(X^0) = a^0 = 1_A$ .

• Soient  $P = \sum_{n \in \mathbb{N}} b_n X^n \in \mathbb{K}[X]$ ,  $Q = \sum_{n \in \mathbb{N}} c_n X^n \in \mathbb{K}[X]$  et  $\alpha \in \mathbb{K}$ .

$$\begin{aligned} \diamond \quad \varphi_a(\alpha P) &= \left( \sum_{n \in \mathbb{N}} (\alpha b_n) X^n \right) (a) = \sum_{n \in \mathbb{N}} (\alpha b_n) a^n \\ &= \alpha \sum_{n \in \mathbb{N}} b_n a^n = \alpha \varphi_a(P). \end{aligned}$$

$$\diamond \quad \varphi_a(P + Q) = \left( \sum_{n \in \mathbb{N}} (b_n + c_n) X^n \right) (a) = \sum_{n \in \mathbb{N}} (b_n + c_n) a^n = \varphi_a(P) + \varphi_a(Q).$$

$$\diamond \quad \varphi_a(PQ) = \left( \sum_{n \in \mathbb{N}} \left( \sum_{k=0}^n (b_{n-k} c_k) \right) X^n \right) (a) = \sum_{n \in \mathbb{N}} \left( \sum_{k=0}^n (b_{n-k} c_k) \right) a^n = \varphi_a(P) \varphi_a(Q), \text{ d'après}$$

les règles de calculs dans l'algèbre  $A$ .

2°)  $\diamond$  L'image d'une algèbre commutative par un morphisme d'algèbres est une sous-algèbre commutative de l'algèbre d'arrivée, donc  $\mathbb{K}[a]$  est une sous-algèbre commutative de  $A$ .

$\diamond$  Lorsque  $P = X$ ,  $P(a) = a$ , donc  $a \in \mathbb{K}[a]$ .

Soit  $B$  une sous-algèbre de  $A$  contenant  $a$ .

Soit  $P \in \mathbb{K}[X]$ .  $a \in B$  et  $B$  est stable pour les trois lois qui structurent  $A$  comme une algèbre, donc  $P(a) \in B$ . Ainsi  $\mathbb{K}[a] \subset B$ .

Ainsi, on a prouvé que  $\mathbb{K}[a]$  est la plus petite sous-algèbre de  $A$  contenant  $a$ .

3°) Soit  $(a, b) \in \mathbb{Q}^2$ .  $a + b\sqrt{2} = P(\sqrt{2})$  si l'on pose  $P(X) = a + bX$ , donc  $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ .

Réciproquement, soit  $x \in \mathbb{Q}[\sqrt{2}]$ . Il existe  $P = \sum_{n \in \mathbb{N}} b_n X^n \in \mathbb{Q}[X]$  tel que  $x = P(\sqrt{2})$ .

Ainsi  $x = \sum_{n \in \mathbb{N}} b_{2n} 2^n + \sqrt{2} \sum_{n \in \mathbb{N}} b_{2n+1} 2^n$ , ce qui prouve l'inclusion réciproque.

4°)  $\varphi_a$  est un morphisme d'anneaux, donc d'après le cours, son noyau est un idéal de  $\mathbb{K}[X]$ , or ce dernier est principal, donc il existe  $\pi_a \in \mathbb{K}[X]$  tel que  $\text{Ker}(\varphi_a) = \pi_a \mathbb{K}[X]$ .  $\text{Ker}(\varphi_a) \neq \{0\}$ , donc  $\pi_a \neq 0$ . Quitte à le diviser par son coefficient dominant, on peut imposer que  $\pi_a$  soit unitaire.

Pour démontrer l'unicité, supposons qu'il existe  $P \in \mathbb{K}[X]$ , unitaire, tel que  $\text{Ker}(\varphi_a) = P\mathbb{K}[X]$ . Alors  $P$  et  $\pi_a$  sont associés, or ils sont unitaires, donc ils sont égaux.

5°) Le polynôme  $X^2 - 2$  est dans  $\mathbb{Q}[X]$  et il annule  $\sqrt{2}$ , donc  $\sqrt{2}$  admet un polynôme minimal.

$\pi_{\sqrt{2}}|(X^2 - 2)$ . De plus,  $\pi_{\sqrt{2}}$  ne peut être de degré 1, sans quoi il existerait  $\alpha \in \mathbb{Q}$  tel que  $0 = (X - \alpha)(\sqrt{2}) = \sqrt{2} - \alpha$ , et  $\sqrt{2}$  serait rationnel ce qui est faux (la démonstration de l'irrationalité de  $\sqrt{2}$  est analogue à celle que nous développerons pour  $\sqrt[3]{2}$  en question 9). Ainsi  $\pi_{\sqrt{2}}$  est un polynôme unitaire de degré au moins 2 et il divise  $X^2 - 2$ . Cela prouve que  $\pi_{\sqrt{2}} = X^2 - 2$ .

6°)  $\diamond$  Soit  $x \in \mathbb{K}[a]$ . Il existe  $P \in \mathbb{K}[X]$  tel que  $x = P(a)$ . Effectuons la division euclidienne de  $P$  par  $\pi_a$ . Il existe  $(Q, R) \in \mathbb{K}[X]^2$  tel que  $P = Q\pi_a + R$  avec  $\deg(R) < n$ . Alors  $x = P(a) = Q(a)\pi_a(a) + R(a) = R(a) \in \text{Vect}(1_A, a, a^2, \dots, a^{n-1})$ , donc  $\mathbb{K}[a] \subset \text{Vect}(1_A, a, a^2, \dots, a^{n-1})$ . Ainsi  $(1_A, a, a^2, \dots, a^{n-1})$  est un système générateur de  $\mathbb{K}[a]$ .

$\diamond$  Soit  $(\alpha_j)_{0 \leq j \leq n-1} \in \mathbb{K}^n$  tel que  $\sum_{j=0}^{n-1} \alpha_j a^j = 0$ . Ainsi le polynôme  $\sum_{j=0}^{n-1} \alpha_j X^j$  annule  $a$ . Or il est de degré strictement inférieur au degré du polynôme minimal, donc ce polynôme est nul. La famille  $(\alpha_j)_{0 \leq j \leq n-1}$  est donc nulle, ce qui prouve que  $(1_A, a, a^2, \dots, a^{n-1})$  est une famille libre. C'est donc une base de  $\mathbb{K}[a]$ .

