

I – Définitions et propriétés usuelles

I.A Polynômes de première espèce

I.A.1 Les polynômes T_0, T_1, T_2 et T_3

On a les relations $\forall \theta \in \mathbb{R}, T_0(\cos \theta) = 1, T_1(\cos \theta) = \cos \theta, T_2(\cos \theta) = 2 \cos^2 \theta - 1$ et $T_3(\cos \theta) = 4 \cos^3 \theta - 3 \cos \theta$.

Comme $\text{Im}(\cos) = [-1, 1]$ est infini, on en déduit (la différence ayant une infinité de racines) que

$$T_0 = 1, T_1 = X, T_2 = 2X^2 - 1 \text{ et } T_3 = 4X^3 - 3X.$$

I.A.2 Expression de T_n

$$\forall \theta \in \mathbb{R}, \forall n \in \mathbb{N}, e^{in\theta} = (\cos \theta + i \sin \theta)^n = \sum_{k=1}^n \binom{n}{k} \cos^{n-k} \theta i^k \sin^k \theta.$$

En prenant la partie réelle des deux membres, on obtient

$$\cos(n\theta) = \sum_{0 \leq k \leq n/2} \binom{n}{2k} (-1)^k \cos^{n-2k} \theta \sin^{2k} \theta = \sum_{0 \leq k \leq n/2} \binom{n}{2k} (-1)^k \cos^{n-2k} \theta (1 - \cos^2 \theta)^k.$$

Et comme l'égalité est valable pour une infinité de réels (tout $[-1, 1]$),

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

I.A.3 Une relation de récurrence entre les T_n

$$\forall n \in \mathbb{N}, T_{n+2}(\cos \theta) + T_n(\cos \theta) = \cos((n+2)\theta) + \cos(n\theta) = 2 \cos((n+1)\theta) \cos \theta = 2 \cos \theta T_{n+1}(\cos \theta).$$

Vrai pour une infinité de réels donc $T_{n+2} + T_n = 2X T_{n+1}$.

Degré et coefficient dominant de T_n

On va montrer par une récurrence d'ordre 2 sur $n \in \mathbb{N}^*$ que $\text{cd } T_n = 2^{n-1}$ et $\text{deg } T_n = n$.

- La propriété est vraie pour $n = 1, 2$ et 3 .
- Soit $n \geq 2$ tel que $\text{cd } T_n = 2^{n-1}$, $\text{cd } T_{n+1} = 2^n$, et $\text{deg } T_n = n$, $\text{deg } T_{n+1} = n+1$. Alors

$$\text{deg } T_{n+2} = \text{deg}(2X T_{n+1} - T_n) = \text{deg}(X T_{n+1}) = 1 + n + 1 = n + 2.$$

$$\text{cd } T_{n+2} = \text{cd}(2X T_{n+1}) = 2 \text{cd } T_{n+1} = 2 \times 2^n = 2^{n+1}.$$

Une méthode qui utilise l'expression de T_n .

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

On remarque que $\forall k \in [0, n/2], n - 2k + 2k = n$, de plus le coefficient de X^n est $\sum_{0 \leq 2k \leq n} \binom{n}{2k}$

On le calcule en introduisant la somme des termes de d'indices impaires en remarquant que

$$\sum_{0 \leq 2k \leq n} \binom{n}{2k} + \sum_{0 \leq 2k+1 \leq n} \binom{n}{2k+1} = \sum_{p=0}^n \binom{n}{p} = 2^n$$

$$\sum_{0 \leq 2k \leq n} \binom{n}{2k} - \sum_{0 \leq 2k+1 \leq n} \binom{n}{2k+1} = \sum_{p=0}^n \binom{n}{p} (-1)^p = 0^n$$

d'après la formule du binôme de Newton. En prenant la demi-somme de ces deux relations, on obtient

$$\sum_{0 \leq 2k \leq n} \binom{n}{2k} = \frac{2^n + 0^n}{2}$$

En conclusion $\text{deg } T_n = n$ et $\text{cd } T_n = 2^{n-1}$ si $n \neq 0, 1$ sinon.

I.A.4 Les racines de T_n

$\forall n \in \mathbb{N}^*$,

$$T_n(\cos \theta) = 0 \iff \cos n\theta = 0 \iff \exists k \in \mathbb{Z}, \theta = \frac{(2k+1)\pi}{2n}.$$

Or \cos est injectif sur $[0, \pi]$ et $\theta_k = \frac{(2k+1)\pi}{2n} \in [0, \pi]$ si et seulement si $k \in \llbracket 0, n-1 \rrbracket$.

