# Centrale MP 2014 Mathématiques II

**I.A.1)** $T_0 = 1$, $T_1 = X$, $T_2 = 2X^2 - 1$, $T_3 = 4X^3 - 2X$

**I.A.2)** $\cos n\theta = \dfrac{e^{in\theta} + e^{-in\theta}}{2} = \dfrac{(e^{i\theta})^n + (e^{-i\theta})^n}{2} = \dfrac{(\cos\theta + i\sin\theta)^n + (\cos\theta - i\sin\theta)^n}{2}$

$$\cos n\theta = \sum_{\ell=0}^{n} \binom{n}{\ell} \frac{(i)^\ell + (-i)^\ell}{2} (\sin\theta)^\ell (\cos\theta)^{n-\ell}$$

$$\cos n\theta = \sum_{k=0}^{E(\frac{n}{2})} \binom{n}{2k} (-1)^k (\sin\theta)^{2k} (\cos\theta)^{n-2k}$$

$$\cos n\theta = \sum_{k=0}^{E(\frac{n}{2})} \binom{n}{2k} (\cos^2\theta - 1)^k (\cos\theta)^{n-2k} = P_n(\cos\theta)$$

avec $P_n = \sum_{0 \le k \le n/2} \binom{n}{2k} (X^2-1)^k X^{n-2k}$. Ceci prouve l'existence de $T_n$

On a $\{\cos\theta, \theta \in [0, 2\pi]\}$ est infini, donc un polynôme est uniquement déterminé par ses valeurs en les $\cos\theta$. Ceci montre que $T_n$ est unique et finalement

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

---

programme Python associé.

```
From scipy import misc      # pour les coefficients binomiaux
From numpy.polynomial import Polynomial

def Tcheb(n):
    res = Polynomial([0])
    X = Polynomial([0,1])
    Y = Polynomial([-1, 0, 1])      # le polynôme X^2 - 1.
    for k in range(n//2 +1):
        res = res + misc.comb(n,2*k, True)*(Y**k)*(X**(n-2*k))
    return res

for i in range(8):
    print(Tcheb i.coef)
```

I.A.3) Pour tout $n$ entier on a, pour tout $\theta$ réel

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

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

les polynômes $T_{n+2} + T_n$ et $2XT_{n+1}$ sont égaux sur $[-1,1]$ qui est infini. Ils sont donc égaux.

On peut alors prouver facilement par récurrence que

$$\forall n \in \mathbb{N} \quad \deg T_n = n.$$
$$\operatorname{dom}(T_0) = 1$$
$$\forall n \geq 1 \quad \operatorname{dom}(T_n) = 2^{n-1}.$$

On peut retrouver ce résultat à partir de l'expression développée de $T_n$. En effet $\forall k \in [0,n]$ $\deg (X^2-1)^k X^{n-2k} = n$. donc $\deg T_n \leq n$ et le coefficient de degré de $T_n$ est

$$\sum_{k=0}^{E(n/2)} \binom{n}{2k} = \frac{1}{2}\left((1+1)^n + (1-1)^n\right) = \begin{cases} 1 & \text{si } n=0 \\ 2^{n-1} & \text{si } n \geq 1. \end{cases}$$

I.A.4) $T_n\left(\cos\frac{(2k+1)\pi}{2n}\right) = \cos\left(k\pi + \frac{\pi}{2}\right) = 0$ si $0 \leq k \leq n-1$,

de plus les $\cos\frac{2k+1}{2n}\pi$, $0 \leq k \leq n-1$ sont distincts car. cos est injectif sur $]0,\pi[$. Donc $T_n$ possède $n$ racines distinctes au moins. Or il est de degré $n$, il est donc scindé et ses racines sont les $\cos\frac{(2k+1)\pi}{2n}$ $0 \leq k \leq n-1$

---

I.B.1. $\forall \theta \in \mathbb{R}$ $-(\sin\theta)\, T'_{n+1}(\cos\theta) = -(n+1)\sin(n+1)\theta$

Donc $\forall \theta \in \mathbb{R} - \pi\mathbb{Z}$ $U_n(\cos\theta) = \dfrac{\sin(n+1)\theta}{\sin\theta}$.

