Polynômes

Olivier Sellès, transcrit par Denis Merigoux

Table des matières

1 La $\mathbb{K}$-algèbre $\mathbb{K}[X]$ 2
1.1 Construction de l'ensemble des polynômes . . . 2
1.1.1 Définitions d'un nouveau produit sur $\mathbb{K}^{\mathbb{N}}$ . . . 2
1.1.2 Construction de $\mathbb{K}^{(\mathbb{N})}$ . . . 3
1.1.3 Identification à des expressions polynômiales classiques . . . 4
1.2 Degré . . . 5
1.3 Fonctions polynômiales . . . 7

2 Arithmétique de l'anneau $\mathbb{K}[X]$ 8
2.1 Généralités . . . 8
2.2 Division euclidienne dans $\mathbb{K}[X]$ et innombrables conséquences . . . 9
2.2.1 Division euclidienne . . . 9
2.2.2 Divisibilité et racines . . . 11
2.2.3 Idéaux de $\mathbb{K}[X]$ . . . 14
2.2.4 PGCD et théorèmes classiques d'arithmétique . . . 15
2.2.5 Décomposition en produit d'irréductibles . . . 17
2.2.6 Ordre d'une racine . . . 18
2.2.7 Généralisation du PGCD et PPCM . . . 19

3 Étude des polynômes à coefficients complexes et réels 20
3.1 Étude de $\mathbb{C}[X]$ . . . 20
3.1.1 Polynôme scindé . . . 20
3.1.2 Corps algébriquement clos . . . 20
3.1.3 Théorème de d'Alembert-Gauss et conséquences . . . 20
3.2 Étude de $\mathbb{R}[X]$ . . . 21
3.2.1 Conjugaison dans $\mathbb{C}[X]$ . . . 21
3.2.2 Polynômes irréductibles de $\mathbb{R}[X]$ . . . 22

4 Fonctions symétriques élémentaires 24
4.1 Faits de base . . . 24
4.2 Relations entre racines et coefficients . . . 26

5 Polynôme dérivé 26
5.1 Généralités . . . 27
5.1.1 Définition et propriétés . . . 27
5.1.2 Dérivation multiple . . . 28
5.2 Polynômes et formule de Taylor . . . 30
5.2.1 Petite histoire . . . 30
5.2.2 Caractérisation de l'ordre d'une racine . . . 30

6 Composition 32
6.1 Définition . . . 32
6.2 Propriétés . . . 32

1 La $\mathbb{K}$-algèbre $\mathbb{K}[X]$

Dans la suite, $\mathbb{K}$ désigne un corps.

1.1 Construction de l'ensemble des polynômes

1.1.1 Définitions d'un nouveau produit sur $\mathbb{K}^{\mathbb{N}}$

On note $\mathbb{K}^{\mathbb{N}}$ l'ensemble des suites d'éléments de $\mathbb{K}$: $\mathbb{K}^{\mathbb{N}} = \mathcal{F}(\mathbb{N}, \mathbb{K})$.
Pour $u, v \in \mathbb{K}^{\mathbb{N}}$, on sait définir :
- $u + v$ comme étant la suite w définie par $\forall n \in \mathbb{N}$, $w_n = u_n + v_n$;
- uv comme étant la suite w définie par $\forall n \in \mathbb{N}$, $w_n = u_n v_n$;
- pour $\alpha \in \mathbb{K}$, αu comme étant la suite w définie par $\forall n \in \mathbb{N}$, $w_n = \alpha u_n$.

On définit aussi un autre produit sur $\mathbb{K}^{\mathbb{N}}$: pour $u, v \in \mathbb{K}^{\mathbb{N}}$, $u \star v$ est la suite w définie par $\forall n \in \mathbb{N}$:

$$w_n = \sum_{k+l=n} u_k v_l$$

La somme porte sur $E_n = \big\{(k,l) \in \mathbb{N}^2 | k + l = n\big\}$. Il est clair que E_n est fini car si $(k,l) \in \mathbb{N}^2$ avec $k + l = n$, alors $k \leqslant n$ et $l \leqslant n$. On a d'autre part : $E_n = \{(k, n-k) \,|k \in [\![0, n]\!]\} = \{(n-l, l) \,|l \in [\![0, n]\!]\}$. Ainsi :

$$\begin{aligned}
\sum_{(k,l)\in E_n} u_k v_l &= \sum_{k=0}^{n} u_k v_{n-k} \\
&= \sum_{l=0}^{n} u_{n-l} v_l \\
&= u_0 v_n + u_1 v_{n-1} + \cdots + u_{n-1} v_1 + u_n v_0
\end{aligned}$$

Existence d'un neutre On note e_0 la suite définie pour $n \in \mathbb{N}$ comme étant :

$$\delta_{n0} = \begin{cases} 1 & \text{si } n = 0 \\ 0 & \text{si } n \geqslant 1 \end{cases}$$

Soit maintenant $u \in \mathbb{K}^{\mathbb{N}}$, alors pour $n \in \mathbb{N}$:

$$\begin{aligned}
(u \star e_0)_n &= \sum_{k=0}^{n} u_k \underbrace{\delta_{(n-k)0}}_{0 \text{ sauf si } k=n} \\
&= u_n \\
&= \sum_{k=0}^{n} \delta_{k0} u_{n-k} \\
&= (e_0 \star u)_n
\end{aligned}$$

e_0 est bien le neutre de $\star$.

Commutativité, associativité La loi est commutative à cause de la commutativité du produit. Montrons l'associativité : soient $u, v, w \in \mathbb{K}^{\mathbb{N}}$ et $n \in \mathbb{N}$. On a alors :

$$\begin{aligned}
((u \star v) \star w)_n &= \sum_{k+l=n} (u \star v)_k \, w_l \\
&= \sum_{k+l=n} \left(\sum_{p+q=k} u_p v_q \right) w_l \\
&= \sum_{p+q+l=n} u_p v_q w_l
\end{aligned}$$

Cette dernière ligne de calcul mérite de plus amples explications [a]. En effet, notons $\Lambda_n = \left\{(p,q,l) \in \mathbb{N}^3 | p+q+l = n\right\} \subset [\![0,n]\!]^3$. Pour $k \in [\![0,n]\!]$, on pose $\Lambda'_k = \{(p,q,l) \in \Lambda_n | p+q = k\}$. Par conséquent, $\{\Lambda'_0, \Lambda'_1, \ldots, \Lambda'_n\}$ forme une partition de Λ_n. Ainsi, d'après le principe de sommation par paquets,

$$\sum_{p+q+l=n} u_p v_q w_l = \sum_{k=0}^{n} \sum_{(p,q,l)\in\Lambda'_k} u_p v_q w_l$$

Or si $(p,q,l) \in \Lambda'_k$, alors $l = n-k$ d'où

$$\begin{aligned}\sum_{p+q+l=n} u_p v_q w_l &= \sum_{k=0}^{n} \left(\sum_{(p,q,l)\in\Lambda'_k} u_p v_q \right) w_{n-k} \\ &= \sum_{k=0}^{n} \left(\sum_{p+q=k} u_p v_q \right) w_{n-k}\end{aligned}$$

Le passage à la dernière ligne de calcul est ainsi expliqué. Transformons maintenant cette expression de manière à obtenir $(u \star (v \star w))_n$: pour $l \in [\![0,n]\!]$, on pose $\Lambda''_l = \{(k,p,q) \in \Lambda_n | p+q = l\}$. À nouveau, les Λ''_l forment une partition de Λ_n d'où :

$$\begin{aligned}\sum_{p+q+l=n} u_k v_p w_q &= \sum_{k=0}^{n} \sum_{(k,p,q)\in\Lambda''_l} u_k v_p w_q \\ &= \sum_{k=0}^{n} u_{n-l} \sum_{(k,p,q)\in\Lambda''_k} v_p w_q \\ &= \sum_{k=0}^{n} u_{n-l} \left(\sum_{p+q=l} v_p w_q \right) \\ &= (u \star (v \star w))_n\end{aligned}$$

Ainsi, $\star$ est associative.

Distributivité Soient $u, v, w \in \mathbb{K}^{\mathbb{N}}$, alors $\forall n \in \mathbb{N}$:

$$\sum_{p+q=n} (u_p + v_p) w_q = \sum_{p+q=n} u_p w_q + \sum_{p+q=n} v_p w_q \Rightarrow ((u+v) \star w) = u \star w + v \star w$$

Le produit étant aussi commutatif, on a aussi :

$$w \star (u+v) = w \star u + w \star v$$

On déduit de toutes les propriétés précédentes que $\left(\mathbb{K}^{\mathbb{N}}, +, \star\right)$ est un anneau commutatif.

1.1.2 Construction de $\mathbb{K}^{(\mathbb{N})}$

On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble des suites d'éléments de $\mathbb{K}$ à support fini : par définition, pour $u \in \mathbb{K}^{\mathbb{N}}$, u est dite à support fini si et seulement si l'ensemble $\{n \in \mathbb{N} | u_n \neq 0\}$ est fini. Cette condition est équivalente à $u \in \mathbb{K}^{(\mathbb{N})} \Leftrightarrow \exists N \in \mathbb{N} / \forall n \geqslant N,\ u_n = 0$.
$\mathbb{K}^{(\mathbb{N})}$ est l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Pour $u, v \in \mathbb{K}^{(\mathbb{N})}$, on a donc $u = v \Leftrightarrow \forall n \in \mathbb{N},\ u_n = v_n$.

a. Même de l'avis du génial M. Sellès !

$\mathbb{K}^{(\mathbb{N})}$ est un sous-anneau de $(\mathbb{K},+,\star)$
- $e_0 \in \mathbb{K}^{(\mathbb{N})}$ car $\{n\in\mathbb{N}|\,(e_0)_n \neq 0\} = \{0\}$ est fini.
- Soient $u,v\in\mathbb{K}^{(\mathbb{N})}$, montrons que :

  (1) $v-u\in\mathbb{K}^{(\mathbb{N})}$;
  Soient $M,N\in\mathbb{N}$ tels que $n>N \Rightarrow u_n = 0$ et $n>M\Rightarrow v_n=0$. Pour $n\geqslant \max(N,M)$, $u_n - v_n = 0-0=0$ d'où le résultat.

  (2) $u\star v\in\mathbb{K}^{(\mathbb{N})}$.
  Soit $n>M+N$, $(p,q)\in\mathbb{N}^2$ tels que $p+q=n$, alors $p>N$ ou $q>M$ car sinon $p+q\leqslant M+N$ donc $u_p=0$ ou $v_q=0$, ce qui implique $u_qv_p=0$. Par conséquent :

$$\sum_{p+q=n} u_pv_q = 0 = (u\star v)_n$$

Ainsi, $\left(\mathbb{K}^{(\mathbb{N})},+,\star\right)$ est un anneau commutatif.

$\mathbb{K}^{(\mathbb{N})}$ est un espace vectoriel On a les propriétés suivantes :
- pour $u\in\mathbb{K}^{(\mathbb{N})}$ et $\alpha\in\mathbb{K}$, il est clair que $\alpha u\in\mathbb{K}^{(\mathbb{N})}$;
- pour $u,v\in\mathbb{K}^{(\mathbb{N})}$, $\alpha\in\mathbb{K}$, $\alpha(u+v)=\alpha u+\alpha v$;
- pour $u\in\mathbb{K}^{(\mathbb{N})}$, $\alpha,\beta\in\mathbb{K}$, $(\alpha+\beta)u=\alpha u+\beta u$;
- $1_{\mathbb{K}}\cdot u = u$;
- $\left(\mathbb{K}^{(\mathbb{N})},+\right)$ est un groupe commutatif.

Ces dernières remarques font de $\left(\mathbb{K}^{(\mathbb{N})},+,\cdot\right)$ un espace vectoriel.

De plus, pour $\alpha\in\mathbb{K}$, $u,v\in\mathbb{K}^{(\mathbb{N})}$,

$$(\alpha u)\star v = u\star(\alpha v) = \alpha(u\star v)$$

En effet, $\forall n\in\mathbb{N}$,

$$\alpha\sum_{p+q=n}u_pv_q = \sum_{p+q=n}(\alpha u_p)v_q = \sum_{p+q=n}u_p(\alpha v_q)$$

Par conséquent, $\left(\mathbb{K}^{(\mathbb{N})},+,\star,\cdot\right)$ est une $\mathbb{K}$-algèbre.

1.1.3 Identification à des expressions polynômiales classiques

On note à présent $X=(\delta_{n1})_{n\in\mathbb{N}}$, avec δ_{n1} qui vaut 1 si $n=1$ et 0 sinon. On a alors $X=(0,1,0,0,\dots$; on voit donc que $X\in\mathbb{K}^{(\mathbb{N})}$.

Proposition Pour $k\in\mathbb{N}$, $X^k=(\delta_{nk})_{n\in\mathbb{N}}$. Montrons ce résultat par récurrence :
- $X^0 = 1_{\mathbb{K}^{(\mathbb{N})}} = e_0 = (\delta_{n0})_{n\in\mathbb{N}}$;
- supposons que $X^k=(\delta_{nk})_{n\in\mathbb{N}}$ pour $k\in\mathbb{N}$. Soit $n\in\mathbb{N}$, alors :

$$\begin{aligned}
\left(X^{k+1}\right)_n &= \left(X^k\star X\right)_n \\
&= \sum_{p=0}^{n}\left(X^k\right)_p (X)_{n-p} \\
&= \sum_{p=0}^{n}\delta_{pk}\delta_{(n-p)1} \\
&= \delta_{(n-k)1} \\
&= \begin{cases} 1 & \text{si } n-k=1\Leftrightarrow n=k+1 \\ 0 & \text{si } n\neq k+1 \end{cases} \\
&= \delta_{n(k+1)}
\end{aligned}$$

X s'appelle l'indéterminée. Soit $u \in \mathbb{K}^{(\mathbb{N})}$, la somme $\sum_{k\in\mathbb{N}} u_k X^k$ a un sens puisque un nombre fini de u_k sont non nuls. Cette somme désigne en fait $\sum_{k\in J} u_k X^k$ où $J = \{k \in \mathbb{N} | u_k \neq 0\}$. Soit maintenant $n \in \mathbb{N}$, on a :

$$\begin{aligned}\left(\sum_{k\in\mathbb{N}} u_k X^k\right)_n &= \sum_{k\in\mathbb{N}} u_k \left(X^k\right)_n \\ &= \sum_{k\in\mathbb{N}} u_k \delta_{nk} \\ &= u_n\end{aligned}$$

On confond donc la suite et la somme, puisque ces deux quantités sont strictement égales.

On notera désormais $\mathbb{K}[X]$ la $\mathbb{K}$-algèbre $\mathbb{K}^{(\mathbb{N})}$ des polynômes à coefficients dans $\mathbb{K}$. Tout polynôme P s'écrit (de façon unique) :

$$P = \sum_{k\in\mathbb{N}} \lambda_k X^k \text{ avec } (\lambda_k) \in \mathbb{K}^{(\mathbb{N})}$$

En réalité, P n'est autre que $(\lambda_k)_{k\in\mathbb{N}}$. De plus, pour $P = \sum_{k\in\mathbb{N}} \lambda_k X^k$ et $Q = \sum_{k\in\mathbb{N}} \mu_k X^k$:

- $P = Q \Leftrightarrow \forall k \in \mathbb{N},\ \lambda_k = \mu_k$;
- $P + Q = \sum_{k\in\mathbb{N}} (\lambda_k + \mu_k) X^k$;
- $P \star Q = \sum_{k\in\mathbb{N}} (\lambda \star \mu)_k X^k$;
- pour $\alpha \in \mathbb{K}$, $\alpha P = \sum_{k\in\mathbb{N}} (\alpha\lambda_k) X^k$.

Vocabulaire On définit les notions suivantes :
- les λ_k s'appellent les coefficients de P ;
- λ_0 est le terme constant de P ;
- les polynômes constants sont ceux de la forme $\lambda \cdot 1_{\mathbb{K}[X]}$ avec $\lambda \in \mathbb{K}$.

En effet, l'application $\lambda \in \mathbb{K} \longmapsto \lambda 1_{\mathbb{K}[X]}$ est un morphisme d'anneau injectif qui permet d'identifier $\lambda \in \mathbb{K}$ et le polynôme constant $\lambda 1_{\mathbb{K}[X]} \in \mathbb{K}[X]$. Désormais, on notera λ au lieu de $\lambda 1_{\mathbb{K}[X]}$.

En particulier, $1_{\mathbb{K}[X]}$ sera noté $1_{\mathbb{K}}$ ou 1 et $0_{\mathbb{K}[X]}$ sera noté $0_{\mathbb{K}}$ ou plus simplement 0.

1.2 Degré

Soit $P = \sum_{k\in\mathbb{N}} \lambda_k X^k \in \mathbb{K}[X] \setminus \{0\}$. L'ensemble $\{k \in \mathbb{N} | \lambda_k \neq 0\}$ est une partie finie non-vide de $\mathbb{N}$ par définition, dont on définit le plus grand élément comme étant le degré de P. Le degré de P est noté $\deg P$.

