Exercice 1

Les réflexes ne sont pas acquis :

- *dans un $\mathbb{Z}/n\mathbb{Z}$ intègre (n premier), on résout les équations en FACTORISANT et en utilisant qu'un produit de facteurs est nul ssi l'un au moins des facteurs est nul*
- *dans un $\mathbb{Z}/n\mathbb{Z}$ non intègre (n non premier), on peut utiliser le théorème des restes chinois (voir plus bas) ou bien tester toutes les possibilités. Dans ce cas, pour résoudre $x^4 = 1$ on peut ne tester que la moitié des classes car $(-x)^4 = x^4$... Le nombre d'opérations est limité et on n'oublie pas de réduire modulo 15 pour éviter les multiplications de trop grands nombres. Par exemple, pour calculer 8^4 modulo 15, on commence par calculer $8^2 = 64 = -1$ modulo 15 puis $8^4 = (8^2)^2 = (-1)^2 = 1$ modulo 15...*

1. 19 est premier, donc $\mathbb{Z}/19\mathbb{Z}$ est un corps donc intègre. Ainsi on peut factoriser en $(\dot{x} - \dot{1}) \cdot (\dot{x}^2 + \dot{x} + \dot{1}) = \dot{0}$ et finalement, $\dot{x} = \dot{1}$ ou bien $\dot{x}^2 + \dot{x} + \dot{1} = 0$. On cherche $\dot{a} et \dot{b}$ tels que $\dot{a} + \dot{b} = -1$ et $\dot{a}\dot{b} = 1$. On trouve $\dot{7}$ et $\dot{11}$.

Finalement, les solutions sont 1,7, et 11.

2. Par contre, 15 n'est pas premier. Par le théorème des restes chinois, si ϕ est l'isomorphisme entre $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z}$, on a $\phi(1mod15) = (1mod3, 1mod5)$.

On résout alors $x_3^4 = 1mod3$ dans $\mathbb{Z}/3\mathbb{Z}$ et $x_5^4 = 1mod5$ dans $\mathbb{Z}/5\mathbb{Z}$. On trouve $x_3 \in \{1mod3, 2mod3\}$ et $x_5 \in \{1mod5, 2mod5, 3mod5, 4mod5\}$. Pour chaque couple (x_3, x_5), on retrouve la classe modulo 15 correspondante en considérant $\phi^{-1}(x_3, x_5)$. On trouve $\phi^{-1}(1mod3, 1mod5) = 1mod15$, $\phi^{-1}(1mod3, 2mod5) = 7mod15$, $\phi^{-1}(1mod3, 3mod5) = 13mod15$, $\phi^{-1}(1mod3, 4mod5) = 4mod15$, $\phi^{-1}(2mod3, 1mod5) = 11mod15$, $\phi^{-1}(2mod3, 2mod5) = 2mod15$, $\phi^{-1}(2mod3, 3mod5) = 8mod15$ et $\phi^{-1}(2mod3, 4mod5) = 14mod15$.

Finalement, l'ensemble de solutions est $\{\dot{1}, \dot{2}, \dot{4}, \dot{7}, \dot{8}, \dot{11}, \dot{13}, \dot{14}\}$.

3.
```
def racineCubique(a,n):
    resultat=[]
    for k in range(n): # la dernière valeur testée est (n-1)...
        if (k**3) \% n == a \% n : # ou bien if (k**3 - a )\% n == 0:
            resultat.append(k)
    return(resultat)
```

4. C'est du cours : x et n sont premiers entre eux $\Leftrightarrow$ x est un élément inversible de $\mathbb{Z}/n\mathbb{Z}$ $\Leftrightarrow x \in (\mathbb{Z}/n\mathbb{Z})^*$.

Alors $x^{Card(\mathbb{Z}/n\mathbb{Z})^*} = 1$ et $Card(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$.

5. x est générateur de $G \Leftrightarrow$ le sous groupe engendré par x est G $\Leftrightarrow$ tout élément de G est une puissance (entière relative) de $x \Leftrightarrow G = \{x^k | k \in \mathbb{Z}\}$.

Le nombre de générateurs de $\mathbb{U}_{2016}$ est égal à $\varphi(2016)$. Là encore, pas besoin de calculette :

$2016 = 2 \times 1008 = 2^2 \times 504 = 2^3 \times 252 = 2^4 \times 126 = 2^5 \times 63 = 2^5 \times 3^2 \times 7$.

Rappelons ensuite que $\varphi(p^k) = p^k - p^{k-1}$ pour p premier et que si n et m sont premiers entre eux, d'après le théorème des restes chinois, $\varphi(nm) = \varphi(n) \times \varphi(m)$.

Finalement, $\varphi(2016) = (2^5 - 2^4) \times (3^2 - 3) \times (7^1 - 7^0) = 16 \times 6 \times 6 = 576$

Problème 1

Partie 1

1.

