Polynômes

1 Rappels

Définition 1. *Un polynôme P à coefficients dans $\mathbb{K}$ est la donnée d'une suite $(a_n)_{n\in\mathbb{N}}\in\mathbb{K}^{\mathbb{N}}$ presque nulle (c'est-à-dire qui à partir d'un certain rang ne prend plus que la valeur 0 ou, ce qui revient au même, n'a qu'un nombre fini de termes non nuls, et on peut écrire :*

$P(X)=\sum_{n=0}^{+\infty} a_n X^n$. *(On peut utiliser indifféremment P ou $P(X)$ dans une telle écriture)*

*Le **degré** de P, que l'on notera $d(P)$ vaut ou bien $-\infty$ si tous les coefficients de P sont nuls, ou bien n si $a_n\neq 0$ et si pour tout $k>n$, $a_k=0$. Si P est de degré n, a_n est appelé le **coefficient dominant** de P, $a_n X^n$ le **terme dominant** de P.*

L'ensemble des polynômes est noté $\mathbb{K}[X]$ et, si $n\in\mathbb{N}$, on désigne par $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré au plus n.

Définition 2. *(et proposition) Soient $P(X)=\sum_{n=0}^{+\infty} a_n X^n$ et $Q(X)=\sum_{n=0}^{+\infty} b_n X^n$ deux polynômes, alors on désigne par $P+Q$ le polynôme $\sum_{n=0}^{+\infty}(a_n+b_n)X^n$, par $P\times Q$ le polynôme $\sum_{n=0}^{+\infty} c_n X^n$ où pour tout n, $c_n=\sum_{k=0}^{n} a_k b_{n-k}$.*

Alors $d(P+Q)\leqslant\max(d(P),d(Q))$. Si $d(P)\neq d(Q)$, alors $d(P+Q)=\max(d(P),d(Q))$. (Si P et Q ont le même degré, alors une étude supplémentaire est nécessaire, par exemple pour savoir si les termes dominants de P et Q s'annulent ou non...)

De plus $d(P\times Q)=d(P)+d(Q)$.

Proposition 3. *Soit $n\in\mathbb{N}$, alors $\mathbb{K}_n[X]$ est de dimension finie $n+1$. $(1,X,\cdots,X^n)$ en est une base, nommée base canonique de $\mathbb{K}_n[X]$.*

Toute famille de polynômes de degrés deux à deux distincts est libre, et en particulier si $(P_0,\cdots,P_n)$ est une famille de polynômes tels que $\forall k\in[\![0,n]\!], d(P_k)=k$, alors $(P_0,\cdots,P_n)$ est une base de $\mathbb{K}_n[X]$ (théorème des degrés étagés, ou échelonnés)

Définition 4. *Soit $P(X)=\sum_{n=0}^{+\infty} a_n X^n$, alors on désigne par P' ou $D(P)$ le polynôme $\sum_{n=1}^{+\infty} n\, a_n X^{n-1}=\sum_{n=0}^{+\infty}(n+1)\,a_{n+1}X^n$ qu'on appelle le polynôme dérivé de P. Rien n'interdit de dériver à nouveau et on notera si $k\in\mathbb{N}^*$, le polynôme $D\circ\cdots\circ D(P)=P^{(k)}$ obtenu et réitérant k fois le procédé précédent.*

Proposition 5. *Soit $P\in\mathbb{K}[X]$, alors si $d(P)>0$, $d(P')=d(P)-1$, et sinon $d(P')=-\infty$. (Pour éviter la discussion, l'inégalité $d(P')\leqslant d(P)-1$ est moins précise, mais au moins est-elle toujours vraie).*

Si $k\in\mathbb{N}^*$ et si $d(P)\geqslant k$, alors $d(P^{(k)})=d(P)-k$ et sinon $P^{(k)}=0$ (et on a toujours $d(P^{(k)})\leqslant d(P)-k$.)