Si on note $d = \deg P$, $P = \sum_{k=0}^{d} \lambda_k X^k$ et $\lambda_d \neq 0$. λ_d s'appelle le coefficient dominant de P que l'on notera $\text{CD}(P)$. P est dit unitaire ou normalisé si $\text{CD}(P) = 1$.

Opérations et degrés Par convention, $\deg 0 = -\infty$ avec les règles suivantes : $\forall n \in \mathbb{N}$, $-\infty < n$, $-\infty + (-\infty) = -\infty$ et $-\infty + n = -\infty$.

Soient $P, Q \in \mathbb{K}[X] \setminus \{0\}$, $d = \deg P$ et $l = \deg Q$. On note $P = \sum_{k\in\mathbb{N}} \lambda_k X^k$ et $Q = \sum_{k\in\mathbb{N}} \mu_k X^k$.

- Pour $n > d+l$, pour $(p,q) \in \mathbb{N}^2$ tels que $p+q=n$, $p>d$ ou $q>l$ donc $\lambda_p = 0$ ou $\mu_q = 0$ d'où $\lambda_p \mu_q = 0$ donc $\sum_{p+q=n} \lambda_k \mu_q = 0$.
- Pour $n = d+l$, pour $(p,q) \in \mathbb{N}^2$ tels que $p+q=n$, on a forcément $(p,q) = (d,l)$. En effet, si $(p,q) \neq (d,l)$, alors $p>d$ ou $q>l$ donc $\lambda_p \mu_q = 0$, ce qui est impossible au vu de la définition du degré. Ainsi :

$$\sum_{p+q=d+l} \lambda_p \mu_q = \lambda_d \mu_l \neq 0$$

donc $PQ \neq 0$.

En récapitulant les résultats précédents, pour $P, Q \in \mathbb{K}[X] \setminus \{0\}$:

$$\deg PQ = \deg P + \deg Q \quad \text{et} \quad \text{CD}(PQ) = \text{CD}(P)\,\text{CD}(Q)$$

Cette proposition est vérifiée pour tous les polynômes grâce aux conventions prises pour les polynômes nuls.

Au passage, $\mathbb{K}[X]$ est un anneau intègre.

On remarque que le terme constant TC de PQ est $\sum_{p+q=0} \lambda_p \mu_q = \lambda_0 \mu_0$. Ainsi, $\text{TC}(PQ) = \text{TC}(P)\,\text{TC}(Q)$.

Avec les notations précédentes :

$$P + Q = \sum_{k \in \mathbb{N}} (\lambda_k + \mu_k) X^k$$

Si $n > \max(l,d)$, alors $\lambda_n = \mu_n = 0$ donc $\lambda_n + \mu_n = 0$ donc $\{k \in \mathbb{N} | \lambda_k + \mu_k \neq 0\} \subset [[0, \max(d,l)]]$ est fini donc $\deg(P+Q) \leqslant \max(d,l)$.

Piège ! L'inégalité peut-être stricte.
Pour $P = X^2 + 1$ et $Q = -X^2 + X + 1$, $\deg(P+Q) = 1 < \max(2,1)$.
Ainsi, si $l < d$, alors $\lambda_d + \mu_d = \lambda_d \neq 0$ donc $\deg(P+Q) = \max(\deg P, \deg Q)$.

Si $P, Q \in \mathbb{K}[X]$, on a

$$\deg(P+Q) \leqslant \max(\deg P, \deg Q)$$

Il y a égalité si $\deg P \neq \deg Q$.

Généralisations

(1) Soient $r \in \mathbb{N}^*$, $P_1, P_2, \ldots, P_r \in \mathbb{K}[X]$, alors

$$\deg\left(\prod_{i=1}^{r} P_i\right) = \sum_{i=1}^{n} \deg P_i$$

De plus, si, $\forall i \in [[1,r]]$, $P_i \neq 0$,

$$\text{CD}\left(\prod_{i=1}^{r} P_i\right) = \prod_{i=1}^{r} \text{CD}(P_i)$$

En particulier, pour $P \in \mathbb{K}[X] \setminus \{0\}$, $\deg P^r = r \deg P$ et $\text{CD}(P^r) = (\text{CD}(P))^r$.

(2) Soient $P_1, P_2, \ldots, P_r \in \mathbb{K}[X]$, alors

$$\deg\left(\sum_{i=1}^{r} P_i\right) \leqslant \max(\deg P_0, \deg P_1, \ldots, \deg P_r)$$

Et si $\exists j \in [[1,r]]$ tel que $\deg P_j > \deg P_i$ pour tout $i \in [[i,r]] \setminus \{j\}$, alors

$$\deg\left(\sum_{i=1}^{r} P_i\right) = \deg P_j$$

1.3 Fonctions polynômiales

Soit $P = \sum_{k\in\mathbb{N}} \lambda_k X^k = \sum_{k=0}^{d} \lambda_k X^k$ où $d \in \mathbb{N}$ tel que $n > d \Rightarrow \lambda_n = 0$.

Pour $x \in \mathbb{K}$, on pose :

$$\widetilde{P}(x) = \sum_{k=0}^{d} \lambda_k x^k \in \mathbb{K}$$

On a donc $\widetilde{P} \in \mathcal{F}(\mathbb{K}, \mathbb{K})$ et on appelle $\widetilde{P}$ la fonction polynômiale associée à P.

Propriétés Soient $P, Q \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$. Alors :

(1) $\alpha P + Q = \sum_{k\in\mathbb{N}} (\alpha\lambda_k + \mu_k) X^k$, d'où

$$\begin{aligned}\widetilde{\alpha P + Q}(x) &= \sum_{k\in\mathbb{N}} (\alpha\lambda_k + \mu_k) x^k \\ &= \alpha \sum_{k\in\mathbb{N}} \lambda_k x^k + \sum_{k\in\mathbb{N}} \mu_k x^k \\ &= \alpha\widetilde{P} + \widetilde{Q}\end{aligned}$$

(2) $PQ = \sum_{k\in\mathbb{N}} \nu_k X^k$ où $\nu_k = \sum_{k=p+q} \lambda_q\mu_p = (u \star v)_k$. Soient $d, l \in \mathbb{N}$ tels que $n > d \Rightarrow \lambda_n = 0$ et $n > l \Rightarrow \mu_n = 0$. Alors $\forall n > l + d$, $\nu_n = 0$ d'où pour $x \in \mathbb{K}$:

$$\widetilde{PQ}(x) = \sum_{k=0}^{l+d} \nu_k x^k$$

Et d'autre part,

$$\begin{aligned}\widetilde{P}\widetilde{Q}(x) &= \sum_{k=0}^{d} \lambda_k x^k \sum_{k=0}^{l} \mu_k x^k \\ &= \sum_{p=0}^{d}\sum_{q=0}^{l} \lambda_p\mu_q x^{p+q} \\ &= \sum_{(p,q)\in[[0,d]]\times[[0,l]]} \lambda_p\mu_q x^{p+q}\end{aligned}$$

Pour $k \in [\![0, l + d]\!]$, posons $E_k = \{(p, q) \in [\![0, d]\!] \times [\![0, l]\!] \,|\, p + q = k\}$. Il est clair que $\{E_0, E_1, \ldots, E_{l+d}\}$ est une partition de $[\![0, d]\!] \times [\![0, l]\!]$ donc :

$$\begin{aligned}\sum_{(p,q)\in[\![0,d]\!]\times[\![0,l]\!]} \lambda_p\mu_q x^{p+q} &= \sum_{k=0}^{l+d} \sum_{(p,q)\in E_k} \lambda_p\mu_q x^{p+q} \\ &= \sum_{k=0}^{l+d} x^k \left(\sum_{(p,q)\in E_k} \lambda_p\mu_q \right)\end{aligned}$$

Ainsi, $\widetilde{P}\widetilde{Q}(x) = \widetilde{PQ}(x)$.

Il est clair que $\widetilde{1}$ et l'application $x \in \mathbb{K} \longmapsto 1_{\mathbb{K}}$ donc $\widetilde{1}$ est bien l'élément neutre de $\mathcal{F}(\mathbb{K}, \mathbb{K})$ pour le produit.

De plus, $\widetilde{X} = \mathrm{Id}_{\mathbb{K}}$ donc l'application

$$\begin{array}{rccc} \sim : & (\mathbb{K}, +, \star, \cdot) & \longrightarrow & (\mathcal{F}(\mathbb{K}, \mathbb{K}), +, \times, \cdot) \\ & P & \mapsto & \widetilde{P} \end{array}$$

est $\mathbb{K}$-linéaire et c'est un morphisme d'anneaux. C'est donc un morphisme de $\mathbb{K}$-algèbre.

Piège ! $\sim$ n'est pas injective.

En effet, on peut avoir $P \neq 0_{\mathbb{K}[X]}$ et $\widetilde{P} = 0_{\mathcal{F}(\mathbb{K},\mathbb{K})}$. Soit p un nombre premier, $\mathbb{K} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On a vu que $\forall x \in \mathbb{F}_p$, $x^p = x$ d'où pour $P = X^p - X$, $P \neq 0_{\mathbb{F}_p}$ et pour $x \in \mathbb{F}_p$, $\widetilde{P}(x) = x^p - x = 0$ donc $\widetilde{P} = 0_{\mathcal{F}(\mathbb{K},\mathbb{K})}$.

On verra plus tard [a] que lorsque $\mathbb{K}$ est infini, $\sim$ est injective et permet de confondre P et $\widetilde{P}$ pour $P \in \mathbb{K}[X]$.

Racines Une fonction $f : \Omega \subset \mathbb{K} \longrightarrow \mathbb{K}$ est oolynômiale s'il existe $P \in \mathbb{K}[X]$ tel que $f = \widetilde{P}$.

Pour $P \in \mathbb{K}[X]$, une racine de P dans $\mathbb{K}$ est un élément $x \in \mathbb{K}$ tel que $\widetilde{P}(x) = 0_{\mathbb{K}}$.

- Il n'existe pas toujours de racines. Par exemple, pour $\mathbb{K} = \mathbb{R}$ et $P = X^4 + 1$, P n'admet pas de racines réelles. Plus généralement, un polynôme constant non nul n'a jamais de racines.
- À l'inverse, tout élément de $\mathbb{K}$ est racine de $0_{\mathbb{K}[X]}$.
- Un polynôme de degré 1 admet toujours une unique racine. Pour $a \in \mathbb{K}^*$, $b, t \in \mathbb{K}$,

$$\begin{aligned} \widetilde{aX + b}(t) &= a + tb \\ &= a\left(t - \frac{-b}{a}\right) \end{aligned}$$

  et $a\left(t - \frac{-b}{a}\right) = 0 \Leftrightarrow t = -\frac{b}{a}$.
- Le théorème de d'Alembert-Gauss stipule que tout polynôme de $\mathbb{C}[X]$ de degré supérieur ou égal à 1 admet au moins une racine dans P [b].

2 Arithmétique de l'anneau $\mathbb{K}[X]$

2.1 Généralités

- $(\mathbb{K}[X], +, \star)$ est un anneau intègre.
- Les unités de $\mathbb{K}[X]$ sont les polynômes constants non nuls :
  - Si $\lambda \in \mathbb{K}^*$, $\lambda \cdot \frac{1}{\lambda} = 1$ où $\frac{1}{\lambda}$ est l'inverse de λ dans $\mathbb{K}$ donc $\lambda \in \mathcal{U}(\mathbb{K}[X])$ [c].
  - Soit $P \in \mathbb{K}[X]$ une unité de $\mathbb{K}[X]$, $\exists Q \in \mathbb{K}[X]$ tel que $P \star Q = 1$ or $\deg 1 = 0 = \deg(P \star Q) = \deg P + \deg Q$ car $P \neq 0$ et $Q \neq 0$. Par conséquent, $\deg P = \deg Q = 0$ donc P est constant non nul.

- Pour $A, B \in \mathbb{K}[X]$, on dit que A divise B (ou B est multiple de A) s'il existe $C \in \mathbb{K}[X]$ tel que $A = BC$.
  On a alors $\forall \lambda \in \mathbb{K}^*$, $\forall A \in \mathbb{K}[X]$, $\lambda \mid A$ car $A = \lambda \cdot \frac{1}{\lambda} A$, et de même $\lambda A \mid A$.
- On définit ainsi pour $A \in \mathbb{K}[X]$ les polynômes associés à A comme ceux de la forme λA avec $\lambda \in \mathbb{K}^*$.

Les unités de $\mathbb{K}[X]$ et les associés de A sont toujours des diviseurs de A, on les qualifie de triviaux et leur étude ne présente pas d'intérêt particulier.

a. Voir page 12.
b. Voir le complément de la section 11.3.2 du cours complet page 182.
c. Ensemble des inversibles de $\mathbb{K}[X]$.

Propriétés

(1) $\forall A \in \mathbb{K}[X]$, $A \mid 0$. Cependant, $0 \mid A \Rightarrow A = 0$.
(2) Si $A \mid B$ et $B \mid C$, alors $A \mid C$.
(3) Si $A \mid B$ et $A \mid C$, alors $\forall U, V \in \mathbb{K}[X]$, $A \mid BU + CV$.
(4) Pour $A, B \in \mathbb{K}[X] \setminus \{0\}$, $B \mid A \Rightarrow \deg B \leqslant \deg A$.
En effet, $A = BC$ avec $C = \mathbb{K}[X] \setminus \{0\}$ d'où $\deg A = \deg B + \deg C$ d'où le résultat.

Remarques

- Si $B \mid A$ et $\deg B = \deg A$, alors B est un associé de A.
- Si $B \mid A$ et $A \mid B$, alors A et B sont associés.
- Si $A \neq 0$, les diviseurs de A de degré 0 sont les unités de $\mathbb{K}[X]$ et les diviseurs de A de degré $\deg A$ sont les associés de A.
- Si A admet un diviseur B non trivial, alors $1 \leqslant \deg B < \deg A$, ce qui impose $\deg A \geqslant 2$.

Polynôme irréductibles

Soit $P \in \mathbb{K}[X]$ un polynôme *non-constant,* P est irréductible dans $\mathbb{K}[X]$ si les seuls diviseurs de P dans $\mathbb{K}[X]$ sont les diviseurs triviaux.

- Tout polynôme de degré 1 est irréductible car pour qu'un polynôme admette des diviseurs non-triviaux il est nécessaire qu'il soit de degré supérieur ou égal à 2.
- Si $A \in \mathbb{K}[X]$ non-constant n'est pas irréductible, A possède un diviseur B tel que $1 \leqslant \deg B < \deg A$ et $A = BC$ avec $C \in \mathbb{K}[X]$ d'où $1 \leqslant \deg C < \deg A$.

Théorème

Soit $A \in \mathbb{K}[X]$ non constant, alors A s'écrit comme un produit de polynômes irréductibles de $\mathbb{K}[X]$.

Démonstration Soit H_n : « Tout polynôme de degré n de $\mathbb{K}[X]$ non constant est produit d'irréductibles. ».

- H_1 est vrai car tous les polynômes de degrés 1 sont irréductibles.
- Soit $n \in \mathbb{N}^*$, supposons que $\forall k \in [\![1, n]\!]$, H_k est vraie. Soit $A \in \mathbb{K}[X]$ de degré $n+1$:
  - Si A est irréductible, H_{n+1} est validée.
  - Si A n'est pas irréductible, alors $\exists B, C \in \mathbb{K}[X]$ tel que $A = BC$ avec $1 \leqslant \deg B < \deg A$ et $1 \leqslant \deg C < \deg A$. D'après H_n, B et C peuvent s'écrire comme un produit de polynômes irréductibles donc A aussi.

Corollaire Soit $A \in \mathbb{K}[X]$ non-constant, alors A s'écrit $A = C \cdot P_1 \cdot P_2 \cdot \cdots \cdot P_r$ avec $r \in \mathbb{N}^*$, $C \in \mathbb{K}^*$ et $P_1, P_2, \ldots, P_r \in \mathbb{K}[X]$ des polynômes irréductibles unitaires.

En effet, A s'écrit $A = Q_1 Q_2 \cdots Q_r$ avec $r \in \mathbb{N}^*$ et $Q_1, Q_2, \ldots, Q_r \in \mathbb{K}[X]$ des polynômes irréductibles. Pour $i \in [\![1, r]\!]$, si on note $\alpha_i = \text{CD}(Q_i)$, alors $Q_i = \alpha_i P_i$ où P_i est un polynôme irréductible unitaire. D'où le résultat avec $C = \alpha_1 \alpha_2 \cdots \alpha_r$.

De plus, on a nécessairement $C = \text{CD}(A)$ par identification des coefficients dominants.