7°)  $\diamond$  Soit  $P \in \mathbb{K}[X]$  tel que  $P(a)$  est inversible dans  $A$ .

Supposons que  $P$  n'est pas premier avec  $\pi_a$ .

Notons  $R = P \wedge \pi_a$  : par hypothèse,  $\deg(R) \geq 1$  ( $\pi_a \neq 0$ , donc  $R \neq 0$ ). il existe  $Q_1, Q_2 \in \mathbb{K}[X]$  tels que  $P = RQ_1$  et  $\pi_a = RQ_2$ .

On a  $P(a)Q_2(a) = (PQ_2)(a) = (RQ_1Q_2)(a) = (\pi_a Q_1)(a) = 0$ , mais  $P(a)$  est inversible dans  $A$ , donc  $Q_2(a) = [P(a)]^{-1}(P(a)Q_2(a)) = 0$ . C'est impossible car  $Q_2 \neq 0$  et  $\deg(Q_2) < \deg(\pi_a)$ . Ainsi  $P$  est premier avec  $\pi_a$ .

$\diamond$  Réciproquement, supposons que  $P$  est premier avec  $\pi_a$ . D'après l'identité de Bezout, il existe  $U, V \in \mathbb{K}[X]$  tel que  $UP + V\pi_a = 1_{\mathbb{K}}$ , donc  $U(a)P(a) + V(a)\pi_a(a) = 1_A$ , puis  $U(a)P(a) = 1$ . Ainsi,  $P(a)$  est inversible dans  $A$  et son inverse  $U(a)$  est dans  $\mathbb{K}[a]$ , donc  $P(a)$  est même inversible dans  $\mathbb{K}[a]$ .

8°) On suppose que  $A$  est une algèbre intègre.

$\diamond$  Montrons qu'alors  $\pi_a$  est irréductible dans  $\mathbb{K}[X]$  : soit  $(P, Q) \in \mathbb{K}[X]^2$  tel que  $\pi_a = PQ$ .  $P(a)Q(a) = (PQ)(a) = \pi_a(a) = 0$ . Or  $A$  est intègre, donc  $P(a) = 0$  ou  $Q(a) = 0$ .

Si  $P(a) = 0$ ,  $P \in \pi_a \mathbb{K}[X]$ , donc  $\pi_a | P$ , or  $P | \pi_a$ . Ainsi, si  $P(a) = 0$ ,  $P$  est associé à  $\pi_a$ , ce qui entraîne que  $Q$  est inversible. Donc les seuls diviseurs de  $\pi_a$  sont les polynômes inversibles et les polynômes associés à  $\pi_a$ .

Ceci montre que  $\pi_a$  est irréductible dans  $\mathbb{K}[X]$ .

$\diamond$   $\mathbb{K}[a]$  est un anneau commutatif non réduit à  $\{0\}$  et si  $P(a) \in \mathbb{K}[a] \setminus \{0\}$ ,  $\pi_a$  ne divise pas  $P$ , or  $\pi_a$  est irréductible, donc d'après le cours,  $\pi_a \wedge P = 1$ , puis d'après la question précédente,  $P(a)$  est inversible dans  $\mathbb{K}[a]$ . Ainsi  $\mathbb{K}[a]$  est un corps.

9°)  $\diamond$  Posons  $a = \sqrt[3]{2}$ .  $a$  est annulé par le polynôme  $X^3 - 2 \in \mathbb{Q}[X]$ , donc  $\pi_a$  est défini et c'est un diviseur dans  $\mathbb{Q}[X]$  de  $X^3 - 2$ .

Supposons que  $\deg(\pi_a) < 3$ . Alors  $\deg(\pi_a) \in \{1, 2\}$  et il existe  $P \in \mathbb{Q}[X]$  tel que  $X^3 - 2 = P\pi_a$ . Nécessairement,  $P$  ou  $\pi_a$  est de degré 1, donc possède une racine dans  $\mathbb{Q}$ . Ainsi l'une des racines complexes de  $X^3 - 2$  est rationnelle. Or ces racines sont  $a, ja$  et  $j^2a$ , donc  $a \in \mathbb{Q}$  : il existe  $p \in \mathbb{Z}, q \in \mathbb{N}^*$  tel que  $a = \frac{p}{q}$  et  $p \wedge q = 1$ . Alors  $2q^3 = p^3$ , donc  $q \mid p^3$  puis d'après le théorème de Gauss,  $q \mid 1$ . Alors  $q = 1$ , puis  $p^3 = 2$ , ce qui est impossible avec  $p \in \mathbb{N}^*$ . On en déduit que  $\deg(\pi_a) = 3$  et que  $\pi_a = X^3 - 2$ .

$\diamond$  D'après les questions précédentes, on sait alors que  $\mathbb{Q}[a]$  est un corps (car  $\mathbb{R}$  est intègre) de dimension 3 en tant que  $\mathbb{Q}$ -espace vectoriel (car  $\deg(\pi_a) = 3$ ), dont une base est  $(1, a, a^2)$ , donc  $\mathbb{Q}[a] = \{\alpha + \beta a + \gamma a^2 \mid \alpha, \beta, \gamma \in \mathbb{Q}\}$ .

## Partie II : Les matrices de Toeplitz

10°) **Notation** : Soit  $M \in \mathcal{M}_n(\mathbb{C})$  et  $k \in [1 - n, n - 1] \cap \mathbb{Z}$  : désignons par “ $k$ -ième diagonale de  $M$ ” la liste des coefficients  $M_{i,j}$  de  $M$  tels que  $i - j = k$ . Notons  $D_k(M)$  l'ensemble des éléments de la  $k$ -ième diagonale de  $M$ , c'est-à-dire

$$D_k(M) = \{M_{i,i+k} \mid \max\{1, 1-k\} \leq i \leq \min\{n, n-k\}\}.$$

Ainsi,  $D_{1-n}(M) = \{M_{n,1}\}$ ,  $D_{2-n}(M) = \{M_{n-1,1}, M_{n,2}\}, \dots$ ,

$D_{-1}(M) = \{M_{2,1}, M_{3,2}, \dots, M_{n,n-1}\}$ ,  $D_0(M) = \{M_{1,1}, \dots, M_{n,n}\}$ , puis

$D_1(M) = \{M_{1,2}, M_{2,3}, \dots, M_{n-1,n}\}, \dots, D_{n-1}(M) = \{M_{1,n}\}$ .