I.B.2a) De $\sin(n+3)\theta + \sin(n+1)\theta = 2\cos\theta \sin(n+1)\theta$.

on déduit comme I.A.3) que

$$\forall n \geq 0 \quad U_{n+2} + U_n = 2X\,U_{n+1}$$

I.B.2b) Un calcul similaire à celui de la question I.A.4) permet de montrer que $U_n$ est scindé (pour $n \geq 1$) et que ses racines sont les $\frac{k\pi}{n+1}$, $1 \leq k \leq n$, qui sont bien dans $]-1,1[$.

---

II.A.1) Comme en I.A.3) de la relation

$$\forall (m,n) \in \mathbb{Z}^2 \quad 2\cos n\theta \cos m\theta = \cos(n+m)\theta + \cos(n-m)\theta$$

on tire

$$\forall (m,n) \in \mathbb{N}^2 \quad 0 \leq m \leq n \quad T_m T_n = \frac{1}{2}\left(T_{n+m} + T_{n-m}\right)$$

De même.

$$\forall (m,n) \in \mathbb{Z}^2 \quad 2\cos m\theta \sin n\theta = \sin(n+m)\theta + \sin(n-m)\theta.$$

donne : $\forall$

$$\forall (m,n) \in \mathbb{N}^2 \quad 0 \leq m < n \quad T_m \cdot U_{n-1} = \frac{1}{2}\left(U_{n+m-1} + U_{n-m-1}\right)$$

II.A.2) On suppose $m < n < 3m$.

Premier cas $2m \leq n < 3m$.

$$T_n = 2\,T_m\,T_{n-m} - T_{n-2m}.$$

Or $\deg T_{n-2m} = n - 2m < m = \deg T_m$.

Nous avons bien là la division euclidienne de $T_n$ par $T_m$.

- Deuxième cas $m < n < 2m$.

$$T_n = 2\,T_m\,T_{m-n} - T_{2m-n}.$$

car $\forall \theta \in \mathbb{R} \quad \cos(2m-n)\theta = \cos((n-2m)\theta)$.

$0 \leq 2m - n < m$ donc $\deg T_{2m-n} < m$, et il s'agit bien à nouveau de la division euclidienne

II.A.2b) $Q_n = 2T_m T_{n-m} - T_{n-2m}$

$= 2T_m T_{n-m} - 2T_m T_{n-3m} + T_{n-4m}$.

(On en déduit, par récurrence sur $p$, que si

$n = (2p+1)m$.

$$T_n = 2\left(T_{n-m} - T_{n-3m} + \dots + (-1)^p T_{n-(2p+1)m}\right) T_m + 0$$

donc $\underline{Q_{n,m} = 2\sum_{k=0}^{p} (-1)^k T_{n-(2k+1)m}}$ et $\underline{R_{n,m} = 0}$

II.A.2c. On effectue la division euclidienne de $n+m$ par $2m$ $\quad n+m = 2pm + r$ avec $0 \leq r < 2m$.

Or $n$ est n'est pas de la forme $(2p-1)m$ : donc $0 < r < 2m$

et $\quad m = 2pm + r - m$ avec $|r-m| < m$.

La même technique que dans la question précédente et doublé de la technique du a) donne.

$$\underline{T_n = 2\left(T_{n-m} + \dots + (-1)^{p-1} T_{n-(2p-1)m}\right) T_m + (-1)^p T_{|n-2pm|}}$$

et $|n-2pm| < m$. Il s'agit bien de la division euclidienne de $T_n$ par $T_m$.

II.B.1) $U_n$ et $U_m$ sont scindé à racines simples, leur pgcd est donc $\prod (X-\alpha)$ où $\alpha$ parcourt les racines communes de $U_n$ et $U_m$.

$\alpha$ est de la forme $\cos\left(\frac{k}{n+1}\pi\right) = \cos\left(\frac{k'}{m+1}\pi\right)$.

Ce qui conduit à $(m+1)k = (n+1)k'$.

En simplifiant par le pgcd de $(m+1)$ et $(n+1)$

$m_1 k = n_1 k'$ avec $(m_1, n_1) = 1$.