Les $\cos \theta_k$ pour $k \in \llbracket 0, n-1 \rrbracket$ sont donc n racines deux à deux distinctes de T_n qui est de degré n , on en déduit qu'il n'y en a pas d'autres et qu'elles sont toutes simples.

Donc T_n admet n racines distinctes sur $] -1, 1[$, à savoir les $\cos \frac{(2k+1)\pi}{2n}$ où $k \in \llbracket 0, n-1 \rrbracket$.

I.B Polynômes de deuxième espèce

I.B.1 Expression de $U_n(\cos \theta)$

En dérivant l'expression $T_{n+1}(\cos \theta) = \cos((n+1)\theta)$ par rapport à la variable θ , on obtient

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

ce qui entraîne que

$$\forall \theta \in \mathbb{R} \setminus \pi\mathbb{Z}, \forall n \in \mathbb{N}, \frac{T'_{n+1}(\cos \theta)}{n+1} = \frac{\sin((n+1)\theta)}{\sin \theta},$$

c'est-à-dire $U_n(\cos \theta) = \frac{\sin((n+1)\theta)}{\sin \theta}$.

I.B.2 a) Une relation de récurrence entre les U_n

$$\forall n \in \mathbb{N}, U_{n+2}(\cos \theta) + U_n(\cos \theta) = \frac{\sin((n+2)\theta) + \sin n\theta}{\sin \theta} = \frac{2 \cos \theta \sin((n+1)\theta)}{\sin \theta} = 2 \cos \theta U_{n+1}(\cos \theta).$$

Le polynôme $U_{n+2} + U_n - 2XU_{n+1}$ ayant une infinité de racines, on obtient $U_{n+2} + U_n = 2XU_{n+1}$.

b) Racines de U_n

Les racines de U_n sont celles de T'_{n+1} . Or T_{n+1} admet $n+1$ racines distinctes sur $] -1, 1[$ d'après I.A.4, donc par application du théorème de Rolle entre deux zéros consécutifs de T_{n+1} (la fonction polynomiale associée étant bien continue sur le segment, dérivable sur son intérieur et prend la même valeur – zéro – aux bornes), on obtient un zéro de T'_{n+1} , ce qui prouve que U_n admet n racines distinctes sur $] -1, 1[$.

$$\forall n \in \mathbb{N}, U_n(\cos \theta) = 0 \iff \sin((n+1)\theta) = 0 \iff \exists k \in \mathbb{Z}, (n+1)\theta = k\pi$$

Or \cos est injectif sur $[0, \pi]$ et $\varphi_k = \frac{k\pi}{n+1} \in [0, \pi]$ si et seulement si $k \in \llbracket 1, n \rrbracket$.

Les $\cos \varphi_k$ pour $k \in \llbracket 1, n \rrbracket$ sont donc n racines deux à deux distinctes de U_n , on en déduit qu'il n'y en a pas d'autres.

Donc les racines de U_n sont les $\cos \frac{k\pi}{n+1}$ où $k \in \llbracket 1, n \rrbracket$.

II – Arithmétique des polynômes de Tchebychev

II.A Division euclidienne

II.A.1 - Soit $m, n \in \mathbb{N}$ tel que $0 \leq m \leq n$ et $\theta \in \mathbb{R}$.

$$\cos((n+m)\theta) + \cos((n-m)\theta) = 2 \cos n\theta \cos m\theta$$

donc $T_{n+m} + T_{n-m} = 2T_n T_m$.

Soit $n, m \in \mathbb{N}$ tel que $0 \leq m < n$ et $\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$.

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

donc $U_{n+m-1} + U_{n-m-1} = 2U_{n-1} T_m$.

II.A.2 a) ■ Si $m < n < 2m$, alors $0 < n-m < m$, donc d'après II.A.1, $T_m T_{n-m} = \frac{1}{2}(T_n + T_{2m-n})$, c'est-à-dire

$$T_n = 2T_{n-m} T_m - T_{2m-n} = 2T_{n-m} T_m - T_{|n-2m|}$$

avec $0 < 2m-n < 2m-m = m = \deg T_m$.

