Chapitre 14

Polynômes

Dans ce chapitre, $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou le corps $\mathbb{C}$.

I Anneau des polynômes

1. L'anneau $\mathbb{K}[X]$

Définition - Polynôme

On appelle *polynôme à coefficients dans* $\mathbb{K}$ la donnée d'une suite $(a_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang. On choisit de noter ce polynôme

$$P = \sum_{k=0}^{+\infty} a_x X^k = a_0 + a_1 X + \ldots + a_n X^n,$$

où $a_k = 0$ pour tout $k \geqslant n$. On appelle X l'*indéterminée* du polynôme, et, si $k \in \mathbb{N}$, on dit que a_k est le k-ème *coefficient* de P. On choisit de le noter $\mathfrak{c}_k[P]$.

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Remarques.

- La somme de la définition n'est pas réellement infinie, les coefficients étant tous nuls à partir d'un certain rang.
- Deux polynômes sont égaux si et seulement si la suite de leurs coefficients, qui les définit, est la même. On retiendra donc que deux polynômes sont égaux si et seulement si leurs coefficients sont égaux.
- La notion d'indéterminée recouvre le fait que nous allons chercher à "incarner" les polynômes dans n'importe quel ensemble E pour lequel, si $x \in E$, $a_0 + a_1 x + \ldots + a_n x^n$ a un sens, c'est-à-dire un ensemble muni de trois lois :

$$\begin{array}{ccc} \mathbb{K}\times E & \to & E \\ (\lambda, x) & \mapsto & \lambda x \end{array}, \qquad \begin{array}{ccc} E\times E & \to & E \\ (x, y) & \mapsto & x+y \end{array}, \qquad \begin{array}{ccc} E\times E & \to & E \\ (x, y) & \mapsto & x\star y \end{array}$$

  La troisième justifie l'écriture x^k, le première justifie l'écriture $a_k x^k$ et la deuxième la somme de ces éléments.

Exemples.

- Le polynôme donné par la suite nulle est appelé le *polynôme nul*, on le note 0, ou $0_{\mathbb{K}[X]}$.
- Un polynôme donné par la suite $(a_k)_{k\in\mathbb{N}}$ avec $a_k = 0$ pour tout $k > 0$ est appelé *polynôme constant*.
- On appelle *monôme* un polynôme dont tous les coefficients sont nuls sans éventuellement l'un d'entre eux.

Opérations dans $\mathbb{K}[X]$. Si $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$ sont deux polynômes et $\lambda \in \mathbb{K}$, alors :

- ◇ **Somme** : $P + Q$ est défini comme le polynôme $\sum_{k=0}^{+\infty} (a_k + b_k) X^k$.
- ◇ **Multiplication par un scalaire** : λP est défini comme le polynôme $\sum_{k=0}^{+\infty} \lambda a_k X^k$.
- ◇ **Produit** : PQ est défini comme le polynôme $\sum_{k=0}^{+\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k$.
- ◇ **Composition** : $P \circ Q$ est défini comme le polynôme donné par $\sum_{k=0}^{+\infty} a_k Q^k$.
- ◇ **Conjugaison** : si $\mathbb{K} = \mathbb{C}$, on définit $\overline{P} = \sum_{k=0}^{+\infty} \overline{a}_k X^k$.

Remarque. L'expression des coefficients du produit de deux polynômes est motivée par le calcul suivant pour $x \in \mathbb{K}$

$$\left(\sum_{i=0}^{+\infty} a_i x^i\right)\left(\sum_{i=0}^{+\infty} b_j x^j\right) = \sum_{i=0}^{+\infty}\sum_{j=0}^{+\infty} a_i b_j x^{i+j} \overset{k=i+j}{=} \sum_{i=0}^{+\infty}\sum_{k=i}^{+\infty} a_i b_{k-i} x^k = \sum_{k=0}^{+\infty}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k,$$

où on a interverti les sommes dans la sommes double triangulaire. On rappelle que, contrairement aux apparences, les sommes sont finies.

Théorème - Anneau $\mathbb{K}[X]$

L'ensemble $\mathbb{K}[X]$ muni des lois de composition internes $+$ et $\times$ décrites ci-dessus est un anneau commutatif ayant pour éléments neutres respectifs le polynôme nul $0_{\mathbb{K}[X]}$ et le polynôme $1_{\mathbb{K}[X]}$ constant égal à 1.

Démonstration.

◇ $(\mathbb{K}[X], +)$ est un groupe abélien dont l'élément neutre est $0_{\mathbb{K}[X]}$: tout polynôme $P \in \mathbb{K}[X]$ a pour inverse le polynôme $-P$.

◇ $\times$ est associative, commutative et distributive par rapport à $+$: si $P = \sum_{k=0}^{+\infty} a_k X^k$, $Q = \sum_{k=0}^{+\infty} b_k X^k$, $R = \sum_{k=0}^{+\infty} c_k X^k$

$$\mathfrak{c}_k[(PQ)R] = \sum_{i=0}^{k}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) c_{k-i} = \sum_{i=0}^{k}\sum_{j=0}^{i} a_j b_{i-j} c_{k-i} = \sum_{j=0}^{k}\sum_{i=j}^{k} a_j b_{i-j} c_{k-i} \overset{i'=i-j}{=} \sum_{j=0}^{k}\sum_{i'=0}^{k-j} a_j b_{i'} c_{k-(i'+j)}$$

pour tout $k \in \mathbb{N}$. Ainsi, $\mathfrak{c}_k[(PQ)R] = \sum_{j=0}^{k} a_j \sum_{i'=0}^{k-j} b_{i'} c_{(k-j)-i'} = \sum_{j=0}^{k} a_j \mathfrak{c}_{k-j}[QR] = \mathfrak{c}_k[P(QR)]$. Par ailleurs :

$$\mathfrak{c}_k[PQ] = \sum_{i=0}^{k} a_i b_{k-i} \overset{i'=k-i}{=} \sum_{i'=0}^{k} b_{i'} a_{k-i'} = \mathfrak{c}_k[QP].$$