$\diamond$  Notons  $TC$  l'ensemble des matrices  $M = (m_{i,j})_{1 \leq i,j \leq n}$  telles que, pour tout  $i, j, k, h \in \{1, \dots, n\}$ ,  $[i - j \equiv k - h \text{ modulo } n \implies m_{i,j} = m_{k,h}]$ .

Alors  $M \in TC$  si et seulement si il existe  $d_0, \dots, d_{n-1} \in \mathbb{C}^n$  tels que  $D_0 = \{d_0\}$ ,

$D_1 = D_{1-n} = \{d_1\}$ ,  $D_2 = D_{2-n} = \{d_2\}, \dots, D_{n-1} = D_{-1} = \{d_{n-1}\}$ , ou encore si et

$$\text{seulement si } M \text{ est de la forme } M = \begin{pmatrix} d_0 & d_1 & \cdots & d_{n-1} \\ d_{n-1} & d_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & d_1 \\ d_1 & \cdots & d_{n-1} & d_0 \end{pmatrix}.$$

$\diamond$  Notons  $c = (c_1, \dots, c_n)$  la base canonique de  $\mathbb{C}^n$  et identifions  $S$  avec son endomorphisme canoniquement associé. Pour tout  $i \in \mathbb{N}_n$ ,  $Sc_i$  est égal à la  $i$ -ème colonne de  $S$ , donc  $Sc_i = c_{i-1}$ , en convenant que, pour tout  $k \in \mathbb{Z}$ , si  $i \in \mathbb{N}_n$  avec  $k \equiv i \text{ modulo } n$ , alors  $c_k = c_i$ .

Par récurrence sur  $k \in \mathbb{N}$ , on en déduit que pour tout  $i \in \mathbb{N}_n$ ,  $S^k c_i = c_{i-k}$ , donc pour tout  $k \in \{0, \dots, n-1\}$ ,  $S^k$  admet l'écriture par blocs :  $S^k = \begin{pmatrix} 0 & I_{n-k} \\ I_k & 0 \end{pmatrix}$ , où les 0 désignent des matrices nulles de dimensions convenables.

$$\text{Ainsi, lorsque } d_0, \dots, d_{n-1} \in \mathbb{C}^n, \begin{pmatrix} d_0 & d_1 & \cdots & d_{n-1} \\ d_{n-1} & d_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & d_1 \\ d_1 & \cdots & d_{n-1} & d_0 \end{pmatrix} = \sum_{k=0}^{n-1} d_k S^k \quad (1).$$

Ceci démontre que  $TC = \text{Vect}(S^0, S^1, \dots, S^{n-1})$ .

Ainsi,  $TC \subset \mathbb{C}[S]$ . De plus,  $S^n = I_n$ , donc si  $k \in \mathbb{N}$  avec  $k \equiv h \text{ modulo } n$  où  $h \in \{0, \dots, n-1\}$ ,  $S^k = S^h = \begin{pmatrix} 0 & I_{n-h} \\ I_h & 0 \end{pmatrix} \in TC$ . Ainsi,  $\mathbb{C}[S] \subset TC$ .

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

**11°)**  $\diamond$  De plus  $(S^0, S^1, \dots, S^{n-1})$  est une famille libre, car si  $\sum_{k=0}^{n-1} d_k S^k = 0$ , alors

$$\begin{pmatrix} d_0 & d_1 & \cdots & d_{n-1} \\ d_{n-1} & d_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & d_1 \\ d_1 & \cdots & d_{n-1} & d_0 \end{pmatrix} = 0, \text{ donc } (d_0, \dots, d_{n-1}) = 0.$$

Ainsi,  $(S^0, S^1, \dots, S^{n-1})$  est une base de  $\mathbb{C}[S]$ .

D'après la question 2,  $\mathbb{C}[S]$  est une algèbre commutative de dimension  $n$ .

$\diamond$   $S$  est annulée par le polynôme  $X^n - 1$  et  $\deg(\pi_S) = \dim(\mathbb{C}[S]) = n$ , donc  $\pi_S = X^n - 1$ . Si  $M = P(S) \in \mathbb{C}[S]$ , d'après la question 7,  $M$  est inversible si et seulement si  $P \wedge (X^n - 1) = 1$  et dans ce cas,  $M^{-1} \in \mathbb{C}[S]$ . Or  $P \wedge (X^n - 1) = 1$  si et seulement si aucune racine complexe de  $X^n - 1$  n'est racine de  $P$ .

D'après la relation (1), les coefficients de  $P$  sont les coefficients de la première ligne de  $M$ , donc  $M$  est inversible si et seulement si

$$\text{pour tout } k \in \{0, \dots, n-1\}, \sum_{j=1}^n M_{1,j} e^{2i\pi \frac{k(j-1)}{n}} \neq 0.$$

**12°)**  $\diamond$  Notons  $TAC$  l'ensemble des matrices  $M = (m_{i,j})_{1 \leq i,j \leq n}$  telles que, pour tout  $i, j, k, h \in \{1, \dots, n\}$ ,  $[i - j = k - h \implies m_{i,j} = m_{k,h}]$  et  $[i - j = k - h - n \implies m_{i,j} = -m_{k,h}]$ . Alors  $M \in TAC$  si et seulement si il existe  $d_0, \dots, d_{n-1} \in \mathbb{C}^n$  tels que  $D_0 = \{d_0\}$ ,  $D_1 = \{d_1\}$  et  $D_{1-n} = \{-d_1\}$ ,  $D_2 = \{d_2\}$  et  $D_{2-n} = \{-d_2\}$ , ...,  $D_{n-1} = \{d_{n-1}\}$  et  $D_{-1} = \{-d_{n-1}\}$ , ou encore si et seulement si  $M$

$$\text{est de la forme } M = \begin{pmatrix} d_0 & d_1 & \cdots & d_{n-1} \\ -d_{n-1} & d_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & d_1 \\ -d_1 & \cdots & -d_{n-1} & d_0 \end{pmatrix}.$$

$\diamond$   $Zc_1 = -c_n$  et pour tout  $i \in \{2, \dots, n\}$ ,  $Zc_i = c_{i-1}$ .

Par récurrence sur  $k \in \{0, \dots, n\}$ , on en déduit que

pour tout  $i \in \{1, \dots, k\}$ ,  $Z^k c_i = -c_{n+i-k}$ , et pour tout  $i \in \{k+1, \dots, n\}$ ,  $Z^k c_i = c_{i-k}$ .