2.2 Division euclidienne dans $\mathbb{K}[X]$ et innombrables conséquences

2.2.1 Division euclidienne

Soit $A \in \mathbb{K}[X]$, $B \in \mathbb{K}[X] \setminus \{0\}$, alors il existe un et un seul couple $(Q, R) \in \mathbb{K}[X]^2$ appelé division euclidienne de A par B dans $\mathbb{K}[X]$ tel que :

(1) $A = BQ + R$
(2) $\deg R < \deg B$

Q est le quotient et R le reste de cette division euclidienne.

Démonstration

Unicité : Si $(Q_1, R_1), (Q_2, R_2) \in \mathbb{K}[X]^2$ vérifient les deux conditions, alors $A = BQ_1 + R_1 = BQ_2 + R_2$ d'où

$$B(Q_1 - Q_2) = R_2 - R_1$$

Si $Q_1 - Q_2 \neq 0$, alors $\deg(B(Q_1 - Q_2)) = \deg B + \deg(Q_1 - Q_2) \geqslant \deg B$ et d'autre part, $\deg(R_1 - R_2) \leqslant \max(\deg R_1, \deg R_2) < \deg B$ d'où la contradiction. Donc $Q_1 - Q_2 = 0$ puis $R_2 - R_1 = 0$.

Existence : Soit H_n : « Si A est un polynôme de degré inférieur ou égal à n, alors $\exists (Q, R) \in \mathbb{K}[X]^2$ avec $A = BQ + R$ et $\deg R < \deg B$ ».

- H_0 est vraie : soit A un polynôme constant.
  - Si $\deg B \geqslant 1$, on a $A = 0B + A$ et $\deg A < \deg B$ [a]. Le couple $(0, A)$ fait l'affaire.
  - Si $\deg B = 0$, alors $B = \lambda \in \mathbb{K}^*$ et $A = \dfrac{A}{\lambda} \cdot \lambda + 0$ donc $\left(\dfrac{A}{\lambda}, 0\right)$ fait l'affaire.
- Supposons H_n vraie pour $n \in \mathbb{N}$ et montrons H_{n+1}. Soit $A \in \mathbb{K}[X]$ de degré plus petit que $n+1$.
  - Si $\deg A \leqslant n$, l'hypothèse de récurrence valide le résultat.
  - Si $\deg A = n+1$, $A = \alpha X^{n+1} + S$ avec $\deg S \leqslant n$.
    - → Si $\deg B > n+1$, alors $(0, A)$ fait l'affaire d'après la note a.
    - → Si $\deg B \leqslant n+1$, B s'écrit $B = \beta X^m + T$ avec $m \in \mathbb{N}^*$, $\deg T < m$ et $\beta \neq 0$. On pose alors :

$$\begin{aligned} A_1 &= A - \frac{\alpha}{\beta} X^{n+1-m} B \\ &= \alpha X^{n+1} + S - \alpha X^{n+1} - \frac{\alpha}{\beta} X^{n+1-m} T \\ &= \underbrace{S}_{\deg \leqslant n} - \frac{\alpha}{\beta} \underbrace{X^{n+1-m} T}_{\deg \leqslant n} \end{aligned}$$

Ainsi, $\deg A_1 \leqslant n$ donc, d'après l'hypothèse de récurrence, A_1 s'écrit $A_1 = BQ_1 + R_1$ avec $\deg R_1 < \deg B$ d'où :

$$A = \underbrace{\left(Q_1 + \frac{\alpha}{\beta} X^{n+1-m}\right)}_{Q} B + R_1$$

Disposition pratique Effectuons la division euclidienne de $A = X^4 + 2X^3 + X^2 + X - 2$ par $B = X^2 + X + 1$:

$$\begin{aligned} A_1 &= A - X^2 B = X^3 + X - 2 \\ A_2 &= A_1 - XB = -X^2 - 2 \\ A_3 &= A_2 + B = X - 1 \end{aligned}$$

Ainsi, en faisant le chemin inverse :

$$\begin{aligned} A &= A_1 + X^2 B \\ &= A_2 + XB + X^2 B \\ &= A_3 - B + XB + X^2 B \\ &= B\left(X^2 + X - 1\right) + (X - 1) \end{aligned}$$

La division euclidienne de A par B est $\left(X^2 + X - 1, X - 1\right)$. On dispose d'un méthode pratique pour arriver à ce résultat [b] :

X^4	$+2X^3$	$+X^2$	$+X$	-2	$X^2 + X + 1$
	X^3	$+0$	$+X$	-2	$X^2 + X - 1$
		$-X^2$	$+0$	-2	
			X	-1	

a. D'une façon générale, si $\deg A < \deg B$ avec $A \in \mathbb{K}[X]$, alors $A = 0B + A$ et $\deg A < \deg B$.

b. Ne pouvant pas transcrire ici les commentaires oraux associés à cette disposition, je vous dirai simplement que le principe est le même que celui de la division suivant les puissances croissantes (voir section 16.4 du cours complet page 258), sauf que l'on range les polynômes suivant les puissances décroissantes.

2.2.2 Divisibilité et racines

Divisibilité Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$, alors $B \mid A$ si et seulement si le reste de la division euclidienne de A par B est nul. En effet :

$\Leftarrow$ On a alors $A = QB$ donc $B \mid A$.

$\Rightarrow$ A s'écrit $A = BC + 0$ et $\deg 0 < \deg B$ donc la division euclidienne de A par B est $(C, 0)$.

Remarque Soit $\mathbb{L}$ un corps, $\mathbb{K}$ un sous-corps de $\mathbb{L}$. Il est clair que $\mathbb{K}[X] \subset \mathbb{L}[X]$. Soient maintenant $A, B \in \mathbb{K}[X]$ avec $B \neq 0$ et (Q, R) la division euclidienne de A par B dans $\mathbb{K}[X]$; alors (Q, R) est aussi la division euclidienne de A par B dans $\mathbb{L}[X]$.

En effet, $(Q, R) \in \mathbb{L}[X]^2$, $\deg R < \deg B$ et $A = BQ + R$.

On en déduit que $B \mid A$ dans $\mathbb{K}[X]$ si et seulement si $B \mid A$ dans $\mathbb{L}[X]$. En effet :

$\Leftarrow$ C'est clair.

$\Rightarrow$ Soit (Q, R) la division euclidienne de A par B dans $\mathbb{K}[X]$, c'est aussi la division euclidienne de A par B dans $\mathbb{L}[X]$ d'après la remarque ci-dessus. Comme $B \mid A$ dans $\mathbb{K}[X]$, $R = 0$ donc $A = BQ$ dans $\mathbb{L}[X]$ donc $B \mid A$ dans $\mathbb{L}[X]$.

Théorème

Soit $P \in \mathbb{K}[X]$, $x \in \mathbb{K}$. x est racine de P si et seulement si $X - x$ divise dans $\mathbb{K}[X]$.

Démonstration

$\Rightarrow$ Soit (Q, R) la division euclidienne de P par $X - x$ dans $\mathbb{K}[X]$, $\deg R < 1$ donc $R = \lambda \in \mathbb{K}$. Ainsi, $P = (X - x)\,Q + \lambda$, donc pour $t \in \mathbb{K}$, $\widetilde{P}(t) = (t - x)\,\widetilde{Q}(t) + \lambda$ or $\widetilde{P}(x) = 0$ donc $\lambda = 0$ puis $R = 0$ donc $X - x \mid P$.

$\Leftarrow$ P s'écrit $P = (X - x)\,T$ avec $T \in \mathbb{K}[X]$ donc pour $t \in \mathbb{K}$, $\widetilde{P}(t) = (t - x)\,\widetilde{T}(t)$ et $\widetilde{P}(x) = 0$ donc x est bien racine de P.

On remarque que si $A \mid B$, toute racine de A est aussi racine de B.

Conséquence 1

Soit $P \in \mathbb{K}[X] \setminus \{0\}$, alors P admet au plus $\deg P$ racines distinctes dans $\mathbb{K}$.

Démonstration Soit H_n : « Si $P \in \mathbb{K}[X] \setminus \{0\}$ est de degré n, alors P admet au plus n racines dans $\mathbb{K}$ ».

- H_0 est vraie car tout polynôme constant non nul n'admet pas de racines.
- Supposons H_n vraie pour $n \in \mathbb{N}$ et soit P un polynôme de degré $n + 1$.
  - Si P n'a pas de racine dans $\mathbb{K}$, le résultat est validé car $0 < n + 1$.
  - Si P a une racine $x \in \mathbb{K}$, alors $X - x \mid P$ et P s'écrit $P = (X - x)\,Q$ avec $Q \in \mathbb{K}[X] \setminus \{0\}$. De plus, $n + 1 = \deg P = \deg(X - x) + \deg Q$ d'où $\deg Q = n$. Pour $t \in \mathbb{K}$, $\widetilde{P}(t) = (t - x)\,\widetilde{Q}(t)$ donc

$$\begin{aligned} t \text{ est racine de } P &\Leftrightarrow 0 = (t - x)\,\widetilde{Q}(t) \\ &\Leftrightarrow t = x \text{ ou } \widetilde{Q}(t) = 0 \text{ car } \mathbb{K} \text{ est un anneau intègre} \end{aligned}$$

L'ensemble des racines de P dans $\mathbb{K}$ est la réunion des racines de Q et du singleton $\{x\}$. Or l'ensemble des racines de Q est de cardinal inférieur à n d'après l'hypothèse de récurrence donc P admet au plus $n + 1$ racines.

Corollaires

(1) Soit $P \in \mathbb{K}[X]$, $n \in \mathbb{N}$, on suppose que $\deg P \leqslant n$ et P admet $n+1$ racines distinctes, alors P est nul.

(2) Soit $n \in \mathbb{N}$, $P, Q \in \mathbb{K}[X]$ avec $\deg P \leqslant n$ et $\deg Q \leqslant n$. Si $\widetilde{P}$ et $\widetilde{Q}$ coïncident en $n+1$ points de $\mathbb{K}$, alors $P = Q$.
En effet, il suffit d'appliquer la propriété précédente à $P - Q$.

(3) Soit $P \in \mathbb{K}[X]$, si P admet une infinité de racines, alors P est nul.

(4) Soient $P, Q \in \mathbb{K}[X]$, si $\widetilde{P}$ et $\widetilde{Q}$ coïncident en une infinité de points, alors $P = Q$.

(5) da$\mathbb{K}$ est infini, alors $\sim : P \in \mathbb{K}[X] \longrightarrow \widetilde{P} \in \mathcal{F}(\mathbb{K}, \mathbb{K})$ est injective.
En effet, si $P \in \operatorname{Ker} \sim$, $\widetilde{P} = 0_{\mathcal{F}(\mathbb{K},\mathbb{K})}$ est la fonction nulle donc $\forall x \in \mathbb{K}$, $\widetilde{P}(x) = 0$. $\mathbb{K}$ étant infini, P admet une infinité de racines dans $\mathbb{K}$ donc $P = 0_{\mathbb{K}[X]}$ donc $\sim$ est injective.

Exemples

(1) Trouvons tous les $P \in \mathbb{R}[X]$ tels que pour tout nombre premier p, $\widetilde{P}(p) = p^2 + 1$.
Si P convient, alors $\widetilde{P}$ et $\widetilde{X^2+1}$ coïncident sur l'ensemble $\mathcal{P}$ des nombres premiers qui est infini donc $P = X^2 + 1$. Réciproquement, il est clair que $X^2 + 1$ convient.

(2) Montrons l'unicité des polynômes de Chebychev [a]. On rappelle que pour $n \in \mathbb{N}$, il existe un unique polynôme de Chebychev $P \in \mathbb{R}[X]$ tel que $\forall \theta \in \mathbb{R}$ $\mathrm{D}\widetilde{P}(\cos\theta) = \cos(n\theta)$.
Si $P, Q \in \mathbb{R}[X]$ conviennent, $\forall \theta \in \mathbb{R}$, $\widetilde{P}(\cos\theta) = \widetilde{Q}(\cos\theta)$. $\widetilde{P}$ et $\widetilde{Q}$ coïncident donc sur $\{\cos\theta | \theta \in \mathbb{R}\} = [-1, 1]$ infini donc $P = Q$.

(3) Montrons l'unicité des polynômes interpolateurs de Lagrange. Soit $n \in \mathbb{N}$, $x_0, x_1, \ldots, x_n$ des éléments distincts de $\mathbb{K}$ et $y_0, y_1, \ldots, y_n$ des éléments quelconques de $\mathbb{K}$. Alors il existe un unique polynôme L de degré plus petit que n tel que $\forall i \in [\![0, n]\!]$, $\widetilde{L}(x_i) = y_i$.
Si L et S conviennent, $\widetilde{L}$ et $\widetilde{S}$ coïncident en $n+1$ points et $\deg L \leqslant n$, $\deg S \leqslant n$ donc $L = S$.

Conséquence 2

Soit $P \in \mathbb{K}[X]$, $r \in \mathbb{N}^*$, $x_1, x_2, \ldots, x_r$ des points distincts de $\mathbb{K}$. Tous les x_i sont racines de $\mathbb{R}$ si et seulement si $\prod_{i=1}^{r}(X - x_i) \mid P$ dans $\mathbb{K}[X]$.

Démonstration

$\Leftarrow$ En posant $A = \prod_{i=1}^{r}(X - x_i)$, $\forall i \in [\![1, r]\!]$, x_i est racine de A et $A \mid P$ donc x_i est aussi racine de P.

$\Rightarrow$ Soit H_r : « Si $T \in \mathbb{K}[X]$ admet r racines distinctes $x_1, x_2, \ldots, x_r$, alors $\prod_{i=1}^{r}(X - x_i) \mid T$ ».

- H_1 est vrai d'après le théorème principal page 11.
- Soit $r \in \mathbb{N}^*$ tel que H_r est vrai et soit $T \in \mathbb{K}[X]$ admettant $r+1$ racines distinctes $x_1, x_2, \ldots, x_{r+1}$. x_{r+1} est racine de T donc $(X - x_{r+1}) \mid T$ donc $\exists Q \in \mathbb{K}[X]$ tel que $T = (X - x_{r+1})Q$. Pour $t \in \mathbb{K}$, $\widetilde{T}(t) = (t - x_{r+1})\widetilde{Q}(t)$ donc pour $i \in [\![1, r]\!]$,
$$0 = \widetilde{T}(x_i) = \underbrace{(x_i - x_{r+1})}_{\neq 0}\widetilde{Q}(x_i) \Rightarrow \widetilde{Q}(x_i) = 0$$
Ainsi, $x_1, x_2, \ldots, x_r$ sont des racines distinctes de Q donc d'après H_r, Q s'écrit $Q = \prod_{i=1}^{r}(X - x_i)S$ avec $S \in \mathbb{K}[X]$ d'où $T = \prod_{i=1}^{r+1}(X - x_i)S$.

a. Notre grand ami Pafnouti est de retour ! Pour l'existence de ces fabuleux polynômes, se reporter à la section 1.2.5.2 du cours complet page 19.

Corollaire Soit $T \in \mathbb{K}[X]$ de degré $n \geqslant 1$. Si T admet n racines distinctes $x_1, x_2, \ldots, x_n$ dans $\mathbb{K}$, alors T s'écrit $T = \lambda \prod_{i=1}^{n} (X - x_i)$ avec $\lambda = \text{CD}(T) \in \mathbb{K}^*$.

En effet, $\prod_{i=1}^{n} (X - x_i) \mid T$ et $\deg \prod_{i=1}^{n} (X - x_i) = n = \deg T$ donc $\prod_{i=1}^{n} (X - x_i)$ est associé à T donc $\exists \lambda \in \mathbb{K}^*$ tel que $T = \lambda \prod_{i=1}^{n} (X - x_i)$. Par identification des coefficients dominants, $\text{CD}(T) = \lambda$.

Exemples

(1) Soit $\mathbb{K}$ un corps fini et $q = \text{Card}\,\mathbb{K}$. Alors $(\mathbb{K}^*, \times)$ est un groupe fini et $\text{Card}\,\mathbb{K}^* = q - 1$. Ainsi, $\forall x \in \mathbb{K}^*$, $x^{q-1} = 1_{\mathbb{K}}$. Soit $P = X^{q-1} - 1$ de degré $q - 1$, il admet $q - 1$ racines distinctes qui sont les éléments de $\mathbb{K}^*$ donc

$$P = \prod_{x \in \mathbb{K}^*} (X - x)$$

Pour $t \in \mathbb{K}$, $\widetilde{P}(t) = t^{q-1} - 1 = \prod_{x \in \mathbb{K}^*} (t - x)$ donc en particulier :

$$\begin{aligned} \widetilde{P}(0_{\mathbb{K}}) &= -1_{\mathbb{K}} \\ &= \prod_{x \in \mathbb{K}^*} -x \\ &= (-1)^{q-1} \prod_{x \in \mathbb{K}^*} x \end{aligned}$$

Ainsi, $\prod_{x \in \mathbb{K}^*} x = (-1)^q$. En particulier, pour $\mathbb{K} = \mathbb{F}_p$ avec p premier impair,

$$\overline{1} \cdot \overline{2} \cdots \overline{p-1} = (-1)^p \overline{1} = \overline{-1} \Leftrightarrow \overline{(p-1)!} = \overline{-1} \Leftrightarrow \overline{(p-1)! + 1} = \overline{0}$$

Si $p = 2$, $2 \mid (2-1)! + 1$. on a ainsi démontré le théorème de Wilson : si p est premier, $p \mid (p-1)! + 1$.