- Si $2m \leq n < 3m$, alors $m \leq n - m < 2m$, donc toujours d'après II.A.1, $T_{n-m} T_m = \frac{1}{2}(T_n + T_{n-2m})$, c'est-à-dire

$$T_n = 2T_{n-m} T_m - T_{n-2m} = 2T_{n-m} T_m - T_{|n-2m|}$$

avec $0 \leq n - 2m < 3m - 2m = m = \deg T_m$.

On conclut que dans tous les cas $Q_{n,m} = 2T_{n-m}$ et $R_{n,m} = -T_{|n-2m|}$.

- b) Soit $n = (2p + 1)m$ où $p \in \mathbb{N}^*$, on applique l'égalité de II.A.1 au couple $(n, m) \leftarrow (2km, m)$ où $k \in \llbracket 1, p \rrbracket$, on obtient $2T_{2km} T_m = T_{(2k+1)m} + T_{(2k-1)m}$, ce qui entraîne que

$$2(-1)^{p-k} T_{2km} T_m = (-1)^{p-k} T_{(2k+1)m} - (-1)^{p-k+1} T_{(2k-1)m},$$

ce qui donne en sommant de $k = 1$ à p , on obtient par télescopage

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

Donc $T_n = T_m \left((-1)^p T_m + 2 \sum_{k=1}^p (-1)^{p-k} T_{2km} \right)$, puis $Q_{n,m} = (-1)^p T_m + 2 \sum_{k=1}^p (-1)^{p-k} T_{2km}$ et $R_{n,m} = 0$.

- c) On considère l'ensemble $A_{n,m} = \{k \in \mathbb{N}^*, (2k-1)m < n\}$.

Par hypothèse $n \neq (2(0)+1)m$, donc $1 \in A_{n,m}$. De plus, $A_{n,m}$ est majoré par $1 + \left\lfloor \frac{n/m+1}{2} \right\rfloor$, donc admet un maximum p .

Comme $p \in A_{n,m}$ et $p+1 \notin A_{n,m}$, $(2p-1)m < n \leq (2p+1)m$. Or n n'est pas produit de m par un entier impair, donc $(2p-1)m < n < (2p+1)m$, c'est-à-dire $|n - 2pm| < m$.

$$\forall k \in \llbracket 0, p-2 \rrbracket, n - (2k+1)m \geq n - (2p-3)m \geq 2m > m$$

donc

$$\forall k \in \llbracket 0, p-2 \rrbracket, 2T_m T_{n-(2k+1)m} = T_{n-2km} + T_{n-(2k+2)m}$$

donc

$$2(-1)^k T_m T_{n-(2k+1)m} = (-1)^k T_{n-2km} - (-1)^{k+1} T_{n-(2k+2)m},$$

ce qui donne par télescopage en sommant de $k = 0$ à $p-2$

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

Or $m < n - (2p-2)m < 3m$, donc d'après la question II.A.2.a,

$$T_{n-(2p-2)m} = 2T_m T_{n-(2p-1)m} - T_{|n-2pm|}$$

et par suite

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

ce qui donne le résultats puisque $|n - 2pm| < m = \deg T_m$.

II.B Plus grand commun diviseur

II.B.1 Pgcd de U_n et U_m

Posons $n+1 = hn_1$ et $m+1 = hm_1$.

Soit r une racine de U_{h-1} , alors in a $k \in \llbracket 0, h \rrbracket$ tel que

$$r = \cos \frac{k\pi}{h} = \cos \frac{kn_1\pi}{n+1} = \cos \frac{km_1\pi}{m+1},$$

donc r est une racine commune de U_n et de U_m .

Réciproquement si r est une racine commune de U_n et de U_m , alors on a $(k, k') \in \llbracket 1, n \rrbracket \times \llbracket 1, m \rrbracket$ tel que

$$r = \cos \frac{k\pi}{n+1} = \cos \frac{k'\pi}{m+1},$$

donc $\frac{k\pi}{n+1} = \frac{k'\pi}{m+1}$ (on est sur $[0, \pi]$) et par suite $km_1 = k'n_1$. Or n_1 et m_1 sont premiers entre eux, donc par le

théorème de Gauss, n_1 divise k , ce qui entraîne en posant $\frac{k}{n_1} = k''$ que $r = \cos \frac{k''\pi}{h}$ c'est-à-dire que r est une racine de U_{h-1} .

On en conclut, comme les polynômes sont simplement scindés, que U_{h-1} est un pgcd de U_n et U_m .