Pour finir, on a : $\mathfrak{c}_k[P(Q+R)] = \sum_{i=0}^{k} a_i(b_{k-i} + c_{k-i} = \sum_{i=0}^{k} a_i b_{k-i} + \sum_{i=0}^{k} a_i c_{k-i}) = \mathfrak{c}_k[PQ + PR]$. □

Remarque. Comme $\mathbb{K}[X]$ est un anneau commutatif, les formules du binôme et de Bernoulli s'appliquent : pour tous $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$,

$$(P+Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^k Q^{n-k}, \qquad P^n - Q^n = (P-Q)\sum_{k=0}^{n-1} P^k Q^{n-1-k}.$$

2. Polynômes et degré

Définition - Degré, coefficient dominant

Soit $P = \sum_{k=0}^{+\infty} a_k X^k$.

- Si P est non nul, on appelle *degré* de P l'entier $\deg P = \max\{k \in \mathbb{N},\ a_k \neq 0\}$. Par convention, le polynôme nul a pour degré $-\infty$.
- Si $\deg P = n \in \mathbb{N}$, on dit que a_n est son *coefficient dominant*, et on le notera ici $\mathfrak{c}_{\text{dom}}[P]$. Si $\mathfrak{c}_{\text{dom}}[P] = 1$, on dit que P est *unitaire*.

Pour tout $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de $\mathbb{K}[X]$ de degré au plus n.

Remarque. $\mathbb{K}_0[X]$ est l'ensemble des polynômes constants, et peut être identifié à $\mathbb{K}$.

Théorème - Degré et opérations

Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}^\star$. On a :

(i) $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$, avec égalité : – si $\deg P \neq \deg Q$, – si $\deg P = \deg Q$ et $\mathfrak{c}_{\text{dom}}[P] + \mathfrak{c}_{\text{dom}}[Q] \neq 0$,

(ii) $\deg(\lambda P) = \deg P$ si $\lambda \neq 0$,

(*iii*) $\deg(PQ) = \deg P + \deg Q$, et si $k \in \mathbb{N}$, alors $\deg P^k = k \deg P$.

(*iv*) $\deg(P \circ Q) = \deg P \times \deg Q$ si Q n'est pas constant.

Remarque. Les opérations ont lieu dans $\overline{R}$: on a $-\infty + x = -\infty$ si $x \in \mathbb{N} \cup \{-\infty\}$.

Démonstration. On note $\mathrm{d}_P = \deg P$ et $d_Q = \deg Q$.

(*i*) Si $k > \max(d_P, d_Q)$, alors $\mathfrak{c}_k[P+Q] = \mathfrak{c}_k[P] + \mathfrak{c}_k[Q] = 0$, donc $\deg(P+Q) \leqslant \max(d_P, d_Q)$.

(*ii*) Le résultat est clair : si $\lambda \neq 0$, $\mathfrak{c}_{d_P}[P] = \lambda \mathfrak{c}_{d_P}[P] \neq 0$.

(*iii*) Si $d_P, d_Q \in \mathbb{N}$ et $k \geqslant d_Q$, on a $\mathfrak{c}_k[PQ] = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=k-d_Q}^{d_P} a_i b_{k-i}$ car si $i > d_P$, $a_i = 0$ et si $i < k - d_Q$, $b_{k-i} = 0$. Ainsi,

- si $k > d_P + d_Q$, alors $k - d_Q > d_P$ et la somme est nulle car elle est vide,
- si $k = d_P + d_Q$, alors $\mathfrak{c}_k[PQ] = a_{d_P} b_{k-d_P} = a_{d_P} b_{d_Q} \neq 0$. On en déduit $\deg PQ = d_P + d_Q$.

Si $d_P = -\infty$ ou $d_Q = -\infty$, alors $PQ = 0$, et $\deg P + \deg Q = -\infty = \deg PQ$, donc l'égalité est vraie.

(*iv*) Les points (*i*) et (*iii*) s'appliquent encore à un nombre fini de polynômes (par récurrence immédiate). Ainsi, on a $\deg(Q^k) = k \deg Q$. Si $\deg Q \neq 0$, alors $P \circ Q$ est une somme de polynômes de degrés deux à deux distincts dont le terme de plus haut degré est $a_{d_P} Q^{d_P}$, qui est de degré $d_P d_Q$. □

⚠ Si Q est constant, on peut avoir $\deg(Q \circ P) \neq \deg P \deg Q$: si $P = X^2 - 1$ et $Q = 1$, alors $\deg Q \circ P = \deg 0 = -\infty$, mais $\deg P \deg Q = 0$.

Théorème - Inversibles de $\mathbb{K}[X]$

Les seuls polynômes inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Démonstration. Si $P = \lambda \in \mathbb{K}^\star$, alors $PQ = 1$ avec $Q = \frac{1}{\lambda}$, donc P est inversible. Réciproquement, si P est inversible, alors il existe $Q \in \mathbb{K}[X]$ tel que $PQ = 1$, ce qui entraîne que $\deg P + \deg Q = 0$, donc $\deg P = \deg Q = 0$. □

Théorème - Intégrité de $\mathbb{K}[x]$

Si $P, Q \in \mathbb{K}[X]$, alors : $PQ = 0 \Leftrightarrow (P = 0 \text{ ou } Q = 0)$.

Démonstration. Si $P = 0$ ou $Q = 0$, on a bien sûr $PQ = 0$. Examinons maintenant la réciproque : si $PQ = 0$, alors on a $\deg(PQ) = -\infty$, ce qui se récrit $\deg P + \deg Q = -\infty$. Ceci n'est possible que si $\deg P = -\infty$ ou $\deg Q = -\infty$, c'est-à-dire si $P = 0$ ou $Q = 0$. □

Remarque. Pour rappel, l'intégrité de $\mathbb{K}[X]$ assure qu'on peut simplifier par tout polynôme non nul : si $A, B, C \in \mathbb{K}[X]$ avec A non nul, alors $AB = AC \Rightarrow B = C$. En effet, si $AB = AC$, alors $A(B - C) = 0_{\mathbb{K}[X]}$, donc $B - C = 0_{\mathbb{K}[X]}$ par intégrité.