(2) On a vu que, pour $n \in \mathbb{N}^*$, $\exists! T_n \in \mathbb{R}[X]$ tel que $\forall \theta \in \mathbb{R}$, $\cos(n\theta) = \widetilde{T_n}(\cos\theta)$. On a vu aussi [a] que $\deg T_n = n$ et $\text{CD}(T_n) = 2^{n-1}$. Pour $\theta \in \mathbb{R}$, $\cos\theta$ est racine de T_n si et seulement si :

$$\begin{aligned} \widetilde{T_n}(\cos\theta) = 0 = \cos(n\theta) &\Leftrightarrow n\theta \in \frac{\pi}{2} + \pi\mathbb{Z} \\ &\Leftrightarrow \exists k \in \mathbb{Z} / n\theta = \frac{\pi}{2} + k\pi \\ &\Leftrightarrow \exists k \in \mathbb{Z} / \theta = \frac{(2k+1)\pi}{2n} \end{aligned}$$

Donc, pour $k \in \mathbb{Z}$, $x_k = \cos\left(\frac{(2k+1)\pi}{2n}\right)$ est racine de T_n. En particulier, $x_0, x_1, \ldots, x_{n-1}$ sont racines de T_n et $0 < x_0 < \cdots < x_{n-1} < \pi$. cos est injective sur $[0, \pi]$ donc $x_0, x_1, \ldots, x_{n-1}$ sont n racines distinctes de T_n qui est lui même de degré n donc

$$T_n = 2^{n-1} \prod_{k=0}^{n-1} \left(X - \cos\left(\frac{(2k+1)\pi}{2n}\right)\right)$$

(3) Intéressons-nous de nouveau aux polynômes interpolateurs de Lagrange [b] et montrons leur existence par construction. Soit $n \in \mathbb{N}^*$, $x_0, x_1, \ldots, x_n \in \mathbb{K}$ distincts et $y_0, y_1, \ldots, y_n \in \mathbb{K}$. Alors trouvons un polynôme L_n de degré inférieur ou égal à n tel que $\forall i \in [\![0, n]\!]$, $\widetilde{L_n}(x_i) = y_i$.

a. Voir section 1.2.5.2 du cours complet page 19.
b. Voir l'exemple (3) page précédente.

– Soit $j \in [[0,n]]$, prouvons qu'il existe un polynôme Q_j de degré inférieur ou égal à n tel que $\widetilde{Q_j}(x_j) = 1$ et pour $i \in [\![0,n]\!] \setminus \{j\}$, $\widetilde{Q_j}(x_i) = 0$.
  ◦ Si Q_j existe, alors $Q_j \neq 0$ et, pour $i \in [\![0,n]\!] \setminus \{j\}$, x_i est racine de Q_j, ce qui fait n racines distinctes. On a donc $\deg Q_j \leqslant n$ et $\deg Q_j \geqslant n$ donc $\deg Q_j = n$ et $Q_j = C_j \prod_{\substack{i=0 \\ i\neq j}}^{n} (X - x_i)$ avec $C_j \in \mathbb{K}^*$. Mais on doit aussi avoir :

$$1 = \widetilde{Q_j}(x_j) = C_j \prod_{\substack{i=0 \\ i\neq j}}^{n} (x_j - x_i) \quad \Rightarrow \quad C_j = \frac{1}{\prod_{\substack{i=0 \\ i\neq j}}^{n} (x_j - x_i)}$$

$$\Rightarrow \quad Q_j = \prod_{\substack{i=0 \\ i\neq j}}^{n} \frac{X - x_i}{x_j - x_i}$$

  ◦ Réciproquement, le polynôme ainsi déterminé convient.

– Soit maintenant, pour $j \in [\![0,n]\!]$, $T_j = y_j Q_j$ donc pour $i \in [\![0,n]\!]$, $\widetilde{T}(x_i) = y_j \widetilde{Q_j}(x_i) = \begin{cases} 0 & \text{si } i \neq j \\ y_j & \text{si } i = j \end{cases}$ et $\deg T_j = \deg Q_j = n$ donc on prend pour L_n :

$$L_n = \sum_{j=0}^{n} T_j = \sum_{k=0}^{n} y_k \prod_{\substack{i=0 \\ i\neq j}}^{n} \frac{X - x_i}{x_j - x_i}$$

Or, pour $i \in [\![0,n]\!]$:

$$\begin{aligned} \widetilde{L_n}(x_i) &= \sum_{j=0}^{n} \widetilde{T_j}(x_i) \\ &= \sum_{j=0}^{n} \delta_{ij} y_j \\ &= y_j \end{aligned}$$

On a bien de plus $\deg L_n \leqslant \max_{i\in[[0,n]]} \deg(T_j) = n$.

2.2.3 Idéaux de $\mathbb{K}[X]$

Un idéal de $\mathbb{K}[X]$ est une partie I de $\mathbb{K}[X]$ telle que :
(1) I est un sous-groupe de $(\mathbb{K}[X], +)$;
(2) $\forall P \in I$, $\forall S \in \mathbb{K}[X]$, $SP \in I$.

Par exemple, $\{0\}$ une$\mathbb{K}[X]$ sont des idéaux de $\mathbb{K}[X]$. De plus, $\{0\} = \{0P | P \in \mathbb{K}[X]\} = 0\mathbb{K}[X]$ et de même, $\mathbb{K}[X] = 1\mathbb{K}[X]$.

Plus généralement, si $A \in \mathbb{K}[X]$, $A\mathbb{K}[X] = \{AP | P \in \mathbb{K}[X]\}$ est un idéal. En effet :
– $A\mathbb{K}[X] \neq \varnothing$ et $\forall P, Q \in \mathbb{K}[X]$, $AP - AQ = A(P - Q) \in A\mathbb{K}[X]$.
– $\forall P, Q \in \mathbb{K}[X]$, $(AP)Q = A(QP) \in \mathbb{K}[X]$.

Remarque Pour $A, B \in \mathbb{K}[X]$, $B \mid A \Leftrightarrow A\mathbb{K}[X] \subset B\mathbb{K}[X]$.

Théorème

Soit I un idéal de $\mathbb{K}[X]$ non-réduit à $\{0\}$. Alors $\exists! A \in \mathbb{K}[X]$ unitaire tel que $I = A\mathbb{K}[X]$.

Démonstration Soit $A \in I \setminus \{0\}$ tel que $\deg A = \min\{\deg P | P \in I \setminus \{0\}\}$. Pour $\alpha \in \mathbb{K}^*$, $\alpha A \in I$ et $\deg A = \deg \alpha A$ donc on peut supposer que A est unitaire.

- Soit $A_1 \in I$ donc $\forall S \in \mathbb{K}[X]$, $A_1 S \in I$ donc $A_1 \mathbb{K}[X] \subset I$.
- Soit $P \in I$, $P = AQ + R$ avec $\deg R < \deg A$ or $R = \underbrace{P}_{\in I} - \underbrace{AQ}_{\in I} \in I$ donc $R = 0$ au vu de la définition du degré de A. Ainsi, $P = AQ \in \mathbb{K}[X]$ donc $I = A\mathbb{K}[X]$.
- Soit B un autre polynôme unitaire tel que $I = B\mathbb{K}[X]$. Ainsi $A\mathbb{K}[X] = B\mathbb{K}[X]$ donc A et B sont associés donc égaux car ils sont tous deux unitaires.

2.2.4 PGCD et théorèmes classiques d'arithmétique

Soient $A, B \in \mathbb{K}[X]$. Alors $\exists ! D \in \mathbb{K}[X]$ nul ou unitaire tel que :
(1) $D \mid A$ et $D \mid B$;
(2) $\forall L \in \mathbb{K}[X]$, si $L \mid A$ et $L \mid B$, alors $L \mid D$.
Le polynôme D s'appelle alors le PGCD de A et de B dans $\mathbb{K}[X]$.

Démonstration

Unicité : On remarque que si $(A, B) \neq (0, 0)$ et que D vérifie (1), alors $D \neq 0$.
- Supposons $A = B = 0$, si D vérifie (1) et (2), alors $0 \mid D$ donc $D = 0$.
- Si A ou B est non nul, alors soient D_1 et D_2 des polynômes vérifiant (1) et (2) donc $D_1 \mid D_2$ et $D_2 \mid D_1$ d'où $D_1 = D_2$ car ils sont tous les deux unitaires.

Existence :
- Si $A = B = 0$, on prend $D = 0$.
- Si A ou B est différent de 0, soit $I = A\mathbb{K}[X] + B\mathbb{K}[X] = \{AU + BV | U, V \in \mathbb{K}[X]\}$. A et B appartiennent à I donc $I \neq \{0\}$. I est un idéal de $\mathbb{K}[X]$. En effet, soient $P, Q, U, V \in \mathbb{K}[X]$:
  - $(AU + BV) - (PA + QB) = A(U - P) + B(V - Q) \in I$;
  - $(AU + BV) P = APU + BPV \in I$.

  Ainsi, d'après le théorème de la section 2.2.3 page ci-contre, il existe un unique $D \in \mathbb{K}[X]$ tel que $I = D\mathbb{K}[X]$. D vérifie alors bien (1) et (2) :
  (1) $A \in I = D\mathbb{K}[X]$ donc $D \mid A$ et de même, $D \mid B$.
  (2) $D \in D\mathbb{K}[X] = I$ donc D s'écrit $AU + BV$ avec $U, V \in \mathbb{K}[X]$. Si $S \in \mathbb{K}[X]$ divise A et B, alors $S \mid AU + BV$ donc $S \mid D$.

Remarques
- $0 \wedge 0 = 0$.
- Pour $A, B \in \mathbb{K}[X]$, $B \mid A \Leftrightarrow A \wedge B$ est associé à B. En effet, soit $D = A \wedge B$:
  $\Leftarrow$ $D \mid A$ et B est associé à D donc $B \mid A$.
  $\Rightarrow$ $B \mid A$ et $B \mid B$ donc $B \mid D$, or $D \mid B$ donc B et D sont associés.

Théorème de Bézout I Soient $A, B \in \mathbb{K}$ et $D = A \wedge B$, alors $\exists U, V \in \mathbb{K}[X]$ tels que $AU + BV = D$ [a].

Algorithme d'Euclide Prenons $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. L'algorithme d'Euclide est le processus suivant :

```
variables R,R',temp
R ← A
R' ← B
tant que R' ≠ 0 faire
    temp ← R
    R ← R'
```

a. Pour toutes les démonstrations qui vont suivre, se reporter à la section 18.2.1.3 du cours complet page 295. Il suffit de remplacer $\mathbb{Z}$ par $\mathbb{K}[X]$ et les minuscules par des majuscules.

```
    R' ← reste de la division euclidienne de temp par R'
fin faire
renvoyer R
```

Principe Cet algorithme se termine bien car $\deg R'$ à la sortie de la boucle est strictement inférieur à $\deg R'$ à l'entrée de la boucle. est continuenale renvoyée est un associé de $A \wedge B$. Prouvons ce résultat :

(1) Si $A, B, Q, R \in \mathbb{K}[X]$ tels que $A = QB + R$, alors $A \wedge B = B \wedge R$. En effet :
$A \wedge B \mid A$ et $A \wedge B \mid B$ donc $A \wedge B \mid B$ et $A \wedge B \mid R$ donc $A \wedge B \mid B \wedge R$. Réciproquement, $B \wedge R \mid B$ et $B \wedge R \mid R$ donc $B \wedge R \mid A = BQ + R$ donc $B \wedge R \mid A \wedge B$. Ces deux polynômes étant unitaires ou nuls, $B \wedge R = A \wedge B$.

(2) Ici, le processus s'écrit :

$$\begin{aligned} A &= BQ_1 + R_1 \quad 0 \leqslant \deg R_1 < \deg B \\ B &= Q_2R_1 + R_2 \quad 0 \leqslant \deg R_2 < \deg R_1 \\ &\vdots \\ R_{N-1} &= Q_{N+1}R_N + 0 \quad R_N \neq 0 \end{aligned}$$

On en déduit que $A \wedge B = B \wedge R_1 = \cdots = R_N \wedge 0 = \dfrac{R_N}{\mathrm{CD}(R_N)}$ d'où le résultat.

Remarques
- L'algorithme d'Euclide donne aussi des polynômes U et V tels que $AU + BV = D$.
- Soit $\mathbb{K}$ un sous-corps de $\mathbb{L}$, $A, B \in \mathbb{K}[X]$. Posons $D = A \wedge B$ dans $\mathbb{K}[X]$ et $\Delta = A \wedge B$ dans $\mathbb{L}[X]$, montrons que $D = \Delta$.
  - $D \mid A$ et $D \mid B$ dans $\mathbb{K}[X]$ donc $D \mid A$ et $D \mid B$ dans $\mathbb{L}[X]$ donc $D \mid \Delta$ dans $\mathbb{L}[X]$.
  - D'autre part, D s'écrit $D = AU + BV$ avec $U, V \in \mathbb{K}[X]$ donc $\Delta \mid A$ et $\Delta \mid B$ dans $\mathbb{L}[X]$ donc $\Delta \mid AU + BV = D$ dans $\mathbb{L}[X]$. D et Δ sont unitaires donc $\Delta = D$.

Polynômes premiers entre eux

$A, B \in \mathbb{K}[X]$ sont premiers entre eux si $A \wedge B = 1$.

- A et B sont premiers entre eux si et seulement si les seuls diviseurs communs de A et B sont les polynômes constants non nuls. En effet :

  $\Rightarrow$ Soit P un diviseur commun de A et B, alors $P \mid A \wedge B = 1$ donc $P \in \mathbb{K}[X]^*$.

  $\Leftarrow$ Si $A \wedge B$ divise A et B, alors $A \wedge B \in \mathbb{K}^*$ or $A \wedge B$ est unitaire donc $A \wedge B = 1$.
- Soit P un polynôme irréductible de $\mathbb{K}[X]$, alors pour $A \in \mathbb{K}[X]$, $P \mid A$ ou $P \wedge A = 1$.
  En effet, $P \wedge A \mid P$ donc, puisque P est irréductible, $P \wedge A \in \mathbb{K}[X]^*$ donc $P \wedge A = 1$ ou bien $P \wedge A$ est associé à P d'où $P \mid A$.
- Soient P, Q deux polynômes irréductibles de $\mathbb{K}[X]$, alors $P \wedge Q = 1$ ou P et Q sont associés.
  En effet, si $P \wedge Q = 1$, alors $P \mid Q$ or $P \notin \mathbb{K}[X]^*$ est irréductible donc P est associé à Q.
- Si P et Q sont irréductibles unitaires, alors $P \wedge Q = 1$ ou $P = Q$.
  Par exemple, pour $a, b \in \mathbb{K}$ et $a \neq b$, $(X - a) \wedge (X - b) = 1$ car $(X - a)$ et $(X - b)$ sont irréductibles unitaires distincts.

Théorèmes
- Bézout II : pour $A, B \in \mathbb{K}[X]$, $A \wedge B = 1 \Leftrightarrow \exists U, V \in \mathbb{K}[X] / AU + BV = 1$.
- Théorème de Gauss et variantes : soient $A, B, C \in \mathbb{K}[X]$,
  - $A \mid BC$ et $A \wedge B = 1 \Rightarrow A \mid C$;
  - $A \mid C$, $B \mid C$ et $A \wedge B = 1 \Rightarrow AB \mid C$;

- $A \wedge B = 1$ et $A \wedge C = 1 \Rightarrow A \wedge BC = 1$;
- $A \wedge B = 1 \Rightarrow \forall p, q \in \mathbb{N},\ A^p \wedge B^q = 1$.

– $\forall a, b \in \mathbb{K}$ avec $a \neq b$, $\forall m, n \in \mathbb{N}$, $(X-a)^n \wedge (X-b)^m = 1$.
– Soit P un polynôme irréductible, si $P \mid AB$, alors $P \mid A$ ou $P \mid B$.
– Plus généralement, pour $A_1, A_2, \ldots, A_n \in \mathbb{K}[X]$, si $P \mid A_1 A_2 \cdots A_n$, alors $\exists i \in [\![1, n]\!]$ tel que $P \mid A_i$.

2.2.5 Décomposition en produit d'irréductibles

Soit $P \in \mathbb{K}[X]$ non-constant, alors P s'écrit de façon essentiellement unique (à l'ordre près des termes) :

$$P = C\prod_{i=1}^{r} P_i$$

avec $C \in \mathbb{K}^*$, $r \in \mathbb{N}^*$ et $P_1, P_2, \ldots, P_r \in \mathbb{K}[X]$ irréductibles unitaires.

