Deuxième composition de mathématiques
Centrale-Supélec – MP – 2014

Polynômes de Tchebychev et de Dickson, applications

PARTIE I - Définitions et propriétés usuelles

Les polynômes de Tchebychev de première espèce $(T_n)_{n\in\mathbf{N}}$ sont définis par la relation

$$\forall n \in \mathbf{N}\,,\ \forall \theta \in \mathbf{R}\,,\quad T_n(\cos(\theta)) = \cos(n\theta)\ .$$

On ne demande pas de justifier l'existence et l'unicité de la famille de polynômes définie par cette relation.

I.A - Polynômes de première espèce

I.A.1) Déterminer T_0, T_1, T_2 et T_3.

I.A.2) En remarquant que pour tout réel θ, on a $e^{in\theta} = (e^{i\theta})^n$, montrer

$$\forall n \in \mathbf{N}\,,\quad T_n = \sum_{0\leq k\leq n/2} \binom{n}{2k} (X^2-1)^k X^{n-2k}\ .$$

I.A.3) Montrer que la suite $(T_n)_{n\in\mathbf{N}}$ vérifie la relation de récurrence

$$\forall n \in \mathbf{N}\,,\quad T_{n+2} = 2XT_{n+1} - T_n \tag{1}$$

En déduire, pour tout entier naturel n, le degré et le coefficient dominant de T_n. Retrouver ce résultat avec l'expression de la question I.A.2).

I.A.4) En utilisant la relation (1), écrire en langage Python une fonction T prenant en argument un entier naturel n et renvoyant la liste des $n+1$ coefficients du polynôme T_n, ordonnée du degré 0 au degré n.

I.A.5) Montrer que, pour tout entier naturel non nul n, le polynôme T_n est scindé sur $\mathbf{R}$, à racines simples appartenant à $]-1;1[$. Déterminer les racines de T_n.

I.B - Polynômes de deuxième espèce

On définit les polynômes de Tchebychev de deuxième espèce $(U_n)_{n\in\mathbf{N}}$ par

$$\forall n \in \mathbf{N}\,,\quad U_n = \frac{1}{n+1} T'_{n+1}\ .$$

I.B.1) Montrer

$$\forall n \in \mathbf{N}\,,\ \forall \theta \in \mathbf{R}\setminus \pi\mathbf{Z}\,,\quad U_n(\cos(\theta)) = \frac{\sin((n+1)\theta)}{\sin(\theta)}\ .$$

I.B.2) En déduire les propriétés suivantes :

a) La suite $(U_n)_{n\in\mathbf{N}}$ vérifie la même relation de récurrence (1) que la suite $(T_n)_{n\in\mathbf{N}}$.

b) Pour tout entier naturel non nul n, le polynôme U_n est scindé sur $\mathbf{R}$ à racines simples appartenant à $]-1;1[$. Déterminer les racines de U_n.

PARTIE II - Arithmétique des polynômes de Tchebychev

II.A - Division euclidienne

II.A.1) Montrer

$$\begin{cases} T_m \cdot T_n = \dfrac{1}{2}\left(T_{n+m} + T_{n-m}\right) & \text{pour tous entiers } 0 \leq m \leq n \\ T_m \cdot U_{n-1} = \dfrac{1}{2}\left(U_{n+m-1} + U_{n-m-1}\right) & \text{pour tous entiers } 0 \leq m < n\ . \end{cases}$$

II.A.2) Pour m et n entiers naturels tels que $m \leq n$, on se propose de déterminer le quotient $Q_{n,m}$ et le reste $R_{n,m}$ de la division euclidienne de T_n par T_m.

a) On suppose $m < n < 3m$. Montrer

$$Q_{n,m} = 2T_{n-m} \quad \text{et} \quad R_{n,m} = -T_{|n-2m|}\ .$$

b) Déterminer $Q_{n,m}$ et $R_{n,m}$ lorsque n est de la forme $(2p+1)m$ avec $p \in \mathbf{N}^*$.

c) On suppose $m > 0$ et que n n'est pas le produit de m par un entier impair. Montrer qu'il existe un unique entier $p \geq 1$ tel que $|n - 2pm| < m$ et qu'on a

$$Q_{n,m} = 2\left(T_{n-m} - T_{n-3m} + \cdots + (-1)^{p-1}T_{n-(2p-1)m}\right) \quad \text{et} \quad R_{n,m} = (-1)^p T_{|n-2pm|}\ .$$

II.B - Plus grand commun diviseur

Dans toute cette sous-partie II.B, on fixe deux entiers naturels m et n.

II.B.1) Soit h le pgcd dans $\mathbf{N}$ de $m+1$ et $n+1$. En examinant les racines communes à U_n et U_m, montrer que U_{h-1} est un pgcd dans $\mathbf{R}[X]$ de U_n et U_m.

II.B.2) Soit $g > 0$ le pgcd de m et n. On pose $m_1 = m/g$ et $n_1 = n/g$.

a) Montrer que si m_1 et n_1 sont impairs, alors T_g est un pgcd de T_n et T_m.

b) Montrer que si l'un des deux entiers m_1 ou n_1 est pair, alors T_n et T_m sont premiers entre eux.

c) Que peut-on dire des pgcd de T_n et T_m lorsque m et n sont impairs ? Lorsque n et m sont deux puissances de 2 distinctes ?

PARTIE III - Un théorème

Dans cette partie, on munit l'ensemble $\mathbf{C}[X]$ des polynômes complexes de la loi de composition interne associative donnée par la composition, notée $\circ$. Plus précisément, étant donné P et Q dans $\mathbf{C}[X]$, si $P = \sum_{k=0}^{+\infty} p_k X^k$, la suite $(p_k)_{k\in\mathbf{N}}$ étant nulle à partir d'un certain rang, on a

$$P \circ Q = \sum_{k=0}^{+\infty} p_k Q^k\ .$$

On dit que les polynômes P et Q commutent si $P \circ Q = Q \circ P$. On note $\mathcal{C}(P)$ l'ensemble des polynômes complexes qui commutent avec le polynôme P, i.e.

$$\mathcal{C}(P) = \{Q \in \mathbf{C}[X] \,|\, P \circ Q = Q \circ P\}\ .$$

On cherche dans cette partie les familles $(F_n)_{n\in\mathbf{N}}$ de polynômes complexes vérifiant

$$\forall n \in \mathbf{N}\,,\ \deg(F_n) = n \quad \text{et} \quad \forall (m,n) \in \mathbf{N}^2\,,\ F_n \circ F_m = F_m \circ F_n\ . \tag{2}$$

Il est clair que la famille $(X^n)_{n\in\mathbf{N}}$ convient.
On note G l'ensemble des polynômes complexes de degré 1, et pour α dans $\mathbf{C}$, on pose $P_\alpha = X^2+\alpha$.