3. Fonctions polynomiales, évaluation

Définition-théorème - Fonction polynomiale

On appelle fonction polynomiale sur $\mathbb{K}$ toute fonction $f : \mathbb{K} \to \mathbb{K}$ de la forme

$$f : x \mapsto a_0 + a_1 x + \ldots + a_n x^n,$$

où $a_0, \ldots, a_n \in \mathbb{K}$. L'ensemble $\mathscr{P}_{\mathbb{K}}$ des fonctions polynomiales sur $\mathbb{K}$ est un sous-anneau de $\mathscr{F}(\mathbb{K}, \mathbb{K})$.

Démonstration. On a bien sûr $\mathscr{P}_{\mathbb{K}} \subset \mathscr{F}(\mathbb{K}, \mathbb{K})$. Par ailleurs, la fonction constante égale à 1 est polynomiale, et $\mathscr{P}_k$ est stable par différence et par produit. □

Définition-théorème - Fonction polynomiale associée

Si $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$, on appelle *fonction polynomiale associée* à P la fonction polynomiale

$$\widetilde{P} \ : \ x \ \mapsto \ \sum_{k=0}^{+\infty} a_k x^k.$$

Si $x \in \mathbb{K}$, on appelle *évaluation* de P en x le nombre $\widetilde{P}(x) \in \mathbb{K}$.

Théorème - Polynômes et fonctions polynomiales

L'application $\Phi : P \ \mapsto \ \widetilde{P}$ est un isomorphisme d'anneaux de $\mathbb{K}[X]$ dans l'anneau $\mathscr{P}_{\mathbb{K}}$ des fonctions polynomiales sur $\mathbb{K}$.

Démonstration. Il est clair que Φ est un morphisme d'anneaux (les opérations sur les polynômes ou sur les fonctions polynomiales ayant le même effet sur les coefficients), et que Φ est surjectif. Nous prouverons l'injectivité plus tard dans ce chapitre. □

Remarques.

- On aura tendance à encore noter P la fonction polynomiale associée à P. Attention toutefois : ce ne sont *pas* les mêmes objets mathématiques.
- Le résultat n'est plus vrai si on remplace $\mathbb{K}$ par un corps fini, on peut d'ailleurs montrer que l'application Φ est injective si et seulement si $\mathbb{K}$ est infini.
- Si $x \in \mathbb{K}$, l'application $P \mapsto \widetilde{P}(x)$, dite *application d'évaluation* est un morphisme d'anneaux de $\mathbb{K}[X]$ dans $\mathbb{K}$.

II Divisibilité dans $\mathbb{K}[X]$

Définition - Multiples, diviseurs

Soient $A, B \in \mathbb{K}[X]$. On dit que B divise A et on note $B \,|\, A$ s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $A = BQ$. On dit alors que A est un *multiple* de B et B est un *diviseur* de A.

On note $B\,\mathbb{K}[X] = \{QB, \ Q \in \mathbb{K}[X]\}$ les multiples de B.

Remarque. Si A est non nul et $B \,|\, A$, alors $\deg B \leqslant \deg A$.

Exemple. Si $n \in \mathbb{N}$, alors $X - 1 \,|\, X^n - 1$: on sait que $X^n - 1 \ = \ (X-1)\sum_{k=0}^{n-1} X^k$.

Théorème - Division euclidienne dans $\mathbb{K}[X]$

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ et $\deg R < \deg B$.

Les polynômes Q et R sont appelés respectivement *quotient* et *reste* dans la division euclidienne de A par B.

Démonstration.

- *Existence.* *Cas* $\deg A < \deg B$: dans ce cas, $Q = 0$ et $R = A$ conviennent : $A = BQ + R$ et $\deg R < \deg B$.
  Cas $\deg A \geqslant \deg B$: Nous allons raisonner par récurrence forte.

  Supposons que pour tout $k < n$, on a existence du quotient et du reste dans la division de A par B lorsque $\deg A = k$. On suppose $\deg A = n$, et on note $a = \mathfrak{c}_{\text{dom}}[A]$ et $b = \mathfrak{c}_{\text{dom}}[B]$, puis

  $$\widehat{A} \ = \ A - \frac{a}{b} X^{n - \deg B} B.$$

  On a $\deg \widehat{A} < n$ car $\mathfrak{c}_n[\widehat{A}] = \mathfrak{c}_n[A] - \frac{a}{b}\mathfrak{c}_{\text{dom}}[B] = 0$. Par hypothèse, il existe alors $Q, R \in \mathbb{K}[X]$ tels que $\widehat{A} = BQ + R$ et $\deg R < \deg B$. Ainsi, $\widehat{A} = B(Q + \frac{a}{b} X^{n-\deg B}) + R$, et on a montré qu'on a encore existence de la division euclidienne lorsque $\deg A = n$.

  On note $n = \deg A$. On déduit de ce qui précède que le résultat est vrai lorsque $n = \deg B$, puis, par récurrence forte, pour tout $n \geqslant \deg B$.

– *Unicité.* Supposons qu'il existe $Q_1, Q_2, R_1, R_2 \in \mathbb{K}[X]$ tels que $A = BQ_1 + R_1 = BQ_2 + R_2$ et $\deg R_1 < \deg B$, $\deg R_2 < \deg B$. Ainsi,

$$B(Q_1 - Q_2) = R_2 - R_1, \quad \text{donc} \quad \deg(R_2 - R_1) = \deg B + \deg(Q_1 - Q_2).$$

Si $Q_1 \neq Q_2$, alors $\deg(Q_1 - Q_2) \geqslant 0$, et $\deg(R_2 - R_1) \geqslant \deg B$. Or $\deg(R_2 - R_1) \leqslant \max(\deg R_1, \deg R_2) < \deg B$ et il y a contradiction. On en déduit $Q_1 = Q_2$, puis $R_1 = R_2$. □

Remarque. Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Le reste de la division euclidienne de P par $X - \alpha$ est $\widetilde{P}(\alpha)$.