Ainsi, pour tout  $k \in \{0, \dots, n\}$ ,  $Z^k$  admet l'écriture par blocs :  $Z^k = \begin{pmatrix} 0 & I_{n-k} \\ -I_k & 0 \end{pmatrix}$ .

$$\text{Ainsi, lorsque } d_0, \dots, d_{n-1} \in \mathbb{C}^n, \begin{pmatrix} d_0 & d_1 & \cdots & d_{n-1} \\ -d_{n-1} & d_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & d_1 \\ -d_1 & \cdots & -d_{n-1} & d_0 \end{pmatrix} = \sum_{k=0}^{n-1} d_k Z^k : (2).$$

Ceci démontre que  $TAC = \text{Vect}(Z^0, Z^1, \dots, Z^{n-1})$ .

Ainsi,  $TAC \subset \mathbb{C}[Z]$ . De plus,  $Z^n = -I_n$ , donc si  $k \in \mathbb{N}$  avec  $k \equiv h \pmod{n}$  où  $h \in \{0, \dots, n-1\}$ ,  $Z^k \in \{Z^h, -Z^h\} \subset TAC$ . Ainsi,  $\mathbb{C}[Z] \subset TAC$ .  
Donc  $\mathbb{C}[Z]$  est l'ensemble des matrices  $M = (m_{i,j})_{1 \leq i,j \leq n}$  telles que, pour tout  $i, j, k, h \in \{1, \dots, n\}$ ,  $[i - j = k - h \implies m_{i,j} = m_{k,h}]$  et  $[i - j = k - h - n \implies m_{i,j} = -m_{k,h}]$ .

◇ De plus  $(Z^0, Z^1, \dots, Z^{n-1})$  est une famille libre, car si  $\sum_{k=0}^{n-1} d_k Z^k = 0$ ,

$$\text{alors } \begin{pmatrix} d_0 & d_1 & \cdots & d_{n-1} \\ -d_{n-1} & d_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & d_1 \\ -d_1 & \cdots & -d_{n-1} & d_0 \end{pmatrix} = 0, \text{ donc } (d_0, \dots, d_{n-1}) = 0.$$

Ainsi,  $(Z^0, Z^1, \dots, Z^{n-1})$  est une base de  $\mathbb{C}[Z]$ .

D'après la question 2,  $\mathbb{C}[Z]$  est une algèbre commutative de dimension  $n$ .

◇  $Z$  est annulée par le polynôme  $X^n + 1$  et  $\deg(\pi_Z) = \dim(\mathbb{C}[Z]) = n$ , donc  $\pi_S = X^n + 1$ .

Si  $M = P(Z) \in \mathbb{C}[Z]$ , d'après la question 7,  $M$  est inversible si et seulement si  $P \wedge (X^n + 1) = 1$  et dans ce cas,  $M^{-1} \in \mathbb{C}[Z]$ . Or  $P \wedge (X^n + 1) = 1$  si et seulement si aucune racine complexe de  $P$  n'est racine de  $X^n + 1$ , c'est-à-dire n'est égale à  $e^{i\pi \frac{2k+1}{n}}$ , avec  $k \in \{0, \dots, n-1\}$ . D'après la relation (2), les coefficients de  $P$  sont les coefficients de la première ligne de  $M$ , donc  $M$  est inversible si et seulement si

pour tout  $k \in \{0, \dots, n-1\}$ ,  $\sum_{j=1}^n M_{1,j} e^{i\pi \frac{(2k+1)(j-1)}{n}} \neq 0$ .

$$\mathbf{13^\circ)} \quad M \in T \text{ si et seulement si } M \text{ est de la forme } M = \begin{pmatrix} d_0 & d_1 & \cdots & d_{n-1} \\ c_{n-1} & d_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & d_1 \\ c_1 & \cdots & c_{n-1} & d_0 \end{pmatrix},$$

où  $\{c_1, \dots, c_{n-1}, d_0, \dots, d_{n-1}\} \subset \mathbb{C}$ .

Ainsi,  $T$  est non vide et stable par combinaison linéaire, donc c'est un sous-espace vectoriel de  $\mathcal{M}_n(\mathbb{C})$ .

Clairement  $TC \subset T$  et  $TAC \subset T$ , donc  $TC + TAC \subset T$ .

$$\text{Soit } M = \begin{pmatrix} d_0 & d_1 & \cdots & d_{n-1} \\ c_{n-1} & d_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & d_1 \\ c_1 & \cdots & c_{n-1} & d_0 \end{pmatrix} \in T. \text{ Alors}$$

$$M = \begin{pmatrix} d_0 & \frac{c_1+d_1}{2} & \dots & \frac{c_{n-1}+d_{n-1}}{2} \\ \frac{c_{n-1}+d_{n-1}}{2} & d_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \frac{c_1+d_1}{2} \\ \frac{c_1+d_1}{2} & \dots & \frac{c_{n-1}+d_{n-1}}{2} & d_0 \end{pmatrix} + \begin{pmatrix} 0 & \frac{-c_1+d_1}{2} & \dots & \frac{-c_{n-1}+d_{n-1}}{2} \\ \frac{c_{n-1}-d_{n-1}}{2} & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \frac{-c_1+d_1}{2} \\ \frac{c_1-d_1}{2} & \dots & \frac{c_{n-1}-d_{n-1}}{2} & 0 \end{pmatrix},$$

donc  $M \in TC + {}^2TAC$ .

En conclusion  $T = TC + TAC = \mathbb{C}[S] + \mathbb{C}[Z]$ .

**14°)**  $\diamond$  Supposons que  $X$  est un vecteur propre de  $M$  pour la valeur propre  $\lambda$ .

Soit  $k \in \mathbb{N}$ . Si  $M^k X = \lambda^k X$ , alors  $M^{k+1} X = \lambda^k M X = \lambda^{k+1} X$ , donc d'après le principe de récurrence, pour tout  $k \in \mathbb{N}$ ,  $M^k X = \lambda^k X$ .

Soit  $P = \sum_{k \in \mathbb{N}} p_k Y^k \in \mathbb{K}[Y]$ . Alors  $P(M)X = \sum_{k \in \mathbb{N}} p_k M^k X = \sum_{k \in \mathbb{N}} p_k \lambda^k X = P(\lambda)X$ , or

$X \neq 0$ , donc  $X$  est un vecteur propre de  $P(M)$  pour la valeur propre  $P(\lambda)$ .