III.A - Préliminaires

III.A.1) Montrer que la famille $(T_n)_{n\in\mathbf{N}}$ vérifie la propriété (2). On pourra comparer $T_n \circ T_m$ et T_{mn}.

III.A.2) Vérifier que G est un groupe pour la loi $\circ$.
L'inverse pour la loi $\circ$ d'un élément U de G sera noté U^{-1}.

III.B - Commutant de X^2 et T_2

III.B.1) Soit α dans $\mathbf{C}$ et Q un polynôme complexe non constant qui commute avec P_α. Montrer que Q est unitaire.

III.B.2) En déduire que, pour tout entier $n \geq 1$, il existe au plus un polynôme de degré n qui commute avec P_α. Déterminer $\mathcal{C}(X^2)$.

III.B.3) Soit P un polynôme complexe de degré 2. Justifier l'existence et l'unicité de U dans G et α dans $\mathbf{C}$ tels que $U \circ P \circ U^{-1} = P_\alpha$. Déterminer ces deux éléments lorsque $P = T_2$.

III.B.4) Justifier $\mathcal{C}(T_2) = \{-1/2\} \cup \{T_n \,|\, n \in \mathbf{N}\}$.

III.C

III.C.1) Montrer que les seuls complexes α tels que $\mathcal{C}(P_\alpha)$ contienne un polynôme de degré trois sont 0 et -2.

III.C.2) En déduire le théorème de Block et Thielmann : si $(F_n)_{n\in\mathbf{N}}$ vérifie (2), alors il existe U dans G tel que

$$\forall n \in \mathbf{N}^*\,,\ F_n = U^{-1} \circ X^n \circ U \quad \text{ou} \quad \forall n \in \mathbf{N}^*\,,\ F_n = U^{-1} \circ T_n \circ U\ .$$

PARTIE IV - Puissances dans $\mathrm{GL}_2(\mathbf{Z})$

Dans toute cette partie, on note $\mathrm{GL}_2(\mathbf{Z})$ l'ensemble des éléments inversibles de l'anneau $\mathscr{M}_2(\mathbf{Z})$, muni de son addition et de sa multiplication usuelle.

IV.A - Justifier qu'un élément M de $\mathscr{M}_2(\mathbf{Z})$ appartient à $\mathrm{GL}_2(\mathbf{Z})$ si et seulement si $|\det(M)| = 1$.

IV.B - On introduit les polynômes de Dickson de première et deuxième espèce, $(D_n)_{n\in\mathbf{N}}$ et $(E_n)_{n\in\mathbf{N}}$, définis sous la forme de fonctions polynomiales de deux variables par

$$D_0(x,a) = 2 \quad D_1(x,a) = x \quad E_0(x,a) = 1 \quad E_1(x,a) = x$$

puis, pour tout entier $n \in \mathbf{N}$,

$$D_{n+2}(x,a) = xD_{n+1}(x,a) - aD_n(x,a) \quad \text{et} \quad E_{n+2}(x,a) = xE_{n+1}(x,a) - aE_n(x,a)\ .$$

Justifier la relation suivante avec les polynômes de Tchebychev

$$\forall (x,a) \in \mathbf{C}^2\,, \quad D_n(2xa,a^2) = 2a^nT_n(x) \quad \text{et} \quad E_n(2xa,a^2) = a^nU_n(x)$$

ainsi que les deux relations suivantes, valables pour tout entier naturel n et tout $(x,a) \in \mathbf{C}^* \times \mathbf{C}$

$$D_n\left(x+\frac{a}{x},a\right) = x^n + \frac{a^n}{x^n} \quad \text{et} \quad \left(x-\frac{a}{x}\right) E_n\left(x+\frac{a}{x},a\right) = x^{n+1} - \frac{a^{n+1}}{x^{n+1}} \ . \tag{3}$$

IV.C - Dans cette sous-partie, on cherche une condition nécessaire et suffisante pour qu'un élément A de $\mathrm{GL}_2(\mathbf{Z})$ soit une puissance n-ième dans $\mathrm{GL}_2(\mathbf{Z})$, c'est-à-dire pour qu'il existe une matrice B dans $\mathrm{GL}_2(\mathbf{Z})$ telle que $A = B^n$. Dans toute la suite, on notera

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \tau = \mathrm{Tr}(A) \quad \delta = \det(A) \ .$$

IV.C.1) Soit B dans $\mathrm{GL}_2(\mathbf{Z})$. On note, dans cette question uniquement, $\sigma = \mathrm{Tr}(B)$ et $\nu = \det(B)$. Montrer pour tout $n \geq 2$, l'égalité

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

où I_2 est la matrice identité d'ordre 2.
Établir $\mathrm{Tr}(B^n) = D_n(\sigma,\nu)$.

IV.C.2) En déduire que si A est une puissance n-ième ($n \geq 2$) dans $\mathrm{GL}_2(\mathbf{Z})$, alors il existe σ dans $\mathbf{Z}$ et ν dans $\{-1,1\}$ tels que

i. $E_{n-1}(\sigma,\nu)$ divise b, c et $a-d$. On justifiera brièvement que $E_{n-1}(\sigma,\nu)$ est bien un entier.

ii. $\tau = D_n(\sigma,\nu)$ et $\delta = \nu^n$.

IV.C.3) On va maintenant établir la réciproque.
Soit A un élément de $\mathrm{GL}_2(\mathbf{Z})$ pour lequel il existe σ dans $\mathbf{Z}$ et ν dans $\{-1,1\}$ vérifiant les deux conditions précédentes i. et ii.. Pour simplifier, on note $p = E_{n-1}(\sigma,\nu)$. On définit alors une matrice $B = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ avec

$$r = \frac{1}{2}\left(\sigma + \frac{a-d}{p}\right) \quad s = \frac{b}{p} \quad t = \frac{c}{p} \quad u = \frac{1}{2}\left(\sigma - \frac{a-d}{p}\right) \ .$$

a) En introduisant une racine complexe du polynôme $X^2 - \sigma X + \nu$ et à l'aide de (3), montrer

$$\tau^2 - 4\delta = p^2(\sigma^2 - 4\nu) \quad \text{puis} \quad ru - st = \nu \ .$$

En déduire que B appartient à $\mathrm{GL}_2(\mathbf{Z})$.

b) Montrer $A = B^n$.

IV.C.4) Montrer que la matrice $A = \begin{pmatrix} 7 & 10 \\ 5 & 7 \end{pmatrix}$ est un cube dans $\mathrm{GL}_2(\mathbf{Z})$ et déterminer une matrice B dans $\mathrm{GL}_2(\mathbf{Z})$ telle que $B^3 = A$.