En effet, la division euclidienne de P par $X - \alpha$ s'écrit $P = (X - \alpha)Q + R$, où $\deg R < 1$, donc R est constant. En évaluant en α, on obtient $\widetilde{R}(\alpha) = \widetilde{P}(\alpha)$, ce qui conclut car R est constant.

Exercice 1. Effectuer la division euclidienne de $X^3 - 3X^2$ par $X^2 - X + 2$.

Exercice 2. Factoriser $X^3 - 6X^2 + 11X - 6$.

Théorème - Caractérisation de la divisibilité dans $\mathbb{K}[X]$

Si $A, B \in \mathbb{K}[X]$ et B est non nul, alors $B \mid A$ si et seulement si le reste dans la division euclidienne de A par B est nul.

Démonstration. Si le reste dans la division euclidienne est nul, il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$, donc $B \mid A$. Si $B \mid A$, l'écriture $A = BQ$ avec $Q \in \mathbb{K}[X]$ est la division euclidienne, donc le reste est nul. □

Théorème et définition - Polynômes associés

Si $A, B \in \mathbb{K}[X]$ deux polynômes non nuls. On a

$$A \mid B \text{ et } B \mid A \quad \Leftrightarrow \quad \exists \lambda \in \mathbb{K}^\star,\ B = \lambda A.$$

On dit alors que les polynômes A, B sont *associés*.

Démonstration. Il est clair que si $B = \lambda A$ avec $\lambda \in \mathbb{K}^\star$, alors les polynômes sont associés. Réciproquement, si A et B sont associés, il existe $P, Q \in \mathbb{K}[X]$ tels que $A = BQ$ et $B = AP$. On a alors $A = APQ$, ce qui donne $A(PQ - 1) = 0$. Par intégrité, on obtient $PQ = 1$, donc P est inversible dans $\mathbb{K}[X]$, et il existe $\lambda \in \mathbb{K}^\star$ tel que $P = \lambda$, ceci conclut. □

III Polynômes dérivés

Définition - Polynômes dérivés

Pour tout polynôme $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$, on appelle *polynôme dérivé* de P le polynôme :

$$P' = \sum_{k=1}^{+\infty} k a_k X^{k-1} = \sum_{k=0}^{+\infty} (k+1) a_{k+1} X^k.$$

On définit par ailleurs les *polynômes dérivés successifs* de P en posant : ◇ $P^{(0)} = P$, ◇ $\forall n \in \mathbb{N},\ P^{(n+1)} = (P^{(n)})'$.

Remarques.
– Si P est un polynôme constant, alors $P^{(n)} = 0$ pour tout $k \in \mathbb{N}^\star$.
– Si $P \in \mathbb{K}[X]$, alors $\widetilde{P'} = \widetilde{P}'$.
– Le terme $k a_k X^{k-1}$ étant nul pour $k = 0$, on note parfois $P' = \sum_{k=0}^{+\infty} k a_k X^{k-1}$.

Exemple. Si $n \in \mathbb{N}$ et $P = X^n$, alors $P^{(k)} = \begin{cases} \frac{n!}{(n-k)!} X^{n-k} & \text{si } k \leqslant n, \\ 0 & \text{si } k > n. \end{cases}$. En particulier, $P^{(n)} = n!$.

Remarque. Si $\deg P = d \geqslant 0$, une récurrence aisée sur n donne que pour tout $n \in [\![0, d]\!]$,

$$P^{(n)} = \sum_{k=n}^{d} k(k-1)\dots(k-n+1)X^{k-n} = \sum_{k=n}^{d} \frac{k!}{(k-n)!}X^{k-n}. \tag{1}$$

On en déduit le résultat suivant sur le degré de $P^{(n)}$.

Théorème - Polynômes dérivés et degré

Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.

- Si $n \leqslant \deg P$, alors $\deg P^{(n)} = \deg P - n$.
- Si $n > \deg P$, alors $P^{(n)} = 0$.

Démonstration. Si $\deg P \leqslant 0$, le résultat est clair. Sinon, (1) donne le résultat pour $n \leqslant \deg P$. Ainsi, $P^{(d)}$ est constant, donc ses dérivées successives sont nulles, et $P^{(n)} = 0$ pour tout $n > d$. □

Théorème - Polynômes dérivés et opérations

Si $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$, alors

$$(\lambda P + \mu Q)' = \lambda P' + \mu Q', \qquad (PQ)' = P'Q + PQ', \qquad (P \circ Q)' = P' \circ Q \times Q'.$$

Démonstration. Le premier point est clair. Pour le second, dans le cas $\mathbb{K} = \mathbb{R}$, on peut utiliser l'isomorphisme Φ entre $\mathbb{R}[X]$ et l'anneau des fonctions polynomiales sur $\mathbb{R}$. Si $P, Q \in \mathbb{R}[X]$, alors

$$\Phi\big((PQ)'\big) = \widetilde{(PQ)'} = \widetilde{PQ}' = \big(\widetilde{P}\widetilde{Q}\big)' = \widetilde{P}'\widetilde{Q} + \widetilde{P}\widetilde{Q}' = \Phi\big(P'Q + PQ'\big).$$

On en déduit bien que $(PQ)' = P'Q + PQ'$. Le cas $\mathbb{K} = \mathbb{C}$ s'en déduit en considérant les parties réelles et imaginaires des polynômes $P, Q \in \mathbb{C}[X]$.

