PCSI - mathématiques

Polynômes à une indéterminée

$\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
Les polynômes sont nécessaires car

- des expressions telles que $a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ prennent un sens lorsqu'on substitue à x des quantités plus générales que des réels ou des complexes (fonctions, suites, endomorphismes, matrices, ..., polynômes !) ;
- lorsque le corps K est "trop petit", p. ex. lorsque $K = \{0_K,\ 1_K\}$, il n'est pas possible de distinguer des fonctions telles que $x \mapsto x^2 - x$, $x \mapsto x^3 + x$, $x \mapsto x^4 - x^2$ ou encore la fonction nulle.

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

On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble des suites à valeurs dans $\mathbb{K}$ et *stationnaires en* 0 :

$$A = (a_n)_{n\in\mathbb{N}} = (a_0,\ a_1, ...,\ a_N,\ 0,\ 0,\ 0,\ ...,\ 0,\ 0,\ ...)\,.$$

$\mathbb{K}^{(\mathbb{N})}$ est muni de l'addition et de la loi externe de $\mathbb{K}^{\mathbb{N}}$, dont on voit facilement qu'il est un sev.

On munit $\mathbb{K}^{(\mathbb{N})}$ de la multiplication définie par : si $A = (a_n)$ et $B = (b_n) \in \mathbb{K}^{(\mathbb{N})}$, $A \times B = C = (c_n)$ où

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

pour tout $n \in \mathbb{N}$. On vérifie que :

- $\times$ est une l.c.i sur $\mathbb{K}^{(\mathbb{N})}$;
- $\times$ est associative et commutative ;
- $\times$ admet pour neutre la suite $e_0 = (1,\ 0,\ 0,\ ...,\ 0,\ 0, ...)$;
- $\times$ est distributive par rapport à $+$.

Alors $\mathbb{K}^{(\mathbb{N})}$, muni de $+$ et $\times$, est un anneau (commutatif).

Définition 1 *On pose* $\mathbb{K}[X] = \left(\mathbb{K}^{(\mathbb{N})},\ +,\ \cdot,\ \times\right)$. $\mathbb{K}[X]$ *est la* $\mathbb{K}$*-algèbre des polynômes à une indéterminée à coefficients dans* $\mathbb{K}$.

1.1 Notation usuelle

Notation 1 *(symbole de Kronecker)*

Si $i,\ j$ sont des objets on note

$$\delta_{i,\ j} = \begin{cases} 1 & \text{si} \quad i = j \\ 0 & \text{si} \quad i \neq j \end{cases}.$$

On définit ensuite le polynôme $e_k = (\delta_{k,\ n})_{n\in\mathbb{N}}$ pour tout $k \in \mathbb{N}$.

Alors pour tout polynôme $A = (a_n)$ on peut écrire

$$A = a_0 e_0 + a_1 e_1 + ... + a_p e_p + ... = \sum a_n e_n \qquad (1)$$

(somme en fait finie, puisque A est stationnaire en 0).

Lemme 1 $e_k \times e_l = e_{k+l}$ *pour tous* $k,\ l \in \mathbb{N}$.

Il en résulte en particulier que $e_1^2 = e_{1+1} = e_2$, $e_1^3 = e_1 e_2 = e_3, ...$, $e_1^n = e_n$ pour tout n.

Notation 2 *On pose*

$$X = e_1.$$

Alors $X^n = e_n$ pour tout n et (1) s'écrit

$$A = a_0 X^0 + a_1 X + ... + a_p X^p + ... = \sum a_n X^n. \qquad (2)$$

1.2 Plongement de $\mathbb{K}$ dans $\mathbb{K}[X]$

Soit l'application $\varphi : \mathbb{K} \to \mathbb{K}[X]\,,\ \lambda \mapsto \lambda e_0 = \lambda X^0$. On vérifie facilement que

- $\varphi(\lambda + \mu) = \varphi(\lambda) + \varphi(\mu)$,
- $\varphi(\lambda\ \mu) = \varphi(\lambda)\ \ \varphi(\mu)$,
- $\varphi(1) = 1_{\mathbb{K}[X]}$,

donc φ est un morphisme d'anneaux.

