Un corrigé du concours Centrale-supélec Math-II- 2014 Filière MP

Proposé par Mr : HAMANI Ahmed

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 $T_3(\cos(\theta)) = 4\cos^3(\theta) - 3\cos(\theta)$.
Donc par unicité, on obtient $T_1 = 1$, $T_2 = X$, $T_2 = 2X^2 - 1$ et $T_3 = 4X^3 - 3X$.

I-A-2 Expression de T_n

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

En prennant la partie réelle des deux membres, on obtient
$\cos(n\theta) = \sum_{0\le k\le n/2} C_n^{2k}(-1)^k \cos^{n-2k}(\theta)\sin^{2k}(\theta) = \sum_{0\le k\le n/2} C_n^{2k}(-1)^k \cos^{n-2k}(\theta)(1-\cos^2(\theta))^k$.

Et par unicité on aura $T_n = \sum_{0\le k\le n/2} C_n^{2k}(-1)^k X^{n-2k}(1-X^2)^k = \sum_{0\le k\le n/2} C_n^{2k} X^{n-2k}(X^2-1)^k$.

I-A-3 Une relation de récurence entre les T_n

$\forall n \in \mathbb{N}$, $T_{n+2}(\cos(\theta)) + T_n(\cos(\theta)) = \cos((n+2)\theta) + \cos(n\theta) = 2\cos((n+1)\theta)\cos(\theta) = 2\cos(\theta)T_{n+1}(\cos(\theta))$.
Ce qui entraine par unicité $T_{n+2} + T_n = 2XT_{n+1}$.

Degré et coefficient dominant de T_n.

On va montrer par une récurrence forte sur n que $\mathrm{dom}(T_n) = 2^{n-1}$ et $\deg(T_n) = n$.
- La propriété est vrai pour $n = 0, 1, 2$ et 3.
- Supposons que pour un certain $n \ge 2$, $\mathrm{dom}(T_n) = 2^{n-1}$, $\mathrm{dom}(T_{n+1}) = 2^n$, et $\deg(T_n) = n$, $\deg(T_{n+1}) = n+1$, alors, $\deg(T_{n+2}) = \deg(2XT_{n+1} - T_n) = \deg(XT_{n+1}) = 1 + n + 1 = n + 2$.
$\mathrm{dom}(T_{n+2}) = \mathrm{dom}(2XT_{n+1}) = 2\mathrm{dom}(T_{n+1}) = 22^n = 2^{n+1}$.

Une méthode qui utilise l'expression de T_n.

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

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

$$\sum_{0\le k\le n/2} C_n^{2k} = \frac{1}{2}\Big(\sum_{k=0}^{n}(1 + (-1)^k)C_n^k\Big) = \frac{1}{2}\sum_{k=0}^{n} C_n^k + \frac{1}{2}\sum_{k=0}^{n}(-1)^k C_n^k = \frac{1}{2}(1+1)^n + \frac{1}{2}(1-1)^n = 2^{n-1}.$$

En conclusion $\deg(T_n) = n$ et $\mathrm{dom}(T_n) = 2^{n-1}$.

I-A-4 Les racines de T_n

$\forall n \in \mathbb{N}^*$, $T_n(\cos(\theta)) = 0 \iff \cos(n\theta) = 0 \iff \theta = \dfrac{(2k+1)\pi}{2n}$, $k \in \mathbb{Z}$.

On a donc $\forall k \in [[0, n-1]]$, $T_n(\cos(\theta_k)) = 0$ où $\theta_k = \dfrac{(2k+1)\pi}{2n}$, de plus $\forall k \in [[0, n-1]], \theta_k \in]0, \pi[$ et la fonction cosinus est bijective de $]-1, 1[$ vers $]0, \pi[$, donc T_n admet n racines distinctes sur $]-1, 1[$, à savoir les $\cos(\theta_k)$ où $k \in [[0, n-1]]$.

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 entraine que
$\forall\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$, $\forall n \in \mathbb{N}$, $\dfrac{T'_{n+1}(\cos(\theta))}{n+1} = \dfrac{\sin((n+1)\theta)}{\sin(\theta)}$, c'est à dire $U_n(\cos(\theta)) = \dfrac{\sin((n+1)\theta)}{\sin(\theta)}$.