Le dernier point s'obtient en montrant par une récurrence immédiate que pour tout $k \in \mathbb{N}^\star$, $(Q^k)' = kQ'Q^{k-1}$ en utilisant la formule précédente. On a alors, en notant a_k les coefficients de P :

$$(P \circ Q)' = \sum_{k=0}^{+\infty} a_k (Q^k)' = \sum_{k=1}^{+\infty} k a_k Q' Q^{k-1} = \sum_{k=1}^{+\infty} k a_k Q^{k-1} \times Q' = P' \circ Q \times Q'.$$ □

Remarque. Nous avons utilisé l'isomorphisme d'anneaux entre $\mathbb{R}[X]$ et $\mathscr{P}_{\mathbb{R}}$, ce qui ne tient que parce que $\mathbb{R}$ est infini. Le résultat ci-dessus reste cependant valable pour n'importe quel corps $\mathbb{K}$, même fini : on peut alors montrer l'égalité en revenant à l'expression des coefficients du polynôme PQ.

La formule suivante exprime que si $\deg P = n$ et si l'on connaît les évaluations en $a \in \mathbb{K}$ des n polynômes dérivés successifs de P en a, alors on connaît tout le polynôme P.

Théorème - Formule de Taylor polynomiale

Si $P \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$, alors

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

Démonstration.

- Soit $P = \sum_{i=0}^{+\infty} a_i X^i \in \mathbb{K}[X]$. Pour tout $k \in \mathbb{N}$, $P^{(k)} = \sum_{i=k}^{+\infty} \frac{i!}{(i-k)!} X^{i-k}$, donc $P^{(k)}(0) = k! a_k$, et $a_k = \frac{P^{(k)}(0)}{k!}$. Ainsi,

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k, \quad \text{ce qui conclut dans le cas } a = 0.$$

- On pose ensuite $Q = P(X+a)$, ce qui entraine que pour tout $k \in \mathbb{N}$, $Q^{(k)}(X) = P^{(k)}(X+a)$. On remarque aussi que $P = Q(X-a)$. Il suffit alors d'appliquer le résultat à Q :

$$Q = \sum_{k=0}^{n} \frac{Q^{(k)}(0)}{k!} X^k = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k, \quad \text{donc} \quad P = Q(X-a) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k. \qquad \square$$

Remarque. On note que, dès à présent, on ne note plus $\widetilde{P}$ la fonction polynomiale associée à P, mais P.

IV Racines et multiplicité

1. Définitons

Définition - Racine

Soit $P \in \mathbb{K}[X]$. On dit que $\alpha \in \mathbb{K}$ est une *racine* de P si $P(\alpha) = 0$.

Remarque. Tout polynôme de $\mathbb{R}[X]$ de degré impair admet au moins une racine réelle.

Démonstration. Si $P = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{C}[X]$ avec $n = \deg P$ impair et $a_n > 0$ (l'autre cas est identique), alors on a $P(x) \underset{x \to -\infty}{\longrightarrow} -\infty$ et $P(x) \underset{x \to +\infty}{\longrightarrow} +\infty$.

Ainsi, le théorème des valeurs intermédiaires permet de conclure qu'il existe $x \in \mathbb{R}$ tel que $P(x) = 0$. $\square$

Théorème - Racines et factorisation

Soit $P \in \mathbb{K}[X]$.

i. Si $\alpha \in \mathbb{K}$, alors α est une racine de P si et seulement si $X - \alpha \mid P$.

ii. Plus généralement, si $\alpha_1, \ldots, \alpha_k$ sont des racines distinctes de P, alors $(X-\alpha_1)\ldots(X-\alpha_k) \mid P$.

Démonstration.

i. Nous avons vu que le reste dans la division euclidienne de P par $X - \alpha$ est donné par $P(\alpha)$. Par conséquent, le reste est nul si et seulement si α est racine de P.

ii. Montrons seulement le sens direct, la réciproque étant claire. Supposons que $\alpha_1, \ldots, \alpha_k$ sont des racines distinctes de P, et montrons que $(X-\alpha_1)\ldots(X-\alpha_m) \mid P$ pour tout $m \in [\![1, k]\!]$ par récurrence.

- Le cas $m = 1$ a été vu dans le point précédent.
- Soit $m \in [\![1, k-1]\!]$. Supposons que $(X-\alpha_1)\ldots(X-\alpha_m) \mid P$, on a $P = (X-\alpha_1)\ldots(X-\alpha_m)Q$ pour un certain $Q \in \mathbb{K}[X]$. On a
$$0 = P(\alpha_{m+1}) = \prod_{i=1}^{m} (\alpha_{m+1} - \alpha_i) Q(\alpha_{m+1}),$$
donc $Q(\alpha_{m+1}) = 0$ car $\alpha_{m+1} - \alpha_i \neq 0$ pour tout i. Ainsi, $(X - \alpha_{m+1}) \mid Q$, ce qui conclut. $\square$

Corollaire - Nombre maximal de racines

Si $P \in \mathbb{K}_n[X]$ est non nul, alors il admet au plus n racines. Autrement dit, un polynôme $P \in \mathbb{K}_n[X]$ qui admet au moins $n+1$ racines est nul.

Par conséquent, deux polynômes de $\mathbb{K}_n[X]$ qui ont des évaluations qui coïncident en $n+1$ points sont égaux.

Démonstration. Si $P \in \mathbb{K}_n[X]$ admet k racines distinctes notées $\alpha_1, \ldots \alpha_k \in \mathbb{K}$, alors $(X-\alpha_1)\ldots(X-\alpha_k) \mid P$, donc $\deg(X-\alpha_1)\ldots(X-\alpha_k) \leqslant \deg P$, et $k \leqslant \deg P \leqslant n$. Le nombre k de racines distinctes est au plus de n.