Théorème 6. *(division euclidienne) Soient $A\in\mathbb{K}[X]$ et $B\in\mathbb{K}[X]\setminus\{0\}$, alors il existe $(Q,R)\in\mathbb{K}[X]^2$ unique tel que $A=BQ+R$ et $d(R)<d(B)$. Q et R sont appelés **quotient** et **reste** de la **division euclidienne** de A par B.*

Proposition 7. *Soient A et B deux polynômes, B étant non nul, alors B divise A (ce que l'on peut noter $B|A$) si, et seulement si le reste de la division euclidienne de A par B est nul.*

Proposition 8. *(formules de Taylor) soit $P\in\mathbb{K}[X]$ et $\lambda\in\mathbb{K}$, alors*

$$P(\lambda+X)=\sum_{n=0}^{+\infty}\frac{P^{(n)}(\lambda)}{n!}X^n, P(X)=\sum_{n=0}^{+\infty}\frac{P^{(n)}(\lambda)}{n!}(X-\lambda)^n$$

Définition 9. *(et proposition) Soit $P\in\mathbb{K}[X]$ et $\lambda\in\mathbb{K}$, alors on dit que λ est une **racine** de P si et seulement si $P(\lambda)=0$ si et seulement si $X-\lambda$ divise P.*

*λ est **racine** de P d'**ordre de multiplicité** m si, et seulement si l'une des conditions suivantes (équivalentes) est satisfaite :*

i. $(X-\lambda)^m$ divise P mais $(X-\lambda)^{m+1}$ ne divise pas P

ii. Il existe $Q\in\mathbb{K}[X]$ tel que $P(X)=(X-\lambda)^m Q(X)$ et $Q(\lambda)\neq 0$

iii. $P(\lambda)=\cdots=P^{(m-1)}(\lambda)=0$ et $P^{(m)}(\lambda)\neq 0$.

*(Si $m=1$, on parle de racine **simple**, et si $m=2$, on parle de racine **double**)*

Proposition 10. *Si $\lambda_1, \cdots, \lambda_n$ sont des racines deux à deux distinctes de P d'ordres de multiplicité respectifs $m_1, \cdots, m_n$, alors $(X-\lambda_1)^{m_1} \cdots (X-\lambda_n)^{m_n}$ divise P.*

Une conséquence est qu'un polynôme non nul P ne peut avoir, comptées avec leurs multiplicités, davatange de racines que son degré.

Remarque 11. On utilise souvent la proposition qui précède ainsi : $d(P) \leqslant n$, mais on voit que P admet $n+1$ racines distinctes (ou $n+1$ racines comptées avec leurs multiplicités) et ainsi P ne peut qu'être nul.

Définition 12. *$P \in \mathbb{K}[X]$ non nul est dit **scindé** si la somme des multiplicités de ses racines vaut $d(P)$, autrement dit s'il s'écrit sous la forme $\lambda (X-\lambda_1)^{m_1} \cdots (X-\lambda_n)^{m_n}$ où $\lambda \in \mathbb{K}^*$ est bien sûr le coefficient dominant de P et où $\lambda_1, \cdots, \lambda_n$ sont les racines de P de multiplicités respectives $m_1, \cdots, m_n$.*

*Il est dit **simple** ou encore **scindé à racines simples** s'il admet exactement autant de racines deux à deux distinctes que son degré, autrement dit s'il s'écrit sous la forme $\lambda (X-a_1) \cdots (X-a_n)$ où $a_1, \cdots, a_n$ sont deux à deux distincts.*

Définition 13. *$P \in \mathbb{K}[X]$ est dit **irréductible** s'il est non constant et si de plus ses seuls diviseurs sont les polynômes constants non nuls et les polynômes qui lui sont associés (autrement dit les polynômes prenant la forme $\lambda \cdot P$)*

Théorème 14. *Tout polynôme P non nul à coefficients dans $\mathbb{K}$ admet, à l'ordre des termes près, une unique décomposition en un produit de facteurs irréductibles unitaires.*