En outre, φ est injective ($\ker\varphi = \{0\}$) (on dit que φ est un *plongement*). Alors, $\mathbb{K}' = \varphi\langle\mathbb{K}\rangle$ est un sous-anneau de $\mathbb{K}[X]$, φ est un isomorphisme de $\mathbb{K}$ sur $\mathbb{K}'$ et donc $\mathbb{K}'$ est un corps comme $\mathbb{K}$. Compte tenu de φ, on identifie $\mathbb{K}$ et son image $\mathbb{K}'$ par φ en convenant que pour tout $\lambda \in \mathbb{K}$, $\lambda = \varphi(\lambda) = \lambda X^0$. $\mathbb{K}$ devient ainsi un sous-anneau de $\mathbb{K}[X]$ et (2) s'écrit plus simplement

$$A = a_0 + a_1 X + ... + a_p X^p + ... = \sum a_n X^n.$$

1.3 Degré

Il s'agit de préciser où s'arrête la somme précédente, qui est finie pour tout $A \in \mathbb{K}[X]$.

Définition 2 *Le* degré *du polynôme* $A \in \mathbb{K}[X]$ *est*

$$\deg(A) = \begin{cases} -\infty \ \ \textit{si}\ A = 0 \\ \max(p \in \mathbb{N} \mid a_p \neq 0) \ \ \textit{si}\ A \neq 0 \end{cases}$$

Cela signifie que si $A \in \mathbb{K}[X]$ et $\deg(A) \leq n$ alors $A = \sum_{k=0}^{n} a_k X^k$. Plus précisément, si $A \neq 0$ et si $d = \deg(A)$, alors $A = \sum_{k=0}^{d} a_k X^k$ avec $a_d \neq 0$.

Définition 3 *a_d est le* coefficient dominant *du polynôme A. (Il n'est défini que si $A \neq 0$).*

Définition 4 *Le polynôme A* (non nul) *est* unitaire *si son coefficient dominant est égal à 1.*

Proposition 1 (Propriétés du degré) *On a pour tous $A,\ B \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$,*

1. $\deg(A+B) \leq \max(\deg(A),\ \deg(B))$*, avec égalité si* $\deg(A) \neq \deg(B)$ *;*
2. $\deg(\lambda\ A) \leq \deg(A)$*, avec égalité si $\lambda \neq 0$;*
3. $\deg(A \times B) = \deg(A) + \deg(B)$.

Corollaire 1 *L'anneau $\mathbb{K}[X]$ est* intègre.

1.4 Polynômes inversibles

Proposition 2 *Il y a équivalence, pour $A \in \mathbb{K}[X] - \{0\}$, entre*

1. *A est inversible dans l'anneau $\mathbb{K}[X]$;*
2. $\deg(A) = 0$.

L'ensemble des éléments inversibles de l'anneau $\mathbb{K}[X]$ est donc

$$\begin{aligned} \mathcal{U}(\mathbb{K}[X]) &= (\mathbb{K}[X])^* = \mathbb{K}^* \\ &= \{A \in \mathbb{K}[X] \mid \deg(A) = 0\}. \end{aligned}$$

Ces polynômes sont appelés *polynômes constants.*

1.5 Le sev $\mathbb{K}_n[X]$.

On pose pour tout $n \in \mathbb{N}$

$$E_n = \mathbb{K}_n[X] = \{A \in \mathbb{K}[X] \mid \deg(A) \leq n\}.$$

On a donc

- $\mathbb{K}_0[X] = \{A \in \mathbb{K}[X] \mid \deg(A) \leq 0\} = \mathbb{K}$ (polynômes constants) ;
- $\mathbb{K}_1[X] = \{A \in \mathbb{K}[X] \mid \deg(A) \leq 1\}$
  $= \{a_0 + a_1 X \mid a_0, a_1 \in \mathbb{K}\}$; etc.

Il résulte immédiatement des propriétés du degré que :

Proposition 3 *$\mathbb{K}_n[X]$ est un sev du $\mathbb{K}$-ev $\mathbb{K}[X]$.*

Attention, $\mathbb{K}_n[X]$ n'est pas un sous-anneau de $\mathbb{K}[X]$!

