Devoir surveillé n°11

- La présentation, la lisibilité, l'orthographe, la qualité de la rédaction et la précision des raisonnements entreront pour une part importante dans l'appréciation des copies.
- On prendra le temps de vérifier les résultats dans la mesure du possible.
- Les calculatrices sont interdites.

Problème 1

1 **1.a** Pour tout $\theta \in \mathbb{R}$, $\cos(0 \times \theta) = 1$ donc $T_0 = 1$.
Pour tout $\theta \in \mathbb{R}$, $\cos(1 \times \theta) = \cos\theta$ donc $T_1 = X$.
Pour tout $\theta \in \mathbb{R}$, $\cos(2\theta) = 2\cos^2\theta - 1$ donc $T_2 = 2X^2 - 1$.
Pour tout $\theta \in \mathbb{R}$,

$$\begin{aligned}
\cos(3\theta) &= \cos(\theta + 2\theta) \\
&= \cos(\theta)\cos(2\theta) - \sin(\theta)\sin(2\theta) \\
&= \cos(\theta)(2\cos^2(\theta) - 1) - 2\sin^2(\theta)\cos\theta \\
&= \cos(\theta)(2\cos^2(\theta) - 1) - 2\sin^2(\theta)\cos\theta \\
&= \cos(\theta)(2\cos^2(\theta) - 1) - 2(1 - \cos^2(\theta))\cos\theta \\
&= 4\cos^3(\theta) - 3\cos(\theta)
\end{aligned}$$

donc $T_3 = 4X^3 - 3X$.

1.b Soit $\theta \in \mathbb{R}$. Alors

$$\cos(n\theta) = \mathrm{Re}(e^{in\theta}) = \mathrm{Re}\left((\cos\theta + i\sin\theta)^n\right) = \mathrm{Re}\left(\sum_{k=0}^{n}\binom{n}{k}\cos(\theta)^{n-k}i^k\sin(\theta)^k\right)$$

Or $i^{2k} = (-1)^k$ et $i^{2k+1} = (-1)^k i$ donc

$$\begin{aligned}
\cos(n\theta) &= \sum_{0\le k\le n/2}\binom{n}{2k}\cos(\theta)^{n-2k}(-1)^k\sin(\theta)^{2k} \\
&= \sum_{0\le k\le n/2}\binom{n}{2k}\cos(\theta)^{n-2k}(-1)^k(1-\cos(\theta)^2)^k \\
&= \sum_{0\le k\le n/2}\binom{n}{2k}\cos(\theta)^{n-2k}(\cos(\theta)^2-1)^k
\end{aligned}$$

On en déduit que

$$T_n = \sum_{0\le k\le n/2}\binom{n}{2k}(X^2-1)^k X^{n-2k}$$

1.c Soient $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$. D'après une formule de factorisation,

$$\cos((n+2)\theta) + \cos(n\theta) = 2\cos\left(\frac{(n+2)\theta - n\theta}{2}\right)\cos\left(\frac{(n+2)\theta + n\theta}{2}\right) = 2\cos(\theta)\cos((n+1)\theta)$$

ou encore

$$T_{n+2}(\cos\theta) + T_n(\cos\theta) = 2\cos(\theta)T_{n+1}(\cos\theta)$$

Ainsi le polynôme $T_{n+2} + T_n - 2XT_{n+1}$ est nul sur l'ensemble infini $\cos(\mathbb{R}) = [-1, 1]$: c'est donc le polynôme nul. On en déduit que $T_{n+2} = 2XT_{n+1} - T_n$.
On peut alors montrer par récurrence que, pour $n \in \mathbb{N}^*$, T_n est un polynôme de degré n et de coefficient dominant 2^{n-1}. On sait par ailleurs que $T_0 = 1$.

Retrouvons ce résultat à l'aide de la question **1.b**. Pour tout entier k tel que $0 \leq k \leq n/2$, $(\mathrm{X}^2-1)^k\mathrm{X}^{n-2k}$ est un polynôme unitaire de degré n. On en déduit que T_n est de degré n et que son coefficient dominant est

$$a_n = \sum_{0\leq 2k\leq n}\binom{n}{2k}$$

Posons également $b_n = \sum_{0\leq 2k+1\leq n}\binom{n}{2k+1}$. Alors

$$a_n + b_n = \sum_{k=0}^{n}\binom{n}{k} = (1+1)^n = 2^n$$

et

$$a_n - b_n = \sum_{k=0}^{n}(-1)^k\binom{n}{k} = (1-1)^n = \begin{cases} 0 & \text{si } n \in \mathbb{N}^* \\ 1 & \text{si } n = 0 \end{cases}$$

On en déduit que $a_n = 2^{n-1}$ si $n \in \mathbb{N}^*$ et $a_0 = 1$.