Par ailleurs, si $P, Q \in \mathbb{K}_n[X]$ et $\widetilde{P}(x_i) = \widetilde{Q}(x_i)$ pour $x_1, \ldots, x_{n+1} \in \mathbb{K}$ deux à deux distincts, le polynôme $P - Q$, de degré au plus n, a alors $n+1$ racines, ce qui entraîne qu'il est nul. $\square$

Remarques.

- En particulier, si $P \in \mathbb{K}[X]$ admet une infinité de racines, alors P est nul.
- On peut maintenant montrer l'injectivité du morphisme d'anneau $\Phi : P \mapsto \widetilde{P}$ de $\mathbb{K}[X]$ dans l'ensemble des fonctions polynomiales sur $\mathbb{K}$.

  Démonstration. Si $\Phi(P) = \Phi(Q)$, alors les fonctions $\widetilde{P}$ et $\widetilde{Q}$ sont égales, donc coïncident en tout point de $\mathbb{K}$, qui est infini. On en déduit que $P = Q$. $\square$

2. Multiplicité

Définition - Multiplicité

Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$, on appelle *multiplicité* de α pour le polynôme P

$$m_\alpha(P) \;=\; \max\{k \in \mathbb{N},\ (X-\alpha)^k \mid P\}.$$

Autrement dit, α est de multiplicité $m \in \mathbb{N}$ pour P si et seulement si

$$\exists Q \in \mathbb{K}[X],\quad P = (X-\alpha)^m Q \ \text{ et } \ Q(\alpha) \neq 0.$$

Une racine de P de multiplicité 1 est dite *simple*, et un racine de multiplicité au moins 2 est dite *multiple*. On dira aussi qu'une racine de multiplicité 2 est *double*.

Remarques.

- On note que le sous-ensemble $\{k \in \mathbb{N},\ (X-\alpha)^k \mid P\}$ de $\mathbb{N}$ admet bien un maximum : il est non vide car contient 0, et majoré par $\deg P$: si $(X-\alpha)^k \mid P$, alors $k = \deg(X-\alpha)^k \leqslant \deg P$.
- Autre formulation : $m_\alpha(P) = m$ si et seulement si $(X-\alpha)^m \mid P$, et $(X-\alpha)^{m+1} \nmid P$.
- Si $\alpha \in \mathbb{K}$, alors α est racine de P si et seulement si $m_\alpha(P) \geqslant 1$.

Théorème - Caractérisation de la multiplicité

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}$. On a :

$$m_\alpha(P) = m \quad \Leftrightarrow \quad P(\alpha) \;=\; P'(\alpha) \;=\; \ldots \;=\; P^{(m-1)}(\alpha) \;=\; 0 \quad \text{et} \quad P^{(m)}(\alpha) \neq 0.$$

Démonstration. On note $n = \deg P$. On a recours à la formule de Taylor polynomiale en α : $P = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k$.
Si $m \leqslant n$,

$$P \;=\; (X-\alpha)^m \sum_{k=m}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^{k-m} \;+\; \sum_{k=0}^{m-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k$$

forme la division euclidienne $P = (X-\alpha)^m Q + R$ de P par $(X-\alpha)^m$. Par conséquent :

- si $m_\alpha(P) = m$, alors le reste R est nul, donc $R(X+\alpha) = 0$. On en déduit que tous ses coefficients sont nuls : $P(\alpha) = P'(\alpha) = \ldots = P^{(m-1)}(\alpha) \;=\; 0$. Par ailleurs, comme $Q(\alpha) \neq 0$, on a $P^{(m)}(\alpha) \neq 0$,
- si $P(\alpha) = P'(\alpha) = \ldots = P^{(m-1)}(\alpha) \;=\; 0$, et $P^{(m)}(\alpha) \neq 0$, alors $R = 0$ donc $(X-\alpha)^m \mid P$, et, comme $P^{(m)}(\alpha) \neq 0$, $Q(\alpha) \neq 0$. □

Exemple. Déterminons la multiplicité de 1 pour le polynôme $P = X^3 - 3X + 2$.

On a :
- $P(1) = 0$, donc $m_1(P) \geqslant 1$,
- $P' = 3X^2 - 3$, donc $P'(1) = 0$, ce qui entraîne que $m_1(P) \geqslant 2$,
- $P'' = 6X$ donc $P''(1) \neq 0$, ce qui entraîne que $m_1(P) = 2$.

Théorème - Propriétés de la multiplicité

Soient $P, Q \in \mathbb{K}[X]$ non nuls et $\alpha \in \mathbb{K}$. On a :

- $m_\alpha(PQ) \;=\; m_\alpha(P) + m_\alpha(Q)$,
- si $P+Q$ est non nul, alors $\quad m_\alpha(P+Q) \;\geqslant\; \min(m_\alpha(P), m_\alpha(Q))$.
- si α est racine de P, alors $m_\alpha(P') = m_\alpha(P) - 1$.

Démonstration.

- On a $P = (X-\alpha)^{m_\alpha(P)} A$ et $Q = (X-\alpha)^{m_\alpha(Q)} B$, où $A, B \in \mathbb{K}[X]$ et $A(\alpha) \neq 0$, $B(\alpha) \neq 0$. Par conséquent, $PQ = (X-\alpha)^{m_\alpha(P)+m_\alpha(Q)} AB$. Ceci conclut car $AB(\alpha) \neq 0$.
- Avec les mêmes notations, si $m_\alpha(P) \leqslant m_\alpha(Q)$, on a $P+Q = (X-\alpha)^{m_\alpha(P)}(A + (X-\alpha)^{m_\alpha(Q)-m_\alpha(P)} B)$, donc $m_\alpha(P+Q) \geqslant m_\alpha(P)$.