1.6 Division euclidienne

Il y a dans $\mathbb{K}[X]$ un théorème analogue à celui de la division euclidienne dans $\mathbb{Z}$.

Théorème 1 (Division euclidienne) *Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$, $B \neq 0$. Il existe un unique couple $(Q,\ R)$ de polynômes tel que*

1. *$A = B \times Q + R$;*
2. $\deg(R) < \deg(B)$.

Q est la quotient, R est le reste dans la division euclidienne de A par B.

Exemple 1 *(et disposition pratique des calculs) :*
$A = X^4 - X^3 + X - 2$ *;* $B = X^2 - 2X + 4$

2 Racines, fonctions polynômes

2.1 Fonction polynôme

Soit E n'importe quelle $\mathbb{K}$-algèbre. Par exemple, $\mathbb{K}$, $\mathbb{K}^{\mathbb{N}}$, $\mathcal{F}(T,\ \mathbb{K})$, $L_{\mathbb{K}}(F)$, $\mathcal{M}_n(\mathbb{K})$, mais aussi pourquoi pas $\mathbb{K}[X]$ lui-même.

Soit $A = \sum a_n X^n$ un polynôme de $\mathbb{K}[X]$. On lui associe la *fonction polynôme*

$$\tilde{A} : \begin{array}{ccl} E & \to & E \\ x & \mapsto & A(x) = \sum a_n\ x^n \end{array}$$

Par exemple :

- Les fonctions polynômes associées aux polynômes constants sont effectivement les fonctions constantes de E dans E,
- $\tilde{1}$ est la fonction constante en 1_E,
- $\tilde{X} = \mathrm{Id}_E$,
- $\widetilde{X^n}$ est la fonction "puissance n" de E dans E.

On vérifie facilement les propriétés suivantes de l'application $X \mapsto \tilde{X}$:

1. $\widetilde{A+B} = \tilde{A} + \tilde{B}$;
2. $\widetilde{\lambda A} = \lambda \tilde{A}$;
3. $\widetilde{A \times B} = \tilde{A} \times \tilde{B}$;
4. $\tilde{1} = 1_{\mathcal{F}(E,E)}$.

Cela signifie que l'application $A \mapsto \tilde{A}$ est un morphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[X]$ dans E. On a en outre la relation :

5. $\tilde{A} \circ \tilde{B} = \widetilde{A(B)}$.

Remarque 1 *Lorsque $E = \mathbb{K}[X]$, et lorsque x est le polynôme X, le calcul de $A(X)$ redonne le polynôme A. Cela explique que l'on rencontre parfois la notation quelque peu redondante $A(X)$ pour désigner simplement A.*

2.2 Division par $X - \alpha$ et racines

Définition 5 *$\alpha \in \mathbb{K}$ est* racine *de $A \in \mathbb{K}[X]$ si $A(\alpha) = 0$.*

Cette définition est la base d'une grande partie de l'arithmétique dans $\mathbb{K}[X]$. En effet, on peut la traduire par un résultat de divisibilité. Si l'on effectue la division euclidienne d'un polynôme A par $X - \alpha$, le reste est de degré < 1, càd est un polynôme constant λ. La constante en question est facile à calculer :

Lemme 2 *Le reste de la division euclidienne de A par $X - \alpha$ est $A(\alpha)$.*

On combine cette remarque avec la définition 5. pour obtenir :

Proposition 4 *α est racine de A dans $\mathbb{K}$* ssi *A est divisible par $X - \alpha$ dans $\mathbb{K}[X]$.*

On peut généraliser ce résultat à plusieurs racines *distinctes* :

Théorème 2 *Soient* α_1, ..., α_n *n scalaires* deux à deux distincts. *Si pour* $i = 1, ..., n$, α_i *est racine de* $A \in \mathbb{K}[X]$,

$$\prod_{i=1}^{n} (X - \alpha_i) \text{ divise } A \text{ dans } \mathbb{K}[X].$$

Ce résultat apporte plusieurs conséquences importantes. Il explique pourquoi les racines d'un polynôme ne peuvent pas être arbitrairement nombreuses par rapport à son degré :

1. Si $A \in \mathbb{K}[X]$, $A \neq 0$, et si A admet n racines distinctes dans $\mathbb{K}$ alors $\deg(A) \geq n$.
2. Si $A \in \mathbb{K}[X]$, si $\deg(A) \leq n$ et si A admet (au moins) $(n+1)$ racines distinctes dans $\mathbb{K}[X]$ alors : $A = 0$.
3. Si $A \in \mathbb{K}[X]$ s'annule sur une partie infinie du corps $\mathbb{K}$ alors : $A = 0$.