Deuxième composition de mathématiques – Centrale-Supélec – MP – 2014

PARTIE I - Définitions et propriétés usuelles

I.A - Polynômes de première espèce

I.A.1) D'après les formules de trigonométrie usuelles les polynômes 1, X, $2X^2-1$ et $4X^3-3X$ vérifient respectivement la relation donnée pour n valant 0, 1, 2 et 3 respectivement. Par l'unicité admise, on en déduit $\boxed{T_0=1,\ T_1=X,\ T_2=2X^2-1 \text{ et } T_3=4X^3-3X.}$

I.A.2) Soit θ un réel et n un entier naturel. On a, en utilisant la formule de de Moivre rappelée dans l'énoncé, et en notant $x=\cos(\theta)$:

$$T_n(x)=\mathrm{Re}\left((x+i\sin(\theta))^n\right)=\sum_{0\leq k\leq n/2}\binom{n}{2k}(-1)^k\sin^{2k}(\theta)x^{n-2k}$$

par linéarité de la partie réelle. Et donc, puisqu'on a $\sin^2(\theta)=1-x^2$, il vient

$$T_n(x)=\sum_{0\leq k\leq n/2}\binom{n}{2k}(x^2-1)^k x^{n-2k}\ .$$

Cette relation est vraie pour tout x dans l'image de cos, i.e. de valeur absolue inférieure à 1. Or l'égalité de deux fonctions polynomiales sur un nombre infini de valeurs de la variable entraîne l'égalité des deux polynômes. On en déduit $\boxed{T_n=\sum_{0\leq k\leq n/2}\binom{n}{2k}(X^2-1)^kX^{n-2k}.}$

I.A.3) Soit n un entier naturel et θ un réel. On a

$$\cos((n+1\pm 1)\theta)=\cos((n+1)\theta)\cos(\theta)\mp\sin((n+1)\theta)\sin(\theta)$$

et donc, en additionnant ces deux relations, $T_n(\cos(\theta))+T_{n+2}(\cos(\theta))=2\cos(\theta)T_{n+1}(\cos(ta))$. Il en résulte que, pour x dans $[-1;1]$, on a $T_n(x)+T_{n+2}(x)=2xT_{n+1}(x)$ et donc, par égalité de fonctions polynomiales sur un nombre infini de valeurs de la variable $\boxed{T_{n+2}=2XT_{n+1}-T_n.}$ Puisque T_0 est de degré 0 et de coefficient dominant 1 et T_1 de degré 1 et de coefficient dominant 1, une récurrence immédiate montre que

$\boxed{\text{pour tout entier naturel } n,\ T_n \text{ est de degré } n \text{ et de coefficient dominant 1 si } n=0 \text{ et } 2^{n-1} \text{ sinon.}}$

Dans l'expression de la question I.A.2), il n'y a aucun terme de degré strictement supérieur à n et celui de degré n est $\displaystyle\sum_{0\leq k\leq n/2}\binom{n}{2k}$. Pour $n=0$ on trouve $\displaystyle\binom{0}{0}$, i.e. 1. Pour $n>0$ on trouve la somme des termes pairs de la n^{e} ligne du triangle de Pascal, i.e. $\dfrac{1}{2}\left((1+1)^n+(1-1)^n\right)$, soit encore 2^{n-1}, ce qui est $\boxed{\text{le résultat précédent.}}$

I.A.4) On initialise une liste contenant les listes des coefficients de T_0 et de T_1 sous forme de listes. Ensuite on transforme la liste de façon à ce qu'à chaque itération elle contienne les listes des

coefficients de T_k et T_{k+1}, en utilisant la formule de récurrence. On termine en affichant la dernière liste obtenue.

```
#! /usr/bin/python3
def T(n):
    T0=[1]
    T1=[0,1]
    c=[T0,T1]
    if n<2: return c[n]
    else:
        k=1
        while k<n:
            l=[-c[0][0]]
            for i in range(1,k):
                l.append(2*c[1][i-1]-c[0][i])
            l.extend([2*c[1][k-1],2*c[1][k]])
            c=[c[1],l]
            k+=1
    return c[1]

def T_par(n):
    P=I=[1]
    for k in range(n//2):
        P=[-P[0]]+[2*I[i-1]-P[i] for i in range(1,k+1)]+[2*I[k]]
        if 2*k<n-2:
            I=[2*P[i]-I[i] for i in range(k+1)]+[2*P[k+1]]
    T=[P,I][n%2]
    return [T[k//2] if k%2==n%2 else 0 for k in range(n+1)]

import numpy as np
def T_rec(n):
    if n<2 : return [0,1][-n-1:]
    else :
        a=np.array([0]+[2*k for k in T_rec(n-1)])
        b=a-np.array(T_rec(n-2)+[0,0])
        return b.tolist()
```

Les deux variantes sont obtenues en tenant compte de la parité des polynômes et en utilisant les listes en compréhension, d'une part, et en utilisant la récursivité, la librairie numpy et ses objets ndarray et la possibilité de les additionner comme des vecteurs (en tenant compte du fait qu'il faut qu'ils soient de même taille) et de les transformer en liste grâce à la méthode tolist. La variante tenant compte de la parité est environ deux fois plus rapide. Celle qui est récursive est par contre beaucoup plus lente, et ce de façon rédhibitoire pour n valant quelques dizaines.

I.A.5) De par la définition de T_n, pour n entier naturel non nul et k dans $[\![0;n-1]\!]$, $\cos\left(\frac{(2k+1)\pi}{2n}\right)$ est racine de T_n. Comme cos réalise une bijection de $]0;\pi[$ sur $]-1;1[$, les réels précédents forment n racines distinctes T_n qui est de degré n et est donc simplement scindé sur $\mathbf{R}$. Par conséquent

$\boxed{T_n \text{ est scindé sur } \mathbf{R}, \text{ à racines simples appartenant à }]-1;1[, \text{ données par } \left(\cos\left(\frac{(2k+1)\pi}{2n}\right)\right)_{0\leq k<n}.}$

I.B - Polynômes de deuxième espèce

I.B.1) Soit n dans $\mathbf{N}$ et θ dans $\mathbf{R}$. Par dérivation de la relation de définition des polynômes de Tchebychev de première espèce, ce qui est licite car les fonctions polynomiales et cos sont de classe C^∞ sur $\mathbf{R}$, il vient $-\sin(\theta)T_n'(\cos(\theta)) = -n\sin(n\theta)$ et donc, si θ n'appartient pas à $\pi\mathbf{Z}$ et donc n'annule pas sin, $\boxed{U_n(\cos(\theta)) = \frac{\sin((n+1)\theta)}{\sin(\theta)}.}$