◇ Si $m = m_\alpha(P) \geqslant 1$, alors P s'écrit $P = (X-\alpha)^m Q$ avec $Q \in \mathbb{K}[X]$ et $Q(\alpha) \neq 0$. On peut alors écrire $P' = m(X-\alpha)^{m-1}Q + (X-\alpha)^m Q' = (X-\alpha)^{m-1}\widehat{Q}$ avec $\widehat{Q} = mQ + (X-\alpha)Q'$. Comme $\widehat{Q}(\alpha) = mQ(\alpha) \neq 0$, on a $m_\alpha(P') = m-1$. □

Théorème - Racines, multiplicité et factorisation

Soient $P \in \mathbb{K}[X]$ et $\alpha_1, \dots, \alpha_k \in \mathbb{K}$ des racines de P de multiplicités respectives $m_1, \dots m_k$. Alors

$$(X-\alpha_1)^{m_1} \dots (X-\alpha_k)^{m_k} \mid P,$$

Par conséquent, $m_1 + \dots + m_k \leqslant \deg P$.

Remarque. On dit alors que le nombre de racines de P, *comptées avec leur multiplicité* (c'est-à-dire écrites plusieurs fois si la racine est multiple), n'excède pas $\deg P$.

Démonstration. Nous raisonnons par récurrence pour montrer que pour tout $i \in [\![1, k]\!]$, $(X-\alpha_1)^{m_1} \dots (X-\alpha_i)^{m_i} \mid P$.

- Le cas $k = 1$ est clair : comme α_1 est de multiplicité 1 pour P, $(X-\alpha_1)^{m_1} \mid P$.
- Pour alléger les notations de la preuve, montrons seulement comment déduire que $(X-\alpha_1)^{m_1}(X-\alpha_2)^{m_2} \mid P$ de $(X-\alpha_1)^{m_1} \mid P$. L'hérédité est en tout point analogue.

  Soit $Q \in \mathbb{Q}[X]$ tel que $P = (X-\alpha_1)^{m_1}Q$, et notons m la multiplicité de α_2 dans Q. On a alors $Q = (X-\alpha_2)^m \widehat{Q}$, où $\widehat{Q} \in \mathbb{K}[X]$ est tel que $\widehat{Q}(\alpha_2) \neq 0$. On a par ailleurs $m \leqslant m_2$ car $(X-\alpha_2)^m \mid P$.

  Par hypothèse, il existe $R \in \mathbb{K}[X]$ tel que $P = (X-\alpha_2)^{m_2} R$. Ainsi,

  $$P = (X-\alpha_1)^{m_1}(X-\alpha_2)^m \widehat{Q} = (X-\alpha_2)^{m_2} R$$

  Par intégrité de $\mathbb{K}[X]$, on peut simplifier par $(X-\alpha_2)^m$, ce qui donne $(X-\alpha_1)^{m_1}\widehat{Q} = (X-\alpha_2)^{m_2-m}R$. Comme $(\alpha_2-\alpha_1)^{m_1}\widehat{Q}(\alpha_2) \neq 0$, on en déduit que α_2 n'est pas racine de $(X-\alpha_2)^{m_2-m}R$, donc $m_2 = m$. Ainsi, on a $P = (X-\alpha_1)^{m_1}(X-\alpha_2)^{m_2}\widehat{Q}$, ce qui conclut. □

3. Polynômes scindés

Définition - Polynôme scindé

On dit qu'un polynôme $P \in \mathbb{K}[X]$ non nul est scindé s'il peut s'écrire comme un produit de polynômes de degré 1. En d'autres termes, P est scindé s'il est de la forme

$$P = \lambda(X-\alpha_1)\dots(X-\alpha_n).$$

Les nombres $\alpha_1, \dots, \alpha_k \in \mathbb{K}$ sont les racines de P et $\lambda \in \mathbb{K}$ son coefficient dominant.

Remarque. Si $\deg P = n \in \mathbb{N}^\star$, P est scindé si et seulement s'il admet exactement n racines comptées avec leur multiplicité. Autrement dit, P admet des racines distinctes $\alpha_1, \dots, \alpha_k$ de multiplicités respectives $m_1, \dots, m_k$, avec $m_1 + \dots + m_k = n$. On a alors

$$P = \mathfrak{c}_{\text{dom}}[P] \prod_{i=1}^{k} (X-\alpha_i)^{m_i}.$$

Remarque. ⚠ Un polynôme $P \in \mathbb{R}[X]$ peut être scindé sur $\mathbb{C}$, vu comme polynôme de $\mathbb{C}[X]$, mais pas sur $\mathbb{R}$ (vu comme polynôme de $\mathbb{R}[X]$) : X^2+1 est scindé sur $\mathbb{C}$ mais pas sur $\mathbb{R}$. On précisera généralement sur quel corps le polynôme est scindé.

Exemple. Soit $n \in \mathbb{N}$. Le polynôme $X^n - 1$ est scindé sur $\mathbb{C}$: $X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X-\omega) = \prod_{k=0}^{n-1} \left(X - \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}\right)$.

Le théorème suivant est un des résultats les plus importants du programme d'algèbre, il dit que tout polynôme de $\mathbb{C}$ de degré n admet exactement n racines comptées avec leur multiplicité. En d'autres termes, on peut toujours l'écrire comme facteur de polynômes de degré 1.

Théorème - Théorème de d'Alembert-Gauss

Si $P \in \mathbb{C}[X]$ est un polynôme non constant, alors il admet une racine. Par conséquent, P est scindé sur $\mathbb{C}$.

Démonstration. Admis. □

⚠ Le théorème ne tient pas sur $\mathbb{R}$: par exemple, le polynôme X^2+1 n'a pas de racine dans $\mathbb{R}$, et n'est donc pas scindé sur $\mathbb{R}$.

4. Relations coefficients-racines

Nous savons déjà qu'il existe des relations entre les racines d'un polynôme de $\mathbb{C}_2[X]$ et ses coefficients : rappelons ce calcul, et tâchons de généraliser ces relations aux degrés supérieurs

Degré 2. Si $P = a_2X^2 + a_1X + a_0 \in \mathbb{C}[X]$ a pour racines x_1, x_2, alors P s'écrit $P = a_2(X-x_1)(X-x_2)$. En développant, on obtient :

$$a_2\left(X^2 - (x_1+x_2)X + x_1x_2\right) = a_2X^2 + a_1X + a_0, \quad \text{donc} \quad \begin{cases} x_1+x_2 &= -\frac{a_1}{a_2} \\ x_1x_2 &= \frac{a_0}{a_2} \end{cases}$$

par identification des coefficients.