1.d On propose une version itérative.

```
def tchebychev(n):
    U, V = [1], [0,1]
    for _ in range(n):
        U, V = V, [2*v-u for (u,v) in zip(U+[0,0], [0]+V)]
    return U
```

```
>>> tchebychev(4)
[1, 0, -8, 0, 8]
```

On peut également proposer une version récursive naïve.

```
def tcheby_pourri(n):
    if n==0:
        return [1]
    if n==1:
        return [0,1]
    U, V = tcheby_pourri(n-2), tcheby_pourri(n-1)
    return [2*v-u for (u,v) in zip(U+[0,0],[0]+V)]
```

```
>>> tcheby_pourri(4)
[1, 0, -8, 0, 8]
```

Mais la complexité de cet algorithme est exponentielle (double appel récursif). On peut néanmoins proposer une version récursive de complexité raisonnable.

```
def aux(n):
    if n==0:
      return [1], [0,1]
    U, V = aux(n-1)
    return V, [2*v-u for (u,v) in zip(U+[0,0], [0]+V)]

def tcheby(n):
    return aux(n)[0]
```

```
>>> tcheby(4)
[1, 0, -8, 0, 8]
```

1.e Soit $n \in \mathbb{N}^*$. Posons $x_k = \cos \dfrac{(2k+1)\pi}{2n}$ pour $k \in [\![0, n-1]\!]$. Par définition de T_n,

$$\mathrm{T}_n(x_k) = \cos\left(\frac{(2k+1)\pi}{2}\right) = 0$$

Les x_k sont donc des racines de T_n. De plus, cos est strictement décroissante sur $[0, \pi]$ donc les $x_0, \dots, x_{n-1}$ sont deux à deux distincts. Puisque $\deg \mathrm{T}_n = n$, T_n est scindé à racines simples et ses racines sont $x_0, \dots, x_{n-1}$. Il est clair qu'elles appartiennent bien toutes à $]-1, 1[$.

$\boxed{2}$ **2.a** Soit $n \in \mathbb{N}$. Pour tout $\theta \in \mathbb{R}$, $\mathrm{T}_{n+1}(\cos\theta) = \cos((n+1)\theta)$. En dérivant cette relation par rapport à θ, on obtient

$$-\sin(\theta)\mathrm{T}'_{n+1}(\cos\theta) = -(n+1)\sin((n+1)\theta)$$

ou encore

$$\sin(\theta)\mathrm{U}_n(\cos\theta) = \sin((n+1)\theta)$$

Notamment, pour $\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$, $\sin\theta \neq 0$ et

$$\mathrm{U}_n(\cos\theta) = \frac{\sin((n+1)\theta)}{\sin\theta}$$

2.b **2.b.i** Soit $\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$. A nouveau, une formule de factorisation montre que

$$\sin((n+1)\theta) + \sin((n+3)\theta) = 2\cos(\theta)\sin((n+2)\theta)$$

ou encore

$$\mathrm{U}_n(\cos\theta) + \mathrm{U}_{n+2}(\cos\theta) = 2\cos(\theta)\mathrm{U}_{n+1}(\cos\theta)$$

On en déduit que le polynôme $\mathrm{U}_n + \mathrm{U}_{n+2} - 2\mathrm{X}\mathrm{U}_{n+1}$ est nul sur l'ensemble infini $]-1, 1[$: c'est donc le polynôme nul et $\mathrm{U}_{n+2} = 2\mathrm{X}\mathrm{U}_{n+1} - \mathrm{U}_n$.

2.b.ii Soit $n \in \mathbb{N}$. Posons $y_k = \cos \dfrac{k\pi}{n+1}$ pour $k \in [\![1, n]\!]$. La question précédente montre que $\mathrm{U}_n(y_k) = 0$ pour tout $k \in [\![1, n]\!]$. A nouveau, la stricte décroissance de cos sur $[0, \pi]$ garantit que $y_1, \dots, y_n$ sont deux à deux distincts. Enfin, $\deg \mathrm{U}_n = \deg \mathrm{T}'_{n+1} = n + 1 - 1 = n$ donc U_n est scindé à racines simples et ses racines sont $y_1, \dots, y_n$. Il est clair que ces racines appartiennent bien à $]-1, 1[$.

$\boxed{3}$ **3.a** Soit $(m, n) \in \mathbb{N}^2$ tel que $m \leq n$. D'après une formule de linéarisation

$$\forall \theta \in \mathbb{R},\ \cos(m\theta)\cos(n\theta) = \frac{1}{2}\left(\cos((n+m)\theta)\cos((n-m)\theta)\right)$$

On en déduit comme auparavant que $\mathrm{T}_m\mathrm{T}_n = \dfrac{1}{2}(\mathrm{T}_{n+m} + \mathrm{T}_{n-m})$.
Soit $(m, n) \in \mathbb{N}^2$ tel que $m < n$. Une formule de linéarisation montre à nouveau que

$$\forall \theta \in \mathbb{R},\ \cos(m\theta)\sin(n\theta) = \frac{1}{2}(\sin((n+m)\theta) + \sin(n-m)\theta)$$