$\diamond$  Supposons de plus que  $P(M) = 0$ . Alors  $P(\lambda)X = P(M)X = 0$ , or  $X \neq 0$ , donc  $P(\lambda) = 0$  : les valeurs propres de  $M$  sont nécessairement des racines de  $P$ .

**15°)**  $S$  est annulée par  $X^n - 1$ , donc les valeurs propres de  $M$  sont nécessairement de la forme  $\omega^k$ , ou  $\omega = e^{\frac{2i\pi}{n}}$  et  $k \in \{0, \dots, n-1\}$ .

Soit  $k \in \{0, \dots, n-1\}$  et  $X = \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} \in \mathbb{C}^n \setminus \{0\}$ .

$$\begin{aligned} SX = \omega^k X &\iff [\forall i \in \{0, \dots, n-2\}, x_{i+1} = \omega^k x_i] \wedge x_0 = \omega^k x_{n-1} \\ &\iff [\forall i \in \{0, \dots, n-1\}, x_i = \omega^{ik} x_0] \wedge x_0 = \omega^k \omega^{k(n-1)} x_0 \\ &\iff [\forall i \in \{0, \dots, n-1\}, x_i = \omega^{ik} x_0], \end{aligned}$$

donc  $SX = \omega^k X \iff X \in \text{Vect} \begin{pmatrix} 1 \\ \omega^k \\ \vdots \\ \omega^{k(n-1)} \end{pmatrix}$ . Ceci montre que les valeurs propres de

$M$  sont exactement les racines  $n$ -ièmes de l'unité et que, pour tout  $k \in \{0, \dots, n-1\}$ , les vecteurs propres associés à la valeur propre  $\omega^k$  sont exactement les vecteurs non nuls de la droite vectorielle engendrée par le vecteur colonne  $(\omega^{kh})_{0 \leq h \leq n-1}$ .

**16°)** Si l'on note  $P_0, \dots, P_{n-1}$  les colonnes de  $P$ , la question précédente indique que, pour tout  $k \in \{0, \dots, n-1\}$ ,  $SP_k = \omega^k P_k$ , donc les colonnes de  $SP$  sont  $P_0, \omega P_1, \dots, \omega^{n-1} P_{n-1}$ .

Notons  $D$  la matrice diagonale dont les coefficients diagonaux sont  $1, \omega, \omega^2, \dots, \omega^{n-1}$ . D'après le cours, la  $k$ -ème colonne de  $PD$  est la combinaison linéaire des colonnes de  $P$ , affectée des coefficients de la  $k$ -ème colonne de  $D$ , donc cette  $k$ -ème colonne est égale à  $\omega^k P_k$ . Ainsi,  $SP = PD$ .

17°) Soit  $h, k \in \{0, \dots, n-1\}$ . Alors

$$[\overline{P}P]_{h,k} = \sum_{\ell=0}^{n-1} \overline{P}_{h,\ell} P_{\ell,k} = \sum_{\ell=0}^{n-1} e^{2i\pi \frac{k\ell-h\ell}{n}} = \sum_{\ell=0}^{n-1} \left( e^{2i\pi \frac{k-h}{n}} \right)^\ell.$$

Si  $h = k$ , alors  $[\overline{P}P]_{h,k} = n$  et si  $h \neq k$ , alors  $|2\pi \frac{k-h}{n}| \in ]0, 2\pi[$ , donc  $e^{2i\pi \frac{k-h}{n}} \neq 1$ .

$$\text{Alors } [\overline{P}P]_{h,k} = \frac{1 - \left( e^{2i\pi \frac{k-h}{n}} \right)^n}{1 - e^{2i\pi \frac{k-h}{n}}} = 0, \text{ donc } \overline{P}P = nI_n.$$

De même on montre que  $P\overline{P} = nI_n$ , donc  $P$  est inversible et  $P^{-1} = \frac{1}{n}\overline{P}$ .

18°) D'après la question 16,  $SP = PD$ , donc  $P^{-1}SP = D$ .

Soit  $k \in \mathbb{N}$ . Si  $P^{-1}S^kP = D^k$ , alors  $P^{-1}S^{k+1}P = P^{-1}S^kPP^{-1}SP = D^{k+1}$ , donc d'après le principe de récurrence, pour tout  $k \in \mathbb{N}$ ,  $P^{-1}S^kP = D^k$ .

Soit  $M \in \mathbb{C}[S]$ . Il existe  $Q = \sum_{k \in \mathbb{N}} q_k Y^k \in \mathbb{K}[Y]$  tel que  $M = Q(S)$ .

Alors  $P^{-1}MP = \sum_{k \in \mathbb{N}} q_k P^{-1}S^kP = \sum_{k \in \mathbb{N}} q_k D^k$  : c'est bien une matrice diagonale.

19°) Notons  $R'$  la matrice diagonale de  $\mathcal{M}_n(\mathbb{C})$  suivante :  $R' = \left( e^{i\pi \frac{h}{n}} \delta_{h,k} \right)_{0 \leq h, k \leq n-1}$ .

Alors  $RR' = R'R = I_n$ , donc  $R$  est inversible et  $R^{-1} = R'$ .

Notons  $(c_0, \dots, c_{n-1})$  la base canonique de  $\mathbb{C}^n$ .

Soit  $j \in \{1, \dots, n-1\}$ . Alors  $RZR^{-1}c_j = RZ \left( e^{i\pi \frac{j}{n}} c_j \right) = e^{i\pi \frac{j}{n}} Rc_{j-1} = e^{i\pi \frac{j}{n}} e^{-i\pi \frac{j-1}{n}} c_{j-1}$ , donc  $RZR^{-1}c_j = e^{i\pi \frac{j}{n}} c_{j-1}$ .

De plus,  $RZR^{-1}c_0 = RZc_0 = -Rc_{n-1} = -e^{-i\pi \frac{n-1}{n}} c_{n-1} = e^{i\pi \frac{n}{n}} c_{n-1}$ .

Ainsi, pour tout  $j \in \{0, \dots, n-1\}$ ,  $RZR^{-1}c_j = e^{i\pi \frac{j}{n}} Sc_j$ , donc  $RZR^{-1} = e^{i\pi \frac{1}{n}} S$ .

