Université Aix–Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

Cours à distance – Semaine 5 – Polynômes – Racines et dérivation

On fixe $\mathbb{K}$ un corps commutatif, par exemple $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

4 Polynômes et analyse

La notion de polynôme est souvent confondue avec celle de fonction polynomiale. Les deux sont toutefois étroitement liées et s'enrichissent l'une l'autre. Dans ce chapitre, nous tâcherons de récupérer, algébriquement, tout ce que l'analyse [1] des fonctions polynomiales apporte.

4.1 Fonctions polynomiales et racines

Mais commençons par expliciter la distinction polynôme/fonction polynomiale.

Définition 4.1.1. Pour tout polynôme $P =: \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, on définit l'*application polynomiale* associée par

$$f_P : \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & \sum_{k=0}^{n} a_k x^k \end{array}.$$

Proposition 4.1.2. L'application

$$\xi_{\mathbb{K}} : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathcal{F}(\mathbb{K},\mathbb{K}) \\ P & \longmapsto & f_P \end{array},$$

où $\mathcal{F}(\mathbb{K},\mathbb{K})$ est l'anneau des applications de $\mathbb{K}$ dans $\mathbb{K}$, est un morphisme unitaire d'anneaux. Lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, on peut même remplacer $\mathcal{F}(\mathbb{K},\mathbb{K})$ par l'anneau des applications continues, dérivables, infiniment dérivables ou même analytiques.

Démonstration. En notant $P_1 := a_0 + a_1 X + \cdots + a_{n_1} X^{n_1} \in \mathbb{K}[X]$, $a_n := 0$ pour $n > n_1$, $P_2 := b_0 + b_1 X + \cdots + b_{n_2} X^{n_2} \in \mathbb{K}[X]$ et $b_n := 0$ pour $n > n_2$, on a bien, pour tout $x \in \mathbb{K}$,

- $\big(\xi_{\mathbb{K}}(P_1 + P_2)\big)(x) = \sum_{i=0}^{\max(n_1,n_2)} (a_i + b_i) x^i = \sum_{i=0}^{n_1} a_i x^i + \sum_{i=0}^{n_2} b_i x^i = \big(\xi_{\mathbb{K}}(P_1) + \xi_{\mathbb{K}}(P_2)\big)(x)$;
- $\big(\xi_{\mathbb{K}}(P_1.P_2)\big)(x) = \sum_{i=0}^{n_1+n_2} \big(\sum_{j=0}^{i} a_j b_{i-j}\big) x^i = \sum_{i=0}^{n_1+n_2} \sum_{j=0}^{i} a_j x^j . b_{i-j} x^{i-j}$
$= \big(\sum_{i=0}^{n_1} a_i x^i\big).\big(\sum_{i=0}^{n_2} b_i x^i\big) = \big(\xi_{\mathbb{K}}(P_1).\xi_{\mathbb{K}}(P_2)\big)(x)$;
- $\big(\xi_{\mathbb{K}}(1)\big)(x) = 1$.

On en déduit que $\xi_{\mathbb{K}}(P_1 + P_2) = \xi_{\mathbb{K}}(P_1) + \xi_{\mathbb{K}}(P_2)$, $\xi_{\mathbb{K}}(P_1.P_2) = \xi_{\mathbb{K}}(P_1).\xi_{\mathbb{K}}(P_2)$ et $\xi_{\mathbb{K}}(1) = 1$, c'est-à-dire que $\xi_{\mathbb{K}}$ est un morphisme unitaire d'anneaux. $\square$

Notation 4.1.3. Par abus de notation, pour tout $P \in \mathbb{K}[X]$ et tout $\alpha \in \mathbb{K}$, on notera dans la suite $P(\alpha)$ pour $f_P(\alpha)$.

Un premier élément, de nature a priori analytique, que nous offrent les fonctions polynomiales, ce sont les racines en lesquelles un polynôme “s'annule”. Donnons une définition algébrique de ces racines et montrons ensuite que cela correspond à notre intuition.

1. au sens de vos cours d'analyse

Définition 4.1.4. On dit que $\alpha \in \mathbb{K}$ est *racine* de $P \in \mathbb{K}[X]$ si P est divisible par $X - \alpha$.