2.3 Racines multiples

On souhaite généraliser la définition 5. tout en précisant par quelle puissance de $X - \alpha$ le polynôme A est divisible :

Définition 6 *Soient* $A \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ *et* $m \in \mathbb{N}^*$. *On dit que* α *est racine de* A *d'ordre de multiplicité* m *si*

1. $(X-\alpha)^m$ *divise* A *dans* $\mathbb{K}[X]$;
2. $(X-\alpha)^{m+1}$ *ne divise pas* A *dans* $\mathbb{K}[X]$.

Ces deux conditions sont équivalentes à l'existence d'un polynôme $Q \in \mathbb{K}[X]$ tel que $A = (X-\alpha)^m Q$ et $Q(\alpha) \neq 0$. On peut donner un sens au cas $m = 0$ en convenant qu'une racine d'ordre 0 est une "non-racine".

α est dit racine simple si $m = 1$, double si $m = 2$, triple si $m = 3$ etc.

Pour obtenir une caractérisation des racines multiples, il faut utiliser la dérivation des polynômes.

2.4 Dérivation dans $\mathbb{K}[X]$

La dérivation des polynômes est une opération purement formelle qui consiste simplement à passer d'une suite de coefficients (un polynôme) à une autre.

Définition 7 *Si* $A = \sum a_n X^n \in \mathbb{K}[X]$ *on pose*

$$D(A) = \sum (n+1) a_{n+1} X^n.$$

On vérifie les propriétés suivantes de l'application $D : \mathbb{K}[X] \to \mathbb{K}[X]$:

1. $D(\lambda A + \mu B) = \lambda D(A) + \mu D(B)$ (D est un endomorphisme de $\mathbb{K}[X]$) ;
2. $D(A \times B) = D(A) \times B + A \times D(B)$.

La dernière propriété confère à D son titre de *dérivation* de la $\mathbb{K}$- algèbre $\mathbb{K}[X]$. Il en résulte :

- $D(A^n) = nA^{n-1} D(A)$;
- $D(A(B)) = D(B) \times A'(B)$.

Si $\mathbb{K} = \mathbb{R}$ et si l'on considère les fonctions polynômes de $\mathbb{R}$ dans $\mathbb{R}$, alors la dérivation formelle des polynômes "correspond" à la dérivation des fonctions réelles dans le sens où

$$\left(\tilde{A}\right)' = \widetilde{D(A)}.$$

Ceci justifie de reprendre la notation $A' = D(A)$ chez les polynômes.

On conserve cette même notation pour les dérivations successives. D^n signifiant $\underbrace{D \circ ... \circ D}_{n \text{ "}D\text{"}}$, on note aussi $A'' = D^2(A)$, $A''' = D^3(A)$, ..., $A^{(n)} = D^n(A)$.

On remarque que si $\deg(A) \leq n$, $\deg(A') \leq n-1$, $\deg(A'') \leq n-2$, ..., $\deg\left(A^{(n)}\right) \leq n - n = 0$: $A^{(n)}$ est un polynôme constant dont il est facile de calculer l'unique coefficient (c'est $n! a_n$), et $A^{(p)} = 0$ pour tout $p > n$.