I-B-2 .

a) **Une relation de récurence entre les U_n**

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

$= \dfrac{2}{\sin(\theta)}(\cos(\theta)\sin((n+1)\theta)) = 2\cos(\theta)U_{n+1}(\cos(\theta))$

ce qui donne par unicité des U_n que $U_{n+2} + U_n = 2XU_{n+1}$.

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 $]-1, 1[$, donc par application du théorème des accroissements finies entre deux zéros consécutifs de T_{n+1}, on obtient un zéro de T'_{n+1}, ce qui prouve que U_n admet n racines distinctes sur $]-1, 1[$.

$\forall n \in \mathbb{N}$, $U_n(\cos(\theta)) = 0 \iff \sin((n+1)\theta) = 0 \iff (n+1)\theta = k\pi \quad , \quad k \in \mathbb{Z}$.
Donc $\forall k \in [[1,n]]$, $U_n(\cos(\varphi_k)) = 0$ où $\varphi_k = \dfrac{k\pi}{n+1}$, les $\cos(\varphi_k)$ sont distincts deux à deux grâce à la bijectivité de $\cos inus$ de $]-1,1[$ vers $]0,\pi[$.
Donc les racines de U_n sont les $\cos(\varphi_k)$ où $k \in [[1,n]]$.

II- Arithmétique des polynômes de Tchebychev

II-A Division euclidienne

II-A-1 - $\forall m,n \in \mathbb{N}$ tel que $0 \leq m \leq n$, $\cos((n+m)\theta) + \cos((n-m)\theta) = 2\cos(n\theta)\cos(m\theta)$, donc $T_{n+m}T_{n-m} = 2T_nT_m$.
$\forall n,m \in \mathbb{N}$ tel que $0 \leq m < n$, $\sin((n+m-1)\theta) + \sin((n-m-1)\theta) = 2\cos(m\theta)\sin((n-1)\theta)$, 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 $(II-A-1)$, $T_mT_{n-m} = \dfrac{1}{2}(T_n + T_{2m-n})$, 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 $(II-A-1)$,
$T_{n-m}T_m = \dfrac{1}{2}(T_n + T_{n-2m})$, 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 $Q_{n,m} = 2T_{n-m}$ 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 $(n,m) \longleftarrow (2km, m)$ où $k \in [[1,p]]$, on obtient $2T_{2km}T_m = T_{(2k+1)m} + T_{(2k-1)m}$, ce qui entraine 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 $k=p$, on obtient par téléscopie

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

Donc $T_n = T_m\left((-1)^pT_m + 2\sum_{k=1}^{p}(-1)^{p-k}T_{2km}\right)$, donc

$Q_{n,m} = (-1)^pT_m + 2\sum_{k=1}^{p}(-1)^{p-k}T_{2km}$ 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 $1 + E\left(\dfrac{n/m+1}{2}\right)$, donc admet un maximum p.
$p \in A_{n,m}$ et $p+1 \notin A_{n,m}$ donc $(2p-1)m < n \leq (2p+1)m$, or n n'est pas produit de m par un entier impair, donc $(2p-1)m < n < (2p+1)m$, c'est à dire $|n-2pm| < m$.
- $\forall k \in [[0,p-2]]$, $n-(2k+1)m \geq n-(2p-3)m \geq 2m > m$, donc
$\forall k \in [[0,p-2]]$, $2T_mT_{n-(2k+1)m} = T_{n-2km} + T_{n-(2k+2)m}$, donc
$2(-1)^kT_mT_{n-(2k+1)m} = (-1)^kT_{n-2km} - (-1)^{k+1}T_{n-(2k+2)m}$, ce qui donne par téléscopie en sommant de $k=0$ à $k=p-2$
$T_n = 2T_m\sum_{k=0}^{p-2}(-1)^kT_{n-(2k+1)m} + (-1)^{p-1}T_{n-(2p-2)m}$.
Or $m < n-(2p-2)m < 3m$, donc d'après la question a),
$T_{n-(2p-2)m} = 2T_mT_{n-(2p-1)m} - T_{|n-2pm|}$ et par suite
$T_n = 2T_m\sum_{k=0}^{p-1}(-1)^kT_{n-(2k+1)m} + (-1)^pT_{|n-2pm|}$, 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 $\exists k \in [[0,h]]$ tel que $r = \cos\left(\dfrac{k\pi}{h}\right) = \cos\left(\dfrac{kn_1\pi}{n+1}\right) = \cos\left(\dfrac{km_1\pi}{m+1}\right)$, 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 $\exists (k,k') \in [[1,n]] \times [[1,m]]$ tel que $r = \cos\left(\dfrac{k\pi}{n+1}\right) = \cos\left(\dfrac{k'\pi}{m+1}\right)$, donc $\dfrac{k\pi}{n+1} = \dfrac{k'\pi}{m+1}$ 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 entraine en posant $\dfrac{k}{n_1} = k''$ que $r = \cos\left(\dfrac{k''\pi}{h}\right)$ c'est à dire que r est une racine de U_{h-1}.
- En conclut que U_{h-1} est le pgcd de U_n et U_m.