En utilisant la question **2.a**, on en déduit que

$$\forall \theta \in \mathbb{R} \setminus \pi\mathbb{Z},\ \mathrm{T}_m(\cos\theta)\mathrm{U}_{n-1}(\cos\theta) = \frac{1}{2}(\mathrm{U}_{n+m-1}(\cos\theta) + \mathrm{U}_{n-m-1}(\cos\theta))$$

Puisque $\cos(\mathbb{R} \setminus \pi\mathbb{Z}) =]-1, 1[$ est infini,

$$\mathrm{T}_m\mathrm{U}_{n-1} = \frac{1}{2}(\mathrm{U}_{n+m-1} + \mathrm{U}_{n-m-1})$$

3.b **3.b.i** Si $m \leq n - m$ i.e. $2m \leq n$, on obtient avec la question précédente

$$2\mathrm{T}_{n-m}\mathrm{T}_m = \mathrm{T}_n + \mathrm{T}_{n-2m}$$

ou encore

$$\mathrm{T}_n = 2\mathrm{T}_{n-m}\mathrm{T}_m - \mathrm{T}_{n-2m}$$

Puisque $\deg \mathrm{T}_{n-2m} = n-2m < m = \mathrm{T}_m$, on en déduit par unicité du couple quotient/reste dans une division euclidienne que $\mathrm{Q}_{n,m} = 2\mathrm{T}_{n-m}$ et $\mathrm{R}_{n,m} = -\mathrm{T}_{n-2m}$.
Supposons maintenant que $m \geq n-m$. En appliquant à nouveau la question précédente,

$$2\mathrm{T}_{n-m}\mathrm{T}_m = \mathrm{T}_n + \mathrm{T}_{2m-n}$$

On en déduit comme précédemment que $\mathrm{Q}_{n,m} = 2\mathrm{T}_{n-m}$ et $\mathrm{R}_{n,m} = -\mathrm{T}_{2m-n}$.
De manière générale, $\mathrm{Q}_{n,m} = 2\mathrm{T}_{n-m}$ et $\mathrm{R}_{n,m} = -\mathrm{T}_{|n-2m|}$.
3.b.ii Remarquons que pour tout $k \in [\![1, p]\!]$,

$$\mathrm{T}_{(2k+1)m} + \mathrm{T}_{(2k-1)m} = 2\mathrm{T}_{2km}\mathrm{T}_m$$

ou encore

$$(-1)^{k+1}\mathrm{T}_{(2k+1)m} - (-1)^k\mathrm{T}_{(2k-1)m} = 2(-1)^{k+1}\mathrm{T}_{2km}\mathrm{T}_m$$

En sommant ces égalités, on obtient par télescopage

$$(-1)^{p+1}\mathrm{T}_{(2p+1)m} - (-1)^1\mathrm{T}_m = 2\left(\sum_{k=1}^{p}(-1)^{k+1}\mathrm{T}_{2km}\right)\mathrm{T}_m$$

ou encore

$$\mathrm{T}_{(2p+1)m} = \left[(-1)^p\mathrm{T}_m + 2\sum_{k=1}^{p}(-1)^{p-k}\mathrm{T}_{2km}\right]\mathrm{T}_m$$

Autrement dit,

$$\mathrm{R}_{n,m} = 0 \qquad \text{et} \qquad \mathrm{Q}_{n,m} = (-1)^p\mathrm{T}_m + 2\sum_{k=1}^{p}(-1)^{p-k}\mathrm{T}_{2km}$$

3.b.iii On cherche à montre l'existence et l'unicité d'un entier p tel que $|n-2pm| < m$ i.e. $(2p-1)m < n < (2p+1)m$. Comme n n'est pas le produit de m par un entier impair, cet entier existe et est unique : il s'agit du plus grand entier p tel que $(2p-1)m < n$. De plus, la condition $|n-2pm| < m$ implique que $p \neq 0$ car $n > m$. Ainsi $p \geq 1$.
A nouveau, pour tout $k \in [\![0, p-2]\!]$,

$$\mathrm{T}_{n-2(k+1)m} + \mathrm{T}_{n-2km} = 2\mathrm{T}_{n-(2k+1)m}\mathrm{T}_m$$

ou encore

$$(-1)^{k+1}\mathrm{T}_{n-2(k+1)m} - (-1)^k\mathrm{T}_{n-2km} = 2(-1)^{k+1}\mathrm{T}_{n-(2k+1)m}\mathrm{T}_m$$

En sommant ces égalités, on obtient par télescopage

$$(-1)^{p-1}\mathrm{T}_{n-2(p-1)m} - \mathrm{T}_n = 2\left(\sum_{k=0}^{p-2}(-1)^{k+1}\mathrm{T}_{n-(2k+1)m}\right)\mathrm{T}_m$$

ou encore

$$\mathrm{T}_n = (-1)^{p-1}\mathrm{T}_{n-2(p-1)m} + 2\left[\sum_{k=0}^{p-2}(-1)^k\mathrm{T}_{n-(2k+1)m}\right]\mathrm{T}_m$$