I.B.2) a) Soit n un entier naturel et θ un réel n'appartenant pas à $\pi\mathbf{Z}$. On a

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

et donc, en additionnant ces deux relations et en divisant par $\sin(\theta)$,

$$U_n(\cos(\theta)) + U_{n+2}(\cos(\theta)) = 2\cos(\theta)U_{n+1}(\cos(\theta)) \ .$$

Il en résulte que, pour x dans $]-1;1[$, on a $U_n(x) + U_{n+2}(x) = 2xU_{n+1}(x)$ et donc, par égalité de fonctions polynomiales sur un nombre infini de valeurs de la variable
$\boxed{U_{n+2} = 2XU_{n+1} - U_n.}$

b) Il résulte du théorème de Rolle que la dérivée d'un polynôme simplement scindé sur $\mathbf{R}$ l'est aussi et que ses racines sont incluses strictement dans l'intervalle où se trouvent les racines du polynôme dont il est la dérivée. De plus l'expression précédente permet de préciser que les quantités $\cos\left(\frac{k\pi}{n+1}\right)$ pour k dans $[\![1;n]\!]$ sont racines de U_n. Comme cos réalise une bijection de $]0;\pi[$ sur $]-1;1[$, on en déduit que

$\boxed{U_n \text{ est scindé sur } \mathbf{R} \text{ à racines simples appartenant à }]-1;1[, \text{ données par } \left(\cos\left(\frac{k\pi}{n+1}\right)\right)_{1\leq k\leq n}.}$

PARTIE II - Arithmétique des polynômes de Tchebychev

II.A - Division euclidienne

II.A.1) Soit θ un réel dans $]0;\pi[$ et m et n deux entiers naturels vérifiant $m \leq n$. Il résulte des formules de trigonométrie en notant $x = \cos(\theta)$,

$$\begin{aligned} T_m(x)T_n(x) &= \cos(m\theta)\cos(n\theta) = \frac{1}{2}\left(\cos((n+m)\theta) + \cos((n-m)\theta)\right) \\ &= \frac{1}{2}\left(T_{n+m}(x) + T_{n-m}(x)\right) \end{aligned}$$

et, si $m < n$,

$$\begin{aligned}\sin(\theta)T_m(x)U_{n-1}(x) &= \cos(m\theta)\sin(n\theta) = \frac{1}{2}\left(\sin((n+m)\theta) + \sin((n-m)\theta)\right)\\ &= \frac{\sin(\theta)}{2}\left(U_{n+m-1}(x) + U_{n-m-1}(x)\right)\ .\end{aligned}$$

Par non-nullité de $\sin(\theta)$ et bijectivité de cos de $]0;\pi[$ sur $]-1;1[$, on en déduit l'égalité sur $]-1;1[$ de fonctions polynomiales et donc des polynômes associés, i.e.

$$\boxed{T_m \cdot T_n = \frac{1}{2}\left(T_{n+m} + T_{n-m}\right) \text{ et, si } m < n,\ T_m \cdot U_{n-1} = \frac{1}{2}\left(U_{n+m-1} + U_{n-m-1}\right).}$$

II.A.2) a) Si $n \geq 2m$, on a $0 \leq m \leq n-m$ et donc la formule précédente donne $2T_mT_{n-m} = T_n + T_{n-2m}$. Si $n < 2m$, on a $0 \leq n-m \leq m$ et la formule donne $2T_{n-m}T_m = T_n + T_{2m-n}$. Or on a $\deg(T_{|n-2m|}) = |n-2m| < m = \deg(T_m)$ et donc par unicité de la division euclidienne, il vient $\boxed{Q_{n,m} = 2T_{n-m} \text{ et } R_{n,m} = -T_{|n-2m|}.}$

b) Le cas $n \geq 2m$ précédent fournit aussi $T_{3m} = 2T_{2m}T_m - T_m$ et, plus généralement, pour p entier naturel non nul, $T_{(2p+1)m} = 2T_{2pm}T_m - T_{(2p-1)m}$, de sorte que, par une récurrence immédiate il vient $\boxed{Q_{(2p+1)m,m} = (-1)^pT_0 + 2\sum_{k=0}^{p-1}(-1)^kT_{2(p-k)m} \text{ et } R_{(2p+1)m,m} = 0.}$

c) Pour p dans $\mathbf{N}^*$, on a $|n-2pm| < m \iff p < \dfrac{n+m}{2m} < p+1$. Or $m < n$ et n n'est pas le produit de m par un entier impair et donc $\dfrac{n+m}{2m}$ est supérieur à 1 et n'est pas entier. Il en résulte qu'il existe $\boxed{\text{un unique entier } p \geq 1 \text{ tel que } |n-2pm| < m, \text{ à savoir } \left[\frac{n+m}{2m}\right].}$

La formule précédente donne également, en convenant qu'une somme vide est nulle,

$$2\sum_{k=0}^{p-2}(-1)^kT_{n-(2k+1)m}T_m = \sum_{k=0}^{p-2}(-1)^k(T_{n-2km} + T_{n-2(k+1)m}) = T_n + (-1)^{p-2}T_{n-2(p-1)m}$$

par somme télescopique, et donc puisque $m < n - 2(p-1)m < 3m$, il vient en utilisant le cas $m < n < 3m$,

$$2\sum_{k=0}^{p-1}(-1)^kT_{n-(2k+1)m}T_m = T_n + (-1)^{p-1}T_{|n-2pm|}$$

et donc, puisque $\deg(T_{|n-2pm|}) = |n-2pm| < m = \deg(T_m)$, par unicité de la division euclidienne on a

$$\boxed{Q_{n,m} = 2\left(T_{n-m} - T_{n-3m} + \cdots + (-1)^{p-1}T_{n-(2p-1)m}\right) \text{ et } R_{n,m} = (-1)^pT_{|n-2pm|}.}$$

II.B - Plus grand commun diviseur

II.B.1) Puisque U_n et U_m sont simplement scindés, leur pgcd est le produit de leurs facteurs du premier degré commun, i.e. des monômes du type $X - \alpha$ avec α racine commune à U_n et U_m.