2. *RAS sauf qu'il est inutile de supposer que le but est un espace vectoriel de dimension finie. Seule la source doit l'être.*

a. *La preuve se fait directement SANS récurrence. D'ailleurs, ceux qui ont cru faire une récurrence remarqueront qu'ils n'ont pas utilisé leur hypothèse de récurrence dans l'hérédité...*

Soit $x \in N_k$. Alors $f^k(x) = 0_E$ et en composant avec f linéaire, $f^{k+1}(x) = 0_E$, donc $x \in N_{k+1}$.

Soit ensuite $y \in I_{k+1}$. Il existe alors $x \in E$ tel que $f^{k+1}(x) = y$. Posons $z = f(x)$. Alors par construction, $f^k(f(x)) = y$. Donc $y \in I_k$.

b. *On voit assez souvent la fin de la preuve : $A = \{p | N_{p+1} = N_p\}$ est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément.*

Par contre, il est rare de voir une preuve correcte de $A \neq \emptyset$.

On peut pour cela regarder les dimensions : la suite $(\dim(N_k))$ est une suite croissante (au sens large) d'après la question précédente. C'est aussi une suite **d'entiers** et majorée par $\dim(E)$ car $N_k \subset E$. Cette suite est donc STATIONNAIRE ! Donc il existe $p \in \mathbb{N}$ tel que $\dim(N_p) = \dim(N_{p+1})$. Comme de plus $N_p \subset N_{p+1}$, $N_p = N_{p+1}$ et A n'est donc pas vide...

c. *Rarement fait : bizarre...*

La réponse est non ! Par exemple l'endomorphisme Δ de la partie 3 est un contre exemple, mais l'endomorphisme de $\mathbb{R}[X]$ $f : P \mapsto P'$ convient également : pour les deux, $N_k = \mathbb{R}_k[X]$ est une suite strictement croissante de noyaux !

d. *Abordé, mais rarement bien fait*

L'inclusion $N_{p_0} \subset N_{p_0+k}$ vient de la croissance de la suite des noyaux.

Réciproquement, montrons que si $N_{p_0} = N_{p_0+1}$, alors $N_{p_0+1} = N_{p_0+2}$. Soit $x \in N_{p_0+2}$. Alors $f^{p_0+1}(f(x)) = 0$ et $f(x) \in N_{p_0+1} = N_{p_0}$. Donc $f^{p_0}(x) = 0$ et $f^{p_0+1}(x) = 0$. Finalement $x \in N_{p_0+1}$.

Par récurrence, on montre alors que $N_{p_0} = N_{p_0+k}$ pour tout k.

3. a. *L'énoncé est souvent mal compris : il faut montrer ici que (I_k) est stationnaire et que le rang correspondant est le même que pour la suite (N_k).*

On sait que la suite (I_k) est croissante. Il en est de même pour la suite des dimensions $(\dim(I_k))$. Cette suite est majorée par $\dim(E)$ et à valeurs entières, donc stationne à partir d'un rang noté q_0.

Par théorème du rang appliqué à f^k (qui est un endomorphisme par composée d'endomorphismes) $\dim(N_k) + \dim(I_k) = \dim(E)$.

Donc $\dim(I_k) = \dim(E) - \dim(N_k)$ et la suite $(\dim(I_k))$ stationne exactement au même rang que la suite $\dim(N_k)$.

Comme $I_k \subset I_{k+1}$, la suite (I_k) stationne aussi exactement à partir de ce rang !

b. *Peu abordée, mais assez bien fait en général.*

Par un argument de dimension (théorème du rang encore), il suffit de montrer que la somme est directe, donc que l'intersection est réduite à $\{0\}$.

Soit $x \in N_{p_0} \cap I_{p_0}$. Alors $f^{p_0}(x) = 0$ et $x = f^{p_0}(y)$. Donc $f^{p_0}(f^{p_0}(y)) = f^{2p_0}(y) = 0$. Donc $y \in N_{2p_0} = N_{p_0}$. Finalement, $x = f^{p_0}(y) = 0$.

4. I_{p_0} est de dimension finie. La bijectivité d'un endomorphisme est donc équivalente à sa surjectivité ou bien son injectivité. Ici, la surjectivité est plus simple car par hypothèse, $I_{p_0+1} = I_{p_0}$, ce qui signifie excatement $f(I_{p_0})) = I_{p_0}$...

5. Montrons que la restriction de f à N_{p_0} est un endomorphisme : soit $x \in N_{p_0}$ alors $f^{p_0}(x) = 0$. Donc $f^x \in N_{p_0+1} = N_{p_0}$.

La restriction de f à N_{p_0} est nilpotente d'ordre inférieur ou égal à p_0 car pour tout $x \in N_{p_0}$, $f^{p_0}(x) = 0$.