20°) Posons  $P' = R^{-1}P$  :  $P'^{-1}ZP' = P^{-1}(RZR^{-1})P = e^{i\pi \frac{1}{n}} P^{-1}SP = e^{i\pi \frac{1}{n}} D$ .

En adaptant la solution de la question 18, on en déduit que, pour tout  $k \in \mathbb{N}$ ,  $P'^{-1}Z^kP' = e^{i\pi \frac{k}{n}} D^k$ , puis que pour  $Q \in \mathbb{C}[Y]$ ,  $P'^{-1}Q(Z)P' = Q(e^{i\pi \frac{1}{n}} D)$ , qui est diagonale. Ainsi, les matrices de  $\mathbb{C}[Z]$  sont simultanément diagonalisables.

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

21°) Montrons que  $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$  défini par  $\varphi(Q) = \overline{Q}$  est un morphisme d'anneaux.

•  $\varphi(1) = \overline{1} = 1_{\mathbb{F}_p[X]}$ .

• Soient  $P = \sum_{n \in \mathbb{N}} b_n X^n \in \mathbb{Z}[X]$  et  $Q = \sum_{n \in \mathbb{N}} c_n X^n \in \mathbb{Z}[X]$ .

$$\diamond \quad \varphi(P+Q) = \varphi \left( \sum_{n \in \mathbb{N}} (b_n + c_n) X^n \right) = \sum_{n \in \mathbb{N}} \overline{b_n + c_n} X^n = \varphi(P) + \varphi(Q).$$

$$\diamond \quad \varphi(PQ) = \varphi \left( \sum_{n \in \mathbb{N}} \left( \sum_{k=0}^n (b_{n-k} c_k) \right) X^n \right) = \sum_{n \in \mathbb{N}} \left( \sum_{k=0}^n \overline{b_{n-k} c_k} \right) X^n = \varphi(P) \varphi(Q), \text{ d'après les règles de calculs dans l'anneau } \mathbb{F}_p[X].$$

**22°)**  $\diamond$  Supposons que  $P$  et  $Q$  sont deux polynômes primitifs de  $\mathbb{Z}[X]$ .

Supposons que  $PQ$  n'est pas primitif. Alors il existe  $p \in \mathbb{P}$  tel que  $p$  soit un diviseur commun des coefficients de  $PQ$ , donc avec les notations de la question précédente,  $\overline{PQ} = 0$ , puis  $\overline{P} \overline{Q} = 0$ , or  $\mathbb{F}_p[X]$  est un anneau intègre d'après le cours, donc  $\overline{P} = 0$  ou  $\overline{Q} = 0$ . Ainsi  $p$  est un diviseur commun des coefficients de  $P$  ou bien des coefficients de  $Q$ , donc  $P$  ou  $Q$  n'est pas primitif. C'est faux, donc  $PQ$  est primitif.

$\diamond$  Soit  $P, Q \in \mathbb{Z}[X]$ .

Si  $P = 0$  ou  $Q = 0$ , alors  $c(P) = 0$  ou  $c(Q) = 0$  et on a bien  $c(PQ) = 0 = c(P)c(Q)$ .

Supposons maintenant que  $P \neq 0$  et  $Q \neq 0$ . Alors  $c(P)$  étant le plus grand commun diviseur des coefficients de  $P$ ,  $P = c(P)P_1$ , où  $P_1$  est un polynôme primitif de  $\mathbb{Z}[X]$ .

De même,  $Q = c(Q)Q_1$ , où  $Q_1$  est un polynôme primitif de  $\mathbb{Z}[X]$ .

Alors  $c(PQ) = c(c(P)c(Q)P_1Q_1) = c(P)c(Q)c(P_1Q_1)$  d'après la distributivité du produit par rapport au pgcd, puis  $c(PQ) = c(P)c(Q)$  car  $P_1Q_1$  est primitif.

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

En notant  $b$  le ppcm des dénominateurs des coefficients non nuls de  $A$ , il existe  $A' \in \mathbb{Z}[X]$  tel que  $A = \frac{1}{b}A'$ . Si l'on pose  $a = c(A')$ ,  $A' = aA_1$  où  $A_1$  est un polynôme primitif de  $\mathbb{Z}[X]$ . Ainsi,  $bA = aA_1$ .

De même, il existe  $c, d \in \mathbb{Z}^*$  et  $B_1$  un polynôme primitif de  $\mathbb{Z}[X]$  tel que  $dB = cB_1$ .

Alors  $bdP = bdAB = acA_1B_1$ . D'après la question précédente,

$$bd \times c(P) = c(bdP) = c(acA_1B_1) = ac, \text{ donc } c(P) = \frac{ac}{bd}$$

puis  $P = \frac{ac}{bd}A_1B_1 = [c(P)A_1]B_1$  : ainsi  $P$  se décompose en le produit de deux polynômes à coefficients entiers de degrés supérieurs à 1.

**24°)**  $\diamond$  Supposons que  $P$  est composé dans  $\mathbb{Q}[X]$ . D'après la question précédente, il existe  $A, B \in \mathbb{Z}[X]$  tels que  $P = AB$  avec  $\deg(A) \geq 1$  et  $\deg(B) \geq 1$ .

Avec les notations de la question 21 et d'après les hypothèses portant sur les coefficients de  $P$ ,  $\overline{P} = \overline{a_n}X^n$ , où  $n = \deg(P)$  et où  $a_n$  est le coefficient dominant de  $P$ .  $p$  ne divise pas  $a_n$ , donc  $\overline{a_n} \neq 0$ .

On a donc  $\overline{A} \overline{B} = \overline{a_n}X^n$ . Or  $X$  est irréductible dans  $\mathbb{F}_p[X]$ , comme tout polynôme de degré 1, donc il existe  $\overline{a}, \overline{b} \in \mathbb{F}_p \setminus \{0\}$  et  $h, k \in \mathbb{N}$  tels que  $\overline{A} = \overline{a}X^h$ ,  $\overline{B} = \overline{b}X^k$  et  $h + k = n$ .

Le coefficient  $a_n$  de degré  $n$  de  $P$  est égal au produit du coefficient dominant  $\alpha$  de  $A$  avec le coefficient dominant  $\beta$  de  $B$ . Donc  $\overline{\alpha} = \overline{a} \neq 0$ ,  $\overline{\beta} = \overline{b} \neq 0$ , et surtout  $h = \deg(A) \geq 1$  et  $k = \deg(B) \geq 1$ . On en déduit que les coefficients constants de  $A$  et de  $B$  vérifient  $\overline{A(0)} = 0 = \overline{B(0)}$ , donc  $p^2$  divise  $A(0)B(0) = a_0$  ce qui est contraire aux hypothèses.