Proposition 4.1.5. Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors α est racine de P si et seulement si $P(\alpha) = 0$.

Démonstration. Si α est racine de P, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)Q$ et on a $P(\alpha) = (\alpha - \alpha)Q(\alpha) = 0$.

Réciproquement, supposons que $P(\alpha) = 0$. Par division euclidienne de P par $X-\alpha$, il existe $Q, R \in \mathbb{K}[X]$ tels que $P = Q.(X - \alpha) + R$ avec $\deg(R) < \deg(X - \alpha) = 1$. Le polynôme R est donc constant égal à $\beta \in \mathbb{K}$. Mais on a alors $R = \beta = Q(\alpha)(\alpha - \alpha) + \beta = P(\alpha) = 0$. On en déduit que $P = Q.(X - \alpha)$ et donc que $X - \alpha$ divise P. □

Outre le fait de rester dans le monde "algébrique", la définition 4.1.4 a d'autres vertus. Il en découle, par exemple, directement ce qui suit.

Proposition 4.1.6. Tout polynôme $P \in \mathbb{K}[X]^*$ non nul admet au plus $\deg(P)$ racines distinctes.

Démonstration. Soit $\alpha_1 \neq \alpha_2 \in \mathbb{K}$ deux racines de P. On a alors $(\alpha_2 - \alpha_1)^{-1}(X - \alpha_1) + (\alpha_1 - \alpha_2)^{-1}(X - \alpha_2) = 1$, et donc $\text{pgcd}(X - \alpha_1, X - \alpha_2) = 1$. Tous les monômes $X - \alpha$, avec α racine de P, sont donc premiers entre eux et ils divisent tous P. D'après le dernier point de la proposition 3.2.6, leur produit divise P et son degré, correspondant au nombre de racines distinctes de P, est donc inférieur à celui de P. □

Cette propriété permet d'expliquer en partie pourquoi, lorsqu'on travaille dans $\mathbb{R}$ ou $\mathbb{C}$, les polynômes sont souvent confondues avec les applications polynomiales. La remarque qui suit montre qu'il faut toutefois faire attention lorsqu'on travaille sur d'autres corps.

Corollaire 4.1.7. Si $\mathbb{K}$ est de cardinal infini, alors l'application $\xi_{\mathbb{K}}$ est injective.

Démonstration. Soit $P \in \text{Ker}(\xi_{\mathbb{K}})$. Alors, pour tout $x \in \mathbb{K}$, x est racine de P. Or, d'après la proposition 4.1.6, si P est non nul, il ne peut posséder qu'un nombre fini de racines. Par contraposée, on en déduit que $P = 0$ et donc que $\xi_{\mathbb{K}}$ est injective. □

Remarque 4.1.8. Dans le cas $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, le corollaire 4.1.7 permet d'identifier les notions de polynôme et de fonction polynomiale. C'est un avantage, mais aussi un inconvénient car cela est susceptible de générer un certain nombre de confusions (notamment chez les étudiants). Pour un corps fini, ces deux notions diffèrent en effet nécessairement car $\mathcal{F}(\mathbb{K}, \mathbb{K})$ est alors de cardinal fini mais pas $\mathbb{K}[X]$; pour $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, par exemple, l'application $f_{X(X+1)}$ est triviale sans que $X(X + 1) = X + X^2$ ne le soit.

Plus généralement, on peut montrer que l'application $\xi_{\mathbb{K}}$ est injective si et seulement si $\mathbb{K}$ est infini, et qu'elle est surjective si et seulement si $\mathbb{K}$ est fini. On remarquera de fait que $\xi_{\mathbb{K}}$ n'est jamais un isomorphisme d'anneaux.

La proposition 4.1.6 peut être raffinée en comptant les racines "avec multiplicité".

Lemme 4.1.9. Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ une racine de P. Alors il existe un unique $k_0 \in \mathbb{N}^*$ tel que P soit divisible par $(X - \alpha)^{k_0}$ mais pas par $(X - \alpha)^{k_0+1}$.