II-B-2 **Pgcd de T_n et T_m**

a) - Soit r une racine de T_g, alors $\exists k \in [[0, g-1]]$ tel que $r = \cos\left(\frac{(2k+1)\pi}{2g}\right) = \cos\left(\frac{(2k+1)m_1\pi}{2m}\right) = \cos\left(\frac{(2k+1)n_1\pi}{2n}\right)$, 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 $\exists (k,k') \in [[0,n-1]]\times[[0,m-1]]$ tel que $r = \cos\left(\frac{(2k+1)\pi}{2n}\right) = \cos\left(\frac{(2k'+1)\pi}{2m}\right)$, 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 $r = \cos\left(\frac{n_2\pi}{2g}\right)$ et l'imparité de n_2 entraine que r est une racine de T_g.
- On conclut que T_g est le 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 qu'ils sont premiers entre eux.
- On conclut que T_n et T_m sont premiers entre eux.

c) • - Cas n, m impairs
- Cette condition exige que n_1 et m_1 sont impairs, donc d'après a), le pgcd de T_n et T_m est T_g où g est le pgcd de m et n.
• - Cas n, m des puissances de 2.
- Dans ce cas l'un des 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**
- $deg(T_n) = n$.
- $\forall \theta \in \mathbb{R}, \forall n, m \in \mathbb{N}$, $T_n o T_m(\cos(\theta)) = T_n(\cos(m\theta)) = \cos(nm\theta) = T_{nm}(\cos(\theta))$, donc par unicité $T_n o T_m = T_{nm} = T_{mn} = T_m o T_n$.

III-A-2 G **est un groupe**
- $\forall P, Q \in G$, $deg(PoQ) = deg(P).deg(Q) = 1$, donc la loi o est une loi de composition interne qui est associative.
- $\forall P \in G$, $PoX = XoP = P$, 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 $P_\alpha o Q = Q o P_\alpha$, 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 in pose $R = Q_1 - Q_2$, on aura $deg(R) < n$.
- $RoP_\alpha = Q_1 o P_\alpha - Q_2 o P_\alpha = P_\alpha o Q_1 - P_\alpha o Q_2 = Q_1^2 - Q_2^2 = (Q_1 - Q_2)(Q_1 + Q_2) = R(Q_1 + Q_2)$, ce qui donne par passage aux degrés que
$2deg(R) = deg(RoP_\alpha) = deg(R(Q_1 + Q_2)) = deg(R) + n$, donc $deg(R) = n$, ce qui est contradictoire avec $deg(R) < n$.
• - $\forall n \in \mathbb{N}^*$, 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 $\lambda^2 = X^2 o P = PoX^2 = \lambda$, 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 $\gamma \neq 0$.
- $UoP = P_\alpha o U \iff \gamma(aX^2 + bX + c) + \beta = (\gamma X + \beta)^2 + \alpha$, 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 $UoT_2oU^{-1} = P_{-2}$, donc
$Q \in \mathcal{C}(T_2) \iff QoT_2 = T_2 oQ \iff UoQoU^{-1}oP_{-2} = P_{-2}oUoQoU^{-1} \iff UoQoU^{-1} \in \mathcal{C}(P_{-2})$.