D'après le théorème de Gauss, ce qui équivaut à $k' = \ell m_1$ $k = \ell n_1$

et finalement

$$\frac{k}{n+1}\pi = \frac{\ell}{k}\pi \qquad \ell \in [1, k-1] \text{ car } \frac{k}{n+1}\pi \in ]0, \pi[.$$

finalement

$$\text{pgcd}(U_n, U_m) = \prod_{\ell=1}^{k-1} \left(X - \cos\left(\frac{\ell}{k}\pi\right)\right) = U_{k-1}.$$

II. B. 2 a) le raisonnement est le même que dans la question précédente. $\text{pgcd}(T_n, T_m) = \prod (X-\alpha)$ où $\alpha$ décrit l'ensemble des racines communes à $T_n$ et $T_m$.

$$\text{On a} \begin{cases} \cos\frac{2k+1}{2n}\pi = \cos\frac{2k'+1}{2m}\pi \iff \frac{2k+1}{n} = \frac{2k'+1}{m} \\ 0 \le k \le n-1 \qquad 0 \le k' \le m-1 \end{cases}$$

$$\iff m_1(2k+1) = n_1(2k'+1)$$

Ici $m_1$ et $n_1$ sont impairs, donc

$$m_1(2k+1) = n_1(2k'+1) \iff \begin{cases} (2k+1) = \ell\, n_1 \\ (2k'+1) = \ell\, n_1 \\ \ell \text{ impair.} \end{cases}$$

Donc $$\text{pgcd}(T_n, T_m) = \prod_{\ell'=0}^{g-1} \left(X - 2\cos\left(\frac{2\ell'+1}{2g}\pi\right)\right) = T_g.$$

II. B. 2 b) Si $m_1$ par exemple est pair, alors puisque $(m_1, n_1) = 1$ $n_1$ est impair donc $m_1(2k+1) = n_1(2k'+1)$ est impossible et $T_n$ et $T_m$ n'ont aucune racine commune et $\text{pgcd}(T_n, T_m) = 1$.

II. B. 2. c) - Si $m$ et $n$ sont impairs $m_1$ et $n_1$ aussi donc $\text{pgcd}(T_m, T_n) = T_{\text{pgcd}(m,n)}$

- Si $m = 2^p$ $n = 2^q$ si $n = m$ $\text{pgcd}(T_m, T_n) = T_m$.
si $n \neq m$ $\text{pgcd}(T_n, T_m) = 1$.

car $m_1$ ou $n_1$ est pair.

III A.1) $(T_n \circ T_m)(\cos\theta) = T_n(\cos m\theta) = \cos(nm\theta) = T_{nm}(\cos\theta)$

$\{\cos\theta\} = [-1,1]$ infini donc $\underline{T_n \circ T_m = T_{nm} = T_m \circ T_n}$.

III A.2) La loi $\circ$ est interne en effet si $P = aX+b$ $Q = cX+d$ avec $a \neq 0$ $c \neq 0$ alors $P \circ Q = acX + ad + b$.

- L'associativité découle de l'associativité de la composition.
- $X$ est élément neutre
- $\frac{1}{a}X - \frac{b}{a}$ est l'inverse de $aX+b$.

$G$ est bien un groupe pour $\circ$ (qui n'est pas commutatif)

III B 1) $Q = a_n X^n + R$ avec $a_n \neq 0$ et $\deg R < n$.

$$Q \circ P_\alpha = a_n (X^2+\alpha)^n + R(X^2+\alpha)$$

$$\underline{Q \circ P_\alpha = a_n X^{2n} + R_1} \text{ avec } \deg R_1 < 2n.$$

$$\underline{P_\alpha \circ Q = (a_n X^n + R)^2 + \alpha = a_n^2 X^{2n} + R_2} \text{ avec } \deg R_2 < 2n.$$

Si $Q \circ P_\alpha = P_\alpha \circ Q$ $\underline{a_n^2 = a_n}$. Or $a_n \neq 0$ donc $a_n = 1$.