D'après I.B.2), ces racines sont de la forme $\cos\left(\frac{k\pi}{n+1}\right)$ et $\cos\left(\frac{\ell\pi}{m+1}\right)$ avec $1 \leq k \leq n$ et $1 \leq \ell \leq m$. Comme cos est bijective sur $[0;\pi]$, deux telles racines sont égales si et seulement si $\frac{k}{n+1} = \frac{\ell}{m+1}$, i.e. $k(m+1) = \ell(n+1)$ ou encore $k\frac{m+1}{h} = \ell\frac{n+1}{h}$. Comme $\frac{m+1}{h}$ et $\frac{n+1}{h}$ sont des entiers premiers entre eux, on a alors, d'après le lemme de Gauss, $\frac{m+1}{h} \mid \ell$ et $\frac{n+1}{h} \mid k$ et on en conclut que l'égalité $k\frac{m+1}{h} = \ell\frac{n+1}{h}$ est équivalente à l'existence de d entier tel que $\ell = d\frac{m+1}{h}$ et $k = d\frac{n+1}{h}$ avec $1 \leq d < h$, de telle sorte que la racine commune soit alors $\cos\left(\frac{d\pi}{h}\right)$, avec la convention qu'il n'en existe pas si $h = 1$. Ainsi les racines communes à U_n et U_m sont celles de U_{h-1} (éventuellement inexistantes si $h = 1$), qui est également simplement scindé (ou constant). Par conséquent $\boxed{U_{h-1} \text{ est un pgcd dans } \mathbf{R}[X] \text{ de } U_n \text{ et } U_m.}$

II.B.2) a) D'après I.A.5) et puisque T_n et T_m sont simplement scindés, leur pgcd est le produit des monômes du type $X - \alpha$ avec α de la forme $\cos\left(\frac{(2k+1)\pi}{2n}\right)$ et aussi $\cos\left(\frac{(2\ell+1)\pi}{2m}\right)$ avec $0 \leq k < n$ et $0 \leq \ell < m$. Par bijectivité de cos sur $[0;\pi]$, en utilisant le lemme de Gauss, on en conclut $\frac{2k+1}{n_1} = \frac{2\ell+1}{m_1} \in [\![1; 2g-1]\!]$ et donc les racines communes de T_m et T_n sont celles de T_g. Comme ce dernier est simplement scindé, $\boxed{T_g \text{ est un pgcd de } T_n \text{ et } T_m.}$

b) Si m_1 ou n_1 est pair, dans le raisonnement précédent, $\frac{2k+1}{n_1}$ ou $\frac{2\ell+1}{m_1}$ ne saurait être entier puisque quotient d'un nombre impair et d'un nombre pair. Il en résulte que T_n et T_m n'ont aucune racine en commun et donc, puisqu'ils sont simplement scindés,
$\boxed{T_n \text{ et } T_m \text{ sont premiers entre eux.}}$

c) Si m et n sont impairs, alors m_1 et n_1 aussi et donc
$\boxed{\text{les pgcd de } T_m \text{ et } T_n \text{ sont les multiples non nuls de } T_g.}$
Si n et m sont deux puissances de 2 distinctes, alors l'un des deux divise l'autre et le quotient du plus grand par le plus petit, qui est aussi le pgcd des deux, est une puissance non nulle de 2, donc est pair. Il en résulte que les deux polynômes sont premiers entre eux et donc $\boxed{\text{les pgcd de } T_m \text{ et } T_n \text{ sont les constantes non nulles.}}$

PARTIE III - Un théorème

III.A - Préliminaires

III.A.1) Soit θ un réel et n et m deux entiers naturels. Par définition des polynômes de Tchebychev on a

$$T_n \circ T_m(\cos(\theta)) = T_n(\cos(m\theta)) = \cos(nm\theta) = T_{nm}(\cos(\theta))$$

et donc, par égalité des fonctions polynomiales associées sur $[-1;1]$, $T_n \circ T_m = T_{nm}$ et, par commutativité de la multiplication dans $\mathbf{N}$, $T_n \circ T_m = T_m \circ T_n$. Il résulte alors de I.A.3) que la famille $\boxed{(T_n)_{n\in\mathbf{N}} \text{ vérifie la propriété (2).}}$

III.A.2) Comme $(\mathbf{C}[X], \circ)$ est un magma associatif unifère, il s'agit de vérifier que G en est un sous-magma, qu'il contient le neutre et qu'en sus tout élément de G admet un inverse dans G. Pour a, b, c, d complexes on a $(aX+b)\circ(cX+d) = acX + ad + b$. On en déduit que $(G, \circ)$ est un sous-magma puisque si a et c sont non nuls alors ac l'est aussi. L'élément neutre étant X, il est de degré 1 et donc appartient à G. La formule précédente montre que $a^{-1}(X-b)$ est l'inverse de $aX+b$ et donc $\boxed{G \text{ est un groupe pour la loi } \circ.}$

Remarque : en fait l'application $\varphi : aX+b \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ est un morphisme de groupes entre G et le sous-groupe de $\mathrm{GL}_2(\mathbf{C})$ formé des matrices dont la transposée fixe e_2. On pourrait donc vérifier que G est un groupe en utilisant un transport de structure. Ceci est un cas particulier de l'étude des homographies. Pour x réel et P dans G, on a, en identifiant le polynôme et la fonction polynomiale associée, $\varphi(P)\begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} P(x) \\ 1 \end{pmatrix}$.

III.B - Commutant de X^2 et T_2

III.B.1) Puisque Q n'est pas constant le coefficient dominant de $Q\circ P_\alpha$ est celui de Q et celui de $P_\alpha \circ Q$ en est le carré. Comme ce dernier n'est pas nul, c'est qu'il est égal à 1, i.e. $\boxed{Q \text{ est unitaire.}}$

III.B.2) Soit n un entier vérifiant $n \geq 1$ et P et Q des polynômes de degré n qui commutent avec P_α. Alors P et Q sont unitaires, donc $P+Q$ est de degré n et $P-Q$ de degré strictement inférieur à n. De plus on a

$$(P-Q)\circ P_\alpha = P\circ P_\alpha - Q\circ P_\alpha = P^2 + \alpha - Q^2 - \alpha = (P-Q)\cdot(P+Q)\,.$$

Or le degré du membre de gauche est le double de celui de $P-Q$ et celui du membre droite est n plus celui de $P-Q$. Il en résulte $P-Q=0$, i.e. il existe

$\boxed{\text{au plus un polynôme de degré } n \text{ commutant à } P_\alpha.}$

Pour $\alpha = 0$ on en conclut que les polynômes non constants commutant à X^2 sont ceux qui appartiennent à la base canonique, ainsi que remarqué en préambule. Ceux qui sont constants sont ceux associés à une constante égale à son propre carré et donc

