TD 12. Algèbre 2 - Géométrie 2

Exercice 1.

3. Notons $D = \text{pgcd}(X^n - 1, (X-1)^n)$.

Alors $D \mid X^n - 1$ et $D \mid (X-1)^n$.

Mais les diviseurs unitaires de $(X-1)^n$ sont les $(X-1)^p$ avec $0 \leq p \leq n$.

Donc $D = (X-1)^p$. Donc 1 est racine de D de multiplicité p. Mais 1 est racine de $X^n - 1$ de multiplicité 1.

Donc $p = 1$. Donc $D = X - 1$.

4. $\text{pgcd}(X^n - 1, X^m - 1) = X^{\text{pgcd}(n,m)} - 1$.

Supposons que $n \geq m$.

Par division euclidienne, $n = mq + r$ avec $0 \leq r < m$.

On a
$$\begin{aligned} X^n - 1 &= X^{mq+r} - 1 \\ &= X^r \times X^{mq} - 1 \\ &= X^r (X^{mq} - 1) + X^r - 1. \end{aligned}$$

$a^p - b^p = (a-b) \sum_{i=0}^{p-1} a^i b^{p-1-i}$.

On a
$$\begin{aligned} X^{mq} - 1 &= (X^m)^q - 1^q \\ &= (X^m - 1) \underbrace{(1 + X^m + X^{m2} + \dots X^{m(q-1)})}_{\varphi} \end{aligned}$$

Donc $X^n - 1 = (X^m - 1) \underbrace{X^r \varphi}_{\tilde{\varphi}} + \underbrace{X^r - 1}_{}$.

Reste car $d^\circ X^r - 1 = r < m = d^\circ X^m - 1$

$$\begin{aligned} \text{pgcd}(X^n - 1, X^m - 1) &= \text{pgcd}(X^m - 1, X^{r_1} - 1) \\ &= \text{pgcd}(X^{r_1} - 1, X^{r_2} - 1) \\ &\ \vdots \\ &= \text{pgcd}(X^{r_{p-1}} - 1, 0) = X^{r_{p-1}} - 1. \end{aligned}$$

$n = mq + r_1$

$m = r_1 q_1 + r_2$

$r_1 = r_2 q_2 + r_3$

$\vdots$

$r_{p-1} = r_p q_p + 0$.

$pgcd(n,m)$

Exercice 2.

- Existence : A et B sont premiers entre eux, donc d'après le théorème de Bezout, il existe $U, V \in \mathbb{K}[X]$ tels que

$$AU + BV = 1.$$

Par division euclidienne de U par B,

$$U = BQ + U_0 \quad \text{avec} \quad \deg U_0 < \deg B.$$

Alors $A(BQ + U_0) + BV = 1$,

donc $AU_0 + B(AQ + V) = 1$.

Posons $V_0 = AQ + V$. Alors $AU_0 + BV_0 = 1$.

On a $\deg(AU_0 + BV_0) = 0$

Donc $\deg(AU_0) = \deg(BV_0)$

Donc $\deg(B) + \deg(V_0) = \deg A + \deg U_0$

Donc $\deg V_0 = \deg A + \deg U_0 - \deg B < \deg A$.

- Unicité : Supposons qu'il existe (U_0, V_0) et (U_1, V_1) des couples de polynômes tels que

$$\begin{cases} AU_0 + BV_0 = 1 & \deg U_0 < \deg B, \quad \deg V_0 < \deg A \\ AU_1 + BV_1 = 1 & \deg U_1 < \deg B, \quad \deg V_1 < \deg A. \end{cases}$$

Donc $AU_0 + BV_0 = AU_1 + BV_1$, $A(U_0 - U_1) = B(V_1 - V_0)$.

Donc $A \mid B(V_1 - V_0)$. Or $pgcd(A, B) = 1$. Donc par le lemme de Gauss, $A \mid V_1 - V_0$.

Comme $\deg(V_1 - V_0) \leq \max(\deg V_1, \deg V_0)$ $\quad V_1 - V_0 = A \times P$

$< \deg A$ $\quad \deg V_1 - V_0 \geq \deg A$.

Donc $V_1 - V_0 = 0$.

Donc $V_1 = V_0$.

Donc $AU_0 = AU_1$, puis $U_0 = U_1$.

D'où l'unicité.

Exercice 3

- $1 \Rightarrow 2$. Supposons 1.