De plus, l'ordre est supérieur à p_0 car par statut de p_0, il existe $x \in E$ tel que $f^{p_0-1}(x) \neq 0$ et $f^{p_0}(x) = 0$. Ce x est un élément de N_{p_0} tel que $f^{p_0-1}(x) \neq 0$ donc la restriction de f à N_{p_0} n'est pas nilpotente d'ordre inférieur à $p_0 - 1$...

6. Démontrer que la suite $(\dim(N_{k+1}) - \dim(N_k))_{k\in\mathbb{N}}$ est décroissante.

C'est la question difficile de l'exercice. Il s'agit de montrer que l'écart entre deux dimensions successives de noyaux itérés va en diminuant. Remarquons par le théorème du rang que cet écart est le même que celui entre deux dimensions d'images itérées successives : $\dim(N_{k+1}) - \dim(N_k) = \dim(I_k) - \dim(I_{k+1})$. Regardons alors comment ce comporte cet écart $e_k = \dim(N_{k+1}) - \dim(N_k)$.

Intuitivement, de $I_{k+1} = f(I_k) \subset I_k$, on perd e_k dimensions. C'est à dire qu'il existe un espace vectoriel k tel que $I_k \oplus F_k = I_{k+1}$ avec $dim(F_k) = e_k$. Que se passe-t-il donc entre I_{k+1} et I_{k+2} ? On a $I_{k+1} = f(I_k)$ et $I_{k+2} = f(I_{k+1})$ et en partant de $I_k \oplus F_k = I_{k+1}$, on obtient en composant par f : $I_{k+1} + f(F_k) = I_{k+2}$. Attention : la somme n'est plus forcément directe dans la dernière égalité. Donc par la formule de Grassman : $e_{k+1} = dim(I_{k+2}) - dim(I_{k+1}) \leq dim(f(F_k)) \leq dim(F_k) = e_k$ car f est une application linéaire (donc qui abaisse les dimensions).

La suite (e_k) est donc bien décroissante.

7. Si g est un endomorphisme nilpotent, la suite (N_k) des noyaux itérés de g est une suite STRICTEMENT croissante jusqu'à un rang p_0 à partir duquel elle est stationnaire à $N_{p_0} = E$ car g est nilpotent.

Donc la suite des dimensions $(\dim(N_k))$ est aussi une suite d'entiers strictement croissante de 0 à $\dim(E)$ puis stationnaire à partir du rang p_0. Donc $p_0 \leq \dim E$ et $g^{p_0} = g^{\dim E} = 0_{\mathcal{L}(E)}$.

L'ordre de nilpotence de g est donc inférieur ou égal à $\dim(E)$.

Partie 3 : un autre exemple

Soit $E = \mathbb{R}[X]$ et $P \in E$. On définit $\Delta(P) = P(X+1) - P(X)$.

1. Δ est linéaire (tout le monde l'a montré. C'est un endomorphisme car $\Delta(P)$ est une somme de composée de polynômes, donc un polynôme.

Inutile de parler de degré dans cette question !

2. *Pratiquement personne n'a argumenté RIGOUREUSEMENT !*

$\ker\Delta = \{P \in \mathbb{K}[X] | P(X+1) - P(X) = 0\}$. Un tel polynôme est donc 1-périodique et pour un tel polynôme, $Q = P - P(0)$ **est un polynôme admettant une infinité de racines (au moins tous les entiers), donc nul !** (cet argument revient constamment dans les exercices !!!)

Finalement, $P = P(0)$ est un polynôme constant.

Réciproquement, tout polynôme constant convient donc $\ker(\Delta) = \mathbb{R}_0[X]$.

Plus difficile : $\ker(\Delta^k) = \mathbb{R}_{k-1}[X]$. Pour $P_k = X^k$, on montre par récurrence que $\deg(\Delta(X^k)) = k-1$. Donc par linéarité de Δ, $\Delta^2(P) = 0 \Leftrightarrow deg(P) \leq 1$ et par récurrence, $\Delta^k(P) = 0 \Leftrightarrow deg(P) \leq k-1$. Finalement, $\ker(\Delta^k) = \mathbb{R}_{k-1}[X]$.

L'endomorphisme Δ n'est pas nilpotent car pour tout $n \in \mathbb{N}$, $\ker(\Delta^k) \neq \mathbb{R}[X]$...

3. Au cas où on n'aurait pas eu l'idée dans la question précédente, si $P_k = X^k$, alors $deg(\Delta(P)) = k-1$. Toujours par linéarité, $\Delta(\mathbb{R}_n[X]) \subset \mathbb{R}_{n-1}[X]$.

a. Par théorème du rang, $dim(Im(\delta)) = (n+1) - dim(ker(\delta)) = n-k$. Or $\delta^k(\mathbb{R}_n[X]) \subset \mathbb{R}_{n-k}[X]$. Par inclusion dimension, $\delta^k(\mathbb{R}_n[X]) = \mathbb{R}_{n-k}[X]$.