Ainsi,  $P$  est bien irréductible dans  $\mathbb{Q}[X]$ .

$\diamond$  Soit  $n \in \mathbb{N}^*$ . Prenons  $p = 2$ . Ainsi  $p$  ne divise pas le coefficient dominant de  $X^n - 2$ ,  $p$  divise ses autres coefficients, et  $p^2 = 4$  ne divise pas 2. D'après le critère d'Eisenstein,  $X^n - 2$  est irréductible dans  $\mathbb{Q}[X]$ .

**25°)** S'il existe  $n \in \mathbb{N}$  tel que  $A(X) = X^n$ , alors  $P = X^n B$ , donc le coefficient de degré  $k$  de  $B$  est égal au coefficient de degré  $n + k$  de  $P$ . Ainsi,  $A, B \in \mathbb{Z}[X]$ .



On raisonne de même s'il existe  $n \in \mathbb{N}$  tel que  $B(X) = X^n$ . On peut donc maintenant supposer que  $A$  et  $B$  ne sont pas des monômes.

Posons  $A(X) = X^n + \sum_{i=0}^{n-1} \frac{p_i}{q_i} X^i$ , avec pour tout  $i \in \{0, \dots, n-1\}$ ,  $p_i \in \mathbb{Z}$  et  $q_i \in \mathbb{N}^*$ .

Notons  $q \in \mathbb{N}^*$  le ppcm de  $q_0, \dots, q_{n-1}$  (c'est une famille non vide d'entiers naturels non nuls). Ainsi,  $A(X) = X^n + \frac{1}{q} \sum_{i=0}^{n-1} z_i X^i$ , avec  $z_i \in \mathbb{Z}$ . Quitte à diviser  $q, z_0, \dots, z_{n-1}$  par leur pgcd, on peut supposer que ce pgcd est égal à 1. Alors  $A_1 = qA$  est un polynôme primitif de  $\mathbb{Z}[X]$ .

De plus,  $P$  et  $A$  étant unitaires,  $B$  est aussi unitaire, donc de même que pour  $A$ , il existe  $r \in \mathbb{N}^*$  tel que  $B_1 = rB$  est un polynôme primitif de  $\mathbb{Z}[X]$ .

Alors  $qrP = (qA)(rB) = A_1 B_1$  est primitif, donc  $1 = c(qrP) = qr \times c(P)$ , mais  $P$  est unitaire dans  $\mathbb{Z}[X]$ , donc il est aussi primitif. Ainsi  $qr = 1$  et  $q, r \in \mathbb{N}^*$ . On en déduit que  $q = r = 1$ , donc  $A = A_1 \in \mathbb{Z}[X]$  et  $B = B_1 \in \mathbb{Z}[X]$ .

**26°)** Pour tout  $k \in \{1, \dots, n\}$ , on sait que le rationnel  $\frac{k}{n}$  admet une unique écriture irréductible  $\frac{k}{n} = \frac{h}{d}$ , où  $d|n$  et  $h \wedge d = 1$ . De plus  $\frac{k}{n} \in ]0, 1]$ , donc  $h \in \{1, \dots, d\}$ .

Ainsi, si l'on pose pour tout entier naturel  $d$  diviseur de  $n$ ,

$C_d = \{\frac{h}{d}/h \in \{1, \dots, d\} \text{ avec } h \wedge d = 1\}$ , la famille  $(C_d)_{d \in \mathbb{N}, d|n}$  est une partition de  $\{\frac{k}{n}/k \in \{1, \dots, n\}\}$ . On en déduit que

$$X^n - 1 = \prod_{k=1}^n (X - e^{2i\pi \frac{k}{n}}) = \prod_{\substack{1 \leq d \leq n \\ d|n}} \left( \prod_{\substack{1 \leq h \leq d \\ h \wedge d = 1}} (X - e^{2i\pi \frac{h}{d}}) \right) = \prod_{\substack{1 \leq d \leq n \\ d|n}} \Phi_d.$$

**27°)** Pour tout  $n \in \mathbb{N}^*$ , notons  $R(n)$  l'assertion :  $\Phi_n \in \mathbb{Z}[X]$ .

Pour  $n = 1$ ,  $\Phi_1 = X - 1 \in \mathbb{Z}[X]$ .

Pour  $n \geq 2$ , supposons que pour tout  $k \in \{1, \dots, n-1\}$ ,  $\Phi_k \in \mathbb{Z}[X]$ .

Ainsi,  $X^n - 1 = \Phi_n Q$ , où  $Q = \prod_{\substack{1 \leq d < n \\ d|n}} \Phi_d \in \mathbb{Z}[X]$ .

$\Phi_n$  est le quotient de la division euclidienne de  $X^n - 1$  par  $Q$ . Ces derniers sont tous deux dans  $\mathbb{Q}[X]$  et  $\mathbb{Q}$  est un corps, donc d'après le cours,  $\Phi_n \in \mathbb{Q}[X]$ . De plus  $X^n - 1$  et  $Q$  sont unitaires, donc d'après la question 25,  $\Phi_n \in \mathbb{Z}[X]$ .

Le principe de récurrence forte permet de conclure.

**28°)**  $\diamond \varphi_p(1) = 1^p = 1$ .

Soit  $A, B \in \mathbb{F}_p[X]$ .  $\varphi_p(AB) = (AB)^p = A^p B^p = \varphi_p(A) \varphi_p(B)$ .

Soit  $\lambda \in \mathbb{F}$ .  $\varphi_p(\lambda A) = \lambda^p A^p = \lambda A^p = \lambda \varphi_p(A)$ , d'après le petit théorème de Fermat.

D'après la formule du binôme de Newton,  $\varphi_p(A + B) = \sum_{k=0}^p \binom{p}{k} A^k B^{p-k}$ .

Soit  $k \in \{1, \dots, p-1\}$ .  $p$  divise  $p(p-1) \cdots (p-k+1) = k! \binom{p}{k}$  car  $k \geq 1$ , donc ce produit contient effectivement le facteur  $p$ , or  $p$  est premier avec  $k!$ , car  $k \leq p-1$  et  $p$  est premier, donc d'après le théorème de Gauss,  $p$  divise  $\binom{p}{k}$ . Ainsi, dans  $\mathbb{F}_p$ ,

$$\varphi_p(A+B) = A^p + B^p = \varphi_p(A) + \varphi_p(B).$$

Ceci prouve que  $\varphi_p$  est un endomorphisme d'algèbre.