II.B.2 Pgcd de T_n et T_m

- a) Raisonnement analogue à la question précédente.
Soit r une racine de T_g , alors on a $k \in \llbracket 0, g-1 \rrbracket$ tel que

$$r = \cos \frac{(2k+1)\pi}{2g} = \cos \frac{(2k+1)m_1\pi}{2m} = \cos \frac{(2k+1)n_1\pi}{2n},$$

or $(2k+1)m_1$ et $(2k+1)n_1$ sont impairs, donc r est une racine commune de T_n et T_m .

Réciproquement si r est une racine commune de T_n et T_m , alors on a $(k, k') \in \llbracket 0, n-1 \rrbracket \times \llbracket 0, m-1 \rrbracket$ tel que

$$r = \cos \frac{(2k+1)\pi}{2n} = \cos \frac{(2k'+1)\pi}{2m},$$

donc $\frac{(2k+1)\pi}{2n} = \frac{(2k'+1)\pi}{2m}$, c'est-à-dire $(2k'+1)n_1 = (2k+1)m_1$. Or n_1 et m_1 sont premiers entre eux, donc n_1 divise $2k+1$ et par suite si on pose $\frac{2k+1}{n_1} = n_2$ qui est impair, on aura $r = \cos \frac{n_2\pi}{2g}$ et l'imparité de n_2 entraîne que r est une racine de T_g .

On conclut que T_g est un pgcd de T_n et T_m .

- b) Soit r une racine commune de T_n et T_m , alors le raisonnement précédent aboutit à l'existence de k, k' tel que $(2k'+1)n_1 = (2k+1)m_1$, donc n_1 et m_1 sont de même parité, ce qui exige par hypothèse que n_1 et m_1 sont pairs, ce qui contredit le fait qu'ils sont premiers entre eux.

On conclut que T_n et T_m sont premiers entre eux.

- c) Si n, m impairs, n_1 et m_1 sont impairs, donc d'après a),

un pgcd de T_n et T_m est T_g où g est le pgcd de m et n .

Si n et m sont des puissances de 2, l'un de n_1 et m_1 est pair et l'autre vaut 1, donc d'après b),

T_n et T_m sont premiers entre eux.

III – Un théorème

III-A Préliminaires

III.A.1 $(T_n)_n$ est suite commutante

- deg $T_n = n$.
- $\forall \theta \in \mathbb{R}, \forall n, m \in \mathbb{N}, T_n \circ T_m(\cos \theta) = T_n(\cos(m\theta)) = \cos(nm\theta) = T_{nm}(\cos \theta)$, donc $T_n \circ T_m = T_{nm} = T_{mn} = T_m \circ T_n$.

III.A.2 G est un groupe

- $\forall P, Q \in G, \deg P \circ Q = \deg P \deg Q = 1$, donc la loi \circ est une loi de composition interne qui est associative.
- $\forall P \in G, P \circ X = X \circ P = P$, donc X est l'élément neutre de G .
- L'inverse de $P = aX + b$ est $P^{-1} = \frac{X-b}{a} \in G$.
- On conclut que G est un groupe.

III-B Commutant de X^2 et T_2

III.B.1 Q est unitaire

Soit Q de degré $n \geq 1$ et de coefficient dominant $q \neq 0$, tel que $P_\alpha \circ Q = Q \circ P_\alpha$. Alors en égalisant les coefficients dominants de ces deux membres, on obtient $q^2 = q$, donc $q = 1$.

III.B.2 Commutant de X^2

- Soit Q_1 et Q_2 deux polynômes de degré $n \geq 1$ commutant avec P_α , alors d'après la question précédente, ils sont unitaires, donc si on pose $R = Q_1 - Q_2$, on aura $\deg R < n$.
On calcule

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

ce qui donne par passage aux degrés que

$$2 \deg R = \deg R \circ P_\alpha = \deg R(Q_1 + Q_2) = \deg R + n,$$

donc, comme $\deg R < n$, $\deg R = -\infty$ et $Q_1 = Q_2$.

Il y a donc bien au plus un polynôme non constant commutant avec P_α .

- $\forall n \in \mathbb{N}^*, X^n$ commute avec X^2 et c'est l'unique polynôme de degré n .
Si $P = \lambda$ est un polynôme constant qui commute avec X^2 , alors $\lambda^2 = X^2 \circ P = P \circ X^2 = \lambda$, donc $\lambda \in \{0, 1\}$.
En conclut que $\mathcal{C}(X^2) = \{0\} \cup \{X^n, n \in \mathbb{N}\}$.