Alors $Im(\Delta) = \mathbb{R}[X]$ car pour tout polynôme P de degré n, il existe toujours au moins un polynôme Q de degré $n+1$ tel que $\delta(Q) = P$.

b. D'après ce qui précède, $\delta^{n+1} = 0$. Donc l'ordre de nilpotence de δ est inférieur ou égal à $n+1$. De plus, $\delta^n(X^n) \neq 0$. Donc l'ordre de nilpotence est égal à $n+1$.

4. **a.** *Attention : coquilles dans le sujet : lire "Montrer que pour tout entier naturel p, $\delta^p(\mathbf{P}) = \sum_{k=0}^{p}(-1)^{p-k}\binom{\mathbf{p}}{k}P(X+k)$." Ceux qui ont abordé la question ont généralement corrigé*

Par récurrence sur p. Je ne fais que l'hérédité :

$$\delta^{p+1}(\mathbf{P}) = \delta(\delta^p(\mathbf{P})) = \delta\left(\sum_{k=0}^{p}(-1)^{p-k}\binom{p}{k}P(X+k)\right) =$$
$$= \sum_{k=0}^{p}(-1)^{p-k}\binom{p}{k}P(X+k+1) - \sum_{k=0}^{p}(-1)^{p-k}\binom{p}{k}P(X+k)$$
$$= \sum_{k=0}^{p}(-1)^{p-k}\binom{p}{k}P(X+k+1) + \sum_{k=0}^{p}(-1)^{p-k+1}\binom{p}{k}P(X+k)$$
$$= \sum_{k'=1}^{p+1}(-1)^{p-k'+1}\binom{p}{k'-1}P(X+k') + \sum_{k=0}^{p}(-1)^{p-k+1}\binom{p}{k}P(X+k)$$
$$= (-1)^{p+1}\binom{p}{0}P(X) + \left(\sum_{k=1}^{p}(-1)^{p-k+1}P(X+k)\left[\binom{p}{k-1} + \binom{p}{k}\right]\right) + (-1)^0\binom{p}{p}P(X+p+1)$$
$$= (-1)^{p+1}\binom{p}{0}P(X) + \left(\sum_{k=1}^{p}(-1)^{p-k+1}P(X+k)\binom{p+1}{k}\right) + (-1)^0\binom{p+1}{p+1}P(X+p+1)$$
$$= \sum_{k=0}^{p+1}(-1)^{p+1-k}\binom{p+1}{k}P(X+k)$$

Récurrence établie (toute ressemblance avec le binôme de Newton ne serait fortuite...)

b. On sait que $\delta^{n+1} = 0$. Donc pour tout P, $\delta^{n+1}(P) = 0$.

Dans cette formule, en isolant le terme $k = 0$, on obtient : $-(-1)^{n+1}P(X) = \sum_{k=1}^{n+1}(-1)^{n+1-k}\binom{n+1}{k}P(X+k)$.

On pose $\lambda_k = (-1)^{k+1}\binom{n+1}{k}$...

Problème : Résultant de deux polynômes

Partie I : Définitions et propriétés

1. Cas où u est bijective

(a) Soit $(A, B) \in F^2$. $\deg(P) = p$ et $\deg(A) \leqslant q-1$ et donc $\deg(PA) \leqslant p+q-1$. De même, $\deg(QB) \leqslant p+q-1$ et donc $\deg(PA+QB) \leqslant p+q-1$. u est effectivement une application de E vers F.

Soient $((A_1, B_1), (A_2, B_2)) \in E^2$ et $(\lambda_1, \lambda_2) \in \mathbb{C}^2$.

$$\begin{aligned} u\left(\lambda_1(A_1, B_1) + \lambda_2(A_2, B_2)\right) &= u\left((\lambda_1 A_1 + \lambda_2 A_2, \lambda_1 B_1 + \lambda_2 B_2)\right) = P(\lambda_1 A_1 + \lambda_2 A_2) + Q(\lambda_1 B_1 + \lambda_2 B_2) \\ &= \lambda_1(PA_1 + QB_1) + \lambda_2(PA_2 + QB_2) = \lambda_1 u\left((A_1, B_1)\right) + \lambda_2 u\left((A_2, B_2)\right). \end{aligned}$$

$$\boxed{u \in \mathscr{L}(E, F).}$$

(b) Si u est bijective, l'élément 1 de F admet un antécédent par u dans E. Donc $\exists (U, V) \in \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X]$ tel que $UP + VQ = 1$. Le théorème de Bézout permet alors d'affirmer que les polynômes P et Q sont premiers entre eux.