L'identité de dérivation d'un produit peut être généralisée à la dérivation $n^{\text{ième}}$; on obtient :

Théorème 3 (Formule de Leibniz) *Si* $A, B \in \mathbb{K}[X]$,

$$\begin{aligned} D^n(A \times B) &= \sum_{i=0}^{n} \binom{n}{i} A^{(i)} \times B^{(n-i)} \\ &= \sum_{j=0}^{n} \binom{n}{j} A^{(n-j)} \times B^{(j)} \\ &= \sum_{i+j=n} \frac{n!}{i!j!} A^{(i)} \times B^{(j)}. \end{aligned}$$

2.5 Formules de Taylor

Contrairement aux formules de Taylor pour les fonctions dérivables, les formules analogues chez les polynômes ne sont pas des *approximations locales* mais des *identités algébriques* valables sans restriction. Elles expriment le fait qu'un polynôme est entièrement déterminé par la connaissance de ses dérivées en un scalaire quelconque.

Théorème 4 (Formules de Taylor - polynômes) *Si* $P \in \mathbb{K}[X]$ *et* $a \in \mathbb{K}$:

1. $P(X+a) = \sum \frac{P^{(n)}(a)}{n!} X^n$;
2. $P(X+a) = \sum \frac{a^n}{n!} P^{(n)}(X)$;
3. $P(X) = \sum \frac{P^{(n)}(a)}{n!} (X-a)^n$.

Ces formules fournissent enfin une caractérisation des racines multiples :

Théorème 5 *Il y a équivalence, pour* $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ *et* $m \in \mathbb{N}^*$, *entre*

1. α *est racine d'ordre* m *de* P *dans* $\mathbb{K}$;
2. $\begin{cases} P(\alpha) = P'(\alpha) = ... = P^{(m-1)}(\alpha) = 0 \\ P^{(m)}(\alpha) \neq 0 \end{cases}$

Nous sommes prêts maintenant à décomposer les polynômes en produit de facteurs premiers.

3 Arithmétique dans $\mathbb{K}[X]$

Rappelons que $\mathbb{K}[X]$ est un anneau intègre dont les éléments inversibles sont exactement les polynômes de degré 0, càd les polynômes constants non nuls.

Dans toutes les questions de factorisation de ce paragraphe, on considère exclusivement des polynômes non nuls.

Comme dans tout anneau intègre, on dispose dans $\mathbb{K}[X]$ de la relation "divise". Remarquons que si $A \mid B$, alors $\deg(A) \leq \deg(B)$.

Définition 8 *Les polynômes A et B sont dits* associés *si $A \mid B$ et $B \mid A$. On le note $A \sim B$.*

La symétrie de la relation, sous-entendue dans la formulation, est évidente. En fait, la relation d'association est une relation d'équivalence sur $\mathbb{K}[X] - \{0\}$. Donnons-en deux caractérisations :

1. $A \sim B$ *ssi* A est le produit de B par un polynôme inversible ($\lambda \in \mathbb{K}^*$).
2. $A \sim B \Leftrightarrow (A \mid B \text{ et } \deg(A) = \deg(B)) \Leftrightarrow (B \mid A \text{ et } \deg(A) = \deg(B))$.

Remarquons que, parmi les diviseurs d'un polynôme A, figurent toujours les polynômes inversibles (qui divisent tout autre) et les polynômes associés à A.

3.1 Polynômes irréductibles

Définition 9 *Un polynôme $P \in \mathbb{K}[X]$ est dit* irréductible *lorsque*

1. *P est non inversible ;*
2. *Les seuls diviseurs de P sont les inversibles et les associés de P.*

Un polynôme est dit *réductible* s'il n'est pas irréductible.

Un polynôme irréductible est ainsi un polynôme qui a aussi peu de diviseurs que possible. Regardons quelques caractérisations et exemples de cette notion importante :

Proposition 5 *P est irréductible dans $\mathbb{K}[X]$* ssi

1. $\deg(P) \geq 1$ *;*
2. $B \mid P \Rightarrow \deg(B) = 0$ *ou* $\deg(B) = \deg(P)$.

Proposition 6 *P est irréductible dans $\mathbb{K}[X]$* ssi

1. $\deg(P) \geq 1$ *;*
2. $P = A \times B \Rightarrow \deg(A) = 0$ *ou* $\deg(B) = 0$.