$\boxed{\mathcal{C}(X^2) = \{0\} \cup \{X^n \,|\, n \in \mathbf{N}\}.}$

III.B.3) De par la définition de $\circ$, on vérifie directement qu'on a, pour A et B dans $\mathbf{C}[X]$, $(A\circ B)' = A'\circ B \cdot B'$. De plus le degré d'un composé étant le produit des degrés, pour tout élément U de G le degré de $U\circ P\circ U^{-1}$ est égal à 2, et de plus ce polynôme est caractérisé par son polynôme dérivé et par sa valeur en 0. Ainsi pour U dans G et α dans $\mathbf{C}$, puisque les dérivés d'éléments de G sont constants et donc en particulier U' et $(U^{-1})'$, avec de plus $(U\circ U^{-1})' = 1 = U'\cdot(U^{-1})'$, il vient

$$\begin{aligned}
U\circ P\circ U^{-1} = P_\alpha &\iff \left(U\circ P\circ U^{-1}\right)' = 2X \quad \& \quad \alpha = U\circ P\circ U^{-1}(0) \\
&\iff U'\cdot P'\circ U^{-1}\cdot (U')^{-1} = 2X \quad \& \quad \alpha = U\circ P\circ U^{-1}(0) \\
&\iff P'\circ U^{-1} = 2X \quad \& \quad \alpha = U\circ P\circ U^{-1}(0) \\
&\iff P' = 2U \quad \& \quad \alpha = U\circ P\circ U^{-1}(0) \\
&\iff U = \frac{1}{2}P' \quad \& \quad \alpha = U\circ P\circ U^{-1}(0)
\end{aligned}$$

d'où $\boxed{\text{l'existence et l'unicité de } U \text{ et } \alpha.}$

Dans le cas de T_2, on a $U = \frac{1}{2}T_2' = U_1 = 2X$ et $\alpha = 2T_2\left(\frac{1}{2}0\right) = -2$: $\boxed{U = 2X \text{ et } \alpha = -2.}$

III.B.4) Soit P dans $\mathcal{C}(T_2)$ et U et α comme précédemment. Alors on a

$$U \circ P \circ U^{-1} \circ P_\alpha = U \circ P \circ T_2 \circ U^{-1} = U \circ T_2 \circ P \circ U^{-1} = P_\alpha \circ U \circ P \circ U^{-1}$$

et donc si P et Q sont dans $\mathcal{C}(T_2)$, non constants et de même degré, alors $U \circ P \circ U^{-1}$ et $U \circ Q \circ U^{-1}$ sont $\mathcal{C}(P_\alpha)$, non constants et de même degré. Il résulte de III.B.2) qu'ils sont égaux et donc P et Q aussi. Il résulte alors de III.A.1) que les seuls polynômes non constants qui commutent à T_2 sont les polynômes de Tchebychev de première espèce. Quant aux polynômes constants, l'équation $2P^2 - 1 = P$ équivaut à $P = 1$ ou $P = -\frac{1}{2}$, et donc $\boxed{\mathcal{C}(T_2) = \{-1/2\} \cup \{T_n \,|\, n \in \mathbf{N}\}.}$

III.C

III.C.1) Soit α dans $\mathbf{C}$ et P dans $\mathcal{C}(P_\alpha)$. Puisque P_α est pair, il vient

$$P_\alpha \circ P \circ (-X) = P \circ P_\alpha \circ (-X) = P \circ P_\alpha = P_\alpha \circ P$$

et donc $P^2 = (P \circ (-X))^2$. On décompose P en sa partie paire et sa partie impaire, i.e. $P = Q + R$ avec $Q = \frac{1}{2}(P + P \circ (-X))$ et $R = \frac{1}{2}(P - P \circ (-X))$, de sorte qu'on a $P \circ (-X) = Q - R$ et l'égalité $P^2 = (P \circ (-X))^2$ équivaut à $QR = 0$, i.e. P est pair ou impair. Si de plus P est de degré 3, alors il est impair et s'écrit donc $P = XP_\beta$ avec β dans $\mathbf{C}$, puisqu'il est unitaire d'après III.B.1). En dérivant l'égalité $P \circ P_\alpha = P_\alpha \circ P$, il vient $2X \cdot P' \circ P_\alpha = 2P \cdot P' = 2XP' \cdot P_\beta$, soit, en notant $P' = 3P_\gamma$ avec $\beta = 3\gamma$, $P_\gamma \circ P_\alpha = P_\gamma \cdot P_\beta$. En dérivant une nouvelle fois il vient $2P_\alpha \cdot 2X = 2XP_\beta + 2XP_\gamma$ et donc $2P_\alpha = P_\beta + P_\gamma$, soit $2\alpha = \beta + \gamma = 4\gamma$. On reprend alors l'équation $P_\gamma \circ P_\alpha = P_\gamma \cdot P_\beta$ et on évalue en 0. Il vient $P_\gamma(\alpha) = P_\gamma(2\gamma) = 4\gamma^2 + \gamma = \gamma \cdot \beta = 3\gamma^2$, soit $\gamma^2 + \gamma = 0$, on en déduit qu'on a nécessairement $\gamma = 0$ ou $\gamma = -1$, i.e. $\alpha = 0$ ou $\alpha = -2$. Il résulte de III.B.2) et III.B.3) que la réciproque est vraie puisque $X^3 \in \mathcal{C}(P_0)$ et $(2X) \circ T_3 \circ (2X)^{-1} \in \mathcal{C}(P_{-2})$, i.e. $X^3 - 3X \in \mathcal{C}(P_{-2})$. Par conséquent les seuls complexes α tels que $\mathcal{C}(P_\alpha)$ contienne un polynôme de degré trois sont $\boxed{0 \text{ et } -2.}$

III.C.2) Soit $(F_n)_{n \in \mathbf{N}}$ vérifiant (2). Alors F_2 est de degré 2 et, grâce à III.B.3), on dispose de U dans G et α dans $\mathbf{C}$ tels que $U \circ F_2 \circ U^{-1} = P_\alpha$. Comme F_3 commute à F_2, il en va de même de $U \circ F_3 \circ U^{-1}$ avec P_α. Il résulte donc de la question précédente qu'on a $\alpha = 0$ ou $\alpha = -2$ et donc, puisque la relation de conjugaison par G est une relation d'équivalence, F_2 est conjugué à X^2 ou à T_2 par un élément de G noté V (on a donc $V = U$ ou $V = (2X)^{-1} \circ U = \frac{1}{2}U$). Son commutant est alors obtenu en conjuguant celui de X^2 ou de T_2 et donc, par l'unicité démontrée en III.B.2), F_n est alors le conjugué par V de X^n ou de T_n respectivement. $\boxed{\text{le théorème de Block et Thielmann en résulte.}}$

PARTIE IV - Puissances dans $\mathrm{GL}_2(\mathbf{Z})$

IV.A - Soit M dans $\mathrm{GL}_2(\mathbf{Z})$ et N son inverse dans $\mathrm{GL}_2(\mathbf{Z})$, alors $MN = I_2$ et donc $1 = \det(MN) = \det(M)\det(N)$ par multiplicativité du déterminant. Comme M et N sont à coefficients entiers, leurs déterminants aussi et ce sont donc des éléments de $\mathbf{Z}^\times$, i.e. de $\{\pm 1\}$. Il en résulte $|\det(M)| = 1$. Réciproquement si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc = \pm 1$, alors l'inverse de M est donné par $(ad-bc)^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, i.e. $(ad-bc)\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ et donc M admet un inverse dans $\mathscr{M}_2(\mathbf{Z})$. Par conséquent, $\boxed{M \text{ appartient à } \mathrm{GL}_2(\mathbf{Z}) \text{ si et seulement si } |\det(M)| = 1.}$