III.B.3 Existence de U et α

- Soit $P = aX^2 + bX + c$ et $U = \gamma X + \beta$ avec $a \neq 0$ et $\gamma \neq 0$.
- $U \circ P = P \circ U \iff \gamma(aX^2 + bX + c) + \beta = (\gamma X + \beta)^2 + a$, ce qui aboutit à un système qui admet une unique solution à savoir $U = aX + \frac{b}{2}$ et $P_\alpha = X^2 + \frac{4ac + 2b - b^2}{4}$.
- Le cas $P = T_2 = 2X^2 - 1$, donne $U = 2X$ et $P_\alpha = X^2 - 2$.

III.B.4 Commutant de T_2

- Soit Q de degré $n \geq 1$.
La question précédente entraine que $U \circ T_2 \circ U^{-1} = P_{-2}$, donc
 $Q \in \mathcal{C}(T_2) \iff Q \circ T_2 = T_2 \circ Q \iff U \circ Q \circ U^{-1} \circ P_{-2} = P_{-2} \circ U \circ Q \circ U^{-1} \iff U \circ Q \circ U^{-1} \in \mathcal{C}(P_{-2})$.
- D'après la question (II.B.2), P_{-2} admet au plus un commutant de degré $n \geq 1$, or $\forall n \geq 1, T_n$ commute avec T_2 , donc $U \circ T_n \circ U^{-1}$ commute avec P_{-2} par unicité c'est le seul de degré $n \geq 1$, donc $Q = T_n$.
- De plus si $P = \lambda$ commute avec T_2 , alors $\lambda = 2\lambda^2 - 1$, ce qui exige que $\lambda \in \{-\frac{1}{2}, 1\}$.
- En conclusion $\mathcal{C}(T_2) = \{-\frac{1}{2}\} \cup \{T_n / n \in \mathbb{N}\}$.

III-C

III.C.1 Les α répondant à la question

- Soit Q un polynôme de degré 3 qui commute avec P_α , alors Q est unitaire de la forme
 $Q = X^3 + aX^2 + bX + c$.
- L'égalité $Q \circ P_\alpha = P_\alpha \circ Q$ se traduit par $(X^2 + \alpha)^3 + a(X^2 + \alpha)^2 + b(X^2 + \alpha) + c = (X^3 + aX^2 + bX + c)^2 + \alpha$, le premier membre est un polynôme pair, donc les coefficients de X^5, X^3, X sont nuls dans le deuxième membre, ceci exige que $a = c = 0$.
- L'égalité devient $(X^2 + \alpha)^3 + b(X^2 + \alpha) = (X^3 + bX)^2 + \alpha$, ce qui exige le système $\begin{cases} 3a = 2b \\ 3a^2 + b = b^2 \\ a^3 + b\alpha = \alpha \end{cases}$ la solution du système est $\alpha \in \{0, -2\}$ et $b = \frac{3}{2}\alpha$, ce qui donne $Q = X^3$ si $\alpha = 0$ et $Q = X^3 - 3X$ si $\alpha = -2$.
- Réciproquement on vérifie que $X^3 - X$ commute avec P_{-2} et X^3 commute avec P_0 .