Cette famille est libre dans $\mathbb{C}_{m+n-1}[X]$, composée de $m+n$ éléments et $\dim \mathbb{C}_{m+n-1}[X] = m+n$. C'est donc une base de $\mathbb{C}_{m+n-1}[X]$ (en particulier, génératrice).

Comme $1 \in \mathbb{C}_{m+n-1}[X]$, on peut écrire

$$1 = \lambda_0 P + \lambda_1 X P + \dots + \lambda_{n-1} X^{n-1} P + \mu_0 Q + \mu_1 X Q + \dots + \mu_{m-1} X^{m-1} Q$$
$$= \underbrace{(\lambda_0 + \lambda_1 X + \dots + \lambda_{n-1} X^{n-1})}_{U \in \mathbb{C}[X]} P + \underbrace{(\mu_0 + \mu_1 X + \dots + \mu_{m-1} X^{m-1})}_{V \in \mathbb{C}[X]} Q$$

($\lambda_i, \mu_i \in \mathbb{C}$).

D'où 2.

- $2 \Rightarrow 3$. Si α est une racine commune de P et Q alors $(UP + VQ)(\alpha) = U(\alpha)P(\alpha) + V(\alpha)Q(\alpha) = 0 \neq 1$ (démo par l'absurde ou par contraposée).

- $3 \Rightarrow 1$. On suppose 3. Alors P et Q sont premiers entre eux.

Soient $\lambda_0, \dots \lambda_{n-1}, \mu_0, \dots \mu_{m-1} \in \mathbb{C}$ tels que

$$\lambda_0 P + \lambda_1 X P + \dots + \lambda_{n-1} X^{n-1} P + \mu_0 Q + \mu_1 X Q + \dots + \mu_{m-1} X^{m-1} Q = 0$$

Alors $UP + VQ = 0$ où $U = \sum_{i=0}^{n-1} \lambda_i X^i$, $V = \sum_{i=0}^{m-1} \mu_i X^i$.

Donc $UP = -VQ$.

Donc $P \mid VQ$ et P et Q sont premiers entre eux, donc par le lemme de Gauss, $P \mid V$. $\qquad V = AP$.

Or $\deg V \leq m-1 < \deg P = m$.

Donc $V = 0$, donc pour tout $i \in \{0..m-1\}$, $\mu_i = 0$.

Donc $UP = 0$; puis $U = 0$ $(P \neq 0)$.

Donc pour tout $i \in \{0..n-1\}$, $\lambda_i = 0$.

Donc la famille est libre. D'où 1.

Exercice 4 $\qquad I = (a)$

$\mathbb{K}[X]$ est un anneau principal (ses idéaux sont principaux).

On a, pour tout $n \in \mathbb{N}$, $I_n \subset I_{n+1}$.

Pour tout $n \in \mathbb{N}$, il existe $P_n \underset{\text{unitaire}}{\in} \mathbb{K}[X]$ tel que $I_n = (P_n)$.

Comme $(P_n) \subset (P_{n+1})$, alors $P_{n+1} \mid P_n$;

donc $\deg P_n \geq \deg P_{n+1}$. $\qquad P_n = AP_{n+1}$

Donc on a une suite $(\underbrace{\deg(P_n)}_{\in \mathbb{N}})_{n\in\mathbb{N}}$ décroissante et à valeurs dans $\mathbb{N}$. Donc il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \in \mathbb{N}$, si $n \geq n_0$ alors $\deg P_n = \deg P_{n_0}$.

Or $P_n \mid P_{n_0}$ pour tout $n \geq n_0$, et $\deg P_n = \deg P_{n_0}$ et P_n et P_{n_0} sont unitaires, donc $P_n = P_{n_0}$.

Donc, pour tout $n \geq n_0$, $(P_n) = (P_{n_0})$, ie $I_n = I_{n_0}$.

Donc $(I_n)_{n\in\mathbb{N}}$ est stationnaire.

Exercice 5

1. • f est linéaire : Soit $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{C}$.

$f(\lambda P + Q)$ est le reste de la D.E. de $A(\lambda P + Q)$ par B.

On a $AP = BP_1 + R_1$ et $AQ = BQ_2 + R_2$, $\deg R_1 < \deg B$
$\deg R_2 < \deg B$

Alors $f(P) = R_1$ et $f(Q) = R_2$.