IV.B - Soit a un réel non nul. Pour tout x réel et n entier naturel on pose $\tilde{D}_n(x) = \dfrac{1}{2a^n} D_n(2xa, a^2)$ et $\tilde{E}_n(x) = a^{-n} E_n(2xa, a^2)$. Par définition, pour tout x réel et n entier naturel, on a $\tilde{D}_0(x) = \tilde{E}_0(x) = 1$, $\tilde{D}_1(x) = x$, $\tilde{E}_1(x) = 2x$ et

$$\tilde{D}_{n+2}(x) = \frac{2xa}{a}\tilde{D}_{n+1}(x) - \frac{a^2}{a^2}\tilde{D}_n(x) = x\tilde{D}_{n+1}(x) - \tilde{D}_n(x)$$

et

$$\tilde{E}_{n+2}(x) = \frac{2xa}{a}\tilde{E}_{n+1}(x) - \frac{a^2}{a^2}\tilde{E}_n(x) = x\tilde{E}_{n+1}(x) - \tilde{E}_n(x)\ .$$

Il en résulte que les familles de fonctions $(\tilde{D}_n)_{n\in\mathbf{N}}$ et $(\tilde{E}_n)_{n\in\mathbf{N}}$ sont des familles de fonctions polynomiales et les familles de polynômes associées satisfont aux mêmes relations de récurrence que les polynômes de Tchebychev et les mêmes conditions initiales que ceux de première et seconde espèce respectivement. Il en résulte que l'égalité recherchée est vraie pour x réel et a réel non nul. Comme on a affaire à des polynômes, l'égalité s'étend, à a fixé, à tout x complexe. Comme on a également affaire à des fonctions polynomiales à x fixé, elle s'étend à a complexe également, i.e. $\boxed{\forall (x,a) \in \mathbf{C}^2,\ D_n(2xa, a^2) = 2a^n T_n(x) \text{ et } E_n(2xa, a^2) = a^n U_n(x).}$

La relation de récurrence définissant les polynômes de Dickson montre que, pour n entier naturel, D_n et E_n sont de degré n en la première variable (et $[n/2]$ en la seconde). On en déduit que les fonctions, à a fixé dans $\mathbf{C}$ et x variant dans $\mathbf{C}^*$, données par $x^n D_n\left(x + \dfrac{a}{x}, a\right)$ et $x^{n+1}\left(x - \dfrac{a}{x}\right) E_n\left(x + \dfrac{a}{x}, a\right)$ sont polynomiales en x de degrés respectifs $2n$ et $2n+2$. De plus on peut les prolonger sur $\mathbf{C}$.

Soit maintenant b dans $\mathbf{C}$ et y dans $\mathbf{C}$ de module 1. On pose $a = b^2$ et $x = by$. Il vient, en notant θ un argument de y, i.e. $y = e^{i\theta}$,

$$x + \frac{a}{x} = b(y + y^{-1}) = 2b\cos(\theta) \quad \text{et} \quad x - \frac{a}{x} = b(y - y^{-1}) = 2ib\sin(\theta)$$

et, pour tout entier naturel n,

$$2b^n x^n \cos(n\theta) = b^n x^n (y^n + y^{-n}) = x^{2n} + b^{2n} = b^{2n}(y^{2n} + 1)$$

et

$$2ib^{n+1}x^{n+1}\sin((n+1)\theta) = b^{n+1}x^{n+1}(y^{n+1} - y^{-n-1}) = b^{2n+2}(y^{2n+2} - 1)\ .$$

On en déduit

$$x^n D_n\left(x + \frac{a}{x}, a\right) = x^n D_n(2by, b^2) = 2b^n x^n T_n(\cos(\theta)) = 2b^n x^n \cos(n\theta) = b^{2n}(y^{2n} + 1)$$

et

$$x^{n+1}\left(x - \frac{a}{x}\right) E_n\left(x + \frac{a}{x}, a\right) = 2ib^{n+1}x^{n+1}\sin((n+1)\theta) = b^{2n+2}(y^{2n+2} - 1)\ .$$

Puisque $(y, b) \mapsto (by, b^2)$ est polynomiale, les expressions de gauche sont toutes deux polynomiales en b et y, tout comme celles de droite et donc l'égalité pour tout y de module 1 entraîne l'égalité pour tout y dans $\mathbf{C}$. Par surjectivité de la fonction carré sur $\mathbf{C}$, l'application $(y, b) \mapsto (by, b^2)$ est surjective de $\mathbf{C} \times \mathbf{C}^*$ dans lui-même et on en déduit l'égalité de fonctions polynomiales (prolongées en $a = 0$)

$$x^n D_n\left(x + \frac{a}{x}, a\right) = x^{2n} + a^n \quad \text{et} \quad x^{n+1}\left(x - \frac{a}{x}\right) E_n\left(x + \frac{a}{x}, a\right) = x^{2n+2} - a^{n+1}$$

et donc, pour tout entier naturel n et tout $(x, a) \in \mathbf{C}^* \times \mathbf{C}$

$$\boxed{D_n\left(x + \frac{a}{x}, a\right) = x^n + \frac{a^n}{x^n} \text{ et } \left(x - \frac{a}{x}\right) E_n\left(x + \frac{a}{x}, a\right) = x^{n+1} - \frac{a^{n+1}}{x^{n+1}}.}$$

IV.C -

IV.C.1) On note $B = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ et, pour $n \geq 2$, on note $(\mathbf{P}_n)$ la propriété $B^n = E_{n-1}(\sigma, \nu) \cdot B - \nu E_{n-2}(\sigma, \nu) \cdot I_2$.

On a

$$B^2 = \begin{pmatrix} r^2 + st & s(r+u) \\ t(r+u) & st + u^2 \end{pmatrix} = (r+u)B + (st - ru)I_2 = \sigma B - \nu I_2$$

et donc, par définition des polynômes de Dickson, $B^2 = E_1(\sigma, \nu) \cdot B - \nu E_0(\sigma, \nu) \cdot I_2$, i.e. $(\mathbf{P}_2)$ est vrai.