Théorème 15. *(D'Alembert-Gauss) Soit $P \in \mathbb{C}[X]$ non constant, alors P admet au moins une racine $a \in \mathbb{C}$.*

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 n'ayant pas de racine réelle (autrement dit les polynômes de degré 2 dont le discriminant est strictement négatif)

Corollaire 16. *Tout polynôme complexe est scindé.*

Proposition 17. *(Somme et produit de racines d'un polynôme scindé) Soit P un polynôme scindé, s'écrivant sous la forme $\lambda (X-\lambda_1) \cdots (X-\lambda_n)$ (où les λ_i ne sont pas ici supposés deux à deux distincts), et supposons que $P(X) = a_n X^n + \cdots + a_0$, alors $\sum \lambda_k = -\frac{a_{n-1}}{a_n}$, $\prod \lambda_k = (-1)^n \frac{a_0}{a_n}$*

2 Polynômes interpolateurs de Lagrange

Vous avez déjà vu, sans le savoir, des polynômes interpolateurs de Lagrange. Par exemple, en cherchant une fonction affine connue par deux valeurs particulières (ce qui revient à chercher une droite passant par deux points), vous cherchez déjà un polynôme interpolateur de Lagrange…

Lemme 18. *Soient $(a_0, \cdots, a_n)$ des éléments de $\mathbb{K}$ deux à deux distincts, alors $\varphi : \mathbb{K}_n[X] \to \mathbb{K}^{n+1}$ définie par $\forall P \in \mathbb{K}_n[X]$, $\varphi(P) = (P(a_0), \cdots, P(a_n))$ est un isomorphisme.*

Corollaire 19. *Etant donnés $(a_0, \cdots, a_n)$ des éléments de $\mathbb{K}$ deux à deux distincts, et $(b_0, \cdots, b_n)$ des éléments de $\mathbb{K}$ quelconques, alors il existe $P \in \mathbb{K}_n[X]$ unique tel que $P(a_0) = b_0, P(a_1) = b_1, \cdots, P(a_n) = b_n$.*

*Cet unique polynôme est appelé **polynôme interpolateur de Lagrange relatif aux points (a_k, b_k)**.*

2.1 Base $(L_0, \cdots, L_n)$

Notation 20. *Etant donnés $(a_0, \cdots, a_n)$ des éléments de $\mathbb{K}$ deux à deux distincts, et $k \in [\![0, n]\!]$, on note L_k le polynôme interpolateur relatif aux $(a_i, \delta_{i,k})$ pour $0 \leqslant i \leqslant n$ (où $\delta_{i,k}$ est le symbole de Kronecker : il vaut 1 si $i = k$ et 0 sinon)*

Exercice 1. Donnez l'expression de L_k

Proposition 21. *$(L_0, \cdots, L_n)$ est une base de $\mathbb{K}_n[X]$. De plus, étant donné $P \in \mathbb{K}_n[X]$, alors les coordonnées de P selon $(L_0, \cdots, L_n)$ sont .. Enfin, $L_0 + \cdots + L_n$ est le polynôme constant 1.*

3 Polynômes de matrices et d'endomorphismes

Etant donnés u un endomorphisme d'un $\mathbb{K}$-espace vectoriel E, et $k \in \mathbb{N}$, on désigne par u^k l'endomorphisme défini par récurrence par : $u^0 = \mathrm{Id}_E$ et, pour tout $k \in \mathbb{N}$, $u^{k+1} = u^k \circ u$. Il est alors une propriété bien connue que pour tout (k, l), $u^{k+l} = u^k \circ u^l$.

De même, si $A \in M_n(\mathbb{K})$, A^k est aussi défini par récurrence par $A^0 = I_n$ et pour tout k, $A^{k+1} = A^k \times A$.