Donc
$$A(\lambda P + Q) = \lambda AP + AQ$$
$$= \lambda(BP_1 + R_1) + BQ_2 + R_2$$
$$= (\lambda P_1 + Q_2)B + \underbrace{\lambda R_1 + R_2}_{\text{reste}}.$$

reste car $\deg(\lambda R_1 + R_2) < \deg B$

Donc
$$f(\lambda P + Q) = \lambda R_1 + R_2$$
$$= \lambda f(P) + f(Q).$$

- Pour tout $P \in \mathbb{C}_3[X]$, on a $AP = BQ + R$ et $\deg R < \deg B = 4$, donc $f(P) = R \in \mathbb{C}_3[X]$.

Donc $f : \mathbb{C}_3[X] \to \mathbb{C}_3[X]$.

2. $\ker f = \{ P \in \mathbb{C}_3[X],\ f(P) = 0 \}$ $\quad AP = BQ$.
$= \{ P \in \mathbb{C}_3[X],\ B \mid AP \}$

...

ou plus précis : calculons la matrice de f dans la base canonique de $\mathbb{C}_3[X]$, $\mathcal{B}_C = (1, X, X^2, X^3)$.

$f(1)$: $A \times 1 = X^4 - 1$ par $X^4 - X$.
$$X^4 - 1 = \underbrace{X^4 - X}_{B} + \underbrace{X - 1}_{R \text{ de } \deg < 4}.$$

$f(1) = X - 1$.

$f(X) = X^2 - X$, $f(X^2) = X^3 - X^2$,

DE de $X^5 - X$ par $X^4 - X$

$f(X^3) = -X^3 + X$.

$$A = \mathrm{mat}_{\mathcal{B}_C} f = \begin{array}{c} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix} \end{array} \begin{array}{l} \leftarrow 1 \\ \leftarrow X \\ \leftarrow X^2 \\ \leftarrow X^3 \end{array}$$

$P = a + bX + cX^2 + dX^3 \in \ker f$

ssi $A \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ ssi $\begin{cases} -a = 0 \\ a - b + d = 0 \\ b - c = 0 \\ c - d = 0 \end{cases}$ ssi $\begin{cases} a = 0 \\ b = d = c \end{cases}$

ssi $P = b(X+X^2+X^3)$.

Donc $\ker f = \{ b(X+X^2+X^3),\ b \in \mathbb{C}\} = \text{Vect}(X+X^2+X^3)$.

4. $\dim \ker f = 1$, donc $\dim \text{Im} f = 4 - 1 = 3$.

$$\text{Im} f = \text{Vect}\left(\begin{pmatrix}-1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\-1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\-1\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\\-1\end{pmatrix}\right)$$

$$= \text{Vect}\left(\begin{pmatrix}-1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\-1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\-1\\1\end{pmatrix}, \cancel{\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}}\right)$$

Donc $\text{Im} f = \text{Vect}(-1+X,\ -X+X^2,\ -X^2+X^3)$

$= \text{Vect}(-1+X,\ X(-1+X),\ X^2(-1+X))$

$= (-1+X)\,\text{Vect}(1, X, X^2)$

$= (X-1)\,\mathbb{C}_2[X]$.

4. $B = X^4 - X = X(X^3-1) = X(X-1)(X^2+X+1)$

$= X(X-1)(X-j)(X-\bar{j})$ où $j = e^{2i\pi/3}$.

Donc $z_1 = 0$, $z_2 = 1$, $z_3 = j$, $z_4 = \bar{j}$.

5. $P_1 = (X-1)(X-j)(X-\bar{j})$, $P_3 = X(X-1)(X-\bar{j})$

$P_2 = X(X-j)(X-\bar{j})$, $P_4 = X(X-1)(X-j)$

Soient $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{C}$ tels que

$\lambda_1 P_1 + \lambda_2 P_2 + \lambda_3 P_3 + \lambda_4 P_4 = 0$.

Pour $X = 0$, $-\lambda_1 = 0$, donc $\lambda_1 = 0$,

Pour $X = 1$, $\lambda_2 \times 1(1-j)(1-\bar{j}) = 0$, $\lambda_2 = 0$.

Pour $X = j$, $\lambda_3 = 0$.

Puis $\lambda_4 = 0$.

Donc la famille est libre, composée de 4 éléments dans l'ev $\mathbb{C}_3[X]$ de dimension 4. C'est donc une base.

6. $A P_k = B(P_k+1) + (z_k - 1) P_k$. $(X-z_k)P_k = B$.

Donc $f(P_k) = (z_k - 1) P_k$.