Démonstration de l'unicité On rappelle [a] que l'on a nécessairement $C = \text{CD}(P)$. Soient $r, s \in \mathbb{N}^*$, $P_1, P_2, \ldots, P_r \in \mathbb{K}[X]$ et $Q_1, Q_2, \ldots, Q_s \in \mathbb{K}[X]$ irréductibles unitaires avec $\prod_{i=1}^{r} P_i = \prod_{i=1}^{s} Q_i$. Montrons que $r = s$ et, à une permutation près, $\forall i \in [\![1, r]\!]$, $Pi = Q_i$.

Sous de telles hypothèses, $P_r \mid \prod_{i=1}^{s} Q_i$ donc P_r divise l'un des Q_i, supposons que ce soit Q_s (quitte à renuméroter les Q_i). Alors $P_r \mid Q_s$ et ces deux polynômes sont irréductibles unitaires donc $P_r = Q_s$. $\mathbb{K}[X]$ étant un anneau intègre, on a :

$$\prod_{i=1}^{r-1} P_i = \prod_{i=1}^{s-1} Q_i$$

On achève la démonstration par récurrence.

Autres formulations Soit $P \in \mathbb{K}[X]$ non constant, alors P s'écrit de façon unique :

$$P = C\prod_{i=1}^{r} P_i^{\alpha_i}$$

Avec $C \in \mathbb{K}^*$, $r \in \mathbb{N}^*$, $P_1, P_2, \ldots, P_r \in \mathbb{K}[X]$ irréductibles unitaires distincts et $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}^*$

Remarques Soient $A, B \in \mathbb{K}[X] \setminus \{0\}$. A et B peuvent s'écrire $A = a\prod_{i=1}^{r} P_i^{\alpha_i}$ et $B = b\prod_{i=1}^{r} P_i^{\beta_i}$ avec $r \in \mathbb{N}^*$, $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}^*$, $\beta_1, \beta_2, \ldots, \beta_r \in \mathbb{N}^*$ car $1_{\mathbb{K}[X]}$ est irréductible unitaire.

– Alors $A = B \Leftrightarrow a = b$ et $\forall i \in [\![1, r]\!]Fo\alpha_i = \beta_i$.
– $A \mid B$ si et seulement si $\forall i \in [\![1, r]\!]$, $\alpha_i \leqslant \beta_i$. En effet :

  $\Leftarrow$ $B = \dfrac{b}{a}\prod_{i=1}^{r} P_i^{\beta i - \alpha_i} a \cdot \prod_{i=1}^{r} P_i^{\alpha_i}$ donc $B = AC$ avec $C \in \mathbb{K}[X]$.

  $\Rightarrow$ Si $B = AC$ avec $C \in \mathbb{K}[X]$, alors $B = a\prod_{i=1}^{r} P_i^{\alpha_i} \times c\prod_{i=1}^{r} P_i^{\gamma_i} \times$autres polynômes irréductibles unitaires.

  Par unicité de l'écriture en produit d'irréductibles, $\beta_i = \alpha_i + \gamma_i \geqslant \alpha_i$.

– $A \wedge B = \prod_{i=1}^{r} P^{\min(\alpha_i, \beta_i)}$.

  En effet, soient $D = A \wedge B$ et $\Delta = \prod_{i=1}^{r} P^{\min(\alpha_i, \beta_i)}$.

a. Pour la démonstration de l'existence, voir page 9.

- ◦ Il est clair que $\Delta \mid A$ et $\Delta \mid B$ donc $\Delta \mid D$.
- ◦ Réciproquement, si P irréductible divise D, alors P divise $A = a\prod_{i=1}^{r} P_i^{\alpha_i}$ donc P divise l'un des P_i donc D va s'écrire $D = \prod_{i=1}^{r} P_i^{\delta_i}$ avec $\delta_1, \delta_2, \ldots, \delta_r \in \mathbb{N}^*$. Il n'y a pas d'autres irréductibles qui divisent D que $P_1, P_2, \ldots, P_r$, $D \mid A$ et $D \mid B$ donc $\delta_i \leqslant \min(\alpha_i, \beta_i)$ d'après la propriété précédente donc $D \mid \Delta$.
- ◦ D et Δ sont unitaires donc $\Delta = D$.

– Si $A \in \mathbb{K}[X]$ est non-constant et si P est irréductible unitaire, alors l'ensemble $\{\alpha \in \mathbb{N} | P^\alpha \mid A\}$ est majoré [a]. En effet :
- ◦ Si $P \nmid A$, alors $\{\alpha \in \mathbb{N} | P^\alpha \mid A\} = \{0\}$.
- ◦ Si $P \mid A$, supposons que $\{\alpha \in \mathbb{N} | P \mid A\}$ n'est pas majoré, alors $\exists \beta \in \mathbb{N}$ tel que $\deg P^\beta = \beta \deg P > \deg A$, ce qui est impossible car $P^\beta \mid A$ et $\deg P \geqslant 1$.

– Soit $A \in \mathbb{K}[X] \setminus \{0\}$ et $\mathcal{I}$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{K}[X]$. Pour $P \in \mathcal{I}$, on note $\mathcal{V}_P(A)$ l'exposant de P dans l'écriture de A sous forme de produit d'irréductibles (en particulier, $\mathcal{V}_P(A) = 0$ si P n'y apparaît pas). Pour $A, B \in \mathbb{K}[X]$, $P \in \mathcal{I}$, $\mathcal{V}_P(AB) = \mathcal{V}_P(A) + \mathcal{V}_P(B)$ et $A \mid B \Leftrightarrow \forall P \in \mathcal{I}$, $\mathcal{V}_P(A) \leqslant \mathcal{V}_P(B)$.C$\mathcal{V}_P(A)$ est l'unique $\alpha \in \mathbb{N}$ tel que $P^\alpha \mid A$ et $P^{\alpha+1} \nmid A$.

2.2.6 Ordre d'une racine

Pour un polynôme irréductible unitaire, on note $\mathcal{V}_P(A)$ l'exposant de P dans l'écriture de $A \in \mathbb{K}[X]$ sous forme de produit d'irréductibles (en particulier, $\mathcal{V}_P(A) = 0$ si P n'y apparaît pas).

Soit $P \in \mathbb{K}[X]$ non-constant et $x \in \mathbb{K}$. $x \in \mathbb{K}$ est racine de P si et seulement si $X - x \mid P$. Si x est racine de P, le polynôme irréductible $X - x$ figure dans l'écriture de P en produit d'irréductibles unitaires. L'ordre de multiplicité de x est alors $\alpha = \mathcal{V}_{X-x}(P)$. On a donc $(X-x)^\alpha \mid P$ mais $(X-x)^{\alpha+1} \nmid P$. x est une racine multiple si son ordre de multiplicité est supérieur ou égal à 2 ; double si $\alpha = 2$, triple si $\alpha = 3$...

Soit $P \in \mathbb{K}[X] \setminus \{0\}$, $x_1, x_2, \ldots, x_r$ distincts dans $\mathbb{K}$ avec $r \in \mathbb{N}^*$. Pour $i \neq j$, $X - x_i$ et $X - xj$ sont irréductibles unitaires distincts donc premiers entre eux. Ainsi, $\forall m, n \in \mathbb{N}$, $(X-x_i)^n \wedge (X-x_j)^m = 1$. En particulier, si $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$ et si $\forall i \in [\![1, r]\!]$, x_i est racine de P d'ordre α_i, alors $\forall i \in [\![1, r]\!]$, $(X-x_i)^{\alpha_i} \mid P$ et on en déduit que $\prod_{i=1}^{r} (X-x_i)^{\alpha_i} \mid P$ car pour $i \neq j$, $(X-x_i) \wedge (X-x_j) = 1$.

On en déduit en particulier que $\deg \prod_{i=1}^{r} (X-x_i)^{\alpha_i} \leqslant \deg P$ donc $\deg P \geqslant \sum_{i=1}^{r} \alpha_i$. Si chaque racine est comptée autant de fois que son ordre de multiplicité P a au plus $\deg P$ racines comptées avec ordre de multiplicité.

Cas particulier Soit $P \in \mathbb{K}[X]$ de degré $n \geqslant 1$, $r \in \mathbb{N}^*$, $x_1, x_2, \ldots, x_r \in \mathbb{K}$ distincts et $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}^*$. On suppose que $\sum_{i=1}^{r} \alpha_i = n$ et $\forall i \in [\![1, r]\!]$, $(X-x_i)^{\alpha_i} \mid P$. Alors P s'écrit (car les polynômes sont premiers entre eux deux à deux) :

$$P = a\prod_{i=1}^{r} (X-x_i)^{\alpha_i}$$

avec $a = \text{CD}(P)$. Ceci est en fait l'écriture de P sous forme de produit d'irréductibles unitaires. Nécessairement, l'ensemble des racines de P est dans $\mathbb{K}$ est $\{x_i | i \in [\![1, r]\!]\}$. Alors $\forall i \in [\![1, r]\!]$, α_i est effectivement l'ordre de la racine x_i (ce que l'on n'avait pas supposé au départ).

a. Après avoir écrit cette dernière ligne, M. Sellès, visiblement perturbé par l'attitude de ses élèves, quitta précipitamment la classe en effaçant ce début de résultat. Votre serviteur ayant toutefois eu le stylo suffisamment leste pour sauver cette remarque, et grâce à l'aide précieuse de M. Dong (ou To-Til pour les intimes), il vous en propose ici une démonstration qui tient la route.

2.2.7 Généralisation du PGCD et PPCM

Soit $n \in \mathbb{N}^*$, $A_1, A_2, \dots, A_n \in \mathbb{K}[X]$. Alors $\exists! D \in \mathbb{K}[X]$ nul ou unitaire tel que :
(1) $\forall i \in [\![1, n]\!]$, $D \mid A_i$;
(2) $\forall P \in \mathbb{K}[X]$, si $\forall i \in [\![1, n]\!]$, $P \mid A_i$, alors $P \mid D$.
D s'appelle le PGCD des A_i et se note $\bigwedge_{i=1}^{n} A_i$.

Résultats

- Si $D = \bigwedge_{i=1}^{n} A_i$, $\exists U_1, U_2, \dots, U_n \in \mathbb{K}[X]$ tel que $D = \sum_{k=1}^{n} U_k A_k$.
- $\bigwedge_{i=1}^{n} A_i = 1 \Leftrightarrow \exists U_1, U_2, \dots, U_n \in \mathbb{K}[X] / \sum_{i=1}^{n} A_i U_i = 1$.

PPCM

Soit $n \in \mathbb{N}^*$, $A_1, A_2, \dots, A_n \in \mathbb{K}[X]$, alors $\exists! M \in \mathbb{K}[X]$ nul ou unitaire tel que :
(1) $\forall i \in [[1, n]]$, $A_i \mid M$;
(2) Si $P \in \mathbb{K}[X]$ est divisé par tous les A_i, alors $M \mid P$.
M s'appelle le PPCM de $A_1, A_2, \dots, A_n$ et se note $\bigvee_{i=1}^{n} A_i$.

Démonstration

Existence : Pour $i \in [\![1, n]\!]$, $I_i = A_i \mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$ donc $I = \bigvee_{i=1}^{n} A_i \mathbb{K}[X]$ aussi. Ainsi, $\exists M \in \mathbb{K}[X]$ nul si $I = \{0\}$, unitaire sinon tel que $I = M\mathbb{K}[X]$:
- pour $i \in [\![1, n]\!]$, $M \in I \subset I_i$ donc $A_i \mid M$;
- si $\forall i \in [\![1, n]\!]$, $A_i \mid P$ avec $P \in \mathbb{K}[X]$, $P \in I$ donc $M \mid P$.

Unicité : Si P et M vérifient (1) et (2), $P \mid M$ et $M \mid P$ donc $M = P$ car les deux polynômes sont unitaires ou nuls.

Remarques

- Si l'un des A_i est nul, alors $M = 0$.
- Pour $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{K}^*$, il est clair que $\bigvee_{i=1}^{n} (\alpha_i A_i) = \bigvee_{i=1}^{n} A_i$. On pourra donc supposer que les A_i sont unitaires ou nuls.
- Pour $A, B \in \mathbb{K}[X]$, $(A \wedge B)(A \vee B) = AB$.
- Pour $A = \prod_{i=1}^{r} P_i^{\alpha_i}$ avec $r \in \mathbb{N}^*$, $P_1, P_2, \dots, P_r \in \mathbb{K}[X]$ irréductibles unitaires, $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{N}$ et $B = \prod_{i=1}^{r} P_i^{\beta_i}$ avec $\beta_1, \beta_2, \dots, \beta_r \in \mathbb{N}$, on a

$$A \vee B = \prod_{i=1}^{r} P_i^{\max(\alpha_i, \beta_i)}$$

3 Étude des polynômes à coefficients complexes et réels

3.1 Étude de $\mathbb{C}[X]$

3.1.1 Polynôme scindé

Soit K un corps, $P \in \mathbb{K}[X]$ non-constant. P est scindé sur $\mathbb{K}$ si P est un produit de polynômes du premier degré.

Remarques

(1) $P \in \mathbb{K}[X]$ est scindé si et seulement si P s'écrit

$$P = \lambda (X - x_1)(X - x_2) \cdots (X - x_n)$$

avec $\lambda \in \mathbb{K}^*$, $x_1, x_2, \ldots, x_n \in \mathbb{K}$ non nécessairement distincts avec $n \in \mathbb{N}^*$. On a alors $n = \deg P$ et $\lambda = \text{CD}(P)$ donc c'est l'écriture de P en produits d'irréductibles. En regroupant les facteurs égaux, P s'écrit aussi

$$P = \lambda (X - y_1)^{\alpha_1} \cdots (X - y_r)^{\alpha_r}$$

avec $\lambda \in \mathbb{K}^*$, $r \in \mathbb{N}^*$, $y_1, y_2, \ldots, y_r \in \mathbb{K}$ distincts et $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}^*$. De même, on en déduit que $\lambda = \text{CD}(P)$, $\alpha_1 + \alpha_2 + \cdots + \alpha_r = \deg P$ et que $\{y_1, y_2, \ldots, y_r\}$ est l'ensemble des racines de P. De plus, $\forall i \in [\![1, r]\!]$, α_i est l'ordre de multiplicité de y_i.

(2) Soit $P \in \mathbb{K}[X]$ non-constant, $n = \deg P$.

- Si P admet r racines distinctes $y_1, y_2, \ldots, y_r \in \mathbb{K}$ et s'il existe $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}^*$ tels que $\sum_{i=1}^{r} \alpha_i = n$ et $\forall i \in [\![1, r]\!]$, $(X - y_i)^{\alpha_i} \mid P$, alors P est scindé et s'écrit

$$P = C \prod_{i=1}^{r} (X - y_i)^{\alpha_i} \quad C \in \mathbb{K}^*$$

3.1.2 Corps algébriquement clos

Soit $\mathbb{K}$ un corps. Les assertions suivantes sont équivalentes :
(1) tout polynôme non constant de $\mathbb{K}[X]$ est scindé ;
(2) tout polynôme non-constant de $\mathbb{K}[X]$ admet au moins une racine ;
(3) les polynômes irréductibles de $\mathbb{K}[X]$ sont les polynômes de degré 1.
Lorsqu'une de ces conditions est vérifiée, on dit que $\mathbb{K}$ est algébriquement clos.

Démonstration

(1) $\Rightarrow$ (2) Cette implication est claire puisque tout polynôme de degré 1 admet toujours une racine.

(2) $\Rightarrow$ (3) Soit $P \in \mathbb{K}[X]$ un polynôme irréductible dans $\mathbb{K}[X]$, montrons que P est de degré 1. On sait que $\deg P \geqslant 1$ donc P admet une racine x dans $\mathbb{K}$. Ainsi, $X - x \mid P$ or P est irréductible et $X - x$ n'est pas constant donc c'est un associé de P. P est donc de degré 1.

(3) $\Rightarrow$ (1) Soit $P \in \mathbb{K}[X]$ non constant, P peut s'écrire comme un produit d'irréductibles de degré 1 donc P est scindé.

3.1.3 Théorème de d'Alembert-Gauss et conséquences

$\mathbb{C}$ est un corps algébriquement clos [a].

a. Voir la section 11.3.2 du cours complet page 182 pour la démonstration de ce théorème.