(c) Supposons P et Q premiers entre eux. Soit $(A, B) \in E$.

$$(A, B) \in \mathrm{Ker}(u) \Leftrightarrow PA + QB = 0 \Leftrightarrow PA = -QB.$$

Donc, si $(A, B) \in \mathrm{Ker}(u)$, Q divise $-QB = PA$ et puisque P et Q sont premiers entre eux, Q divise A d'après le théorème de Gauss. Donc $A \in Q\mathbb{C}[X] \cap \mathbb{C}_{q-1}[X] = \{0\}$ car $\deg(Q) = q > q-1$. Par suite, A est nul puis B est nul car $QB = 0$ et $Q \neq 0$.
On a montré que $\mathrm{Ker}(u) \subset \{(0, 0)\}$ et donc $\mathrm{Ker}(u) = \{(0, 0)\}$.
Ainsi, u est une application linéaire injective. Comme de plus $\dim(E) = \dim(F) = p+q < +\infty$, on sait que u est bijective.

$$\boxed{u \text{ est bijective si et seulement si } P \text{ et } Q \text{ sont premiers entre eux.}}$$

2. Matrice de u

(a) Soit $k \in [\![0, q-1]\!]$.

$$u\left((X^k, 0)\right) = PX^k = \sum_{m=0}^{p} a_k X^{m+k}.$$

De même, pour $k \in [\![0, p-1]\!]$, $u\left((0, X^k)\right) = \sum_{m=0}^{q} b_k X^{m+k}$. Donc

$$\boxed{\mathrm{Mat}_{\mathcal{B},\mathcal{B}'}(u) = M_{P,Q}.}$$

(b) D'après les questions 2.(a), 1.(b), et 1.(c),

$$\mathrm{Res}(P,Q) \neq 0 \Leftrightarrow \det(M_{P,Q}) \neq 0 \Leftrightarrow u \text{ bijective} \Leftrightarrow P \text{ et } Q \text{ premiers entre eux.}$$

3. Racine multiple **(a)** Soit P de $\mathbb{C}[X]$ de degré supérieur ou égal à 1. On sait qu'une racine multiple de P est encore racine de P' et qu'une racine commune à P et P' est racine multiple de P. Donc, d'après la question 2.(b),

$$P \text{ admet une racine multiple} \Leftrightarrow P \text{ et } P' \text{ admettent une racine commune} \Leftrightarrow \mathrm{Res}(P,P') = 0.$$

(b) Si $P = X^3 + aX + b$ alors $P' = 3X^2 + a$ puis

$$\begin{aligned}
\mathrm{Res}(P,P') &= \begin{vmatrix} b & 0 & a & 0 & 0 \\ a & b & 0 & a & 0 \\ 0 & a & 3 & 0 & a \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = b \begin{vmatrix} b & 0 & a & 0 \\ a & 3 & 0 & a \\ 0 & 0 & 3 & 0 \\ 1 & 0 & 0 & 3 \end{vmatrix} + a \begin{vmatrix} a & b & a & 0 \\ 0 & a & 0 & a \\ 1 & 0 & 3 & 0 \\ 0 & 1 & 0 & 3 \end{vmatrix} \\
&= 3b \begin{vmatrix} b & a & 0 \\ 0 & 3 & 0 \\ 1 & 0 & 3 \end{vmatrix} + a^2 \begin{vmatrix} a & 0 & a \\ 0 & 3 & 0 \\ 1 & 0 & 3 \end{vmatrix} + a \begin{vmatrix} b & a & 0 \\ a & 0 & a \\ 1 & 0 & 3 \end{vmatrix} \\
&= 9b \begin{vmatrix} b & a \\ 0 & 3 \end{vmatrix} + 3a^2 \begin{vmatrix} a & a \\ 1 & 3 \end{vmatrix} - a^2 \begin{vmatrix} a & a \\ 1 & 3 \end{vmatrix} \\
&= 27b^2 + 4a^3.
\end{aligned}$$

Ainsi,

$$\boxed{X^3 + aX + b \text{ a une racine double si et seulement si } 27b^2 + 4a^3 = 0.}$$

Partie II : Applications

4. Equation de Bézout. (a)

$$\begin{aligned}
\mathrm{Res}(P,Q) &= \begin{vmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & -1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & -1 & 1 \\ 1 & 1 & 0 & -1 & 1 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{vmatrix} \quad (C_4 \leftarrow C_4 - C_1) \\
&= \begin{vmatrix} 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ 1 & 0 & -1 & 1 & 0 & -1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ 1 & 0 & 0 & 1 & 0 & -1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{vmatrix} \quad (C_3 \leftarrow C_3 + C_4) \\
&= \begin{vmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 \\ 1 & 0 & 1 & 0 & -1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & -1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{vmatrix} \quad (C_1 \leftarrow C_1 - C_3) \\
&= -\begin{vmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ 0 & 0 & 1 \end{vmatrix} = -\begin{vmatrix} -1 & 1 \\ 0 & 1 \end{vmatrix} = 1 \neq 0.
\end{aligned}$$

Donc

P et Q sont premiers entre eux.