Démonstration. Si $\alpha \in \mathbb{K}$ est racine de $P \in \mathbb{K}[X]$, c'est que $X - \alpha$ divise P. De plus, si $(X - \alpha)^{k+1}$ divise P avec $k \in \mathbb{N}^*$, alors $(X - \alpha)^k$ aussi. Enfin, d'après le lemme 3.1.1, $(X - \alpha)^{\deg(P)+1}$ ne peut pas diviser P. On en déduit que l'ensemble $I_\alpha := \{k \in \mathbb{N}^* \mid (X - \alpha)^k \text{ divise } P\}$ est un ensemble fini non vide de la forme $\{1, 2, \ldots, k_0 - 1, k_0\}$ et que $k_0 := \max I_\alpha$ est l'unique entier vérifiant les propriétés voulues. □

Définition 4.1.10. Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ une racine de P. On appelle *multiplicité* de α l'unique $k \in \mathbb{N}^*$ tel que P soit divisible par $(X-\alpha)^k$ mais pas par $(X-\alpha)^{k+1}$. Si α est racine de multiplicité 1, on parle de *racine simple*, sinon on parle de *racine multiple*.

Remarque 4.1.11. D'après la proposition 4.1.5, α est donc racine de P avec multiplicité k si et seulement si $P = (X-\alpha)^k Q$ avec $Q(\alpha) \neq 0$.

Proposition 4.1.12. Tout polynôme $P \in \mathbb{K}[X]^*$ non nul admet au plus $\deg(P)$ racines, comptées avec multiplicité, c'est-à-dire

$$\sum_{\alpha \text{ racine de } P} k_\alpha \leq \deg(P),$$

où k_α est la multiplicité de α comme racine de P.

Démonstration. On va procéder comme pour la preuve de la proposition 4.1.6, mais pour cela, il faut montrer que, pour $\alpha \neq \beta \in \mathbb{K}$ racines de P, les polynômes $(X-\alpha)^{k_\alpha}$ et $(X-\beta)^{k_\beta}$ sont premiers entre eux. Supposons donc par l'absurde qu'il existe un facteur commun Q, que l'on suppose irréductible, alors Q divise $(X-\alpha)^{k_\alpha}$ et donc, en itérant le lemme d'Euclide, il divise $X-\alpha$. De même, il divise $X-\beta$. Or nous avons déjà montré que $X-\alpha$ et $X-\beta$ sont premiers entre eux, ils ne peuvent donc pas posséder de diviseur commun non trivial. □

4.2 Dérivation

Dans le cas des fonctions polynomiales réelles, les racines multiples se détectent grâce à l'annulation des dérivées successives. Ce principe a un pendant algébrique.

Définition 4.2.1. Pour tout $P =: \sum_{k=0}^{\deg(P)} a_k X^k \in \mathbb{K}[X]$, on définit la *dérivée* de P par

$$P' := \sum_{k=1}^{\deg(P)} k a_k X^{k-1}.$$

Pour tout $n \in \mathbb{N}$, on définit alors récursivement la $n^{\text{ième}}$ *dérivée* de P par $P^{(0)} := P$ lorsque $n = 0$ et $P^{(n)} = (P^{(n-1)})'$ lorsque $n > 0$.

Remarque 4.2.2. Cette définition est motivée par le fait que, pour tout $P \in \mathbb{R}[X]$, $f_{P'} = f'_P$.

Proposition 4.2.3.
- Pour tout $P \in \mathbb{K}[X]$, $\deg(P') = \deg(P) - 1$ si $\deg(P) \geq 1$ et $\deg(P') = -\infty$ si $\deg(P) \leq 0$.
- Pour tous $P_1, P_2 \in \mathbb{K}[X]$, on a
  - $(P_1 + P_2)' = P_1' + P_2'$;
  - $(P_1.P_2)' = P_1'.P_2 + P_1.P_2'$.
- Pour tout $P \in \mathbb{K}[X]$ et tout $n \in \mathbb{N}^*$, on a $(P^n)' = nP'.P^{n-1}$. En particulier, pour tout $\alpha \in \mathbb{K}$ et $n \in \mathbb{N}^*$, on a $\big((X-\alpha)^n\big)' = n(X-\alpha)^{n-1}$.

Remarque 4.2.4. L'application $D \colon \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ P & \longmapsto & P' \end{array}$ est donc un endomorphisme d'espace vectoriel, mais pas un endomorphisme d'anneaux !

Démonstration. Le premier point se vérifie directement lorsque $\deg(P) \leq 1$ et provient de ce que $\deg(P).a_{\deg(P)} \neq 0$ lorsque $\deg(P) \geq 1$.