Mais $(2p-1)m < n < (2p+1)m$ donc $m < n-2(p-1)m < 3m$. D'après la question **3.b.i**,

$$\mathrm{T}_{n-2(p-1)m} = 2\mathrm{T}_{n-(2p-1)m}\mathrm{T}_m - \mathrm{T}_{|n-2pm|}$$

On en déduit que

$$\mathrm{T}_n = (-1)^p\mathrm{T}_{|n-2pm|} + 2\left[\sum_{k=0}^{p-1}(-1)^k\mathrm{T}_{n-(2k+1)m}\right]\mathrm{T}_m$$

Enfin, on constate que $\deg \mathrm{T}_{|n-2m|} = |n-2m| < m = \deg \mathrm{T}_m$. On en déduit bien que

$$\mathrm{Q}_{n,m} = 2(\mathrm{T}_{n-m} - \mathrm{T}_{n-3m} + \cdots + (-1)^{p-1}\mathrm{T}_{n-(2p-1)m}) \qquad \text{et} \qquad \mathrm{R}_{n,m} = (-1)^p\mathrm{T}_{|n-2pm|}$$

4 **4.a** On a vu que les racines de U_m étaient les $\cos\dfrac{k\pi}{m+1}$ pour $k \in [\![1, m]\!]$. De même les racines de U_n sont les $\cos\dfrac{\ell\pi}{n+1}$ pour $\ell \in [\![1, n]\!]$.
Soit α une racine commune de U_m et U_n. Il existe donc $(k, \ell) \in [\![1, m]\!] \times [\![1, n]\!]$ tel que

$$\alpha = \cos\frac{k\pi}{m+1} = \cos\frac{\ell\pi}{n+1}$$

Par injectivité de cos sur $[0, \pi]$, on a alors

$$\frac{k\pi}{m+1} = \frac{\ell\pi}{n+1}$$

ou encore

$$k(n+1) = \ell(m+1)$$

Il existe $(a, b) \in \mathbb{N}^2$ tel que $n + 1 = ha$ et $m + 1 = hb$. On a alors $kb = \ell a$ et $a \wedge b = 1$. D'après le lemme de Gauss, a divise k et b divise ℓ. Il existe alors $q \in \mathbb{N}$ tel que $k = qa$ et $\ell = qb$. Alors

$$\alpha = \cos\frac{k\pi}{m+1} = \cos\frac{\ell\pi}{n+1} = \cos\frac{q\pi}{h}$$

On en déduit que α est une racine de U_{h-1}.
Réciproquement, avec les notations précédentes,

$$\forall q \in [\![1, h]\!],\ \cos\frac{q\pi}{h} = \cos\frac{aq\pi}{m+1} = \cos\frac{bq\pi}{n+1}$$

donc les racines de U_{h-1} sont bien des racines communes de U_m et U_n.
Finalement, les racines communes de U_m et U_n sont exactement les racines de U_{h-1}. Comme U_m, U_n et U_{h-1} sont scindés à racines simples, on peut conclure que U_{h-1} est un pgcd de U_m et U_n.

4.b 4.b.i Soit α une racine commune de T_n et T_m. Il existe donc $(k, \ell) \in [\![0, m-1]\!] \times [\![0, n-1]\!]$ tel que

$$\alpha = \cos\frac{(2k+1)\pi}{2m} = \cos\frac{(2\ell+1)\pi}{2n}$$

Par injectivité de cos sur $[0, \pi]$,

$$\frac{(2k+1)\pi}{2m} = \frac{(2\ell+1)\pi}{2n}$$

ou encore

$$n_1(2k+1) = m_1(2\ell+1)$$

Or $m_1 \wedge n_1 = 1$ donc m_1 divise $2k+1$ et n_1 divise $2\ell+1$. Il existe donc un entier q tel que $2k+1 = m_1 q$ et $2\ell+1 = n_1 q$. Comme m_1 et n_1 sont imapirs, q l'est également. Alors

$$\alpha = \cos\frac{(2k+1)\pi}{2m} = \cos\frac{(2\ell+1)\pi}{2n} = \cos\frac{q\pi}{2g}$$

est une racine de T_g.
Réciproquement, avec les notations précédentes,

$$\forall q \in [\![0, g-1]\!],\ \cos\frac{(2q+1)\pi}{2g} = \cos\frac{(2q+1)m_1\pi}{2m} = \cos\frac{(2q+1)n_1\pi}{2n}$$

donc les racines de T_g sont bien des racines communes de T_m et T_n car $(2q+1)m_1$ et $(2q+1)n_1$ sont des entiers impairs.
Finalement, les racines communes de T_m et T_n sont exactement les racines de T_g. Comme T_m, T_n et T_g sont scindés à racines simples, on peut conclure que T_g est un pgcd de T_m et T_n.