(b) Soit $(A,B)\in\mathbb{C}_2[X]\times\mathbb{C}_3[X]$. Posons $A=\alpha_0+\alpha_1X+\alpha_2X^2$ et $B=\beta_0+\beta_1X+\beta_2X^2+\beta_3X^3$ de sorte que

$$(A,B)=\alpha_0(1,0)+\alpha_1(X,0)+\alpha_2(X^2,0)+\beta_0(0,1)+\beta_1(0,X)+\beta_2(0,X^2)+\beta_3(0,X^3).$$

$$PA+QB=1\Leftrightarrow u((A,B))=1\Leftrightarrow M_{P,Q}\begin{pmatrix}\alpha_0\\\alpha_1\\\alpha_2\\\beta_0\\\beta_1\\\beta_2\\\beta_3\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\end{pmatrix}$$

Maintenant

$$M_{P,Q}\begin{pmatrix}\alpha_0\\\alpha_1\\\alpha_2\\\beta_0\\\beta_1\\\beta_2\\\beta_3\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\end{pmatrix}\Leftrightarrow\begin{pmatrix}1&0&0&1&0&0&0\\0&1&0&-1&1&0&0\\0&0&1&0&-1&1&0\\1&0&0&1&0&-1&1\\1&1&0&0&1&0&-1\\0&1&1&0&0&1&0\\0&0&1&0&0&0&1\end{pmatrix}\begin{pmatrix}\alpha_0\\\alpha_1\\\alpha_2\\\beta_0\\\beta_1\\\beta_2\\\beta_3\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\end{pmatrix}$$

$$\Leftrightarrow\begin{cases}\alpha_0+\beta_0=1\\\alpha_1-\beta_0+\beta_1=0\\\alpha_2-\beta_1+\beta_2=0\\\alpha_0+\beta_0-\beta_2+\beta_3=0\\\alpha_0+\alpha_1+\beta_1-\beta_3=0\\\alpha_1+\alpha_2+\beta_2=0\\\alpha_2+\beta_3=0\end{cases}\Leftrightarrow\begin{cases}\beta_0=1-\alpha_0\\\beta_3=-\alpha_2\\\alpha_0+\alpha_1+\beta_1=1\\\alpha_2-\beta_1+\beta_2=0\\-\beta_2-\alpha_2=-1\\\alpha_0+\alpha_1+\beta_1+\alpha_2=0\\\alpha_1+\alpha_2+\beta_2=0\end{cases}$$

$$\Leftrightarrow\Leftrightarrow\begin{cases}\alpha_2=-1\\\beta_3=1\\\beta_2=2\\\beta_1=1\\\alpha_1=-1\\\alpha_0=1\\\beta_0=0\end{cases}\Leftrightarrow A=1-X-X^2\text{ et }B=X+2X^2+X^3.$$

On peut prendre $(A_0,B_0)=(1-X-X^2,X+2X^2+X^3)$.

(c) Soit $(A,B)\in\mathbb{C}[X]$.

$$AP+BQ=1\Leftrightarrow AP+BQ=A_0P+B_0Q\Leftrightarrow P(A-A_0)=Q(B_0-B).$$

Nécessairement, P divise $Q(B_0-B)$ et donc, puisque $P\wedge Q=1$, P divise B_0-B d'après le théorème de Gauss. Donc il existe un polynôme S tel que $B_0-B=SP$. De même, il existe un polynôme R tel que $A=A_0+QR$.
Réciproquement, si $A=A_0+QR$ et $B=B_0-PS$,

$$AP+BQ=1\Leftrightarrow A_0P+B_0Q+QP(R-S)=1\Leftrightarrow QP(R-S)=0\Leftrightarrow R=S.$$

$$\mathscr{S}=\left\{(1-X-X^2-S(X^3-X+1)),X+2X^2+X^3+S(X^4+X^3+1)),\ S\in\mathbb{C}[X]\right\}.$$