Soit maintenant $n \geq 3$ tel que $B^{n-1} = E_{n-2}(\sigma, \nu) \cdot B - \nu E_{n-3}(\sigma, \nu) \cdot I_2$. Il vient

$$\begin{aligned} B^n &= E_{n-2}(\sigma, \nu) \cdot B^2 - \nu E_{n-3}(\sigma, \nu) \cdot B \\ &= (\sigma E_{n-2}(\sigma, \nu) - \nu E_{n-3}(\sigma, \nu))\, B - \nu E_{n-2}(\sigma, \nu) \cdot I_2 \\ &= E_{n-1}(\sigma, \nu) \cdot B - \nu E_{n-2}(\sigma, \nu) \cdot I_2 \end{aligned}$$

d'après les propriétés de définition des polynômes de Dickson de seconde espèce. On en déduit que la propriété $(\mathbf{P}_n)$ est héréditaire pour $n \geq 2$. Il résulte du principe de récurrence que, pour tout $n \geq 2$, on a $\boxed{B^n = E_{n-1}(\sigma, \nu) \cdot B - \nu E_{n-2}(\sigma, \nu) \cdot I_2.}$

En prenant la trace il vient $\mathrm{Tr}(B^n) = \sigma E_{n-1}(\sigma, \nu) - 2\nu E_{n-2}(\sigma, \nu)$. En tant que combinaison linéaire de fonctions polynomiales vérifiant la même relation de récurrence, on en déduit que, pour $n \geq 2$, $\mathrm{Tr}(B^{n+2}) = \sigma\,\mathrm{Tr}(B^{n+1}) - \nu\,\mathrm{Tr}(B^n)$. De plus on a $\mathrm{Tr}(B^0) = \mathrm{Tr}(I_2) = 2 = D_0(\sigma, \nu)$,

$\mathrm{Tr}(B^1) = \sigma = D_1(\sigma,\nu)$, $B^2 = \sigma B - \nu I_2$ et donc $\mathrm{Tr}(B^2) = \sigma^2 - 2\nu = \sigma D_1(\sigma,\nu) - \nu D_0(\sigma,\nu) = D_2(\sigma,\nu)$ et enfin $B^3 = \sigma B^2 - \nu B = (\sigma^2 - \nu)B - \sigma\nu I_2$ et donc

$$\mathrm{Tr}(B^3) = \sigma^3 - 3\sigma\nu = \sigma(\sigma^2 - 2\nu) - \nu\sigma = \sigma D_2(\sigma,\nu) - \nu D_1(\sigma,\nu) = D_3(\sigma,\nu)$$

de sorte que $(\mathrm{Tr}(B^n))_{n\in\mathbf{N}}$ vérifie la même relation de récurrence que $(D_n(\sigma,\nu))$ et coïncide sur les deux premiers termes. On en conclut $\boxed{\mathrm{Tr}(B^n) = D_n(\sigma,\nu).}$

IV.C.2) Soit B dans $\mathrm{GL}_2(\mathbf{Z})$ tel que $A = B^n$ alors en reprenant les notations précédentes on a $B = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ avec r, s, t et u entiers, $\nu = ru - st \in \mathbf{Z}$ et $\sigma = r + u \in \mathbf{Z}$. Comme E_{n-1} est une fonction polynomiale à coefficients entiers, comme le montre une récurrence immédiate, $\boxed{E_{n-1}(\sigma,\nu) \text{ est entier.}}$

De plus $b = sE_{n-1}(\sigma,\nu)$, $c = tE_{n-1}(\sigma,\nu)$, $a - d = (r-u)E_{n-1}(\sigma,\nu)$, $\tau = D_n(\sigma,\nu)$ et $\delta = \det(B^n) = \det(B)^n = \nu^n$. et donc $\boxed{E_{n-1}(\sigma,\nu) \text{ divise } b,\ c \text{ et } a-d,\ \tau = D_n(\sigma,\nu) \text{ et } \delta = \nu^n.}$

IV.C.3) a) Soit x une racine complexe de $X^2 - \sigma X + \nu$ de sorte qu'on a $X^2 - \sigma X + \nu = (X - x)(X - \nu/x)$ et $\sigma = x + \dfrac{\nu}{x}$. Il vient

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

en utilisant d'abord l'équation de gauche dans (3), puis celle de droite, et en remarquant $\left(x - \dfrac{\nu}{x}\right)^2 = \left(x + \dfrac{\nu}{x}\right)^2 - 4\nu$. On a donc $\boxed{\tau^2 - 4\delta = p^2(\sigma^2 - 4\nu).}$

Or, par définition, $ru - st = \dfrac{1}{4p^2}(p^2\sigma^2 - (a-d)^2 - 4bc) = \dfrac{1}{4p^2}(p^2\sigma^2 - \tau^2 + 4\delta)$ et donc, en utilisant ce qui précède, $\boxed{ru - st = \nu.}$

Par hypothèse sur A, B est à coefficients entiers. Comme son déterminant est dans $\mathbf{Z}^\times$, il résulte de IV.A que $\boxed{B \text{ appartient à } \mathrm{GL}_2(\mathbf{Z}).}$

b) D'après la relation établie en IV.A, $B^n - pB$ est scalaire et, par définition, $A - pB$ est également scalaire avec $A - pB = \dfrac{\tau - p\sigma}{2} I_2$. Ces deux matrices sont donc égales si et seulement si elles ont même trace, i.e. si et seulement si $\mathrm{Tr}(A) = \mathrm{Tr}(B^n)$. Or on a $\mathrm{Tr}(B) = \sigma$ par construction et on vient de démontrer $\det(B) = \nu$. Il résulte de IV.C.1) qu'on a $\mathrm{Tr}(B^n) = D_n(\sigma,\nu)$ et donc, par hypothèse, on a $\mathrm{Tr}(B^n) = \mathrm{Tr}(A)$. On en conclut $\boxed{A = B^n.}$

IV.C.4) Par définition on a $\tau = 14$, $\delta = -1$, $n = 3$ et donc nécessairement $\nu = -1$. Comme $E_2(x,a) = x^2 - a$, nécessairement $\sigma^2 + 1$ est un diviseur de 0, 5 et 10 donc σ appartient à $\{-2, 0, 2\}$. Comme $D_3(x,a) = x^3 - 3xa$, on a nécessairement $14 = \sigma(\sigma^2 + 3)$ et donc finalement $\sigma = 2$. Comme le couple $(\sigma,\nu) = (2,-1)$ permet de vérifier les conditions i. et ii., on en conclut que $\boxed{A \text{ est un cube dans } \mathrm{GL}_2(\mathbf{Z}).}$

De plus les formules précédentes donnent $p = 5$ puis $\boxed{B = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}}$.

Remarque : un calcul direct donne effectivement $B^2 = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$ et $B^3 = \begin{pmatrix} 7 & 10 \\ 5 & 7 \end{pmatrix}$.