III B.2) Soit $Q_1$ et $Q_2$ deux polynômes commutants avec $P_\alpha$. On peut écrire $\begin{cases} Q_1 = X^n + R_1 \text{ avec } \deg R_1 < n. \\ Q_2 = X^n + R_2 \end{cases}$

$P_\alpha \circ Q_1 = Q_1 \circ P_\alpha$ $P_\alpha \circ Q_2 = Q_2 \circ P_\alpha$. Par soustraction.

$$Q_1^2 - Q_2^2 = (R_1 - R_2) \circ P_\alpha.$$

$\underline{(R_1 - R_2)(Q_1 + Q_2) = (R_1 - R_2) \circ P_\alpha}$. Si $R_1 - R_2 \neq 0$ soit $p$ le degré de $R_1 - R_2$. alors $p < n$ et

$\underline{\deg (R_1 - R_2)(Q_1 + Q_2) = n + p \quad \deg (R_1 - R_2) \circ P_\alpha = 2p}$

Il y a une contradiction donc $R_1 - R_2 = 0$ et

$\underline{R_1 = R_2}$ puis $Q_1 = Q_2$

$\mathcal{C}(X^2) = \{ Q \in \mathbb{C}[X],\ Q(X^2) = Q(X)^2 \}$

Soit $Q$ non nul dans $\mathcal{C}(X^2)$ on sait que $Q$ est unitaire. $Q = X^n + R(X)$ avec $\deg R < n$.

$Q(X^2) = X^{2n} + R(X^2)$ $\quad Q(X)^2 = X^{2n} + 2X^n R(X) + R(X)^2$.

Si $R \neq 0$ $\deg R(X^2) < \deg (X^n R(X) + R(X)^2)$ donc

$Q(X^2) \neq Q(X)^2$.

Par conséquent $\mathcal{C}(X^2) \subset \{0\} \cup \{X^n, n \in \mathbb{N}\}$.

L'autre inclusion est claire $\underline{\mathcal{C}(X^2) = \{0\} \cup \{X^n, n \in \mathbb{N}\}}$

II. B. 3) On cherche $U = aX + b$ $a \neq 0$ et $\alpha$ tels que

$U \circ P = P_\alpha \circ U$ soit $a(AX^2 + BX + C) = (aX + b)^2 + \alpha$.

si $P = AX^2 + BX + C$. $A \neq 0$

Il s'agit de résoudre

$$\begin{cases} aA = a^2 \\ aB = 2ab \\ aC = b^2 + \alpha \end{cases} \qquad \begin{cases} a = A \\ b = \frac{B}{2} \\ \alpha = AC - \frac{B^2}{4} \end{cases}$$

$U$ existe et est unique $\underline{U = AX + \frac{B}{2}}$ $\underline{\alpha = AC - \frac{B^2}{4}}$

Si $\underline{P = T_2 = 2X^2 - 1}$ $\underline{U = 2X}$ $\underline{\alpha = -2}$

III. B. 4) $T_2 = U^{-1} \circ P_{-2} \circ U$

$T_2 \circ P = P \circ T_2 \iff U^{-1} \circ P_2 \circ U \circ P = P \circ U^{-1} \circ P_{-2} \circ U$

$\iff P_2 \circ (U \circ P \circ U^{-1}) = (U \circ P \circ U^{-1}) \circ P_2$

On a $\deg (U \circ P \circ U^{-1}) = \deg P$ et pour tout $n \geq 1$ il existe au plus un polynôme de degré $n$ commutant avec $P$.

2) $T_n$ commute avec $T_2$ pour $n \geq 1$.

Donc $T_n$ est le seul polynôme de degré $n$ commutant avec $T_2$ pour $n \geq 1$.

Cherchons les polynômes constants commutant avec $T_2$.

$T_2 \circ C = 2C^2 - 1 \qquad C \circ T_2 = C$.

On cherche $C$ tel que $2C^2 - 1 = C$.

on obtient $C = 1$, dont $T_0$ et $C = -\frac{1}{2}$.

On a bien $\underline{\mathcal{C}(T_2) = \{-\frac{1}{2}\} \cup \{T_n, n \in \mathbb{N}\}}$

III. C. 1) On cherche bien $\alpha$ tels qu'il existe $P$ avec $\deg P = 3$ et $P \circ P_\alpha = P_\alpha \circ P$. On sait que $P$ est unitaire. $P = X^3 + R$. avec.

$$(X^3+R)^2 + \alpha = (X^2+\alpha)^3 + R(X^2+\alpha)$$

$$\underline{X^6 + 2RX^3 + R^2 + \alpha = X^6 + 3\alpha X^4 + 3\alpha^2 X^2 + \alpha^3 + R(X^2+\alpha)}$$

Si $\deg R = 2$ on obtient une contradiction, donc $R$ est degré au plus 1.