Conséquences

- On sait décrire l'ensemble $\mathcal{I}$ des polynômes irréductibles unitaires de $\mathbb{C}[X]$: ce n'est autre que l'ensemble $\{X - z | z \in \mathbb{C}\}$.
- Soient $A, B \in \mathbb{C}[X] \setminus \{0\}$, $A \mid B$ dans $\mathbb{C}[X]$ si et seulement si $\forall z \in \mathbb{C}$, $\mathcal{V}_{X-z}(A) \leqslant \mathcal{V}_{X-z}(B)$, et si et seulement si toute racine de A d'ordre de multiplicité $\alpha \in \mathbb{N}^*$ est aussi racine de B d'ordre de multiplicité $\beta \geqslant \alpha$.
- Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$ (par exemple $\mathbb{Q}$ ou $\mathbb{R}$), pour $A, B \in \mathbb{K}[X] \setminus \{0\}$, $A \mid B$ dans $\mathbb{K}[X] \Leftrightarrow A \mid B$ dans $\mathbb{C}[X]$. Ainsi, $A \mid B$ si et seulement si toute racine x de A dans $\mathbb{C}$ d'ordre de multiplicité α est aussi racine de B d'ordre de multiplicité $\beta \geqslant \alpha$.
  Par exemple, trouvons les entiers naturels non nuls n tels que $1 + X + X^2 \mid 1 + X^n + X^{2n}$ dans $\mathbb{R}[X]$. $1 + X + X^2$ admet j et $\overline{j}$ pour racines complexes, ce sont des racines simples donc

$$\begin{aligned} 1 + X + X^2 \mid 1 + X^n + X^{2n} &\Leftrightarrow j \text{ et } \overline{j} \text{ sont racines de } 1 + X^n + X^{2n} \\ &\Leftrightarrow j \text{ est racine de } 1 + X^n + X^{2n} \end{aligned}$$

  - Si $n \equiv 0$ [3], alors $\exists k \in \mathbb{N}^*$ tel que $n = 3k$ donc $1 + j^n + j^{2n} = 3 \neq 0$ car $j^3 = 1$.
  - Si $n \equiv 1$ [3], alors $n = 3k + 1$ donc $1 + j^n + j^{2n} = 1 + j + \overline{j} = 0$.
  - Si $n \equiv 2$ [3], alors $n = 3k + 2$ donc $1 + j^n + j^{2n} = 0$.

  Ainsi, $1 + X + X^2 \mid 1 + X^n + X^{2n} \Leftrightarrow 3 \nmid n$.
- Soient $A, B \in \mathbb{C}[X] \setminus \{0\}$. $A \wedge B = 1$ si et seulement si A et B n'ont aucune racine commune dans $\mathbb{C}$.

  $\Rightarrow$ Si A et B ont une racine commune x dans $\mathbb{C}$, alors $X - x \mid A$ et $X - x \mid B$ donc $X - x \mid A \wedge B = 1$, ce qui est absurde.

  $\Leftarrow$ Si $A \wedge B \neq 1$, $A \wedge B$ n'est pas constant donc il admet une racine x dans $\mathbb{C}$ commune à A et B.
- Si $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, pour $A, B \in \mathbb{K}[X] \setminus \{0\}$,

$$\begin{aligned} A \wedge B = 1 \text{ dans } \mathbb{K}[X] &\Leftrightarrow A \wedge B = 1 \text{ dans } \mathbb{C}[X] \\ &\Leftrightarrow A \text{ et } B \text{ n'ont pas de racine commune dans } \mathbb{C} \end{aligned}$$

- Soit $P \in \mathbb{C}[X]$ non-constant, $\mathcal{R} = \{x \in \mathbb{C} | x \text{ est racine de } P\}$. Pour $z \in \mathcal{R}$, soit $\alpha(z)$ l'ordre de multiplicité de z dans P et $\lambda = \text{CD}(P)$. Alors

$$P = \lambda \prod_{z \in \mathcal{R}} (X - z)^{\alpha(z)}$$

3.2 Étude de $\mathbb{R}[X]$

3.2.1 Conjugaison dans $\mathbb{C}[X]$

Pour $P \in \mathbb{C}[X]$, $P = \sum_{k \in \mathbb{N}} \lambda_k X^k$ et $\overline{P} = \sum_{k \in \mathbb{N}} \overline{\lambda_k} X^k$. De plus, pour $z \in \mathbb{C}$:

$$\begin{aligned} \widetilde{\overline{P}}(z) &= \sum_{k \in \mathbb{N}} \overline{\lambda_k} z^k \\ &= \overline{\sum_{k \in \mathbb{N}} \lambda_k \overline{x^k}} \\ &= \overline{\widetilde{P}(\overline{z})} \end{aligned}$$

Propriétés

(1) $P \in \mathbb{R}[X] \Leftrightarrow P = \overline{P}$

(2) Pour $P, Q \in \mathbb{C}[X]$, $\overline{P + Q} = \overline{P} + \overline{Q}$, $\overline{PQ} = \overline{P} \cdot \overline{Q}$.

(3) $\overline{\overline{P}} = P$ [a].

a. *« Lui c'est P-Attila. Parce que P-Attila c'est un P barre-barre ! »*

Résultats Soit $A \in \mathbb{C}[X]$ non constant et $z \in \mathbb{C}$, $\alpha \in \mathbb{N}^*$:

$$\begin{aligned}(X-z)^\alpha \mid A &\Leftrightarrow \overline{(X-z)^\alpha} \mid \overline{A} \\ &\Leftrightarrow \overline{X-z}^\alpha \mid \overline{A} \\ &\Leftrightarrow (X-\overline{z})^\alpha \mid \overline{A}\end{aligned}$$

On a donc les résultats suivants :

Pour $A \in \mathbb{C}[X]$ et $z \in \mathbb{C}$:

z est racine de A d'ordre de multiplicité $\alpha \Leftrightarrow \overline{z}$ est racine de $\overline{A}$ d'ordre de multiplicité α

Donc, si $A \in \mathbb{R}[X]$ et $z \in \mathbb{C}$:

z est racine de A d'ordre de multiplicité $\alpha \Leftrightarrow \overline{z}$ est racine de A d'ordre de multiplicité α

3.2.2 Polynômes irréductibles de $\mathbb{R}[X]$

On sait que tous les polynômes de degré 1 sont irréductibles. Quels sont les irréductibles de degré supérieur ou égal à 2 ?

Soit $P \in \mathbb{R}[X]$ irréductible avec $\deg P \geqslant 2$, P ne peut avoir de racines réelles : si x est racine de P, $X-x \mid P$ ce qui est faux.

Piège ! La réciproque est fausse : $\left(X^2+1\right)^2$ n'est pas irréductible mais n'admet pas de racines dans $\mathbb{R}$.

Ici, le même polynôme P pris dans $\mathbb{C}[X]$ est non-constant et P admet une racine $z \in \mathbb{C}\backslash\mathbb{R}$. On sait que $\overline{z}$ est également racine de P et $z \neq \overline{z}$ car $z \notin \mathbb{R}$. Ainsi, $(X-z)(X-\overline{z}) \mid P$ dans $\mathbb{C}[X]$. Or $(X-z)(X-\overline{z}) = X^2 - 2\Re\mathrm{e}(z)X + |z|^2 \in \mathbb{R}$ donc ce polynôme est un diviseur non-constant de P dans $\mathbb{R}[X]$ donc c'est un associé de P car P est irréductible, donc $\deg P = 2$.

Il reste donc à trouver quels sont les polynômes irréductibles de degré 2.

Lemme général Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ avec $\deg P \in \{2,3\}$. Alors P est irréductible dans $\mathbb{K}[X]$ si et seulement si P n'admet pas de racines dans $\mathbb{K}$.

$\Rightarrow$ Si P admet une racine $x \in \mathbb{K}$, $X-x$ divise P dans $\mathbb{K}$ et $X-x$ est non-trivial, donc c'est impossible.

$\Leftarrow$ Si P n'est pas irréductible, P s'écrit $P = ST$ avec $S, T \in \mathbb{K}[X]$ et $\deg S, \deg T \in [\![1, \deg P]\!]$ or $\deg P = \deg S + \deg T \in \{2,3\}$ donc $\deg S = 1$ ou $\deg T = 1$ donc S ou T est irréductible et admet une racine.

Ici, soit $P = aX^2 + bX + c$ avec $a \in \mathbb{R}^*$ et $b, c \in \mathbb{R}$. Pour $t \in \mathbb{R}$,

$$\begin{aligned}\widetilde{P}(t) &= at^2 + bt + c \\ &= a\left(\left(t + \frac{b}{2a}\right)^2 - \frac{b^2-4ac}{4a^2}\right)\end{aligned}$$

Posons $\Delta = b^2 - 4ac$.

- Si $\Delta < 0$, $\dfrac{\Delta}{4a^2} < 0$ et $\forall t \in \mathbb{R}$, $\left(t + \dfrac{b}{2a}\right)^2 - \dfrac{\Delta}{4a^2} > 0$ donc $\widetilde{P}$ ne s'annule jamais, P est irréductible.
- Si $\Delta \geqslant 0$, alors pour $t \in \mathbb{R}$,

$$\begin{aligned}\left(t + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2} &= \left(t + \frac{b}{2a}\right)^2 - \left(\frac{\sqrt{\Delta}}{2a}\right)^2 \\ &= \left(t - \frac{-b+\sqrt{\Delta}}{2a}\right)\left(t - \frac{-b-\sqrt{\Delta}}{2a}\right)\end{aligned}$$

P s'annule en deux points donc il n'est pas irréductible.

Bilan

Les polynômes irréductibles de $\mathbb{R}[X]$ sont :
– les polynômes de degré 1 ;
– les polynômes de degré 2 à discriminant strictement négatif.

Conséquences

– Tout polynôme $P \in \mathbb{R}[X]$ de degré impair a au moins une racine réelle.
  ◦ C'est vrai pour les polynômes de degré 1.
  ◦ Soit $m \in \mathbb{N}^*$, supposons que tout polynôme de degré impair inférieur à $2m+1$ admet une racine. Soit $P \in \mathbb{R}[X]$ de degré $2m+3$, P n'est pas irréductible car $\deg P \geqslant 3$ et p s'écrit $P = ST$ avec $\deg S \geqslant 1$, $\deg T \geqslant 1$ et $\deg S + \deg T = 2m+3$ donc $\deg S$ ou $\deg T$ est impair inférieur à $2m+1$ donc S ou T admet au moins une racine donc P aussi.
– Tout $P \in \mathbb{R}[X]$ de degré supérieur ou égal à 1 s'écrit donc

$$P = C\prod_{i=1}^{r}(X-x_i)^{\alpha_i}\prod_{j=1}^{s}\left(X^2+b_iX+c_i\right)^{\beta_i}$$

avec $C \in \mathbb{R}^*$, $r, s \in \mathbb{N}$ tels que $r+s \geqslant 1$, $x_1, x_2, \ldots, x_r \in \mathbb{R}$ distincts, $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}^*$, $(b_1, c_1), (b_2, c_2), \ldots, (b_s, c_s)$ $\mathbb{R}^2$ distincts avec $\forall i \in [\![1, s]\!]$, $b_i^2 - 4c_i > 0$ et $\beta_1, \beta_2, \ldots, \beta_s \in \mathbb{N}^*$. On a tout de suite $C = \text{CD}(P)$, $x_1, x_2, \ldots, x_r$ sont les racines réelles de P et pour $i \in [\![1, r]\!]$, α_i est l'ordre de multiplicité de x_i.

Comment obtenir cette écriture en pratique ? On factorise d'abord P dans $\mathbb{C}[X]$. Pour $z \in \mathbb{C}\backslash\mathbb{R}$, z est racine de P d'ordre α si et seulement si $\overline{z}$ est racine de P d'ordre α. Les éventuelles racines non-réelles se regroupent par 2 : $z_1, \overline{z_1}, z_2, \overline{z_2}, \ldots, z_s, \overline{z_s}$ et $\forall i \in [[1, s]]$ on désigne par β_i l'ordre de z_i et $\overline{z_i}$.

Soient $x_1, x_2, \ldots, x_r$ les éventuelles racines réelles de P, et $\forall i \in [[1, r]]$, α_i l'ordre éventuel de x_i. Dans $\mathbb{C}[X]$,

$$\begin{aligned} P &= C\prod_{i=1}^{r}(X-x_i)^{\alpha_i}\prod_{j=1}^{s}(X-z_j)^{\beta_i}(X-\overline{z_j})^{\beta_i} \\ &= C\prod_{i=1}^{r}(X-x_i)^{\alpha_i}\prod_{j=1}^{s}\left(X^2-2\Re\text{e}(z_j)X+|z_j|^2\right) \end{aligned}$$

Or, $\forall j \in [[1, r]]$, $X^2 - 2\Re\text{e}(z_j)X + |z_j|^2$ est irréductible car

$$\begin{aligned} 4\Re\text{e}(z_j)^2 - 4|z_j|^2 &= 4\left(\Re\text{e}(z_j)^2 - |z_j|^2\right) \\ &= -4\Im\text{m}(z_j)^2 < 0 \quad \text{car } \Im\text{m}(z_j) \neq 0 \end{aligned}$$

On obtient bien aussi la factorisation de P dans $\mathbb{C}[X]$. Il peut y avoir d'autres façons de procéder.

Exemple Factoriser $P = X^4 + 1$ dans $\mathbb{R}[X]$.

– On a d'une première façon :

$$\begin{aligned} X^4+1 &= X^4+2X^2+1-2X^2 \\ &= \left(X^2+1\right)^2 - \left(\sqrt{2}X\right)^2 \\ &= \left(X^2-\sqrt{2}X+1\right)\left(X^2+\sqrt{2}X+1\right) \end{aligned}$$

– $\text{e}^{i\frac{\pi}{4}}$ est racine de P dans $\mathbb{C}$ donc $\text{e}^{-i\frac{\pi}{4}}$ aussi. Or P est pair donc $-\text{e}^{i\frac{\pi}{4}}$ et $-\text{e}^{-i\frac{\pi}{4}}$ sont aussi des racines de P dans $\mathbb{C}$. P est de degré 4 et admet 4 racines distinctes donc

$$\begin{aligned} P &= \left(X-\text{e}^{i\frac{\pi}{4}}\right)\left(X-\text{e}^{-i\frac{\pi}{4}}\right)\left(X+\text{e}^{i\frac{\pi}{4}}\right)\left(X+\text{e}^{-i\frac{\pi}{4}}\right) \\ &= \left(X^2-\sqrt{2}X+1\right)\left(X^2+\sqrt{2}x+1\right) \end{aligned}$$

4 Fonctions symétriques élémentaires

4.1 Faits de base

Soit $n \in \mathbb{N}^*$, $\mathbb{K}$ un corps quelconque. On définit n fonctions de $\mathbb{K}^n$ dans $\mathbb{K}$ par $\forall (x_1, x_2, \ldots, x_n) \in \mathbb{K}^n$:

$$\begin{aligned}
\sigma_1(x_1, x_2, \ldots, x_n) &= \sum_{i=1}^{n} x_i \\
\sigma_2(x_1, x_2, \ldots, x_n) &= \sum_{1 \leqslant i < j \leqslant n} x_i x_j = \sum_{A \in \mathcal{P}_2(n)} \prod_{\alpha \in A} x_\alpha \\
&\vdots \\
\sigma_k(x_1, x_2, \ldots, x_n) &= \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \cdots x_{i_k} = \sum_{A \in \mathcal{P}_k(n)} \prod_{\alpha \in A} x_\alpha \\
&\vdots \\
\sigma_n(x_1, x_2, \ldots, x_n) &= \prod_{i=1}^{n} x_i
\end{aligned}$$

On rappelle que pour $k \in [\![1, n]\!]$, $\mathcal{P}_k(n)$ est l'ensemble des parties à k éléments de $[\![1, n]\!]$.

Exemples

- Pour $n = 2$ et $(x_1, x_2) \in \mathbb{K}^2$, $\sigma_1(x_1, x_2) = x_1 + x_2$ et $\sigma_2(x_1, x_2) = x_2 x_1$.
- Pour $n = 3$, $(x_1, x_2, x_3) \in \mathbb{K}^3$:

$$\begin{aligned}
\sigma_1(x_1, x_2, x_3) &= x_1 + x_2 + x_3 \\
\sigma_2(x_1, x_2, x_3) &= x_1 x_2 + x_1 x_3 + x_2 x_3 \\
\sigma_3(x_1, x_2, x_3) &= x_1 x_2 x_3
\end{aligned}$$

- Pour $n = 4$, $(x_1, x_2, x_3, x_4) \in \mathbb{K}^4$:

$$\begin{aligned}
\sigma_1(x_1, x_2, x_3, x_4) &= x_1 + x_2 + x_3 + x_4 \\
\sigma_2(x_1, x_2, x_3, x_4) &= x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4 \\
\sigma_3(x_1, x_2, x_3, x_4) &= x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4 \\
\sigma_4(x_1, x_2, x_3, x_4) &= x_1 x_2 x_3 x_4
\end{aligned}$$

Explication du terme symétrique Pour $\tau \in S_n$ et $f \in \mathcal{F}(\mathbb{K}^n, \mathbb{K})$, on définit $\tau \star f$ par $\forall (x_1, x_2, \ldots, x_n) \in \mathbb{K}^n$, $\tau \star f(x_1, x_2, \ldots, x_n) = f\left(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}\right)$.