4.b.ii Remarquons déjà que $m_1 \wedge n_1 = 1$ donc seul un des deux entiers m_1 et n_1 est pair tandis que l'autre est impair. On reprend le raisonnement de la question précédente en supposant l'existence d'une racine commune de T_m et T_g. Il existerait donc des entiers k et ℓ tels que

$$n_1(2k+1) = m_1(2\ell+1)$$

Mais ceci est impossible puisque les deux membres de cette égalité sont de parités distinctes. Ainsi T_m et T_n sont scindés et ne possèdent pas de racine commune : ils sont donc premiers entre eux.

4.b.iii Si m et n sont impairs, alors m_1 et n_1 sont également impairs. Ainsi un pgcd de T_m et T_n est T_g.
Supposons que m et n soient des puissances de 2 distinctes. Sans perte de généralité, on peut supposer $m < n$. Il existe donc des entiers naturels q et r tels que $m = 2^q$, $n = 2^r$ et $q < r$. Alors $g = m = 2^q$, $m_1 = 1$ et $n_1 = 2^{r-q}$. Ainsi m_1 est impair et n_1 est pair. D'après la question précédente, T_m et T_n sont premiers entre eux.

$\boxed{5}$ **5.a** Soit $(m, n) \in \mathbb{N}^2$. Par définition des polynômes de Tchebychev,

$$\forall \theta \in \mathbb{R},\ \mathrm{T}_n \circ \mathrm{T}_m(\cos\theta) = \mathrm{T}_n(\cos(m\theta)) = \cos(nm\theta) = \mathrm{T}_{nm}(\cos\theta)$$

Les polynômes $\mathrm{T}_n \circ \mathrm{T}_m$ et T_{nm} coïncident sur l'ensemble infini $[-1, 1]$: ils sont donc égaux. Par conséquent,

$$\mathrm{T}_n \circ \mathrm{T}_m = \mathrm{T}_{nm} = \mathrm{T}_{mn} = \mathrm{T}_m \circ \mathrm{T}_n$$

De plus, $\deg \mathrm{T}_n = n$ pour tout $n \in \mathbb{N}$ donc la famille $(\mathrm{T}_n)_{n\in\mathbb{N}}$ vérifie ($\blacktriangle$).

5.b On vérifie tout d'abord que G est stable par $\circ$. En effet, pour tout $(P, Q) \in G^2$, $\deg(P \circ Q) = \deg P \deg Q = 1$. On sait également que la loi $\circ$ est associative. Ensuite, $X \in G$ est clairement neutre pour $\circ$. Enfin, $aX + b$ avec $(a, b) \in \mathbb{C}^* \times \mathbb{C}$ est bien inversible pour la loi $\circ$ d'inverse $\frac{1}{a}X - \frac{b}{a}$. On en déduit que $(G, \circ)$ est bien un groupe.

$\boxed{6}$ **6.a** Notons a le coefficient dominant de Q. Alors le coefficient dominant de $Q \circ P_\alpha$ est a tandis que celui de $P_\alpha \circ Q$ est a^2. Comme $Q \circ P_\alpha = P_\alpha \circ Q$, $a^2 = a$ et donc $a = 1$ car $a \neq 0$. Q est donc bien unitaire.

6.b Supposons qu'il existe deux polynômes Q_1 et Q_2 de degré $n \in \mathbb{N}^*$ commutant avec P_α. Alors

$$(Q_1 - Q_2) \circ P_\alpha = Q_1 \circ P_\alpha - Q_2 \circ P_\alpha = P_\alpha \circ Q_1 - P_\alpha \circ Q_2 = (Q_1^2 + \alpha) - (Q_2^2 + \alpha) = (Q_1 - Q_2)(Q_1 + Q_2)$$

Ainsi

$$\deg((Q_1 - Q_2) \circ P_\alpha) = \deg((Q_1 - Q_2)(Q_1 + Q_2))$$

ou encore

$$2 \deg(Q_1 - Q_2) = \deg(Q_1 - Q_2) + \deg(Q_1 + Q_2)$$

Comme $\deg(Q_1 - Q_2) \neq -\infty$, on aurait alors

$$\deg(Q_1 - Q_2) = \deg(Q_1 + Q_2)$$

Mais comme Q_1 et Q_2 sont unitaires de degré n, $\deg(Q_1 - Q_2) < n$ et $\deg(Q_1 + Q_2) = n$, ce qui est contradictoire. Il existe donc au plus un polynôme de degré $n \in \mathbb{N}^*$ commutant avec P_α.
Soit $n \in \mathbb{N}^*$. On constate que X^n commute avec X^2. D'après ce qui précède, c'est donc l'unique polynôme de degré n commutant avec X^2. De plus, on voit aisément que les seuls polynômes constants commutant avec X^2 sont 0 et 1. Ainsi

$$\mathcal{C}(X^2) = \{0\} \cup \{X^n,\ n \in \mathbb{N}\}$$

6.c Il existe $(c, d, e) \in \mathbb{C}^* \times \mathbb{C}^2$ tel que $P = cX^2 + dX + e$. On cherche $U \in G$ et $\alpha \in \mathbb{C}$ tel que $U \circ P \circ U^{-1} = P_\alpha$ i.e. $U \circ P = P_\alpha \circ U$. Il existe $(a, b) \in \mathbb{C}^* \times \mathbb{C}$ tel que $U = aX + b$. Un calcul montre que

$$U \circ P = acX^2 + adX + ae + b \qquad \text{et} \qquad P_\alpha \circ U = a^2X^2 + 2bX + b^2 + \alpha$$