III.C.2 Théorème de Block et Thielmann

- Soit $(F_n)_n$ une suite vérifiant (III-1) et soit $n \geq 1$, alors F_n commute avec F_2 , or d'après (III.B.3), $\exists \alpha \in \mathbb{C}$ et $U \in G$ tel que $F_2 = U^{-1} \circ P_\alpha \circ U$, or F_3 commute avec $F_2 = U^{-1} \circ P_\alpha \circ U$, donc $U \circ F_3 \circ U^{-1}$ commute avec P_α qui est de degré 3, ce qui entraine d'après la question précédente que $\alpha \in \{0, 1\}$.
- - Si $\alpha = 0$, on aura $F_2 = U^{-1} \circ P_0 \circ U = U^{-1} \circ X^2 \circ U$, et par suite F_n commute avec $U^{-1} \circ X^2 \circ U$, c'est à dire $U \circ F_n \circ U^{-1}$ commute avec X^2 , or $\mathcal{C}(X^2) = \{0\} \cup \{X^n / n \in \mathbb{N}\}$, donc $U \circ F_n \circ U^{-1} = X^n$ c'est à dire $F_n = U^{-1} \circ X^n \circ U$.
- - Si $\alpha = -2$, on aura $F_2 = U^{-1} \circ P_{-2} \circ U$, donc F_n commute avec $U^{-1} \circ P_{-2} \circ U$, et par suite $U \circ F_n \circ U^{-1}$ commute avec P_{-2} , or d'après la question (III.B.3), $P_{-2} = V \circ T_2 \circ V^{-1}$ avec $V = 2X \in G$, ce qui entraine que $V^{-1} \circ U \circ F_n \circ U^{-1} \circ V$ commute avec T_2 , or $\mathcal{C}(T_2) = \{-\frac{1}{2}\} \cup \{T_n / n \in \mathbb{N}\}$, donc $W \circ F_n \circ W^{-1} = T_n$ d'où $F_n = W^{-1} \circ T_n \circ W$ avec $W = V^{-1} \circ U$.

IV – Puissances dans $GL_2(\mathbb{Z})$

IV.A Condition nécessaire et suffisante d'inversibilité

(\implies) Soit $M \in GL_2(\mathbb{Z})$, alors $MM^{-1} = I_2$, donc $\det M \det M^{-1} = 1$, or $\det M \in \mathbb{Z}$ et $\det M^{-1} \in \mathbb{Z}$, donc $\det M = \pm 1$.

(\impliedby) Soit $M \in \mathcal{M}_2(\mathbb{Z})$ tel que $\det M = \pm 1$, alors $M^{-1} = \frac{1}{\det M} (\text{Com} A)^T = \pm (\text{Com} A)^T \in \mathcal{M}_n(\mathbb{Z})$, donc $M \in GL_2(\mathbb{Z})$.

IV.B Relations entre les polynômes de Dickson et Tchebychev

- Soit $(x, a) \in \mathbb{C} \times \mathbb{C}^*$, alors en posant $G_n(x) = \frac{1}{2a^n} D_n(2xa, a^2)$ et $H_n(x) = \frac{1}{a} E_n(2xa, a^2)$, on aura
- $G_0(x) = 1, G_1(x) = \frac{1}{2a} xa = x$ et $G_{n+2}(x) = \frac{1}{2a^{n+2}} D_{n+2}(2xa, a^2) = \frac{1}{2a^{n+2}} (2xa D_{n+1}(2xa, a^2) - a^2 D_n(2xa, a^2)) = \frac{x}{a^{n+1}} D_{n+1}(2xa, a^2) - \frac{1}{2a^n} D_n(2xa, a^2) = 2x G_{n+1}(x) - G_n(x)$.
- La suite $(G_n)_n$ vérifie la relation (I-1), donc par unicité $\forall n \in \mathbb{N}, G_n = T_n$, ce ci entraine que $\forall (x, a) \in \mathbb{C} \times \mathbb{C}^*, D_n(2xa, a^2) = 2a^n T_n(x)$. les fonctions sont polynômiales des deux variables x, a , donc l'égalité est vraie sur \mathbb{C}^2 .
- De même on vérifie $H_0(x) = 1, H_1(x) = 2x$ et $H_{n+2}(x) = 2x H_{n+1}(x) - H_n(x)$, donc par unicité $\forall n \in \mathbb{N}, H_n = U_n$ et pour les mêmes raisons l'égalité est vraie sur \mathbb{C}^2 .
- On va montrer par récurrence l'égalité $D_n\left(x + \frac{a}{x}, a\right) = x^n + \frac{a^n}{x^n}$.

- L'égalité est vrai pour $n=0$ et $n=1$.

- Supposons que pour un certain $n \in \mathbb{N}$, l'égalité est satisfaite pour n et $n+1$, alors

$$D_{n+2}\left(x + \frac{a}{x}, a\right) = \left(x + \frac{a}{x}\right) D_{n+1}\left(x + \frac{a}{x}, a\right) - a D_n\left(x + \frac{a}{x}, a\right) = \\ = \left(x + \frac{a}{x}\right) \left(x^{n+1} + \frac{a^{n+1}}{x^{n+1}}\right) - a \left(x^n + \frac{a^n}{x^n}\right) = x^{n+2} + \frac{a^{n+2}}{x^{n+2}}, \text{ ce qui établit la récurrence.}$$

- De même on montre par récurrence l'égalité $\left(x - \frac{a}{x}\right) E_n\left(x + \frac{a}{x}, a\right) = \left(x^{n+1} - \frac{a^{n+1}}{x^{n+1}}\right)$.