On dit que f est symétrique si $\forall \tau \in S_n$, $\tau \star f = f$. Ici, $\sigma_1, \sigma_2, \ldots, \sigma_n$ sont des fonctions symétriques de $\mathbb{K}^n$ dans $\mathbb{K}$.

Explication du terme élémentaire

Si $f : \mathbb{K}^n \longrightarrow \mathbb{K}$ est polynômiale et symétrique, alors f s'exprime comme un polynôme en $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Par exemple, soit $f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} x_i^2$. on notera pour simplifier σ_k au lieu de $\sigma_k(x_1, x_2, \ldots, x_n)$. On

a alors :

$$\begin{aligned}\sigma_1^2 &= \sum_{i=1}^{n} x_i \sum_{j=1}^{n} x_j \\ &= \sum_{i,j\in[[1,n]]} x_i x_j \\ &= \sum_{i=1}^{n} x_i^2 + \sum_{i\neq j} x_i x_j \\ &= \sum_{i=1}^{n} x_i^2 + 2\sum_{i<j} x_i x_j\end{aligned}$$

D'où $\sigma_1^2 = f + 2\sigma_2 \Leftrightarrow f = \sigma_1^2 - 2\sigma_2$. On a bien écrit f comme fonction polynômiale des fonctions symétriques élémentaires.

Théorème

Pour $n \in \mathbb{N}^*$, $(x_1, x_2, \ldots, x_n) \in \mathbb{K}^n$:

$$\prod_{k=1}^{n} (X - x_k) = X^n + \sum_{k=1}^{n} (-1)^k \sigma_k X^{n-k}$$

On note σ_k à la place de $\sigma_k(x_1, x_2, \ldots, x_n)$.

Démonstration

– Vérifions le résultat pour $n = 2$. Soient $x, y \in \mathbb{K}$,

$$(X - x)(X - y) = X^2 - \underbrace{(x + y)X}_{\sigma_1(x,y)} + \underbrace{xy}_{\sigma_2(x,y)}$$

– Supposons le résultat vrai pour $n \in \mathbb{N}$, on note $\widetilde{\sigma_1}, \widetilde{\sigma_2}, \ldots, \widetilde{\sigma_n}$ les n fonctions symétriques élémentaires sur $\mathbb{K}^n$ et $\sigma_1, \sigma_2, \ldots, \sigma_{n+1}$ les $n+1$ fonctions symétriques élémentaires sur $\mathbb{K}^n$. On notera pour simplifier $\widetilde{\sigma_k}$ au lieu de $\widetilde{\sigma_k}(x_1, x_2, \ldots, x_n)$. Tout d'abord :

$$\prod_{k=1}^{n+1} (X - x_k) = (X - x_{n+1}) \prod_{k=1}^{n} (X - x_k)$$

donc, d'après l'hypothèse de récurrence,

$$\begin{aligned}\prod_{k=1}^{n+1} (X - x_k) &= (X - x_{n+1})\left(X^n - \widetilde{\sigma_1}X^{n-1} + \widetilde{\sigma_2}X^{n-2} + \cdots + (-1)^n \widetilde{\sigma_n}\right) \\ &= X^{n+1} - \underbrace{(\widetilde{\sigma_1} + x_{n+1})}_{\sigma_{n+1}(x_1,x_2,\ldots,x_{n+1})} X^n + (\widetilde{\sigma_2} + x_{n+1}\widetilde{\sigma_1}) X^{n-1} + \cdots + (-1)^{n+1} \sigma_{n+1}(x_1, x_2, \ldots, x_{n+1})\end{aligned}$$

Reste à montrer que $\forall k \in [[2,n]]$, $(-1)^k \sigma_k(x_1,x_2,\dots,x_{n+1}) = \widetilde{\sigma_k} + x_{n+1}\widetilde{\sigma_{k-1}}$. Pour $k \in [\![2,n]\!]$:

$$\begin{aligned}
\sigma_k(x_1,x_2,\dots,x_{n+1}) &= \sum_{A\in\mathcal{P}_k(n+1)} \prod_{\alpha\in A} x_\alpha \\
&= \sum_{\substack{A\in\mathcal{P}_k(n+1)\\ n+1\notin A}} \prod_{\alpha\in A} x_\alpha + \sum_{\substack{A\in\mathcal{P}_k(n+1)\\ n+1\in A}} \prod_{\alpha\in A} x_\alpha \\
&= \sum_{A\in\mathcal{P}_k(n)} \prod_{\alpha\in A} x_\alpha + \sum_{\substack{A\in\mathcal{P}_k(n+1)\\ n+1\in A}} x_{n+1} \prod_{\alpha\in A\setminus\{n+1\}} x_\alpha \\
&= \widetilde{\sigma_k} + x_{n+1} \underbrace{\sum_{\substack{A\in\mathcal{P}_k(n+1)\\ n+1\notin A}} \prod_{\alpha\in A\setminus\{n+1\}} x_\alpha}_{\sum_{B\in\mathcal{P}_{k-1}(n)} \prod_{\alpha\in B} x_\alpha} \\
&= \widetilde{\sigma_k} + x_{n+1}\widetilde{\sigma_{k-1}}
\end{aligned}$$

D'où la formule et le résultat.

4.2 Relations entre racines et coefficients

Soit $n \in \mathbb{N}^*$, $P \in \mathbb{K}[X]$ un polynôme scindé de degré n. P s'écrit donc $P = C\prod_{i=1}^{n}(X-x_i)$ avec $C \in \mathbb{K}^*$ et $x_1,x_2,\dots,x_n \in \mathbb{K}$ non-nécessairement distinctes. Les x_i sont les racines de P répétées autant de fois que leur ordre de multiplicité. Or P s'écrit d'autre part $P = a_0 + a_1X + \cdots + a_nX^n$ et $\text{CD}(P) = C = a_n \in \mathbb{K}^*$. D'après ce qui précède,

$$a_nX^n + \sum_{k=1}^{n} a_{n-k}X^{n-k} = P = C\prod_{i=1}^{n}(X-x_i) = CX^n + \sum_{k=1}^{n} C(-1)^k \sigma_k(x_1,x_2,\dots,x_n)X^{n-k}$$

Ainsi, pour $k \in [\![1,n]\!]$,

$$a_{n-k} = C(-1)^k\sigma_k(x_1,x_2,\dots,x_n) \Leftrightarrow \frac{a_{n-k}}{a_n} = (-1)^k\sigma_k(x_1,x_2,\dots,x_n)$$

En particulier, pour $k=1$ et $k=n$:

$$\frac{a_{n-1}}{a_n} = -\sum_{k=1}^{n} x_k \quad \text{et} \quad \frac{a_0}{a_n} = (-1)^n\prod_{i=1}^{n} x_i$$

5 Polynôme dérivé

Dans ce paragraphe, $\mathbb{K}$ est un corps de caractéristique nulle : $\forall n \in \mathbb{N}^*$, $n1_{\mathbb{K}} \neq 0$. Par exemple $\mathbb{R}$, $\mathbb{Q}$ ou $\mathbb{C}$ vérifient cette propriété.

5.1 Généralités

5.1.1 Définition et propriétés

Soit $P \in \mathbb{K}[X]$, $P = \sum_{k\in\mathbb{N}} a_k X^k$, on définit le polynôme dérivé de P par :

$$P' = \sum_{k\in\mathbb{N}^*} k a_k X^{k-1}$$

Si P s'écrit $P = a_0 + a_1 X + \cdots a_N X^N$ avec $N \in \mathbb{N}^*$, alors $P' = a_1 + 2a_2 X + \cdots + N a_N X^{N-1} \in \mathbb{K}[X]$. L'application $D : \begin{array}{l}\mathbb{K}[X] \longrightarrow \mathbb{K}[X] \\ P \mapsto D(P) = P'\end{array}$ s'appelle la dérivation.

Propriétés

(1) est linéaire : pour $P, Q \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$,

$$D(\alpha P + Q) = \alpha D(P) + D(Q)$$

En particulier, pour $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{N}^*$ et $Q_1, Q_2, \ldots, Q_n \in \mathbb{K}[X]$,

$$D\left(\sum_{i=1}^{n} \alpha_i Q_i\right) + \alpha \sum_{i=1}^{n} D(Q_i)$$

(2) $\forall P, Q \in \mathbb{K}[X]$,

$$D(PQ) = D(P)\,Q + D(Q)\,P$$

(3) Soit $P \in \mathbb{K}[X]$ de degré plus grand que 1, alors $\deg P' = \deg P - 1$. $P' = 0 \Leftrightarrow P$ est constant.

Démonstrations

(1) Notons $P = \sum_{k\in\mathbb{N}} a_k X^k$ et $Q = \sum_{k\in\mathbb{N}} b_k X^k$, alors $\alpha P + Q = \sum_{k\in\mathbb{N}} (\alpha a_k + b_k) X^k$ donc :

$$\begin{aligned} D(\alpha P + Q) &= \sum_{k\in\mathbb{N}^*} k(\alpha a_k + b_k) X^{k-1} \\ &= \alpha \sum_{k\in\mathbb{N}^*} k a_k X^{k-1} + \sum_{k\in\mathbb{N}^*} k b_k X^{k-1} \\ &= \alpha D(P) + D(Q) \end{aligned}$$

(2) On a $PQ = \sum_{k\in\mathbb{N}} c_k X^k$ où $c_k = \sum_{p+q=k} a_p b_q$. Ainsi

$$\begin{aligned} D(PQ) &= \sum_{k\in\mathbb{N}^*} k c_k X^{k-1} \\ &= \sum_{k\in\mathbb{N}} (k+1) c_{k+1} X^k \end{aligned}$$

Or

$$D(P) = \sum_{k\in\mathbb{N}} (k+1) a_{k+1} X^k \quad \text{et} \quad D(Q) = \sum_{k\in\mathbb{N}} (k+1) b_{k+1} X^k$$

Donc $D(P)Q = \sum_{k\in\mathbb{N}} u_k X^k$ où $u_k = \sum_{p+q=k} (p+1)\,a_{p+1}b_q$ et $D(Q)P = \sum_{k\in\mathbb{N}} v_k X^k$ où $v_k = \sum_{p+q=k} a_p b_{q+1}\,(q+1)$ d'où

$$D(P)Q + D(Q)P = \sum_{k\in\mathbb{N}} (u_k + v_k) X^k$$

Montrons alors que $\forall k \in [[1,n]]$, $u_k v_k = (k+1)\,c_k$. Pour $k \in \mathbb{N}$:

$$\begin{aligned}
u_k + v_k &= \sum_{p+q=k} (p+1)\,a_{p+1}b_q + a_p\,(q+1)\,b_{q+1} \\
&= \sum_{p=0}^{k} (p+1)\,a_{p+1}b_{k-p} + \sum_{q=0}^{k} a_{k-q}\,(q+1)\,b_{q+1} \\
&= \sum_{j=1}^{k+1} j a_j b_{k+1-j} + \sum_{i=1}^{k+1} i b_i a_{k+1-i} \\
&= \sum_{j=1}^{k+1} j a_j b_{k+1-j} + \sum_{j=0}^{k} (k+1-j)\,b_{k+1-j}a_j \\
&= (k+1)\,a_{k+1}b_0 + \sum_{j=1}^{k} (k+1)\,a_j b_{k+1-j} + (k+1)\,a_0 b_{k+1} \\
&= (k+1)\left[a_{k+1}b_0 + a_0 b_{k+1} + \sum_{j=1}^{k} a_j b_{k+1-j}\right] \\
&= (k+1)\sum_{j=0}^{k+1} a_j b_{k+1-j} \\
&= (k+1)\,c_{k+1}
\end{aligned}$$

(3) Soit $d = \deg P \in \mathbb{N}^*$, P s'écrit $P = a_0 + a_1 X + \cdots + a_d X^d$ avec $a_d \neq .$ d'où $P' = a_1 + 2a_2 X + \cdots + d a_d X^{d-1}$ avec $d a_d \neq 0$ car $d \in \mathbb{N}^*$, d'où le résultat. En particulier, $P' \neq 0$. Si P est constant, il est évident que P' est nul.

5.1.2 Dérivation multiple

On rappelle que la dérivation est $D : \mathbb{K}[X] \longrightarrow \mathbb{K}[X]$, on peut définir pour $m \in \mathbb{N}$ D^m par :
- $D^0 = \mathrm{Id}_{\mathbb{K}[X]}$;
- $\forall m \in \mathbb{N}$, $D^{m+1} = D^m \circ D$.

Pour $P \in \mathbb{K}[X]$, $D^m(P)$ est aussi noté $P^{(m)}$ comme pour les fonctions. Par ailleurs pour $n \in \mathbb{N}$, on note $\mathbb{K}_m[X] = \{P \in \mathbb{K}[X] \mid \deg P \leqslant m\}$. On a de manière immédiate, $\forall P, Q \in \mathbb{K}_m[X]$ et $\forall \alpha \in \mathbb{K}$, $\alpha P + Q \in \mathbb{K}_m[X]$.

Montrons que $D(\mathbb{K}_m[X]) = \mathbb{K}_{m-1}[X]$:
- soit $P \in \mathbb{K}_m[X]$, $\deg P \leqslant m$. Si P est constant, $P \in \mathbb{K}_{m-1}[X]$, sinon $\deg D(P) = \deg P - 1 \leqslant m-1$ donc $D(P) \in \mathbb{K}_{m-1}[X]$.
- Soit $Q = a_0 + a_1 X + \cdots + a_{m-1}X^{m-1} \in \mathbb{K}_{m-1}[X]$, alors $Q = D(P)$ où

$$P = a_0 + \frac{a_1}{2}X \cdots + \frac{a_{m-1}}{m}X^m \in \mathbb{K}_m[X]$$

.

On a alors pour $m \geqslant 2$,

$$\begin{aligned}
D^2(\mathbb{K}_m[X]) &= D(D(\mathbb{K}_m[X])) \\
&= D(\mathbb{K}_{m-1}[X]) \\
&= \mathbb{K}_{m-2}[X]
\end{aligned}$$

donc $D^m(\mathbb{K}_m[X]) = \mathbb{K}_0[X]$ et $D^{m+1}(\mathbb{K}_m[X]) = D(\mathbb{K}_0[X]) = \{0\}$.

Maintenant, prouvons que pour $P \in \mathbb{K}[X]$ et $m \in \mathbb{N}^*$, $\deg P \leqslant m \Leftrightarrow D^{m+1}(P) = 0$.

$\Rightarrow$ $D^{m+1}(\mathbb{K}_m[X]) = 0$ d'où cette implication.

$\Leftarrow$ Si $\deg P > m$, alors $\deg D^{m+1}(P) = \deg P - (m+1) \geqslant 0$ donc $D^{m+1}(P) \neq 0$.

Formule de Leibniz $\forall P, Q \in \mathbb{K}[X]$, $\forall n \in \mathbb{N}$,

$$D^n(PQ) = \sum_{k=0}^{n} \binom{n}{k} D^k(P) D^{n-k}(Q) = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$$

La démonstration est absolument identique à celle vu sur les fonctions [a].

Dérivée k-ième de $(X-a)^n$ Pour $n \in \mathbb{N}$, $k \in [[0,n]]$ et $a \in \mathbb{K}$, montrons que

$$D^k\left((X-a)^n\right) = \frac{n!}{(n-k)!}(X-a)^{n-k}$$

Soit $a \in \mathbb{K}$ et H_n : « $\forall k \in [[0,n]]$, $D^k\left((X-a)^n\right) = \frac{n!}{(n-k)!}(X-a)^{n-k}$ ».

– H_0 est vraie car $D^0\left((X-a)^0\right) = 1 = \dfrac{0!}{(0-0)!}(X-a)^{0-0}$.

– Supposons H_n vraie pour $n \in \mathbb{N}$ et prouvons H_{n+1}, soit $k \in [[0,n]]$. Alors

$$\begin{aligned} D^k\left((X-a)^{n+1}\right) &= D^k\left((X-a)^n (X-a)\right) \\ &= \sum_{p=0}^{k} \binom{k}{p} D^p\left((X-a)^n\right) D^{k-p}(X-a) \end{aligned}$$

◦ Si $k = 0$, alors $D^0\left((X-a)^{n+1}\right) = (X-a)^{n+1}$ et $\dfrac{(n+1)!}{(n+1-0)!}(X-a)^{n+1} = (X-a)^{n+1}$ d'où le résultat.