En examinant le terme en $X^4$ $R = \frac{3\alpha}{2} X + b$.

En examinant ensuite le terme en $X^3$ on obtient $b = 0$

et finalement

$$X^6 + 3\alpha X^4 + \frac{9\alpha^2}{4} X^2 + \alpha = X^6 + 3\alpha X^4 + 3\alpha^2 X^2 + \alpha^3 + \frac{3\alpha}{2} X^2 + \frac{3\alpha^2}{2}$$

Donc $\frac{9\alpha^2}{4} = 3\alpha^2 + \frac{3\alpha}{2}$ $\qquad \underline{\alpha = 0 \text{ ou } \alpha = -2}$.

On vérifie que les valeurs $\alpha = 0$ et $\alpha = -2$ sont admissibles.

III.C.2) - Il est clair que ces deux familles vérifient III.1) car $(X^n)$ et $(T_n)$ vérifie III.1) et si $U \in G$ et $(F_n)$ vérifie III.1 alors $(U^{-1} \circ F_n \circ U)_{n\geq 0}$ vérifie aussi III.1 (car $U^{-1} \circ P \circ Q \circ U = (U^{-1} \circ P \circ U) \circ (U^{-1} \circ Q \circ U^{-1})$).

- Soit $(F_n)$ une suite de polynôme vérifiant III.1) alors il existe $U$ tel que $\underline{U \circ F_2 \circ U^{-1} = P_\alpha}$.

$\underline{P_\alpha \circ (U \circ F_3 \circ U^{-1}) = (U \circ F_3 \circ U^{-1}) \circ P_\alpha}$. et $\deg(U \circ F_3 \circ U^{-1}) = 3$. Donc d'après la question précédente. $\alpha = 0$ ou $\alpha = -2$.

$\underline{\text{Si } \alpha = 0}$ d'après III.B.2) $U \circ F_n \circ U^{-1} = X^n$. si $n \geq 0$

Soit $\underline{F_n = U^{-1} \circ X^n \circ U}$.

$\underline{\text{Si } \alpha = -2}$ d'après III.B.2) $U \circ F_n \circ U^{-1} = U_1 \circ T_n \circ U_1^{-1}$

où $U_1$ est tel que $U_1 \circ T_2 \circ U_1^{-1} = P_{-2}$.

donc $\exists U_2 = U_1^{-1} \circ U$ $\underline{\forall n \in \mathbb{N}^* \; F_n = U_2^{-1} \circ T_n \circ U_2}$

Le théorème de Block et Thielmann est prouvé

**IV.A** Si $M$ appartient à $GL_2(\mathbb{Z})$, alors il existe $N$ dans $\mathcal{M}_2(\mathbb{Z})$ telle que $MN = I_2$. Donc $\det M \det N = 1$. Or $\det M \in \mathbb{Z}$ et $\det N \in \mathbb{Z}$ donc $\det M = \pm 1$.

Réciproquement si $\det M = \pm 1$ alors $N = \frac{1}{\det M} {}^t\mathrm{com}(M)$ appartient à $\mathcal{M}_2(\mathbb{Z})$ et vérifie $MN = NM = I_2$ donc $M$ est inversible dans $\mathcal{M}_2(\mathbb{Z})$

**IV.B** Soit $\Delta_n(x) = \frac{1}{2a^n} D_n(2xa, a^2)$, alors

$\Delta_0(x) = 1$ $\Delta_1(x) = X$ et $\Delta_{n+2}(x) = x\Delta_{n+1}(x) - \Delta_n(x)$

(en divisant par $\frac{1}{2a^{n+2}}$ la relation $D_{n+2}(2xa, a^2) = 2axD_{n+1}(2ax, a^2) - a^2 D_n(2xa, a^2)$)

$(\Delta_n)_{n\geq 0}$ vérifie la même relation de récurrence que la suite de fonctions polynomiales $(T_n(x))_{n\geq 0}$ Donc.

$\forall n \in \mathbb{N}$ $\forall x \in \mathbb{R}$ $\Delta_n(x) = T_n(x)$.

$\forall n \in \mathbb{N}$ $\forall x \in \mathbb{R}$ $D_n(2xa, a^2) = 2a^n T_n(x)$.