Ainsi la condition $U \circ P = P_\alpha \circ U$ équivaut à

$$\begin{cases} ac = a^2 \\ ad = 2b \\ ae + b = b^2 + \alpha \end{cases}$$

c'est-à-dire

$$\begin{cases} a = c \\ b = \dfrac{cd}{2} \\ \alpha = ce + \dfrac{cd}{2} - \dfrac{c^2d^2}{4} \end{cases}$$

On en déduit donc bien l'existence et l'unicité de U et α.
Si $P = T_2 = 2X^2 - 1$, on a avec les notations précédentes $c = 2$, $d = 0$ et $e = -1$, ce qui donne $a = 2$, $b = 0$, c'est-à-dire $U = 2X$, ainsi que $\alpha = -2$.

6.d Posons $U = 2X$. Soit $Q \in \mathbb{C}[X]$. D'après la question précédente, Q commute avec T_2 si et seulement si $U \circ Q \circ U^{-1}$ commute avec P_{-2}. Or $\deg U \circ Q \circ U^{-1} = \deg Q$ car $\deg U = \deg U^{-1} = 1$ et on sait qu'il existe au plus un polynôme de degré $n \in \mathbb{N}^*$ qui commute avec P_{-2}. Il existe donc également au plus un polynôme de degré $n \in \mathbb{N}^*$ qui commute avec T_2. Or, pour $n \in \mathbb{N}^*$, T_n est de degré n et commute avec T_2, c'est donc le seul polynôme de degré $n \in \mathbb{N}^*$ qui commute avec T_2. On vérifie aisément que les seuls polynômes constants qui commutent avec T_2 sont $-\frac{1}{2}$ et 1 donc

$$\mathcal{C}(T_2) = \{-1/2\} \cup \{T_n,\ n \in \mathbb{N}\}$$

$\boxed{7}$ **7.a** Soit $\alpha \in \mathbb{C}$. Supposons qu'il existe un polynôme Q de degré 3 commutant avec P_α. On sait déjà que Q est unitaire. Il existe alors $(a, b, c) \in \mathbb{C}^3$ tel que $P = X^3 + aX^2 + bX + c$. L'égalité $Q \circ P_\alpha = P_\alpha \circ Q$ donne

$$X^6 + (3\alpha + a)X^4 + (3\alpha^2 + 2\alpha a + b)X^2 + \alpha^3 + a\alpha^2 + b\alpha + c = X^6 + 2aX^5 + (a^2 + 2b)X^4 + (2ab + 2c)X^3 + (b^2 + 2ac)X^2 + 2bcX + c^2$$

En examinant les coefficients des temres de degrés impairs, on obtient $2a = 2ab + 2c = 2bc = 0$ ce qui donne $a = c = 0$. L'agalité précédente devient alors :

$$X^6 + 3\alpha X^4 + (3\alpha^2 + b)X^2 + \alpha^3 + b\alpha = X^6 + 2bX^4 + b^2X^2$$

ce qui donne notamment $\begin{cases} 3\alpha = 2b \\ 3\alpha^2 + b = b^2 \end{cases}$. On en déduit que $3\alpha^2 + \frac{3\alpha}{2} = \frac{9\alpha^2}{4}$ ce qui équivaut à $\alpha^2 + 2\alpha = 0$ et donc $\alpha \in \{0, -2\}$. Si $\alpha = 0$, alors $b = 0$ et si $\alpha = -2$, alors $b = -3$.
Réciproquement, on vérifie que X^3 commute avec $P_0 = X^2$ et que $X^3 - 3X$ commute avec $P_{-2} = X^2 - 2$.
Les seuls complexes α tels que $\mathcal{C}(P_\alpha)$ contienne un polynôme de degré 3 sont donc 0 et -2.

7.b Soit $(F_n)_{n\in\mathbb{N}}$ une suite de polynômes vérifiant (▲). Comme $\deg F_2 = 2$, la question **6.c** montre qu'il existe $U \in G$ et $\alpha \in \mathbb{C}$ tels que $U \circ F_2 \circ U^{-1} = P_\alpha$. Comme F_3 est un polynôme de degré 3 commutant avec F_2, $U \circ F_3 \circ U^{-1}$ est également un polynôme de degré 3 commutant avec $U \circ F_2 \circ U^{-1} = P_\alpha$, ce qui impose $\alpha \in \{0, -2\}$.
Supposons $\alpha = 0$. Soit $n \in \mathbb{N}^*$. Comme F_n est un polynôme de degré n qui commute avec F_2, $U \circ F_n \circ U^{-1}$ est un polynôme de degré n qui commute avec $U \circ F_2 \circ U^{-1} = P_0 = X^2$. D'après la question **6.b**, $U \circ F_n \circ U^{-1} = X^n$ i.e. $F_n = U^{-1} \circ X^n \circ U$.
Supposons $\alpha = -2$. Soit $n \in \mathbb{N}^*$. Comme F_n est un polynôme de degré n qui commute avec F_2, $U \circ F_n \circ U^{-1}$ est un polynôme de degré n qui commute avec $U \circ F_2 \circ U^{-1} = P\_2$. Mais d'après la question **6.c**, en posant $V = 2X$, $V \circ T_2 \circ V^{-1} = P_{-2}$. Ainsi, en posant $W = V^{-1} \circ U$, $W \circ F_2 \circ W^{-1} = T_2$. Mais alors $W \circ F_n \circ W^{-1}$ est un polynôme de degré n qui commute avec T_2. D'après la question **6.d**, $W \circ F_n \circ W^{-1} = T_n$ i.e. $F_n = W^{-1} \circ T_n \circ W$.