◦ Si $k \geqslant 1$, $D^k(X-a) = \delta_{1k}$ car $\deg(X-a) = 1$ donc

$$\begin{aligned} D^k\left((X-a)^{n+1}\right) &= \binom{k}{0} D^k\left((X-a)^n\right) D^0(X-a) + \binom{k}{1} D^{k-1}\left((X-a)^n\right) D(X-a) \\ &= D^k\left((X-a)^n\right)(X-a) + k D^{k-1}\left((X-a)^n\right) \cdot 1 \end{aligned}$$

→ Si $k = n+1$, alors $\deg(X-a)^n = n$ donc $D^{n+1}\left((X-a)^n\right) = 0$ donc

$$\begin{aligned} D^{n+1}\left((X-a)^{n+0}\right) &= (n+1) D^n\left((X-a)^n\right) \\ &= (n+1)\frac{n!}{(n-n)!}(X-a)^{n-n} \\ &= (n+1)! \\ &= \frac{(n+1)!}{(n+1-(n+1))!}(X-a)^{n+1-(n+1)} \end{aligned}$$

→ Si $k \in [[1,n]]$, alors

$$\begin{aligned} D^k\left((X-a)^{n+1}\right) &= \frac{n!}{(n-k)!}(X-a)^{n-k}(X-a) + k\frac{n!}{(n+1-k)!}(X-a)^{n+1-k} \\ &= (X-a)^{n+1-k}\frac{n!}{(n-k)!}\left[1 + \frac{k}{n+1-k}\right] \\ &= \frac{(n+1)!}{(n+1-k)!}(X-a)^{n+1-k} \end{aligned}$$

a. Voir section 14.3.1.3 du cours complet page 217.

Remarque $\forall m \in \mathbb{N}^*$, $\forall P_1, P_2, \ldots, P_m \in \mathbb{K}[X]$,

$$D\left(\prod_{i=1}^{m} P_i\right) = \sum_{k=1}^{m} D(P_k) \prod_{\substack{i=1 \\ i\neq k}}^{m} P_i$$

D'où $\forall P \in \mathbb{K}[X]$, $m \in \mathbb{N}^*$, $D(P^m) = \sum_{k=1}^{m} P' P^{m-1} = mP' P^{m-1}$.

5.2 Polynômes et formule de Taylor

5.2.1 Petite histoire

Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, on note $P = \sum_{k\in\mathbb{N}} \lambda_k X^k$. Pour $k \geqslant 1$ et écrit :

$$\begin{aligned} X^k &= [(X-a)+a]^k \\ &= \sum_{p=0}^{k} \binom{k}{p} a^{k-p} (X-a)^p \end{aligned}$$

Donc P peut s'écrire $P = \sum_{k\in\mathbb{N}} \mu_k (X-a)^k$. C'est toujours en fait une somme finie, $\exists N \in \mathbb{N}$ tel que $\forall k \geqslant N$, $\lambda_k = 0$ d'où $\mu_k = 0$. Soit alors $j \in \mathbb{N}$:

$$\begin{aligned} D^j(P) &= D^j\left(\sum_{k\in\mathbb{N}} \mu_k (X-a)^k\right) \\ &= \sum_{k\in\mathbb{N}} \mu_k \underbrace{D^j\left((X-a)^k\right)}_{0 \text{ si } j>k} \\ &= \sum_{k\geqslant j} \mu_k D^j\left((X-a)^k\right) \\ &= \sum_{k\geqslant j} \mu_k \frac{k!}{(k-j)!} (X-a)^{k-j} \\ &= \mu_j j! + \sum_{k\geqslant j+1} \mu_k \frac{k!}{(k-j)!} (X-a)^{k-j} \end{aligned}$$

Or, pour $t \in \mathbb{K}$, $\widetilde{D^j(P)}(t) = \mu_j j! + \sum_{k\geqslant j+1} \mu_k \frac{k!}{(k-j)!} (t-a)^{k-j}$ donc $\widetilde{D^j(P)}(a) = \mu_j j!$ donc $\mu_j = \dfrac{\widetilde{D^j(P)}(a)}{j!}$.

Ainsi, $\forall P \in \mathbb{K}[X]$ et $\forall a \in \mathbb{K}$, P s'écrit

$$P = \sum_{k\in\mathbb{N}} \frac{\widetilde{D^j(P)}(a)}{j!} (X-a)^k$$

Cette somme est finie puisque $D^k(P) = 0$ si $k > \deg P$.

5.2.2 Caractérisation de l'ordre d'une racine

Lemme Soit $P \in \mathbb{K}[X]$, $x \in \mathbb{K}$ et $n \in \mathbb{N}^*$. x est d'ordre de multiplicité α si et seulement si $P = (X-x)^\alpha Q$ où $Q \in \mathbb{K}[X]$ et $\widetilde{Q}(x) \neq 0$. En particulier, x est racine simple de P si et seulement si $P = (X-x)Q$ avec $\widetilde{Q}(x) \neq 0$.

$\Rightarrow$ $(X-x)^\alpha \mid P$ donc $P = (X-x)^\alpha Q$ avec $Q \in \mathbb{K}[X]$. Si $\widetilde{Q}(x) = 0$, $X - x \mid Q$ donc $(X-x)^{\alpha+1} \mid P$ ce qui contredit la définition de α.

$\Leftarrow$ $(X-x)^\alpha \mid P$ donc $\beta = \mathcal{V}_{X-x}(P) \geqslant \alpha$ donc $P = (X-x)^\beta T = (X-x)^\alpha Q$ donc $(X-x)^{\beta-\alpha} T = Q$ et $\widetilde{Q}(x) = 0$ si $\beta > \alpha$ donc $\beta = \alpha$.

Théorème

Soit $P \in \mathbb{K}[X]$ non-constant, $\alpha \in \mathbb{N}^*$ et $x \in \mathbb{K}$. Alors x est racine de P d'ordre α si et seulement si $0 = \widetilde{P}(x) = \widetilde{P'}(x) = \cdots = \widetilde{P^{\alpha-1}}(x)$ et $\widetilde{P^\alpha}(x) \neq 0$.
En particulier :

(1) x est racine simple de P si et seulement si $\widetilde{P}(x) = 0$ et $\widetilde{P'}(x) \neq 0$;

(2) x est racine double de P si et seulement si $\widetilde{P}(x) = 0$, $\widetilde{P'}(x) = 0$ et $\widetilde{P''}(x) \neq 0$;

(3) x est racine multiple de P si et seulement si $0 = \widetilde{P}(x) = \widetilde{P'}(x)$.

Démonstration Montrons que pour $k \in \mathbb{N}^*$, $(X-x)^k \mid P \Leftrightarrow 0 = \widetilde{P}(x) = \widetilde{P'}(x) = \cdots = \widetilde{P^{k-1}}(x)$

$\Leftarrow$**Formulès** la formule de Taylor,

$$\begin{aligned} P &= \sum_{j\in\mathbb{N}} \underbrace{\frac{\widetilde{P^j}(x)}{j!}}_{0 \text{ si } j\leqslant k-1} (X-x)^j \\ &= \sum_{j\geqslant k} \frac{\widetilde{P^j}(x)}{j!} (X-x)^j \\ &= (X-x)^k \sum_{j\geqslant k} \frac{\widetilde{P^j}(x)}{j!} (X-x)^{j-k} \end{aligned}$$

Donc $(X-x)^k \mid P$.

$\Rightarrow$ Supposons que $(X-x)^k \mid P$, on écrit $P = (X-x)^k Q$ avec $Q \in \mathbb{K}[X]$. Pour $p \in [\![0, k-1]\!]$,

$$\begin{aligned} P^{(p)} &= \left[(X-x)^k Q\right]^{(p)} \\ &= \sum_{j=0}^{p} \binom{p}{j} D^j\left((X-x)^k\right) D^{p-j}(Q) \\ &= \sum_{j=0}^{p} \binom{p}{j} \frac{k!}{(k-j)!} (X-x)^{k-j} D^{p-j}(Q) \end{aligned}$$

D'où

$$\begin{aligned} \widetilde{P^{(p)}}(x) &= \sum_{j=0}^{p} \binom{p}{j} \frac{k!}{(k-j)!} \underbrace{0^{k-j}}_{0 \text{ car } k\geqslant j} D^{p-j}(Q) \\ &= 0 \end{aligned}$$

Ce résultat entraîne immédiatement le théorème.

Remarque Prenons $\mathbb{K} = \mathbb{C}$ et $P \in \mathbb{C}[X]$ non-constant.

- Toute racine x de P d'ordre de multiplicité $\alpha \geqslant 2$ est également racine de P' d'ordre $\alpha - 1$. Les racines simples de P ne sont pas racines de P'. En d'autres termes, $\forall x \in \mathbb{C}, \mathcal{V}_{X-x}(P) \geqslant 1 \Rightarrow \mathcal{V}_{X-x}(P') = \mathcal{V}_{X-x}(P) - 1$.
  En effet, $0 = \widetilde{P}(x) = \widetilde{P'}(x) = \cdots = \widetilde{P^{\alpha-1}}(x)$ donc $\widetilde{P^{\alpha-1}}(x) = \widetilde{P'^{\alpha-2}}(x) = \widetilde{P'}(x)$ et $\widetilde{P'^{\alpha-1}}(x) \neq 0$ d'où le résultat.

– P n'a que des racines simples dans $\mathbb{K}$ si et seulement si P et P' n'ont pas de racines communes, c'est-à-dire si $P \wedge P' = 1$.
En particulier, soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$. Soit $P \in \mathbb{K}[X]$ irréductible, $\deg P \geqslant 1 \Rightarrow \deg P' = \deg P - 1$, P' est non nul et $\deg P' < \deg P$ donc $P \nmid P'$ donc $P \wedge P' = 1$ dans $\mathbb{K}[X]$ car P est irréductible. On a vu que alors $P \wedge P' = 1$ dans $\mathbb{C}[X]$ donc P n'a que des racines simples dans $\mathbb{C}$.

6 Composition

6.1 Définition

Pour $P = \sum_{k\in\mathbb{N}} a_k X^k$, $Q \in \mathbb{K}[X]$, $P \circ Q$ est le polynôme

$$P \circ Q = \sum_{k\in\mathbb{N}} a_k Q^k$$

6.2 Propriétés

Composition et degré

Si Q est constant, alors $\forall P \in \mathbb{K}[X]$, $P \circ Q$ est constant. Si P n'est pas nul et Q non-constant, alors

$$\deg(P \circ Q) = \deg P \deg Q$$

Et de plus, $\mathrm{CD}(P \circ Q) = \mathrm{CD}(P)\,\mathrm{CD}(Q)^{\deg Q}$.

En effet, soit $d = \deg P \in \mathbb{N}$, $P = a_0 + a_1 X + \cdots + a_d X^d$ avec $a_d \neq 0$ et $P \circ Q = a_0 + a_1 Q + \cdots + a_d Q^d$. On a alors

$$\begin{aligned} \deg\left(a_d Q^d\right) &= \deg(a_d) + \deg\left(Q^d\right) \\ &= d \deg Q \end{aligned}$$

Et pour $k < d$, $\deg\left(a_k Q^k\right) = k \deg Q < d \deg Q$ donc $\deg(P \circ Q) = d \deg Q$.

Propriétés de la composition à droite Soit Q fixé dans $\mathbb{K}[X]$, alors $\varphi_Q : P \in K[X] \longrightarrow P \circ Q \in \mathbb{K}[X]$ est un morphisme de $\mathbb{K}$-algèbre : $\forall S, T \in \mathbb{K}[X]$, $\forall \alpha \in \mathbb{K}$,
– $\varphi_Q(\alpha S + T) = \alpha \varphi_Q(S) + \varphi_Q(T)$;
– $\varphi_Q(ST) = \varphi_Q(S)\,\varphi_Q(T)$;
– $\varphi_Q(1) = 1$.

En effet, soit $\alpha \in \mathbb{K}$ et $S = \sum_{k=0}^{N} s_k X^k$, $T = \sum_{k=0}^{N} t_k X^k$, alors

$$\begin{aligned} (\alpha S + T) \circ Q &= \left(\sum_{k=0}^{N} (\alpha s_k + t_k) X^k\right) \circ Q \\ &= \sum_{k=0}^{N} (\alpha s_k + t_k) Q^k \\ &= \alpha \sum_{k=0}^{N} s_k Q^k + \sum_{k=0}^{N} t_k Q^k \\ &= \alpha S \circ Q + T \circ Q \end{aligned}$$

De plus,

$$\begin{aligned}(S\circ Q)(T\circ Q) &= \sum_{k=0}^{N} s_k Q^k \sum_{j=0}^{N} t_j Q^j \\ &= \sum_{k=0}^{N}\sum_{j=0}^{N} s_k t_j Q^{k+j} \\ &= \sum_{l=0}^{2N}\left(\sum_{k+j=l} s_k t_j\right) Q^l \quad \text{en convenant } s_m = t_m = 0 \text{ pour } m > N \\ &= (ST)\circ Q\end{aligned}$$

Propriétés diverses

– $X \circ Q = Q$ et

$$\begin{aligned}\left(\prod_{i=1}^{m}(X-a_i)^{\alpha_i}\right)\circ Q &= \prod_{i=1}^{m}(X-a_i)^{\alpha_i}\circ Q \\ &= \prod_{i=1}^{m}((X-a_i)\circ Q)^{\alpha_i} \\ &= \prod_{i=1}^{m}(Q-a_i)^{\alpha_i}\end{aligned}$$

Car $\forall P_1, P_2, \ldots, P_m \in \mathbb{K}[X]$, $(P_1P_2\cdots P_m)\circ Q = (P_1\circ Q)(P_2\circ Q)\cdots(P_m\circ Q)$.

– Pour $P, Q \in \mathbb{K}[X]$, $\widetilde{P\circ Q} = \widetilde{P}\circ\widetilde{Q}$.

Associativité de la composition Pour $P, Q, R \in \mathbb{K}[X]$,

$$P\circ(Q\circ R) = (P\circ Q)\circ R$$

Fixons Q et R, pour $P \in \mathbb{K}[X]$, $P\circ(Q\circ R) = \varphi_{Q\circ R}(P)$ et

$$\begin{aligned}(P\circ Q)\circ R &= \varphi_R(P\circ Q) \\ &= \varphi_R(\varphi_Q(P)) \\ &= \varphi_R\circ\varphi_Q(P)\end{aligned}$$

Il s'agit de montrer que $\varphi_{Q\circ R} = \varphi_R\circ\varphi_Q$. On a $\varphi_{Q\circ R}(X) = Q\circ R$ et $\varphi_R\circ\varphi_Q(X) = Q\circ R$ donc $f = \varphi_{Q\circ R}$ et $g = \varphi_R\circ\varphi_Q$ sont deux morphismes de $\mathbb{K}$-algèbre de $\mathbb{K}[X]$ dans $\mathbb{K}[X]$ tels que $f(X) = g(X)$. Pour $P \in \mathbb{K}[X]$ on écrit $P = \sum_{k\in\mathbb{N}} \lambda_k X^k$ d'où

$$\begin{aligned}f(P) &= \sum_{k\in\mathbb{N}} \lambda_k f\left(X^k\right) \\ &= \sum_{k\in\mathbb{N}} \lambda_k f(X)^k \\ &= \sum_{k\in\mathbb{N}} \lambda_k g(X)^k \\ &= g(P)\end{aligned}$$

Dérivée d'une composition Pour $P, Q \in \mathbb{K}[X]$, $(P\circ Q)' = Q'(P'\circ Q)$.

– On a vu le résultat pour $P = X^m$ [a], $m \in \mathbb{N}$: $(Q^m)' = mQ'Q^{m-1}$ si $m \geqslant 1$ et $\left(Q^0\right)' = 0$.

a. Voir la remarque page 30.

– Pour $P=\sum_{m\in\mathbb{N}}\lambda_m X^m$, $P\circ Q=\sum_{m\in\mathbb{N}}\lambda_m X^m\circ Q$ d'où

$$\begin{aligned}
D(P\circ Q) &= \sum_{m\in\mathbb{N}}\lambda_m D\left(X^m\circ Q\right)\\
&= \sum_{m\in\mathbb{N}}\lambda_m Q'D\left(X^m\right)\circ Q\\
&= Q'\sum_{m\in\mathbb{N}}\lambda_m\left(D\left(X^m\right)\circ Q\right)\\
&= Q'\left(\sum_{m\in\mathbb{N}}\lambda_m D\left(X^m\right)\right)\circ Q\\
&= Q'D\left(\sum_{m\in\mathbb{N}}\lambda_m X^m\right)\circ Q\\
&= Q'\left(P'\circ Q\right)
\end{aligned}$$

Remarque

– Pour $P\in\mathbb{C}[X]$, $t\in\mathbb{R}\longmapsto\widetilde{P}(t)$ est de classe $\mathcal{C}^\infty$ et on a $\forall t\in\mathbb{R}$, $\widetilde{P}'(t)=\widetilde{P'}(t)$. Plus généralement, $\forall t\in\mathbb{R}$ et $\forall k\in\mathbb{N}$, $\widetilde{P}^{(k)}(t)=\widetilde{P^{(k)}}(t)$.

– Pour $P\in\mathbb{K}[X]$, $P\circ X=P$ d'où la notation $P(X)$ au lieu de P.