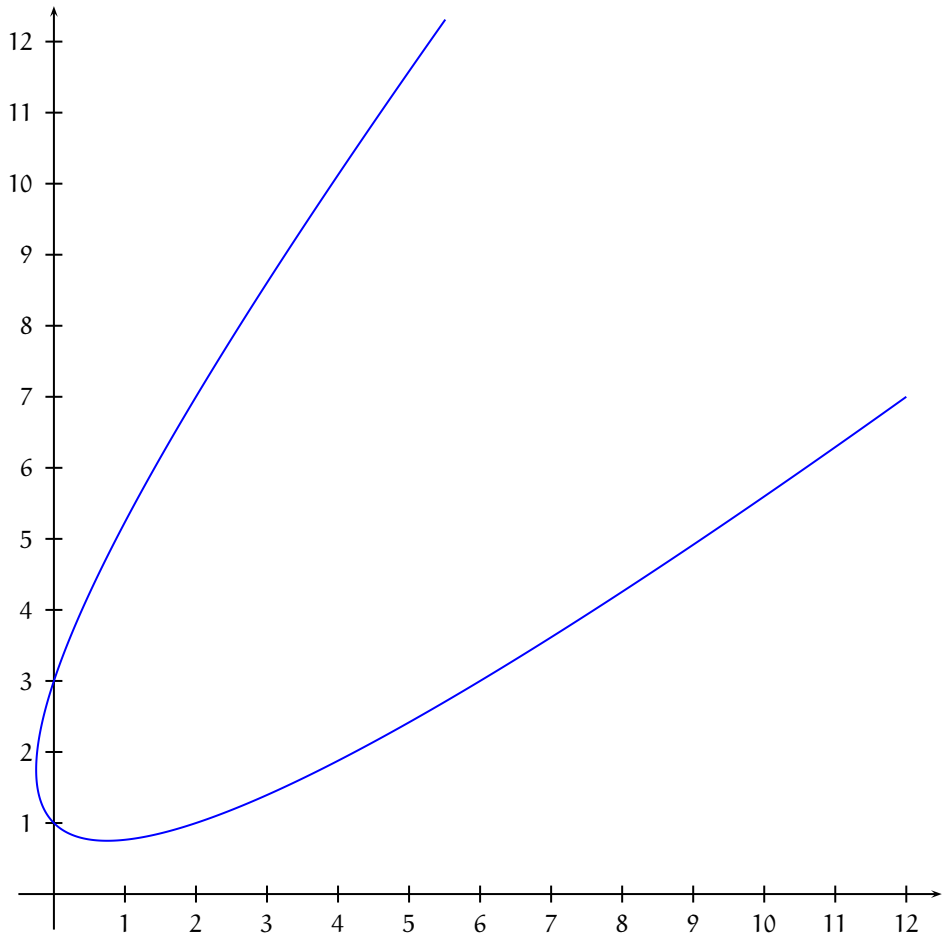
4. Equation d'une courbe **(a)** Pour $t\in\mathbb{R}$, $\overrightarrow{\frac{dM}{dt}}(t)=\begin{pmatrix}2t+1\\2t-1\end{pmatrix}$. En particulier, $\forall t\in\mathbb{R}$, $\overrightarrow{\frac{dM}{dt}}(t)\neq\overrightarrow{0}$ et Γ est un arc régulier.

Tableau de variations conjointes de x et y

t	$-\infty$		$-\frac{1}{2}$		$\frac{1}{2}$		$+\infty$
$x'(t)$		$-$	0	$+$			
x	$+\infty$	$\searrow$	$-\frac{1}{4}$	$\nearrow$			$+\infty$
y	$+\infty$			$\searrow$	$\frac{3}{4}$	$\nearrow$	$+\infty$
$y'(t)$			$-$		0	$+$	

Etude des branches infinies. Quand t tend vers $\pm\infty$, $x(t)$ et $y(t)$ tend vers $+\infty$ puis $\dfrac{y(t)}{x(t)} = \dfrac{t^2-t+1}{t^2+t}$ tend vers 1 et enfin $y(t)-x(t) = -2t+1$ tend vers $-\infty$ quand t tend vers $+\infty$ et vers $+\infty$ quand t tend vers $-\infty$.
On en déduit que Γ admet une direction asymptotique d'équation $y = x$ mais n'admet pas de droite asymptote.

Tracé de Γ



(b) $M(x,y) \in \Gamma \Leftrightarrow \exists t \in \mathbb{R}/ \begin{cases} x = x(t) \\ y = y(t) \end{cases} \Leftrightarrow \exists t \in \mathbb{R}/ \begin{cases} A(t) = 0 \\ B(t) = 0 \end{cases}$ $\Leftrightarrow$ A et B ont une racine commune dans $\mathbb{R}$.
Maintenant,

A et B ont une racine commune dans $\mathbb{C} \Leftrightarrow \mathrm{Res}(A,B) = 0$

$$\Leftrightarrow \begin{vmatrix} -x & 0 & 1-y & 0 \\ 1 & -x & -1 & 1-y \\ 1 & 1 & 1 & -1 \\ 0 & 1 & 0 & 1 \end{vmatrix} = 0$$

$$\Leftrightarrow -x \begin{vmatrix} -x & -1 & 1-y \\ 1 & 1 & -1 \\ 1 & 0 & 1 \end{vmatrix} + (1-y) \begin{vmatrix} 1 & -x & 1-y \\ 1 & 1 & -1 \\ 0 & 1 & 1 \end{vmatrix} = 0$$

$$\Leftrightarrow -x((-x+1)+(y)) + (1-y)(2-(-x-1+y)) = 0$$

$$\Leftrightarrow x^2 - 2xy + y^2 - 4y + 3 = 0.$$

En résumé,

$$\begin{aligned} M(x,y) \in \Gamma &\Leftrightarrow A \text{ et } B \text{ ont une racine commune dans } \mathbb{R} \\ &\Rightarrow A \text{ et } B \text{ ont une racine commune dans } \mathbb{C} \\ &\Leftrightarrow x^2 - 2xy + y^2 - 4y + 3 = 0. \end{aligned}$$

$$\boxed{\text{Si } M(x,y) \in \Gamma \text{ alors } x^2 - 2xy + y^2 - 4y + 3 = 0.}$$