On démontrerait de même $\forall n \in \mathbb{N}$ $\forall x \in \mathbb{R}$ $E_n(2xa, a^2) = a^2 U_n(x)$

$$D_0\left(x + \frac{a}{x}, a\right) = 2 = x^0 + \frac{a^0}{x^0}$$

$$D_1\left(x + \frac{a}{x}, a\right) = x + \frac{a}{x}.$$

On suppose.

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

alors

$$D_{n+2}\left(x + \frac{a}{x}, a\right) = \left(x + \frac{a}{x}\right)\left(x^{n+1} + \frac{a^{n+1}}{x^{n+1}}\right) - a\left(x^n + \frac{a^n}{x^n}\right) = x^{n+2} + \frac{a^{n+2}}{x^{n+2}}.$$

Le résultat est prouvé par récurrence

La deuxième relation se démontre de la même manière

IV. C.1) $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ $B^2 = \begin{pmatrix} \alpha^2+\beta\gamma & (\alpha+\delta)\beta \\ (\alpha+\delta)\gamma & \beta\gamma+\delta^2 \end{pmatrix}$

On a bien $B^2 = (\alpha+\delta) B - (\alpha\delta - \beta\gamma) I_2 = \sigma B - \nu I_2$

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

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

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

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

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

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

le résultat est alors vrai à l'ordre $n+1$.

On a donc prouvé le résultat par récurrence.

Partons de la relation $B^2 = \sigma B - \nu I_2$ et multiplions là par $B^n$. On obtient $B^{n+2} = \sigma B^{n+1} - \nu B^n$ donc

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

la suite $(tr(B^n))_{n\geq 0}$ vérifie donc la même relation de récurrence que la suite $(D_n(\sigma,\nu))_{n\geq 0}$.

Or $tr(B^0) = tr(I_2) = 2 = D_0(\sigma,\nu)$

$tr(B) = \sigma = D_1(\sigma,\nu)$.

On peut en déduire par récurrence : $\forall n \in \mathbb{N}$ $tr(B^n) = D_n(\sigma,\nu)$

IV. C.2) $A = B^n$ $A \in GL_2(\mathbb{Z})$, $B \in GL_2(\mathbb{Z})$ (car $B(B^{n-1}A^{-1}) = I_2$) donc $\det B = \pm 1$. Soit $\sigma = tr(B)$ et $\nu = \det B$, alors $\sigma \in \mathbb{Z}$ $\nu \in \mathbb{Z}$ et $\nu = \pm 1$

D'après la question précédente $tr(A) = tr(B^n) = D_n(\sigma,\nu)$

et il est clair que $\det A = (\det B)^n = \nu^n$

Si $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in Gl_2(\mathbb{Z})$, on aura

$$A = E_{n-1}(\sigma, \nu) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} - \nu E_{n-2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Or o donc.

(*) $\underline{c = E_{n-1}(\sigma, \nu)\gamma \quad b = E_{n-1}(\sigma, \nu)\beta \quad a - d = E_{n-1}(\sigma, \nu)(\alpha - \delta)}$

$E_0(\sigma, \nu) = 1 \in \mathbb{Z}$ $E_1(\sigma, \nu) = \sigma \in \mathbb{Z}$, $(\sigma, \nu) \in \mathbb{Z}^2$ donc par récurrence $\forall p \in \mathbb{N}$ $E_p(\sigma, \nu) \in \mathbb{Z}$.

Il résulte alors de (*) que $\underline{E_{n-1}(\sigma, \nu) \text{ divise } b, c \text{ et } a - d}$

IV C.3a) Soit $r_1$ et $r_2$ les racines de $X^2 - \sigma X + \nu$, on a $r_2 = \frac{\nu}{r_1}$. $(D_p(\sigma, \nu))_{p \geq 0}$ est solution de la récurrence linéaire $\underline{D_{p+2}(\sigma, \nu) - \sigma D_{p+1}(\sigma, \nu) + \nu D_p(\sigma, \nu) = 0}$

il existe donc $(\lambda, \mu) \in \mathbb{C}^2$ $\forall p$ $D_p(\sigma, \nu) = \lambda r_1^p + \mu r_2^p$,

les conditions $D_0(\sigma, \nu) = 2$ $D_1(\sigma, \nu) = \sigma = r_1 + r_2$ conduisent à $\lambda = \mu = 1$. et $\forall p$ $\underline{D_p = r_1^p + r_2^p}$.