- L'égalité est vraie pour $n=0$ et $n=1$.

- Supposons que pour un certain n , l'égalité est vraie à l'ordre n et $n+1$, alors

$$\left(x - \frac{a}{x}\right) E_{n+2}\left(x + \frac{a}{x}, a\right) = \left(x + \frac{a}{x}\right) \left(x - \frac{a}{x}\right) E_{n+1}\left(x + \frac{a}{x}, a\right) - a \left(x - \frac{a}{x}\right) E_n\left(x + \frac{a}{x}, a\right) = \\ = \left(x + \frac{a}{x}\right) \left(x^{n+2} - \frac{a^{n+2}}{x^{n+2}}\right) - a \left(x^{n+1} - \frac{a^{n+1}}{x^{n+1}}\right) = \left(x^{n+3} - \frac{a^{n+3}}{x^{n+3}}\right), \text{ ce qui établit la récurrence.}$$

IV.C

IV.C.1 On montre cette égalité par récurrence sur $n \geq 2$.

- Pour $n=2$, c'est le théorème de Cayley-Hamilton. $O_2 = \chi_B(B) = B^2 - \text{Tr}(B)B + \det(B)I_2$, donc

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

- Supposons que pour un certain $n \geq 2$, l'égalité est vérifiée, alors

$$B^{n+1} = E_{n-1}(\sigma, \nu)B^2 - \nu E_{n-2}(\sigma, \nu)B = (\sigma E_{n-1}(\sigma, \nu) - \nu E_{n-2}(\sigma, \nu))B - \nu E_{n-1}(\sigma, \nu)I_2 = \\ = E_n(\sigma, \nu)B - \nu E_{n-1}(\sigma, \nu)I_2, \text{ ce qui établit la récurrence.}$$

• Soit $\lambda, \mu \in \mathbb{C}^*$ les valeurs propres de B , alors $\lambda\mu = \det(B) = \nu$ et $\lambda + \mu = \lambda + \frac{\nu}{\lambda} = \text{Tr}(B) = \sigma$,

donc en profitant de la relation $(IV-1)$, on obtient

$$\text{Tr}(B^n) = \lambda^n + \mu^n = \lambda^n + \frac{\nu^n}{\lambda^n} = D_n\left(\lambda + \frac{\nu}{\lambda}, \nu\right) = D_n(\sigma, \nu).$$

IV.C.2 A étant une puissance $n^{\text{ième}}$ dans $GL_2(\mathbb{Z})$, alors $\exists B \in GL_2(\mathbb{Z})$ tel que $A = B^n$, on note comme dans $(IV-C-1)$ $\sigma = \text{Tr}(B)$ et $\nu = \det(B)$, alors d'après l'égalité précédente,

$$A = B^n = E_{n-1}(\sigma, \nu)B - \nu E_{n-2}(\sigma, \nu)I_2, \text{ ce qui donne par comparaison des coefficients et en notant } B = (b_{i,j})_{1 \leq i,j \leq 2}$$

$$a-d = (b_{1,1} - b_{2,2})E_{n-1}(\sigma, \nu), \quad c = b_{2,1}E_{n-1}(\sigma, \nu) \text{ et } b = b_{1,2}E_{n-1}(\sigma, \nu).$$

- σ et ν sont dans \mathbb{Z} , on va montrer par récurrence sur $n \in \mathbb{N}$ que $E_n(\sigma, \nu) \in \mathbb{Z}$.

- $E_0(\sigma, \nu) = 1 \in \mathbb{Z}$ et $E_1(\sigma, \nu) = \sigma \in \mathbb{Z}$.

- Supposons que pour un certain $n \in \mathbb{N}$, $E_n(\sigma, \nu) \in \mathbb{Z}$ et $E_{n+1}(\sigma, \nu) \in \mathbb{Z}$, alors

$$E_{n+2}(\sigma, \nu) = \sigma E_{n+1}(\sigma, \nu) - \nu E_n(\sigma, \nu) \in \mathbb{Z}, \text{ ce qui établit la récurrence.}$$

- Les égalités précédentes assure la proposition (i).