8 Supposons que $M \in GL_2(\mathbb{Z})$. Alors M est inversible et $M^{-1} \in \mathcal{M}_2(\mathbb{Z})$. De plus, $\det(M)\det(M^{-1}) = \det(I_2) = 1$. Comme M et M^{-1} sont à coefficients dans $\mathbb{Z}$, $\det(M)$ et $\det(M^{-1})$ sont des entiers. On en déduit que $\det(M) = \pm 1$.
Réciproquement, supposons que $\det(M) = \pm 1$. D'après la formule de la comatrice, $\operatorname{com}(M)^\top M = \det(M) I_n = \pm I_n$. Ainsi M est inversible et $M^{-1} = \pm \operatorname{com}(M)^\top$. Comme M est à coefficients entiers, $\operatorname{com}(M)$ l'est également. Ainsi $M^{-1} \in \mathcal{M}_2(\mathbb{Z})$ et $M \in GL_2(\mathbb{Z})$.

9 Toutes ces relations se prouvent par des récurrences doubles sans grande difficulté.

10 **10.a** Comme B est une matrice carrée de taille 2, $\chi_B = X^2 - \operatorname{tr}(B)X + \det(B) = X^2 - \sigma X + \nu$. D'après le théorème de Cayley-Hamilton :

$$B^2 = \sigma B - \nu I_2 = E_1(\sigma, \nu)B - \nu E_0(\sigma, \nu)I_2$$

Supposons qu'il existe $n \geq 2$ tel que

$$B^n = E_{n-1}(\sigma, \nu)B - \nu E_{n-2}(\sigma, \nu)I_2$$

Alors

$$\begin{aligned} B^{n+1} &= E_{n-1}(\sigma, \nu)B^2 - \nu E_{n-2}(\sigma, \nu)B \\ &= E_{n-1}(\sigma, \nu)(\sigma B - \nu I_2) - \nu E_{n-2}(\sigma, \nu)B \\ &= (\sigma E_{n-1}(\sigma, \nu) - \nu E_{n-2}(\sigma, \nu))B - \nu E_{n-1}(\sigma, \nu)I_2 \\ &= E_n(\sigma, \nu)B - \nu E_{n-1}(\sigma, \nu)I_2 \end{aligned}$$

On a donc prouvé par récurrence que

$$\forall n \geq 2,\ B^n = E_{n-1}(\sigma, \nu)B - \nu E_{n-2}(\sigma, \nu)I_2$$

Comme B est trigonalisable dans $\mathbb{C}$, sa trace et son déterminant sont respectivement la somme et le produit de ses valeurs propres complexes. Notons $\lambda \in \mathbb{C}^*$ une valeur propre de B. Alors sa seconde valeur propre est $\det(B)/\lambda = \nu/\lambda$. Par conséquent, $\sigma = \operatorname{tr}(B) = \lambda + \frac{\nu}{\lambda}$. Les valeurs propres de B^n sont alors λ^n et ν^n/λ^n. Ainsi, en vertu d'une des relations de (■),

$$\operatorname{tr}(B^n) = \lambda^n + \frac{\nu^n}{\lambda^n} = D_n(\lambda + \frac{\nu}{\lambda}, \nu) = D_n(\sigma, \nu)$$

10.b Il existe $B \in GL_2(\mathbb{Z})$ tel que $A = B^n$. Posons comme précédemment $\sigma = \operatorname{tr} B$ et $\nu = \det B$.
Comme B est à coefficients entiers, $\sigma \in \mathbb{Z}$.
D'après la question **8**, $\nu \in \{-1, 1\}$.
D'après la question précédente

$$A = B^n = E_{n-1}(\sigma, \nu) - \nu E_{n-2}(\sigma, \nu)I_2$$

On en déduit que

$$\begin{cases} a = E_{n-1}(\sigma, \nu)B_{1,1} - \nu E_{n-2}(\sigma, \nu) \\ b = E_{n-1}(\sigma, \nu)B_{1,2} \\ c = E_{n-1}(\sigma, \nu)B_{2,1} \\ d = E_{n-1}(\sigma, \nu)B_{2,2} - \nu E_{n-2}(\sigma, \nu) \end{cases}$$

Comme σ et ν sont des entiers, une récurrence double montrerait que $E_{n-1}(\sigma, \nu)$ est un entier. La deuxième ligne et la troisième ligne du système précédent montrent que $E_{n-1}(\sigma, \nu)$ divise b et c. En effectuant la différence de la première et de la quatrième ligne, on obtient que $E_{n-1}(\sigma, \nu)$ divise $a - d$.
Enfin, d'après la question précédente, $\tau = \operatorname{tr}(A) = \operatorname{tr}(B^n) = D_n(\sigma, \nu)$ et $\delta = \det(A) = \det(B^n) = \det(B)^n = \nu^n$.