Montrons maintenant le second point. Soit $P_1, P_2 \in \mathbb{K}[X]$ dont on note respectivement $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ les coefficients. Par définition, on a

$$\begin{aligned}
P_1' + P_2' &= \sum_{k=1}^{\deg(P_1)} k a_k X^{k-1} + \sum_{k=1}^{\deg(P_2)} k b_k X^{k-1} = \sum_{k=1}^{\max\left(\deg(P_1),\deg(P_2)\right)} k(a_k+b_k)X^{k-1} \\
&= \left(\sum_{k=0}^{\max\left(\deg(P_1),\deg(P_2)\right)} (a_k+b_k)X^k\right)' = (P_1+P_2)'
\end{aligned}$$

ainsi que

$$\begin{aligned}
P_1.P_2' + P_1'.P_2 &= \left(\sum_{k=0}^{\deg(P_1)} a_k X^k\right).\left(\sum_{k=1}^{\deg(P_2)} k b_k X^{k-1}\right) + \left(\sum_{k=1}^{\deg(P_1)} k a_k X^{k-1}\right).\left(\sum_{k=0}^{\deg(P_2)} b_k X^k\right) \\
&= \left(\sum_{k=0}^{\deg(P_1)} a_k X^k\right).\left(\sum_{k=0}^{\deg(P_2)-1} (k+1) b_{k+1} X^{k}\right) + \left(\sum_{k=0}^{\deg(P_1)-1} (k+1) a_{k+1} X^{k}\right).\left(\sum_{k=0}^{\deg(P_2)} b_k X^k\right) \\
&= \sum_{k=0}^{\deg(P_1)+\deg(P_2)-1}\left(\sum_{\substack{i_1,i_2\in\mathbb{N}\\ i_1+i_2=k}} a_{i_1}(i_2+1)b_{i_2+1}\right)X^k + \sum_{k=0}^{\deg(P_1)+\deg(P_2)-1}\left(\sum_{\substack{i_1,i_2\in\mathbb{N}\\ i_1+i_2=k}} (i_1+1)a_{i_1+1}b_{i_2}\right)X^k \\
&= \sum_{k=0}^{\deg(P_1)+\deg(P_2)-1}\left(\sum_{\substack{i_1,i_2\in\mathbb{N}\\ i_1+i_2=k+1}} i_2 a_{i_1}b_{i_2}\right)X^k + \sum_{k=0}^{\deg(P_1)+\deg(P_2)-1}\left(\sum_{\substack{i_1,i_2\in\mathbb{N}\\ i_1+i_2=k+1}} i_1 a_{i_1}b_{i_2}\right)X^k \\
&= \sum_{k=0}^{\deg(P_1)+\deg(P_2)-1}\sum_{\substack{i_1,i_2\in\mathbb{N}\\ i_1+i_2=k+1}} (i_2+i_1)a_{i_1}b_{i_2}X^k = \sum_{k=0}^{\deg(P_1)+\deg(P_2)-1}\sum_{\substack{i_1,i_2\in\mathbb{N}\\ i_1+i_2=k+1}} (k+1)a_{i_1}b_{i_2}X^k \\
&= \sum_{k=0}^{\deg(P_1)+\deg(P_2)-1}(k+1)\left(\sum_{\substack{i_1,i_2\in\mathbb{N}\\ i_1+i_2=k+1}} a_{i_1}b_{i_2}\right)X^k = \sum_{k=1}^{\deg(P_1)+\deg(P_2)} k\left(\sum_{\substack{i_1,i_2\in\mathbb{N}\\ i_1+i_2=k}} a_{i_1}b_{i_2}\right)X^{k-1} \\
&= (P_1.P_2)'
\end{aligned}$$

Le dernier point provient d'une récurrence immédiate. □

Proposition 4.2.5. Soit $P_1, P_2 \in \mathbb{K}[X]$ tels que $P_1' = P_2'$, alors il existe $a \in \mathbb{K}$ tel que $P_2 = P_1 + a$.