- L'égalité $A = B^n$ entraîne que $\tau = \text{Tr}(A) = \text{Tr}(B^n) = D_n(\sigma, \nu)$ (d'après la question précédente, et

$$\tau = \det(A) = \det(B^n) = (\det(B))^n = \nu^n,$$

ce qui établit (ii).

IV.C.3 a) • Soit $\alpha, \frac{\nu}{\alpha}$ les racines du polynôme $X^2 - \sigma X + \nu$, alors d'après la condition (ii) et l'égalité $(IV-1)$,

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

donc grâce à cette égalité et à $\delta = \nu^n$ de la condition (ii), $\tau^2 - 4\delta = \left(\alpha^n + \frac{\nu^n}{\alpha^n}\right)^2 - 4\nu^n = \left(\alpha^n - \frac{\nu^n}{\alpha^n}\right)^2$, ce qui donne d'après l'égalité $(IV-1)$,

$$\tau^2 - 4\delta = \left(\alpha - \frac{\nu}{\alpha}\right)^2 E_{n-1}^2(\sigma, \nu), \text{ or } \left(\alpha - \frac{\nu}{\alpha}\right)^2 = \left(\alpha + \frac{\nu}{\alpha}\right)^2 - 4\nu = \sigma^2 - 4\nu, \text{ donc}$$

$$\tau^2 - 4\delta = p^2(\sigma^2 - 4\nu). \\ \bullet \quad ru - st = \frac{1}{4} \left(\sigma^2 - \frac{(a-d)^2}{p^2} \right) - \frac{bc}{p^2} = \frac{1}{4} \left(\sigma^2 - \frac{(a+b)^2 - 4(ad-bc)}{p^2} \right) = \\ = \frac{1}{4} \left(\sigma^2 - \frac{\tau^2 - 4\delta}{p^2} \right) = \frac{1}{4} (\sigma^2 - (\sigma^2 - 4\nu)) = \nu.$$

• C'est clair que la condition (i) entraîne que $s \in \mathbb{Z}$ et $t \in \mathbb{Z}$, donc $ru = \nu + st \in \mathbb{Z}$, de plus $(\sigma - \frac{a-d}{p})(\sigma + \frac{a-d}{p}) = 4ru$

est pair, donc l'un des entiers $\sigma - \frac{a-d}{p}$ ou $\sigma + \frac{a-d}{p}$ est pair, ce qui entraîne que $u \in \mathbb{Z}$ ou $r \in \mathbb{Z}$, mais puisque

$u+r = \sigma \in \mathbb{Z}$, il suffit que l'une des deux soit dans \mathbb{Z} pour que l'autre soit aussi dans \mathbb{Z} , donc $u \in \mathbb{Z}$ et $r \in \mathbb{Z}$.

- $\det(B) = \nu = \pm 1$, donc d'après $(IV-A)$ $B \in GL_2(\mathbb{Z})$.

b) - L'égalité $B^n = E_{n-1}(\sigma, \nu)B - \nu E_{n-2}(\sigma, \nu)I_2$ entraîne que $B^n = pB - \nu E_{n-2}(\sigma, \nu)I_2 = \begin{pmatrix} x & b \\ c & y \end{pmatrix}$ où on a posé

$$x = pr - \nu E_{n-2}(\sigma, \nu) \text{ et } y = pu - \nu E_{n-2}(\sigma, \nu).$$

- Reste à montrer que $(x, y) = (a, d)$.

- L'égalité $\tau = D_n(\sigma, \nu) = \text{Tr}(B^n)$, entraîne que $a + b = x + y$ et des égalités $r = \frac{1}{2}\left(\sigma + \frac{a-d}{p}\right)$, $u = \frac{1}{2}\left(\sigma - \frac{a-d}{p}\right)$

on tire $r - u = \frac{a-d}{p}$, donc $x - y = a - d$.

- On a donc $\begin{cases} x + y = a + d \\ x - y = a - d \end{cases}$, donc $a = x$ et $d = y$, ce qui entraîne que $B^n = A$.

IV.C.4 - On choisit σ et ν pour que $E_2(\sigma, \nu) = \sigma^2 - \nu$ divise 5 et 10 et $7 - 7 = 0$. $\sigma = 2$ et $\nu = -1$ conviennent.

- On obtient $r = 1, s = 2, t = 1$ et $u = 1$, donc $B = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$, on vérifie bien que $B^3 = A$.

Fin