Polynômes de Tchebychev et de Dickson, applications

I Définitions et propriétés usuelles

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

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

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 $e^{in\theta} = \left(e^{i\theta}\right)^n$, montrer que

$$\forall n \in \mathbb{N}, \qquad T_n = \sum_{0\leqslant k\leqslant n/2} \binom{n}{2k} (X^2-1)^k\, X^{n-2k}$$

Écrire en langage Maple ou Mathematica une fonction T prenant en argument un entier naturel n et renvoyant l'expression développée du polynôme T_n.

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

$$\forall n \in \mathbb{N}, \qquad T_{n+2} = 2XT_{n+1} - T_n \tag{I.1}$$

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

I.B – Polynômes de deuxième espèce

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

$$\forall n \in \mathbb{N}, \qquad U_n = \frac{1}{n+1} T'_{n+1}$$

I.B.1) Montrer que

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

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

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

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

II Arithmétique des polynômes de Tchebychev

II.A – Division euclidienne

II.A.1) Montrer que

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

II.A.2) Pour m et n entiers naturels tels que $m \leqslant n$, 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 que

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

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

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

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

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 $\mathbb{N}$ 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 $\mathbb{R}[X]$ 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 ?

III Un théorème

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

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

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

$$\forall n \in \mathbb{N}, \quad \deg F_n = n \qquad \text{et} \qquad \forall (m,n) \in \mathbb{N}^2, \qquad F_n \circ F_m = F_m \circ F_n \tag{III.1}$$

Il est clair que la famille $(X^n)_{n\in\mathbb{N}}$ convient.

On note G l'ensemble des polynômes complexes de degré 1, et pour $\alpha \in \mathbb{C}$, on pose $P_\alpha = X^2 + \alpha$.

III.A – Préliminaires

III.A.1) Montrer que la famille $(T_n)_{n\in\mathbb{N}}$ vérifie la propriété (III.1). 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 $\alpha \in \mathbb{C}$ et soit 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 $n \geqslant 1$, 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 $U \in G$ et $\alpha \in \mathbb{C}$ tels que $U \circ P \circ U^{-1} = P_\alpha$. Déterminer ces deux éléments lorsque $P = T_2$.

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

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 $(F_n)_{n\in\mathbb{N}}$ vérifie (III.1), alors il existe $U \in G$ tel que

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

IV Puissances dans $\mathrm{GL}_2(\mathbb{Z})$

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

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

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

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

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

$$D_{n+2}(x,a) = x\,D_{n+1}(x,a) - a\,D_n(x,a) \qquad \text{et} \qquad E_{n+2}(x,a) = x\,E_{n+1}(x,a) - a\,E_n(x,a)$$

Justifier la relation suivante avec les polynômes de Tchebychev

$$\forall (x,a) \in \mathbb{C}^2, \qquad D_n(2xa, a^2) = 2a^n T_n(x) \quad \text{et} \quad E_n(2xa, a^2) = a^n U_n(x)$$

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

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

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

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \tau = \operatorname{Tr} A \qquad \delta = \det A$$

IV.C.1) Soit $B \in \mathrm{GL}_2(\mathbb{Z})$. On note, *dans cette question uniquement*, $\sigma = \operatorname{Tr} B$ et $\nu = \det B$. Montrer pour tout $n \geqslant 2$, 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 que $\operatorname{Tr}(B^n) = D_n(\sigma,\nu)$.

IV.C.2) En déduire que si A est une puissance n-ième ($n \geqslant 2$) dans $\mathrm{GL}_2(\mathbb{Z})$, alors il existe $\sigma \in \mathbb{Z}$ et $\nu \in \{-1,1\}$ 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 $\mathrm{GL}_2(\mathbb{Z})$ pour lequel il existe $\sigma \in \mathbb{Z}$ et $\nu \in \{-1,1\}$ 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

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

a) En introduisant une racine complexe du polynôme $X^2 - \sigma X + \nu$ et à l'aide de (IV.1), montrer que

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

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

b) Montrer que $A = B^n$.

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

• • • FIN • • •