Il va sans dire que si A est la matrice de u selon une certaine base $\mathcal{B}$ de E, alors pour tout k, A^k est la matrice de u^k selon cette même base $\mathcal{B}$ de E.

et $P(X) = a_p X^p + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$, on note $P(u)$ l'endomorphisme $a_p u^p + \cdots + a_1 u + a_0 \mathrm{Id}_E$, et si $A \in M_n(\mathbb{K})$, on désigne par $P(A)$ la matrice $a_p A^p + \cdots + a_1 A + a_0 I_n$.

Remarque 22. Ne pas oublier que le coefficient constant a_0 du polynôme devient $a_0 \mathrm{Id}_E$ pour un polynôme d'endomorphisme, et $a_0 I_n$ pour un polynôme de matrice. On le retient assez aisément en notant que $P(X) = a_p X^p + \cdots + a_0 X^0$ et qu'ainsi $P(u) = a_p u^p + \cdots + a_0 u^0 = a_p u^p + \cdots + a_0 \mathrm{Id}_E$ et que $P(A) = a_p A^p + \cdots + a_0 A^0 = a_p A^p + \cdots + a_1 A + a_0 I_n$.

Proposition 23. *Soit u un endomorphisme de E et $(P, Q) \in \mathbb{K}[X]$, $A \in M_n(\mathbb{K})$ alors*

1. $\forall (\lambda, \mu) \in \mathbb{K}^2, (\lambda P + \mu Q)(u) = \lambda P(u) + \mu Q(u)$ *et* $(\lambda P + \mu Q)(A) = \lambda P(A) + \mu Q(A)$.
2. $(P \times Q)(u) = P(u) \circ Q(u)$ *et* $(P \times Q)(A) = P(A) \times Q(A)$

Remarque 24. Sur $\mathbb{K}[X]$, on sait que la multiplication est commutative. Il n'en va pas de même de la composition $\circ$ des endomorphismes de E ou du produit matriciel. Néanmoins, étant donnés deux polynômes P et Q, alors comme $P \times Q = Q \times P$, on déduit de ce qui précède que les endomorphismes $P(u)$ et $Q(u)$ (respectivement les matrices $P(A)$ et $Q(A)$) commutent.

Un cas particulier est celui de u et de $P(u)$ qui eux aussi commutent.

Une conséquence est que l'image et le noyau de $P(u)$ sont stables par u.

Proposition 25. *Soit $(A, B) \in M_n(\mathbb{K})$ et $Q \in \mathbb{K}[X]$. On suppose qu'il existe $P \in GL_n(\mathbb{K})$ telle que $B = PAP^{-1}$ (A et B sont **semblables**), alors $Q(B) = PQ(A)P^{-1}$ (ainsi $Q(A)$ et $Q(B)$ sont semblables à leur tour)*

3.1 Application au calcul d'inverses et de puissances de matrices

Le plus simple est d'étudier un exercice :

Exercice 2. Soit A la matrice $\begin{pmatrix} 1 & 0 & 0 \\ -1 & -1 & 1 \\ -3 & -6 & 4 \end{pmatrix}$

1. Calculer $A^2 - 3A + 2I_3$
2. En déduire l'inversibilité de A et la valeur de A^{-1}
3. Calculer, pour tout $n \in \mathbb{N}$, A^n.

4 Rappel : formule du binôme et une application (Tchebychev)

Théorème 26. *Etant donnés deux complexes x et y (ou deux matrices A et B d'ordre p qui commutent) :*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \left(\text{resp. } (A+B)^n = \sum_{k=0}^{n} \binom{n}{k} A^k B^{n-k} \text{ où } A^0 = B^0 = I_p \right)$$

Exercice 3. Soit $n \in \mathbb{N}$, montrer l'existence et l'unicité d'un polynôme $T_n \in \mathbb{R}[X]$ tel que pour tout $\theta \in \mathbb{R}$

$$T_n(\cos(\theta)) = \cos(n\theta)$$

Préciser de plus le degré de T_n, son coefficient dominant et montrer que T_n admet n racines simples, toutes dans $[-1, 1]$.