Remarque.

$$\begin{aligned} M(x,y) \in \Gamma &\Leftrightarrow \exists t \in \mathbb{R} / \left\{ \begin{array}{l} x = t^2 + t \\ y = t^2 - t + 1 \end{array} \right. \Leftrightarrow \exists t \in \mathbb{R} / \left\{ \begin{array}{l} x - y = 2t - 1 \\ y = t^2 - t + 1 \end{array} \right. \\ &\Leftrightarrow \exists t \in \mathbb{R} / \left\{ \begin{array}{l} t = \dfrac{1}{2}(x - y + 1) \\ y = \dfrac{1}{4}(x - y + 1)^2 - \dfrac{1}{2}(x - y + 1) + 1 \end{array} \right. \Leftrightarrow y = \frac{1}{4}(x - y + 1)^2 - \frac{1}{2}(x - y + 1) + 1 \\ &\Leftrightarrow x^2 - 2xy + y^2 - 4y + 3 = 0. \end{aligned}$$

(c) La matrice de q dans la base canonique est $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$. Cette matrice est de rang 1 et on sait que la courbe d'équation $x^2 - 2xy + y^2 - 4y + 3 = 0$ est une conique du genre parabole et donc soit une parabole, soit une droite, soit est vide. En tenant compte du tracé de la question (a), cette courbe est une parabole.

6. Nombre algébrique. Déterminons le résultant de P et Q.

$$\begin{aligned} \text{Res}(P,Q) &= \begin{vmatrix} -3 & 0 & y^2-7 & 0 \\ 0 & -3 & -2y & y^2-7 \\ 1 & 0 & 1 & -2y \\ 0 & 1 & 0 & 1 \end{vmatrix} = -3 \begin{vmatrix} -3 & -2y & y^2-7 \\ 0 & 1 & -2y \\ 1 & 0 & 1 \end{vmatrix} + \begin{vmatrix} 0 & y^2-7 & 0 \\ -3 & -2y & y^2-7 \\ 1 & 0 & 1 \end{vmatrix} \\ &= -3(-3 + (3y^2 + 7)) + ((3y^2 - 21) + (y^4 - 14y^2 + 49)) = y^4 - 20y^2 + 16. \end{aligned}$$

Si $y = \sqrt{3}+\sqrt{7}$, alors P et Q ont une racine commune dans $\mathbb{C}$ à savoir $\sqrt{3}$ et donc $\text{Res}(P,Q) = 0$. Ainsi, pour $y = \sqrt{3}+\sqrt{7}$, on a $y^4 - 20y^2 + 16 = 0$ et donc

$$\boxed{\sqrt{3} + \sqrt{7} \text{ est racine du polynôme } X^4 - 20X^2 + 16.}$$

Ensuite, pour $z \in \mathbb{C}$,

$$\begin{aligned} z^4 - 20z^2 + 16 = 0 &\Leftrightarrow (z^2 - 10)^2 = 84 \Leftrightarrow z^2 = 10 + 2\sqrt{21} \text{ ou } z^2 = 10 - 2\sqrt{21} \\ &\Leftrightarrow z^2 = (\sqrt{3} + \sqrt{7})^2 \text{ ou } z^2 = (\sqrt{3} - \sqrt{7})^2 \\ &\Leftrightarrow z \in \{\sqrt{3} + \sqrt{7}, -\sqrt{3} + \sqrt{7}, \sqrt{3} - \sqrt{7}, -\sqrt{3} - \sqrt{7}. \end{aligned}$$

$$\boxed{\text{Les racine du polynôme } X^4 - 20X^2 + 16 \text{ sont } \sqrt{3} + \sqrt{7},\ -\sqrt{3} + \sqrt{7},\ \sqrt{3} - \sqrt{7} \text{ et } -\sqrt{3} - \sqrt{7}.}$$

Remarque. $\alpha = \sqrt{3} + \sqrt{7} \Rightarrow \alpha^2 = 10 + 2\sqrt{21} \Rightarrow (\alpha^2 - 10)^2 = 84 \Rightarrow \alpha^4 - 20\alpha^2 + 16 = 0.$