Exemple 2

1. *Tout polynôme de degré 1 est irréductible.*
2. Si *un polynôme de degré ≥ 2 admet une racine dans $\mathbb{K}$,* alors *il est réductible dans $\mathbb{K}[X]$.*
3. *Un polynôme de degré 2 ou 3 est irréductible dans $\mathbb{K}[X]$* ssi *il n'admet pas de racine dans $\mathbb{K}$.*
   (a) *$X^2 - 1$ est réductible dans $\mathbb{R}[X]$.*
   (b) *$X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ mais réductible dans $\mathbb{C}[X]$.*
4. (a) *$X^4 - 1$ est réductible dans $\mathbb{R}[X]$ (et dans $\mathbb{C}[X]$).*
   (b) *$X^4 + 1$ n'a pas de racine réelle, mais est réductible dans $\mathbb{R}[X]$.*

La relation d'association partage $\mathbb{K}[X]$ en *classes d'équivalence.* Dans chaque classe de polynômes irréductibles figure un et un seul polynôme *unitaire.*

Définition 10 *Un polynôme* premier *est un polynôme irréductible unitaire.*

On note $\mathcal{P}$ l'ensemble des polynômes premiers de $\mathbb{K}[X]$. On a alors un théorème de décomposition en produit de facteurs premiers dans $\mathbb{K}[X]$ analogue à celui de $\mathbb{Z}$:

Théorème 6 *Soit $A \in \mathbb{K}[X] - \{0\}$. A s'écrit de manière unique*

$$A = \lambda \prod_{P \in \mathcal{P}} P^{m_P}$$

où $\lambda \in \mathbb{K}^*$, et le produit s'étend au nombre fini *des facteurs premiers P pour lesquels $m_P > 0$.*

Comme tout polynôme premier est unitaire, on remarque que λ est nécessairement le coefficient dominant de A. En outre, selon les propriétés du degré, on a $\deg(A) = \sum m_P \deg(P)$.

Cette factorisation donne lieu à des relations particulières lorsqu'elle ne comporte que des polynômes premiers *de degré 1* :

3.2 Polynômes scindés

Définition 11 *Un polynôme $A \in \mathbb{K}[X] - \{0\}$ est dit* scindé *sur $\mathbb{K}$ si sa décomposition ne comporte que des facteurs premiers de degré 1.*

La décomposition d'un tel polynôme s'écrit

$$A = \lambda \prod_{\alpha \in \mathbb{K}} (X - \alpha)^{m_\alpha}$$

où seuls figurent dans le produit les racines α de A, m_α étant la multiplicité correspondante. Autrement dit, m_α est > 0 seulement pour un nombre fini de scalaires qui sont les racines de A. Le degré de A est alors $\sum m_\alpha$. Cela signifie qu'en comptant deux fois les racines doubles, trois fois les racines triples, etc., *un polynôme scindé a autant de racines que son degré.*

3.3 Relations coefficients-racines

Soit $A \in \mathbb{K}[X]$ un polynôme *scindé*. Notons $n = \deg(A)$, $A = \sum_{k=0}^{n} a_k X^k$ et soient x_1, ..., x_n les racines de *A comptées autant de fois que leur multiplicité.*

On définit les *fonctions symétriques élémentaires*[1] :

$$\begin{aligned}
\sigma_1 &= \sum_{1\leq i\leq n} x_i \\
\sigma_2 &= \sum_{1\leq i<j\leq n} x_i x_j \\
&\vdots \\
\sigma_k &= \sum_{1\leq i_1<i_2<\ldots<i_k\leq n} x_{i_1}x_{i_2}\ldots x_{i_k} \\
&\vdots \\
\sigma_n &= \prod_{1\leq i\leq n} x_i
\end{aligned}$$

Comparons les écritures

$$\begin{aligned}
A &= a_n\left(X^n+\frac{a_{n-1}}{a_n}X^{n-1}+\ldots+\frac{a_1}{a_n}X+\frac{a_0}{a_n}\right) \\
&= a_n\left(X-x_1\right)\left(X-x_2\right)\ldots\left(X-x_n\right)
\end{aligned}$$

Si l'on développe la deuxième forme on obtient

$$A=a_n\left(X^n-\sigma_1X^{n-1}+\sigma_2X^{n-2}+\ldots+\left(-1\right)^n\sigma_n\right)$$