◇ Soit  $h \in \mathbb{Z}[X]$ . Posons  $h(X) = \sum_{n \in \mathbb{N}} a_n X^n$ .  $(\bar{h}(X))^p = \varphi_p\left(\sum_{n \in \mathbb{N}} \bar{a}_n X^n\right)$ , donc d'après

$$\text{la question précédente, } (\bar{h}(X))^p = \sum_{n \in \mathbb{N}} \bar{a}_n \varphi_p(X^n) = \sum_{n \in \mathbb{N}} \bar{a}_n X^{pn} = \bar{h}(X^p).$$

**29°)**  $\omega$  est annulé par  $X^n - 1 \in \mathbb{Q}[X]$ , donc  $\pi_\omega$  est bien défini dans  $\mathbb{Q}[X]$ .

$\pi_\omega$  divise  $X^n - 1$ , dans  $\mathbb{Q}[X]$ , donc il existe  $h \in \mathbb{Q}[X]$  tel que  $X^n - 1 = \pi_\omega(X)h(X)$ . Or  $X^n - 1$  et  $\pi_\omega$  sont unitaires, donc d'après la question 25,  $\pi_\omega$  et  $h$  sont dans  $\mathbb{Z}[X]$ . De plus  $h$  est unitaire.

**30°)** **a)** ◇  $u^n - 1 = \pi_\omega(u)h(u) = 0$ , donc  $u^n = 1$ , puis  $(u^p)^n = 1$ .

Ainsi,  $0 = (u^p)^n - 1 = \pi_\omega(u^p)h(u^p)$ , or on suppose que  $\pi_\omega(u^p) \neq 0$ , donc  $h(u^p) = 0$ .

◇  $h(X^p)$  annule  $u$ , donc  $\pi_u$  est défini et divise  $h(X^p)$ .

$\pi_\omega$  annule  $u$ , donc  $\pi_u \mid \pi_\omega$ . Mais d'après la question 8,  $\pi_\omega$  est irréductible, donc  $\pi_u = \pi_\omega$ .

Ainsi,  $\pi_\omega$  divise  $h(X^p)$  : il existe  $g \in \mathbb{Q}[X]$  tel que  $h(X^p) = \pi_\omega(X)g(X)$ . Mais  $h(X^p)$  et  $\pi_\omega$  sont unitaires, donc d'après la question 25,  $g(X) \in \mathbb{Z}[X]$ .

**b)**  $\bar{\pi}_\omega \times \bar{g} = \overline{h(X^p)} = (\bar{h})^p$ , or  $P$  divise  $\bar{\pi}_\omega$ , donc  $P$  divise  $(\bar{h})^p$ , mais  $P$  est irréductible donc  $P$  divise  $\bar{h}$ . Il existe donc  $R, S \in \mathbb{F}_p[X]$  tels que  $\bar{h} = RP$  et  $\bar{\pi}_\omega = SP$ , donc  $\overline{X^n - 1} = \bar{\pi}_\omega \bar{h} = P^2 SR$ , ce qu'il fallait démontrer.

**c)** Dérivons l'égalité  $X^n - \bar{1} = P^2 Q$  :  $nX^{n-1} = 2PP'Q + P^2Q'$ , donc  $P$  divise  $X^n - \bar{1}$  et  $\bar{n}X^{n-1}$ . Or  $\bar{n} \neq 0$  car  $p$  ne divise pas  $n$ , donc  $P$  divise  $X^{n-1}$ , et donc aussi  $X^n$ , or il divise  $X^n - \bar{1}$ , donc  $P$  divise  $\bar{1}$ , ce qui est impossible car,  $P$  étant irréductible, il n'est pas constant.

En conséquence,  $\pi_\omega(u^p) = 0$ , pour tout racine complexe  $u$  de  $\pi_\omega$ .

**31°)** Soit  $s \in \mathbb{N}$ . Notons  $R(s)$  l'assertion : pour toute famille  $p_1, \dots, p_s$  de nombres premiers qui ne divisent pas  $n$ ,  $\pi_\omega(\omega^{p_1 \cdots p_s}) = 0$ .

Si  $s = 0$ , le produit vide  $p_1 \cdots p_s$  est égal à 1, donc  $\pi_\omega(\omega^{p_1 \cdots p_s}) = 0$ .

Supposons que  $s \geq 1$  et que  $R(s-1)$  est vraie.

Soit  $p_1, \dots, p_s$  une famille de nombre premiers qui ne divisent pas  $n$ .

Par hypothèse de récurrence,  $u = \omega^{p_1 \cdots p_{s-1}}$  est une racine de  $\pi_\omega$ , or  $p_s$  est un nombre premier qui ne divise pas  $n$ , donc d'après la question précédente,  $\pi_\omega(u^{p_s}) = 0$ . Ceci prouve  $R(s)$ .

D'après le principe de récurrence, pour tout  $s \in \mathbb{N}$ , pour toute famille  $p_1, \dots, p_s$  de nombres premiers qui ne divisent pas  $n$ ,  $\pi_\omega(\omega^{p_1 \cdots p_s}) = 0$ .

Soit  $k \in \{1, \dots, n\}$  tel que  $k \wedge n = 1$ . Notons  $p_1 \cdots p_s$  la décomposition primaire de  $k$ .  $k$  étant premier avec  $n$ , pour tout  $i \in \mathbb{N}_s$ ,  $p_i$  ne divise pas  $n$ , donc  $\pi_\omega(\omega^k) = 0$ .

**32°)**  $\omega$  est une racine de  $\Phi_n$ , donc  $\pi_\omega$  divise  $\Phi_n$ .

D'après la question précédente, toutes les racines de  $\Phi_n$  sont racines de  $\pi_\omega$ , or ces racines sont toutes simples, donc  $\Phi_n$  divise  $\pi_\omega$ . De plus,  $\Phi_n$  et  $\pi_\omega$  sont unitaires, donc ils sont égaux. Mais d'après la question 8,  $\pi_\omega$  est irréductible dans  $\mathbb{Q}[X]$ , donc  $\Phi_n$  est irréductible dans  $\mathbb{Q}[X]$ .