(Si $r_1 = r_2$ alors $\sigma^2 = 4\nu$, or $\nu = \pm 1$. Donc $\nu = 1$ et $\sigma = \pm 2$.

$D_0 = 2 = 2r_1^0$ $D_1 = \sigma = 2r_1$ Donc $\forall p$ $D_p = 2r_1^p$, le résultat reste valable)

Or $\tau = D_n(\sigma, \nu) = r_1^n + r_2^n = r_1^n + \frac{\nu^n}{r_1^n} = r_1^n + \frac{\delta^n}{r_1^n}$

donc $\tau^2 - 4\delta = \left(r_1^n + \frac{\delta^n}{r_1^n}\right)^2 - 4\delta = \left(r_1^n - \frac{\delta^n}{r_1^n}\right)^2 = \left(r_1 - \frac{\nu}{r_1}\right)^2 E_{n-1}(\sigma, \nu)^2$

or $\left(r_1 - \frac{\nu}{r_1}\right)^2 = \left(r_1 + \frac{\nu}{r_1}\right)^2 - 4\nu = (r_1 + r_2)^2 - 4\nu = \sigma^2 - 4\nu$

et on a bien $(\tau^2 - 4\delta) = p^2(\sigma^2 - 4\nu)$, puis

$$ru - st = \frac{1}{4}\left(\sigma^2 - \frac{(a-d)^2}{p^2}\right) - \frac{bc}{p^2} = \frac{1}{4}\left(\sigma^2 - \frac{(a-d)^2 + 4bc}{p^2}\right) = \frac{1}{4}\left(\sigma^2 - \frac{(a+d)^2 - 4(ad-bc)}{p^2}\right)$$

$$ru - st = \frac{1}{4}\left(\sigma^2 - \frac{\tau^2 - 4\delta}{p^2}\right) = \frac{1}{4}\left(\sigma^2 - (\sigma^2 - 4\nu)\right) = \nu.$$

- $s$ et $t$ sont des entiers et $ru = \nu + st$ aussi.

$\sigma$ et $\frac{a-d}{p}$ sont des entiers, donc

$\sigma + \frac{a-d}{p}$ et $\sigma - \frac{a-d}{p}$ $\left(= \sigma + \frac{a-d}{p} - 2 \times \frac{a-d}{p}\right)$ sont

des entiers de même parité. Pour que leur produit soit divisible par 4, ce qui est le cas car $ru$ est entier, il est nécessaire qu'ils soient pairs. On en déduit que

$r$ et $u$ sont des entiers et que $B$ est dans $GL_2(\mathbb{Z})$

($B \in M_2(\mathbb{Z})$ et $\det B = ru - st = \nu = \pm 1$).

II (3.b) On a $\beta = ps$ $\alpha = pt$.

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

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

$$\operatorname{tr}(B^n) = p\sigma - 2\nu E_{n-2}(\sigma,\nu)$$

$$2 = p\sigma - 2\nu E_{n-2}(\sigma,\nu)$$

Finalement $\nu E_{n-2}(\sigma,\nu) = \frac{p\sigma - 2}{2} = \frac{p\sigma - (a+d)}{2}$

Finalement

$$B^n = p \begin{pmatrix} \frac{1}{2}\left(\sigma + \frac{a-d}{p}\right) & \frac{b}{p} \\ \frac{c}{p} & \frac{1}{2}\left(\sigma - \frac{(a-d)}{p}\right) \end{pmatrix} - \begin{pmatrix} \frac{p\sigma-(a+d)}{2} & 0 \\ 0 & \frac{p\sigma-(a+d)}{2} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A.$$

IV. (4) On cherche $\sigma$ et $\nu$ tels que $\nu \in \{-1, 1\}$

$14 = 2 = D_3(\sigma,\nu)$ $\nu^3 = -1$. Donc $\nu = -1$. $14 = \sigma^3 + 3\sigma$ $\sigma = 2$.

$E_2(2,-1) = 5$. $5 \mid 5$ $5 \mid 10$ et $5 \mid 7 - 7$. Donc $A$ est un

cube dans $GL_2(\mathbb{Z})$. Les formules données conduisent

à $A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}^3$