10.c 10.c.i Soit α une racine du polynôme $X^2 - \sigma X + \nu$. La deuxième racine de ce polynôme est alors ν/α. De plus, $\alpha + \nu/\alpha = \sigma$. Ainsi

$$\tau = D_n(\sigma, \nu) = D_n\left(\alpha + \frac{\nu}{\alpha}, \nu\right) = \alpha^n + \frac{\nu^n}{\alpha^n}$$

puis

$$\begin{aligned}
\tau^2 - 4\delta &= \alpha^{2n} + 2\nu^n + \frac{\nu^{2n}}{\alpha^{2n}} - 4\nu^n \\
&= \left(\alpha^n - \frac{\nu^n}{\alpha^n}\right)^2 \\
&= \left(\alpha - \frac{\nu}{\alpha}\right)^2 E_{n-1}\left(\alpha + \frac{\nu}{\alpha}, \nu\right)^2 \\
&= \left(\alpha - \frac{\nu}{\alpha}\right)^2 E_{n-1}(\sigma, \nu)^2
\end{aligned}$$

De plus,

$$\sigma^2 - 4\nu = \left(\alpha + \frac{\nu}{\alpha}\right)^2 - 4\nu = \left(\alpha - \frac{\nu}{\alpha}\right)^2$$

On obtient bien

$$\tau^2 - 4\delta = p^2(\sigma^2 - 4\nu)$$

On en déduit en particulier que

$$\nu = \frac{\sigma^2}{4} - \frac{\tau^2 - 4\delta}{4p^2}$$

Par ailleurs,

$$\begin{aligned}
ru - st &= \frac{1}{4}\left(\frac{\sigma^2}{-}\frac{(a-d)^2}{p^2}\right) - \frac{bc}{p^2} \\
&= \frac{\sigma^2}{4} - \frac{(a-d)^2 + 4bc}{4p^2} \\
&= \frac{\sigma^2}{4} - \frac{(a+d)^2 - 4(ad - bc)}{4p^2} \\
&= \frac{\sigma^2}{4} - \frac{\tau^2 - 4\delta}{4p^2} = \nu
\end{aligned}$$

On sait que p divise b et c donc s et t sont entiers. Comme p divise $a - d$ et $\sigma \in \mathbb{Z}$, $\alpha = 2r$ et $\beta = 2u$ sont entiers. Mais $ru = st + \nu$ est également entier. On en déduit que 4 divise $\alpha\beta$. Ainsi 2 divise α ou β car il est premier. Si 2 divise α, alors r est entier mais alors $r + u = \sigma \in \mathbb{Z}$ donc u est également entier. De même, si 2 divise β, r et u sont entiers. Finalement, $(p, q, r, s, t) \in \mathbb{Z}^4$ i.e. $B \in \mathcal{M}_2(\mathbb{Z})$. Mais $\det(B) = ru - st = \nu = \pm 1$ donc $B \in GL_2(\mathbb{Z})$ d'après la question **8**.

10.c.ii D'après la question **10.a**,

$$B^n = E_{n-1}(\sigma, \nu)B - \nu E_{n-2}(\sigma, \nu)I_2 = pB - \nu E_{n-2}(\sigma, \nu)I_2 = \begin{pmatrix} x & b \\ c & y \end{pmatrix}$$

avec $x = pr - \nu E_{n-2}(\sigma, \nu)$ et $y = pu - \nu E_{n-2}(\sigma, \nu)$.
D'après cette même question, $x + y = \mathrm{tr}(B^n) = D_n(\sigma, \nu) = \tau = a + d$. De plus, $x - y = p(r - u) = a - d$. On en déduit que $x = a$ et $y = d$ et enfin que $A = B^n$.

10.d On doit choisir $p = E_2(\sigma, \nu) = \sigma^2 - \nu$ tel que p divise 10 et 5 (et $7 - 7 = 0$). On a donc $p = 1$ ou $p = 5$. De plus, $\nu = \pm 1$ et $p + \nu = \sigma^2$ doit être un carré d'entier. On a donc $p = 5$ et $\nu = -1$ puis $\sigma = 2$ par exemple. On obtient alors $r = 1$, $s = 2$, $t = 1$ et $u = 1$. On pose donc $B = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$. On vérifie alors que $B^3 = A$.