- 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 UoT_noU^{-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 $QoP_\alpha = P_\alpha oQ$ 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 $\begin{cases} 3\alpha = 2b \\ 3\alpha^2 + b = b^2 \\ \alpha^3 + b\alpha = \alpha \end{cases}$

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. avec

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 $F_2 = U^{-1}oP_\alpha oU$, or F_3 commute avec $F_2 = U^{-1}oP_\alpha oU$, donc UoF_3oU^{-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 $F_2 = U^{-1}oP_0oU = U^{-1}oX^2oU$, et par suite F_n commute avec $U^{-1}oX^2oU$, c'est à dire UoF_noU^{-1} commute avec X^2, or $\mathcal{C}(X^2) = \{0\} \cup \{X^n \ / \ n \in \mathbb{N}\}$, donc $UoF_noU^{-1} = X^n$ c'est à dire $F_n = U^{-1}oX^noU$.
• - Si $\alpha = -2$, on aura $F_2 = U^{-1}oP_{-2}oU$, donc F_n commute avec $U^{-1}oP_{-2}oU$, et par suite UoF_noU^{-1} commute avec P_{-2}, or d'après la question $(III-B-3)$, $P_{-2} = VoT_2oV^{-1}$ avec $V = 2X \in G$, ce qui entraine que $V^{-1}oUoF_noU^{-1}oV$ commute avec T_2, or $\mathcal{C}(T_2) = \{-\frac{1}{2}\} \cup \{T_n \ / \ n \in \mathbb{N}\}$, donc $WoF_noW^{-1} = T_n$ d'où $F_n = W^{-1}oT_noW$ avec $W = V^{-1}oU$.

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

IV-A **Condition nécessaire et suffisante d'inversibilité**

- $\Longrightarrow$ 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 $\det(M) = \pm 1$.
- $\Longleftarrow$ Soit $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in M_2(\mathbb{Z})$ tel que $\det(M) = \pm 1$, alors $M^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$ si $\det(M) = 1$ et $M^{-1} = \begin{pmatrix} -d & c \\ b & -a \end{pmatrix}$.

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 $G_{n+2}(x) = \frac{1}{2a^{n+2}}D_{n+2}(2xa, a^2) =$
$= \frac{1}{2a^{n+2}}(2xaD_{n+1}(2xa, a^2) - a^2D_n(2xa, a^2)) = \frac{x}{a^{n+1}}D_{n+1}(2xa, a^2) - \frac{1}{2a^n}D_n(2xa, a^2) =$
$= 2xG_{n+1}(x) - G_n(x)$.
- 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 $\forall (x, a) \in \mathbb{C}\times\mathbb{C}^*$, $D_n(2xa, a^2) = 2a^nT_n(x)$. 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 $H_{n+2}(x) = 2xH_{n+1}(x) - H_n(x)$, 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
$D_{n+2}\left(x + \frac{a}{x}, a\right) = \left(x + \frac{a}{x}\right)D_{n+1}\left(x + \frac{a}{x}, a\right) - aD_n\left(x + \frac{a}{x}, a\right) =$
$= \left(x + \frac{a}{x}\right)\left(x^{n+1} + \frac{a^{n+1}}{x^{n+1}}\right) - a\left(x^n + \frac{a^n}{x^n}\right) = x^{n+2} + \frac{a^{n+2}}{x^{n+2}}$, ce qui établie 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
$\left(x - \frac{a}{x}\right) E_{n+2}\left(x + \frac{a}{x}, a\right) = \left(x + \frac{a}{x}\right)\left(x - \frac{a}{x}\right) E_{n+1}\left(x + \frac{a}{x}, a\right) - a\left(x - \frac{a}{x}\right) E_n\left(x + \frac{a}{x}, a\right) =$
$= \left(x + \frac{a}{x}\right)\left(x^{n+2} - \frac{a^{n+2}}{x^{n+1}}\right) - a\left(x^{n+1} - \frac{a^{n+1}}{x^{n+1}}\right) = \left(x^{n+3} - \frac{a^{n+3}}{x^{n+3}}\right)$, ce qui établie la récurrence.

IV-C .