Plus généralement, l'identification des coefficients de X^{n-k} donne :

$$\left(-1\right)^k\sigma_k=\frac{a_{n-k}}{a_n}$$

Exemple 3

1. $A=aX^2+bX+c$
2. $A=aX^3+bX^2+cX+d$

3.4 Factorisation dans $\mathbb{C}\left[X\right]$

Proposition 7 *Pour un corps K, il y a équivalence entre les conditions suivantes :*

1. *Tout polynôme de degré ≥ 1 admet au moins une racine dans K ;*
2. *Les polynômes irréductibles de $K\left[X\right]$ sont les polynômes de degré 1 ;*
3. *Les polynômes premiers de $K\left[X\right]$ sont les $X-\alpha$ pour $\alpha\in K$;*
4. *Tout polynôme de $K\left[X\right]$ est scindé sur K.*

Si l'une de ces conditions équivalentes est remplie, on dit que K est *algébriquement clos.* C'est le cas du corps $\mathbb{C}$ des complexes :

Théorème 7 (d'Alembert-Gauss)

$\mathbb{C}$ est algébriquement clos.

Ainsi, tout polynôme de $\mathbb{C}\left[X\right]$ admet la décomposition simple des polynômes scindés, et pour factoriser un polynôme sur $\mathbb{C}$, il est nécessaire et suffisant de connaître ses racines et leurs ordres de multiplicités.

[1] Une fonction *symétrique* est invariante par toute permutation des x_i. Les fonctions σ_i sont fondamentales dans le sens suivant : toute fonction polynômiale symétrique en les x_i admet une expression polynômiale à l'aide des σ_i.

Exemples de factorisations dans $\mathbb{C}\left[X\right]$

- X^n-1 ;
- X^n+1.

Définissons maintenant la conjugaison des polynômes complexes afin de préparer la factorisation sur $\mathbb{R}$ des polynômes : si $A=\sum a_nX^n\in\mathbb{C}\left[X\right]$, le *polynôme conjugué* de A est $\bar{A}=\sum\bar{a}_nX^n$.

On vérifie facilement les propriétés suivantes :

- $\overline{A+B}=\bar{A}+\bar{B}$;
- $\overline{A\times B}=\bar{A}\times\bar{B}$;
- $\overline{\lambda A}=\bar{\lambda}\bar{A}$;
- $\overline{A^n}=\bar{A}^n$;
- $\overline{X-\alpha}=X-\bar{\alpha}$;
- $\overline{\left(X-\alpha\right)^n}=\left(X-\bar{\alpha}\right)^n$;
- $A\in\mathbb{R}\left[X\right]\Leftrightarrow A=\bar{A}$.

3.5 Factorisation dans $\mathbb{R}\left[X\right]$

On a vu des exemples de polynômes irréductibles de degré 2 sur $\mathbb{R}$ qui prouvent que $\mathbb{R}$ n'est pas algébriquement clos. On ne peut donc pas préjuger du degré des polynômes premiers de $\mathbb{R}\left[X\right]$. Toutefois, pour décomposer un polynôme sur $\mathbb{R}$, on peut toujours le décomposer sur $\mathbb{C}$ et regrouper les termes deux à deux conjugués.

Les résultats suivants garantissent que c'est toujours possible :

Proposition 8 *Si $A\in\mathbb{R}\left[X\right]$, si $z\in\mathbb{C}-\mathbb{R}$ et si z est racine de A dans $\mathbb{C}$, $\bar{z}$ l'est également et $X^2-2\Re\left(z\right)X+\left|z\right|^2$ divise A dans $\mathbb{R}\left[X\right]$.*

Proposition 9 *Si $A\in\mathbb{R}\left[X\right]$, si $z\in\mathbb{C}-\mathbb{R}$ et si z est racine d'ordre m de A dans $\mathbb{C}$, $\bar{z}$ l'est également et $\left(X^2-2\Re\left(z\right)X+\left|z\right|^2\right)^m$ divise A dans $\mathbb{R}\left[X\right]$.*

Exemples de factorisations dans $\mathbb{R}\left[X\right]$

- $X^{2n}-1$;
- $X^{2n}+1$;
- $X^{2n+1}-1$;
- $X^{2n+1}+1$.