Démonstration. Notons $P_2 - P_1 =: \sum_{k=0}^{n} a_k X^k$. On a alors

$$\sum_{k=1}^{n} k a_k X^{k-1} = (P_2 - P_1)' = P_2' - P_1' = 0.$$

Mais, la famille $(1, X, \ldots, X^{n-1})$ étant libre, on peut en déduire que $k a_k = 0$ pour tout $k \in [\![1, n]\!]$, et donc $a_k = 0$. En posant $a := a_0$, on obtient bien $P_2 = P_1 + a$. □

Corollaire 4.2.6 (formule de Taylor)**.** Pour tout $P \in \mathbb{K}[X]^*$ et tout $\alpha \in \mathbb{K}$, on a

$$P = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k.$$

Démonstration. On travaille par récurrence généralisée sur $\deg(P) \in \mathbb{N}$. Le résultat est clair si $\deg(P) = 0$, c'est-à-dire si P est un polynôme constant. Supposons maintenant le résultat vrai au rang n et considérons un polynôme $P \in \mathbb{K}[X]$ de degré $n+1$. Le polynôme P' est alors de degré au plus n et, par hypothèse de récurrence, on a donc $P' = \sum_{k=0}^{\deg(P)-1} \frac{P^{(k+1)}(\alpha)}{k!}(X-\alpha)^k$. Mais alors

$$\left(\sum_{k=0}^{\deg(P)} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k\right)' = \sum_{k=1}^{\deg(P)} \frac{P^{(k)}(\alpha)}{(k-1)!}(X-\alpha)^{k-1} = \sum_{k=0}^{\deg(P)-1} \frac{P^{(k+1)}(\alpha)}{k!}(X-\alpha)^k = P',$$

et donc, d'après la proposition précédente, $\sum_{k=0}^{\deg(P)} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k = P + a$ avec $a \in \mathbb{K}$. En évaluant en α, on obtient enfin $a = 0$. $\square$

Proposition 4.2.7. Soit $P \in \mathbb{K}[X]$. Un élément $\alpha \in \mathbb{K}$ est racine de multiplicité $k_\alpha \in \mathbb{N}^*$ si et seulement si $P^{(k)}(\alpha) = 0$ pour tout $k \in [\![0, k_\alpha - 1]\!]$ mais $P^{(k_\alpha)}(\alpha) \neq 0$.

Démonstration. En utilisant le corollaire 4.2.6, il est clair que, si $P^{(k)}(\alpha)$ s'annule en α pour tout $k \in [\![0, k_0 - 1]\!]$ mais pas pour $k = k_0$, alors α est racine de multiplicité k_0 pour P.

Pour la réciproque, on commence par remarquer que, sous la convention qu'une racine de multiplicité 0 est une non racine et que $[\![0, -1]\!] = \emptyset$, le résultat est vrai pour $k_\alpha = 0$. De plus, on peut remarquer que, si $\alpha \in \mathbb{K}$ est racine de multiplicité $k_\alpha \in \mathbb{N}^*$ de P, alors $P = (X-\alpha)^{k_\alpha} Q$ avec $Q \in \mathbb{K}[X]$ vérifiant $Q(\alpha) \neq 0$, et donc $P' = k_\alpha (X-\alpha)^{k_\alpha - 1} Q + (X-\alpha)^{k_\alpha} Q' = (X-\alpha)^{k_\alpha - 1}\widetilde{Q}$ avec $\widetilde{Q} := \big(k_\alpha Q + (X-\alpha)Q'\big)$ vérifiant $\widetilde{Q}(\alpha) = k_\alpha Q(\alpha) \neq 0$. Autrement dit, α est racine de multiplicité $k_\alpha - 1$ de P'. La preuve se fait dès lors par récurrence sur $k_\alpha \in \mathbb{N}$. Supposons donc le résultat vrai au rang $n \in \mathbb{N}$ et considérons une racine α de multiplicité $k_\alpha = n+1$ pour P. Alors α est racine de multiplicité n pour P' et, par hypothèse de récurrence, on a $P^{(k)}(\alpha) = (P')^{(k-1)}(\alpha) = 0$ pour tout $k \in [\![1, n]\!]$, ainsi que $P^{(n+1)}(\alpha) = (P')^{(n)}(\alpha) \neq 0$. De plus $P^{(0)} = P(\alpha) = 0$ car α est racine de P puisque $n + 1 \geq 1$. $\square$