IV-C-1 On montrer cette égalité par récurrence sur $n \geq 2$.
- Pour $n = 2$, c'est le théorème de Gayley-Hamilton. $O_2 = \chi_B(B) = B^2 - \mathrm{Tr}(B)B + \det(B)I_2$, 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
$B^{n+1} = E_{n-1}(\sigma,\nu)B^2 - \nu E_{n-2}(\sigma,\nu)B = (\sigma E_{n-1}(\sigma,\nu) - \nu E_{n-2}(\sigma,\nu))\, B - \nu E_{n-1}(\sigma,\nu)I_2 =$
$= E_n(\sigma,\nu)B - \nu E_{n-1}(\sigma,\nu)I_2$, ce qui établie la récurrence.
• - Soit $\lambda, \mu \in \mathbb{C}^*$ les valeurs propres de B, alors $\lambda\mu = \det(B) = \nu$ et $\lambda + \mu = \lambda + \frac{\nu}{\lambda} = \mathrm{Tr}(B) = \sigma$, donc en profitant de la relation $(IV-1)$, on obtient
$\mathrm{Tr}(B^n) = \lambda^n + \mu^n = \lambda^n + \frac{\nu^n}{\lambda^n} = D_n\left(\lambda + \frac{\nu}{\lambda}, \nu\right) = D_n(\sigma,\nu)$.

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 $(IV-C-1)$ $\sigma = \mathrm{Tr}(B)$ et $\nu = \det(B)$, alors d'après l'égalité précédente,
$A = B^n = E_{n-1}(\sigma,\nu).B - \nu E_{n-2}(\sigma,\nu).I_2$, ce qui donne par comparaison des coefficients et en notant $B = (b_{i,j})_{1\leq i,j\leq 2}$
$a - d = (b_{1,1} - b_{2,2})E_{n-1}(\sigma,\nu)$, $\quad c = b_{2,1}E_{n-1}(\sigma,\nu)$ et $\quad b = b_{1,2}E_{n-1}(\sigma,\nu)$.
- 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
$E_{n+2}(\sigma,\nu) = \sigma E_{n+1}(\sigma,\nu) - \nu E_n(\sigma,\nu) \in \mathbb{Z}$, ce qui établie la récurrence.
- Les égalités précédentes assure la proposition (i).
- L'égalité $A = B^n$ entraine que $\tau = \mathrm{Tr}(A) = \mathrm{Tr}(B^n) = D_n(\sigma,\nu)$ (d'après la question précédente, et $\tau = \det(A) = \det(B^n) = (\det(B))^n = \nu^n$, ce qui établie (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 $(IV-1)$,
$\tau = D_n(\sigma,\nu) = D_n(\alpha + \frac{\nu}{\alpha}, \nu) = \alpha^n + \frac{\nu^n}{\alpha^n}$, 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 $(IV-1)$,
$\tau^2 - 4\delta = \left(\alpha - \frac{\nu}{\alpha}\right)^2 E_{n-1}^2(\sigma,\nu)$, or $\left(\alpha - \frac{\nu}{\alpha}\right)^2 = \left(\alpha + \frac{\nu}{\alpha}\right)^2 - 4\nu = \sigma^2 - 4\nu$, donc
$\tau^2 - 4\delta = p^2(\sigma^2 - 4\nu)$.
• $ru - st = \frac{1}{4}\left(\sigma^2 - \frac{(a-d)^2}{p^2}\right) - \frac{bc}{p^2} = \frac{1}{4}\left(\sigma^2 - \frac{(a+b)^2 - 4(ad-bc)}{p^2}\right) =$
$= \frac{1}{4}\left(\sigma^2 - \frac{\tau^2 - 4\delta}{p^2}\right) = \frac{1}{4}\left(\sigma^2 - (\sigma^2 - 4\nu)\right) = \nu$.
• C'est clair que la condition (i) entraine 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 dse entiers $\sigma - \frac{a-d}{p}$ ou $\sigma + \frac{a-d}{p}$ est pair, ce qui entraine 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 $B^n = E_{n-1}(\sigma,\nu).B - \nu E_{n-2}(\sigma,\nu).I_2$ entraine que $B^n = p.B - \nu E_{n-2}(\sigma,\nu).I_2 = \begin{pmatrix} x & b \\ c & y \end{pmatrix}$ où on a posé $x = pr - \nu E_{n-2}(\sigma,\nu)$ et $y = pu - \nu E_{n-2}(\sigma,\nu)$.
- Reste à montrer que $(x,y) = (a,d)$.
- L'égalité $\tau = D_n(\sigma,\nu) = \mathrm{Tr}(B^n)$, entraine 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 entraine 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 $B^3 = A$.