Degré 3. Si $P = a_3X^3 + a_X^2 + a_1X + a_0 \in \mathbb{K}[X]$ est scindé, et a pour racines x_1, x_2, x_3, alors P s'écrit $P = a_3(X-x_1)(X-x_2)(X-x_3)$. En développant, on obtient :

$$P = a_3\left(X^3 - (x_1+x_2)X^2 + (x_1x_2+x_1x_3+x_2x_3)X - x_1x_2x_3\right), \quad \text{donc} \quad \begin{cases} x_1+x_2+x_3 &= -\frac{a_1}{a_3} \\ x_1x_2+x_1x_3+x_2x_3 &= \frac{a_2}{a_3} \\ x_1x_2x_3 &= -\frac{a_0}{a_3} \end{cases}$$

On constate donc qu'on peut "lire" sur tout polynôme scindé de degré 3 la somme et le produit des racines, mais aussi la somme $x_1x_2 + x_1x_3 + x_2x_3$ de tous les produits de 2 facteurs [1] des racines, notée σ_2 ci-dessous, et qu'on remarque qu'on peut récrire :

$$\sigma_2 = \sum_{1 \leqslant i < j \leqslant n} x_ix_j.$$

Le résultat suivant affirme qu'on peut plus généralement retrouver, à partir des coefficients de tout polynôme scindé de degré n, la somme des produits de k facteurs des racines, pour tout $k \in [\![1, n]\!]$.

Théorème - Relations coefficients-racines de Viète

Soient $P = a_nX^n + \ldots + a_1X + a_0 \in \mathbb{K}[X]$ un polynôme scindé de degré $n \in \mathbb{N}^\star$, de racines $x_1, \ldots, x_n$ comptées avec leur multiplicité. Pour tout $k \in [\![1, n]\!]$, on note

$$\sigma_k = \sum_{0 \leqslant i_1 < \ldots < i_k \leqslant n} x_{i_1} \ldots x_{i_k}$$

la somme de tous les produits de k facteurs des $x_1, \ldots, x_n$. On a alors

$$P = a_n\left(X^n - \sigma_1X^{n-1} + \sigma_2X^{n-2} - \sigma_3X^{n-3} + \ldots + (-1)^n\sigma_n\right), \quad \text{soit} \quad \forall k \in [\![1,n]\!],\ \sigma_k = (-1)^k\frac{a_{n-k}}{a_n}.$$

Remarque. Si $n=3$: $\sigma_1 = x_1+x_2+x_3$, $\sigma_2 = x_1x_2+x_1x_3+x_2x_3$, $\sigma_3 = x_1x_2x_3$.
Si $n=4$: $\sigma_1 = x_1+x_2+x_3+x_4$, $\sigma_2 = x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4$,
$\sigma_3 = x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4$, $\sigma_4 = x_1x_2x_3x_4$.

Démonstration. Pour éviter un excès de détails techniques, donnons une idée de preuve, qui généralise le procédé rencontré ci-dessus pour les degrés 2 et 3 : on cherche à développer et ordonner P, pour identifier les coefficients.

On sait que P s'écrit $P = a_n(X-x_1)\ldots(X-x_n)$. Chaque terme obtenu après développement de P correspond à un choix, dans chacun des facteurs, du terme X ou du terme $-x_i$. Le coefficient $\mathfrak{c}_k[P]$ correspond à la somme des

1. où, pour tout i, x_i apparaît au plus une fois dans chaque produit.

termes où X a été choisi k fois, et les $-x_i$ l'ont été $(n-k)$ fois. Il s'agit donc de la somme des termes de la forme $a_n(-x_{i_1})\dots(-x_{i_{n-k}})$, où les $i_1,\dots,i_{n-k}$ sont distincts. Finalement, $\mathfrak{c}_k[P] = a_k = (-1)^{n-k}\sigma_{n-k}\,a_n$, d'où le résultat. En prenant $k' = n-k$, on obtient que $\sigma_{k'} = (-1)^{k'}\frac{a_{n-k'}}{a_n}$. □

Remarque. On retiendra en particulier qu'on a $\sigma_1 = \sum_{i=1}^{n} x_i$ et $\sigma_n = \prod_{i=1}^{n} x_i$, donc on peut toujours "lire" sur un polynôme scindé la produit et la somme des racines.

$$P = a_nX^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$$

a_{n-1} : $-a_n \sum_{i=1}^{n} x_i$; a_0 : $(-1)^n a_n \prod_{i=1}^{n} x_i$

Exemples.

1. Le polynôme $P = X^3 - 2X^2 - X + 2$ a pour racines évidentes 1 et -1. Comme on sait que le produit de ses racines dans $\mathbb{C}$ est -2, on en déduit que la dernière racine est 2.
2. Le polynôme $Q = X^3 - 6X^2 + 11X - 6$ a pour racine évidente $x_1 = 1$. On note x_2, x_3 les deux autres racines complexes de Q (éventuellement confondues). Comme $x_1 + x_2 + x_3 = 6$ et $x_1x_2x_3 = 6$, on a

$$\begin{cases} x_2 + x_3 &= 5 \\ x_2x_3 &= 6 \end{cases}$$

Ainsi, x_2 et x_3 sont les racines du polynôme $X^2 - 5X + 6$, c'est-à-dire 2 et 3.

Exercice 3. On considère le polynôme $P = X^3 - 11X + 12$.

1. Montrer que P a trois racines réelles distinctes, qu'on notera a, b, c et qu'on ne cherchera pas à calculer.
2. Calculer $\arctan a + \arctan b + \arctan c$.